Manuel d’administration de SafeGuard Enterprise

Manuel d’administration
Version: 8.3

Table des matières

1. À propos de SafeGuard Enterprise..... 11

2. Installation..... 15

2.1 Composants de SafeGuard Enterprise..... 15

2.2 Démarrage..... 19

2.2.1 Quelles sont les étapes essentielles ?..... 20

2.2.2 Compatibilité avec les autres produits Sophos..... 22

2.3 Configuration du serveur SafeGuard Enterprise..... 23

2.3.1 Conditions préalables..... 23

2.3.2 Installation et configuration des services Internet (IIS) de Microsoft..... 24

2.3.3 Installation du serveur SafeGuard Enterprise..... 27

2.4 Configuration de la base de données SafeGuard Enterprise..... 28

2.4.1 Authentification de la base de données..... 29

2.4.2 Génération de la base de données SafeGuard Enterprise..... 33

2.4.3 Modification des droits d’accès à la base de données SafeGuard Enterprise..... 35

2.4.4 Vérification des services SQL, des canaux nommés et des paramètres TCP/IP..... 35

2.4.5 Création d’une règle de pare-feu Windows sur Windows Server..... 36

2.4.6 Configuration de l’authentification Windows pour la connexion au serveur SQL..... 37

2.5 Installation de SafeGuard Management Center..... 38

2.5.1 Conditions préalables..... 38

2.5.2 Installation de SafeGuard Management Center..... 39

2.5.3 Configuration de SafeGuard Management Center..... 39

2.5.4 Installation de la structure organisationnelle dans SafeGuard Management Center..... 45

2.5.5 Importation du fichier de licence..... 47

2.6 Test de la communication..... 47

2.6.1 Ports/connexions..... 47

2.6.2 Méthode d’authentification..... 48

2.6.3 Définition des paramètres du serveur proxy..... 48

2.6.4 Vérification de la connexion..... 49

2.7 Sécurisation des connexions de transport avec SSL..... 49

2.7.1 Certificats..... 50
2.7.2 Activation du chiffrement SSL dans SafeGuard Enterprise..... 51
2.7.3 Configuration de la page Web SGNSRV pour utiliser SSL..... 52
2.7.4 Configuration des terminaux pour l’utilisation de SSL..... 53
2.7.5 Assignation du certificat SSL aux terminaux Windows..... 53
2.7.6 Importation du certificat SSL sur les Macs..... 54
2.8 Enregistrement et configuration du serveur SafeGuard Enterprise..... 55
2.8.1 Enregistrement et configuration du serveur SafeGuard Enterprise pour l’ordinateur en cours d’utilisation..... 56
2.8.2 Enregistrement et configuration du serveur SafeGuard Enterprise pour un ordinateur différent..... 56
2.8.3 Modification des propriétés du serveur SafeGuard Enterprise..... 57
2.8.4 Enregistrement du serveur SafeGuard Enterprise avec le pare-feu Sophos activé..... 59
2.9 Création des packages de configuration..... 59
2.9.1 Création d’un package de configuration pour les terminaux..... 59
2.9.2 Création d’un package de configuration pour les ordinateurs non administrés (Windows uniquement)..... 60
2.10 Configuration de SafeGuard Enterprise sur les terminaux..... 61
2.10.1 À propos des terminaux administrés et non administrés..... 62
2.10.2 Restrictions..... 62
2.10.3 Vérification de la disponibilité du certificat SSL sur les terminaux Windows..... 63
2.10.4 Préparation pour la prise en charge du Chiffrement de lecteur BitLocker..... 64
2.10.5 Préparation de SafeGuard Full Disk Encryption avec l’authentification au démarrage..... 64
2.10.6 Préparation pour le stockage Cloud..... 66
2.11 Installation du logiciel de chiffrement sur Windows..... 66
2.11.1 Installation des packages et fonctions..... 67
2.11.2 Installation locale du logiciel de chiffrement..... 69
2.11.3 Installation centralisée du logiciel de chiffrement..... 70
2.11.4 Installations sur les disques durs à chiffrement automatique compatibles Opal..... 77
2.12 Installation du logiciel de chiffrement sur macOS..... 78
2.12.1 Installation automatisée de SafeGuard Native Device Encryption..... 79
2.12.2 Installation manuelle de SafeGuard Native Device Encryption..... 80

2.12.3 Installation automatisée de SafeGuard File Encryption..... 81
2.12.4 Installation manuelle de SafeGuard File Encryption.....81
2.13 Installation de Web Helpdesk.....82
2.13.1 Configuration requise du serveur..... 83
2.13.2 Configuration du serveur Web avec SSL/TLS.....83
2.13.3 Langues prises en charge.....84
2.14 À propos de la mise à niveau.....84
2.14.1 Mise à niveau de SafeGuard Management Center..... 85
2.14.2 Mise à niveau du serveur SafeGuard Enterprise et de Web Helpdesk.....86
2.14.3 Mise à niveau des terminaux.....86
2.14.4 Mise à niveau des packages de configuration des terminaux.....87
2.15 À propos de la migration.....88
2.15.1 Modification de l’installation de SafeGuard sur les terminaux..... 88
2.15.2 Migration des terminaux vers un autre système d’exploitation.....89
3. SafeGuard Management Center.....90
3.1 Connexion à SafeGuard Management Center..... 91
3.1.1 Connexion en mode indépendant..... 91
3.2 Interface utilisateur de SafeGuard Management Center.....91
3.2.1 Paramètres de langue..... 94
3.2.2 Vérification de l’intégrité de la base de données..... 95
3.3 Utilisation de stratégies..... 95
3.3.1 Création de stratégies.....95
3.3.2 Modification des paramètres de stratégie..... 96
3.3.3 Groupes de stratégies.....97
3.3.4 Sauvegarde de stratégies et de groupes de stratégies..... 99
3.3.5 Restauration de stratégies et de groupes de stratégies.....100
3.3.6 Assignation des stratégies.....100
3.3.7 Gestion des stratégies dans Utilisateurs et ordinateurs.....102
3.4 Utilisation des packages de configuration.....102
3.4.1 Création d’un package de configuration pour les terminaux.....103
3.4.2 Création d’un package de configuration pour les terminaux non administrés..... 105
3.4.3 Création d’un package de configuration pour les Macs..... 106

3.5 Authentification renforcée : le groupe .Utilisateurs non confirmés....107
3.5.1 Confirmation des utilisateurs....108
3.5.2 Confirmation automatique des utilisateurs....109
3.6 Assignation utilisateur/machine....109
3.6.1 Types d’utilisateur....110
3.6.2 Assignation utilisateur machine dans SafeGuard Management Center....111
3.6.3 Assignation de groupes d’utilisateurs et d’ordinateurs....115
3.7 Amélioration de Sophos SafeGuard par envoi de données d'utilisation anonymes....116
3.7.1 Création d’une stratégie pour désactiver l’envoi de données d’utilisation anonymes....117
3.8 SafeGuard Management Center : options avancées....117
3.8.1 Maintenance de la base de données....117
3.8.2 Utilisation de plusieurs configurations de base de données (mutualisées)....118
3.8.3 Avertissement à l'expiration du certificat d'entreprise....125
3.8.4 Recherche d’utilisateurs, d’ordinateurs et de groupes dans la base de données SafeGuard Enterprise....125
3.8.5 Affichage des propriétés d’objet dans Utilisateurs et ordinateurs....126
3.8.6 Désactivation du déploiement de stratégies....127
3.8.7 Règles d’assignation et d’analyse des stratégies....127
3.8.8 Données d’inventaire et d’état....134
3.8.9 Responsables de la sécurité de SafeGuard Enterprise....141
3.8.10 Gestion de la structure organisationnelle....161
3.8.11 Clés et certificats....173
3.8.12 Ordres de changement du certificat d’entreprise (CCO)....185
3.8.13 Licences....189
3.8.14 Tokens et cartes à puce....195
3.8.15 Planification des tâches....214
3.8.16 Audit....225
3.8.17 Types de stratégie et champs d’application....253
3.8.18 Réparation d’une installation corrompue de SafeGuard Management Center....306
3.8.19 Résolution des problèmes....307
4. Administration des terminaux Windows....321
4.1 Gestion du Chiffrement de lecteur BitLocker....321

4.1.1 Authentification avec le Chiffrement de lecteur BitLocker.....322
4.1.2 Bon usage : paramètres des stratégies et expérience utilisateur..... 324
4.1.3 Conditions préalables à la gestion de BitLocker sur les terminaux.....326
4.1.4 Gestion du Chiffrement de lecteur BitLocker avec SafeGuard Enterprise..... 327
4.1.5 Chiffrement avec BitLocker géré par SafeGuard Enterprise.....328
4.1.6 BitLocker To Go.....332
4.1.7 Récupération des terminaux chiffrés avec BitLocker.....333
4.2 Chiffrement de fichiers par emplacement..... 336
4.2.1 Configuration des règles de chiffrement dans les stratégies de chiffrement de fichiers par emplacement..... 337
4.2.2 Configuration des paramètres de chiffrement des fichiers par emplacement dans les stratégies Paramètres généraux.....344
4.2.3 Complément Outlook pour le chiffrement par emplacement..... 346
4.2.4 Utilisation de plusieurs stratégies de chiffrement de fichiers par emplacement..... 349
4.2.5 Évaluation des règles de chiffrement de fichiers par emplacement sur les terminaux.....349
4.2.6 Conflit entre les règles de chiffrement de fichiers par emplacement.....350
4.2.7 Chiffrement de fichiers par emplacement et SafeGuard Data Exchange.....350
4.3 Stockage Cloud.....351
4.3.1 Conditions requises pour le logiciel de stockage Cloud.....351
4.3.2 Création de définitions de stockage Cloud.....352
4.3.3 Création d’une stratégie de protection des périphériques avec une définition Stockage Cloud.....357
4.4 SafeGuard Data Exchange.....358
4.4.1 Bon usage.....359
4.4.2 Clés de groupe..... 365
4.4.3 Clés locales..... 365
4.4.4 Phrase secrète des supports..... 366
4.4.5 Configuration des applications fiables et ignorées pour SafeGuard Data Exchange.....367
4.4.6 Configuration des périphériques ignorés pour SafeGuard Data Exchange.....368
4.4.7 Configuration du chiffrement permanent pour SafeGuard Data Exchange..... 369
4.4.8 SafeGuard Data Exchange et File Encryption.....369
4.5 SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique..... 369

4.5.1 Comment SafeGuard Enterprise intègre-t-il les disques durs compatibles Opal ?....370
4.5.2 Amélioration des disques durs compatibles Opal avec SafeGuard Enterprise....370
4.5.3 Administration avec SafeGuard Enterprise des terminaux équipés de disques durs compatibles Opal....371
4.5.4 Chiffrement de disques durs compatibles Opal....371
4.5.5 Verrouillage des disques durs compatibles Opal....371
4.5.6 Autorisation de déverrouillage des disques durs compatibles Opal aux utilisateurs....372
4.5.7 Journalisation des événements pour les terminaux équipés de disques durs compatibles Opal....372
4.6 SafeGuard Configuration Protection....372
4.7 À propos de la désinstallation....373
4.7.1 Désinstallation....373
4.7.2 Interdiction de la désinstallation sur les terminaux....374
5. Administration des terminaux Mac....375
5.1 Création d'un package de configuration pour les Macs....375
5.2 À propos de SafeGuard Native Device Encryption pour Mac....376
5.2.1 Gestion des terminaux FileVault 2 avec SafeGuard Management Center....376
5.2.2 Stratégies de chiffrement pour le chiffrement intégral du disque FileVault 2....377
5.2.3 Stratégies....377
5.2.4 Fonctionnement du chiffrement....378
5.2.5 Chiffrement initial....378
5.2.6 Déchiffrement....379
5.2.7 Ajout d'un utilisateur FileVault 2....379
5.2.8 Suppression d'un utilisateur FileVault 2....380
5.2.9 Synchronisation avec le serveur backend....380
5.2.10 Options de ligne de commande....381
5.2.11 Clé de secours pour terminaux Mac....383
5.2.12 Gestion de la clé de récupération....384
5.2.13 Gestion des mots de passe....385
5.3 À propos de Sophos SafeGuard File Encryption pour Mac....385
5.3.1 Options de configuration administrées centralement....389

5.3.2 Stratégies....389
5.3.3 Chiffrement de fichiers dans le stockage Cloud....389
5.3.4 Chiffrement initial....392
5.3.5 Permutation rapide d'utilisateur....393
5.3.6 Utilisation de clés locales....393
5.3.7 Options de ligne de commande....393
5.3.8 Utilisation de Time Machine....397
5.3.9 Utilisation des supports multimédia amovibles....398
5.4 Résolution des problèmes....399
5.4.1 Réinitialisation en cas d’oubli du mot de passe....399
5.4.2 Problèmes d'accès aux données....400
5.4.3 Problèmes d’utilisation des machines virtuelles....401
5.4.4 Fichiers récupérés par SafeGuard....401
5.4.5 Token sécurisé manquant....401
5.5 Données d'inventaire et d'état des Mac....401
5.6 Désinstallation du Chiffrement de périphériques des terminaux Mac....402
5.7 Désinstallation du Chiffrement de fichiers des terminaux Mac....403
6. Synchronized Encryption....404
6.1 Bon usage : support multi-clés pour Synchronized Encryption....405
6.1.1 Création d’une stratégie de chiffrement de fichiers à plusieurs clés....405
6.2 Configuration requise....407
6.2.1 Installation des terminaux....408
6.2.2 Mise à niveau des terminaux....408
6.2.3 Migration à partir du module de Chiffrement de fichiers sur Windows....408
6.2.4 Migration à partir du module de Chiffrement de fichiers sur macOS....410
6.2.5 Déploiement partiel de Synchronized Encryption....411
6.3 Chiffrement des données....414
6.3.1 Clé Synchronized Encryption....415
6.3.2 Chiffrement automatique des fichiers conformément à la stratégie de chiffrement asynchrone....415
6.3.3 Listes d’application....417
6.3.4 Chiffrement initial....419

6.3.5 Création de stratégies pour le chiffrement de fichiers par application..... 422
6.4 Complément Outlook pour Synchronized Encryption.....433
6.4.1 Création de stratégies pour l’activation du complément Outlook de SafeGuard Enterprise.....433
6.5 Intégration avec Sophos Central Endpoint Protection.....435
6.5.1 Création de stratégies pour supprimer les clés sur les machines compromises..... 436
6.6 Partage du jeu de clés SafeGuard Enterprise avec les appareils mobiles administrés par Sophos Mobile.....436
6.6.1 Configuration de la synchronisation du jeu de clés.....437
6.7 Configuration des applications sécurisées et des appareils ignorés.....439
6.7.1 Configuration des applications sécurisées pour le chiffrement de fichiers par application.....439
6.7.2 Configuration des périphériques ignorés.....440
6.8 Stratégies de Chiffrement de fichiers par application dans le RSOP..... 441
7. Gestion avancée.....442
7.1 Conseils pratiques..... 442
7.1.1 Déploiement..... 442
7.1.2 Serveur backend.....447
7.1.3 Stratégies..... 448
7.1.4 Terminaux : toutes les plates-formes.....451
7.1.5 Terminaux Windows.....454
7.1.6 Terminaux macOS..... 455
7.2 Recommandations en matière de sécurité..... 456
7.3 Réplication de la base de données SafeGuard Enterprise..... 458
7.4 Web Helpdesk.....459
7.4.1 Portée de Web Helpdesk..... 460
7.4.2 Autorisation de connexion à Web Helpdesk pour les utilisateurs sans SafeGuard Enterprise.....461
7.4.3 Authentification.....464
7.4.4 Récupération pour les terminaux administrés (clients SafeGuard Enterprise administrés).....466
7.4.5 Récupération à l’aide de clients virtuels.....470
7.4.6 Récupération pour les terminaux non administrés (clients Sophos SafeGuard autonomes).....474

7.4.7 Journalisation des événements de Web Helpdesk..... 477
7.5 Récupération.....478
7.5.1 Flux de travail Challenge/Réponse.....478
7.5.2 Lancement de l’assistant de récupération.....479
7.5.3 Récupération par appareils mobiles.....479
7.6 Outils..... 480
7.6.1 Outil « Client/Server Connectivity Check » pour Windows..... 480
7.6.2 Affichage des stratégies Synchronized Encryption sur les terminaux.....481
7.6.3 Affichage de l’état du système avec SGNState.....483
7.6.4 Annulation d’une installation en échec avec SGNRollback.....485
7.6.5 Récupération de l'accès aux ordinateurs à l'aide de l'outil KeyRecovery..... 488
7.6.6 Restauration des systèmes de chiffrement intégral du disque SafeGuard Windows BIOS..... 488
7.6.7 Restauration des systèmes de Challenge/Réponse Windows UEFI BitLocker.....492
7.6.8 Mise hors service de volumes chiffrés..... 494
7.6.9 Mise hors service de disques durs à chiffrement automatique compatibles Opal..... 497
8. Support technique.....499
9. Mentions légales..... 500

1. À propos de SafeGuard Enterprise

SafeGuard Enterprise est une solution de sécurité des données complète qui utilise une stratégie de chiffrement pour assurer une protection fiable des données sur les postes de travail, les partages réseau et les appareils mobiles. Elle permet aux utilisateurs de partager en toute sécurité leurs informations et de travailler sur des fichiers présents sur des appareils Windows, macOS, iOS et Android à l'aide de l'app Sophos Secure Workspace. Retrouvez plus de renseignements à la section Composants de SafeGuard Enterprise *(page 15)*.

SafeGuard Management Center vous permet d'administrer les stratégies de sécurité, les clés et les certificats à l'aide d'une stratégie d'administration déléguée. Les journaux et rapports détaillés vous garantissent d'être toujours informé 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.

Synchronized Encryption : chiffrement de fichiers par application

Synchronized Encryption a été conçu à partir de deux choses évidentes : toutes les données sont importantes et doivent être protégées (chiffrées) et le chiffrement doit être appliqué en permanence où que se trouvent les données. En outre, les données importantes doivent être chiffrées automatiquement et de manière transparente pour l'utilisateur afin qu'il n'ait pas à décider si un fichier est assez important pour devoir être chiffré ou non. Cette hypothèse fondamentale appelant à protéger toutes les données importantes permet de garantir que toutes les données sont chiffrées sans qu'aucune intervention de l'utilisateur ne soit nécessaire. Ceci permet de maintenir la productivité de l'utilisateur qui peut continuer à travailler sereinement en sachant que ses données sont sécurisées. Retrouvez plus de renseignements à la section Synchronized Encryption *(page 404)*.

Chiffrement de fichiers par emplacement

- **Stockage Cloud**

  Les services de stockage dans le Cloud sont très utiles pour aider les utilisateurs à récupérer leurs données où qu'ils soient et quel que soit le type d'appareils qu'ils utilisent. Bien qu'il soit important d'améliorer la productivité des utilisateurs, il est tout aussi crucial de garantir que vos informations sensibles restent sécurisées une fois qu'elles sont transférées dans le Cloud. SafeGuard Enterprise chiffre et déchiffre automatiquement et en toute transparence les fichiers au fur et à mesure qu'ils sont chargés ou téléchargés du Cloud.

  - Chiffre tous les fichiers transférés dans les services de stockage dans le Cloud

- Permet le partage sécurisé des données partout
- Détecte et supporte automatiquement les services de stockage dans le Cloud tels que Box, Dropbox, OneDrive et Egnyte
- Lit les fichiers chiffrés grâce à notre application gratuite Sophos Secure Workspace pour iOS et Android.

- **Chiffrement de fichiers**

  Le chiffrement ne sert pas seulement à maintenir les données à l'abri des regards indiscrets en dehors de votre entreprise. Il permet également la collaboration sécurisée et le contrôle des fichiers au sein de l'entreprise. SafeGuard Enterprise va au-delà des simples permissions d'accès, garantissant que seules les personnes autorisées puissent lire les fichiers sur réseau tout en permettant au service informatique de gérer les fichiers et les sauvegardes.

  - Configure le chiffrement des fichiers pour les dossiers partagés
  - Garantit que seuls certains utilisateurs ou groupes ont accès aux données.
  - Ne requiert aucune interaction avec vos utilisateurs.
  - Fournit une couche supplémentaire de protection en cas de transfert de vos serveurs de l'entreprise dans le Cloud.

- **Échange de données**

- SafeGuard Enterprise assure le chiffrement automatique et transparent des fichiers sur les supports amovibles de type clés USB, cartes mémoire ou CD/DVD.

  - Vous pourrez facilement partager vos données chiffrées sur les supports amovibles au sein de votre entreprise sans impacter vos utilisateurs
  - L'utilisation d'une application amovible et d'un mot de passe permet aux utilisateurs ne se servant pas de SafeGuard Enterprise de partager en toute facilité et en toute sécurité les supports/périphériques amovibles chiffrés
  - La mise sur liste blanche des supports amovibles permet une plus grande facilité et souplesse d'administration du chiffrement.

Chiffrement intégral du disque avec BitLocker

Vous permet de gérer BitLocker sur les terminaux Windows 8.1 et Windows 10.

Protection de vos Macs

Les données sur Mac sont tout aussi précieuses que celles sur PC. C’est pourquoi il est vital d’inclure vos systèmes Mac dans votre stratégie de chiffrement des données. SafeGuard Enterprise protège vos Mac grâce au chiffrement des fichiers et des disques et garantit que les données sur vos Mac sont sécurisées en permanence. Il inclut les fonctions de chiffrement pour les supports amovibles, les partages de fichiers réseau et pour le Cloud sur Mac.

- Permet de gérer le chiffrement des fichiers ou des disques pour les Mac via le même Management Center que les autres appareils.
- Gère les appareils chiffrés avec FileVault 2
- Fonctionne en tâche de fond sans affecter les performances
- Offre une visibilité complète et des rapports sur l’état de chiffrement

Les modules mentionnés ci-dessous sont disponibles pour les terminaux Mac.

	Synchronized Encryption **- Par application**	**Sophos SafeGuard File Encryption** **- Par emplacement**	**Sophos SafeGuard Native Device Encryption** **- Gestion FileVault 2**
macOS 10.13	**OUI**	**OUI**	**OUI**
macOS 10.14	**OUI**	**OUI**	**OUI**
macOS 10.15	**OUI**	**OUI**	**OUI**

Sophos Secure Workspace

Les clés de chiffrement du jeu de clés SafeGuard Enterprise peuvent être mises à disposition dans l’app Sophos Secure Workspace (SSW) administrée par Sophos Mobile. Les utilisateurs de l’app peuvent alors utiliser les clés pour déchiffrer et consulter les documents ou pour chiffrer

des documents. Ces fichiers peuvent être partagés en toute sécurité entre tous les utilisateurs de SafeGuard Enterprise et de Sophos Secure Workspace. Retrouvez plus de renseignements dans la documentation de Sophos Secure Workspace.

2. Installation

La disponibilité des fonctions dépend de votre type de licence. Veuillez contacter votre Partenaire commercial pour obtenir plus de renseignements sur ce qui est inclus dans votre licence.

2.1 Composants de SafeGuard Enterprise

Une base de données Microsoft SQL stocke les informations relatives aux clients (terminaux) sur le réseau d'entreprise. Le responsable principal de la sécurité (MSO, Master Security Officer), utilise SafeGuard Management Center pour gérer le contenu de la base de données et créer des instructions de sécurité (stratégies).

Les terminaux lisent les stratégies dans la base de données et lui envoient des rapports. La communication entre la base de données et les terminaux est maintenue par le serveur Web des services Internet (IIS) sur lequel le serveur SafeGuard Enterprise est installé.

SafeGuard Enterprise Web Helpdesk est un composant optionnel qui offre une solution Web de récupération des clients administrés.

SafeGuard Enterprise est composé de trois modules principaux :

- Serveur backend
- Logiciels pour terminaux Windows
- Logiciels pour terminaux macOs

Chaque module contient plusieurs composants.

SafeGuard Enterprise Backend BKD Le serveur backend fournit les stratégies d'administration des terminaux SafeGuard Enterprise. Il est composé de :	
Srv	**Serveur SafeGuard Enterprise** : Il est maintenu à jour par un serveur Web IIS (Internet Information Services) et gère la communication entre la base de données et les terminaux. Package d'installation SGNServer.msi. Le serveur SafeGuard Enterprise exécute une application sur un serveur Web des services Internet (IIS) de Microsoft et autorise la communication entre la base de données SafeGuard Enterprise et le terminal SafeGuard Enterprise. Sur demande, le serveur SafeGuard Enterprise envoie les paramètres de stratégie aux terminaux. .NET Framework 4.5 et ASP.NET 4.5 sont requis.

	Lorsque SSL est la méthode de chiffrement du transport pour la communication du serveur client, veuillez installer le rôle *Authentification de base*. Il inclut deux sous-composants :
	Web Helpdesk (facultatif) **WHD** Web Heldesk est une solution Web de récupération pour les clients administrés. Grâce à un mécanisme de Challenge/Réponse convivial, Web Helpdesk aide les utilisateurs qui ne peuvent pas se connecter ou qui ne peuvent pas accéder aux données chiffrées de SafeGuard Enterprise comme indiqué à la section Web Helpdesk *(page 459)*.
	Planificateur de tâches du serveur **STS** SafeGuard Management Center inclut le **Planificateur de tâches** permettant de créer et de planifier des tâches périodiques basées sur des scripts. Par exemple ; pour synchroniser Active Directory et SafeGuard Enterprise Management Center. Les tâches sont automatiquement exécutées par un service sur le serveur SafeGuard Enterprise pour exécuter les scripts spécifiées.
MC	**SafeGuard Management Center** Le responsable principal de la sécurité (MSO, Master Security Officer), utilise SafeGuard Management Center pour gérer le contenu de la base de données et créer des instructions de sécurité (stratégies). Outil d'administration centralisée pour les terminaux protégés par SafeGuard Enterprise, la gestion des clés et des certificats, les utilisateurs et les ordinateurs et la création des stratégies SafeGuard Enterprise. SafeGuard Management Center communique avec la base de données SafeGuard Enterprise. .NET Framework 4.5 est requis. Package d'installation SGNManagementCenter.msi
	Mode mutualisé **MTM** Le package d'installation de SafeGuard Management Center offre une option d'installation en mode mutualisé.

	Si vous choisissez cette option, SafeGuard Management Center prend en charge plusieurs bases de données via les configurations mutualisées de base de données (Multi Tenancy). Vous pouvez créer et maintenir à jour différentes bases de données SafeGuard Enterprise pour différents locataires tels que les différents locaux d'une d'entreprise, les différents unités organisationnelles ou les différents domaines. Pour chaque base de données (le locataire), vous devez configurer une instance séparée de SafeGuard Enterprise. Chaque base de données doit avoir la même version. Par exemple, il n'est pas possible d'administrer les bases de données SGN 7 et les bases de données SGN 8.3 uniquement avec la version 8.3 de Management Center.
DB	**Base de données SafeGuard Enterprise** 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. La base de données est accessible via le serveur SafeGuard Enterprise et uniquement par un seul responsable de la sécurité via SafeGuard Management Center, généralement le responsable principal de la sécurité. Les bases de données SafeGuard Enterprise peuvent être générées et configurées à l'aide d'un assistant ou de scripts. Vous pouvez créer la base de données au cours de la première configuration de SafeGuard Management Center à l'aide de l'assistant ou d'un script et établir manuellement la connexion entre SafeGuard Management Center, la base de données et le serveur SafeGuard Enterprise.

- **Service Microsoft Active Directory** (facultatif) :

  Vous pouvez importer la structure organisationnelle de votre entreprise avec les utilisateurs et les ordinateurs depuis Active Directory.

Terminaux Windows WinClient

SafeGuard Enterprise fournit des packages d'installation pour le chiffrement intégral des disques et le chiffrement de fichiers.

Selon vos besoins, vous pouvez choisir entre plusieurs packages de chiffrement de fichiers. Vous devez déterminer si vous voulez chiffrer tous les fichiers enregistrés par des applications spécifiques sur tout l'ordinateur (par application) ou si vous voulez chiffrer les fichiers à certains emplacements uniquement (par emplacement).

Vous ne pouvez pas installer Synchronized Encryption (par application) et les packages de chiffrement par emplacement (CS, FE, DX) sur un seul ordinateur.

Les terminaux protégés par SafeGuard Enterprise peuvent soit être connectés à un serveur SafeGuard Enterprise (administré), soit être utilisés sans aucune connexion à un serveur SafeGuard Enterprise (non administré). Les terminaux administrés reçoivent leurs stratégies directement du serveur SafeGuard Enterprise. Les terminaux non administrés reçoivent leurs stratégies et les mises à jour dans des packages de configuration qui doivent être installés sur les ordinateurs.

CBM	**Module de base client** Le Module de base client offre les services essentiels et les modules d'authentification.
BL	**BitLocker** (Chiffrement d'appareils de Windows) Vous permet de gérer BitLocker sur les terminaux Windows 8.1 et Windows 10.
SyncEnc	**Synchronized Encryption** Chiffre les fichiers quel que soit leur emplacement. (par application). Vous pouvez définir une liste des applications pour lesquelles les fichiers seront chiffrés automatiquement.
CS	**Stockage Cloud** Offre le chiffrement basé sur fichier des données stockées dans le Cloud (par emplacement).
FE	**Chiffrement de fichiers** Offre le chiffrement basé sur fichier sur les lecteurs locaux et les emplacements réseau, surtout pour les groupes de travail et les partages réseau.
DX	**Échange de données** Offre le chiffrement de données stockées sur des supports amovibles connectés à un ordinateur afin d'échanger ces données avec d'autres utilisateurs Windows en toute sécurité.

Terminaux macOS macClient

SafeGuard Enterprise fournit des packages d'installation pour l'administration du chiffrement intégral des disques FileVault 2 et du chiffrement de fichiers. Si vous voulez chiffrer les fichiers et les partager avec les terminaux Windows, vous devez utiliser SafeGuard File Encryption pour macOS.

FV2	**FileVault 2** (SafeGuard Native Device Encryption pour Mac) Vous permet d’administrer FileVault2 sur les Macs.
macOSFE	**SafeGuard File Encryption** Offre le chiffrement des fichiers sur les lecteurs locaux, les partages réseaux, les lecteurs amovibles et dans le Cloud. SafeGuard File Encryption pour Mac vous permet de chiffrer et de déchiffrer les fichiers puis d’échanger ces fichiers avec d’autres utilisateurs sur les ordinateurs Macs ou Windows. Pour lire les fichiers chiffrés par SafeGuard Enterprise sur des appareils mobiles, veuillez utiliser Sophos Secure Workspace pour iOS ou Android.

Conseils d’utilisation

Pour bénéficier de performances optimales, veuillez prendre en compte ce qui suit lors du positionnement des composants sur le réseau :

- SafeGuard Enterprise Management Center doit être aussi près que possible de la base de données SQL.
- Il en va de même pour SafeGuard Enterprise Server.
- Ces deux composants doivent pouvoir accéder à un contrôleur de domaine sur le même réseau afin de garantir une synchronisation rapide d’Active Directory avec SafeGuard Enterprise.

2.2 Démarrage

Cette section vous guide tout au long des étapes d’installation de SafeGuard Enterprise en vous donnante des exemples et des conseils d’utilisation. Elle s’adresse aux administrateurs système/réseau/base de données qui installent SafeGuard Enterprise (SGN) et décrit une installation qui fournira une sécurité et des performances optimales en matière de communication entre les composants individuels.

Ce document décrit une situation de domaine dans laquelle toutes les machines appartiennent au même domaine. En conséquence, les tâches spécifiques peuvent varier lors de l’utilisation d’autres logiciels ou d’un autre environnement de groupe de travail.

- Première installation : le Conseiller d’installation SGN simplifie la première installation des composants d’administration, notamment les stratégies par défaut. Pour lancer le Conseiller

d’installation SGN pour procéder à une nouvelle installation de SafeGuard Enterprise, démarrez SGNInstallAdvisor.bat fourni avec le produit. Un assistant vous guide tout au long de l’installation.

- Mise à jour de l’installation : veuillez suivre les étapes décrites ci-dessous : À propos de la mise à niveau *(page 84)*.

2.2.1 Quelles sont les étapes essentielles ?

Avant de déployer le client SafeGuard Enterprise, il est indispensable de disposer d’un backend en état de fonctionnement. Par conséquent, nous vous conseillons de respecter les étapes d’installation décrites ci-dessous.

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

Étape	Description	Package à installer / outil à utiliser
1	Vérification de la configuration système requise Retrouvez plus de renseignements sur la configuration matérielle et logicielle requises, sur les Service Packs et l’espace disque requis au cours de l’installation et sur le mode de fonctionnement optimal sur la page des Notes de publication de SafeGuard.	S/O
2	Téléchargement des programmes d’installation Utilisez l’adresse Web et les codes d’accès de téléchargement fournis par votre administrateur système pour télécharger les programmes d’installation sur le site Web de Sophos. Placez-les à un emplacement auquel vous pouvez accéder pour effectuer l’installation. Retrouvez plus de renseignements dans l’article 111195 de la base de connaissances de Sophos.	N/A
3	Assurez-vous que les plus récentes mises à jour Windows ont été appliquées sur le serveur Windows. Installez .NET Framework et d’ASP.NET 4.6.1	N/A

Étape	Description	Package à installer / outil à utiliser
4	Installez les services Internet (IIS) pour SafeGuard Enterprise comme indiqué à la section Installation et configuration des services Internet (IIS) de Microsoft *(page 24)* et installez le rôle *Authentification de base*.	N/A
	Retrouvez plus de renseignements sur le rôle d'Authentification de base dans le document de Microsoft Authentification de base. Assurez-vous que .NET Framework 4.5 est installé sur tous les ordinateurs sur lesquels vous voulez installer les composants SafeGuard Enterprise.	
5	Installez le serveur SafeGuard Enterprise.	SGNServer.msi
6	Configurez l'authentification de la base de données Microsoft SQL Server pour le responsable principal de la sécurité de SafeGuard Enterprise comme indiqué à la section Authentification de la base de données *(page 29)*.	N/A
7	**Facultatif** : Générez les bases de données SafeGuard Enterprise à l'aide d'un script. L'assistant de configuration de SafeGuard Management Center peut créer la base de données automatiquement après l'installation de SafeGuard Management Center (étape 9).	Scripts livrés avec le produit
8	Installez SafeGuard Management Center pour la gestion centralisée des utilisateurs, ordinateurs, stratégies, clés et rapports.	SGNManagementCenter.msi
9	Configurez SafeGuard Management Center : connexion base de données et serveur de base de données, certificats, informations d'identification du responsable principal de la sécurité.	Assistant de configuration de SafeGuard Management Center
10	Enregistrez et configurez le serveur SafeGuard Enterprise : créez un package de configuration du serveur et déployez-le sur le serveur Web.	Outil de package de configuration de SafeGuard Management Center

Étape	Description	Package à installer / outil à utiliser
11	Créez la structure organisationnelle depuis Active Directory ou manuellement.	SafeGuard Management Center
12	Préparez les terminaux au chiffrement	SGxClientPreinstall.msi
13	Créez le package de configuration client initial pour la configuration des terminaux.	Outil de package de configuration de SafeGuard Management Center
14	Installez le logiciel de chiffrement et le package de configuration initiale sur les terminaux.	Retrouvez plus de renseignements sur les packages disponibles à la section À propos des terminaux administrés et non administrés *(page 62)*.

2.2.2 Compatibilité avec les autres produits Sophos

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

2.2.2.1 Compatibilité à Sophos Central

- SafeGuard Enterprise Device Encryption ne peut pas être installé avec Sophos Central Device Encryption sur les terminaux Windows et Mac.
- SafeGuard Enterprise 8.3 File Encryption peut être installé avec Sophos Central Device Encryption sur les terminaux Windows et Mac.

2.2.2.2 Compatibilité avec SafeGuard LAN Crypt

SafeGuard Enterprise 8.3 ne peut pas être utilisé avec SafeGuard LAN Crypt sur un terminal.

2.2.2.3 Compatibilité avec Sophos Enterprise Console

Si vous utilisez Sophos Enterprise Console (SEC) pour administrer le chiffrement, n’installez ni le serveur SafeGuard Enterprise et ses composants (Web Helpdesk et le planificateur de tâches du serveur) ni SafeGuard Management Center sur le serveur sur lequel le serveur d’administration SEC est installé.

2.2.2.4 Compatibilité avec Sophos Mobile

SafeGuard Enterprise et Sophos Mobile partagent le même jeu de clé. Ceci signifie que les utilisateurs peuvent accéder en toute sécurité depuis leurs appareils mobiles à leurs fichiers chiffrés avec la clé SGN. De même, les utilisateurs peuvent créer des fichiers sur leur app Sophos Secure Workspace et les ouvrir sur un ordinateur protégé par SGN.

Conditions préalables :

- Enregistrez le serveur Sophos Mobile avec son certificat sur le serveur SGN dans SafeGuard Management Center (**Outils > Outil de package de configuration > Serveurs**).
- Établissez une connexion SSL/TLS sécurisée entre les serveurs. Nous conseillons fortement d'utiliser le protocole de chiffrement TLS 1.2 afin d'éviter les attaques SSL les plus répandues.
- Utilisez Active Directory afin d'identifier les utilisateurs d'appareils mobiles dans SGN à l'aide de leurs informations Active Directory.

2.3 Configuration du serveur SafeGuard Enterprise

Le serveur SafeGuard Enterprise sert d'interface avec les clients SafeGuard Enterprise. Comme SafeGuard Management Center, il permet d'accéder à la base de données. Il s'exécute en tant qu'application sur un serveur Web basé sur les services Internet (IIS) de Microsoft. Assurez-vous d'utiliser la version la plus récente des services Internet (IIS) avec toutes les dernières mises à jour.

Pour une sécurité et des performances optimales, nous vous conseillons d'installer le serveur SafeGuard Enterprise sur une machine dédiée. Ceci permet d'assurer que d'autres applications ne soient pas en conflit avec SafeGuard Enterprise.

Le serveur SafeGuard Enterprise inclut le Planificateur de tâches pour créer et planifier des tâches périodiques basées sur des scripts. Les tâches sont automatiquement exécutées sur le serveur SafeGuard Enterprise. Plusieurs scripts pour différents cas d'utilisation sont fournis avec le produit SafeGuard Enterprise. Vous pouvez les utiliser en tant que modèles pour votre environnement.

À partir de la version 8.1, SafeGuard Enterprise Web Helpdesk est inclus dans le package d'installation de SGNServer.msi. Retrouvez plus de renseignements à la section Web Helpdesk *(page 459)*.

2.3.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

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

  IIS est disponible au téléchargement sur le site Web de Microsoft.
- Si vous utilisez le chiffrement de transport SSL entre le serveur SafeGuard Enterprise et le client SafeGuard Enterprise, veuillez configurer IIS à l’avance de façon appropriée. Retrouvez plus de renseignements à la section Sécurisation des connexions de transport avec SSL *(page 49)*.
  - Un certificat doit être généré et le serveur des services Internet (IIS) configuré pour utiliser SSL et sélectionner le certificat.
  - Le nom du serveur indiqué lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui indiqué sur le certificat SSL. Faute de quoi, la communication entre le client et le serveur est impossible. Les alias DNS ne sont pas compatibles car ils risquent d’entraîner des conflits lors de la mise en place de SSL.
  - Un certificat SSL distinct est nécessaire pour chaque serveur SafeGuard Enterprise.

    Si vous administrez des terminaux Windows et macOS, les certificats SSL doivent être émis par une autorité de certification. En effet, à partir de macOS 10.12, Apple n’autorise plus les certificats auto-signés pour les connexions SSL.
  - Si vous utilisez un équilibreur de charge réseau, vérifiez que la plage de ports inclut le port SSL.
- .NET Framework 4.5 et ASP.NET 4.5 (livrés avec SafeGuard Enterprise) doivent être installés.

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

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

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

IIS est disponible au téléchargement sur le site Web de Microsoft.

1. Dans le menu **Démarrer**, cliquez sur **Tous les programmes > Outils d’administration > Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **RôlesAjouter 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 suivante, 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 les services des sous-rôles.

7. Sélectionnez les **Scripts et outils de gestion IIS** nécessaire à une configuration correcte des services Internet (IIS).

8. Cliquez sur **Suivant > Installer > Fermer**.

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

9. Vérifiez que la page Web apparaît correctement à l'aide de http://<nom serveur>. Retrouvez plus de renseignements sur : http://support.microsoft.com.

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

.NET Framework 4.5 est requis. Ce programme est fourni avec le produit SafeGuard Enterprise.

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

1. À partir du menu **Démarrer**, sélectionnez **Exécuter...**.
2. Saisissez la commande suivante : Appwiz.cpl. Tous les programmes installés sur l'ordinateur apparaissent à l'écran.
3. Vérifiez si .NET Framework Version 4.5 apparaît. Si elle n'apparaît pas, installez cette version. Suivez les étapes de l'assistant d'installation et confirmez tous les paramètres par défaut.
4. Pour vérifier si l'installation est correctement enregistrée, allez dans C:\Windows \Microsoft.NET\Framework. Chaque version installée doit être visible sous la forme d'un dossier distinct montrant la version comme nom de dossier, par exemple « v 4.5 ».

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

La version 4.5 de ASP.NET est requise.

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

La version 4.5 doit apparaître pour ASP.NET.

2.3.2.2 Installation et configuration des services Internet (IIS) 8 sur Microsoft Windows Server 2012/2012 R2 et Windows Server 2016

IIS est disponible au téléchargement sur le site Web de Microsoft.

1. Sur le tableau de bord du **Gestionnaire de serveurs**, sélectionnez **Gérer > Ajouter des rôles et des fonctionnalités**.

2. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, sur la page **Avant de commencer**, vérifiez les éléments suivants :

   • Le compte administrateur a un mot de passe fort.

   • Les paramètres réseau, par exemple les adresses IP, sont configurés.

   • Les dernières mises à jour de sécurité de Windows Update sont installées.

3. Sélectionnez **Rôles du serveur** sur le volet de gauche, puis **Serveur Web (IIS)**. Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche. Le **Rôle Serveur Web (IIS)** apparaît dans la zone de navigation de l'**Assistant Ajout de rôles et de fonctionnalités**.

4. Dans le volet de gauche, sélectionnez **Services de rôle** sous **Rôle Serveur Web (IIS)**. Conservez les services de rôles par défaut.

5. Défilez jusqu'au nœud **Développement d'applications** et sélectionnez :
   • **ASP.NET 4.5**
   • **Extensions ISAPI**
   • **Filtres ISAPI**

   Les services de sous-rôles nécessaires sont sélectionnés automatiquement.

6. Sous le nœud **Sécurité**, sélectionnez :
   • **Authentification de base**
   • **Authentification Windows**

7. Cliquez sur **Suivant > Installer > Fermer**.

IIS est installé avec une configuration par défaut pour l'hébergement d'ASP.NET sous Windows Server.

Confirmez que le serveur Web fonctionne avec http://(saisissez ici le nom de la machine sans parenthèses). Si la page Web ne s'affiche pas proprement, veuillez consulter la base de connaissances de Microsoft (http://support.microsoft.com) pour retrouver plus de renseignements.

2.3.3 Installation du serveur SafeGuard Enterprise.

Après avoir configuré IIS, vous pouvez installer le serveur SafeGuard Enterprise sur le serveur IIS. Le package d'installation SGNServer.msi est livré avec le produit. Il vous permet d'installer les modules suivants :

- Le serveur
- Le service du planificateur (facultatif)
- Web Helpdesk (facultatif)

1. Sur le serveur sur lequel vous voulez installer le serveur SafeGuard Enterprise, cliquez deux fois sur SGNServer.msi. Un assistant vous guide tout au long des étapes nécessaires.
2. Sélectionnez les composants supplémentaires à installer :
   - **Planificateur de tâches**

     Le Planificateur de tâches est automatiquement installé avec une installation de type **Par défaut**.
   - **Web Helpdesk**

     À partir de la version 8.1, SafeGuard Enterprise Web Helpdesk est inclus dans le package d'installation de SGNServer.msi. Retrouvez plus de renseignements à la section Web Helpdesk *(page 459)*.
3. Cliquez sur **Install**.

SafeGuard Enterprise Server et les composants supplémentaires sont installés.

Assurez-vous que l'installation se soit déroulée avec succès en ouvrant le **Gestionnaire des services Internet** (exécutez `inetmgr`) et vérifiez que le page Web nommée SGNSRV est désormais disponible.

2.3.3.1 Événements journalisés sur le serveur

Suite à l'installation du serveur SafeGuard Enterprise, la connexion des événements journalisés est désactivée pour la base de données SafeGuard Enterprise afin d'optimiser les performances. Toutefois, la connexion des événements journalisés est nécessaire pour la protection de l'intégrité des événements journalisés. La concaténation de toutes les entrées du tableau des événements permet de voir clairement lorsqu'une entrée a été supprimée et de lancer une vérification de l'intégrité. Pour utiliser la protection d'intégrité, vous devez définir manuellement la connexion des événements consignés dans le journal. Retrouvez plus de renseignements à la section Rapports *(page 228)*.

Vous devez installer un package d'installation du client SafeGuard pour permettre au serveur de transférer les événements à la base de données SafeGuard Enterprise.

2.4 Configuration de la base de données SafeGuard Enterprise

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

Vérifiez la liste des types de serveurs SQL actuellement pris en charge dans la section des configurations système requises de la version actuelle des Notes de publication.

Lors de l'utilisation de SQL Express Edition, veuillez prendre en compte les limites de taille de fichier de la base de données imposées par Microsoft. SQL Express Edition n'est pas adapté à une utilisation sur des environnements de plus grande taille.

Vous pouvez configurer la base de données soit automatiquement à la première configuration dans SafeGuard Management Center soit manuellement à l'aide de scripts SQL fournis avec votre produit. Selon l'environnement de votre entreprise, vérifiez la méthode à choisir. Dans les deux cas, veuillez d'abord vous assurer que vous disposez des droits d'accès nécessaires à la base de données. Retrouvez plus de renseignements à la section Droits d'accès à la base de données *(page 29)*.

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). En mode mutualisé, tous les locataires doivent avoir installé la même version de SafeGuard Enterprise. Retrouvez plus de renseignements sur la configuration mutualisée à la section Utilisation de plusieurs configurations de base de données (mutualisées) *(page 118)*.

Pour communiquer avec SQL par le biais d'un pare-feu, les ports TCP/IP 1433 et 1434 sont nécessaires.

2.4.1 Authentification de la base de données

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

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

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

Utilisez l'authentification SQL pour des ordinateurs ne faisant pas partie d'un domaine, sinon utilisez l'authentification Windows. Si vous utilisez l'authentification SQL, nous conseillons vivement de protéger la connexion de et vers le serveur de base de données avec SSL. Retrouvez plus de renseignements à la section Sécurisation des connexions de transport avec SSL *(page 49)*.

2.4.1.1 Droits d'accès à la base de données

SafeGuard Enterprise est configuré d'une telle façon que pour utiliser la base de données SQL, vous n'avez besoin que d'un seul compte utilisateur avec des droits d'accès minimaux pour la base de données.

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

Lorsque SafeGuard Enterprise est en cours d'exécution, un seul responsable de la sécurité de SafeGuard Management Center nécessite uniquement les droits en lecture/écriture sur la base de données de SafeGuard Management Center.

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

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

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

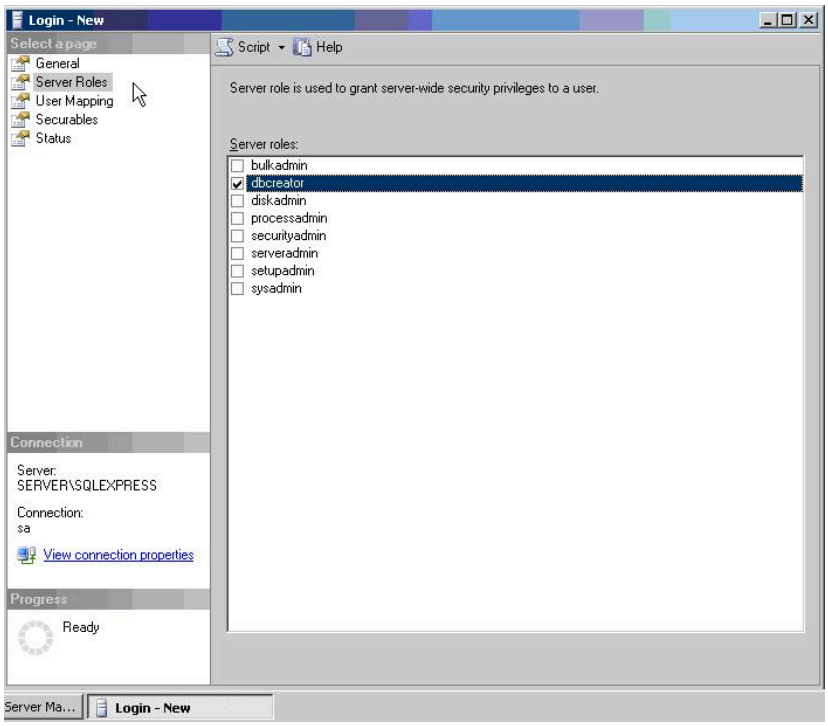
2.4.1.2 Configuration d’un compte Windows pour la connexion au serveur SQL

La description des étapes de configuration individuelle ci-dessous est destinée aux administrateurs SQL et concerne Microsoft Windows Server 2008 R2 et Microsoft SQL Server Standard ou Express Edition.

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

1. Ouvrez SQL Server Management Studio. Connectez-vous à SQL Server à l’aide de vos codes d’accès.
2. Ouvrez l’**Explorateur d’objets**, cliquez avec le bouton droit de la souris sur **Sécurité**, choisissez **Nouveau**, puis cliquez sur **Connexion**.
3. Dans **Nouvelle connexion** sur la page **Général**, sélectionnez **Authentification Windows**.
4. Cliquez sur **Rechercher**. Recherchez le nom utilisateur Windows respectif et cliquez sur **OK**. Le nom utilisateur apparaît comme **Nom de connexion**.
5. Dans **Base de données par défaut**, si aucun script n’a été utilisé pour créer une base de données SafeGuard Enterprise, sélectionnez **Maître**.
6. Cliquez sur **OK**.
7. Pour créer automatiquement la base de données lors de la première configuration de SafeGuard Management Center, vous devez changer les droits d’accès. Dans **Nouvelle connexion**, assignez

les droits d'accès/rôles en cliquant à gauche sur **Rôles du serveur**. Sélectionnez **dbcreator**. Dès que SafeGuard Enterprise est installé, vous pouvez réinitialiser le rôle de la base de données sur **dbowner**.



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

Tous les utilisateurs autorisés à utiliser SafeGuard Management Center doivent avoir un compte d'utilisateur SQL valide lorsqu'ils ont recours à l'authentification Windows pour se connecter à la base de données SafeGuard.

La description des étapes de configuration individuelles ci-dessous est destinée aux administrateurs SQL. Elle concerne toutes les éditions de Microsoft Windows Server 2008 R2 avec Microsoft SQL Server 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.

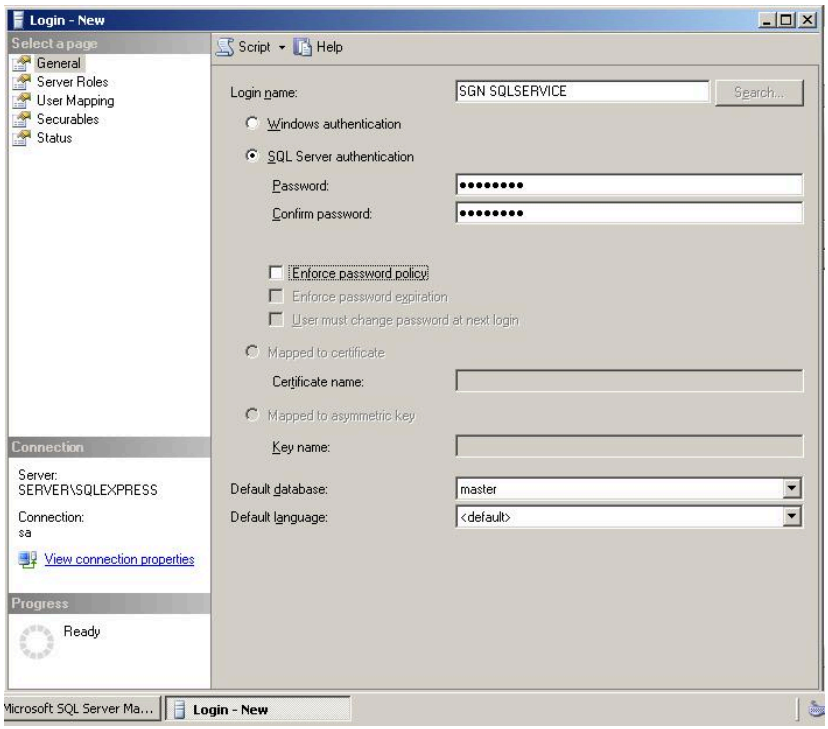
2. Ouvrez l'**Explorateur d'objets**, cliquez avec le bouton droit de la souris sur **Sécurité**, puis cliquez sur **Nouvelle > Connexion**.

3. Dans **Nouvelle connexion** sur la page **Général**, sélectionnez **Authentification SQL Server**.

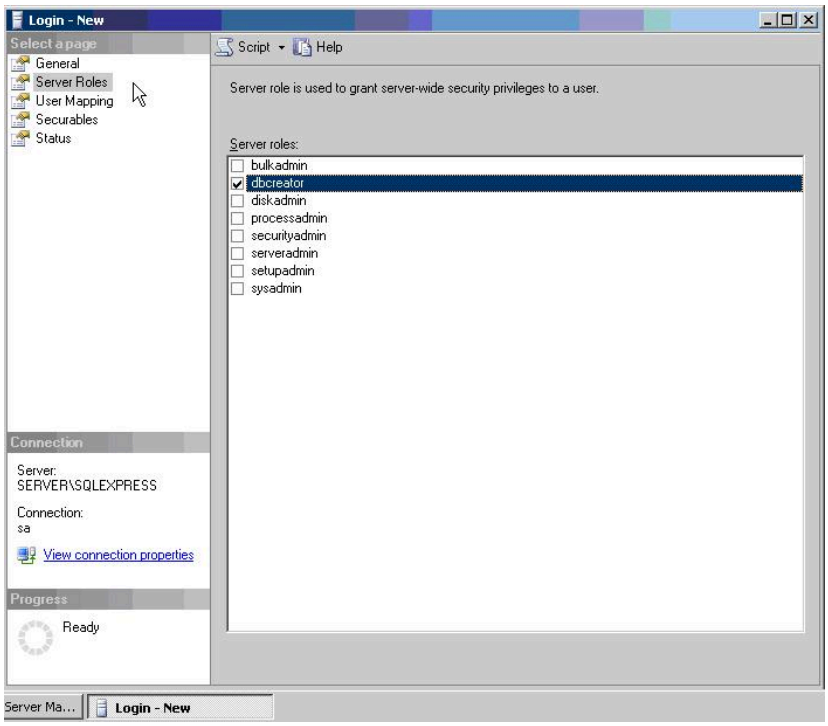
4. Sur la page **Général**, dans **Nom de connexion**, procédez de la manière suivante :
    a. Saisissez le nom du nouvel utilisateur, par exemple SGN SQLSERVICE.

b. Saisissez et confirmez le mot de passe du compte.
c. Dessélectionnez **Appliquer la stratégie des mots de passe**.
d. Dans **Base de données par défaut**, si aucun script n'a été utilisé pour créer une base de données SafeGuard Enterprise, sélectionnez **Maître**. Cliquez sur **OK**.

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



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



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

2.4.2 Génération de la base de données SafeGuard Enterprise

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

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

  Au titre de responsable de la sécurité, vous pouvez facilement créer la base de données SafeGuard Enterprise suite à l'installation de SafeGuard Management Center. L'assistant de configuration de SafeGuard Management Center vous guide tout au long de la configuration de base qui inclut également la création de la base de données. Installez et configurez SafeGuard Management Center comme indiqué à la section Installation de SafeGuard Management Center *(page 38)*, puis changez les droits d'accès correspondants comme indiqué à la section Modification des droits d'accès à la base de données SafeGuard Enterprise *(page 35)*.

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

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

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

2.4.2.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

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

2.4.2.2 Génération de la base de données SafeGuard Enterprise avec un script

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

- CreateDatabase.sql
- CreateTables.sql

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

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

1. Copiez les scripts CreateDatabase.sql et CreateTables.sql inclus dans le produit SafeGuard Enterprise sur le serveur SQL.
2. Cliquez deux fois sur le script **CreateDatabase.sql**. Microsoft SQL Server Management Studio démarre.
3. Connectez-vous à SQL Server à l’aide de vos codes d’accès.

4. Assurez-vous que les deux chemins cible se trouvant au début du script, sous **FILENAME** (MDF, LDF), sont bien présents sur le lecteur de disque dur local. Corrigez-les si nécessaire.
5. Cliquez sur le bouton **Exécuter** depuis la barre d'outils pour générer la base de données. Vous avez créé la base de données **SafeGuard**. Utilisez maintenant le script CreateTables.sql fourni avec le produit pour générer les tables.
6. Cliquez deux fois sur **CreateTables.sql**. Un autre volet s'ouvre dans Microsoft SQL Server Management Studio.
7. Dans la partie supérieure du script, saisissez use SafeGuard pour sélectionner la base de données SafeGuard Enterprise dans laquelle les tables doivent être créées.
8. Cliquez sur le bouton **Exécuter** depuis la barre d'outils pour générer les tables.

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

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

Lorsque la base de données de SafeGuard Enterprise a été créée, le compte d'utilisateur doit être autorisé à accéder à la base de données. Ces droits d'accès doivent être donnés à tous les responsables de la sécurité qui utilisent SafeGuard Management Center avec l'authentification Windows NT. Comme il est possible d'assigner différents rôles et autorisations à un utilisateur sur une base de données, seuls les droits minimaux requis 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 deux fois sur **Connexions**.
3. Cliquez avec le bouton droit de la souris sur le nom d'utilisateur respectif et cliquez sur **Propriétés**.
4. Sélectionnez **Mappage des utilisateurs** sur la gauche. Sous **Utilisateurs mappés à cette connexion** , sélectionnez la base de données **SafeGuard**.
5. Sous **Appartenance au rôle de base de données** définissez les droits d'accès minimaux pour utiliser la base de données SafeGuard Enterprise : sélectionnez **db_datareader**, **db_datawriter** et **public**.
6. Cliquez sur **OK**.

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

Pour installer SafeGuard Management Center, le service SQL Browser doit être utilisé et les options **Canaux nommés** et **TCP/IP** doivent être activées. Ces paramètres sont nécessaires à l'accès au serveur SQL à partir d'autres machines. Vous pouvez vérifier ceci dans le **Gestionnaire de**

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

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

2.4.5 Création d'une règle de pare-feu Windows sur Windows Server

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

1. Sur l'ordinateur hébergeant l'instance de SQL Server, cliquez sur **Démarrer**, sélectionnez **Outils d'administration**, puis cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.
2. À partir de l'arborescence de navigation sur la gauche, sélectionnez **Règles de trafic entrant**.
3. Cliquez sur **Action** dans la barre de menus, puis sur **Nouvelle règle**. L'**Assistant Nouvelle règle de trafic entrant** démarre.
4. Sur la page **Type de règle**, sélectionnez **Personnaliser** et cliquez sur **Suivant**.
5. Sur la page **Programme**, sélectionnez le programme et les services auxquels cette règle doit s'appliquer et cliquez sur **Suivant**.
6. Sur la page **Protocole et ports**, sélectionnez **TCP** en tant que **Type de protocole**. Pour le **Port local**, sélectionnez **Ports spécifiques** et saisissez `1433, 1434`. 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**.

2.4.6 Configuration de l’authentification Windows pour la connexion au serveur SQL

Cette section concerne Microsoft Windows Server avec Microsoft SQL Server 2012 Standard Edition et IIS 7.

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

1. Sélectionnez **Démarrer**, puis **Exécuter**. Saisissez **dsa.msc**. Ouvrez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory.
2. Dans l’arborescence de navigation sur la gauche, développez l’arborescence du domaine et sélectionnez **Builtin**.
3. Ajoutez l’utilisateur Windows respectif dans les groupes suivants : IIS_IUSRS, Utilisateurs du journal de performance, Utilisateurs de l’Analyseur de performances.
4. Quittez le composant logiciel enfichable.
5. Dans le système de fichiers local, dans l’Explorateur Windows, cliquez avec le bouton droit de la souris sur le dossier C:\Windows\Temp et sélectionnez **Propriétés**. Dans **Propriétés**, sélectionnez l’onglet **Sécurité**.
6. Dans **Sécurité**, cliquez sur **Ajouter** et saisissez le nom d’utilisateur Windows respectif dans le champ **Entrez les noms d’objets à sélectionner**. Cliquez sur **OK**.
7. Dans l’onglet **Sécurité**, sous **Autorisations**, cliquez sur **Avancé**. Dans la boîte de dialogue **Paramètres de sécurité avancés pour Temp**, sous l’onglet **Autorisations**, cliquez sur **Modifier les autorisations**. Puis, modifiez les autorisations dans la boîte de dialogue **Objet** sur **Autoriser** : **Liste du dossier / lecture des données**, **Création de fichier / écriture de données**, **Suppression**.
8. Cliquez sur **OK**, puis fermez la boîte de dialogue **Propriétés de : Temp** et l’Explorateur Windows.
9. Ouvrez le **Gestionnaire des services IIS**.
10. Dans le volet **Connexions** à gauche, sélectionnez **Pools d’applications** du nœud serveur correspondant.
11. Dans la liste **Pools d’applications** à droite, sélectionnez **SGNSRV-Pool**.
12. Dans le volet **Actions** à gauche, sélectionnez **Paramètres avancés**.
13. Dans **Paramètres avancés**, sous **Modèle de processus**, pour la propriété **Identité**, cliquez sur le bouton **...**
14. Dans **Identité du pool d’applications**, sélectionnez **Compte personnalisé** et cliquez sur **Définir**.
15. Dans **Définir les codes d’accès**, saisissez le nom d’utilisateur Windows correspondant sous la forme suivante : `Domaine\<nom utilisateur Windows>`. Saisissez et confirmez le mot de passe Windows respectif, puis cliquez sur **OK**.
16. Dans le volet **Connexions** à gauche, sélectionnez le nœud serveur correspondant et cliquez sur **Redémarrer** dans le volet **Actions**.

17. Dans le volet **Connexions** à gauche, sous le nœud serveur correspondant, sous **Sites**, **Sites Web par défaut**, sélectionnez **SGNSRV**.
18. Sur la page d'accueil SGNSRV, cliquez deux fois sur **Authentification**.
19. Cliquez avec le bouton droit de la souris sur **Authentification anonyme** et sélectionnez **Modifier**.
20. Pour **Identité utilisateur anonyme**, sélectionnez **Utilisateur spécifique** et vérifiez que le nom utilisateur est **IUSR**. Corrigez-le si nécessaire.
21. Cliquez sur **OK**.

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

2.5 Installation de SafeGuard Management Center

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

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

SafeGuard Management Center prend en charge plusieurs bases de données via les configurations mutualisées de base de données (Multi Tenancy). Vous pouvez créer et maintenir à jour différentes bases de données SafeGuard Enterprise pour différents locataires tels que les différents locaux d'une d'entreprise, les différents unités organisationnelles ou les différents domaines. Pour faciliter l'administration, les configurations de ces bases de données peuvent également être exportées dans des fichiers et importées à partir de fichiers.

2.5.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Assurez-vous de disposer des droits d'administrateur Windows.
- La version 4.5 ou supérieure de .NET Framework doit être installée. Le logiciel est fourni avec le produit SafeGuard Enterprise.
- Si vous voulez créer une nouvelle base de données SafeGuard Enterprise lors de la configuration de SafeGuard Management Center, vous avez besoin des droits d'accès et des

informations d’identification SQL nécessaires. Retrouvez plus de renseignements à la section Droits d’accès à la base de données *(page 29)*.

2.5.2 Installation de SafeGuard Management Center

1. Démarrez SGNManagementCenter.msi à partir du dossier d’installation du produit livré. Un assistant vous guide tout au long des étapes nécessaires.
2. Acceptez les valeurs par défaut des boîtes de dialogue qui suivent exception faite de la suivante : Sur la page de sélection du **Type d’installation**, procédez de l’une des manières suivantes :

   - Pour que SafeGuard Management Center prenne en charge une seule base de données, sélectionnez **Standard**.
   - L’option **Personnalisée** permet aux utilisateurs de choisir les fonctions à installer.
   - Pour que SafeGuard Management Center prenne en charge plusieurs bases de données en mode **(Mutualisé)**, sélectionnez **Complète**. Retrouvez plus de renseignements à la section Utilisation de plusieurs configurations de base de données (mutualisées) *(page 118)*.

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

2.5.3 Configuration de SafeGuard Management Center

L’assistant de configuration de SafeGuard Management Center vous aide à spécifier les paramètres de base de SafeGuard Management Center et à paramétrer les connexions à la base de données pendant la configuration initiale. Il s’ouvre automatiquement lorsque vous démarrez SafeGuard Management Center pour la première fois après l’installation.

L’**Aide** de SafeGuard Management Center est une aide contextuelle et de recherche en texte intégral. Elle est configurée pour offrir les fonctionnalités complètes des pages de contenu du système d’aide suite à l’activation de JavaScript dans votre navigateur. En cas de désactivation de JavaScript, vous pouvez toujours afficher et naviguer dans le système d’aide de SafeGuard Management Center. Toutefois, certaines fonctionnalités, telle que la recherche, ne pourront pas être utilisées.

2.5.3.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Assurez-vous de disposer des droits d’administrateur Windows.
- Le pare-feu doit être configuré correctement.
- Munissez-vous des informations suivantes : si nécessaire, vous pouvez les obtenir auprès de votre administrateur SQL.
  - Codes d’accès SQL
  - Le nom du serveur SQL sur lequel la base de données SafeGuard Enterprise doit être exécutée.
  - Le nom de la base de données SafeGuard Enterprise si elle a déjà été créée.

2.5.3.2 Configuration initiale de SafeGuard Management Center

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

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

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

2.5.3.3 Configuration de la connexion au serveur de base de données

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

Sur la page **Connexion au serveur de base de données**, effectuez les opérations suivantes :

1. 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.
2. Sélectionnez **Utiliser SSL** pour protéger la connexion entre SafeGuard Management Center et le serveur de base de données SQL. Nous vous conseillons fortement d’effectuer cette opération lorsque vous avez sélectionné **Utiliser l’authentification SQL Server avec les codes d’accès**

suivants sous **Authentification** car ce paramètre chiffrera le transport des codes d'accès SQL. Le chiffrement SSL exige un environnement SSL de chiffrement sur le serveur de base de données SQL que vous avez préalablement configuré. Retrouvez plus de renseignements à la section Sécurisation des connexions de transport avec SSL *(page 49)*.

3. Sous **Authentification**, sélectionnez le type d'authentification à utiliser pour accéder à cette instance du serveur de base de données.

   - Sélectionnez **Utiliser l'authentification Windows NT** pour utiliser vos codes d'accès Windows.

     Utilisez ce type d'authentification si votre ordinateur appartient à un domaine. Par contre, une configuration obligatoire supplémentaire est nécessaire car l'utilisateur doit être autorisé à se connecter à la base de données. Reportez-vous aux sections Configuration d'un compte Windows pour la connexion au serveur SQL *(page 30)* et Configuration de l'authentification Windows pour la connexion au serveur SQL *(page 37)*.

   - Sélectionnez **Utiliser l'authentification SQL Server avec les codes d'accès suivants** pour accéder à la base de données avec les codes d'accès SQL adéquats. 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.

4. Cliquez sur **Suivant**.

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

2.5.3.4 Création ou sélection d'une base de données

Sur la page **Paramètres de base de données**, il est possible de créer une nouvelle base de données ou d'en utiliser une déjà existante. Lorsque la base de données a déjà été créée par les scripts SQL, l'assistant sélectionne automatiquement la base de données existantes. Dans ce cas, aucune configuration supplémentaire n'est requise.

Si la base de données n'a pas déjà été créée, procédez de la manière suivante :

1. Sélectionnez **Créer une base de données nommée** et saisissez un nom pour la nouvelle base de données. Pour ce faire, vous devez disposer des droits d'accès SQL appropriés. Retrouvez plus de renseignements à la section Droits d'accès à la base de données *(page 29)*. 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 (_).

2. Cliquez sur **Suivant**.

2.5.3.5 Définition de l’authentification Active Directory

Avant de créer une nouvelle base de données, vous pouvez définir tous les paramètres nécessaires à l’accès à Active Directory. À ce stade, vous indiquez le nom du serveur et les codes d’accès de l’utilisateur.

Nous vous conseillons de fournir des codes d’accès Active Directory à ce stade afin que la structure de base d’Active Directory puisse être importée automatiquement. L’importation inclut tous les conteneurs synchronisés avec la base de données SafeGuard Enterprise et notamment les unités organisationnelles et les groupes. Aucun ordinateur ou utilisateur n’est inclus dans cette première opération d’importation du répertoire. En revanche, toutes les clés sont créées et assignées aux conteneurs correspondants. Suite à l’opération d’importation, les responsables de la sécurité peuvent assigner des stratégies à différents conteneurs sans avoir à effectuer une synchronisation AD. Les ordinateurs et les utilisateurs recevront leurs stratégies dès qu’ils se seront enregistrés dans le serveur SGN.

Si vous n’avez pas encore vos codes d’accès, vous pouvez ignorer cette étape et configurer manuellement l’importation d’Active Directory.

Pour les grandes entreprises aux structures AD complexes ainsi que pour le traitement des objets supprimés, modifiés ou déplacés, veuillez utiliser l’assistant **Authentification LDAP**. Retrouvez plus de renseignements à la section Importation d’une structure Active Directory *(page 163)*.

1. Sur la page **Authentification Active Directory**, saisissez le nom du serveur ou son adresse IP.
2. Nous conseillons l’utilisation de SSL pour sécuriser la connexion entre le serveur SafeGuard Enterprise et les terminaux.
3. Indiquez vos codes d’accès d’utilisateur.
4. Cliquez sur **Suivant**.

Dès que la base de données SafeGuard Enterprise a été créée et que l’Assistant de configuration initiale a terminé, la structure de base du répertoire défini est importée dans la base de données. Toutes les clés nécessaires sont créées et assignées aux conteneurs correspondants.

2.5.3.6 Création du responsable principal de la sécurité

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

Le responsable principal de la sécurité (MSO ou Master Security Officer) est l’administrateur disposant de tous les droits.

1. Sur la page **Données du responsable de la sécurité** sous **Identifiant du responsable principal de la sécurité**, saisissez un nom de responsable principal de la sécurité (par exemple, `MSO`).

2. Dans **Certificat du responsable principal de la sécurité**, procédez d'une des manières suivantes :
   - Création du certificat du responsable principal de la sécurité *(page 43)*
   - Importation du certificat MSO *(page 43)*
   - Exportation du certificat MSO *(page 44)*

Création du certificat du responsable principal de la sécurité

Sur **Création du certificat du responsable principal de la sécurité**, vous pouvez créer un mot de passe pour le magasin de certificats personnels. Le magasin de certificats de SafeGuard Enterprise est un magasin virtuel contenant les certificats de SafeGuard Enterprise. Ce magasin n'est pas associé à la fonctionnalité de Microsoft. Le mot de passe créé à cette étape est le mot de passe qui sera utilisé pour se connecter à Management Center.

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

Le certificat MSO est créé et enregistré localement (<nom_mso>.cer).

Nous vous conseillons de noter ce mot de passe et de le conserver en lieu sûr. Vous en aurez besoin pour accéder à SafeGuard Management Center.

Importation du certificat MSO

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

Il est impossible d'importer le 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. Nous vous conseillons d'utiliser un certificat d'au moins 2048 bits.

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

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

Exportation du certificat MSO

Le certificat MSO est exporté dans un fichier de clé privée (P12). Dans **Exporter le certificat**, créez un mot de passe pour protéger cette clé de fichier privée. Le fichier de clés privées est nécessaire pour restaurer une installation interrompue de SafeGuard Management Center.

Pour exporter un certificat MSO :

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

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

⚠ **Important :** 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.

Dès que le certificat du responsable de la sécurité est exporté et que le magasin de certificats et le responsable de la sécurité sont créés, l'assistant crée le certificat de l'entreprise.

2.5.3.7 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 qui a été endommagée.

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

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

   Pour les terminaux sur lesquels des versions de SafeGuard Enterprise plus anciennes que 6.1 sont installées, veuillez sélectionner **SHA-1** sous **Algorithme de hachage pour les certificats générés**. Retrouvez plus de renseignements à la section Modification de l'algorithme pour les certificats autosignés *(page 182)*.

3. Cliquez sur **Suivant**.

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

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

Retrouvez plus de renseignements sur la restauration d’une configuration de base de données corrompue à la section Réparation d’une configuration corrompue de la base de données *(page 117)*.

2.5.3.8 Configuration initiale complète de SafeGuard Management Center

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

Un fichier de configuration est créé.

Vous avez créé :

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

SafeGuard Management Center démarre une fois que l’assistant de configuration a fermé. Retrouvez plus de renseignements à la section Connexion à SafeGuard Management Center *(page 91)*.

2.5.4 Installation de la structure organisationnelle dans SafeGuard Management Center

Remarque :

L’importation de la structure organisationnelle ou sa création manuelle est uniquement nécessaire si vous passez l’importation initiale déclenchée par l’Assistant de configuration de SafeGuard Management Center.

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

- Importation d’une structure Active Directory.

  Lors de la synchronisation avec Active Directory, les ordinateurs, les utilisateurs et les groupes sont importés dans SafeGuard Management Center et leurs informations sont stockées 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 permettant de ne pas utiliser de services d’annuaire, vous pouvez créer de nouveaux domaines/groupes de travail auxquels l’utilisateur ou l’ordinateur peut se connecter.

Vous pouvez utiliser l’une de ces deux options ou les combiner. Par exemple, vous pouvez importer un service Active Directory (AD) partiellement ou intégralement, et créer manuellement d’autres unités organisationnelles.

En associant deux méthodes, les unités organisationnelles créées manuellement ne sont pas redirigées vers le service AD. Si vous voulez rediriger vers AD les unités organisationnelles créées dans SafeGuard Enterprise, veuillez-les ajouter séparément à AD.

Retrouvez plus de renseignements sur l’importation ou la création d’une structure organisationnelle à la section Gestion de la structure organisationnelle *(page 161)*.

2.5.4.1 Comment empêcher la suppression des domaines, des nœuds UO et des groupes de travail

Vous pouvez configurer SafeGuard Enterprise pour empêcher la suppression des nœuds UO importés. Sous cette configuration, seul le responsable principal de la sécurité peut supprimer les nœuds UO dans SafeGuard Management Center. Cette option est activée par défaut.

Pour empêcher la suppression des nœuds UO :

1. Dans SafeGuard Management Center, sélectionnez **Options** dans le menu **Outils**.
2. Allez dans l’onglet **Répertoire**.
3. Activez l’option **Empêcher la suppression des domaines, des nœuds UO et des groupes de travail**.
4. Cliquez sur **OK**.

Si un responsable de la sécurité n’a pas les droits suffisants pour supprimer des domaines, des nœuds UO et des groupes de travail, un message apparaît indiquant que la suppression des domaines, des nœuds UO et des groupes de travail est désactivée et qu’elle doit être activée par un responsable principal de la sécurité ou un responsable de la sécurité disposant des droits adéquats.

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

2.5.5 Importation du fichier de licence

SafeGuard Enterprise dispose d'un compteur de licences intégré. Lorsque vous téléchargez le produit, vous pouvez également télécharger une licence d'essai. Cette licence d'évaluation inclut cinq licences pour chaque module et doit être importée dans SafeGuard Management Center. Ceci doit faciliter l'évaluation d'autres modules SafeGuard Enterprise sans aucun effet secondaire. Lors de l'achat de SafeGuard Enterprise, chaque client reçoit un fichier de licence personnalisé qui doit être importé dans SafeGuard Management Center.

Retrouvez plus de renseignements à la section Licences *(page 189)*.

2.6 Test de la communication

Une fois le serveur SafeGuard Enterprise, la base de données et SafeGuard Management Center configurés, nous vous conseillons de tester la connexion. Cette section contient les conditions préalables et les paramètres requis pour l'essai de la connexion.

2.6.1 Ports/connexions

Les terminaux doivent créer les connexions suivantes :

Connexion du terminal SafeGuard à	Port
Serveur SafeGuard Enterprise	Port 443 lors de l’utilisation de la connexion de transport SSL Port 80/TCP **Remarque :** Les ports doivent être ouverts pour assurer la communication bi-directionnelle.

SafeGuard Management Center doit créer les connexions suivantes :

Connexion de SafeGuard Management Center à	Port
Base de données SQL	Port dynamique SQL Server : Port 1433/TCP et port 1434/TCP

Connexion de SafeGuard Management Center à	Port
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 (Express)
Active Directory	Port 389/TCP

2.6.2 Méthode d'authentification

1. Sur l'ordinateur sur lequel est installé le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Dans l'arborescence, sélectionnez le serveur adéquat et cliquez sur**Sites > Site Web par défaut > SGNSRV**.
3. Sous **IIS**, cliquez deux fois sur l'icône **Authentification** et vérifiez les paramètres suivants :
   - Définissez **Authentification anonyme** sur **Activer**.
   - Définissez l'**Authentification Windows** sur **Désactiver**.

2.6.3 Définition des paramètres du serveur proxy

Définissez les paramètres du serveur proxy pour le serveur Web et le terminal 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**.

2.6.4 Vérification de la connexion

1. Sur l'ordinateur sur lequel est installé le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Dans l'arborescence, sélectionnez le serveur adéquat et cliquez sur**Sites > Site Web par défaut > SGNSRV**.
3. Cliquez avec le bouton droit de la souris sur **SGNSRV**, sélectionnez **Gérer une application** et cliquez sur **Parcourir** pour ouvrir la page **Sophos SafeGuard Web Service**.
4. Sur la page **Sophos SafeGuard Web Service**, une liste des actions possibles apparaît. Cliquez sur **CheckConnection > Invoquer**.

La sortie suivante indique que le test de connexion a réussi :

```
<Dataroot><WebService>OK</WebService><DBAuth>OK</DBAuth>
```

Si la communication entre le client et le serveur SafeGuard Enterprise ne fonctionne pas correctement, veuillez consulter l'article 109662 de la base de connaissances de Sophos.

2.7 Sécurisation des connexions de transport avec SSL

SafeGuard Enterprise prend en charge le chiffrement des connexions de transport avec SSL entre ses composants. Vous pouvez utiliser SSL pour chiffrer le transport entre les composants suivants :

- Serveur de base de données <-> Serveur SafeGuard Enterprise avec IIS
- Serveur de base de données <-> SafeGuard Management Center
- Serveur SafeGuard Enterprise avec IIS <-> terminaux administrés

Avant d'activer SSL dans SafeGuard Enterprise, veuillez installer un environnement SSL de travail.

Les tâches générales suivantes sont nécessaires pour installer SSL :

- Facultatif : installez une autorité de certification pour générer des certificats utilisés par le chiffrement SSL.
- Un certificat doit être généré et le serveur des services Internet (IIS) configuré pour utiliser SSL et sélectionner le certificat.
- Le nom du serveur indiqué lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui indiqué sur le certificat SSL. Faute de quoi, la communication entre le client et le serveur est impossible. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.

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

Retrouvez plus de renseignements auprès de notre support technique ou consultez :

- Le document de Microsoft Comment faire pour configurer un Service HTTPS dans IIS
- Le document de Microsoft Comment activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC

Chiffrement du transport exclusif SafeGuard pour les installations de test

Pour les installations de démonstration ou de test, vous avez la possibilité de sécuriser la connexion entre le serveur SafeGuard Enterprise et les terminaux administrés par SafeGuard Enterprise avec le chiffrement exclusif SafeGuard. Pour une sécurité et des performances optimales, nous vous conseillons vivement d'utiliser la communication chiffrée avec SSL. Si, pour quelque raison que ce soit, vous ne pouvez pas le faire et que le chiffrement SafeGuard est utilisé, la connexion à une instance unique du serveur est limité à 1000 clients maximum.

Remarque : Si vous administrez des Macs, veuillez utiliser le chiffrement SSL.

2.7.1 Certificats

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

Un certificat autosigné

Si vous administrez des terminaux Mac et Windows, utilisez un certificat avec les extensions d'utilisation de clé adéquates. À partir de macOS 10.12, Apple autorise uniquement les certificats conformes à ces exigences pour établir une connexion SSL.

Vous pouvez créer un certificat avec les extensions adéquates dans IIS lorsque vous configurez la page Web SGNSRV pour SSL comme indiqué à la section Configuration de la page Web SGNSRV pour utiliser SSL *(page 52)*.

Un certificat émis par une infrastructure de clés publiques (PKI) avec un certificat privé ou un certificat racine public.

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

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

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

- Le nom du certificat doit correspondre à celui de la machine qui apparaît sur le nœud supérieur dans le gestionnaire d'Internet Information Services (IIS).
- Le certificat doit être émis sur la machine à l'aide du nom de domaine complet (FQDN). Assurez-vous que le client est en mesure de résoudre le nom FQDN par DNS.

2.7.2 Activation du chiffrement SSL dans SafeGuard Enterprise

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

  Activez le chiffrement SSL en enregistrant le serveur SafeGuard Enterprise à l'aide de l'outil de package de configuration de SafeGuard Management Center. Retrouvez plus de renseignements à la section Configuration de la connexion au serveur de base de données *(page 40)* ou dans l'article 109012 de la base de connaissances de Sophos.

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

  Activez le chiffrement SSL dans l'Assistant de configuration de SafeGuard Management Center. Retrouvez plus de renseignements à la section Configuration de la connexion au serveur de base de données *(page 40)*.

- Connexion entre le serveur SafeGuard Enterprise et le terminal protégé par SafeGuard Enterprise :

  Activez le chiffrement SSL lors de la création du package de configuration pour les terminaux administrés dans l'outil de package de configuration de SafeGuard Management Center. Retrouvez plus de renseignements à la section Création d'un package de configuration pour les terminaux *(page 59)*.

  Retrouvez plus de renseignements sur la configuration du serveur SafeGuard Enterprise afin d'utiliser SSL pour sécuriser les communications à la section Configuration de la page Web SGNSRV pour utiliser SSL *(page 52)*.

  Mettez les certificats à disposition sur les terminaux :
  - Retrouvez plus de renseignements sur les terminaux Windows à la section Assignation du certificat SSL aux terminaux Windows *(page 53)*.
  - Retrouvez plus de renseignements sur les terminaux macOS à la section Importation du certificat SSL sur les Macs *(page 54)*.

Nous vous conseillons de définir le chiffrement SSL pour SafeGuard Enterprise lors de la première configuration des composants SafeGuard Enterprise. Si vous le faites ultérieurement, vous allez devoir créer un nouveau package de configuration et l'installer sur le serveur ou sur les terminaux administrés adéquats.

2.7.3 Configuration de la page Web SGNSRV pour utiliser SSL

La description suivante fait référence à Microsoft Windows Server 2012.

1. Ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Dans le volet **Connexions**, sélectionnez le serveur qui héberge la page Web SGNSRV.
3. Dans le volet de droite, cliquez deux fois sur **Certificats de serveur** dans la section **IIS**.
   - Vous pouvez créer un certificat autosigné à utiliser pour le chiffrement du transport SSL.
   - Vous pouvez importer un certificat existant. Passez à l'étape 5.
4. Pour créer un certificat, cliquez sur **Créer un certificat auto-signé** dans le volet **Actions** sur le côté droit.

   a. Saisissez le nom du serveur qui héberge la page Web SGNSRV en tant que nom convivial et cliquez sur **OK**.
   Le certificat est affiché dans le volet **Certificats du serveur**.

   b. Cliquez deux fois sur le certificat pour exporter la partie publique.
   Distribuez la partie publique du certificat sur tous les terminaux comme indiqué aux sections Assignation du certificat SSL aux terminaux Windows *(page 53)* et Importation du certificat SSL sur les Macs *(page 54)*.

   c. Dans la boîte de dialogue **Certificat**, sélectionnez l'onglet **Détails**.

   d. Cliquez sur **Copier dans le fichier**.

   e. Dans **Assistant Exportation du certificat**, cliquez sur **Suivant**.

   f. Sélectionnez **Non, ne pas exporter la clé privée** et cliquez sur **Suivant**.

   g. Conservez la sélection par défaut du format de fichier exporté et cliquez sur **Suivant**.

   h. Cliquez sur **Parcourir**, sélectionnez un emplacement et saisissez un nom de fichier pour le fichier de certificat. Cliquez sur **Enregistrer**.

   i. Cliquez sur **Suivant**, puis sur **Terminer**.

   j. Passez à l'étape 6.

5. Pour importer un certificat, cliquez sur **Importer** dans le volet **Actions** sur le côté droit.

a. Naviguez jusqu'au fichier de certificat.

b. Sélectionnez le fichier de type **Échange d'informations personnelles** et cliquez sur **Ouvrir**.

c. Saisissez votre mot de passe et cliquez sur **OK**.
Le certificat est affiché dans le volet **Certificats du serveur**.

6. Depuis le volet **Connexions** sur la gauche, sélectionnez le nom du serveur sur lequel le certificat est installé.
7. Sous **Sites**, sélectionnez le site à sécuriser avec SSL.
8. Depuis le volet **Actions** à droite, sélectionnez **Liaisons**.
9. Dans la boîte de dialogue **Liaisons de sites**, cliquez sur **Ajouter**.
10. Sous **Type :**, sélectionnez **https** et sous **Certificat SSL :**, sélectionnez le certificat que vous avez installé auparavant.
11. Cliquez sur **OK** et fermez la boîte de dialogue **Liaisons de sites**.
12. Dans le volet de navigation, sélectionnez le serveur et cliquez sur **Redémarrer** dans le volet **Actions**.

2.7.4 Configuration des terminaux pour l'utilisation de SSL

Pour utiliser SSL sur des terminaux protégés par SafeGuard Enterprise :

1. Assignez le certificat SSL aux terminaux Windows et importez les certificats SSL sur les Macs comme indiqué aux sections Assignation du certificat SSL aux terminaux Windows *(page 53)* et Importation du certificat SSL sur les Macs *(page 54)*.
2. Créez un package de configuration client qui inclut SSL. Retrouvez plus de renseignements à la section Création d'un package de configuration pour les terminaux *(page 59)*.

2.7.5 Assignation du certificat SSL aux terminaux Windows

WinClient

Il existe plusieurs façons d'assigner un certificat à un terminal. L'une d'entre elles consiste à l'assigner à l'aide d'une stratégie de groupe Microsoft, décrite dans cette section. Si vous voulez utiliser une méthode différente, assurez-vous que le certificat est enregistré dans le magasin de certificats de l'ordinateur local.

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

1. Ouvrez la console **Gestion de la stratégie de groupe** (gpedit.msc).

2. Créez un nouvel Objet de stratégie de groupe (GPO) qui contiendra les paramètres du certificat. Assurez-vous que l'Objet de stratégie de groupe est associé au domaine, au site ou à une unité organisationnelle contenant les utilisateurs que vous souhaitez administrer avec la stratégie.
3. Cliquez avec le bouton droit de la souris sur l'Objet de stratégie de groupe et sélectionnez **Modifier**.

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

2.7.6 Importation du certificat SSL sur les Macs

Avant de procéder à l'installation, assurez-vous que le certificat SSL du serveur SafeGuard Enterprise a été importé dans le trousseau d'accès **système** et qu'il est défini sur **Toujours approuver** pour SSL.

1. Demandez à l'administrateur de votre serveur SafeGuard de vous fournir le certificat du serveur SafeGuard Enterprise pour la connexion SSL (fichier <*nom certificat*>.*cer*).

2. Importez le fichier <*nom certificat*>.*cer* dans votre trousseau d'accès. Allez dans **Applications > Utilitaires** et cliquez deux fois sur **Trousseaux d'accès.app**.

3. Dans le volet de gauche, sélectionnez **Système**.

4. Ouvrez une fenêtre Finder et sélectionnez le fichier <*nom certificat* >.*cer*.

5. Faites glisser et déposer le fichier de certificat dans la fenêtre **Trousseaux d'accès système**.

6. Saisissez votre mot de passe macOS lorsque vous y êtes invité.

7. Cliquez sur **Modifier le trousseau** pour confirmer.

8. Dans **Trousseaux d'accès.app**, cliquez deux fois sur le fichier <*nom certificat*>.*cer*.

9. Cliquez sur la flèche de gauche située à côté de **Se fier** pour ouvrir les paramètres de confiance.

10. Pour **Secure Sockets Layer (SSL)**, sélectionnez l’option **Toujours approuver**.
11. Fermez la boîte de dialogue.
12. Saisissez votre mot de passe macOS et cliquez sur **Réglages de mise à jour** pour confirmer. Un symbole + bleu apparaît dans le coin inférieur droit de l’icône de certificat. Il indique que ce certificat est marqué comme fiable pour tous les utilisateurs.

13. Ouvrez un navigateur Web et saisissez `https://<nomserveur>/SGNSRV` pour vérifier la disponibilité de votre serveur SafeGuard Enterprise.

Vous pouvez à présent commencer l’installation.

2.7.6.1 Déploiement automatisé

Utilisez la commande suivante pour importer les certificats :

sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.keychain -r trustAsRoot -p ssl « /<dossier>/<nom du certificat>.cer ».

Celle-ci peut être utilisée pour le déploiement automatisé à l’aide d’un script. Changez les noms de dossier et de certificat en fonction de vos paramètres.

2.8 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 terminal protégé par SafeGuard. Les informations sont stockées dans un package de configuration de serveur.

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

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

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

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

1. Démarrez SafeGuard Management Center.
2. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**.
3. Sélectionnez l'onglet **Serveurs**, puis **Faire de cet ordinateur un serveur SGN**. Cette option n'est pas disponible si le mode mutualisé est activé.

   L'assistant d'installation démarre automatiquement.

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

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

Remarque :

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

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

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

1. Démarrez SafeGuard Management Center.
2. Dans le menu **Outils**, cliquez sur **Outil du package de configuration**.
3. Sélectionnez l'onglet **Serveurs**, puis cliquez sur **Ajouter...**.

4. Dans la boîte de dialogue **Enregistrement du serveur**, cliquez sur **[...]** pour sélectionner le certificat machine du serveur sous C:\Program Files (x86)\Sophos\SafeGuard Enterprise \MachCert sur le serveur IIS exécutant le serveur SafeGuard Enterprise. Son nom de fichier est <Nomordinateur>.cer. Lorsque le serveur SafeGuard Enterprise est installé sur un autre ordinateur que celui sur lequel SafeGuard Management Center est installé, ce fichier .cer doit être accessible sous la forme d'une copie ou en utilisant une autorisation réseau.

   Ne sélectionnez pas le certificat MSO.

   Le nom complet de domaine (FQDN), par exemple serveur.monentreprise.com et les informations de certificat apparaissent. Lorsque vous utilisez le chiffrement de transport SSL entre le terminal et le serveur SafeGuard Enterprise, le nom du serveur indiqué ici doit être identique à celui affiché dans le certificat SSL. Sinon, ils ne peuvent pas communiquer.

5. Cliquez sur **OK**.

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

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

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

7. Cliquez sur **OK** pour confirmer le message de succès.

8. Sur l'onglet **Serveurs**, cliquez sur **Fermer**.

Vous avez terminé l'enregistrement et la configuration du serveur SafeGuard Enterprise.

Étapes suivantes :

- Installez le package de configuration du serveur (MSI) sur l'ordinateur exécutant le serveur SafeGuard Enterprise.
- Redémarrez IIS pour charger la nouvelle configuration.

À tout moment, vous pouvez changer la configuration du serveur sur l'onglet **Serveurs**.

2.8.3 Modification des propriétés du serveur SafeGuard Enterprise

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

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

Élément	Description
Scripts autorisés	Cliquez pour activer l'utilisation de l'API de SafeGuard Enterprise Management. Les tâches administratives peuvent donc être effectuées par des scripts.
Win. Auth. WHD	Cliquez pour activer l'authentification Windows pour Web Helpdesk. Par défaut, cette option est désactivée.
Récupération par mobile	Cliquez sur cette option pour activer l'envoi des clés de récupération du chiffrement intégral du disque à votre serveur Sophos Mobile.
Rôles de serveur	Cliquez pour sélectionner/dessélectionner un rôle de responsable de la sécurité responsable du serveur sélectionné.
Ajouter un rôle de serveur...	Cliquez pour ajouter d'autres rôles spécifiques de responsable de la sécurité du serveur sélectionné si besoin est. Vous êtes invité à sélectionner le certificat du serveur. Le rôle de responsable de la sécurité est ajouté et peut être affiché sous **Rôles de serveur**.
Connexion à la base de données	Cliquez sur **[...]** pour configurer une connexion à une base de données spécifique pour un serveur Web enregistré, notamment les codes d'accès de base de données et le chiffrement de transport entre le serveur Web et le serveur de base de données. Retrouvez plus de renseignements à la section Configuration de la connexion au serveur de base de données *(page 40)*. Même si la vérification de la connexion à la base de données n'a pas réussi, un nouveau package de configuration du serveur peut être créé. **Remarque :** Il n'est pas nécessaire de relancer l'assistant de configuration 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 lorsque le package du serveur mis à jour est installé sur le serveur.

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

La nouvelle configuration de serveur devient active.

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

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

Pour contourner le problème, effectuez l'une des opérations suivantes :

- Débloquez les connexions NetBIOS dans le pare-feu.
- Incluez le nom pleinement qualifié du serveur SafeGuard Enterprise dans le package de configuration du serveur. Retrouvez plus de renseignements à la section Enregistrement et configuration du serveur SafeGuard Enterprise pour un ordinateur différent *(page 56)*.

2.9 Création des packages de configuration

En fonction de la configuration requise, créez les packages de configuration appropriés pour les terminaux dans SafeGuard Management Center :

- Pour les terminaux administrés (Windows et macOS) : packages client administrés
- Pour les terminaux non administrés (Windows) : packages client autonomes

Lorsque vous créez un package client administré, le système créé un package pour Windows et un package (format ZIP) pour Mac. Le package ZIP est également utilisé par le serveur Sophos Mobile pour se connecter au serveur backend de SafeGuard Enterprise.

Le package de configuration initiale doit être installé sur les terminaux avec le logiciel de chiffrement.

2.9.1 Création d'un package de configuration pour les terminaux

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Sous **Serveur principal**, cliquez sur la liste déroulante et sélectionnez le serveur enregistré.
4. Si nécessaire, indiquez un groupe de stratégies à appliquer à l'ordinateur. Elle doit avoir été créée auparavant dans SafeGuard Management Center. Si vous voulez utiliser des comptes de service pour les tâches postérieures à l'installation sur l'ordinateur, assurez-vous d'inclure le paramètre de stratégie respectif dans ce premier groupe de stratégie. Retrouvez plus de renseignements dans le Manuel d'administration de SafeGuard Enterprise.
5. Sélectionnez le mode **Chiffrement du transport** définissant la manière de chiffrer la connexion entre le client SafeGuard Enterprise et le serveur SafeGuard Enterprise. Retrouvez plus de renseignements à la section Sécurisation des connexions de transport avec SSL *(page 49)*.
6. Indiquez un chemin de sortie pour le package de configuration (MSI).
7. Cliquez sur **Créer un package de configuration**.
   Si vous avez sélectionnez le chiffrement SSL en tant que mode de **Chiffrement du transport**, la connexion au serveur est validée. En cas d'échec de la connexion, un message d'avertissement s'affiche. Vous pouvez ignorer le message et créer le package de configuration. Toutefois, veuillez-vous assurer que la communication entre le client SafeGuard et le serveur SafeGuard est possible avec SSL.

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

2.9.2 Création d'un package de configuration pour les ordinateurs non administrés (Windows uniquement)

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client autonome**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Indiquez un **Groupe de stratégies** préalablement créé dans SafeGuard Management Center et que vous souhaitez appliquer aux ordinateurs.

6. Sous **Emplacement de la sauvegarde de la clé**, indiquez ou sélectionnez un chemin réseau partagé pour le stockage du fichier de récupération de clé. Saisissez le chemin de partage sous la forme suivante : \\ordinateur réseau\, par exemple \\monentreprise.edu\. Si vous n'indiquez pas de chemin ici, l'utilisateur final sera invité à indiquer l'emplacement de stockage de ce fichier lors de sa première connexion au terminal, suite à l'installation.

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

   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 technique d'une façon différente. Ce fichier est chiffré par le certificat d'entreprise. Il peut donc être enregistré sur un support externe ou sur le réseau pour être fourni au support technique à des fins de récupération. Il peut également être envoyé par e-mail.

7. Sous **Groupe d'authentification au démarrage**, vous pouvez sélectionner le groupe d'utilisateurs de l'authentification au démarrage à assigner au terminal. Les utilisateurs de l'authentification au démarrage peuvent accéder au terminal pour des tâches administratives après activation de l'authentification au démarrage. Pour assigner des utilisateurs de l'authentification au démarrage, le groupe d'authentification au démarrage doit avoir été préalablement créé dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center.

8. Indiquez un chemin de sortie pour le package de configuration (MSI).

9. Cliquez sur **Créer un package de configuration**.

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

2.10 Configuration de SafeGuard Enterprise sur les terminaux

Dès que le backend s'exécute, le déploiement et l'installation des clients SafeGuard Enterprise peut commencer. Nous vous conseillons de suivre les étapes préliminaires décrites dans cette section afin que la procédure d'installation se déroule facilement.

Le client SafeGuard Enterprise peut être installé sur différents types de matériel et sur différents systèmes d'exploitation. Retrouvez une liste de tous les systèmes d'exploitation pris en charge et des conditions minimales requises est disponible dans les Notes de publication.

Les recommandations générales de préparation de votre système à l'installation de SafeGuard Enterprise sont disponibles dans l'article 108088 de la base de connaissances Sophos.

2.10.1 À propos des terminaux administrés et non administrés

Vous pouvez configurer les terminaux SafeGuard Enterprise comme suit :

- **Administré**

  Administration centralisée basée sur serveur dans SafeGuard Management Center.

  Il existe une connexion au serveur SafeGuard Enterprise pour les terminaux administrés. Ils reçoivent leurs stratégies par le biais du serveur SafeGuard Enterprise.

- **Non administré**

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

  Restrictions :
  - l’administration locale n’est pas possible avec macOS.
  - Synchronized Encryption n’est pas disponible sur les terminaux non administrés.

  Les terminaux non administrés ne sont pas connectés au serveur SafeGuard Enterprise et fonctionnent donc en mode autonome. Les terminaux non administrés reçoivent les stratégies SafeGuard Enterprise par le biais des packages de configuration.

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

Différents packages d’installation et modules sont fournis pour chaque type de terminal.

2.10.2 Restrictions

Notez les restrictions suivantes pour les terminaux administrés :

- **Restrictions pour le chiffrement initial :**

  La configuration initiale des terminaux administrés peut impliquer la création de stratégies de chiffrement pouvant être distribuées aux terminaux protégés par SafeGuard Enterprise sous forme de package de configuration. Toutefois, lorsque le terminal protégé par SafeGuard Enterprise n'est pas connecté à un serveur SafeGuard Enterprise juste après l'installation

du package de configuration, mais est temporairement hors ligne, seules les stratégies de chiffrement présentant les paramètres spécifiques suivants sont immédiatement actives :

Le chiffrement intégral des disques par volume qui utilise la **Clé machine définie** en tant que 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 terminal protégé par SafeGuard Enterprise, le package de configuration correspondant doit également être réaffecté à l'unité organisationnelle du terminal. Les clés définies par l'utilisateur sont alors créées uniquement lorsque la connexion entre le terminal et le serveur SafeGuard Enterprise est rétablie.

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

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

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

2.10.3 Vérification de la disponibilité du certificat SSL sur les terminaux Windows

Le certificat doit être assigné à l'ordinateur et pas à l'utilisateur. Le fichier de certificat doit être disponible dans le magasin de certificats Microsoft sous le nom de Autorités de certification racines de confiance.

1. Ouvrez une session sur le terminal en tant qu'administrateur.
2. Cliquez sur **Exécuter** > mmc.
3. Dans la fenêtre **Console1**, cliquez sur le menu **Fichier** et cliquez sur **Ajouter/Supprimer un composant enfichable**.
4. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, sélectionnez **Certificats** dans le volet de gauche et cliquez sur **Ajouter**.

5. Sur la page Composant logiciel enfichable Certificats, sélectionnez l'option **Un compte d'ordinateur**.
6. Sur la page **Sélectionner un ordinateur**, sélectionnez **L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)** et cliquez sur **Terminer**.
7. Cliquez sur **OK** dans la boîte de dialogue **Ajouter/Supprimer un composant enfichable**.
8. Dans le volet de gauche, cliquez sur **Racine de la console > Certificats (ordinateur local) > Autorités de certification racines de confiance > Certificats**.
9. Dans le volet de droite, assurez-vous que le certificat créé auparavant est disponible dans le magasin. Si le certificat apparaît dans la liste, cette étape est terminée. En cas contraire, procédez de la manière suivante :
10. Cliquez sur **Exécuter** > gpupdate /force.
    Une fenêtre de commande Windows s'ouvre.
11. Patientez jusqu'à la fermeture de cette fenêtre et effectuez de nouveau les étapes mentionnés ci-dessus en commençant à l'étape 1.

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

Si vous souhaitez utiliser SafeGuard Enterprise pour administrer les terminaux BitLocker, effectuez les préparations spécifiques suivantes sur le terminal :

- Windows 7 ou Windows 8 doit être installé sur le terminal.
- Le Chiffrement de lecteur BitLocker doit être installé et activé.
- Le Service de chiffrement de lecteur BitLocker doit être en cours d’exécution.

  Remarque : Exécutez `services.mcs` et vérifiez si le **Service de chiffrement de lecteur BitLocker** fonctionne.

- Si TPM doit être utilisé pour l’authentification, TPM doit être initialisé, assigné à un propriétaire et activé.

2.10.5 Préparation de SafeGuard Full Disk Encryption avec l'authentification au démarrage

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

- Un compte d'utilisateur doit être configuré et actif sur les terminaux.
- Assurez-vous de disposer des droits d'administrateur Windows.
- Créez une sauvegarde complète des données sur le terminal.
- Les lecteurs à chiffrer doivent être complètement formatés et disposer d'une lettre de lecteur.

- Sophos fournit un fichier de configuration matérielle pour réduire le risque de conflits entre l'authentification au démarrage et le matériel de votre terminal. Le fichier est contenu dans le package du logiciel de chiffrement. Nous vous conseillons d'installer une version mise à jour de ce fichier avant de procéder au déploiement de SafeGuard Enterprise. Retrouvez plus de renseignements dans l'article 65700 de la base de connaissances Sophos.

  Vous pouvez nous aider à améliorer la compatibilité en exécutant un outil que nous vous fournissons pour recueillir seulement les informations matérielles correspondantes. L'outil est très simple à utiliser. Les informations recueillies sont ajoutées au fichier de configuration matérielle. Retrouvez plus de renseignements dans l'article 110285 de la base de connaissances Sophos.

- Recherchez les erreurs sur le(s) disque(s) dur(s) à l'aide de la commande suivante : chkdsk %drive% /F /V /X

  Veuillez ensuite redémarrer votre système.

  ⚠ **Important :** N'installez pas SafeGuard Enterprise avant d'avoir redémarré !

- Utilisez l'outil de défragmentation de Windows appelé defrag pour localiser et consolider les éléments fragmentés, notamment les fichiers de démarrage, les fichiers de données et les dossiers sur les volumes locaux.
- Désinstallez les gestionnaires de démarrage tiers, tels que PROnetworks Boot Pro et Boot-US.
- Si un outil d'imagerie a été utilisé pour installer le système d'exploitation, s vous conseillons de réécrire l'enregistrement de démarrage principal (MBR, master boot record).
- Si la partition de démarrage du terminal a été convertie du format FAT au format NTFS et si l'ordinateur n'a pas été redémarré depuis, redémarrez l'ordinateur une fois. Sinon, il se peut que l'installation ne se soit pas terminée avec succès.
- Pour les clients SafeGuard Enterprise (administrés) uniquement : vérifiez s'il existe une connexion avec le serveur SafeGuard Enterprise. Sélectionnez cette adresse Web dans Internet Explorer sur les terminaux : http://<AdresseIPServeur>/sgnsrv. Si la page **Trans** affiche **Vérifier la connexion**, la connexion avec le serveur SafeGuard Enterprise a été établie avec succès.

Retrouvez plus de renseignements dans l'article 108088 de la base de connaissances Sophos.

2.10.6 Préparation pour le stockage Cloud

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

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

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

Pour préparer les terminaux à l'installation de Cloud Storage :

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

2.11 Installation du logiciel de chiffrement sur Windows

La configuration du logiciel de chiffrement SafeGuard Enterprise sur les terminaux peut être effectuée de deux manières :

- Installation locale du logiciel de chiffrement (sous surveillance). Ce type d'installation est conseillée, par exemple, lors d'une installation de test.
- Installation centralisée du logiciel de chiffrement (sans surveillance). L'installation standard sur plusieurs terminaux est ainsi garantie.

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

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

2.11.1 Installation des packages et fonctions

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

L'installation par défaut contient uniquement le chiffrement intégral du disque. Sur les terminaux sous Windows 7, SafeGuard Full Disk Encryption est installé. Sur les terminaux à partir de Windows 8, BitLocker est installé. Si vous voulez installer un module de chiffrement de fichiers, veuillez sélectionner une installation **Personnalisée** et sélectionnez les composants requis. Veuillez noter que vous pouvez soit installer Synchronized Encryption soit le chiffrement de fichiers par emplacement mais pas les deux.

Si le terminal fonctionne sous un système d'exploitation Windows 64 bits, installez la variante 64 bits des packages d'installation (<nom du package>_x64.msi).

Package	Contenu	Disponible pour les terminaux administrés	Disponible pour les terminaux non administrés
SGxClientPreinstall.msi (Windows 7 uniquement)	**Package de préinstallation** Le package doit être installé avant d'installer tout package d'installation de chiffrement. Fournit aux terminaux les configurations requises pour une installation réussie du logiciel de chiffrement actuel.	✔ obligatoire	✔ obligatoire
vstor-redist.exe	**Facultatif** : uniquement nécessaire si toutes les mises à jour Windows actuelles ne sont pas installées.		
SGNClient.msi SGNClient_x64.msi	**Package d'installation du client SafeGuard** Fournit aux terminaux les configurations requises pour une installation réussie du logiciel de chiffrement actuel. Pour le chiffrement intégral		

Package	Contenu	Disponible pour les terminaux administrés	Disponible pour les terminaux non administrés
	des disques durs internes et externes, SafeGuard Enterprise offre les alternatives **SafeGuard Full Disk Encryption** ou **BitLocker**.		
	BitLocker ou **C/R BitLocker** SafeGuard Enterprise gère le moteur de chiffrement Microsoft BitLocker. Sur les plates-formes UEFI, l'authentification préalable au démarrage BitLocker s'effectue à l'aide d'un mécanisme de Challenge / Réponse SafeGuard tandis que la version BIOS permet d'obtenir la clé de récupération à partir de SafeGuard Management Center.	✔	✔
	SafeGuard Full Disk Encryption (Windows 7 BIOS uniquement) SafeGuard Full Disk Encryption inclus l'authentification au démarrage SafeGuard.	✔	✔
	Synchronized Encryption Inclut le chiffrement de fichiers par application et la fonctionnalité de fichier HTML à auto-déchiffrement permettant de chiffrer automatiquement les pièces jointes d'email à l'aide de Microsoft Outlook.	✔	✘
	Stockage Cloud Chiffrement basé sur fichier des données stockées dans le Cloud. Les copies locales des données stockées dans le Cloud sont toujours chiffrées de manière transparente. Pour envoyer ou recevoir des données depuis le Cloud, le logiciel recommandé par le fournisseur doit être utilisé.	✔	✘
	Chiffrement de fichiers Chiffrement basé sur fichier des données présentes sur les disques durs locaux et	✔	✘

Package	Contenu	Disponible pour les terminaux administrés	Disponible pour les terminaux non administrés
	sur les partages réseau, surtout pour les groupes de travail. **Échange de données** SafeGuard Data Exchange : chiffrement basé sur fichier des données présentes sur les supports amovibles sur toutes les plates-formes sans nouveau chiffrement nécessaire.	✔	✔

2.11.2 Installation locale du logiciel de chiffrement

Conditions préalables :

- Les ordinateurs d'extrémité doivent avoir été préparés pour le chiffrement, reportez-vous à la section Configuration de SafeGuard Enterprise sur les terminaux *(page 61)*.
- Décidez du package de chiffrement et des fonctions à installer. Par exemple, le package `SGxClientPreinstall.msi` n'est plus requis à partir de Windows 8. Les étapes relatives au fichier POACFG concernent uniquement le chiffrement de périphériques avec l'authentification au démarrage et BitLocker avec Challenge/Réponse.

Pour installer localement le logiciel de chiffrement :

1. Ouvrez une session sur le terminal en tant qu'administrateur.
2. Copiez les packages `SGNClient_x64.msi` et `SGxClientPreinstall.msi` sur le client.
3. Installez le package `SGxClientPreinstall.msi` pour que le terminal bénéficie des configurations requises à une installation réussie du logiciel de chiffrement actuel. Plutôt que d'utiliser `SGxClientPreinstall.msi`, vous pouvez installer le package `vcredist_x86.exe` de Microsoft qui est également fournit avec votre produit.
4. Installez le programme `vcredist14_x86.exe` fourni avec le produit.
5. Téléchargez le fichier POACFG comme indiqué dans l'article 65700 de la base de connaissances Sophos.
6. Enregistrez la dernière version du fichier POACFG sous un emplacement central accessible à tous les terminaux.

7. Ouvrez une ligne de commande administrative sur le client.
8. Passez dans le dossier contenant les fichiers d’installation de SafeGuard.
9. Commencez l’installation avec cette commande : `MSIEXEC /i <client.msi> POACFG=<chemin du fichier de configuration POA>`
   L’assistant d’installation du client SafeGuard Enterprise s’ouvre.
10. Dans l’assistant, validez les valeurs par défaut dans toutes les boîtes de dialogue qui suivent. Dans une première installation, nous vous conseillons de sélectionner une installation **Complète** dès le départ. Pour installer uniquement un sous-ensemble de fonctions, sélectionnez l’installation **Custom**.
11. Accédez à l’emplacement d’enregistrement du package de configuration correspondant (MSI) créé auparavant dans SafeGuard Management Center. Des packages de configuration spécifiques doivent être installés pour les terminaux administrés et non administrés comme indiqué à la section Création des packages de configuration *(page 59)*.
12. Installez le package de configuration (MSI) correspondant sur l’ordinateur.
13. Pour activer l’authentification au démarrage, veuillez redémarrer le terminal à deux reprises.
14. Redémarrez le terminal une troisième fois pour effectuer une sauvegarde des données de noyau à chaque initialisation Windows. Assurez-vous que l’ordinateur n’est pas en veille prolongée, en mode de veille ou en mode de veille hybride avant le troisième redémarrage pour exécuter avec succès la sauvegarde du noyau.

SafeGuard Enterprise est installé sur le terminal. Retrouvez plus de renseignements le comportement de connexion de l’ordinateur après l’installation de SafeGuard Enterprise dans le *Manuel d’utilisation de* SafeGuard Enterprise.

2.11.3 Installation centralisée du logiciel de chiffrement

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

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

Pour une installation centrale, effectuez les opérations suivantes :

- Vérifiez les packages et les fonctions de chiffrement disponibles pour les terminaux administrés et non administrés comme indiqué à la section Installation des packages et fonctions *(page 67)*.
- Vérifiez les options de ligne de commande.

- Vérifiez la liste des paramètres des fonctions pour l'option de ligne de commande ADDLOCAL.
- Vérifiez les exemples de commandes.
- Préparez le script d'installation.

2.11.3.1 Installation centralisée du logiciel de chiffrement avec Active Directory

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

Remarque : Dans le cadre de la distribution centralisée des logiciels, les packages d’installation et de configuration peuvent uniquement être attribués à un terminal et non à un utilisateur.

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

  1. package de préinstallation
  2. package du logiciel de chiffrement
  3. package de configuration du terminal

  Retrouvez plus de renseignements sur les packages à la section Préparation du script d’installation *(page 71)*.

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

2.11.3.2 Préparation du script d’installation

Conditions préalables :

- Les terminaux doivent avoir été préparés pour le chiffrement.
- Décidez du package de chiffrement et des fonctions à installer.

Pour installer le logiciel de chiffrement de manière centralisée :

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

Package	Description
Package de préinstallation SGxClientPreinstall.msi **(Windows 7 uniquement)**	Le package obligatoire fournit aux terminaux la configuration requise pour une installation réussie du logiciel de chiffrement actuel, par exemple la DLL requise MSVCR100.dll. **Remarque :** Si ce package n'est pas installé, l'installation du logiciel de chiffrement échoue.
Package du logiciel de chiffrement	Pour une liste des packages disponibles, reportez-vous à la section Installation des packages et fonctions *(page 67)*.
Package de configuration pour les terminaux	Utilisez les packages de configuration créés auparavant dans SafeGuard Management Center. Différents packages de configuration doivent être installés pour les terminaux administrés et non administrés comme indiqué à la section Création des packages de configuration *(page 59)*. Veillez à d'abord supprimer toutes les anciennes versions.

3. Créez un script avec les commandes de l'installation préconfigurée. Le script doit indiquer quelles fonctions du logiciel de chiffrement vous voulez installer comme indiqué à la section Paramètres des fonctions de l'option ADDLOCAL *(page 74)*. Ouvrez une invite de commande et saisissez les commandes de script. Pour la syntaxe de ligne de commande, reportez-vous à la section Options de ligne de commande pour l'installation centralisée *(page 73)*.

4. Distribuez ce package sur les terminaux à l'aide des mécanismes de distribution de logiciels de l'entreprise.

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

5. Pour activer l'authentification au démarrage, veuillez redémarrer le terminal à deux reprises. Redémarrez le terminal une troisième fois pour effectuer une sauvegarde des données de noyau à chaque initialisation Windows. Assurez-vous que l'ordinateur n'est pas en veille prolongée, en mode de veille ou en mode de veille hybride avant le troisième redémarrage pour exécuter avec succès la sauvegarde du noyau.

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

Windows Installer. Retrouvez plus de renseignements dans les articles 107781 et 107785 de la base de connaissances Sophos.

2.11.3.3 Préparation pour Synchronized Encryption

Pour un fonctionnement correct du module Synchronized Encryption, veuillez installer le programme `vstor-redist.exe` de Microsoft. Ce fichier va installer Microsoft Visual Studio 2010 Tools for Office Runtime et il est inclus dans le package d'installation.

Nous vous conseillons d'installer les composants dans l'ordre suivant :

1. `vstor-redist.exe`
2. `SGNClient.msi`
3. package de configuration

Remarque : Vous pouvez déployer le package de configuration pendant l'installation de `vstor-redist.exe`.

2.11.3.4 Options de ligne de commande pour l’installation centralisée

Pour une installation centrale, nous conseillons de préparer un script utilisant le composant Windows Installer msiexec qui effectue automatiquement une installation préconfigurée de SafeGuard Enterprise. msiexec est inclus dans Windows. Retrouvez plus de renseignements sur https://msdn.microsoft.com/fr-fr/library/aa372024(v=vs.85).aspx.

Syntaxe de la ligne de commande

```
msiexec /i <chemin+nom package msi> / ADDLOCAL=<Fonctions SGN>
```

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

- Les paramètres de Windows Installer qui, par exemple, consignent les avertissements et les messages d’erreur dans un fichier journal lors de l’installation.
- Les fonctions de SafeGuard Enterprise à installer, par exemple, le chiffrement intégral du disque.

Options de ligne de commande

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

Option	Description
/i	Indique qu'il s'agit d'une installation.
/qn	Exécute une installation sans interaction de l'utilisateur et n'affiche pas d'interface utilisateur.
ADDLOCAL=	Répertorie les fonctions SafeGuard Enterprise à installer. Si l'option n'est pas indiquée, toutes les fonctions d'une installation standard sont installées. Retrouvez une liste des fonctions de SafeGuard Enterprise dans chaque package d'installation et de leur disponibilité selon la configuration du terminal à la section Installation des packages et fonctions *(page 67)*. Retrouvez une liste des paramètres des fonctions pour l'option ADDLOCAL à la section Paramètres des fonctions de l'option ADDLOCAL *(page 74)*.
ADDLOCAL=ALL	Sous Windows 7 (BIOS), ADDLOCAL=ALL installe le chiffrement SafeGuard à base de volumes et toutes les autres fonctions disponibles. À partir de Windows 8, ADDLOCAL=ALL installe la prise en charge de BitLocker et Synchronized Encryption.
REBOOT=NORESTART | ReallySuppress	Force ou supprime un redémarrage après l'installation. Si rien n'est spécifié, le redémarrage est forcé après l'installation.
/L*VX `<chemin + nom de fichier>`	Consigne tous les avertissements et messages d'erreur dans le fichier journal spécifié. Le paramètre /Le `<chemin + nom de fichier>` ne journalise que les messages d'erreur.

2.11.3.5 Paramètres des fonctions de l'option ADDLOCAL

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

- Séparez les fonctions par une virgule.
- Respectez les caractères majuscules et minuscules.
- Si vous sélectionnez une fonction, vous devez également ajouter toutes les fonctions parentes à la ligne de commande.
- Veuillez noter que les noms des fonctions peuvent être différents des noms de modules correspondants. Vous les retrouverez dans le tableau ci-dessous entre parenthèses.
- Veuillez toujours indiquer les fonctions **Client** et **CredentialProvider**.

Le tableau ci-dessous dresse la liste des fonctions qui peuvent être installées sur les terminaux. Retrouvez plus de renseignements sur : Installation des packages et fonctions *(page 67)*.

Fonctions parentes	Fonction
Client	**CredentialProvider** Obligatoire. La fonction active la connexion avec le fournisseur de codes d'accès.
Client, **BaseEncryption**	**SectorBasedEncryption** (chiffrement de volumes SafeGuard)
Client,**BaseEncryption**	**BitLockerSupport** Windows 7 uniquement : **SectorBasedEncryption** **BitLockerSupport** (BitLocker)
Client,**BaseEncryption**,**BitLockerSupport**	**BitLockerSupportCR** (C/R BitLocker)
Client, **NextGenDataProtection**	**NextGenDataProtection** (Synchronized Encryption)
Client, **LocationBasedEncryption**	**SecureDataExchange** (Data Exchange)
Client, **LocationBasedEncryption**	**FileShare** (chiffrement de fichiers)
Client, **LocationBasedEncryption**	**CloudStorage** (Cloud Storage)

2.11.3.6 Exemple de commandes : installation de SafeGuard File Encryption uniquement

```
msiexec /i C:\Software\SGxClientPreinstall.msi /qn /L*VX C:\Temp
\SGxClientPreinstall.log
```

Les terminaux reçoivent la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement. Un fichier journal SGxClientPreinstall.log est créé dans C:\Temp\.

Utilisez l'option /L*VX si vous avez un problème avec un package d'installation. Ceci n'est pas obligatoire.

```
msiexec /i C:\Software\SGNClient.msi
ADDLOCAL=Client,CredentialProvider,LocationBasedEncryption,FileShare
```

Les composants suivants sont installés :

- Connexion aux terminaux à l'aide du fournisseur de codes d'accès Windows.
- SafeGuard File Encryption avec le chiffrement des données basé sur fichier sur le disque dur local et les partages réseau.

Le répertoire d'installation est C:\Program Files\Sophos\SafeGuard Enterprise.

```
msiexec /i C:\Software\SGNConfig_managed.msi
```

Installe le package de configuration qui configure le terminal en tant que terminal administré et permet la connexion au serveur SafeGuard Enterprise.

2.11.3.7 Exemple de commandes : installation de la prise en charge de SafeGuard BitLocker

```
msiexec /i C:\Software\SGxClientPreinstall.msi
```

Les terminaux reçoivent la configuration requise pour garantir la réussite de l’installation du logiciel de chiffrement.

```
msiexec /i C:\Software\SGNClient_x64.msi
ADDLOCAL=Client,CredentialProvider,BaseEncryption,BitLockerSupport
```

Les composants suivants sont installés :

- Connexion aux terminaux à l’aide du fournisseur de codes d’accès Windows.
- Prise en charge de SafeGuard BitLocker.

Le répertoire d’installation est C:\Program Files\Sophos\SafeGuard Enterprise.

```
msiexec /i C:\Software\SGNConfig_managed.msi
```

Installe le package de configuration qui configure le terminal en tant que terminal administré et permet la connexion au serveur SafeGuard Enterprise.

2.11.3.8 Exemple de commandes : installation de la prise en charge de SafeGuard BitLocker et du Chiffrement des fichiers

```
msiexec /i C:\Software\SGxClientPreinstall.msi
```

Les terminaux reçoivent la configuration requise pour garantir la réussite de l’installation du logiciel de chiffrement.

```
msiexec /i C:\Software\SGNClient_x64.msi
ADDLOCAL=Client,CredentialProvider,BaseEncryption,BitLockerSupport,LocationBasedEncryptio
```

Les composants suivants sont installés :

- Connexion aux terminaux à l’aide du fournisseur de codes d’accès Windows.
- Prise en charge de SafeGuard BitLocker.

- SafeGuard File Encryption avec le chiffrement des données basé sur fichier sur le disque dur local et les partages réseau.

Le répertoire d'installation est C:\Program Files\Sophos\SafeGuard Enterprise.

```
msiexec /i C:\Software\SGNConfig_managed.msi
```

Installe le package de configuration qui configure le terminal en tant que terminal administré et permet la connexion au serveur SafeGuard Enterprise.

2.11.4 Installations sur les disques durs à chiffrement automatique compatibles Opal

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

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

- **Vérifications fonctionnelles**

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

- **Vérifications de sécurité**

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

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

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

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

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

```
MSIEXEC /i SGNClient.msi OPALMODE=0
```

Remarque : La mise à niveau de SafeGuard Enterprise 7.0 ou 8.0 vers SafeGuard Enterprise 8.3 sur un système équipé d’un disque dur Opal utilisé en mode de chiffrement HW Opal conservera le mode de chiffrement HW.

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

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

```
MSIEXEC /i SGNClient.msi IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

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

2.12 Installation du logiciel de chiffrement sur macOS

Le chapitre suivant décrit l’installation du logiciel de chiffrement Sophos sur les clients macOS. Les produits suivants sont disponibles :

- Sophos SafeGuard Native Device Encryption
- Sophos SafeGuard File Encryption

Deux méthodes d'installation sont possibles pour ces produits :

- Installation automatisée (sans surveillance)
- Installation manuelle (sous surveillance).

Si vous voulez utiliser SafeGuard File Encryption et SafeGuard Native Device Encryption, veuillez utiliser la version 8 de ces deux logiciels.

2.12.1 Installation automatisée de SafeGuard Native Device Encryption

L'installation automatisée (sans surveillance) ne nécessite aucune intervention de la part de l'utilisateur pendant la procédure d'installation.

Cette section décrit les étapes de base pour l'installation automatisée de SafeGuard Native Device Encryption pour Mac. Veuillez utiliser le logiciel d'administration installé sur votre système. Les étapes peuvent varier selon la solution d'administration que vous utilisez.

Pour installer SafeGuard Native Device Encryption pour Mac sur les ordinateurs clients, effectuez les étapes suivantes :

1. Téléchargez le programme d'installation *Sophos SafeGuard DE.dmg*.

2. Copiez le fichier sur les machines cibles.

3. Installez le fichier sur les machines cibles. Si vous utilisez Apple Remote Desktop, les étapes 2 et 3 représentent une seule et même étape.

4. Sélectionnez le fichier ZIP de configuration et copiez-le sur les machines cibles. Retrouvez plus de renseignements à la section Création d'un package de configuration pour les Macs *(page 106)*.

5. Exécutez la commande suivante sur les machines cibles :
   /usr/bin/sgdeadmin --import-config /full/path/to/SGNConfig_managed.zip

6. Changez */full/path/to/file* en fonction de vos paramètres. Cette commande doit être exécutée à l'aide des droits administrateur. Si vous utilisez Apple Remote Desktop, saisissez `root` dans le champ **Nom d'utilisateur** pour indiquer quel utilisateur a émis la commande mentionnée ci-dessus.

   Retrouvez plus de renseignements dans l'article 120507 de la base de connaissances Sophos.

2.12.2 Installation manuelle de SafeGuard Native Device Encryption

Une installation manuelle (ou sous surveillance) vous permet de contrôler et de tester l'installation étape par étape. Elle est effectuée sur un seul Mac.

1. Ouvrez le fichier *Sophos SafeGuard DE.dmg*.
2. Après avoir lu le fichier « readme », cliquez deux fois sur *Sophos SafeGuard DE.pkg* et suivez les instructions de l'assistant d'installation. Vous allez être invité à saisir votre mot de passe pour permettre l'installation du nouveau logiciel. Le produit va être installé dans le dossier */Library/Sophos SafeGuard DE/*.
3. Cliquez sur **Fermer** pour terminer l'installation.
4. Suite au redémarrage de l'ordinateur, connectez-vous à l'aide de votre mot de passe Mac.
5. Ouvrez les **Préférences Système** et cliquez sur l'icône Sophos Encryption pour afficher les paramètres du produit.
   
6. Cliquez sur l'onglet **Serveur**.
7. Si les informations du serveur et du certificat apparaissent, passez les étapes suivantes et rendez-vous directement à l'étape 11. Si aucune information n'apparaît, passez à l'étape suivante.
8. Sélectionnez le fichier ZIP de configuration et copiez-le sur les machines cibles. Retrouvez plus de renseignements à la section Création d'un package de configuration pour les Macs *(page 106)*.
9. Faites glisser le fichier ZIP dans la boîte de dialogue **Serveur** et déposez-le dans la zone de dépôt.
10. Vous allez être invité à saisir un mot de passe d'administrateur Mac. Saisissez le mot de passe et cliquez sur **OK** pour confirmer.
11. Vérifiez la connexion au serveur SafeGuard Enterprise : les détails du certificat d'entreprise sont affichés dans la section inférieure de la boîte de dialogue **Serveur**. Cliquez ensuite sur **Synchroniser**. Une connexion réussie entraînera la mise à jour des informations sous « Dernier contact » (Onglet **Serveur**, zone **Informations sur le serveur**, **Dernier contact :**). Un échec de la connexion sera indiqué par l'icône ci-dessous :
    
    Retrouvez plus de renseignements dans le fichier d'historique du système.

2.12.3 Installation automatisée de SafeGuard File Encryption

L'installation automatisée (sans surveillance) ne nécessite aucune intervention de la part de l'utilisateur pendant la procédure d'installation.

Cette section décrit les étapes de base pour l'installation automatisée de SafeGuard File Encryption pour Mac. Veuillez utiliser le logiciel d'administration installé sur votre système. Les étapes peuvent varier selon la solution d'administration que vous utilisez.

Pour installer SafeGuard File Encryption pour Mac sur les ordinateurs clients, effectuez les étapes suivantes :

1. Téléchargez le programme d'installation *Sophos SafeGuard FE.dmg*.
2. Copiez le fichier sur les machines cibles.
3. Installez le fichier sur les machines cibles. Si vous utilisez Apple Remote Desktop, les étapes 2 et 3 représentent une seule et même étape.
4. Sélectionnez le fichier ZIP de configuration et copiez-le sur les machines cibles. Retrouvez plus de renseignements à la section Création des packages de configuration *(page 59)*.
5. Exécutez la commande suivante sur les machines cibles :
   /usr/bin/sgdeadmin --import-config /full/path/to/file.zip
6. Changez */full/path/to/file* en fonction de vos paramètres. Cette commande doit être exécutée à l'aide des droits administrateur. Si vous utilisez Apple Remote Desktop, saisissez `root` dans le champ **Nom d'utilisateur** pour indiquer quel utilisateur a émis la commande mentionnée ci-dessus.
7. Vous pouvez ajouter des étapes supplémentaires à votre processus en fonction de vos paramètres (par exemple, arrêter les machines cibles).
   Retrouvez plus de renseignements dans l'article 120507 de la base de connaissances de Sophos.

2.12.4 Installation manuelle de SafeGuard File Encryption

Une installation manuelle (ou sous surveillance) vous permet de contrôler et de tester l'installation étape par étape. Elle est effectuée sur un seul Mac.

1. Ouvrez le fichier *Sophos SafeGuard FE.dmg*.
2. Après avoir lu le fichier « readme », cliquez deux fois sur *Sophos SafeGuard FE.pkg* et suivez les instructions de l'assistant d'installation. Vous allez être invité à saisir votre mot de passe

pour permettre l'installation du nouveau logiciel. Le produit va être installé dans le dossier */Library/Sophos SafeGuard FS/*.

3. Cliquez sur **Fermer** pour terminer l'installation.
4. Ouvrez les **Préférences Système** et cliquez sur l'icône Sophos Encryption pour afficher les paramètres du produit.
   
5. Cliquez sur l'onglet **Serveur**.
6. Si les informations du serveur et du certificat apparaissent, passez les étapes suivantes et rendez-vous directement à l'étape 11. Si aucune information n'apparaît, passez à l'étape suivante.
7. Sélectionnez le fichier ZIP de configuration et copiez-le sur les machines cibles. Retrouvez plus de renseignements à la section Création des packages de configuration *(page 59)*.
8. Faites glisser le fichier ZIP dans la boîte de dialogue **Serveur** et déposez-le dans la zone de dépôt.
9. Vous allez être invité à saisir un mot de passe d'administrateur Mac. Saisissez le mot de passe et cliquez sur **OK** pour confirmer.
10. Saisissez votre mot de passe Mac pour demander votre certificat d'utilisateur SafeGuard.
11. Vérifiez la connexion au serveur SafeGuard Enterprise : les détails du certificat d'entreprise sont affichés dans la section inférieure de la boîte de dialogue **Serveur**. Cliquez ensuite sur **Synchroniser**. Une connexion réussie entraînera la mise à jour des informations sous « Dernier contact » (Onglet **Serveur**, zone **Informations sur le serveur**, **Dernier contact :**). Un échec de la connexion sera indiqué par l'icône ci-dessous :
    
    Retrouvez plus de renseignements dans le fichier d'historique du système.

2.13 Installation de Web Helpdesk

Web Helpdesk est installé dans le cadre de l'installation du serveur SafeGuard Enterprise comme indiqué à la section Installation du serveur SafeGuard Enterprise. *(page 27)*.

Après l'installation de Web Helpdesk, vous devez configurer le serveur Web.

Un seul navigateur Internet doit être installé sur l'ordinateur du responsable de Web Helpdesk.

2.13.1 Configuration requise du serveur

La configuration requise du serveur est décrite en détail dans les Notes de publication.

- Assurez-vous de disposer des droits d'administration Windows.
- Les services Internet (IIS) de Microsoft doivent être installés.
- .NET Framework 4.5 et ASP.NET 4.5 doivent être installés.
- Pour Windows Server 2012 : le rôle ASP.NET doit être installé (Rôles du serveur > Serveur Web (IIS) > Serveur Web > Développement d'applications > ASP.NET 4.5).

Remarque : Pour Windows Server 2012, les conditions suivantes s'appliquent : les applications ASP.NET sont livrées pré-connectées avec une section Gestionnaires dans web.config. Dans la Délégation des fonctionnalités des services Internet (IIS), l'option est paramétrée sur lecture seule. Dans le Gestionnaire des services Internet (IIS), vérifiez en allant dans nom du serveur > délégation des fonctionnalités. Si les mappages de gestionnaires ne sont pas en lecture seule et que les fichiers web.config du site ont une section Gestionnaires, veuillez changer la valeur sur Lecture/écriture.

2.13.2 Configuration du serveur Web avec SSL/TLS

1. Déployez Web Helpdesk uniquement sur intranet.
   Pour des raisons de sécurité, n'accordez pas l'accès à Web Helpdesk sur Internet.

2. Établissez une connexion SSL/TLS.
   Vous pouvez limiter la disponibilité de Web Helpdesk aux utilisateurs définis en utilisant la configuration des services Internet (IIS) standard fournie avec les des services Internet. Assurez-vous que le certificat de sécurité SSL/TLS est installé sur le serveur des services Internet (IIS). Toutes les communications de Web Helpdesk seront prises en charge via le protocole SSL/TLS. Les tâches générales suivantes doivent être effectuées pour l'installation du serveur Web pour SSL/TLS :
   a. Une autorité de certification doit être installée pour générer des certificats utilisés pour le chiffrement SSL/TLS.
   b. Un certificat doit être généré et le serveur des services Internet (IIS) configuré pour utiliser SSL/TLS et sélectionner le certificat.
   c. Le nom du serveur indiqué lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui indiqué dans le certificat SSL/TLS. Faute de quoi, la communication entre le client et le serveur est impossible. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.
   d. Les processus de travail du pool d'applications SGNWHD-Pool ne doivent pas être supérieurs à 1 (valeur par défaut). Faute de quoi, l'autorisation d'accès à Web Helpdesk est impossible.

Retrouvez plus de renseignements auprès de notre support technique ou consultez :

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

2.13.3 Langues prises en charge

Web Helpdesk prend en charge plusieurs langues. Vous pouvez modifier de façon dynamique la langue de l'application dans l'écran Connexion de Web Helpdesk. Cliquez sur la langue souhaitée que l'application utilise alors immédiatement.

2.14 À propos de la mise à niveau

À partir de la version 8.0, SafeGuard Enterprise peut être directement mis à niveau vers la dernière version de SafeGuard Enterprise. Si vous voulez procéder à la mise à niveau à partir d'anciennes versions, commencez par une mise à niveau vers la version 8.0.

Pendant la mise à niveau, vous ne pouvez pas modifier les fonctions ou modules installés. Si des modifications sont nécessaires, veuillez exécuter de nouveau le programme d'installation de la version déjà en place pour modifier l'installation. Retrouvez plus de renseignements à la section À propos de la migration *(page 88)*.

Pour que l'opération réussisse, les numéros de versions de la base de données SafeGuard Enterprise, du serveur SafeGuard et de SafeGuard Management Center doivent correspondre. Ils doivent être à la même version que celle des clients ou à une version plus récente. La gestion des nouveaux clients (par exemple 8.10) avec des composants backend plus anciens (par exemple 8.0) n'est pas prise en charge.

Les composants suivants sont mis à niveau au cours de la mise à niveau vers la dernière version de SafeGuard Enterprise. Procédez à la mise à niveau dans l'ordre ci-dessous :

1. SafeGuard Management Center (avec la mise à niveau de la base de données)
2. SafeGuard Enterprise Server et Web Helpdesk
3. Terminaux protégés par SafeGuard Enterprise
4. Packages de configuration SafeGuard Enterprise

Par défaut, toutes les stratégies **Chiffrement de fichiers** sont converties ou traitées comme des stratégies au **Type de chiffrement** défini **Par emplacement**.

Remarque : Dès que tous les composants de SafeGuard Enterprise et que tous les terminaux ont été mis à niveau, nous vous conseillons d'utiliser l'algorithme **SHA-256** plus sécurisé pour signer

les certificats générés par SafeGuard Enterprise. Retrouvez plus de renseignements à la section Modification de l’algorithme pour les certificats autosignés *(page 182)*.

2.14.1 Mise à niveau de SafeGuard Management Center

Conditions préalables :

- SafeGuard Management Center 8.0 ou une version supérieure doit être installé. Les versions antérieures à la version 8.0 doivent d’abord être mises à niveau vers SafeGuard Management Center 8.0.
- Pour que l’opération réussisse, les numéros de versions de la base de données SafeGuard Enterprise, du serveur SafeGuard et de SafeGuard Management Center doivent correspondre.
- SafeGuard Management Center 8.30 peut administrer les terminaux protégés par la version 6.0 ou supérieure de SafeGuard Enterprise.
- .NET Framework 4.5 est requis. Il doit être installé avant la mise à niveau. Il est fourni avec le produit SafeGuard Enterprise.
- Assurez-vous de disposer des droits d’administrateur Windows.

Pour mettre à niveau SafeGuard Management Center :

1. Installez la dernière version du package d’installation de SafeGuard Management Center avec les fonctions requises. Retrouvez plus de renseignements à la section À propos de la migration *(page 88)*.
2. Démarrez SafeGuard Management Center.
3. Le système vérifie la version de la base de données SafeGuard Enterprise et la met automatiquement à niveau à la nouvelle version.
4. Le système vous invite à effectuer une copie de sauvegarde de votre base de données avant la mise à jour.

SafeGuard Management Center et la base de données sont mis à niveau vers la dernière version.

Suite à la mise à niveau, ne transférez pas les utilisateurs de l’authentification au démarrage sur les terminaux protégés par SafeGuard Enterprise. En effet, ils seraient considérés comme des utilisateurs normaux et enregistrés comme utilisateurs sur les terminaux respectifs.

Si vous avez exporté des stratégies pour effectuer des copies de sauvegarde, veuillez les exporter de nouveau suite à la mise à niveau de SafeGuard Management Center. Les stratégies exportés à l’aide d’anciennes versions ne peuvent pas être importées.

2.14.2 Mise à niveau du serveur SafeGuard Enterprise et de Web Helpdesk

À partir de la version 8.1, Web Helpdesk est inclus dans le package d'installation du serveur SafeGuard Enterprise. Lorsque vous procédez à la mise à niveau du serveur SafeGuard Enterprise, Web Helpdesk est automatiquement mis à jour.

Conditions préalables

- La version 8.0 supérieure de SafeGuard Enterprise Server doit être installée. Les versions antérieures doivent d'abord être mises à niveau vers SafeGuard Enterprise Server 8.0.
- .NET Framework 4.5 et ASP.NET 4.5 (livrés avec SafeGuard Enterprise) doivent être installés.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour mettre à niveau le serveur SafeGuard Enterprise :

Installez la dernière version du package d'installation du serveur SafeGuard Enterprise avec `SGNServer.msi`.

Dès que tous les composants SafeGuard Enterprise (Management Center, serveur, Web Helpdesk) ont été mis à niveau, veuillez redémarrer le serveur SafeGuard Enterprise.

2.14.3 Mise à niveau des terminaux

Cette section concerne les terminaux administrés et non administrés.

Conditions préalables

- La version 8.0 ou supérieure du logiciel de chiffrement SafeGuard Enterprise doit être installée. Les anciennes versions doivent d'abord être mises à niveau vers la version 8.0.

- La base de données SafeGuard Enterprise, le serveur SafeGuard Enterprise et SafeGuard Management Center doivent avoir été mis à jour vers la dernière version. Pour que l'opération réussisse, les numéros de versions de la base de données SafeGuard Enterprise, du serveur SafeGuard et de SafeGuard Management Center doivent correspondre.

- SafeGuard Management Center 8.30 et SafeGuard Enterprise Server 8.30 peuvent administrer les terminaux protégés à partir de la version 6.0 de SafeGuard Enterprise. Toutefois, nous vous conseillons d'utiliser la même version que celle du logiciel de chiffrement sur tous les terminaux.

- Assurez-vous de disposer des droits d’administrateur Windows.

Pour mettre à niveau les terminaux protégés par SafeGuard Enterprise :

1. Ouvrez une session sur l’ordinateur en tant qu’administrateur.
2. Installez le package de préinstallation `SGxClientPreinstall.msi` le plus récent. Il va fournir au terminal la configuration requise pour une installation réussie du nouveau logiciel de chiffrement.
   N’installez pas d’anciens packages de préinstallation car ceux-ci sont mis à jour automatiquement.
3. Installez la dernière version du logiciel de chiffrement SafeGuard Enterprise. Selon la version que vous avez installée, il est possible que la mise à niveau directe ne soit pas prise en charge. Les anciennes versions doivent être mises à niveau version par version jusqu’à la version 8.0.

   Windows Installer reconnaît les fonctions déjà installées et les met à niveau. Si l’authentification au démarrage est installée, un noyau de l’authentification au démarrage mis à jour est également disponible après une mise à jour réussie (stratégies, clés, etc.). SafeGuard Enterprise est automatiquement redémarré sur l’ordinateur.
4. Suite à l’installation, redémarrez le terminal lorsque vous y êtes invité.

   ⚠ **Important :** Redémarrez le système lorsque vous y êtes invité. Tant que vous ne redémarrez pas, le fournisseur de codes d’accès SafeGuard ne sera pas disponible. Sous Windows 10, l’arrêt et le démarrage du terminal ne remplace pas le redémarrage. Vous devez actuellement redémarrer le système.

La dernière version du logiciel de chiffrement SafeGuard Enterprise est installée sur les terminaux. Procédez ensuite à la configuration du terminal.

Remarque : Vous ne pouvez pas modifier les modules installés pendant la mise à niveau. Retrouvez plus de renseignements sur les modifications à la section À propos de la migration *(page 88)*.

2.14.4 Mise à niveau des packages de configuration des terminaux

Suite à la mise à niveau du logiciel backend de SafeGuard, nous vous conseillons vivement de supprimer tous les anciens packages de configuration pour des raisons de sécurité. De nouvelles installations du client SafeGuard doivent être effectuées à l'aide d'un package de configuration du terminal créé dans la version 8.30 de SafeGuard Management Center. Les packages de configuration

générés à l'aide d'une version précédente de SafeGuard Management Center ne sont pas pris en charge.

Les packages de configuration pour terminaux installés sur les terminaux dé configurés doivent être mis à niveau dans les cas suivants :

- Un des serveurs SafeGuard configuré a changé (applicable uniquement aux terminaux administrés).
- Les stratégies doivent être modifiées (applicable uniquement aux terminaux autonomes).
- Application d'un ordre de changement du certificat (CCO, Certificate Change Order).
- Lorsque l'algorithme de hachage utilisé pour signer les certificats autosignés passe de SHA-128 à SHA-256.

Retrouvez plus de renseignements à la section Modification de l’algorithme pour les certificats autosignés *(page 182)*.
Il n'est pas possible de remettre un terminal administré en mode autonome en désinstallant le package de configuration administré et en installant un package de configuration non administré.

2.15 À propos de la migration

La migration signifie le changement de produits, modules ou de fonctions installés sur la même version. Il pourrait donc être nécessaire de migrer votre produit dans le cadre de votre ancienne version ou de procéder d’abord à la mise à niveau de l’installation puis à la migration.

Si vous ne trouvez pas le produit ou la version du produit que vous utilisez dans ce guide, ceci signifie que la mise à niveau ou la migration directe n’est pas prise en charge. Veuillez consulter la documentation de votre produit pour plus d’informations sur une mise à niveau éventuelle ou sur les chemins de migration.

Si votre cas de figure de migration implique la modification de la licence de votre logiciel de chiffrement Sophos, assurez-vous que votre nouvelle licence est disponible pour la migration.

2.15.1 Modification de l’installation de SafeGuard sur les terminaux

Si des modifications des modules installés sont nécessaires, veuillez exécuter de nouveau le programme d’installation de la version déjà en place pour modifier l’installation.

Veuillez remarquer que :

- **Synchronized Encryption** ne peut pas être installé sur les terminaux sur lesquels le **Chiffrement de fichiers** (chiffrement de fichiers par emplacement est déjà installé.

- Le passage de **SafeGuard Full Disk Encryption** (chiffrement par volume) à **BitLocker** ou vice-versa nécessite la désinstallation et la réinstallation du produit. Les fichiers chiffrés doivent être déchiffrés.
- Le passage de la prise en charge BitLocker à BitLocker avec Challenge/Réponse ou vice versa nécessite la désinstallation et la réinstallation du produit. Les fichiers chiffrés doivent être déchiffrés.
- Le passage de **Data Exchange** au **Chiffrement de fichiers** nécessite de redémarrer deux fois l'ordinateur et de disposer d'une connexion qui va activer le chiffrement transparent sur les partages réseau.

Retrouvez plus de renseignements sur les conditions requises pour chaque module dans les Notes de publication.

Retrouvez plus de renseignements sur la migration à un autre système d'exploitation à la section Migration des terminaux vers un autre système d'exploitation *(page 89)*.

2.15.2 Migration des terminaux vers un autre système d'exploitation

Les terminaux sur lesquels SafeGuard Enterprise est installé peuvent être migrés de Windows 7/8 à Windows 10. Pour les terminaux exécutant Windows 7 et SafeGuard Full Disk Encryption, veuillez d'abord désinstaller ce dernier avant de migrer vers Windows 10. SafeGuard Full Disk Encryption n'est pas compatible avec Windows 10. Retrouvez plus de renseignements sur la désinstallation à la section À propos de la désinstallation *(page 373)*. Retrouvez plus de renseignements sur l'utilisation de BitLocker à la section Préparation pour la prise en charge du Chiffrement de lecteur BitLocker *(page 64)*.

Il n'est pas possible de migrer les terminaux de Windows 7 vers Windows 8 lorsque SafeGuard Enterprise est installé. Si vous utilisez des systèmes d'exploitation plus anciens que Windows 10, il est uniquement possible de mettre à jour la version du Service Pack du système d'exploitation installé.

3. SafeGuard Management Center

SafeGuard Management Center est la console permettant de gérer les ordinateurs chiffrés avec SafeGuard Enterprise. SafeGuard Management Center vous permet de créer une stratégie de sécurité dans toute l'entreprise et de l'appliquer aux terminaux. SafeGuard Management Center vous permet de :

- Créer ou importer la structure organisationnelle.
- Créer des responsables de la sécurité.
- Définir des stratégies.
- Exporter et importer des configurations.
- Surveiller les ordinateurs via les fonctionnalités de journalisation étendues.
- Récupérer des mots de passe et l'accès aux ordinateurs chiffrés.

SafeGuard Management Center vous fait bénéficier du support mutualisé pour l'administration de plusieurs domaines et bases de données. Vous pouvez gérer plusieurs bases de données SafeGuard Enterprise et gérer différentes configurations.

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

Seuls les utilisateurs disposant des privilèges (les responsables de la sécurité) peuvent accéder à SafeGuard Management Center. Plusieurs responsables de la sécurité peuvent travailler simultanément sur les données. Les différents responsables de la sécurité peuvent effectuer leurs opérations conformément aux rôles et aux droits qui leur ont été attribués.

Vous pouvez personnaliser les stratégies et les paramètres selon vos besoins. Après l'enregistrement de nouveaux paramètres dans la base de données, ils peuvent être transférés sur les terminaux, où ils deviennent actifs.

Conseil :

Cette section contient des renseignements sur les procédures principales de gestion des terminaux. Retrouvez plus de renseignements sur la gestion avancée à la section SafeGuard Management Center : options avancées *(page 117)*.

3.1 Connexion à SafeGuard Management Center

Au cours de la configuration initiale de SafeGuard Enterprise, un compte est créé pour le responsable principal de la sécurité. Ce compte est obligatoire la première fois que vous vous connectez à SafeGuard Management Center. Pour démarrer SafeGuard Management Center, l'utilisateur doit connaître le mot de passe du magasin de certificats et disposer de la clé privée du certificat.

Retrouvez plus de renseignements à la section Création du responsable principal de la sécurité *(page 42)*.

La procédure de connexion dépend de l'exécution de SafeGuard Management Center connecté à une base de données (mode Indépendant) ou à plusieurs bases de données (mode Mutualisé).

Remarque : Deux responsables de la sécurité ne doivent pas utiliser le même compte Windows sur le même ordinateur. Dans le cas contraire, il est impossible de distinguer correctement leurs droits d'accès.

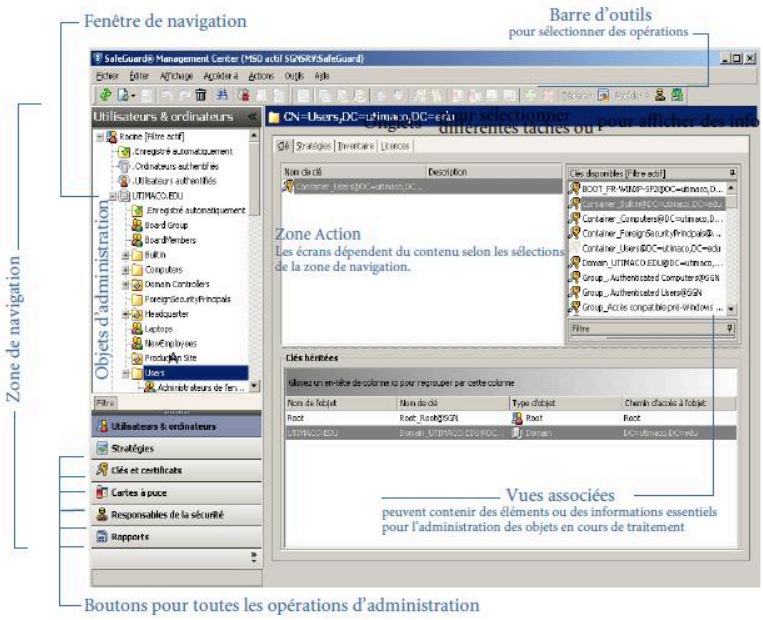
3.1.1 Connexion en mode indépendant

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

SafeGuard Management Center démarre.

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

3.2 Interface utilisateur de SafeGuard Management Center



1. **Zone de navigation**
2. **Fenêtre de navigation** avec objets administratifs.
3. **Boutons pour toutes les tâches administratives**
4. **Barre d'outils**
5. **Onglets** pour sélectionner différentes tâches ou afficher des informations.
6. **Zone d'action** s'affichant selon la sélection dans la zone de navigation.
7. **Vues associées** contenant les éléments ou les informations indispensables à l'administration de l'objet en cours de traitement.

Zone de navigation

La zone de navigation contient des boutons pour toutes les opérations d'administration :

- **Utilisateurs et ordinateurs**

  Pour importer des groupes et des utilisateurs à partir d'un annuaire actif, à partir du domaine ou d'un ordinateur individuel.

- **Stratégies**

  Pour créer des stratégies.

- **Clés et certificats**

  Pour gérer les clés et les certificats.

- **Tokens**

  Pour gérer les tokens et les cartes à puce.

- **Responsables de la sécurité**

  Pour créer des responsables de la sécurité ou des rôles et définir les opérations qui nécessitent une autorisation supplémentaire.

- **Rapports**

  Pour créer et gérer des comptes-rendus de tous les événements liés à la sécurité.

Fenêtre de navigation

Les objets devant être traités ou pouvant être créés apparaissent dans la fenêtre de navigation (objets Active Directory tels que les OU, utilisateurs et ordinateurs, éléments de stratégies, etc.). Les objets affichés dépendent de la tâche sélectionnée.

Remarque : Dans **Utilisateurs et ordinateurs**, les objets affichés dans l'arborescence de la fenêtre de navigation dépendent des droits d'accès du responsable de la sécurité pour les objets du répertoire. L'arborescence affiche seulement les objets auxquels peut accéder le responsable de la sécurité connecté. Les objets refusés n'apparaissent pas, sauf s'il existe des nœuds inférieurs dans l'arborescence pour lesquels le responsable de la sécurité a les droits d'accès. Dans ce cas, les objets refusés sont grisés. Si le responsable de la sécurité à les droits d'**Accès complet**, l'objet apparaît en noir. Les objets avec un accès en **Lecture seule** apparaissent en bleu.

Zone d'action

Dans la zone d'action, définissez les paramètres des objets sélectionnés dans la fenêtre de navigation. La zone d'action contient différents onglets permettant de traiter les objets et de définir les paramètres.

La zone d'action comporte également des informations concernant les objets sélectionnés.

Vues associées

Dans ces vues, des objets et des informations supplémentaires apparaissent. Elles fournissent des informations utiles concernant l'administration du système et en simplifient l'utilisation. Vous pouvez par exemple assigner des clés à des objets avec l'opération de glisser-déplacer.

Barre d’outils

Contient des symboles pour les différentes opérations de SafeGuard Management Center. Les symboles sont affichés tels qu’ils sont disponibles et quand ils sont disponibles pour l’objet sélectionné.

Après la connexion, SafeGuard Management Center s’ouvre toujours avec la dernière vue utilisée avant sa fermeture.

3.2.1 Paramètres de langue

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

Assistants

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

SafeGuard Management Center

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

- Dans SafeGuard Management Center, cliquez sur **Outils > Options > Général**. Sélectionnez **Utiliser la langue définie par l’utilisateur** et sélectionnez une langue disponible.
- Redémarrez SafeGuard Management Center. Il apparaît dans la langue sélectionnée.

SafeGuard Enterprise sur les terminaux

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

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

3.2.2 Vérification de l’intégrité de la base de données

Lorsque vous vous connectez à la base de données, l’intégrité de cette dernière est vérifiée automatiquement. La boîte de dialogue **Vérification de l’intégrité de la base de données** s’affiche si cette vérification renvoie des erreurs.

Vous pouvez également lancer la vérification de l’intégrité de la base de données et afficher la boîte de dialogue **Vérification de l’intégrité de la base de données** :

1. Dans SafeGuard Management Center, sélectionnez **Outils > Intégrité de la base de données**.
2. Vérifiez les tables en cliquant sur **Tout vérifier** ou **Vérifier la sélection**.

Les tables erronées sont indiquées dans la boîte de dialogue. Pour les réparer, cliquez sur **Réparer**.

Pour réparer les tables de données, vous devez être **Responsable principal de la sécurité** ou **Responsable de la récupération des bases de données** comme indiqué à la section Rôles prédéfinis *(page 143)*).

Remarque : Suite à la sauvegarde d’une mise à jour SafeGuard Enterprise (SQL), la vérification de l’intégrité de la base de données sera toujours déclenchée. La vérification doit uniquement être effectuée une seule fois par base de données SafeGuard Enterprise afin d’effectuer la mise à jour.

3.3 Utilisation de stratégies

Les sections suivantes décrivent les tâches administratives relatives aux stratégies, par exemple la création, le regroupement et la sauvegarde.

Pour l’assignation, la suppression ou la modification des stratégies, vous avez besoin des droits d’**Accès complet** aux objets appropriés ainsi qu’à tout groupe activé pour les stratégies données.

Retrouvez une description détaillée de tous les paramètres de stratégie disponibles dans SafeGuard Enterprise à la section Types de stratégie et champs d’application *(page 253)*.

3.3.1 Création de stratégies

1. Connectez-vous à SafeGuard Management Center avec le mot de passe défini lors de la configuration initiale.

2. Dans la zone de navigation, cliquez sur **Stratégies**.

3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis sélectionnez **Nouveau**.
4. Sélectionnez le type de stratégie.

   Une boîte de dialogue permettant de nommer la nouvelle stratégie s'affiche.

5. Saisissez un nom et éventuellement une description de la nouvelle stratégie.

   Stratégies de protection des périphériques :

   Si vous créez une stratégie de protection du périphérique, spécifiez d'abord la cible de la protection du périphérique. Les cibles possibles sont les suivantes :

   - Stockage de masse (volumes de démarrage/autres volumes)
   - Supports amovibles
   - Lecteurs optiques
   - Modèles de périphériques de stockage
   - Périphériques de stockage distincts
   - Stockage Cloud

   Une stratégie distincte doit être créée pour chaque cible. Vous pouvez ultérieurement combiner les stratégies individuelles dans un groupe de stratégies nommé *Chiffrement* par exemple.

6. Cliquez sur **OK**.

La nouvelle stratégie s'affiche dans la fenêtre de navigation sous **Éléments de stratégie**. Dans la zone d'action, tous les paramètres du type de stratégie sélectionné s'affichent et peuvent être changés.

3.3.2 Modification des paramètres de stratégie

Lors de la sélection d'une stratégie dans la fenêtre de navigation, vous pouvez modifier les paramètres de la stratégie dans la zone d'action.

Remarque :

non configuré	Une icône rouge en regard d'un paramètre **Non configuré** indique qu'une valeur doit être définie pour ce paramètre de stratégie. Pour enregistrer la stratégie, sélectionnez d'abord un paramètre autre que **non configuré**.

Restauration des valeurs par défaut de paramètres de stratégie

Dans la barre d'outils, les icônes suivantes servent à la configuration des paramètres de stratégie :

Icône	Paramètre de stratégie
	Affiche les valeurs par défaut des paramètres de stratégie qui n'ont pas été configurés (paramètre **Non configuré**). Les valeurs par défaut pour les paramètres des stratégies sont affichés par défaut. Cliquez sur l'icône pour masquer les valeurs par défaut.
	Définit le paramètre de stratégie défini sur **non configuré**.
	Définit tous les paramètres de stratégie d'une zone sur **Non configuré**.
	Définit la valeur par défaut de la stratégie marquée.
	Définit tous les paramètres de stratégie d'une zone sur la valeur par défaut.

Différences entre les stratégies spécifiques d'une machine et les stratégies spécifiques d'un utilisateur

Stratégie affichée en bleu	La stratégie s'applique uniquement aux machines et non aux utilisateurs.
Stratégie affichée en noir	La stratégie s'applique aux machines et aux utilisateurs.

3.3.3 Groupes de stratégies

Les stratégies SafeGuard Enterprise peuvent être combinées dans des groupes de stratégies. Un groupe de stratégies peut contenir différents types de stratégies. Dans SafeGuard Management Center, le groupe de stratégies **Par défaut** disponible est assigné à la **Racine** sous **Utilisateurs et ordinateurs**.

Si vous rassemblez des stratégies du même type dans un groupe, les paramètres sont fusionnés automatiquement. Dans ce cas, vous pouvez définir des priorités d'utilisation des paramètres. Les paramètres d'une stratégie ayant une priorité supérieure remplacent ceux d'une stratégie de priorité inférieure.

Un paramètre de stratégie défini remplace les paramètres des autres stratégies, si

- la stratégie avec ce paramètre a une priorité supérieure.
- le paramètre de stratégie n'a pas encore été défini (**non configuré**).

Remarque : Les stratégies se chevauchant assignées à un groupe peuvent aboutir à un calcul incorrect des priorités. Assurez-vous d'utiliser des paramètres de stratégie disjonctifs.

Les groupes de stratégies doivent toujours contenir au moins une stratégie. Les groupes de stratégies sans contenu perturbent l'utilisation des stratégies. Assurez-vous d'utiliser les groupes de stratégies uniquement s'ils contiennent également une stratégie.

Exception concernant la protection des périphériques :

Les stratégies de protection des périphériques sont fusionnées uniquement si elles ont été définies pour la même cible (volume de démarrage, par exemple). Les paramètres sont ajoutés si elles désignent des cibles différentes.

Terminaux non administré

Les groupes de stratégies sont communément utilisés pour la première configuration des terminaux Windows non administrés sur lesquels SafeGuard Enterprise est installé.

3.3.3.1 Combinaison de stratégies dans des groupes

Condition préalable : Les stratégies individuelles de différents types doivent être tout d'abord créées.

1. Dans la zone de navigation, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Groupes de stratégies** et sélectionnez **Nouveau**.
3. Cliquez sur **Nouveau groupe de stratégies**. Une boîte de dialogue pour nommer le groupe de stratégies s'affiche.
4. Saisissez le nom et éventuellement la description du groupe de stratégies. Cliquez sur **OK**.
5. Le nouveau groupe de stratégies s'affiche dans la fenêtre de navigation sous **Groupes de stratégies**.
6. Sélectionnez le groupe de stratégies. La zone d'action indique tous les éléments requis pour regrouper les stratégies.
7. Pour ajouter les stratégies au groupe, glissez-les de la liste de stratégies disponibles dans la zone de stratégies.
8. Vous pouvez définir une **priorité** pour chaque stratégie en les organisant grâce au menu contextuel.

   Si vous rassemblez des stratégies du même type dans un groupe, les paramètres sont fusionnés automatiquement. Dans ce cas, vous pouvez définir des priorités d'utilisation des paramètres. Les paramètres d'une stratégie ayant une priorité supérieure remplacent ceux d'une stratégie de

priorité inférieure. Si une option est définie sur **Non configuré**, le paramètre n’est **pas remplacé** dans une stratégie de priorité inférieure.

Exception concernant la protection des périphériques :

Les stratégies de protection des périphériques sont fusionnées uniquement si elles ont été définies pour la même cible (volume de démarrage, par exemple). Les paramètres sont ajoutés si elles pointent des cibles différentes.

9. Enregistrez la stratégie avec **Fichier > Enregistrer**.

Le groupe de stratégies contient désormais les paramètres de toutes les stratégies individuelles.

3.3.3.2 Résultats du regroupement de stratégies

Le résultat du regroupement de stratégies s’affiche séparément.

Pour afficher le résultat, cliquez sur l’onglet **Résultat**.

- Un onglet distinct s’affiche pour chaque type de stratégie.

  Les paramètres obtenus de la combinaison des stratégies individuelles dans un groupe s’affichent.

- Pour les stratégies de protection des périphériques, un onglet s’affiche pour chaque cible de stratégie (volumes de démarrage, lecteur X, etc.).

3.3.4 Sauvegarde de stratégies et de groupes de stratégies

Vous pouvez créer des sauvegardes de stratégies et de groupes de stratégies sous forme de fichiers XML. Si nécessaire, les stratégies/groupes de stratégies correspondants peuvent ensuite être restaurés à partir de ces fichiers XML.

1. Dans la fenêtre de navigation, sélectionnez la stratégie/le groupe de stratégies sous **Éléments de stratégie** ou **Groupes de stratégies**.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Sauvegarder la stratégie**.

   Remarque : La commande **Sauvegarder la stratégie** est également accessible dans le menu **Actions**.

3. Dans la boîte de dialogue **Enregistrer sous**, saisissez le nom du fichier XML, puis sélectionnez un emplacement de stockage. Cliquez sur **Enregistrer**.

La sauvegarde de la stratégie/du groupe de stratégies est stockée sous forme de fichier XML dans le répertoire spécifié.

Lorsque vous ajoutez des stratégies à un groupe de stratégies sauvegardées, elles sont automatiquement ajoutées à la sauvegarde.

3.3.5 Restauration de stratégies et de groupes de stratégies

La copie de sauvegarde d'une stratégie ou d'un groupe de stratégies doit avoir été créée à l'aide de la même version de SafeGuard Enterprise que vous avez utilisée pour la restaurer. Par exemple : vous ne pouvez pas restaurer une copie de sauvegarde d'un groupe de stratégies qui a été créé dans SafeGuard Enterprise 7.0 avec SafeGuard Enterprise 8.1.

Pour restaurer une stratégie/un groupe de stratégies à partir d'un fichier XML:

1. Dans la fenêtre de navigation, sélectionnez **Éléments de stratégie/Groupes de stratégies**.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Restaurer une stratégie**.

   Remarque : La commande **Restaurer une stratégie** est également accessible depuis le menu **Actions**.

3. Sélectionnez le fichier XML à partir duquel la stratégie/le groupe de stratégies doit être restauré, puis cliquez sur **Ouvrir**.

La stratégie/le groupe de stratégie est restauré(e).

3.3.6 Assignation des stratégies

Pour assigner des stratégies, vous avez besoin des droits d'**Accès complet** aux objets concernés.

1. Cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation, sélectionnez l'objet conteneur requis (par exemple, OU ou domaine).
3. Allez dans l'onglet **Stratégies**.

Tous les éléments requis pour l’assignation de la stratégie sont affichés dans la zone d’action.

4. Pour assigner une stratégie, faites-la glisser de la liste dans l’onglet **Stratégies**.
5. Vous pouvez définir une **Priorité** pour chaque stratégie en les organisant grâce au menu contextuel. Les paramètres des stratégies de niveau supérieur remplacent celles qui lui sont inférieures. Si vous sélectionnez **Ne pas remplacer** pour une stratégie, ses paramètres ne sont pas remplacés par ceux d’autres stratégies.

   Remarque :

   Si vous sélectionnez **Ne pas remplacer** pour une stratégie de priorité inférieure, celle-ci acquiert une priorité plus élevée que celle d’une stratégie de niveau supérieur.

   Pour changer la **Priorité** ou le paramètre **Ne pas remplacer** pour des stratégies dans **Utilisateurs et ordinateurs**, vous avez besoin des droits d’**Accès complet** pour tous les objets auxquels les stratégies sont assignées. Si vous n’avez pas les droits d’**Accès complet** pour tous les objets, les paramètres ne sont pas modifiables. Si vous essayez de modifier ces champs, une message d’information apparaît.

6. Les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d’activation.

La stratégie s’applique à tous les groupes au sein de l’OU et/ou du domaine.

3.3.6.1 Activation des stratégies pour des groupes individuels

Les stratégies sont toujours assignées à une unité organisationnelle (OU), à un domaine ou à un groupe de travail. Elles s'appliquent par défaut à tous les groupes de ces objets conteneurs (les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation).

Toutefois, vous pouvez également définir des stratégies et les activer pour un ou plusieurs groupes. Ces stratégies s'appliquent ensuite exclusivement à ces groupes.

Remarque : Pour activer les stratégies de groupes individuels, vous avez besoin des droits d'**Accès complet** pour le groupe concerné.

1. Assignez la stratégie à l'OU contenant le groupe.
2. Les utilisateurs authentifiés et les ordinateurs authentifiés sont affichés dans la zone d'activation.
3. Faites glisser ces deux groupes de la zone d'activation jusqu'à la liste des **Groupes disponibles**. Dans cette constellation, la stratégie n'est efficace ni pour les utilisateurs ni pour les ordinateurs.
4. À présent, faites glisser le groupe requis (ou plusieurs groupes) de la liste des **Groupes disponibles** jusqu'à la zone d'activation.

Cette stratégie s'applique désormais exclusivement à ce groupe.

Si des stratégies ont également été assignées à l'OU de niveau supérieur, cette stratégie s'applique à ce groupe en plus de celles définies pour l'OU tout entière.

3.3.7 Gestion des stratégies dans Utilisateurs et ordinateurs

À part la zone **Stratégies** dans SafeGuard Management Center, vous pouvez aussi afficher et modifier le contenu d’une stratégie où l’assignation des stratégies est effectuée dans **Utilisateurs et ordinateurs**.

1. Cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l’objet conteneur requis.
3. Vous pouvez ouvrir les stratégies pour les afficher/modifier à partir de deux emplacements.
   - Passez sur l’onglet **Stratégies**, ou
   - passez sur l’onglet **RSOP**.
4. Cliquez avec le bouton droit de la souris sur la stratégie assignée ou disponible requise et sélectionnez **Ouvrir** dans le menu contextuel.
   La boîte de dialogue des stratégies apparaît et vous pouvez visualiser et modifier les paramètres de stratégie.
5. Cliquez sur **OK** pour enregistrer vos changements.
6. Pour afficher les propriétés de stratégie, cliquez avec le bouton droit de la souris sur la stratégie et sélectionnez **Propriétés** dans le menu contextuel.
   La boîte de dialogue **Propriétés** de la stratégie apparaît. Ici, vous pouvez afficher les informations **Général** et **Assignation**.

3.4 Utilisation des packages de configuration

Dans SafeGuard Management Center, vous pouvez créer les types de packages de configuration suivants :

- **Package de configuration pour le serveur SafeGuard Enterprise**

  Pour garantir un bon fonctionnement, vous devez créer un package de configuration pour le serveur SafeGuard Enterprise qui définira la base de données et la connexion SSL, activera l’API de script ou qui utilisera SafeGuard Enterprise avec Sophos Mobile.

- **Package de configuration pour terminaux administrés**

  Les terminaux connectés au serveur SafeGuard Enterprise reçoivent leurs stratégies par le biais de ce serveur. Pour garantir un bon fonctionnement une fois le logiciel client SafeGuard Enterprise installé, vous devez créer un package de configuration pour les ordinateurs administrés et le déployer sur ceux-ci.

  Une fois la première configuration du terminal effectuée par le package de configuration, l'ordinateur reçoit des stratégies par le biais du serveur SafeGuard Enterprise après que vous avez assigné celles-ci dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center.

- **Package de configuration pour les Mac**

  Les ordinateurs Macs reçoivent l'adresse du serveur et le certificat d'entreprise par le biais de ce package. Ils envoient les informations sur leur état qui sont ensuite affichées dans SafeGuard Management Center. Retrouvez plus de renseignements sur la création des packages de configuration pour Macs à la section Création d'un package de configuration pour les Macs *(page 106)*.

- **Package de configuration pour terminaux non administrés**

  Les terminaux non administrés ne sont connectés au serveur SafeGuard Enterprise à aucun moment, et fonctionnent en mode autonome. Ces ordinateurs reçoivent leurs stratégies par packages de configuration. Pour garantir un bon fonctionnement, vous devez créer un package de configuration contenant les groupes de stratégies appropriés, puis le distribuer sur les terminaux à l'aide des mécanismes de distribution de l'entreprise. À chaque fois que vous modifiez des paramètres de stratégie, vous devez créer de nouveaux packages de configuration et les distribuer sur les terminaux.

  Remarque : Les packages de configuration pour terminaux non administrés peuvent uniquement être utilisés sur les terminaux Windows.

Vérifiez votre réseau et vos ordinateurs à intervalles réguliers pour détecter les anciennes versions ou les versions inutilisées des packages de configuration. De même, pour des raisons de sécurité, n'oubliez pas de les supprimer. Assurez-vous de toujours désinstaller les « anciens » packages de configuration avant d'installer tout nouveau package de configuration sur l'ordinateur/le serveur.

3.4.1 Création d'un package de configuration pour les terminaux

Conditions préalables

- Dans la zone de navigation **Utilisateurs et ordinateurs**, sous l'onglet **Inventaire**, vérifiez si une modification d'un certificat d'entreprise est nécessaire pour les terminaux qui doivent recevoir le nouveau package de configuration. Si le champ **Certificat d'entreprise actuel** n'est pas sélectionné, les certificats d'entreprise actuellement actifs dans la base de données SafeGuard Enterprise et sur l'ordinateur diffèrent et une modification de certificat d'entreprise est donc requise.

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Assignez un serveur SafeGuard Enterprise principal (le serveur secondaire n'est pas nécessaire).
6. Si besoin est, indiquez un groupe de stratégies, créé auparavant dans SafeGuard Management Center, qui sera appliqué aux terminaux. Si vous voulez utiliser des comptes de service pour les tâches postérieures à l'installation sur le terminal, assurez-vous d'inclure le paramètre de stratégie respectif dans ce premier groupe de stratégie. Retrouvez plus de renseignements dans le Manuel d'administration de SafeGuard Enterprise.
7. Si le certificat d'entreprise actuellement actif dans la base de données SafeGuard Enterprise diffère de celui présent sur les terminaux qui doivent recevoir le nouveau package de configuration, sélectionnez le **CCO** (Company Certificate Change Order) adéquat. Dans **Utilisateurs et ordinateurs**, dans l'onglet **Inventaire** du domaine approprié, de l'OU ou de l'ordinateur, une coche manquante sous **Certificat d'entreprise actuel** indique qu'une modification de certificat d'entreprise est nécessaire. Les informations sont disponibles sur le CCO requis dans l'onglet **CCO** de l'**Outil du package de configuration** dans le menu **Outils**.

   Remarque : Si les certificats d'entreprise actuellement actifs dans la base de données SafeGuard Enterprise et sur le terminal ne correspondent pas et si aucun **CCO** approprié n'est inclus, le déploiement du nouveau package de configuration sur le terminal échouera.

8. 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. Le chiffrement SSL est sélectionné par défaut.

9. Indiquez un chemin de sortie pour le package de configuration (MSI).

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

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

3.4.2 Création d'un package de configuration pour les terminaux non administrés

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

2. Sélectionnez **Packages du client autonome**.

3. Cliquez sur **Ajouter un package de configuration**.

4. Donnez un nom au package de configuration.

5. Indiquez un **Groupe de stratégies** préalablement créé dans SafeGuard Management Center et que vous souhaitez appliquer aux terminaux.

6. Sous **Groupe d'authentification au démarrage**, vous pouvez sélectionner le groupe d'utilisateurs de l'authentification au démarrage à assigner au terminal. Les utilisateurs de l'authentification au démarrage peuvent accéder au terminal pour des tâches administratives après activation de l'authentification au démarrage SafeGuard. Pour assigner des utilisateurs de l'authentification au démarrage, le groupe d'authentification au démarrage doit avoir été préalablement créé dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center.

7. Si le certificat d'entreprise actuellement actif dans la base de données SafeGuard Enterprise diffère de celui présent sur les terminaux qui doivent recevoir le nouveau package de configuration, sélectionnez le **CCO** (Company Certificate Change Order) adéquat.

   Remarque : Si les certificats d'entreprise actuellement actifs dans la base de données SafeGuard Enterprise et sur le terminal ne correspondent pas et si aucun **CCO** approprié n'est inclus, le déploiement du nouveau package de configuration sur le terminal échouera.

8. Sous **Emplacement de la sauvegarde de la clé**, indiquez ou sélectionnez un chemin réseau partagé pour le stockage du fichier de récupération de clé. Saisissez le chemin de partage sous la forme suivante : \\ordinateur réseau\, par exemple \\monentreprise.edu\. Si vous n'indiquez pas

de chemin ici, l’utilisateur final sera invité à indiquer l’emplacement de stockage de ce fichier lors de sa première connexion au terminal, 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 technique à des fins de récupération. Il peut également être envoyé par email.

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

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

3.4.3 Création d’un package de configuration pour les Macs

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

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Assignez un serveur SafeGuard Enterprise principal (le serveur secondaire n’est pas nécessaire).
6. Sélectionnez **SSL** comme **Chiffrement du transport** pour la connexion entre le terminal et le serveur SafeGuard Enterprise. **Sophos** en tant que **Chiffrement de transport** n’est pas pris en charge pour Mac.
7. Indiquez un chemin de sortie pour le package de configuration (ZIP).
8. Cliquez sur **Créer un package de configuration**.

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

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

3.5 Authentification renforcée : le groupe .Utilisateurs non confirmés

Les utilisateurs qui se connectent à SafeGuard Enterprise doivent s'authentifier dans Active Directory avant de pouvoir accéder à leurs jeux de clés.

Si certains utilisateurs ne peuvent pas s'authentifier lorsqu'ils se connectent, ils seront déplacés dans le groupe **.Utilisateurs non confirmés**. Ce groupe apparaît sous le nœud principal général et dans tous les domaines ou groupes de travail. L'authentification renforcée s'applique aux utilisateurs Windows et macOS.

Les raisons éventuelles pour lesquelles les utilisateurs ne sont pas en mesure de s'authentifier à la connexion sont :

- L'utilisateur a fourni des codes d'accès qui ne correspondent pas aux codes d'accès stockés dans Active Directory.
- L'utilisateur est un utilisateur local sur le terminal.

  Seuls les utilisateurs Active Directory peuvent être authentifiés à l'aide d'un contrôleur de domaine, par conséquent, un utilisateur local sera toujours déplacé dans le groupe **.Utilisateurs non confirmés** lorsqu'il se connectera pour la première fois.
- Le serveur d'authentification Active Directory est injoignable.
- L'utilisateur appartient à un domaine qui n'est pas importé à partir d'Active Directory.

  Dans ce cas, les utilisateurs seront ajoutés au groupe **.Utilisateurs non confirmés** qui apparaît directement sous le nœud **Racine** dans **Utilisateurs et ordinateurs**.
- L'authentification a échoué en raison d'une erreur inattendue.

Retrouvez plus de renseignements dans l'article 124328 de la base de connaissances de Sophos.)

Tant que les utilisateurs se trouvent dans le groupe **.Utilisateurs non confirmés**, ils n'ont pas accès à leurs jeux de clés.

Si vous cliquez sur un groupe **.Utilisateurs non confirmés**, les informations des utilisateurs du groupe (par exemple ; la raison pour laquelle un utilisateur est dans un groupe) apparaissent sur l'onglet **Utilisateurs non confirmés** dans le volet de droite.

Sur les terminaux Windows, la boîte de dialogue **État du client** affiche **Utilisateur non confirmé** sous **État d'utilisateur SGN**.

Sur les terminaux macOS, l'onglet **Utilisateur** du volet des préférences de Sophos SafeGuard affiche **Utilisateur non confirmé** sous l'**État de l'utilisateur SafeGuard**.

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

Authentification renforcée et BitLocker

Si vous utilisez BitLocker administré par SafeGuard Enterprise, vous devez autoriser l'enregistrement des nouveaux utilisateurs SGN sur **Tout le monde** :

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres de machine spécifiques** ou sélectionnez-en une.
2. Dans la section **Assignation utilisateur/machine (AUM)**, allez sur le paramètre **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** et sélectionnez **Tout le monde** dans la liste déroulante.
3. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la stratégie à vos groupes d'utilisateurs.

3.5.1 Confirmation des utilisateurs

En tant que responsable de la sécurité, vous devez vérifier les utilisateurs dans le groupe **.Utilisateurs non confirmés**. Si les utilisateurs sont autorisés, vous devez formellement les confirmer pour autoriser l'accès aux jeux de clés. Sans leur jeu de clés, les utilisateurs ne pourront pas accéder aux données chiffrées.

Pour confirmer les utilisateurs dans le groupe **.Utilisateurs non confirmés** :

1. Dans SafeGuard Management Center, sélectionnez le groupe **.Utilisateurs non confirmés**. Les utilisateurs qui n'ont pas été authentifiés dans Active Directory sont répertoriés dans la liste. Vous pouvez cliquer sur chaque utilisateur pour voir des informations détaillées dans le volet de droite.

2. Vérifiez si les utilisateurs sont autorisés à accéder au jeu de clé SafeGuard Enterprise.

3. S'ils le sont, cliquez avec le bouton droit de la souris sur l'utilisateur dans le volet gauche sous **.Utilisateurs non confirmés** et cliquez sur **Confirmer l'utilisateur**.

Vous pouvez confirmer tous les utilisateurs dans le groupe **.Utilisateurs non confirmés** en sélectionnant le groupe lui-même et en cliquant sur **Confirmer tous les utilisateurs** dans le menu contextuel.

Les utilisateurs confirmés seront déplacés dans la bonne structure Active Directory et pourront accéder à leur jeu de clé.

La confirmation des utilisateurs peut également être effectuée à l'aide de scripts d'appels API.

3.5.2 Confirmation automatique des utilisateurs

Vous pouvez configurer SafeGuard Enterprise pour confirmer automatiquement les utilisateurs qui ne peuvent pas être authentifiés dans Active Directory.

Pour confirmer automatiquement les utilisateurs dans le groupe **.Utilisateurs non confirmés** :

1. Dans SafeGuard Management Center, sélectionnez **Options** dans le menu **Outils**.
2. Allez dans l'onglet **Répertoire**.
3. Activez l'option **Confirmer automatiquement les utilisateurs qui ne peuvent pas être authentifiés par Active Directory**.
4. Cliquez sur **OK**.

Tous les utilisateurs sont déplacés dans le groupe **.Utilisateurs non confirmés** lorsque leur connexion est confirmée automatiquement et ont accès à leurs jeux de clés.

3.6 Assignation utilisateur/machine

SafeGuard Enterprise gère les informations concernant les utilisateurs autorisés à se connecter à une machine donnée dans une liste appelée d'AUM (Assignation utilisateur/machine).

Pour qu'un utilisateur soit inclus dans l'AUM, il doit s'être connecté une fois à un ordinateur sur lequel SafeGuard Enterprise a été installé et être inscrit dans SafeGuard Management Center comme utilisateur "complet" en termes de SafeGuard Enterprise. Un utilisateur "complet" désigne un utilisateur pour lequel un certificat a été généré après la première connexion et pour lequel un jeu de clés a été créé. Alors seulement les données de cet utilisateur peuvent être dupliquées sur d'autres ordinateurs. Après la duplication, l'utilisateur peut se connecter à cet ordinateur lors de l'authentification au démarrage SafeGuard.

Si le paramètre par défaut s'applique, le premier utilisateur à se connecter à l'ordinateur après l'installation de SafeGuard Enterprise est saisi dans l'AUM en tant que propriétaire de cet ordinateur.

Cet attribut permet à l'utilisateur s'étant authentifié à l'authentification au démarrage, d'autoriser d'autres utilisateurs à se connecter à cet ordinateur. Retrouvez plus de renseignements dans le

Manuel d’administration de SafeGuard Enterprise. Ils seront également ajoutés à l’AUM pour cet ordinateur.

Une liste automatique est générée et détermine quel utilisateur est autorisé à se connecter à quel ordinateur. Cette liste peut être modifiée dans SafeGuard Management Center.

3.6.1 Types d’utilisateur

Il existe différents types d’utilisateur dans SafeGuard Enterprise. Retrouvez plus de renseignements sur la manière de changer le comportement par défaut de ces types d’utilisateur à la section Types de stratégie et champs d’application *(page 253)*.

- **Propriétaire** : le premier utilisateur se connectant au terminal suite à l’installation de SafeGuard Enterprise est considéré comme un utilisateur SGN mais également comme le propriétaire de ce terminal. Si les paramètres par défaut n’ont pas été modifiés, un propriétaire a le droit d’autoriser d’autres utilisateurs à se connecter au terminal et à devenir des utilisateurs SGN.

- **Utilisateur SGN :** Un utilisateur SGN « complet » est autorisé à se connecter à l’authentification au démarrage SafeGuard, est ajouté à l’assignation utilisateur/machine et se voit fournir un certificat d’utilisateur et un jeu de clés lui permettant d’accéder aux données chiffrées.

- **Utilisateur Windows de SGN :** Un utilisateur Windows de SGN n’est pas ajouté à l’authentification au démarrage SafeGuard. En revanche, il dispose d’un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur SGN. Il est également ajouté à l’Assignation utilisateur/machine et autorisé à se connecter à Windows depuis ce terminal.

- **Utilisateur invité de SGN :** Un utilisateur invité SGN n’est pas ajouté à l’assignation utilisateur/machine, ne dispose pas des droits de connexion à l’authentification au démarrage SafeGuard, n’a pas de certificat ou de jeu de clés et n’est pas enregistré dans la base de données. Retrouvez plus de renseignements sur la manière d’empêcher la connexion d’un utilisateur invité de SGN à Windows à la section Paramètres de machine spécifiques - Paramètres de base *(page 296)*.

- **Compte de service :** Grâce aux comptes de service, les utilisateurs (par exemple, les opérateurs chargés du déploiement ou les membres de l’équipe informatique) peuvent se connecter aux terminaux après l’installation de SafeGuard Enterprise, sans avoir à activer l’authentification au démarrage SafeGuard et sans être ajoutés en tant qu’utilisateurs SGN (propriétaires) sur les ordinateurs. Les utilisateurs figurant sur une liste de comptes de service sont considérés comme des utilisateurs invités de SGN après s’être connectés à Windows sur le terminal.

- **Utilisateur POA :** Suite à l’activation de l’authentification au démarrage (POA), il pourrait être nécessaire d’effectuer des tâches administratives. Les utilisateurs de l’authentification au

démarrage disposent de comptes locaux autorisés à passer l'authentification au démarrage. Il n'y a pas de connexion automatique à Windows. Les utilisateurs se connectant avec leurs comptes utilisateur d'authentification au démarrage doivent se connecter à Windows avec leurs comptes Windows existants. Les comptes sont définis dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center (identifiant utilisateur et mot de passe) et assignés aux terminaux dans les groupes d'authentification au démarrage. Retrouvez plus de renseignements dans le Manuel d'administration de SafeGuard Enterprise.

3.6.2 Assignation utilisateur machine dans SafeGuard Management Center

Les utilisateurs peuvent être affectés à des ordinateurs spécifiques de SafeGuard Management Center. Si un utilisateur est affecté à un ordinateur dans SafeGuard Management Center (ou réciproquement) cette affectation est intégrée à l'AUM. Les données de l'utilisateur (certificat, clé etc.) sont dupliquées sur cet ordinateur et l'utilisateur peut s'y connecter. Lorsqu'un utilisateur est supprimé de l'AUM, toutes ses données utilisateur sont automatiquement supprimées de l'authentification au démarrage SafeGuard. L'utilisateur ne peut plus se connecter à l'authentification au démarrage SafeGuard avec son nom et son mot de passe.

Remarque : Dans **Utilisateurs et ordinateurs**, pour visualiser l'assignation des utilisateurs et des ordinateurs, vous avez besoin au moins de droits d'accès en **Lecture seule** pour l'un des objets (utilisateur ou ordinateur) en question. Pour définir ou changer l'assignation, vous avez besoin des droits d'**Accès complet** pour les deux objets en question. L'affichage AUM montrant les utilisateurs/machines disponibles est filtré en fonction de vos droits d'accès. Dans l'affichage de la grille AUM, qui montre les utilisateurs aux ordinateurs et vice-versa, les objets pour lesquels vous n'avez pas les droits d'accès requis apparaissent pour information, mais l'assignation ne peut pas être modifiée.

Lorsque vous assignez un utilisateur à un ordinateur, vous pouvez aussi spécifier qui peut autoriser d'autres utilisateurs à se connecter à cet ordinateur.

Sous **Type**, SafeGuard Management Center indique la méthode selon laquelle l'utilisateur a été ajouté à la base de données SafeGuard Enterprise. **Adopté** signifie que l'utilisateur a été ajouté à l'AUM sur un terminal.

Si personne n'est assigné dans SafeGuard Management Center et si aucun utilisateur n'est spécifié comme propriétaire, le premier utilisateur à se connecter à l'ordinateur après l'installation de SafeGuard Enterprise est saisi en tant que propriétaire. Cet utilisateur peut ensuite autoriser d'autres utilisateurs à se connecter à cet ordinateur. Si des utilisateurs sont assignés à cet ordinateur dans SafeGuard Management Center à une date ultérieure, ils peuvent ensuite se connecter lors de l'authentification au démarrage SafeGuard. Néanmoins, ces utilisateurs doivent être des utilisateurs complets (avec un certificat et une clé existants). Le propriétaire de l'ordinateur n'a pas besoin d'assigner des droits d'accès dans ce cas.

Les paramètres suivants permettent de spécifier qui est autorisé à ajouter des utilisateurs à l'AUM :

- **Peut devenir propriétaire** : si ce paramètre est sélectionné, l'utilisateur peut être enregistré comme le propriétaire d'un ordinateur.

- **Utilisateur propriétaire** : ce paramètre signifie que l'utilisateur est saisi dans l'AUM en tant que propriétaire. Un seul utilisateur par ordinateur peut être saisi dans l'AUM en tant que propriétaire.

  Le paramètre de stratégie **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** des **Paramètres machine spécifiques** détermine qui est autorisé à ajouter d'autres utilisateurs à l'AUM. Le paramètre **Activer l'enregistrement des utilisateurs Windows de SGN** dans les stratégies **Paramètres machine spécifiques** détermine quels utilisateurs Windows de SGN peuvent être enregistrés sur le terminal et ajoutés à l'AUM.

- **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour**

  Personne

  Même l'utilisateur saisi comme propriétaire ne peut pas ajouter d'autres utilisateurs à l'AUM. L'option permettant à un propriétaire d'ajouter d'autres utilisateurs est désactivée.

  Propriétaire (paramètre par défaut)

  Remarque : Un responsable de la sécurité peut toujours ajouter des utilisateurs dans SafeGuard Management Center.

  Tout le monde

  Lève la restriction selon laquelle les utilisateurs ne peuvent être ajoutés que par le propriétaire.

  Remarque : Pour les terminaux sur lesquels le module Protection des périphériques n'est pas installé, le paramètre **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** doit être défini sur **Tout le monde** s'il est possible d'ajouter plusieurs utilisateurs à l'Assignation utilisateur/machine avec accès à leur jeu de clés. Autrement, les utilisateurs peuvent uniquement être ajoutés dans SafeGuard Management Center. Ce paramètre est uniquement évalué sur les terminaux administrés. Retrouvez plus de renseignements dans l'article 110659 de la base de connaissances de Sophos.

- **Activer l'enregistrement des utilisateurs Windows de SGN**

  Si vous sélectionnez **Oui**, les utilisateurs Windows de SGN peuvent être enregistrés sur le terminal. Un utilisateur Windows de SGN n'est pas ajouté à l'authentification au démarrage SafeGuard. En revanche, il dispose d'un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur SGN. Si vous sélectionnez ce paramètre, tous les utilisateurs, qui seraient autrement devenus des utilisateurs invités, deviennent des utilisateurs Windows de SGN. Les utilisateurs sont ajoutés à l'Assignation utilisateur/machine dès qu'ils se connectent à Windows.

Les utilisateurs Windows de SGN peuvent être supprimés automatiquement de l'AUM sur les terminaux administrés et manuellement sur les terminaux non administrés. Retrouvez plus de renseignements à la section Paramètres de machine spécifiques - Paramètres de base *(page 296)*.

Exemple :

L'exemple suivant montre comment assigner des droits de connexion dans SafeGuard Management Center à trois utilisateurs seulement (Utilisateur_a, Utilisateur_b, Utilisateur_c) pour Ordinateur_ABC.

Premièrement : indiquez la réponse dont vous avez besoin dans SafeGuard Management Center. SafeGuard Enterprise est installé sur tous les terminaux au cours de la nuit. Le matin, les utilisateurs doivent pouvoir se connecter à leur ordinateur avec leurs codes d'accès.

1. Dans SafeGuard Management Center, assignez Utilisateur_a, Utilisateur_b et Utilisateur_c à Ordinateur_ABC. (**Utilisateurs& ordinateurs** -> Sélectionnez Ordinateur_ABC - Assignez l'utilisateur par Glisser-déposer). Vous avez ainsi spécifié une AUM.

2. Dans une stratégie de type **Paramètres de machine spécifiques**, définissez **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** sur **Personne**. Puisque l'Utilisateur_a, l'Utilisateur_b et l'Utilisateur_c ne sont pas autorisés à ajouter de nouveaux utilisateurs, il n'est pas nécessaire de spécifier un utilisateur comme propriétaire.

3. Assignez la stratégie à l'ordinateur et/ou à un point de la structure du répertoire auquel elle sera active pour l'ordinateur.

Lorsque le premier utilisateur se connecte à Ordinateur_ABC, une connexion automatique est mise en œuvre pour l'authentification au démarrage SafeGuard. Les stratégies de l'ordinateur sont envoyées au terminal. Puisque l'Utilisateur_a est inclus dans l'AUM, il deviendra un utilisateur complet lors de sa connexion à Windows. Les stratégies de l'utilisateur, les certificats et les clés sont envoyés au terminal. L'authentification au démarrage SafeGuard est activée.

Remarque : L'utilisateur peut vérifier le message d'état dans l'icône de barre d'état de SafeGuard (infobulle) lorsque ce processus est terminé.

L'Utilisateur_a est à présent un utilisateur complet selon les termes de SafeGuard Enterprise et après la première connexion, il peut s'authentifier à l'authentification au démarrage SafeGuard et il est connecté automatiquement.

L'Utilisateur_a quitte à présent l'ordinateur et l'Utilisateur_b souhaite se connecter. Comme l'authentification au démarrage SafeGuard est activée, il n'y a plus de connexion automatique.

L'Utilisateur_b et l'Utilisateur_c ont deux possibilités pour accéder à cet ordinateur.

- L’Utilisateur_a désactive l’option **Connexion automatique vers Windows** dans la boîte de dialogue de connexion à l’authentification au démarrage SafeGuard et se connecte.

- L’Utilisateur_b utilise la procédure Challenge/Réponse pour se connecter à l’authentification au démarrage SafeGuard.

Dans les deux cas, la boîte de dialogue de connexion de Windows s’affiche.

L’Utilisateur_b peut saisir ses codes d’accès Windows. Les stratégies de l’utilisateur, les certificats et les clés sont envoyés au terminal. L’utilisateur est activé dans l’authentification au démarrage SafeGuard. L’Utilisateur_b est à présent un utilisateur complet selon les termes de SafeGuard Enterprise et après la première connexion, il peut s’authentifier lors de l’authentification au démarrage SafeGuard et sera connecté automatiquement.

Alors que la stratégie de l’ordinateur indique que personne ne peut importer d’utilisateurs sur cet ordinateur (car ces utilisateurs sont déjà dans l’AUM), l’Utilisateur_b et l’Utilisateur_c obtiennent néanmoins l’état utilisateur "complet" à la connexion Windows et sont activés dans l’authentification au démarrage SafeGuard.

Aucun autre utilisateur ne sera ajouté à l’AUM ou ne pourra s’identifier lors de l’authentification au démarrage. Tout utilisateur se connectant à Windows qui n’est pas Utilisateur_a, Utilisateur_b ou Utilisateur_c est exclu de l’AUM dans ce scénario et ne sera jamais activé dans l’authentification au démarrage SafeGuard.

Les utilisateurs peuvent toujours être ajoutés par la suite dans SafeGuard Management Center. Cependant, leur jeu de clés ne sera pas disponible après la première connexion, la synchronisation n’étant pas déclenchée par la première connexion. Après une deuxième connexion, le jeu de clés sera disponible et les utilisateurs pourront accéder à leur ordinateur selon les stratégies appliquées. S’ils n’ont jamais réussi à se connecter au terminal, il est possible de les ajouter comme indiqué ci-dessus.

Remarque : Si un responsable de la sécurité ou un responsable de la sécurité principale supprime le dernier certificat d’utilisateur valide de l’AUM, les utilisateurs pourront se connecter automatiquement à l’authentification au démarrage SafeGuard de l’ordinateur correspondant. Il en va de même si le domaine du terminal change. Seuls les codes d’accès Windows sont nécessaires pour se connecter à l’ordinateur, réactiver l’authentification au démarrage SafeGuard et pour ajouter un utilisateur en tant que propriétaire.

Cette description s’applique uniquement aux terminaux Windows et pas aux Macs. L’ajout de différents utilisateurs à un Mac sur des environnements de grande taille peut entraîner de sérieux problèmes de performances lors de l’alignement des stratégies entre le terminal et le serveur et au cours de la synchronisation Active Directory dans le SafeGuard Management Center ou dans le gestionnaire de tâches. Nous vous conseillons vivement de ne pas assigner d’utilisateurs aux Macs dans SafeGuard Management Center.

3.6.2.1 Blocage de l'utilisateur

Si vous sélectionnez la case dans la colonne **Bloquer l'utilisateur**, l'utilisateur n'est pas autorisé à se connecter à l'ordinateur concerné. Si l'utilisateur se connecte lorsque la stratégie contenant ce paramètre est activée sur l'ordinateur, il est déconnecté.

3.6.2.2 Groupes

Dans SafeGuard Management Center, des groupes d’ordinateurs peuvent être assignés à un utilisateur (compte) et/ou peuvent être assignés à un ordinateur.

Pour créer un groupe : Dans **Utilisateurs et ordinateurs**, cliquez avec le bouton droit de la souris sur le nœud de l’objet approprié sur lequel vous voulez créer le groupe et sélectionnez **Nouveau > Créer un groupe > Nom complet**. Saisissez le nom du groupe et une description (facultative). Cliquez sur **OK**.

Exemple : Compte de service

Il est par exemple possible d’utiliser un seul compte de service pour entretenir un grand nombre d’ordinateurs. À cette fin, les ordinateurs concernés doivent se trouver dans un même groupe. Ce groupe est ensuite assigné à un compte de service (utilisateur). Le propriétaire du compte de service peut ensuite se connecter à tous les ordinateurs de ce groupe.

En outre, le fait d’assigner un groupe contenant différents utilisateurs permet à ces derniers de se connecter ensuite à un ordinateur spécifique en une seule étape.

3.6.3 Assignation de groupes d’utilisateurs et d’ordinateurs

Dans **Utilisateurs et ordinateurs**, pour visualiser l’assignation des groupes d’utilisateurs et d’ordinateurs, vous avez besoin au moins de droits d’accès en **Lecture seule** pour l’un des objets (groupe d’utilisateurs ou d’ordinateurs) en question. Pour définir ou changer l’assignation, vous avez besoin des droits d’**Accès complet** pour les deux objets en question. L’affichage AUM montrant les utilisateurs/machines disponibles est filtré en fonction de vos droits d’accès.

Remarque : Vous pouvez assigner des utilisateurs individuels à un ordinateur ou réciproquement en utilisant le même processus que pour les groupes.

1. Cliquez sur **Utilisateurs et ordinateurs**.
2. Pour assigner un groupe d’ordinateurs à un utilisateur unique, sélectionnez ce dernier.
3. Cliquez sur l’onglet **Ordinateur** dans la zone d’action.

Tous les ordinateurs et groupes d’ordinateurs sont affichés sous **Ordinateurs disponibles**.

4. Faites glisser les groupes sélectionnés de la liste des **Groupes disponibles** jusqu’à la zone d’activation.
5. Une boîte de dialogue s’affiche demandant si l’utilisateur doit être le propriétaire de tous les ordinateurs.

   S’il n’y a pas de propriétaire spécifique dans SafeGuard Management Center, le premier utilisateur à se connecter à cet ordinateur est automatiquement entré en tant que propriétaire. Cet utilisateur peut autoriser d’autres utilisateurs à accéder à cet ordinateur. La condition est que l’utilisateur **Peut devenir propriétaire**.

   - Si vous répondez **Oui**, le premier utilisateur à se connecter à cet ordinateur en devient le propriétaire et peut en autoriser l’accès à d’autres utilisateurs.
   - Si vous répondez **Non**, l’utilisateur ne sera pas le propriétaire de cet ordinateur.

   Il n’est généralement pas nécessaire pour le propriétaire d’un compte de service d’être en même temps le propriétaire de l’ordinateur. Ce paramètre peut être modifié après l’assignation initiale.

Tous les ordinateurs du groupe assigné sont affichés dans la zone d’action.

L’utilisateur peut se connecter à tous les ordinateurs assignés de cette manière.

Un groupe d’utilisateurs peut être assigné à un seul ordinateur en utilisant la même procédure.

3.7 Amélioration de Sophos SafeGuard par envoi de données d'utilisation anonymes

Sophos s'efforce en permanence d'améliorer SafeGuard Enterprise. Dans ce but, les clients envoient régulièrement des données anonymes à Sophos. Ces données sont exclusivement utilisées dans le but d'améliorer notre produit. Elles ne peuvent pas être utilisées pour identifier les clients ou leurs machines et ne contiennent aucune autre information confidentielle. Retrouvez plus de renseignements dans l’article 123768 de la base de connaissances de Sophos.

L'envoi de données à Sophos est facultatif. Toutes les données étant envoyées de manière anonyme, la fonction de récupération des données est activée par défaut. Vous pouvez désactiver cette fonction dans SafeGuard Management Center (Stratégies > Paramètres généraux > Commentaires > Aidez-nous à améliorer Sophos SafeGuard® en envoyant des données d'utilisation anonymes).

3.7.1 Création d’une stratégie pour désactiver l’envoi de données d’utilisation anonymes

Pour désactiver l’envoi de données d’utilisation anonymes :

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.
   L’onglet **Paramètres généraux** apparaît.
2. Rendez-vous dans la section **Commentaires**.
3. À partir de la liste déroulante **Aidez-nous à améliorer Sophos SafeGuard® en envoyant des données d’utilisation anonymes**, sélectionnez **Non**.
4. Dans **Utilisateurs et ordinateurs**, assignez la nouvelle stratégie à vos utilisateurs et ordinateurs.
   La fonction est désormais désactivée. Aucune donnée d’utilisation ne sera envoyée à Sophos.

3.8 SafeGuard Management Center : options avancées

Retrouvez plus de renseignements sur les fonctions avancées d’administration dans la présente section.

3.8.1 Maintenance de la base de données

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

Retrouvez plus de renseignements dans l’article 113001 de la base de connaissances Sophos.

3.8.1.1 Réparation d’une configuration corrompue de la base de données

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

- Les certificats d’entreprise et du responsable principal de la sécurité pour la configuration de la base de données correspondante doivent avoir été exportés sous la forme de fichiers .p12. Les données doivent être disponibles et valides.

- Vous devez également connaître les mots de passe de ces deux fichiers .p12, ainsi que du magasin de certificats.

Nous conseillons seulement de suivre cette procédure si aucune sauvegarde de base de données valide n’est disponible. Tous les ordinateurs qui se connectent à un serveur backend réparé perdent leur assignation utilisateur/machine. En conséquence, l’authentification au démarrage est temporairement désactivée. Les mécanismes de challenge/réponse ne seront pas disponibles tant que le terminal correspondant n’aura pas renvoyé avec succès les informations sur sa clé.

Pour réparer une configuration de base de données corrompue :

1. Réinstallez le package d’installation de SafeGuard Management Center. Ouvrez SafeGuard Management Center. L’**Assistant de configuration** démarre automatiquement.

2. Dans **Connexion à la base de données**, cochez la case **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. Cliquez sur **Importer le certificat d’authentification** pour rechercher le fichier de certificat sauvegardé. Sous **Fichier de clés**, saisissez le mot de passe du fichier. Cliquez sur **OK**.

5. Le certificat du responsable principal de la sécurité est alors importé. Cliquez sur **Suivant**.

6. Dans **Certificat d’entreprise**, cochez la case **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** dans le message affiché.

   Le certificat d’entreprise est alors importé.

7. Cliquez sur **Suivant**, puis sur **Terminer**.

La configuration de la base de données est réparée.

3.8.2 Utilisation de plusieurs configurations de base de données (mutualisées)

Condition préalable :

- La fonction de configuration en mode Mutualisé doit avoir été installée via une installation de type **Complète**. Retrouvez plus de renseignements à la section Installation *(page 15)*.
- La configuration initiale de SafeGuard Management Center doit avoir été réalisée. Retrouvez plus de renseignements à la section Configuration initiale de SafeGuard Management Center *(page 40)*.

Le mode Mutualisé vous permet de configurer différentes instances de base de données SafeGuard Enterprise et de les gérer avec une instance de SafeGuard Management Center. Ceci s'avère particulièrement utile pour disposer de configurations de base de données différentes pour différents domaines, unités organisationnelles ou locaux d'entreprise.

Pour chaque base de données (le locataire), vous devez configurer une instance séparée de SafeGuard Enterprise. Chaque base de données doit avoir la même version. Par exemple, il n'est pas possible d'administrer les bases de données SGN 7 et les bases de données SGN 8.3 uniquement avec la version 8.3 de Management Center.

Pour simplifier la configuration, vous pouvez :

- Créer plusieurs configurations de base de données.
- Sélectionner des configurations de base de données créées précédemment.
- Supprimer des configurations de base de données de la liste.
- Importer une configuration de base de données créée précédemment à partir d'un fichier.
- Exporter une configuration de base de données à réutiliser ultérieurement.

3.8.2.1 Création de configurations de base de données supplémentaires

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

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

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

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

3.8.2.2 Configuration des instances supplémentaires de SafeGuard Management Center

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

SafeGuard Enterprise gère les droits d’accès à 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 à SafeGuard Management Center. La connexion à SafeGuard Management Center nécessite uniquement le mot de passe du magasin de certificats.

1. Installez SGNManagementCenter.msi sur un autre ordinateur avec les fonctionnalités requises.

2. Démarrez SafeGuard Management Center sur l’ordinateur de l’administrateur. L’assistant de configuration démarre et vous guide tout au long des étapes nécessaires.

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

4. Dans la boîte de dialogue **Connexion au serveur de base de données**, sous **Serveur de base de données**, sélectionnez, dans la liste, l’instance de base de données SQL souhaitée. Tous les serveurs de base de données disponibles sur votre ordinateur ou sur votre réseau s’affichent. Sous **Authentification**, activez le type d’authentification à utiliser pour accéder à cette instance du serveur de base de données. Si vous sélectionnez **Utiliser l’authentification SQL avec les codes d’accès suivants**, saisissez les codes d’accès du compte utilisateur SQL que votre administrateur SQL a créé. Cliquez sur **Suivant**.

5. Sur la page **Paramètres de base de données**, cliquez sur **Sélectionner une base de données disponible** et sélectionnez la base de données correspondante dans la liste. Cliquez sur **Suivant**.

6. Dans **Authentification à SafeGuard Management Center**, sélectionnez une personne autorisée dans la liste. Si le mode Mutualisé est activé, la boîte de dialogue affiche la configuration à laquelle l'utilisateur est sur le point de se connecter. Saisissez et confirmez le mot de passe du magasin de certificats.
   Un magasin de certificats est créé pour le compte utilisateur actuel et il est protégé par ce mot de passe. Pour toute connexion future, vous n'avez besoin que de ce mot de passe.

7. Cliquez sur **OK**.

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

8. Pour importer les données, cliquez sur **Oui**, puis sur **OK**. Cette opération démarre le processus d'importation.

9. Dans **Importation du fichier de clé pour l'authentification**, cliquez sur **[...]** et sélectionnez le fichier de clé. Saisissez maintenant le **mot de passe du fichier de clé**. Saisissez le mot de passe du magasin de certificats défini précédemment dans **Mot de passe du magasin de certificat ou code confidentiel de la carte**. Sélectionnez **Importer dans le magasin de certificats** ou sélectionnez **Copier sur le token** pour stocker le certificat sur un token.

10. Saisissez le mot de passe une nouvelle fois pour initialiser le magasin de certificats.

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

3.8.2.3 Connexion à une configuration de base de données existante

Pour travailler avec une configuration de base de données SafeGuard Enterprise :

1. Démarrez SafeGuard Management Center.

   La boîte de dialogue **Sélection d'une configuration** s'affiche.

2. Sélectionnez la configuration de base de données souhaitée dans la liste déroulante et cliquez sur **OK**.

   La configuration de base de données sélectionnée est reliée à SafeGuard Management Center et devient active.

3. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

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

3.8.2.4 Exportation d’une configuration dans un fichier

Pour enregistrer ou réutiliser une configuration de base de données, vous pouvez l’exporter dans un fichier :

1. Démarrez SafeGuard Management Center.

   La boîte de dialogue **Sélection d’une configuration** s’affiche.

2. Sélectionnez la configuration de base de données respective dans la liste et cliquez sur **Exporter...**.

3. Pour sécuriser le fichier de configuration, vous êtes invité à saisir et à confirmer un mot de passe qui chiffre le fichier de configuration.

4. Cliquez sur **OK**.

5. Indiquez un nom et un emplacement de stockage pour le fichier de configuration exporté *.SGNConfig.

   Si cette configuration existe déjà, vous êtes invité à confirmer le remplacement de la configuration existante.

Le fichier de configuration de base de données est enregistré à l’emplacement de stockage spécifié.

3.8.2.5 Importation d’une configuration à partir d’un fichier

Pour utiliser ou modifier une configuration de base de données, vous pouvez importer une configuration créée précédemment dans SafeGuard Management Center. Pour ce faire, vous pouvez procéder de deux façons :

- Via SafeGuard Management Center (Mutualisé)
- En cliquant deux fois sur le fichier de configuration (Indépendant et Mutualisé).

3.8.2.6 Importation d’une configuration avec SafeGuard Management Center

1. Démarrez SafeGuard Management Center.

La boîte de dialogue **Sélection d’une configuration** s’affiche.

2. Cliquez sur **Importer...**, recherchez le fichier de configuration souhaité, puis cliquez sur **Ouvrir**.
3. Saisissez le mot de passe du fichier de configuration défini lors de l’exportation, puis cliquez sur **OK**.

   La configuration sélectionnée s’affiche.

4. Pour activer la configuration, cliquez sur **OK**.
5. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

SafeGuard Management Center est ouvert et relié à la configuration de base de données importée.

3.8.2.7 Importation d’une configuration en cliquant deux fois sur le fichier de configuration (Indépendant et Mutualisé)

Remarque : Cette tâche est disponible en mode Indépendant et Mutualisé.

Vous pouvez également exporter une configuration et la distribuer vers plusieurs responsables de la sécurité. Les responsables de la sécurité cliquent deux fois alors sur le fichier de configuration pour ouvrir une instance de SafeGuard Management Center totalement configurée.

Scénarios d’utilisation :

- vous utilisez l’authentification SQL pour la base de données et souhaitez éviter que chaque administrateur connaisse le mot de passe SQL :

  Dans ce cas, vous ne le saisissez ensuite qu’une seule fois, vous créez un fichier de configuration et vous le distribuez vers les ordinateurs des responsables de la sécurité concernés.

- Vous voulez exécuter Web Helpdesk sur plusieurs ordinateurs :

  Tous ces ordinateurs doivent être connectés à la base de données. Pour simplifier l’installation sur ces ordinateurs, vous pouvez créer un fichier de configuration et le distribuer aux responsables du support.

Condition préalable : La configuration initiale de SafeGuard Management Center doit avoir été effectuée. Retrouvez plus de renseignements à la section Installation de SafeGuard Management Center *(page 38)*.

1. Démarrez SafeGuard Management Center.
2. Sélectionnez **Options** dans le menu **Outils** et sélectionnez l'onglet **Base de données**.
3. Saisissez et confirmez les codes d'accès de la connexion au serveur de base de données SQL.
4. Cliquez sur **Exporter la configuration** pour exporter cette configuration vers un fichier.
5. Saisissez et confirmez un mot de passe pour le fichier de configuration.
6. Saisissez un nom de fichier et spécifiez un emplacement de stockage.
7. Déployez ce fichier de configuration sur les ordinateurs des responsables de la sécurité. Fournissez-leur le mot de passe de ce fichier et du magasin de certificats nécessaires pour s'authentifier dans SafeGuard Management Center.
8. Les responsables de la sécurité cliquent simplement deux fois sur le fichier de configuration.
9. Ils sont invités à saisir le mot de passe du fichier de configuration.
10. Pour s'authentifier dans SafeGuard Management Center, ils sont invités à saisir leur mot de passe de magasin de certificats.

SafeGuard Management Center démarre avec la configuration importée. Cette configuration est la nouvelle configuration par défaut.

3.8.2.8 Basculement rapide entre les configurations de base de données

Pour simplifier la gestion administrative de différents titulaires, SafeGuard Management Center permet de basculer rapidement entre les configurations de base de données.

Remarque : Cette tâche est également disponible en mode Indépendant.

1. Dans SafeGuard Management Center, sélectionnez **Changer la configuration...** dans le menu **Fichier**.
2. Dans la liste déroulante, sélectionnez la base de données à laquelle vous souhaitez basculer et cliquez sur **OK**.

SafeGuard Management Center redémarre automatiquement avec la configuration sélectionnée.

3.8.2.9 Connexion en mode mutualisé

Le processus de connexion à SafeGuard Management Center est plus long lorsque plusieurs bases de données ont été configurées (mutualisation). Retrouvez plus de renseignements à la section Utilisation de plusieurs configurations de base de données (mutualisées) *(page 118)*.

1. Démarrez SafeGuard Management Center à partir du dossier des produits dans le menu **Démarrer**. La boîte de dialogue **Sélection d'une configuration** s'affiche.

2. Sélectionnez la configuration de base de données que vous souhaitez utiliser dans la liste déroulante et cliquez sur **OK**.
   La configuration de base de données sélectionnée est reliée à SafeGuard Management Center et devient active.

3. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

SafeGuard Management Center est ouvert et relié 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 tentatives ratées de connexion sont consignées dans le journal.

3.8.3 Avertissement à l'expiration du certificat d'entreprise

À la connexion, SafeGuard Management Center commence par afficher un avertissement six mois avant l'expiration du certificat d'entreprise et vous invite à le renouveler et à le déployer sur les terminaux. Sans certificat d'entreprise valide, un terminal ne peut pas se connecter au serveur.

Vous pouvez renouveler le certificat d'entreprise à tout moment. Même si le certificat d'entreprise a déjà expiré. Un certificat d'entreprise expiré sera aussi indiqué par une boîte de message. Retrouvez plus de renseignements sur le renouvellement du certificat d'entreprise à la section Renouvellement du certificat d'entreprise *(page 186)*.

3.8.4 Recherche d'utilisateurs, d'ordinateurs et de groupes dans la base de données SafeGuard Enterprise

Pour afficher des objets dans la boîte de dialogue **Rechercher des utilisateurs, ordinateurs et groupes**, vous avez besoin des droits en **Lecture seule** ou d'**Accès complet** pour les objets concernés.

Remarque : Lorsque vous recherchez des objets, vous obtenez uniquement les résultats de la recherche sur les zones (domaines) sur lesquelles vous disposez de droits d'accès en tant que responsable de la sécurité. Seul un Responsable principal de la sécurité peut effectuer une recherche sur la racine.

Dans **Utilisateurs et ordinateurs**, vous pouvez rechercher des objets à l'aide de différents filtres. Par exemple, vous pouvez facilement identifier les doubles qui peuvent avoir été provoqués par un

processus de synchronisation AD avec le filtre **Utilisateurs et ordinateurs dupliqués**. Ce filtre affiche tous les ordinateurs portant le même nom dans un domaine et tous les utilisateurs avec le même nom, nom de connexion ou nom de connexion avant 2000 dans un domaine.

Pour rechercher les objets :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation **Utilisateurs et ordinateurs**, sélectionnez le conteneur requis.
3. Dans la barre de menus de SafeGuard Management Center, cliquez sur **Édition > Rechercher**.

   La boîte de dialogue **Rechercher des utilisateurs, ordinateurs et groupes** s'affiche.
4. Sélectionnez le filtre requis dans la liste déroulante **Rechercher**.
5. Dans le champ **Dans**, le conteneur sélectionné apparaît.

   Vous pouvez changer ceci en sélectionnant une option différente de la liste déroulante.
6. Si vous recherchez un objet spécifique, saisissez son nom dans le champ **Rechercher le nom**.
7. Avec la case à cocher **Supprimer les résultats après chaque recherche**, spécifiez si les résultats doivent être effacés après chaque processus de recherche.
8. Cliquez sur **Rechercher maintenant**.

Les résultats apparaissent dans la boîte de dialogue **Rechercher des utilisateurs, ordinateurs et groupes**. Si vous cliquez sur un des résultats dans cette boîte de dialogue, l'entrée correspondante est marquée dans l'arborescence **Utilisateurs et ordinateurs**. Si vous avez recherché les doublons par exemple, vous pouvez maintenant les supprimer facilement.

3.8.5 Affichage des propriétés d'objet dans Utilisateurs et ordinateurs

Pour afficher les propriétés d'objet, vous avez besoin des droits d'**Accès complet** ou en **Lecture seule** aux objets concernés.

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation **Utilisateurs et ordinateurs**, cliquez avec le bouton droit de la souris sur l'objet requis et sélectionnez **Propriétés**.

Les propriétés de l’objet sélectionné apparaissent. Si vous avez des droits d’accès en **Lecture seule** à l’objet en question, les informations sur les propriétés sont grisées dans la boîte de dialogue et vous ne pouvez pas les modifier.

3.8.6 Désactivation du déploiement de stratégies

En tant que responsable de la sécurité, vous pouvez désactiver le déploiement des terminaux. Pour ce faire, cliquez sur le bouton **Activer/désactiver le déploiement des stratégies** dans la barre d’outils de SafeGuard Management Center ou sélectionnez la commande **Activer/désactiver le déploiement des stratégies** dans le menu **Éditer**. Après désactivation du déploiement de stratégies, aucune stratégie n’est envoyée aux terminaux. Pour inverser la désactivation du déploiement de stratégies, cliquez sur le bouton ou sélectionnez de nouveau la commande.

Remarque : Pour désactiver le déploiement de stratégies, un responsable de la sécurité doit disposer du droit "Activer/désactiver le déploiement des stratégies". Par défaut, ce droit a été affecté aux rôles prédéfinis de responsable principal de la sécurité et de responsable de la sécurité, mais il peut aussi être affecté à de nouveaux rôles définis par l’utilisateur.

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

3.8.7 Règles d’assignation et d’analyse des stratégies

La gestion et l’analyse des stratégies s’effectuent selon les règles décrites dans cette section.

Définitions

L’origine de la stratégie décide s’il s’agit d’une stratégie d’utilisateur ou d’une stratégie d’ordinateur. Un objet de l’utilisateur « appelle » une stratégie d’utilisateur, et un ordinateur « appelle » une stratégie d’ordinateur. La même stratégie peut être une stratégie d’ordinateur ou d’utilisateur, selon le point de vue.

- **Stratégie d’utilisateur**

  Toute stratégie fournie par l’utilisateur pour l’analyse. Si une stratégie est mise en œuvre via un seul utilisateur, les paramètres associés à l’ordinateur de cette stratégie ne sont pas appliqués. En d’autres termes, les paramètres associés à l’ordinateur ne s’appliquent pas. Les valeurs par défaut s’appliquent.

- **Stratégie d’ordinateur**

  Toute stratégie fournie par l’ordinateur pour l’analyse. Si une stratégie est mise en œuvre via un seul ordinateur, les paramètres spécifiques à l’utilisateur pour cette stratégie sont également

appliqués. La stratégie de l’ordinateur représente par conséquent une stratégie pour tous les utilisateurs.

Assignation et activation des stratégies

Pour activer une stratégie devant être mise en œuvre pour un utilisateur ou un ordinateur, vous devez d’abord l’assigner à un objet conteneur (nœuds racine, domaine, UO, conteneur intégré ou groupe de travail). Pour que la stratégie assignée à un utilisateur ou à un ordinateur devienne effective, lorsque vous assignez une stratégie à un point quelconque de la hiérarchie, tous les ordinateurs (ordinateurs authentifiés) et tous les utilisateurs (utilisateurs authentifiés) sont activés automatiquement (l’assignation sans activation ne suffit pas). Tous les utilisateurs et tous les ordinateurs sont combinés dans ces groupes.

Héritage de stratégie

Les stratégies ne peuvent être transmises qu’entre objets conteneurs. Les stratégies peuvent être activées au sein d’un conteneur à supposer qu’il ne contienne aucun autre objet conteneur (au niveau du groupe). L’héritage entre groupes est impossible.

Hiérarchie d’héritage de stratégie

Lorsque des stratégies sont assignées le long d’une chaîne hiérarchique, la stratégie la plus proche dans le cas d’un objet cible (utilisateur ou ordinateur) a le niveau le plus élevé. Cela signifie que si la distance entre une stratégie et l’objet cible augmente, elle sera remplacée par toute autre stratégie plus proche.

Assignation directe des stratégies

L’utilisateur ou l’ordinateur reçoit une stratégie assignée directement à l’objet conteneur dans lequel il se trouve (l’appartenance d’un utilisateur de groupe placé dans un autre objet conteneur n’est pas suffisante). L’objet conteneur n’a pas hérité de cette stratégie.

Assignation indirecte des stratégies

L’utilisateur ou l’ordinateur reçoit une stratégie que l’objet conteneur dans lequel il se trouve (l’appartenance en tant qu’utilisateur d’un groupe situé dans un autre objet conteneur n’est pas suffisante) a hérité d’un objet conteneur de niveau supérieur.

Activation/désactivation de stratégies

Pour qu’une stratégie soit effective pour un ordinateur/utilisateur, elle doit être activée au niveau du groupe (les stratégies peuvent uniquement être activées au niveau du groupe). Que ce groupe se trouve ou non dans le même objet conteneur n’a pas d’importance. Le seul point important est que l’utilisateur ou l’ordinateur ait été assigné directement ou indirectement (par héritage) à la stratégie.

Si un ordinateur ou un utilisateur se trouve en dehors d'une UO, ou d'une ligne d'héritage, et fait partie d'un groupe qui se trouve lui-même dans cette UO, cette activation ne s'applique **pas** à cet utilisateur ou cet ordinateur. En effet, il n'existe pas d'assignation valide pour cet utilisateur ou cet ordinateur (directement ou indirectement). Le groupe était, en effet, activé mais une activation peut seulement s'appliquer aux utilisateurs et aux ordinateurs pour lesquels il existe aussi une assignation de stratégie. Ce qui signifie que l'activation des stratégies ne peut pas aller au-delà des limites de conteneur s'il n'y a pas d'assignation directe ou indirecte de la stratégie pour cet objet.

Une stratégie devient effective lorsqu'elle a été activée pour des groupes d'utilisateurs ou des groupes d'ordinateurs. Les groupes d'utilisateurs puis les groupes d'ordinateurs sont analysés (les utilisateurs authentifiés et les ordinateurs authentifiés sont également des groupes). Les deux résultats sont reliés par une instruction OR. Si ce lien OR donne une valeur positive pour la relation ordinateur/utilisateur, la stratégie s'applique.

Remarque : Si plusieurs stratégies sont actives pour un objet, les stratégies individuelles sont groupées, en respectant néanmoins les règles décrites et fusionnées. Ce qui signifie que les paramètres réels d'un objet peuvent être composés de plusieurs stratégies différentes.

Un groupe peut avoir les paramètres d'activation suivants:

- Activé

  Une stratégie a été assignée. Le groupe est affiché dans la zone d'activation de SafeGuard Management Center.

- Non activé

  Une stratégie a été assignée. Le groupe ne se trouve pas dans la zone d'activation.

Si une stratégie est assignée à un conteneur, le paramètre d'activation d'un groupe (activé) détermine si cette stratégie pour ce conteneur est incluse dans le calcul de la stratégie résultante.

Les stratégies héritées ne peuvent pas être contrôlées par ces activations. **Bloquer l'héritage de stratégie** doit être défini dans l'OU plus locale pour annuler l'effet de la stratégie globale à cet endroit.

Paramètres de l'utilisateur ou du groupe

Les paramètres de stratégie pour les utilisateurs (affichés en **noir** dans SafeGuard Management Center) sont prioritaires sur les paramètres de stratégie pour les ordinateurs (affichés en **bleu** dans SafeGuard Management Center). Si les paramètres de l'utilisateur sont indiqués dans une stratégie pour les ordinateurs, ces paramètres seront remplacés par la stratégie pour l'utilisateur.

Remarque : Seuls les paramètres de l'utilisateur sont remplacés. Si une stratégie pour les utilisateurs comporte également des paramètres d'ordinateurs (affichés en **bleu**), ils ne sont pas remplacés par une stratégie d'utilisateur !

Exemple 1 :

Si une longueur de mot de passe de 4 a été définie pour un groupe d'ordinateurs, et si la valeur 3 du même paramètre a été définie pour le groupe d'utilisateurs, un mot de passe de longueur 3 s'applique à cet utilisateur sur un ordinateur appartenant à ce groupe d'ordinateurs.

Exemple 2 :

Si un intervalle de connexion au serveur de 1 minute est défini pour un groupe d'utilisateurs, et la valeur 3 pour un groupe d'ordinateurs, la valeur 3 est utilisée car la valeur 1 minute est un paramètre d'ordinateur ayant été défini dans une stratégie pour les utilisateurs.

Stratégies de chiffrement contradictoires

Deux stratégies, P1 et P2, sont créées. Le chiffrement basé sur fichier du lecteur E:\ a été défini pour P1, et le chiffrement basé sur volume du lecteur E:\ a été défini pour P2. P1 se voit assigner l'UO **FBE-User** et P2 l'UO **VBE-User**.

Cas de figure 1 : un utilisateur de l'UO **FBE-User** se connecte le premier au client W7-100 (ordinateur du conteneur). Le chiffrement du lecteur E:\ est basé sur les fichiers. Si un utilisateur de l'UO **VBE-User** se connecte ensuite au client W7-100, le chiffrement du lecteur E:\ est basé sur les volumes. Si les deux utilisateurs ont la même clé, tous deux peuvent accéder aux lecteurs ou aux fichiers.

Cas de figure 2 : un utilisateur de l'OU **VBE-User** se connecte le premier à l'ordinateur XP-100 (ordinateur du conteneur). Le chiffrement du lecteur est basé sur les volumes. Si, à présent, un utilisateur de l'UO **FBE-User** se connecte et a la même clé que les utilisateurs de l'UO **VBE-User**, le chiffrement du lecteur E:\ sera basé sur les fichiers dans le chiffrement basé sur les volumes (le chiffrement basé sur les volumes est conservé). Toutefois, si l'utilisateur de l'UO **FBE-User** n'a pas la même clé, il ne peut pas accéder au lecteur E:\.

Priorités au sein d'une assignation

Au sein d'une assignation, la stratégie ayant la plus haute priorité (1) se range au-dessus d'une stratégie ayant une priorité inférieure.

Remarque : Si une stratégie ayant une priorité inférieure mais ayant été désignée **Ne pas remplacer** est assignée au même niveau qu'une stratégie d'un niveau supérieur, cette stratégie sera prioritaire en dépit de son niveau inférieur.

Priorités au sein d’un groupe

Au sein d’un groupe, la stratégie ayant la plus haute priorité (1) se range au-dessus d’une stratégie ayant une priorité inférieure.

Indicateurs d’état

La définition d’indicateurs d’état permet de changer les règles par défaut pour les stratégies.

- **Bloquer l’héritage de stratégie**

  Paramètre des conteneurs pour lesquels vous ne souhaitez pas que des stratégies de niveau supérieur s’appliquent (cliquez avec le bouton droit sur l’objet dans la fenêtre de navigation Propriétés).

  Si vous ne souhaitez pas qu’un objet conteneur hérite d’une stratégie d’un objet plus élevé, sélectionnez **Bloquer l’héritage de stratégie** pour l’en empêcher. Si **Bloquer l’héritage de stratégie** a été sélectionné pour un objet conteneur, il ne sera pas affecté par les paramètres d’une stratégie d’un niveau supérieur (exception : **Ne pas remplacer** activé lorsqu’une stratégie a été assignée).

- **Ne pas remplacer**

  Définie au cours de l’assignation, cette stratégie ne peut pas être remplacée par une autre.

  Plus l’assignation de la stratégie **Ne pas remplacer** est éloignée de l’objet cible, plus cette stratégie a d’effet sur tous les objets conteneurs de niveau inférieur. Cela signifie qu’un conteneur de niveau supérieur soumis à **Ne pas remplacer** remplace les paramètres de stratégie d’un conteneur de niveau inférieur. Il est donc, par exemple, possible de définir une stratégie de domaine dont les paramètres ne peuvent pas être remplacés, même si **Bloquer l’héritage de stratégie** a été défini pour une UO.

  Remarque : Si une stratégie ayant une priorité inférieure mais ayant été désignée **Ne pas remplacer** est assignée au même niveau qu’une stratégie d’un niveau supérieur, cette stratégie sera prioritaire en dépit de son niveau inférieur.

3.8.7.1 Paramètres dans les stratégies

Répéter les paramètres machine

Retrouvez ce paramètre sous **Éléments de stratégie > Paramètres généraux > Chargement des paramètres > Mode de récursivité des stratégies**.

Si vous sélectionnez **Répéter les paramètres machine** dans le champ **Mode de récursivité des stratégies** d'une stratégie du type **Paramètres généraux** et que la stratégie provient d'un ordinateur (**Répéter les paramètres machine** n'affecte pas les stratégies utilisateur), cette stratégie est relue à la fin de l'analyse. Ceci remplace ensuite les paramètres de l'utilisateur et les paramètres de la machine s'appliquent. Tous les paramètres de la machine hérités directement ou indirectement par la machine (y compris les stratégies qui n'ont pas été appliquées par le mode de récursivité des stratégies **Répéter les paramètres machine**) sont remplacés.

Ignorer l'utilisateur

Retrouvez ce paramètre sous **Éléments de stratégie > Paramètres généraux > Chargement des paramètres > Mode de récursivité des stratégies**.

Si vous sélectionnez **Ignorer l'utilisateur** pour une stratégie d'ordinateur dans le champ **Mode de récursivité des stratégies** d'une stratégie du type **Paramètres généraux** et si la stratégie provient d'une machine, seuls les paramètres de la machine sont analysés. Les paramètres de l'utilisateur ne sont pas analysés.

Aucun bouclage

Retrouvez ce paramètre sous **Éléments de stratégie > Paramètres généraux > Chargement des paramètres > Mode de récursivité des stratégies**.

Aucun blocage décrit le comportement standard. Les stratégies de l’utilisateur sont prioritaires sur celles de l’ordinateur.

Analyse des paramètres « Ignorer l'utilisateur » et « Répéter les paramètres machine »

S'il existe des assignations de stratégies actives, les stratégies de la machine sont analysées et regroupées d'abord. Si, avec le **Mode de récursivité des stratégies**, ce regroupement de stratégies individuelles aboutit à la valeur **Ignorer l'utilisateur**, les stratégies définies pour l'utilisateur ne sont pas analysées. Cela signifie que les mêmes stratégies s'appliquent à la fois pour l'utilisateur et pour la machine.

Si, après regroupement des stratégies individuelles, la valeur avec l'attribut **Mode de récursivité des stratégies** est **Répéter les paramètres machine**, les stratégies de l'utilisateur sont combinées à celles de la machine. Après le regroupement, les stratégies de la machine sont réécrites et, le cas échéant, remplacent les paramètres de stratégie de l'utilisateur. Si un paramètre est présent dans les deux stratégies, la valeur de la stratégie de la machine remplace celle de la stratégie de l'utilisateur.

Si le regroupement des stratégies individuelles de la machine produit la valeur par défaut (**Pas de mode de récursivité des stratégies**), les paramètres de l'utilisateur sont prioritaires par rapport à ceux de la machine.

Ordre d'exécution des stratégies

Ignorer l'utilisateur Ordinateurs

Répéter les paramètres machine Ordinateur -> Utilisateur -> Ordinateur. La première « exécution sur machine » est requise pour les stratégies qui sont écrites avant que la connexion utilisateur n'intervienne (par exemple, image d'arrière-plan lors de la connexion).

Aucun bouclage (paramètre standard) : Ordinateur -> Utilisateur

3.8.7.2 Stratégies de type Aucun chiffrement

Lorsque des stratégies sont assignées le long d'une chaîne hiérarchique, la stratégie la plus proche dans le cas d'un objet cible (utilisateur ou ordinateur) a le niveau le plus élevé. Cela signifie que si la distance entre une stratégie et l'objet cible augmente, elle sera remplacée par toute autre stratégie plus proche. Les stratégies de type **Aucun chiffrement** peuvent être utilisées pour interrompre l'utilisation d'anciennes stratégies de chiffrement sur certains emplacements dans la hiérarchie. La stratégie **Aucun chiffrement** s'applique également aux niveaux subordonnés.

Le comportement des terminaux varie en fonction du module et de sa version.

Terminaux avec Synchronized Encryption

Les stratégies de type **Par application (Synchronized Encryption)** ne sont PAS fusionnées. La stratégie correspondant le plus à l'objet cible (utilisateur ou ordinateur) dans la hiérarchie est toujours appliquée. Si elle se trouve en haut de la hiérarchie, la stratégie **Aucun chiffrement** sera appliquée.

Terminaux avec la version 8 du module Chiffrement de fichiers

Les stratégies de type **Par emplacement** sont fusionnées. Si plusieurs stratégies sont assignées, leur contenu est évalué selon certaines règles. Retrouvez plus de renseignements à la section Règles d'assignation et d'analyse des stratégies *(page 127)*. Retrouvez plus de renseignements sur le RSOP (ensemble de stratégies) à la section Stratégies de chiffrement de fichiers par emplacement dans le RSOP *(page 349)*. Au sein d'une assignation, la stratégie ayant la plus haute priorité (1) se range au-dessus d'une stratégie ayant une priorité inférieure. Si elle se trouve en haut de la hiérarchie, la stratégie **Aucun chiffrement** sera appliquée.

Terminaux avec une version antérieure à la version 8 du module Chiffrement de fichiers

Une stratégie **Aucun chiffrement** n'aura aucun sur ces terminaux. Les terminaux avec la version 7.0 ou inférieure du module **Chiffrement de fichiers** ne reconnaissent pas le paramètre **Type de chiffrement**. Les règles issues des stratégies **Chiffrement de fichiers Par emplacement** s'appliquent.

Ceci est tout particulièrement important si vous devez gérer simultanément des terminaux sur lesquels sont installées la version 8 et d'autres avec d'anciennes versions.

3.8.8 Données d'inventaire et d'état

SafeGuard Enterprise lit une quantité considérable de données d'inventaire et d'état provenant des terminaux. Ces données indiquent l'état général en cours de chaque ordinateur. Ces données s'affichent clairement dans SafeGuard Management Center, dans **Utilisateurs et ordinateurs** dans l'onglet **Inventaire**.

En tant que responsable de la sécurité, vous pouvez afficher, exporter et imprimer les données d'inventaire et d'état. Par exemple, vous pouvez créer des rapports de conformité pour prouver que des terminaux ont été chiffrés. Les fonctions de tri et de filtrage étendus sont disponibles pour vous aider à sélectionner les données pertinentes.

L'**Inventaire** propose, par exemple, les données suivantes sur chaque machine :

- La stratégie appliquée.
- Le dernier contact du serveur.
- L'état de chiffrement de tous les supports.
- L'état et le type de l'authentification au démarrage.
- Les modules SafeGuard Enterprise installés.
- L'état de l'éveil par appel réseau sécurisé (WOL).
- Les données de l'utilisateur.

3.8.8.1 Terminaux Mac dans l'inventaire

L'**Inventaire** permet d'obtenir des données d'état pour les Macs administrés dans SafeGuard Management Center. Retrouvez plus de renseignements à la section Données d'inventaire et d'état des Mac *(page 401)*.

3.8.8.2 Affichage des données d'inventaire

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation, cliquez sur le conteneur concerné (domaine, groupe de travail ou ordinateur) à gauche.
3. Dans la zone d'action, accédez à l'onglet **Inventaire** à droite.
4. Dans la zone **Filtre**, sélectionnez le filtre à appliquer à l'écran d'inventaire comme indiqué à la section Filtrage des données d’inventaire *(page 136)*.

   Remarque : Si vous sélectionnez un ordinateur particulier, les données d'inventaire sont reçues dès que vous accédez à l'onglet **Inventaire**. La zone **Filtre** n'est pas disponible ici.

5. Dans la zone **Filtre**, cliquez sur la loupe.

Les données d'inventaire et d'état s'affichent sous forme de tableau récapitulatif de toutes les machines du conteneur sélectionné. Les onglets **Lecteurs**, **Utilisateurs** et **Fonctions** sont également disponibles pour chaque machine.

Cliquez sur l'en-tête de la colonne pour trier les données d'inventaire par les valeurs de la colonne sélectionnée. Le menu contextuel de chaque colonne propose de nombreuses fonctions de tri, de regroupement et de personnalisation de l'affichage. En fonction de vos droits d'accès, les éléments dans l'inventaire apparaissent dans des couleurs différentes :

- Les éléments des objets pour lesquels vous avez des droits d'**Accès complet** apparaissent en noir.
- Les éléments des objets pour lesquels vous avez des droits d'accès en **Lecture seule** apparaissent en bleu.
- Les éléments des objets pour lesquels vous n'avez aucun droit d'accès sont grisés.

3.8.8.3 Affichage des colonnes masquées

Dans l’affichage des données d’inventaire, certaines colonnes sont masquées par défaut.

1. Dans cet affichage, cliquez avec le bouton droit de la souris sur la barre d’en-têtes de colonnes.
2. Dans le menu contextuel, sélectionnez **Exécuter la personnalisation de colonne**.

   La fenêtre **Personnalisation** apparaît affichant les colonnes cachées.

3. Déplacez la colonne requise depuis la fenêtre **Personnalisation** vers la barre d’en-têtes de colonnes.

La colonne apparaît dans l’affichage des données d’inventaire Pour la masquer de nouveau, déplacez-la de nouveau dans la fenêtre **Personnalisation**.

3.8.8.4 Filtrage des données d’inventaire

Lorsque vous utilisez une OU, des filtres peuvent être définis pour limiter l’affichage en fonction d’un critère particulier.

Les champs suivants sont disponibles pour définir des filtres dans la zone **Filtre** de l’onglet **Inventaire** :

Champ	Description
Nom de l’ordinateur	Pour afficher les données d’inventaire et d’état d’un ordinateur particulier, entrez le nom de l’ordinateur dans ce champ.
Sous-conteneurs inclus	Activez ce champ pour inclure les sous-conteneurs à l’écran.
Afficher la dernière modification	Indiquez dans ce champ le nombre de modifications à afficher.

Vous pouvez également utiliser l’éditeur de filtres pour créer des filtres définis par l’utilisateur. Vous pouvez ouvrir l’éditeur de filtres depuis le menu contextuel de chaque colonne. Dans la fenêtre **Générateur de filtres**, vous pouvez définir des filtres personnalisés et les appliquer à la colonne concernée.

3.8.8.5 Actualisation des données d’inventaire

Les terminaux envoient et mettent généralement à jour les données d’inventaire lorsqu’elles sont modifiées.

La commande **Demander une actualisation de l’inventaire** peut être utilisée pour demander manuellement une actualisation des données d’inventaire actuelles de l’ordinateur. Cette commande est disponible pour un ordinateur particulier ou pour tous les ordinateurs d’un nœud (pouvant inclure des nœuds secondaires) depuis le menu contextuel et le menu **Actions** de la barre de menus de SafeGuard Management Center. La commande peut également être sélectionnée via le menu contextuel des entrées de la liste.

Si vous sélectionnez cette commande ou cliquez sur l’icône **Demander une actualisation de l’inventaire** dans la barre d’outils, les ordinateurs concernés envoient leurs données d’inventaire actuelles.

Comme cela est le cas avec d’autres zones de SafeGuard Management Center, vous pouvez utiliser la commande **Actualiser** pour actualiser l’affichage. Vous pouvez sélectionner cette commande dans le menu contextuel pour les ordinateurs individuels ou tous les ordinateurs d’un nœud et dans le menu

Afficher de la barre de menus. Vous pouvez également utiliser l'icône à double flèche **Actualiser** dans la barre d'outils pour actualiser l'affichage.

3.8.8.6 Vue générale

Les colonnes individuelles dans la vue générale proposent les informations suivantes :

Remarque : Certains colonnes sont cachées par défaut. Vous pouvez personnaliser l'affichage pour les montrer. Retrouvez plus de renseignements à la section Affichage des colonnes masquées *(page 135)*.

Colonne	Explication
Nom de l'ordinateur	Indique le nom de l'ordinateur.
Domaine	Indique le nom du domaine de l'ordinateur.
Domaine pré 2000	Indique le nom du domaine avant Windows 2000.
Nom d'utilisateur (propriétaire)	Indique le nom utilisateur du propriétaire de l'ordinateur, s'il est disponible.
Prénom	Indique le prénom du propriétaire, s'il est disponible.
Nom	Indique le nom de famille du propriétaire, s'il est disponible.
Adresse électronique	Indique l'adresse électronique du propriétaire, s'il est disponible.
Autres utilisateurs enregistrés	Affiche les noms des autres utilisateurs enregistrés de l'ordinateur, s'ils sont disponibles.
Système d'exploitation	Indique le système d'exploitation de l'ordinateur.
Dernier contact du serveur	Indique la date et l'heure auxquelles l'ordinateur a communiqué avec le serveur pour la dernière fois.
Dernière stratégie reçue	Indique la date et l'heure auxquelles l'ordinateur a reçu la dernière stratégie.
Lecteurs chiffrés	Indique les lecteurs chiffrés de l'ordinateur.
Lecteurs non chiffrés	Indique les lecteurs non chiffrés de l'ordinateur.
Type d'authentification au démarrage	Indique si l'ordinateur est un terminal SafeGuard Enterprise natif, un terminal BitLocker avec Challenge/Réponse SafeGuard, un terminal BitLocker avec mécanisme de récupération natif, un terminal FileVault 2 ou un terminal avec un lecteur de disque dur conforme à la norme d'auto-chiffrement Opal.
Authentification au démarrage (POA)	Indique si l'authentification au démarrage SafeGuard est activée pour l'ordinateur.
Éveil par appel réseau (WOL)	Indique si l'éveil par appel réseau est activé pour l'ordinateur.
Date de modification	Indique la date à laquelle les données d'inventaire ont changé en raison d'une demande d'actualisation de l'inventaire ou de l'envoi de l'ordinateur de nouvelles données d'inventaire.
Actualisation demandée	Indique la date de la dernière demande d'actualisation. La valeur affichée dans ce champ sera supprimée une fois la demande traitée par l'ordinateur.

Colonne	Explication
DSN parent	Indique le nom distinctif de l’objet conteneur auquel l’ordinateur est subordonné. Cette colonne ne s’affiche que si le champ **Sous-conteneurs inclus** a été activé dans la zone **Filtre**.
Certificat d’entreprise actuel	Indique si l’ordinateur utilise le certificat d’entreprise actuel.

3.8.8.7 Onglet Lecteurs

L’onglet **Lecteurs** indique les données d’inventaire et d’état des lecteurs sur l’ordinateur concerné.

Colonne	Explication
Nom du lecteur	Indique le nom du lecteur.
Étiquette	Identifie un lecteur Mac
Type	Indique le type de lecteur, par exemple **Fixe**, **Support amovible** ou **CD-ROM/DVD**.
État	Indique l’état de chiffrement d’un lecteur. Si la gestion de SafeGuard BitLocker est installée sur un terminal, il se peut que l’état de chiffrement d’un lecteur indique **Non préparé**. Ceci signifie que le lecteur ne peut actuellement pas être chiffré avec BitLocker car les préparations d’usage n’ont pas encore été effectuées. Ceci s’applique uniquement aux terminaux administrés. En effet, les terminaux non administrés ne sont pas en mesure de créer des rapports sur les données d’inventaire. Retrouvez plus de renseignements sur les conditions préalables requises pour gérer et chiffrer les lecteurs BitLocker à la section Conditions préalables à la gestion de BitLocker sur les terminaux *(page 326)*. Cette colonne indique également si BitLocker a été suspendu ou repris par ses utilisateurs. L’état de chiffrement d’un terminal non administré peut être vérifié à l’aide de l’outil de ligne de commande SGNState comme indiqué à la section Affichage de l’état du système avec SGNState *(page 483)*.
Méthode de chiffrement	Pour les lecteurs chiffrés, ce champ indique l’algorithme utilisé pour le chiffrement.

3.8.8.8 Onglet Utilisateurs

L’onglet **Utilisateurs** indique les données d’inventaire et d’état des utilisateurs sur l’ordinateur.

Colonne	Explication
Nom d’utilisateur	Indique le nom de l’utilisateur.
Nom distinctif	Indique le nom DNS de l’utilisateur, par exemple : CN=Administrateur,CN=Utilisateurs,DC=domaine,DC=monentreprise,DC=net
Utilisateur propriétaire	Indique si l’utilisateur est défini comme étant le propriétaire de l’ordinateur.
Utilisateur verrouillé	Indique si l’utilisateur est verrouillé.
Utilisateur Windows de SGN	Indique si l’utilisateur est un utilisateur Windows de SGN. Un utilisateur Windows de SGN n’est pas ajouté à l’authentification au démarrage SafeGuard. En revanche, il dispose d’un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur SGN. Vous pouvez activer l’enregistrement des utilisateurs Windows de SGN sur les terminaux grâce à des stratégies de type **Paramètres de machine spécifiques**.

3.8.8.9 Onglet Fonctions

L’onglet **Fonctions** propose une présentation de tous les modules SafeGuard Enterprise installés sur l’ordinateur.

Colonne	Explication
Nom du module	Indique le nom du module SafeGuard Enterprise installé.
Version	Indique la version logicielle du module SafeGuard Enterprise installé et, si un module de chiffrement de fichiers est installé, la version du pilote du Chiffrement de fichiers.

3.8.8.10 Onglet Certificat d’entreprise

L’onglet **Certificat d’entreprise** affiche les propriétés du certificat d’entreprise actuellement utilisé et indique si un certificat plus récent est disponible.

Colonne	Explication
Objet	Affiche le nom distinctif du sujet du certificat d’entreprise.
Série	Affiche le numéro de série du certificat d’entreprise.
Émetteur	Affiche le nom distinctif de l’émetteur du certificat d’entreprise.
Valide à compter du	Affiche la date et l’heure du début de la validité du certificat d’entreprise.
Valide jusqu’au	Affiche la date et l’heure de l’expiration du certificat d’entreprise.
Un certificat d’entreprise plus récent est disponible	Indique si un certificat d’entreprise plus récent que celui en cours d’utilisation sur le terminal est disponible.

3.8.8.11 Création de rapports des données d'inventaire

En tant que responsable de la sécurité, vous pouvez créer des rapports des données d'inventaire dans différents formats. Par exemple, vous pouvez créer des rapports de conformité pour prouver que des terminaux ont été chiffrés. Les rapports peuvent être imprimés ou exportés dans un fichier.

Impression de rapports d’inventaire

1. Dans la barre de menus de SafeGuard Management Center, cliquez sur **Fichier**.
2. Vous pouvez soit imprimer le rapport directement, soit afficher un aperçu avant impression.

   L’aperçu avant impression fournit plusieurs fonctions, par exemple pour la modification de la mise en page (en-tête et pied de page, etc.).

   - Pour obtenir un aperçu avant impression, sélectionnez **Aperçu avant impression**.
   - Pour imprimer le document sans afficher l’aperçu, sélectionnez **Imprimer**.

Exportation des rapports d’inventaire dans les fichiers

1. Dans la barre de menus de SafeGuard Management Center, cliquez sur **Fichier**.
2. Sélectionnez **Aperçu avant impression**.

   Le rapport d’inventaire **Aperçu** apparaît.

   L’aperçu fournit plusieurs fonctions, par exemple pour la modification de la mise en page (en-tête et pied de page, etc.).

3. Dans la barre d’outils de la fenêtre **Aperçu**, sélectionnez la liste déroulante de l’icône **Exporter le document...**.
4. Dans la liste, sélectionnez le type de fichier requis.
5. Indiquez les options d’exportation nécessaires et cliquez sur **OK**.

Le rapport d’inventaire est exporté dans un fichier du type spécifié.

3.8.9 Responsables de la sécurité de SafeGuard Enterprise

SafeGuard Enterprise peut être administré par un ou plusieurs responsables de la sécurité. La gestion basée sur le rôle de SafeGuard Enterprise permet de répartir l'administration entre plusieurs utilisateurs. Un utilisateur peut se voir assigner un ou plusieurs rôles. Pour améliorer la sécurité, l'autorisation supplémentaire d'une action peut être assignée au rôle d'un responsable.

Au cours de la configuration initiale de SafeGuard Management Center, un administrateur de niveau supérieur, le responsable principal de la sécurité, possédant tous les droits et un certificat, est créé par défaut. Retrouvez plus de renseignements à la section Création du responsable principal de la sécurité *(page 42)*. Le certificat du responsable principal de la sécurité expire après 5 ans et peut être renouvelé dans la section **Responsables de la sécurité** de SafeGuard Management Center. D'autres responsables de la sécurité peuvent être assignés à des tâches spécifiques, comme le support ou l'audit.

Dans la zone de navigation de SafeGuard Management Center, vous pouvez réorganiser les responsables de la sécurité de façon hiérarchique pour refléter la structure organisationnelle de votre entreprise. Toutefois, cette hiérarchie ne tient pas compte des droits et des rôles.

Remarque : Deux responsables de la sécurité ne doivent pas utiliser le même compte Windows sur le même ordinateur. Dans le cas contraire, il est impossible de distinguer correctement leurs droits d'accès. Une authentification supplémentaire est plus sûre lorsque les responsables de la sécurité doivent s'authentifier à l'aide de tokens/cartes à puce.

3.8.9.1 Rôles du responsable de la sécurité

Pour plus de simplicité, SafeGuard Enterprise propose des rôles prédéfinis pour les responsables de la sécurité dotés de diverses fonctions. Un responsable de la sécurité possédant les droits nécessaires peut également définir de nouveaux rôles à partir d'une liste d'actions/de droits et les assigner à des responsables de la sécurité particuliers.

Les types de rôle suivants sont fournis :

- Rôle du responsable principal de la sécurité
- Rôles prédéfinis
- Rôles personnalisés

Responsable principal de la sécurité

Après avoir installé SafeGuard Enterprise, un responsable principal de la sécurité (MSO, Master Security Officer) est créé par défaut au cours de la configuration initiale de SafeGuard Management Center. Le responsable principal de la sécurité est un responsable de la sécurité de niveau supérieur. Il bénéficie de tous les droits et peut accéder à tous les objets (semblable à un administrateur Windows). Les droits du responsable principal de la sécurité ne peuvent pas être modifiés.

Plusieurs responsables principaux de la sécurité peuvent être créés pour une seule instance de SafeGuard Management Center. Pour des raisons de sécurité, la création d'au moins un MSO supplémentaire est fortement recommandée. Les MSO supplémentaires peuvent être supprimés. Toutefois, il doit toujours rester un utilisateur bénéficiant du rôle de MSO et créé de manière explicite en tant que MSO dans la base de données SafeGuard Enterprise.

Un responsable principal de la sécurité peut déléguer des tâches à une autre personne. Pour ce faire, vous pouvez procéder de deux façons :

- Un nouveau responsable de la sécurité peut être créé dans **Responsables de la sécurité**.
- Un utilisateur ou tous les membres d'un conteneur importé d'Active Directory et visibles dans le répertoire racine de SafeGuard Management Center peuvent être promus au rang de responsable de la sécurité dans **Utilisateurs et ordinateurs**.

Un ou plusieurs rôles peuvent alors être assignés aux responsables de la sécurité. Par exemple, un utilisateur peut se voir assigner le rôle de responsable supervision et celui de responsable du support.

Toutefois, le responsable principal de la sécurité peut également créer des rôles personnalisés et les assigner à des utilisateurs particuliers.

Exportation du certificat du responsable principal de la sécurité

Dans une installation SafeGuard Enterprise, le certificat du responsable principal de la sécurité est un élément essentiel devant être sauvegardés dans un emplacement sûr. Nous vous conseillons de réaliser cette tâche immédiatement après la configuration initiale de SafeGuard Management Center.

Pour sauvegarder le certificat du responsable principal de la sécurité connecté à SafeGuard Management Center :

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Options**.
2. Sélectionnez l'onglet **Certificats** et cliquez sur **Exporter** dans la section **Certificat de <administrateur>**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Saisissez un mot de passe, confirmez-le, puis cliquez sur **OK**.

4. Saisissez un nom et un emplacement de stockage pour le fichier à exporter et cliquez sur **OK**.

Le certificat du responsable principal de la sécurité actuellement connecté est exporté sous la forme d'un fichier .p12 à l'emplacement défini et peut être utilisé à des fins de récupération.

Rôles prédéfinis

Dans SafeGuard Management Center, les rôles de responsable de la sécurité suivants, sauf ceux du MSO, sont prédéfinis. L'assignation des droits à ces rôles prédéfinis ne peut être changée. Par exemple, si un rôle prédéfini possède le droit de « création d'éléments de stratégie et de groupes de stratégies », ce droit ne peut pas être supprimé du rôle. De même, un nouveau droit ne peut pas être ajouté à un rôle prédéfini. Toutefois, vous pouvez assigner à tout moment une authentification responsable à des rôles prédéfinis.

- **Superviseur**

  Les responsables supervision peuvent accéder à leurs propres nœuds dans la zone **Responsables de la sécurité**. De même, ils sont autorisés à gérer les responsables de la sécurité inclus dans leurs nœuds respectifs.

- **Responsable de la sécurité**

  Les responsables de la sécurité possèdent des droits étendus, notamment sur la configuration de SafeGuard Enterprise, la gestion des stratégies et des clés, ainsi que sur les autorisations relatives au contrôle et à la récupération.

- **Responsable du support**

  Les responsables du support ont le droit d'effectuer des actions de récupération. Ils peuvent également afficher la plupart des zones de fonctions de SafeGuard Management Center.

- **Responsable de l'audit**

  Pour contrôle SafeGuard Enterprise, les responsables d'audit peuvent afficher la plupart des zones de fonctions de SafeGuard Management Center.

- **Responsable de la récupération**

  Les responsables de la récupération ont le droit de réparer la base de données SafeGuard Enterprise.

Rôles personnalisés

En tant que responsable de la sécurité possédant les droits nécessaires, vous pouvez définir de nouveaux rôles à partir d'une liste d'actions/de droits, puis les assigner à un responsable de la sécurité existant ou nouveau. De même qu'avec les rôles prédéfinis, vous pouvez activer l'authentification responsable supplémentaire pour une fonction du rôle à tout moment.

Lors de l'assignation d'un nouveau rôle, notez les informations suivantes relatives à l'authentification supplémentaire :

Remarque : Si un utilisateur a deux rôles avec les mêmes droits et si l'authentification supplémentaire est assignée à l'un des rôles, elle s'applique automatiquement à l'autre également.

Un responsable de la sécurité avec les droits nécessaires peut ajouter des droits à un rôle personnalisé, ou en supprimer. Contrairement aux rôles prédéfinis, les rôles personnalisés peuvent être modifiés et même supprimés le cas échéant. Lorsque vous supprimez le rôle, il n'est plus assigné à aucun utilisateur. Si un seul rôle est assigné à un utilisateur et si ce rôle est supprimé, l'utilisateur ne peut plus se connecter à SafeGuard Management Center.

Remarque : Le rôle et les actions définis dans le cadre de celui-ci déterminent ce qu'un utilisateur peut faire et ne pas faire. Ceci est également vrai si l'utilisateur a plusieurs rôles. Lorsque l'utilisateur s'est connecté à SafeGuard Management Center, les seules zones qui sont activées et affichées sont celles qui sont nécessaires pour son rôle respectif. Ceci s'applique également aux zones des scripts et de l'API. Il est donc important de toujours activer l'affichage de la zone dans laquelle les actions respectives sont définies. Les actions sont triées par zone de fonctions et disposées de manière hiérarchique. Cette structure permet de visualiser les actions nécessaires à l'exécution d'autres actions.

Authentification d'un responsable supplémentaire

L'authentification d'un responsable supplémentaire (également appelée « règle des deux personnes ») peut être assignée à des actions spécifiques d'un rôle. Cela signifie que l'utilisateur de ce rôle n'est autorisé à effectuer qu'une certaine action si un utilisateur d'un autre rôle est présent et le confirme. À chaque fois qu'un utilisateur effectue cette action, un autre utilisateur doit la confirmer.

Vous pouvez assigner une authentification supplémentaire indifféremment à des rôles prédéfinis ou personnalisés. Dès qu'un autre responsable a le même rôle, le rôle personnalisé peut également être sélectionné.

Le rôle consistant à effectuer l'autorisation supplémentaire doit être préalablement assigné à un utilisateur. De plus, la base de données SafeGuard Enterprise doit compter au moins deux responsables de la sécurité. Lorsqu'une action requiert une authentification supplémentaire, celle-ci est nécessaire même si l'utilisateur détient un autre rôle ne nécessitant pas d'authentification supplémentaire pour la même action.

Si un responsable crée un rôle alors qu'il ne possède pas le droit de modification de l'authentification supplémentaire, les paramètres relatifs à une authentification supplémentaire du nouveau rôle seront pré-renseignés afin de correspondre à ceux définis pour le responsable de la création de ce rôle.

3.8.9.2 Création d'un rôle

Condition préalable : pour créer un rôle, vous devez posséder le droit d'affichage et de création de rôles de responsable de la sécurité. Pour assigner une authentification supplémentaire, vous devez posséder le droit de « modification des paramètres d'authentification supplémentaire ».

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Cliquez avec le bouton droit de la souris sur **Rôles personnalisés** et sélectionnez **Nouveau > Nouveau rôle personnalisé**.
3. Dans le champ **Nouveau rôle personnalisé**, saisissez un nom et une description pour le rôle.
4. Assignez les actions à ce rôle : Sélectionnez les cases en regard de l'action requise dans la colonne **Activé**.

   Les actions sont triées par zone de fonctions et disposées de manière hiérarchique. Cette structure permet de visualiser les actions nécessaires à l'exécution d'autres actions.

5. Si nécessaire, assignez une **Authentification d'un autre responsable** : Cliquez sur le paramètre par défaut **Aucune** et, depuis la liste, sélectionnez le rôle requis.

   Si un responsable crée un rôle sans posséder de droit de modification de l'authentification supplémentaire, les paramètres relatifs à l'authentification supplémentaire seront préalablement renseignés en fonction de l'authentification supplémentaire définie pour les rôles du responsable.

6. Cliquez sur **OK**.

Le nouveau rôle est affiché sous **Rôles personnalisés** dans la fenêtre de navigation. Lorsque vous cliquez sur le rôle, les actions autorisées sont affichées dans la zone d'action de droite.

3.8.9.3 Assignation d'un rôle à un responsable de la sécurité

Condition préalable : pour assigner un rôle, vous devez posséder le droit d'affichage et de modification des responsables de la sécurité.

1. Sélectionnez le responsable approprié dans la fenêtre de navigation.

Les propriétés s'affichent dans la zone d'action de droite.

2. Assignez les rôles nécessaires en sélectionnant les cases correspondantes en regard des rôles disponibles.

   Les rôles prédéfinis s'affichent en gras.

3. Cliquez sur le symbole à double flèche d'**Actualiser** dans la barre d'outils.

Le rôle est assigné au responsable de la sécurité.

Remarque : Les rôles personnalisés complexes peuvent entraîner de légers problèmes de performances lors de l'utilisation de SafeGuard Management Center.

3.8.9.4 Affichage des propriétés du responsable et du rôle

Condition préalable : pour obtenir un aperçu des propriétés du responsable ou de l’assignation du rôle, vous devez posséder le droit d’affichage des responsables de la sécurité et des rôles de ces derniers.

Pour afficher les propriétés du responsable et du rôle :

1. Dans SafeGuard Management Center, cliquez sur **Responsables de la sécurité**.
2. Dans la zone de navigation de gauche, cliquez deux fois sur l’objet dont vous souhaitez obtenir un aperçu.

Les informations disponibles dans la zone d’action à droite dépendent de l’objet sélectionné.

Affichage des propriétés du responsable principal de la sécurité

Les informations générales et de modification relatives au responsable principal de la sécurité s’affichent.

Affichage des propriétés des responsables de la sécurité

Les informations générales et de modification relatives au responsable de la sécurité s’affichent.

Dans **Propriétés**, sélectionnez l’onglet **Actions** afin d’afficher un résumé des actions autorisées et des rôles assignés au responsable de la sécurité.

Affichage des droits et des rôles des responsables de la sécurité

Un résumé des actions de tous les rôles assignés au responsable de la sécurité s'affiche. L'arborescence affiche les actions nécessaires à l'exécution d'autres actions. Les rôles assignés peuvent également être affichés.

1. Dans la boîte de dialogue **<Nom du responsable de la sécurité> Propriétés**, dans l'onglet **Actions**, sélectionnez une action pour afficher tous les rôles assignés qui contiennent cette action.
2. Cliquez deux fois sur un rôle dans la liste **Rôles assignés avec l'action sélectionnée**. La boîte de dialogue **<Nom du responsable de la sécurité> Propriétés** se ferme et les propriétés du rôle s'affichent.

Affichage des propriétés du rôle

Les informations générales et de modification relatives au rôle s'affichent.

Dans **Propriétés**, sélectionnez l'onglet **Assignation** afin d'afficher les responsables de la sécurité assignés à ce rôle.

Affichage de l'assignation du rôle

Dans **<Nom du rôle> Propriétés**, dans l'onglet **Assignation**, cliquez deux fois sur un responsable de la sécurité. La boîte de dialogue **Propriétés** se ferme et les données générales et les rôles du responsable de la sécurité s'affichent.

3.8.9.5 Modification d'un rôle

Vous pouvez effectuer les étapes suivantes :

- Modifier l'authentification supplémentaire uniquement.
- Modifier toutes les propriétés du rôle.

L'icône en regard des rôles affiche l'action disponible :

Icône	Description
	Le rôle peut être modifié (ajouter/supprimer des actions).
	L'authentification supplémentaire peut être modifiée.
	Les deux types de modification sont disponibles.

Remarque : Vous ne pouvez pas modifier les rôles prédéfinis et les actions qui leur sont assignées. Si une authentification supplémentaire est activée, celle-ci peut être modifiée pour tous les rôles, même les rôles prédéfinis.

Modification de l'authentification supplémentaire uniquement

Condition préalable : pour assigner une authentification supplémentaire, vous devez posséder le droit d'affichage des rôles du responsable de la sécurité et de « modification des paramètres d'authentification supplémentaire ».

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez sur le rôle à modifier. Dans la zone d'action de droite, cliquez sur le paramètre requis dans la colonne **Authentification de responsable de la sécurité supplémentaire** et sélectionnez un rôle différent dans la liste.

   Les rôles prédéfinis s'affichent en gras.

3. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

L'authentification responsable supplémentaire a été modifiée pour ce rôle.

Modification de toutes les propriétés d’un rôle

Condition préalable : pour modifier un rôle personnalisé, vous devez posséder le droit d’affichage et de modification des rôles de responsable de la sécurité. Pour assigner de nouveau une authentification supplémentaire, vous devez posséder le droit de « modification des paramètres d’authentification supplémentaire ».

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez avec le bouton droit de la souris sur le rôle à modifier et sélectionnez **Modifier un rôle personnalisé**.
3. Modifiez les propriétés selon vos besoins. Modifiez les propriétés d’authentification supplémentaire en cliquant sur la valeur de cette colonne et en sélectionnant le rôle requis.
4. Cliquez sur l’icône **Enregistrer** de la barre d’outils pour enregistrer vos modifications dans la base de données.

Le rôle a été modifié.

3.8.9.6 Copie d’un rôle

Pour créer un rôle dont les propriétés sont identiques à celles d’un rôle existant, vous pouvez utiliser le rôle existant comme modèle pour le nouveau rôle. Vous pouvez sélectionner un rôle prédéfini ou personnalisé comme modèle.

Condition préalable : vous pouvez utiliser des rôles existants comme modèles uniquement si le responsable de la sécurité actuellement authentifié possède tous les droits contenus dans le modèle de rôle spécifique. Par conséquent, cette fonction peut ne pas être disponible pour les responsables ne possédant qu’un nombre d’actions limité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le rôle à copier et sélectionnez **Nouveau > Nouvelle copie du rôle**.
   Dans **Nouveau rôle personnalisé**, toutes les propriétés du rôle existant sont présélectionnées.
3. Saisissez un nouveau nom pour ce rôle et modifiez les propriétés selon les besoins.
4. Cliquez sur l’icône **Enregistrer** de la barre d’outils pour enregistrer vos modifications dans la base de données.

Le nouveau rôle est créé.

3.8.9.7 Suppression d’un rôle

Remarque : Les rôles prédéfinis ne peuvent pas être supprimés.

Condition préalable : pour supprimer un rôle, vous devez posséder le droit d’affichage et de suppression des rôles de responsable de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, sous **Rôles personnalisés**, cliquez avec le bouton droit sur le rôle à supprimer et sélectionnez **Supprimer**. En fonction des propriétés du rôle, un message d’avertissement spécifique s’affichera.

   Remarque : Lorsque vous supprimez un rôle, tous les responsables de la sécurité auxquels ce rôle est assigné perdent ce dernier. Si le rôle est le seul assigné à un responsable de la sécurité, ce dernier ne peut plus se connecter à SafeGuard Management Center, sauf s’il se voit assigner un nouveau rôle par un responsable de la sécurité supérieur. Si le rôle est utilisé à des fins d’authentification supplémentaire, le MSO devra effectuer une authentification supplémentaire.

3. Pour supprimer le rôle, cliquez sur **Oui** dans le message d’avertissement.
4. Cliquez sur l’icône **Enregistrer** de la barre d’outils pour enregistrer vos modifications dans la base de données.

Le rôle est supprimé de la fenêtre de navigation et de la base de données.

3.8.9.8 Création d’un responsable principal de la sécurité

Condition préalable : pour créer un responsable principal de la sécurité, vous devez posséder le droit d’affichage et de création de responsables de la sécurité.

Remarque : Un moyen rapide de créer de nouveaux responsables principaux de la sécurité est de promouvoir un responsable de la sécurité. Retrouvez plus de renseignements à la section Promotion des responsables de la sécurité *(page 156)*.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le nœud **Responsables principaux de la sécurité** et sélectionnez **Nouveau > Nouveau responsable principal de la sécurité**.
3. Saisissez les informations correspondantes dans **Nouveau responsable principal de la sécurité** :

Champ/ case à cocher	Description
Activé	Le responsable de la sécurité peut être désactivé jusqu’à nouvel avis. Le responsable de la sécurité est dans le système mais ne peut pas encore se connecter à SafeGuard Management Center. Il peut seulement le faire et effectuer ses tâches d’administration lorsqu’un autre responsable l’active.
Nom	Saisissez le nom du responsable de sécurité tel qu’il est fourni dans les certificats créés par SafeGuard Enterprise sous la forme cn =. Le responsable de la sécurité est également affiché sous ce nom dans la fenêtre de navigation de SafeGuard Management Center. Ce nom doit être unique. Valeur maximale : 256 caractères
Description	Facultatif Valeur maximale : 256 caractères
Téléphone portable	Facultatif Valeur maximale : 128 caractères

Champ/ case à cocher	Description
Email	Facultatif Valeur maximale : 256 caractères
Connexion au token	La connexion peut s'effectuer de la façon suivante : **Aucun token**. Le responsable de la sécurité ne peut pas se connecter avec un token. Il doit se connecter en saisissant les informations de connexion (nom d'utilisateur/mot de passe). **Facultatif**. La connexion peut s'effectuer avec un token ou en saisissant les informations de connexion. Le responsable de la sécurité a le choix. **Obligatoire**. Un token doit être utilisé pour la connexion. Pour ce faire, la clé privée appartenant au certificat du responsable de la sécurité doit se trouver sur le token.
Certificat	Un responsable de la sécurité a toujours besoin d'un certificat pour se connecter à SafeGuard Management Center. Le certificat peut être créé par SafeGuard Enterprise lui-même ou un certificat existant peut être utilisé. Si la connexion avec un token est essentielle, le certificat doit être ajouté au token du responsable de la sécurité. **Créer :** Le certificat et le fichier de clé sont créés et enregistrés dans un emplacement choisi. Saisissez et confirmez un mot de passe pour le fichier P12. Le fichier .p12 doit être à la disposition du responsable de la sécurité lorsqu'il se connecte. Le certificat créé est assigné automatiquement au responsable de la sécurité et affiché dans **Certificat**. Si des règles de mot de passe de SafeGuard Enterprise sont utilisées, celles-ci doivent être désactivées dans Active Directory. **Remarque :** Longueur max. du chemin d'enregistrement et du nom de fichier : 260 caractères. Lors de la création d'un responsable de la sécurité, la partie publique du certificat suffit. Lors de la connexion à SafeGuard Management Center, cependant, la partie privée du certificat (le fichier de clé) est également requise. Si elle n'est pas disponible dans la base de données, elle doit l'être pour le responsable de la sécurité (sur une carte mémoire, par exemple), et peut être stockée dans le magasin de certificats pendant la connexion.
Certificat	**Importation :**

Champ/ case à cocher	Description
	Un certificat existant est utilisé et assigné au responsable de la sécurité lors de l'importation. Si l'importation s'effectue à partir d'un fichier de clé .p12, le mot de passe du certificat doit être connu. Si un conteneur de certificats PKCS#12 est sélectionné, tous les certificats sont chargés dans la liste de certificats assignables. L'assignation du certificat s'effectue après l'importation, en le sélectionnant dans la liste déroulante.

4. Pour confirmer, cliquez sur **OK**.

Le nouveau responsable principal de la sécurité apparaît dans la fenêtre de navigation, sous le nœud **Responsables principaux de la sécurité**. Leurs propriétés peuvent être affichées en sélectionnant le responsable de la sécurité concerné dans la fenêtre de navigation. Le MSO peut se connecter à SafeGuard Management Center avec le nom affiché.

3.8.9.9 Création d'un responsable de la sécurité

Condition préalable : Pour créer un responsable de la sécurité, vous devez posséder le droit d'affichage et de création de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le nœud du responsable de la sécurité où vous souhaitez placer le nouveau responsable de la sécurité, puis sélectionnez **Nouveau > Nouveau responsable de la sécurité**.
3. Procédez de la façon suivante dans la boîte de dialogue **Nouveau responsable de la sécurité** :

Champ/case à cocher	Description
Activé	Le responsable de la sécurité peut être désactivé jusqu'à nouvel avis. Le responsable de la sécurité est dans le système mais ne peut pas encore se connecter à SafeGuard Management Center. Il peut seulement le faire et effectuer ses tâches d'administration lorsqu'un autre responsable l'active.
Nom	Saisissez le nom du responsable de sécurité tel qu'il est fourni dans les certificats créés par SafeGuard Enterprise sous la forme cn =. Le responsable de la sécurité est également affiché sous ce nom dans la fenêtre de navigation de SafeGuard Management Center. Ce nom doit être unique. Valeur maximale : 256 caractères

Champ/case à cocher	Description
Description	Facultatif Valeur maximale : 256 caractères
Téléphone portable	Facultatif Valeur maximale : 128 caractères
Email	Facultatif Valeur maximale : 256 caractères
Validité	Sélectionnez les dates de début et de fin d'autorisation de connexion du responsable de la sécurité à SafeGuard Management Center.
Connexion au token	La connexion peut s'effectuer de la façon suivante : **Aucun token**. Le responsable de la sécurité ne peut pas se connecter avec un token. Il doit se connecter en saisissant ses informations de connexion (nom d'utilisateur/mot de passe). **Facultatif**. La connexion peut s'effectuer avec un token ou en saisissant les informations de connexion. Le responsable de la sécurité a le choix. **Obligatoire**. Un token doit être utilisé pour la connexion. Pour ce faire, la clé privée appartenant au certificat du responsable de la sécurité doit se trouver sur le token.
Certificat	Un responsable de la sécurité a toujours besoin d'un certificat pour se connecter à SafeGuard Management Center. Le certificat peut être créé par SafeGuard Enterprise lui-même ou un certificat existant peut être utilisé. Si la connexion avec un token est essentielle, le certificat doit être ajouté au token du responsable de la sécurité. **Créer :** Le certificat et le fichier de clé sont créés et enregistrés dans un emplacement choisi. Saisissez et confirmez un mot de passe pour le fichier P12. Le fichier .p12 doit être à la disposition du responsable de la sécurité lorsqu'il se connecte. Le certificat créé est assigné automatiquement au responsable de la sécurité et affiché dans **Certificat**. Si des règles de mot de passe de SafeGuard Enterprise sont utilisées, celles-ci doivent être désactivées dans Active Directory.

Champ/case à cocher	Description
	Remarque : Longueur max. du chemin d'enregistrement et du nom de fichier : 260 caractères. Lors de la création d'un responsable de la sécurité, la partie publique du certificat suffit. Lors de la connexion à SafeGuard Management Center, cependant, la partie privée du certificat (le fichier de clé) est également requise. Si elle n'est pas disponible dans la base de données, elle doit l'être pour le responsable de la sécurité (sur une carte mémoire, par exemple), et peut être stockée dans le magasin de certificats pendant la connexion.
Certificat	**Importation :** Un certificat existant est utilisé et assigné au responsable de la sécurité lors de l'importation. Si l'importation s'effectue à partir d'un fichier de clé .p12, le mot de passe du certificat doit être connu. Si un conteneur de certificats PKCS#12 est sélectionné, tous les certificats sont chargés dans la liste de certificats assignables. L'assignation du certificat s'effectue après l'importation, en le sélectionnant dans la liste déroulante.
Rôles du responsable de la sécurité	**Rôles** Des rôles prédéfinis ou personnalisés peuvent être assignés au responsable de la sécurité. Les droits associés à chaque rôle s'affichent sous **Action autorisée** dans la zone d'action en cliquant sur le rôle respectif ou en cliquant avec le bouton droit de la souris sur le responsable de la sécurité et en sélectionnant **Propriétés**, **Actions**. Il est possible d'assigner plusieurs rôles à un utilisateur.

4. Pour confirmer, cliquez sur **OK**.

Le nouveau responsable de la sécurité apparaît dans la fenêtre de navigation, sous le nœud **Responsables de la sécurité** respectif. Leurs propriétés peuvent être affichées en sélectionnant le responsable de la sécurité concerné dans la fenêtre de navigation. Le responsable de la sécurité peut se connecter à SafeGuard Management Center avec le nom affiché. Vous devez ensuite assigner les objets/domaines de répertoire au responsable de la sécurité afin que celui-ci puisse exécuter ses tâches.

3.8.9.10 Assignation d'objets de répertoire à un responsable de la sécurité

Afin que les responsables de la sécurité puissent exécuter ses tâches, il doit posséder les droits d'accès aux objets de répertoire. Les droits d'accès peuvent être accordés aux domaines, aux

unités organisationnelles (UO) et aux groupes d'utilisateurs ainsi qu'au nœud « .Enregistré automatiquement » situé sous le répertoire racine.

Dans **Utilisateurs et ordinateurs**, vous pouvez changer les droits d'accès d'un autre responsable de la sécurité si vous avez l'accès complet pour le conteneur approprié et êtes responsable du responsable de la sécurité en question. Vous ne pouvez pas changer vos propres droits d'accès. Si vous assignez un responsable de la sécurité à un objet de répertoire pour la première fois, le responsable de la sécurité hérite de vos droits d'accès pour ce conteneur.

Remarque : Vous ne pouvez pas accorder à d'autres responsables de la sécurité des droits d'accès plus élevés que vos propres droits d'accès.

Condition préalable: si vous voulez accorder/refuser au responsable de la sécurité le droit d'accéder aux objets de répertoire et de les gérer, vous devez posséder les droits « utilisateurs et ordinateurs », « d'affichage des droits d'accès des responsables de la sécurité » et « d'autoriser/de refuser l'accès au répertoire ». En plus, vous avez besoin des droits d'**Accès complet** pour les objets de répertoire en question.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, sélectionnez les objets de répertoire requis. L'arborescence n'affiche que les objets de répertoire pour lesquels vous avez les droits d'accès. Si vous avez des droits d'**Accès complet**, l'objet apparaît en noir. Les objets avec un accès en **Lecture seule** apparaissent en bleu. Un nœud grisé n'est pas accessible mais apparaît quand même, s'il existe des nœuds au-dessous auxquels vous avez accès.
3. Dans la zone d'action de droite, cliquez sur l'onglet **Accès**.
4. Pour assigner les droits pour les objets sélectionnés, faites glisser le responsable requis depuis l'extrémité droite dans le tableau **Accès**.
5. Dans la colonne **Droits d'accès**, sélectionnez les droits que vous voulez accorder au responsable de la sécurité pour les objets sélectionnés :
   - **Accès complet**
   - **Lecture seule**
   - **Refusé**

   Pour annuler l'assignation des droits pour les objets sélectionnés, faites glisser le responsable de la sécurité en retour dans le tableau **Responsables**.
6. Pour enregistrer les modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

Les objets sélectionnés sont disponibles pour le responsable de la sécurité correspondant.

Si deux responsables de la sécurité travaillent sur la même base de données SafeGuard Enterprise en même temps et si l'un d'entre eux change ses droits d'accès, un message apparaît pour informer l'autre responsable de la sécurité et tous les changements non enregistrés sont perdus. Si un

responsable de la sécurité perd complètement les droits d’accès pour un nœud, l’accès n’est plus accordé et un message approprié apparaît. La fenêtre de navigation est actualisée en conséquence.

3.8.9.11 Affichage des droits du responsable de la sécurité pour les objets du répertoire

Les droits d’accès assignés aux responsables de la sécurité pour les objets du répertoire sont affichés sur l’onglet **Accès** des objets correspondants dans **Utilisateurs et ordinateurs**.

L’onglet **Accès** n’affiche que les droits d’accès pour les conteneurs auxquels vous avez les droits d’accès. De la même façon, il n’affiche que les responsables de la sécurité dont vous êtes responsable.

L’onglet **Accès** affiche les informations suivantes :

- La colonne **Responsables** affiche les types et les noms des responsables de la sécurité qui ont été assignés aux objets du répertoire.
- La colonne **Assigné par** affiche la manière dont le responsable de la sécurité a reçu les droits d’accès :
- La **Date d’assignation**
- La colonne **Droits d’accès** affiche les droits accordés : **Accès complet**, **Refusé** ou en **Lecture seule**.
- La colonne **Origine** indique le nom complet du nœud où le droit d’accès a été assigné au responsable correspondant. Par exemple : Si le droit a été assigné à un nœud parent de l’objet de répertoire sélectionné, le nœud parent apparaît ici. Dans ce cas, le responsable de la sécurité a hérité du droit d’accès pour l’objet de répertoire sélectionné par l’assignation à son nœud parent.
- La colonne **État** affiche comment le responsable de la sécurité a reçu le droit d’accès :
    - **Hérité** (couleur bleue du texte) : Le droit d’accès a été hérité d’un nœud parent.
    - **Remplacé** (couleur marron du texte) : Le droit d’accès a été hérité d’un nœud parent, mais a changé au nœud sélectionné par assignation directe.
    - **Directement affecté** (couleur noire du texte) : Le droit d’accès a été assigné directement au nœud sélectionné.

  Pour les droits hérités, vous pouvez afficher une infobulle dans la colonne **État** indiquant l’origine du droit correspondant.

3.8.9.12 Promotion des responsables de la sécurité

Procédez comme suit :

- Élevez un utilisateur au grade de responsable de la sécurité dans la zone **Utilisateurs et ordinateurs**.

- Élevez un responsable de la sécurité au grade de responsable principal de la sécurité dans la zone **Responsables de la sécurité**.

Conditions préalables

Un responsable de la sécurité avec les droits nécessaires peut promouvoir des utilisateurs au rang de responsables de la sécurité et leur assigner des rôles.

Les responsables de la sécurité ainsi créés peuvent se connecter à SafeGuard Management Center avec leurs codes d'accès Windows ou leur code confidentiel de token/carte à puce. Ils peuvent travailler et être gérés comme tout autre responsable de la sécurité.

Les conditions préalables suivantes doivent être remplies :

- Les utilisateurs à promouvoir doivent avoir été importés depuis un Active Directory et être visibles dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center.

- Pour permettre à un utilisateur promu de se connecter à SafeGuard Management Center en tant que responsable de la sécurité, un certificat d'utilisateur est nécessaire. Vous pouvez créer ce certificat pour promouvoir l'utilisateur comme indiqué à la section Promotion d'un utilisateur au rang de responsable de la sécurité *(page 157)*. Pour rendre possible la connexion avec les codes d'accès Windows, le fichier.p12 contenant la clé privée doit se trouver dans la base de données SafeGuard Enterprise. Pour se connecter avec un code confidentiel de token ou de carte à puce, le fichier.p12 contenant la clé privée doit se trouver sur le token ou la carte à puce.

  Remarque :

  Si vous créez le certificat lors de la promotion d'un utilisateur, ce dernier va devoir utiliser le mot de passe du certificat pour se connecter à SafeGuard Management Center. Il va devoir saisir le mot de passe du certificat même s'il est invité à saisir le mot de passe Windows. Ceci s'applique également lors de la connexion à SafeGuard Enterprise Web Help Desk.

Promotion d'un utilisateur au rang de responsable de la sécurité

Condition préalable : Pour promouvoir un utilisateur, vous devez être responsable principal de la sécurité ou responsable de la sécurité avec les droits nécessaires.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Cliquez avec le bouton droit sur l'utilisateur que vous souhaitez promouvoir au rang de responsable de la sécurité et sélectionnez **Faire de cet utilisateur un responsable de la sécurité**.

3. L’étape suivante est différente selon qu’un certificat utilisateur est disponible ou non pour l’utilisateur sélectionné.

    - Si un certificat utilisateur a déjà été assigné à cet utilisateur, la boîte de dialogue **Sélection d’un ou des rôles** apparaît. Passez à l’étape 4.

    - Si aucun certificat utilisateur est disponible, un message apparaît vous demandant si une paire de clés à signature automatique doit être créée pour cet utilisateur. Cliquez sur **Oui** et saisissez et confirmez un mot de passe dans la boîte de dialogue **Mot de passe pour le nouveau certificat**. Maintenant, la boîte de dialogue **Sélection du ou des rôles** apparaît.

4. Dans la boîte de dialogue **Sélection du ou des rôles**, sélectionnez les rôles requis et cliquez sur **OK**.

L’utilisateur est désormais promu et apparaît dans la zone **Responsables de la sécurité** avec son nom d’utilisateur. Leurs propriétés peuvent être affichées en sélectionnant le responsable concerné dans la fenêtre de navigation. La clé privée de l’utilisateur est stockée dans la base de données et l’option **Aucun token** est activée. L’option **Facultatif** est activée si la clé privée de l’utilisateur est sur le token ou sur la carte à puce.

Si nécessaire, vous pouvez faire glisser le responsable de la sécurité à la position requise dans l’arborescence **Responsables de la sécurité**.

Le responsable de la sécurité peut se connecter à SafeGuard Management Center avec le nom affiché.

Promotion d’un responsable de la sécurité au rang de responsable principal de la sécurité

Condition préalable : pour promouvoir un responsable de la sécurité, vous devez posséder le droit d’affichage et de modification de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable de la sécurité à promouvoir et sélectionnez **Promouvoir au rang de responsable principal de la sécurité**.
3. Si le responsable promu possède des enfants, vous êtes invité à sélectionner un nouveau nœud parent pour les enfants.

Le responsable de la sécurité a été promu et apparaît sous le nœud **Responsables principaux de la sécurité**. En tant que responsable principal de la sécurité, le responsable promu recevra tous les droits sur l’ensemble des objets. Par conséquent, il perdra tous les droits assignés ainsi que l’accès au domaine autorisé de manière individuelle dans **Utilisateur et ordinateurs**.

3.8.9.13 Rétrogradation de responsables principaux de la sécurité

Condition préalable : Pour rétrograder des responsables principaux de la sécurité au rang de responsable de la sécurité, vous devez être responsable principal de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur le responsable principal de la sécurité que vous voulez rétrograder et sélectionnez **Rétrograder au rang de responsable de la sécurité**.
3. Vous êtes invité à sélectionner un nœud parent pour le responsable et à assigner au moins un rôle.

Le responsable de la sécurité a été rétrogradé et s'affiche sous le nœud **Responsables de la sécurité** sélectionné. Le responsable ainsi rétrogradé perd tous ses droits sur l'ensemble des objets et ne reçoit que ceux assignés à son ou ses rôles. Un responsable rétrogradé ne possède aucun droit sur les domaines. Vous devez accorder individuellement des droits d'accès dans la zone **Utilisateurs et ordinateurs**, sous l'onglet **Accès**.

3.8.9.14 Modification du certificat du responsable de la sécurité

Condition préalable : pour modifier le certificat d'un responsable de la sécurité ou d'un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de modification des responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez sur le responsable de la sécurité dont vous souhaitez modifier le certificat. Le certificat actuellement assigné apparaît dans la zone d'action de droite, dans le champ **Certificats**.
3. Dans la zone d'action, cliquez sur la liste déroulante **Certificats** et sélectionnez un certificat différent.
4. Pour enregistrer les modifications apportées à la base de données, cliquez sur l'icône **Enregistrer** de la barre d'outils.

3.8.9.15 Organisation des responsables de la sécurité dans l'arborescence

Vous pouvez organiser les responsables de la sécurité de manière hiérarchique dans la fenêtre de navigation **Responsables de la sécurité** et ce, afin de représenter la structure organisationnelle de votre société.

L'arborescence peut être organisée pour l'ensemble des responsables de la sécurité, à l'exception des responsables principaux de la sécurité. Les responsables principaux de la sécurité sont affichés dans une liste à un niveau, sous le nœud Responsable principal de la sécurité (MSO). Le nœud des

responsables de la sécurité comporte une arborescence dans laquelle chaque nœud représente un responsable de la sécurité. Toutefois, cette hiérarchie ne tient pas compte des droits et des rôles.

Condition préalable : pour déplacer un responsable de la sécurité dans l'arborescence, vous devez posséder le droit d'affichage et de modification de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, faites glisser le responsable que vous souhaitez déplacer vers le nœud approprié.

Tous les enfants du responsable sélectionné seront également déplacés.

3.8.9.16 Basculement rapide de responsables de la sécurité

À titre pratique, vous pouvez redémarrer rapidement SafeGuard Management Center afin de vous connecter sous le nom d'un autre responsable.

1. Dans SafeGuard Management Center, sélectionnez **Fichier > Changer de responsable**. SafeGuard Management Center redémarre et la boîte de dialogue de connexion s'affiche.
2. Sélectionnez le responsable de la sécurité que vous souhaitez connecter à SafeGuard Management Center, puis saisissez son mot de passe. Si vous travaillez en mode mutualisé (Multi Tenancy), vous serez connecté selon la même configuration de base de données.

SafeGuard Management Center redémarre et la vue assignée au responsable connecté s'affiche.

3.8.9.17 Suppression d'un responsable de la sécurité

Condition préalable : pour supprimer un responsable de la sécurité ou un responsable principal de la sécurité, vous devez posséder le droit d'affichage et de suppression de responsables de la sécurité.

1. Dans SafeGuard Management Center, sélectionnez **Responsables de la sécurité**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit sur le responsable de la sécurité ou le responsable principal de la sécurité à supprimer et sélectionnez **Supprimer**. Vous ne pouvez pas supprimer le responsable de la sécurité sous le nom duquel vous êtes connecté.
3. Si le responsable possède des enfants, vous êtes invité à sélectionner un nouveau nœud parent pour les enfants.

Le responsable est supprimé de la base de données.

Remarque : Un responsable principal de la sécurité explicitement créé en tant que responsable et non seulement promu au rang de responsable de la sécurité doit cependant être conservé dans la base de données. Si un utilisateur promu au rang de responsable de la sécurité est supprimé de la base de données, son compte utilisateur l'est également.

Remarque : Si le responsable à supprimer s'est vu assigner un rôle incluant une authentification supplémentaire et si le responsable est le seul à qui ce rôle a été assigné, le responsable sera tout de même supprimé. Nous considérons que le responsable principal de la sécurité sera en mesure de prendre le contrôle de l'autorisation supplémentaire.

3.8.10 Gestion de la structure organisationnelle

La structure organisationnelle peut être reproduite dans SafeGuard Management Center de deux façons :

- Vous pouvez importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise, par exemple par l'intermédiaire d'Active Directory.
- Vous pouvez créer manuellement votre structure organisationnelle en créant des groupes de travail et des domaines ainsi qu'une structure pour la gestion des éléments de la stratégie.

3.8.10.1 Importation à partir d'Active Directory

Vous pouvez importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise à l'aide d'Active Directory.

Remarque : La première importation est déclenchée par l'Assistant de configuration de SafeGuard Management Center. Lorsque vous exécutez l'assistant, vous pouvez ignorer cette étape et configurer manuellement l'importation d'Active Directory ultérieurement.

Nous vous conseillons de créer un compte de service Windows dédié qui sera utilisé pour toutes les tâches d'importation et de synchronisation. Retrouvez plus de renseignements dans l'article 107979 de la base de connaissances de Sophos.

Avec le Planificateur de tâches SafeGuard Management, vous pouvez créer des tâches périodiques pour la synchronisation automatique entre Active Directory et SafeGuard Enterprise. Votre produit livré contient à cet effet un modèle de script prédéfini. Pour plus d'informations, reportez-vous aux sections Planification des tâches *(page 214)* et Scripts prédéfinis pour les tâches périodiques *(page 222)*.

Remarque : Nous vous conseillons de diviser en plusieurs opérations l'importation de plus de 400 000 objets depuis AD. Il se peut que l'opération ne soit pas possible s'il y a plus de 400 000 objets dans une seule unité organisationnelle.

Droits d’accès du responsable de la sécurité et importation Active Directory

Assurez-vous d’avoir les droits d’accès adéquats lorsque vous importez la structure organisationnelle. Les informations suivantes vous indiquent quels sont les conditions requises pour les droits d’accès.

- Si vous ajoutez une connexion Active Directory à un domaine déjà existant, les conditions suivantes s’appliquent :
  - Si vous avez les droits d’**Accès complet** pour le domaine (DNS), les codes d’accès de connexion au répertoire sont mises à jour.
  - Si vous avez des droits **Lecture seule** ou moins pour le domaine (DNS), les codes d’accès ne sont pas mis à jour, mais vous pouvez utiliser des codes d’accès existants à des fins de synchronisation.
- Pour l’importation et la synchronisation d’Active Directory, les droits d’accès à un conteneur ou à un domaine s’étendent à l’arborescence du domaine que vous importez ou synchroniser. Si vous n’avez pas les droits **Accès complet** pour une arborescence secondaire, il ne peut pas être synchronisé. Si une sous-arborescence ne peut pas être modifiée, elle n’apparaît pas dans l’arborescence de synchronisation.
- Quels que soient les droits d’accès aux objets du répertoire de votre responsable de la sécurité, vous pouvez importer un nouveau domaine à partir d’Active Directory, s’il n’existe pas encore dans la base de données SafeGuard Enterprise. Des droits d’**Accès complet** au nouveau domaine seront accordés automatiquement à vous et à votre responsable de la sécurité.
- Si vous sélectionnez un sous-conteneur pour la synchronisation, celle-ci doit être effectuée jusqu’à la racine. Dans l’arborescence de synchronisation, tous les conteneurs correspondants sont sélectionnés automatiquement, même s’il y a des conteneurs au-dessus du sous-conteneur qui sont en **Lecture seule** ou **Refusés** en fonction de vos droits d’accès. Si vous dessélectionnez un sous-conteneur, vous allez également devoir, en fonction de vos droits d’accès, dessélectionner les conteneurs jusqu’à la racine.

  Si un groupe avec un accès en **Lecture seule** ou **Refusé** est inclus au processus de synchronisation :
  - Les membres du groupe ne sont pas mis à jour.
  - Si le groupe a été supprimé dans Active Directory, il ne sera pas supprimé de la base de données SafeGuard Enterprise.
  - Si le groupe a été déplacé dans Active Directory, il sera déplacé dans la structure SafeGuard Enterprise. Le groupe sera déplacé dans un conteneur sur lequel vous n’avez pas les droits d’**Accès complet**.

  Si un conteneur avec un accès en **Lecture seule** ou **Refusé** est inclus à la synchronisation parce qu’il se trouve à la racine et s’il contient un groupe avec **Accès complet**, ce groupe sera synchronisé. Les groupes avec un accès en **Lecture seule** ou **Refusé** ne le seront pas.

Importation d’une structure Active Directory

SafeGuard Enterprise vous permet d'importer une structure Active Directory dans SafeGuard Management Center. La première importation est déclenchée par l’Assistant de configuration de SafeGuard Management Center comme indiqué à la section Définition de l’authentification Active Directory *(page 42)*. Lors de la synchronisation avec Active Directory, les ordinateurs, les utilisateurs et les groupes sont importés dans SafeGuard Management Center. Toutes les données sont stockées dans la base de données SafeGuard.

Pour configurer Active Directory, procédez comme suit :

1. Ouvrez SafeGuard Management Center.
2. Authentifiez-vous à l'aide du mot de passe défini dans le magasin de certificats.
3. Dans le volet inférieur gauche, sélectionnez **Utilisateurs et ordinateurs**.
4. Dans la fenêtre supérieure gauche, sélectionnez **Racine [Filtre actif]**.
5. Dans le volet de droite, sélectionnez l'onglet **Synchronisation**. L'assistant **Authentification LDAP** démarre automatiquement.
6. Dans l'assistant **Authentification LDAP**, saisissez les codes d'accès de connexion que vous voulez utiliser pour la synchronisation et indiquez le nom du serveur ou l'adresse IP du contrôleur de domaine. Le nom d'utilisateur doit être au format Utilisateur@Domaine pour éviter tout problème de résolution du nom de domaine NetBIOS.
7. Dès que la connexion au répertoire est établie, le champ **DSN de répertoire** affiche les informations sur le domaine. Cliquez sur le symbole en forme de loupe afin de lire Active Directory.
8. Lorsque le processus de lecture est terminé, la structure du domaine s'affiche dans le volet central. Sélectionnez les unités organisationnelles que vous voulez importer dans SafeGuard Enterprise. Il n'est pas possible de sélectionner des machines, des groupes ou des objets d'utilisateur individuellement. Toutefois, il est possible de sélectionner les unités organisationnelles.
9. Décidez si les membres du groupe Active Directory doivent être synchronisés par SafeGuard Management Center. L'importation des membres du groupe peut être évitée en désélectionnant la case **Synchroniser l'appartenance**. Ne pas importer, ni synchroniser les membres du groupe a un effet positif sur les performances de SafeGuard Management Center (particulièrement sur les structures AD de grande taille).
   Par défaut, SafeGuard Enterprise crée une clé pour chaque conteneur, unité organisationnelle (UO) et objet de domaine importé. La création des clés est une procédure assez longue à effectuer. Par conséquent, et tout particulièrement lors de l'importation d'environnements de

grande taille, nous vous conseillons de ne pas activer la création de clés pour les groupes si ceci n'est pas nécessaire.

10. Démarrez la synchronisation en cliquant sur **Synchroniser**. Les informations détaillées issues d'Active Directory vont être lues. À la fin de la synchronisation, un résumé de toutes les modifications est affiché.

11. Cliquez sur **OK** pour écrire toutes les modifications dans la base de données SafeGuard Enterprise.

Lorsque le processus est terminé, la structure du domaine s'affiche dans le volet de gauche. L'importation d'Active Directory dans SafeGuard Management Center est à présent terminée.

Synchronisation de la structure organisationnelle

Si des éléments ont été déplacés d’une sous-arborescence vers une autre dans Active Directory, les deux sous-arborescences doivent être synchronisées avec la base de données SQL. La synchronisation d’une seule sous-arborescence aboutit à la suppression d’objets au lieu de leur déplacement.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.

2. Dans la fenêtre de navigation de gauche, cliquez sur le répertoire racine **Racine [Filtre actif]**.

3. Dans la zone d’action de droite, sélectionnez l’onglet **Synchroniser**.

4. Sélectionnez le répertoire requis dans la liste **DSN répertoire** et cliquez sur l’icône de la loupe (en haut à droite).

   Une représentation graphique de la structure Active Directory des unités organisationnelles de votre entreprise s’affiche.

5. Cochez les unités organisationnelles (OU) qui doivent être synchronisées. Il n’est pas nécessaire d’importer l’ensemble du contenu d’Active Directory.

6. Pour également synchroniser les appartenances, sélectionnez la case à cocher **Synchroniser l’appartenance**.

7. Pour également synchroniser l’état activé par l’utilisateur, sélectionnez la case à cocher **Synchroniser l’état activé par l’utilisateur**.

8. Lorsque vous synchronisez les comptes d’utilisateur désactivés à partir d’Active Directory, ils sont également désactivés dans SafeGuard Enterprise. Pour des raisons de sécurité, la réactivation du compte dans Active Directory et sa synchronisation n’entraîne pas l’activation automatique du compte d’utilisateur dans SafeGuard Enterprise. Pour synchroniser ces comptes, vous devez activer l’option **Synchroniser l’état activé par l’utilisateur**.

9. Au bas de la zone d’action, cliquez sur **Synchroniser**.

   Lors de la synchronisation d’utilisateurs avec leur appartenance à un groupe, l’appartenance à un « groupe principal » n’est pas synchronisée car elle n’est pas visible pour le groupe.

Les domaines sont synchronisés. Des informations sur la synchronisation s’affichent. Cliquez sur le message qui s’affichent dans la barre d’état en dessous à gauche des boutons pour voir un protocole de synchronisation. Cliquez sur le protocole, pour le copier dans le Presse-papiers et le coller dans un e-mail ou un fichier.

Remarque : Pendant la synchronisation Active Directory, les utilisateurs ne sont pas automatiquement enregistrés dans SafeGuard Enterprise. Les utilisateurs qui s’enregistrent au cours de la synchronisation doivent redémarrer leur ordinateur après avoir effectué la synchronisation pour pouvoir se connecter à SafeGuard Enterprise. Retrouvez plus de renseignements à la section Enregistrement automatique d’un nouvel utilisateur *(page 167)*.

Importation d’un nouveau domaine à partir d’Active Directory

1. Dans la fenêtre de navigation de gauche, cliquez sur le répertoire racine **Racine [Filtre actif]**.
2. Sélectionnez **Fichier > Nouveau > Importer un domaine à partir d’Active Directory**..
3. Dans la zone d’action de droite, sélectionnez **Synchroniser**.
4. Sélectionnez le répertoire requis dans la liste **DSN répertoire** et cliquez sur l’icône de la loupe (en haut à droite).

   Une représentation graphique de la structure Active Directory des unités organisationnelles de votre entreprise s’affiche.

5. Cochez le domaine à synchroniser et cliquez sur **Synchroniser** au bas de la zone de navigation.

Remarque : Si des éléments ont été déplacés d’une sous-arborescence vers une autre dans Active Directory, les deux sous-arborescences doivent être synchronisées avec la base de données SQL. La synchronisation d’une seule sous-arborescence aboutit à la suppression d’objets au lieu de leur déplacement.

Remarque : La synchronisation AD ne synchronise pas le nom avant Windows 2000 (NetBIOS) du domaine, si le contrôleur de domaine est configuré avec une adresse IP. Configurez le contrôleur de domaine pour utiliser le nom de serveur (NetBIOS ou DNS) à la place. Le client (sur lequel la synchronisation AD fonctionne) doit soit faire partie du domaine, soit pouvoir résoudre le nom DNS vers le contrôleur de domaine cible.

Importation des utilisateurs et des ordinateurs à partir d'Active Directory sur le conteneur

Si vous avez déjà une structure organisationnelle dans SafeGuard Management Center et si vous avez le droit d'importer des objets du répertoire, vous pouvez importer les utilisateurs et les ordinateurs à partir d'Active Directory sur le conteneur. Seuls les utilisateurs ou ordinateurs nouvellement créés ou déplacés dans le conteneur sélectionné ou ses sous-conteneurs seront synchronisés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur le conteneur dans lequel se trouvent les utilisateurs et les ordinateurs à synchroniser.
3. Dans le menu contextuel, cliquez sur **Nouveau** puis sur **Importer les utilisateurs et les ordinateurs à partir d'Active Directory**.

   La boîte de dialogue **Importation des utilisateurs et des ordinateurs à partir d'Active Directory** s'affiche et le processus d'importation commence.

   Le résultat de la l'importation sera répertorié. Le Nom, le nom de connexion et l'état des utilisateurs et ordinateurs importés sont affichés. L'**État** peut être **Importé** ou **Déplacé**.
4. Cliquez sur **Fermer**.

Les utilisateurs et ordinateurs sont affichés dans la fenêtre de navigation de gauche.

Recherche et importation des utilisateurs et ordinateurs

Pour effectuer ces tâches, vous devez avoir le droit de créer des objets du répertoire.

Si vous avez déjà une structure organisationnelle dans SafeGuard Management Center, vous pouvez rechercher les utilisateurs et les ordinateurs Active Directory et les importer directement dans la structure organisationnelle.

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation **Utilisateurs et ordinateurs**, cliquez sur le répertoire racine **Racine [Filtre actif]**.
3. Dans la barre de menus de SafeGuard Management Center, cliquez sur **Édition > Rechercher**.

   La boîte de dialogue **Rechercher des utilisateurs, ordinateurs et groupes** s'affiche.
4. Sélectionnez l'onglet **Active Directory**.

5. Sélectionnez le filtre requis dans la liste déroulante **Rechercher**.
6. Dans la liste déroulante **Dans**, sélectionnez le domaine dans lequel vous souhaitez effectuer la recherche.
7. Si vous recherchez un utilisateur ou un ordinateur spécifique, indiquez le nom recherché dans le champ **Rechercher le nom**.
8. Cliquez sur **Rechercher maintenant**.
   Le résultat de la recherche apparaît sur l'onglet **Active Directory**. Tous les nouveaux objets ont une case à cocher sur la gauche.
9. Sélectionnez les objets que vous voulez importer.
10. Cliquez sur **Importer la sélection**.
    Les objets sont importés et affichés dans la fenêtre de navigation de gauche.
11. Cliquez sur **Fermer**.

3.8.10.2 Création des groupes de travail et des domaines

Les responsables de la sécurité avec les droits nécessaires peuvent créer manuellement des groupes de travail ou des domaines avec une structure de gestion des éléments de la stratégie. Il est également possible d'attribuer des stratégies et/ou des stratégies de chiffrement aux utilisateurs locaux.

Veuillez créer un nouveau domaine uniquement si vous ne voulez pas ou ne pouvez pas importer un domaine à partir d'Active Directory (AD) (par exemple, parce qu'aucun AD n'est disponible).

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

Enregistrement automatique d'un nouvel utilisateur

Lorsqu'un nouvel utilisateur se connecte à SafeGuard Enterprise dès que son ordinateur a contacté le serveur SafeGuard Enterprise, il est enregistré et apparaît automatiquement dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center sous son domaine ou groupe de travail respectif.

Le répertoire de ces utilisateurs/ordinateurs (`.Enregistré automatiquement`) est créé automatiquement sous le répertoire racine et sous chaque domaine ou groupe de travail. Il ne peut être ni renommé ni déplacé. Les objets de ce répertoire ne peuvent pas non plus être déplacés manuellement.

Tant qu'il n'y a pas de domaine ou de groupe de travail, les objets restent dans le répertoire `.Enregistré automatiquement`. Lorsque le domaine ou le groupe de travail est synchronisé avec le contact suivant dans la base de données SafeGuard Enterprise, l'objet est déplacé vers

le domaine ou groupe de travail respectif. Autrement, il reste sous le répertoire **.Enregistré automatiquement**.

Généralement, seul le responsable principal de la sécurité peut gérer les objets enregistrés automatiquement.

Pour donner aux responsables de la sécurité le droit de gérer les objets dans le répertoire `.Enregistré automatiquement`, par exemple, pour la récupération d'un ordinateur dans ce groupe, vous devez créer manuellement le domaine ou le groupe de travail auquel cet objet appartient. Vous pouvez ensuite assigner les droits aux responsables de la sécurité pour ces domaines ou groupes de travail. Les objets seront ensuite déplacés automatiquement dans leur domaine.

Les utilisateurs locaux ne peuvent pas se connecter à SafeGuard Enterprise avec un mot de passe vide. Les utilisateurs locaux qui se connectent à SafeGuard Enterprise avec un mot de passe vide restent des invités et ne sont pas enregistrés dans la base de données. Si l'ouverture de session automatique Windows est activée pour ces utilisateurs, la connexion est refusée. Pour se connecter à SafeGuard Enterprise, un nouveau mot de passe doit être créé et l'ouverture de session automatique Windows doit être désactivée dans le registre du terminal.

Les comptes Microsoft sont toujours considérés comme des utilisateurs invités de SafeGuard Enterprise.

Remarque : Pendant la synchronisation Active Directory, les utilisateurs ne sont pas automatiquement enregistrés dans SafeGuard Enterprise. Les utilisateurs qui s'enregistrent au cours de la synchronisation doivent redémarrer leur ordinateur après avoir effectué la synchronisation pour pouvoir se connecter à SafeGuard Enterprise.

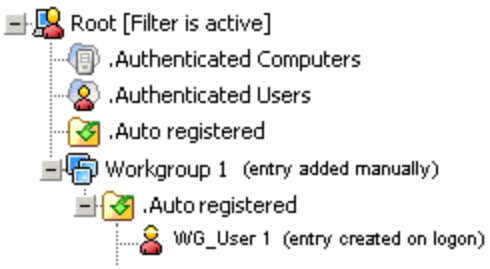
Exemples d'enregistrement automatique

Vous trouverez ci-après deux exemples de comportement d'objets enregistrés automatiquement.

Utilisateurs ou ordinateurs ne faisant pas partie d'Active Directory

Dans une entreprise, tous les objets utilisateur ou ordinateur ne font pas nécessairement partie d'Active Directory (AD), les utilisateurs locaux par exemple. Une entreprise peut disposer d'un ou de plusieurs groupes de travail, un AD n'est donc pas nécessaire.

Cette entreprise souhaite déployer SafeGuard Enterprise, puis ajouter des stratégies à ses objets utilisateur ou ordinateur. La structure organisationnelle de l'entreprise est créée manuellement dans SafeGuard Management Center de la manière suivante :



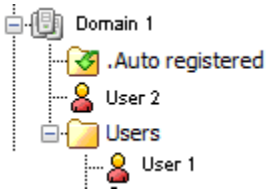
Les objets restent dans le dossier .Enregistré automatiquement. Ils peuvent être gérés correctement à l'aide de SafeGuard Management Center en appliquant des stratégies sur le dossier .Enregistré automatiquement.

Base de données de SafeGuard Enterprise et Active Directory non synchronisés

Un utilisateur fait déjà partie d'un Active Directory (AD) d'entreprise. La base de données de SafeGuard Enterprise et AD ne sont cependant pas synchronisés. L'**Utilisateur 1** se connecte à SafeGuard Enterprise et il apparaît automatiquement dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center sous le domaine fourni avec la connexion (**Domaine 1**).

L'utilisateur fait désormais partie du dossier .Enregistré automatiquement. L'objet peut être géré correctement à l'aide de SafeGuard Management Center en appliquant des stratégies sur le dossier .Enregistré automatiquement.

À la prochaine synchronisation entre AD et la base de données SafeGuard Enterprise, l'**Utilisateur 1** sera automatiquement déplacé dans son unité organisationnelle (**Utilisateurs**).



Pour activer les stratégies pour l'**Utilisateur 1**, celles-ci doivent désormais être assignées à l'unité organisationnelle **Utilisateurs**.

Clés et certificats pour les objets enregistrés automatiquement

Pour chaque objet enregistré automatiquement, un certificat est généré en fonction des besoins par le serveur.

Un utilisateur local obtient deux clés :

- la clé du conteneur .Enregistré automatiquement
- la clé privée générée en fonction des besoins par le serveur

Les utilisateurs locaux n’obtiennent aucune autre clé pour leur conteneur assigné ni de clé racine.

Les groupes de travail n’obtiennent pas de clé.

Stratégies pour les objets enregistrés automatiquement

Pour les objets enregistrés automatiquement, les stratégies peuvent être créées sans aucune restriction.

Les utilisateurs locaux sont ajoutés au groupe « Utilisateurs authentifiés ». Les ordinateurs sont ajoutés au groupe « Ordinateurs authentifiés ». Les stratégies activées pour ces groupes s’appliquent en conséquence.

Création de groupes de travail

Les responsables de la sécurité disposant des droits requis peuvent créer un conteneur sous le répertoire racine qui représente un groupe de travail Windows. Les groupes de travail n’ont pas de clé. Ils ne peuvent pas être renommés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur **Racine [Filtre actif]** et sélectionnez **Nouveau > Créer un nouveau groupe de travail (enregistrement auto)**.
3. Sous **Informations communes**, procédez comme suit :
    a. Saisissez un **Nom complet** pour le groupe de travail.
    b. Vous pouvez éventuellement ajouter une **description**.
    c. Le type d’objet est affiché dans le champ **État de connexion**, dans ce cas **Groupe de travail**.
    d. Pour empêcher l’héritage de stratégie, vous pouvez sélectionner **Bloquer l’héritage de stratégie**.
    e. Cliquez sur **OK**.

Le groupe de travail est créé. Le répertoire **.Enregistré automatiquement** par défaut est créé automatiquement sous le conteneur du groupe de travail. Il ne peut être ni renommé ni supprimé.

Suppression de groupes de travail

Pour supprimer des groupes de travail, vous avez besoin des droits d'**Accès complet** pour le groupe de travail concerné. Les membres appartenant au groupe de travail sont également supprimés. Ils sont réenregistrés automatiquement lors de la prochaine connexion.

Pour supprimer un groupe de travail, vous avez besoin des droits d'**Accès complet** pour tous les objets concernés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur le groupe de travail que vous voulez supprimer et sélectionnez **Supprimer**.
3. Pour confirmer, cliquez sur **Oui**.

Le groupe de travail est supprimé. Ses membres éventuels sont également supprimés.

Remarque : Si vous n'avez pas les droits d'**Accès complet** pour tous les membres du groupe de travail, la suppression du groupe de travail échoue et un message d'erreur apparaît.

Création d'un domaine

Les responsables de la sécurité disposant des droits requis peuvent créer un domaine sous le répertoire racine. Veuillez créer un nouveau domaine uniquement si vous ne voulez pas ou ne pouvez pas importer un domaine à partir d'Active Directory (AD) (par exemple, parce qu'aucun AD n'est disponible).

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur **Racine [Filtre actif]** et sélectionnez**Nouveau > Créer un domaine (enregistrement auto)**.
3. Sous **Informations communes**, saisissez les informations suivantes concernant le contrôleur de domaine.

   Les deux entrées de noms doivent être correctes. Faute de quoi le domaine n'est pas synchronisé.

   a. **Nom complet :** par exemple *nom ordinateur.domaine.fr* ou l'adresse IP du contrôleur de domaine
   b. **Nom distinctif** (lecture seule) : Nom DNS, par exemple DC=nomordinateur3,DC=domaine,DC=pays
   c. Une description de domaine (facultatif)
   d. **Nom Netbios** : nom du contrôleur de domaine
   e. Le type d'objet est affiché sous **État de connexion**, dans ce cas **Domaine**.
   f. Pour empêcher l'héritage de stratégie, vous pouvez sélectionner **Bloquer l'héritage de stratégie**.

g. Cliquez sur **OK**.

Le nouveau domaine est créé. Les utilisateurs et/ou ordinateurs sont automatiquement assignés à ce domaine au cours de l'enregistrement automatique. Le répertoire par défaut **.Enregistré automatiquement** est créé automatiquement sous le conteneur du domaine. Il ne peut être ni renommé ni supprimé.

Changement de nom d'un domaine

Les responsables de la sécurité disposant des droits requis peuvent renommer un domaine et définir des propriétés supplémentaires. Vous avez besoin des droits d'**Accès complet** pour le domaine correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit de la souris sur le domaine à renommer puis sélectionnez **Propriétés**.
3. Dans **Informations communes**, sous **Nom complet**, changez le nom du domaine et sa description.
4. Vous pouvez changer le nom du contrôleur de domaine dans **Nom NetBios**.
5. Vous pouvez également définir le mode Éveil par appel réseau pour le redémarrage automatique dans l'onglet **Paramètres de conteneur**.
6. Pour confirmer, cliquez sur **OK**.

À présent, les modifications sont enregistrées.

Suppression d'un domaine

Les responsables de la sécurité dotés des droits requis peuvent supprimer des domaines. Pour supprimer un domaine, vous avez besoin des droits d'**Accès complet** pour le domaine concerné. Les membres appartenant au domaine sont également supprimés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation de gauche, cliquez avec le bouton droit sur le domaine à supprimer puis sélectionnez **Supprimer**.
3. Cliquez sur **Oui**.

Le domaine est supprimé. Ses membres éventuels sont également supprimés.

Si vous avez moins que les droits d'**Accès complet** pour tous les membres du domaine, la suppression du domaine échoue et un message d'erreur apparaît.

Suppression des ordinateurs enregistrés automatiquement

Lorsqu'un ordinateur enregistré automatiquement est supprimé, tous les utilisateurs locaux de cet ordinateur le sont également. Ils seront réenregistrés automatiquement à leur prochaine connexion à cet ordinateur.

Affichage et recherche des utilisateurs locaux

Dans **Utilisateurs et ordinateurs**, vous pouvez filtrer la vue dans la zone de navigation à gauche en fonction des utilisateurs locaux ou rechercher des utilisateurs locaux donnés.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la partie inférieure gauche de la fenêtre de navigation, cliquez sur **Filtrer**.
3. Sélectionnez **Utilisateur local** en tant que **Type**. Si vous recherchez un utilisateur particulier, saisissez son nom.
4. Cliquez sur l'icône de la loupe.

La vue **Utilisateurs et ordinateurs** est filtrée en fonction des critères.

Les comptes Microsoft sont toujours considérés comme des utilisateurs invités de SafeGuard Enterprise.

3.8.11 Clés et certificats

Lors de l'importation de la structure du répertoire, SafeGuard Enterprise dans sa configuration par défaut génère automatiquement des clés pour :

- Domaines
- Conteneurs/OU

et les assigne aux objets correspondants. Des clés d'ordinateur et d'utilisateur sont générées selon les besoins.

Clés pour les groupes

Dans a configuration par défaut, SafeGuard Enterprise ne génère pas automatiquement de clés pour les groupes. Ce comportement est désactivé par défaut. En tant que responsable de la sécurité, vous pouvez changer ce comportement sur l'onglet **Clés** en sélectionnant **Outils > Options**. Si **Groupes** est coché sur l'onglet **Clés**, SafeGuard Enterprise génère automatiquement des clés de groupe, lorsque la base de données est synchronisée. En bas de l'onglet **Synchronisation**, il est indiqué pour quels éléments des clés sont générées lors de la synchronisation.

Les clés ne peuvent pas être supprimées. Elles sont conservées en permanence dans la base de données de SafeGuard Enterprise.

Lorsqu'un terminal est démarré pour la première fois, SafeGuard Enterprise lui génère une clé d'ordinateur (clé machine définie).

La clé machine définie est uniquement générée lorsque le chiffrement de volume est installé sur le terminal.

Chaque utilisateur obtient toutes ses clés lors de la connexion à partir de son jeu de clés. Le jeu de clés utilisateur comporte les éléments suivants :

- Les clés des groupes auxquels appartient l'utilisateur ;
- Les clés des conteneurs/OU globaux des groupes auxquels appartient l'utilisateur.

Les clés du jeu de clés de l'utilisateur déterminent les données auxquelles l'utilisateur peut accéder. L'utilisateur peut uniquement accéder aux données pour lesquelles il possède une clé spécifique.

Pour éviter que trop de clés de groupes non utilisées apparaissent dans le jeu de clés de l'utilisateur, vous pouvez indiquer les clés à masquer. Retrouvez plus de renseignements à la section Masquage des clés *(page 177)*.

Pour afficher toutes les clés d'un utilisateur, cliquez sur **Utilisateurs et ordinateurs** et sélectionnez l'onglet **Clés**.

Pour afficher toutes les clés, cliquez sur **Clés et certificats** dans SafeGuard Management Center et sélectionnez **Clés**. Vous pouvez générer des listes de **Clés assignées** et de **Clés inactives**.

La liste **Certificats assignés** indique seulement les clés assignées aux objets pour lesquels vous avez des droits en **Lecture seule** ou d'**Accès complet**. La vue **Clés** indique le nombre de clés disponibles, quels que soient vos droits d'accès. La liste **Clés assignées** indique le nombre de clés visibles en fonction de vos droits d'accès.

1. Cliquez sur **Utilisateurs et ordinateurs** pour ouvrir l'affichage.

2. Les clés d'un objet sélectionné sont affichées dans la zone action et dans les vues respectives.

3. L'affichage dans la zone d'action dépend des sélections dans la zone de navigation. Toutes les clés assignées à l'objet sélectionné sont affichées.

4. Sous **Clés disponibles**, toutes les clés disponibles s'affichent. Les clés déjà assignées à l'objet sélectionné sont grisées. Sélectionnez **Filtre** pour basculer entre des clés déjà assignées à un objet (actives) et des clés non assignées à un objet (inactives).

Après l’importation, chaque utilisateur reçoit un certain nombre de clés utilisables pour le chiffrement des données.

3.8.11.1 Clés pour le chiffrement des données

Des clés sont assignées aux utilisateurs pour le chiffrement de volumes spécifiques lors de la définition de stratégies du type **Protection des périphériques**.

Dans une stratégie de type **Protection des périphériques**, vous pouvez spécifier le paramètre **Clé à utiliser pour le chiffrement** pour chaque support.

Ici, vous pouvez décider quelles sont les clés que l'utilisateur peut ou doit utiliser pour le chiffrement:

- **Toute clé du jeu de clés utilisateur**

  Après s'être connectés à Windows, les utilisateurs peuvent sélectionner les clés qu'ils souhaiteraient utiliser pour chiffrer un volume particulier. Une boîte de dialogue s'affiche pour permettre aux utilisateurs de sélectionner la clé de leur choix.

- **Toute clé du jeu de clés utilisateur sauf la clé utilisateur**

  Les utilisateurs ne sont pas autorisés à utiliser leurs clés personnelles pour chiffrer des données.

- **Toute clé de groupe du jeu de clés utilisateur**

  Les utilisateurs ne peuvent sélectionner qu'une des clés de groupe présentes dans leur jeu de clés.

- **Clé machine définie**

  C'est la clé unique générée exclusivement pour cet ordinateur par SafeGuard Enterprise lors du premier démarrage. L'utilisateur n'a pas d'autre option. Une clé machine définie est généralement utilisée par la partition d'initialisation et système et pour les unités sur lesquelles se trouve le répertoire Documents and Settings.

- **Clé définie dans la liste**

  Cette option permet de définir une clé particulière que l'utilisateur doit utiliser pour le chiffrement. Pour indiquer une clé d'utilisateur de cette manière, veuillez définir une clé sous **Clé définie pour le chiffrement**. Cette option s'affiche une fois que vous sélectionnez **Clé définie sur la liste**.

Cliquez sur le bouton **[...]** situé en regard de **Clé définie pour le chiffrement** pour afficher une boîte de dialogue dans laquelle vous pouvez spécifier une clé. Assurez-vous que l'utilisateur a aussi la clé correspondante.

Marquez la clé sélectionnée et cliquez sur **OK**. La clé sélectionnée sera utilisée pour le chiffrement sur l'ordinateur client.

Assignation de clés dans Utilisateurs et ordinateurs

Pour assigner des clés aux utilisateurs, vous avez besoin des droits d'**Accès complet** sur l'objet concerné.

Pour assigner une nouvelle clé aux utilisateurs :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'objet requis (par exemple, utilisateur, groupe ou conteneur).
3. Cliquez avec le bouton droit de la souris sur l'onglet **Clés** et sélectionnez **Assigner une nouvelle clé** dans le menu contextuel.
4. Dans la boîte de dialogue **Assignation d'une nouvelle clé** :
    a. Saisissez un **Nom symbolique** et une **Description** pour la clé.
    b. Pour masquer la clé dans le jeu de clés de l'utilisateur, sélectionnez la case à cocher **Masquer la clé**.
5. Cliquez sur **OK**.

La clé est assignée et affichée dans l'onglet **Clé**.

Annulation de l'assignation de clés dans Utilisateurs et ordinateurs

Assurez-vous de disposer du droit **Annuler l'assignation de clés**. Ceci fait partie du rôle de **Responsable de la sécurité** prédéfini.

Pour annuler l'assignation d'une **Clé personnelle**, vous devez également disposer du droit **Gérer des clés personnelles**. Par défaut, seul un responsable principal de la sécurité dispose de ce droit.

Pour annuler l'assignation d'une clé :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'objet requis (par exemple, utilisateur, groupe ou conteneur).
3. Sur l'onglet **Clé**, sélectionnez la clé.
4. Cliquez avec le bouton droit de la souris sur la clé et sélectionnez **Supprimer** dans le menu contextuel.
5. Dans la boîte de dialogue de confirmation, cliquez sur **Oui**.

6. Cliquez sur **OK**.

L’assignation de la clé est annulée. La clé est supprimée de l’onglet **Clé** et apparaît dans la liste **Clés disponibles**.

Masquage des clés

Pour éviter que trop de clés de groupes non utilisées apparaissent dans le jeu de clés d’un utilisateur sur le terminal, vous pouvez indiquer les clés à masquer. Les clés qui n’apparaissent pas dans le jeu de clés de l’utilisateur peuvent quand même être utilisées pour accéder aux fichiers chiffrés, mais pas pour en chiffrer des nouveaux.

Pour masquer les clés :

1. Dans SafeGuard Management Center, cliquez sur **Clés et certificats**.
2. Dans la zone de navigation, cliquez sur **Clés > Clés assignées**.

   La vue **Clés assignées** apparaît affichant la colonne **Masquer la clé**.

3. Il existe deux moyens de spécifier que les clés doivent être masquées :

   - Sélectionnez la case à cocher dans la colonne **Masquer la clé** de la clé requise.
   - Sélectionnez une ou plusieurs clés et cliquez avec le bouton droit de la souris pour ouvrir un menu contextuel.

     Sélectionnez **Masquer la clé à l’utilisateur**.

4. Enregistrez vos changements dans la base de données.

Les clés indiquées n’apparaissent pas dans le jeu de clés de l’utilisateur.

Retrouvez plus de renseignements sur l’affichage du jeu de clés de l’utilisateur sur le terminal dans le *Manuel d’utilisation de SafeGuard Enterprise*, au chapitre *Accès à SafeGuard Enterprise*.

Si une stratégie indique une clé masquée à utiliser pour le chiffrement, le paramètre **Masquer la clé** n’affecte pas le chiffrement sur le terminal.

3.8.11.2 Clés personnelles pour le chiffrement de fichiers par File Encryption

Une clé personnelle est un type particulier de chiffrement créé pour un utilisateur donné qui ne peut pas être partagé avec d’autres utilisateurs. Une clé personnelle qui est active pour un utilisateur

donné est appelée une clé personnelle active. Les clés personnelles actives ne peuvent pas être assignées à d'autres utilisateurs.

Dans les stratégies **Chiffrement de fichiers**, vous pouvez définir des règles de chiffrement qui utilisent l'espace réservé **Clé personnelle** au lieu d'un nom de clé. Pour de telles règles, la clé de chiffrement à utiliser est la clé personnelle active de l'utilisateur.

Lorsque vous définissez une règle de chiffrement pour que le chemin *C:\encrypt* soit chiffré avec la clé personnelle, des clés différentes sont utilisées pour différents utilisateurs. Vous pouvez ainsi vous assurer que les informations dans les dossiers spécifiques sont privées pour les utilisateurs. Retrouvez plus de renseignements à la section Chiffrement de fichiers par emplacement *(page 336)*.

Si une règle de chiffrement de fichiers définit une clé personnelle à utiliser pour le chiffrement, des clés personnelles sont créées automatiquement pour les utilisateurs correspondants, s'ils n'ont pas encore de clés personnelles actives.

En tant que responsable de la sécurité avec les droits requis, vous pouvez créer des clés personnelles pour des utilisateurs sélectionnés ou pour tous les utilisateurs de groupes sélectionnés dans SafeGuard Management Center. Vous pouvez aussi rétrograder des clés personnelles actives, par exemple lorsqu'un utilisateur quitte la société.

Création automatique de clés personnelles

Si une règle de chiffrement File Encryption définit une clé personnelle à utiliser pour le chiffrement et si l'utilisateur n'a pas encore de clé personnelle active, le serveur SafeGuard Enterprise la crée automatiquement. Lors du délai entre la réception de la stratégie sur le terminal et la mise à disposition de la clé personnelle active requise, l'utilisateur n'est pas autorisé à créer de nouveaux fichiers dans les dossiers couverts par la règle File Encryption.

Pour un déploiement initial des stratégies de **Chiffrement de fichiers** avec des règles de chiffrement à l'aide de clés personnelles sur un groupe plus important d'utilisateurs (des centaines ou plus) qui n'ont pas encore de clés personnelles actives, nous conseillons de créer les clés personnelles dans SafeGuard Management Center. Retrouvez plus de renseignements à la section Création de clés personnelles pour plusieurs utilisateurs *(page 179)*. La charge sur le serveur SafeGuard Enterprise sera réduite.

Création d'une clé personnelle pour un utilisateur unique

Pour créer une clé personnelle, vous avez besoin des droits **Créer des clés** et **Assigner des clés**. En plus, vous avez besoin des droits d'**Accès complet** pour l'objet en question. Pour remplacer une clé personnelle active, vous avez besoin du droit **Gérer les clés personnelles**.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'utilisateur requis.
3. Cliquez avec le bouton droit de la souris sur l'onglet **Clés** et sélectionnez **Assigner une nouvelle clé** dans le menu contextuel.
4. Dans la boîte de dialogue **Assignation d'une nouvelle clé** :

   a. Saisissez une description pour la clé personnelle.
   b. Pour cacher la clé personnelle dans le jeu de clés de l'utilisateur, sélectionnez **Masquer la clé**.
5. Selon que vous créez une clé personnelle pour un utilisateur qui n'a pas encore de clé personnelle active ou pour un utilisateur qui en a une, la boîte de dialogue **Assignation d'une nouvelle clé** affiche des cases à cocher différentes. Sélectionnez la case à cocher affichée, pour définir la clé nouvellement créée comme une clé personnelle :
   - **Clé personnelle** : cette case à cocher apparaît pour les utilisateurs qui n'ont pas encore de clé personnelle active.
   - **Remplacer la clé personnelle active** : cette case à cocher apparaît pour les utilisateurs qui ont déjà une clé personnelle active.
6. Cliquez sur **OK**.

La clé personnelle est créée pour l'utilisateur sélectionné. Dans l'onglet**Clé**, la clé apparaît comme la **Clé personnelle active** pour l'utilisateur. Pour un utilisateur qui avait déjà une clé personnelle active, la clé existante est rétrogradée et l'utilisateur en reçoit une nouvelle. La clé personnelle rétrogradée reste dans le jeu de clés de l'utilisateur. La clé personnelle active ne peut pas être assignée à d'autres utilisateurs.

Création de clés personnelles pour plusieurs utilisateurs

Pour créer des clés personnelles, vous avez besoin des droits **Créer des clés** et **Assigner des clés**. En plus, vous avez besoin des droits d'**Accès complet** pour les objets en question. Pour remplacer des clés personnelles actives existantes, vous avez besoin du droit **Gérer les clés personnelles**.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, cliquez avec le bouton droit de la souris sur le nœud pour lequel vous voulez créer des clés personnelles :
   - un nœud de domaine,
   - le nœud .Enregistré automatiquement à la racine ou dans les domaines ou
   - un nœud Unité Organisationnelle.
3. Dans le menu contextuel, sélectionnez **Créer des clés personnelles pour les utilisateurs**.
4. Dans la boîte de dialogue **Créer des clés personnelles pour les utilisateurs** :
   a. Saisissez une description pour les clés personnelles.
   b. Pour cacher les clés personnelles dans les jeux de clés des utilisateurs, sélectionnez **Masquer la clé**.
   c. Pour remplacer les clés personnelles actives existantes par les nouvelles, sélectionnez **Remplacer les clés personnelles actives existantes**.
5. Cliquez sur **OK**.

Les clés personnelles sont créées comme pour tous les utilisateurs du nœud sélectionné. Dans l'onglet**Clé**, les clés apparaissent comme des **Clés personnelles actives** pour les utilisateurs. Si les utilisateurs avaient déjà des clés personnelles actives et si vous avez sélectionné **Remplacer les clés personnelles actives existantes**, les clés existantes sont rétrogradées et les utilisateurs en reçoivent

des nouvelles. Les clés personnelles rétrogradées restent dans les jeux de clés des utilisateurs. Les clés personnelles actives individuelles ne peuvent pas être assignées à d'autres utilisateurs.

Rétrogradation des clés personnelles actives

Pour rétrograder manuellement des clés personnelles actives, vous avez besoin des droits **Modifier des clés** et **Gérer des clés personnelles**. Par défaut, le droit **Gérer des clés personnelles** a été assigné au rôle prédéfini de responsable principal de la sécurité, mais il peut aussi être assigné aux nouveaux rôles définis par l'utilisateur. En plus, vous avez besoin des droits d'**Accès complet** pour l'objet en question.

Vous pouvez rétrograder manuellement des clés personnelles actives, par exemple si un utilisateur quitte la société. Dans la mesure où vous avez le droit **Gérer des clés personnelles**, vous pouvez assigner la clé personnelle rétrogradée de cet utilisateur à d'autres utilisateurs pour leur donner un accès en lecture seule aux fichiers chiffrés avec cette clé. Mais ils ne peuvent pas utiliser cette clé pour le chiffrement des fichiers.

Ceci ne peut pas être annulé. Une clé personnelle rétrogradée ne peut jamais devenir une clé personnelle active quel que soit l'utilisateur.

1. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs**.
2. Dans la zone de navigation, sélectionnez l'utilisateur requis.
3. Dans l'onglet **Clé**, cliquez avec le bouton droit de la souris sur la **Clé personnelle active** requise et sélectionnez **Rétrograder la clé personnelle** dans le menu contextuel.

La clé est rétrogradée. C'est encore une clé personnelle, mais elle ne peut plus être utilisée comme clé personnelle active. Si une règle File Encryption définit une clé personnelle à utiliser pour le chiffrement et si l'utilisateur n'a pas encore de clé personnelle active, le serveur SafeGuard Enterprise la crée automatiquement.

3.8.11.3 Certificats

- Un seul certificat peut être affecté par utilisateur. Si ce certificat utilisateur est stocké sur un token, les utilisateurs peuvent donc utiliser ce token (token cryptographique - Kerberos) pour se connecter à leur terminal.

- Notez que lors de l'importation d'un certificat utilisateur, la section publique et la section privée de ce certificat sont importées toutes les deux. Si uniquement la partie publique est importée, seule l'authentification par token est prise en charge.

- La combinaison des certificats AC et de la CRL (Certificate Revocation List, liste de révocation des certificats) doit correspondre. Dans le cas contraire, les utilisateurs ne peuvent pas se connecter à leurs ordinateurs respectifs. Vérifiez que la combinaison est correcte. SafeGuard Enterprise n'effectue pas cette vérification.

- Si des certificats de l’autorité de certification (AC) sont supprimés dans la base de données et si vous ne souhaitez plus les utiliser, veuillez les supprimer manuellement du magasin local de tous les ordinateurs administrateurs.

  SafeGuard Enterprise peut ensuite uniquement communiquer avec les certificats ayant expiré si les clés nouvelles et anciennes sont présentes sur le même token.

- Les certificats de l’AC ne peuvent pas provenir d’un token et être stockés dans la base de données ou dans le magasin de certificats. Si vous utilisez des certificats de l’AC, ces derniers doivent être disponibles sous forme de fichiers et pas seulement sous forme de token. Ceci s’applique également aux CRL.

- Les certificats générés par SafeGuard Enterprise sont signés avec SHA-1 ou SHA-256 pour vérification. SHA-256 fournit une sécurité optimale et il est utilisé par défaut sur toutes les premières installations. Si la version 6 de SafeGuard Enterprise ou une version précédente doit tout de même être gérée ou si la mise à niveau a lieu à partir d’une version antérieure, l’algorithme SHA-1 est utilisé par défaut.

- Les certificats fournis par le client et importés dans SafeGuard Enterprise ne sont actuellement pas vérifiés conformément à RFC3280. Par exemple, nous n’empêchons pas l’utilisation de certificats de signature à des fins de chiffrement.

- Les certificats de connexion des responsables de la sécurité doivent se trouver dans le magasin de certificats «MY».

La liste **Certificats assignés** dans **Clés et certificats** indique seulement les certificats assignés aux objets pour lesquels vous avez des droits en **Lecture seule** ou d’**Accès complet**. La vue **Certificat** indique le nombre de certificats disponibles, quels que soient vos droits d’accès. La liste **Certificats assignés** indique le nombre de certificats disponibles en fonction de vos droits d’accès.

Pour modifier les certificats, vous avez besoin des droits d’**Accès complet** au conteneur dans lequel résident les utilisateurs.

Importation des certificats d’autorité de certification et des listes de révocation de certificats

Si des certificats AC (autorité de certification) sont utilisés, veuillez importer toute la hiérarchie AC, y compris toutes les listes de révocation des certificats dans la base de données SafeGuard. Les certificats AC ne peuvent pas être récupérés à partir de tokens. Ils doivent être mis à disposition sous la forme de fichier afin que vous puissiez les importer dans la base de données SafeGuard Enterprise. Ceci s’applique également aux listes de révocation de certificats.

1. Dans SafeGuard Management Center, cliquez sur **Clés et certificats**.

2. Sélectionnez **Certificats** et cliquez sur l'icône **Importer les certificats de l'AC** de la barre d'outils. Naviguez jusqu'aux fichiers du certificat AC que vous souhaitez importer.
   Les certificats importés s'affichent dans la zone d'action de droite.

3. Sélectionnez **Certificats** et cliquez sur l'icône **Importer la liste de révocation de certificats** de la barre d'outils. Naviguez jusqu'aux fichiers de la liste de révocation de certificats que vous souhaitez importer.
   Les listes de révocation de certificats importées s'affichent dans la zone d'action de droite.

4. Vérifiez que l'AC et la liste de révocation de certificats sont correctes. Les certificats de l'AC doivent correspondre à la liste de révocation de certificats pour que les utilisateurs puissent se connecter aux ordinateurs concernés. SafeGuard Enterprise n'effectue pas cette vérification.

Modification de l'algorithme pour les certificats autosignés

- tous les composants SafeGuard Enterprise doivent être à la version 6.1 ou supérieure.

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

Lors de la mise à niveau à partir de SafeGuard Enterprise 6 ou d'une version antérieure, l'algorithme **SHA-1** est automatiquement utilisé pour les certificats autosignés. Vous pouvez le modifier manuellement sur **SHA-256** pour une sécurité optimale suite à la mise à niveau.

Modifiez uniquement l'algorithme sur **SHA-256** si tous les composants et terminaux SafeGuard Enterprise ont été mis à niveau à la version en cours. **SHA-256** n'est pas pris en charge dans les environnements mixtes. Par exemple, les terminaux SafeGuard Enterprise 6 sont administrés par SafeGuard Management Center 7. Si vous avez un environnement mixte, vous devez effectuer cette tâche et ne pas modifier l'algorithme sur **SHA-256**.

La modification de l'algorithme pour les certificats autosignés s'effectue de la manière suivante :

- Modification de l'algorithme.
- Création d'un ordre de changement du certificat (CCO, Certificate Change Order).
- Création d'un package de configuration contenant le CCO.
- Redémarrage des serveurs (base de données) SafeGuard Enterprise.
- Distribution et déploiement des packages de configuration sur les terminaux.

Pour modifier l'algorithme pour les certificats autosignés :

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Options**.

2. Dans l'onglet **Général**, sous **Certificats**, sélectionnez l'algorithme nécessaire dans **Algorithme de hachage pour les certificats générés** et cliquez sur **OK**.

3. Dans l'onglet **Certificats**, sous **Demander**, cliquez sur **Mettre à jour**. Dans la boîte de dialogue **Mettre à jour le certificat d'entreprise**, saisissez un nom de CCO et indiquez un chemin de sauvegarde. Saisissez un mot de passe pour le fichier P12 et retapez-le. En option, saisissez un commentaire et cliquez sur **Créer**.

4. Lorsque vous y êtes invité, veuillez confirmer que vous êtes bien conscient que ce changement ne peut pas être annulé et que tous les packages de configuration créés après la mise à jour de ce certificat d'entreprise ont besoin que ce CCO soit inclus pour être utilisés sur les terminaux déjà installés.

5. Lorsque vous y êtes invité, veuillez confirmer que la mise à jour a réussi et qu'un CCO à inclure dans tous les packages de configuration a été créé. Cliquez sur **OK**.

6. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**.

7. Sélectionnez le type de package de configuration des terminaux : **Packages du client administré** ou **Packages du client autonome**.

8. Cliquez sur **Ajouter un package de configuration** et saisissez un nom pour le package de configuration.

9. Sélectionnez le **CCO** que vous aviez créé auparavant.

10. Procédez à toutes les autres sélections de votre choix.

11. Indiquez un chemin de sortie pour le package de configuration (MSI).

12. Cliquez sur **Créer un package de configuration**.
    Le package de configuration (MSI) a été créé dans le répertoire spécifié.

13. Redémarrez tous les serveurs (base de données) SafeGuard Enterprise.

14. Distribuez et déployez ce package aux terminaux protégés par SafeGuard Enterprise.

Tous les certificats générés par SafeGuard Enterprise sont signés avec le nouvel algorithme. Retrouvez plus de renseignements dans l'article 116791 de la base de connaissances de Sophos.

Assignation d'un certificat à partir d'Active Directory

- Le certificat doit être répertorié dans la liste figurant sur l'onglet **Certificats publiés** des propriétés de l'utilisateur dans Active Directory.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Sélectionnez l’utilisateur à qui vous voulez assigner un certificat et ouvrez l’onglet **Certificat** dans la zone de travail à droite.
3. Cliquez sur l’icône **Rechercher un certificat dans le répertoire** de la barre d’outils de SafeGuard Management Center ou sélectionnez **Rechercher un certificat dans le répertoire** dans le menu **Actions**.
4. Sélectionnez le certificat dans la boîte de dialogue **Assigner un certificat à partir du répertoire**.
5. Cliquez sur **OK**.

Le certificat est assigné à l’utilisateur. Un seul certificat peut être assigné par utilisateur.

Création et assignation d’un certificat

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Sélectionnez l’utilisateur à qui vous voulez assigner un certificat et ouvrez l’onglet **Certificat** dans la zone de travail à droite.
3. Cliquez sur l’icône **Ajouter un certificat** de la barre d’outils de SafeGuard Management Center ou sélectionnez **Ajouter un certificat** dans le menu **Actions**.
4. Saisissez un mot de passe et confirmez-le.
5. Cliquez sur **OK**.

Le certificat est assigné à l’utilisateur. Un seul certificat peut être assigné par utilisateur.

3.8.11.4 Exportation du certificat d’entreprise et du responsable principal de la sécurité

Dans une installation SafeGuard Enterprise, les deux éléments suivants sont essentiels et doivent être sauvegardés dans un emplacement sûr :

- Le certificat d’entreprise enregistré dans la base de données SafeGuard.
- Le certificat du responsable principal de la sécurité (MSO) se trouvant dans le magasin de certificats de l’ordinateur sur lequel SafeGuard Management Center est installé.

Vous pouvez exporter ces deux certificats sous la forme de fichiers .p12 à des fins de sauvegarde. Pour restaurer les installations, vous pouvez importer le certificat d’entreprise et du responsable de la sécurité correspondant sous la forme de fichiers .p12 et les utiliser lorsque vous paramétrez une nouvelle base de données. Ceci pour éviter de restaurer l’intégralité de la base de données.

Remarque :

Nous vous conseillons de réaliser cette tâche immédiatement après la configuration initiale de SafeGuard Management Center.

Retrouvez plus de renseignements sur l'exportation du certificat du responsable principal de la sécurité à la section Exportation du certificat du responsable principal de la sécurité *(page 142)*.

Exportation des certificats d'entreprise

Seuls les responsables principaux de la sécurité sont autorisés à exporter les certificats d'entreprise à des fins de sauvegarde.

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Options**.
2. Cliquez sur l'onglet **Certificats**, puis sur **Exporter** dans la section **Certificat d'entreprise**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Saisissez un mot de passe, confirmez-le, puis cliquez sur **OK**.
4. Saisissez un nom et un emplacement de stockage pour le fichier, puis cliquez sur **OK**.

Le certificat d'entreprise est exporté sous la forme d'un fichier .p12 à l'emplacement désigné et peut être utilisé à des fins de récupération.

3.8.12 Ordres de changement du certificat d'entreprise (CCO)

Les ordres de changement du certificat d'entreprise (CCO, Company Certificate Change Orders) sont utilisés dans les cas suivants :

- **Renouvellement du certificat d'entreprise** en cas d'expiration.

  Le renouvellement du certificat d'entreprise est possible pour les terminaux administrés et les terminaux autonomes. Il peut uniquement être activé à partir de la console d'administration.
- **Déplacement des terminaux non administrés** dans un environnement différent. Par exemple, si vous avez deux environnements Sophos SafeGuard différents et souhaitez les fusionner en un environnement Sophos SafeGuard unique au sein duquel l'un des deux environnements devra toujours être l'environnement cible.

  Vous pouvez effectuer ceci en échangeant le certificat d'entreprise des terminaux d'un environnement par le certificat d'entreprise de l'environnement cible.

  Seuls les responsables principaux de la sécurité sont autorisés à créer des ordres de changement du certificat d'entreprise (CCO). Pour permettre à d'autres responsables de la sécurité de créer des ordres de changement du certificat d'entreprise, le Responsable principal de la sécurité doit créer un rôle personnalisé et assigner le droit **Gérer les CCO** à ce rôle.

3.8.12.1 Renouvellement du certificat d’entreprise

Un certificat d’entreprise sur le point d’expirer peut être renouvelé dans SafeGuard Management Center. À la connexion, SafeGuard Management Center commence à afficher un avertissement six mois avant l’expiration du certificat d’entreprise. Sans certificat d’entreprise valide, un terminal ne peut pas se connecter au serveur. Le renouvellement du certificat d’entreprise comprend trois étapes :

- Création d’un ordre de changement du certificat (CCO, Certificate Change Order).
- Création d’un package de configuration contenant le CCO.
- Redémarrage des serveurs et distribution et déploiement des packages de configuration sur les terminaux.

Pour renouveler un certificat d’entreprise :

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Options**.
2. Sélectionnez l’onglet **Certificats** et cliquez sur **Mettre à jour** dans la section **Demander**.
3. Dans la boîte de dialogue **Mettre à jour le certificat d’entreprise**, saisissez un nom de CCO et indiquez un chemin de sauvegarde. Saisissez un mot de passe pour le fichier P12 et retapez-le. En option, saisissez un commentaire et cliquez sur **Créer**.
4. Lorsque vous y êtes invité, veuillez confirmer que vous êtes bien conscient que ce changement ne peut pas être annulé et que tous les packages de configuration créés après la mise à jour de ce certificat d’entreprise ont besoin que ce CCO soit inclus pour être utilisés sur les terminaux déjà installés.
5. Lorsque vous y êtes invité, veuillez confirmer que la mise à jour a réussi et qu’un CCO à inclure dans tous les packages de configuration a été créé. Cliquez sur **OK**.
6. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**.
7. Sélectionnez **Packages du client administré**.
8. Cliquez sur **Ajouter un package de configuration** et saisissez un nom pour le package de configuration.
9. Assignez un **Serveur principal** (le **serveur secondaire** n’est pas nécessaire).
10. Sélectionnez le **CCO** que vous avez créé auparavant pour mettre à jour le certificat d’entreprise.
11. Sélectionnez le mode **Chiffrement du transport** définissant la manière de chiffrer la connexion entre le client et le serveur SafeGuard Enterprise : chiffrement du transport SafeGuard ou chiffrement SSL.
    Le protocole SSL présente l’avantage d’être standard et de permettre d’établir une connexion plus rapidement qu’en utilisant le chiffrement du transport SafeGuard. Le chiffrement SSL est

sélectionné par défaut. Retrouvez plus de renseignements sur la sécurisation des connexions de transport avec SSL à la section Sécurisation des connexions de transport avec SSL *(page 49)*.

12. Indiquez un chemin de sortie pour le package de configuration (MSI).

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

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Assurez-vous de redémarrer tous les serveurs SGN. Vous devez maintenant distribuer et déployer ce package sur les terminaux administrés par SafeGuard Enterprise.

3.8.12.2 Remplacement du certificat d'entreprise

Le remplacement du certificat d'entreprise est nécessaire lorsque vous voulez déplacer un terminal d'un environnement autonome à un autre différent. Le terminal à déplacer doit avoir le certificat d'entreprise de l'environnement dans lequel il va être déplacé. Sinon, le terminal n'accepte pas les stratégies du nouvel environnement.

Les conditions préalables suivantes doivent être remplies :

Décidez quel environnement Management Center sera la source et la cible. SafeGuard Management Center source est celui que vous avez utilisé pour créer les packages de configuration des terminaux à déplacer. SafeGuard Management Center cible est celui dans lequel les terminaux seront déplacés.

Pour remplacer le certificat d'entreprise :

1. Ouvrez SafeGuard Management Center cible et sélectionnez **Outils > Options**.

2. Sélectionnez l'onglet **Certificats** et cliquez sur le bouton **Exporter** sous **Certificat d'entreprise**.

3. Saisissez et confirmez un mot de passe pour la sauvegarde du certificat lorsque vous y êtes invité et sélectionnez un répertoire de destination et un nom de fichier également lorsque vous y êtes invité.
   Le certificat d'entreprise est exporté (fichier cer).

4. Ouvrez SafeGuard Management Center source et sélectionnez **Outils > Options**.

5. Sélectionnez l'onglet **Certificats** et cliquez sur **Créer...** dans la section **Demander**.

6. Dans la boîte de dialogue **Création d'un ordre de changement du certificat d'entreprise (CCO)**, naviguez jusqu'au certificat d'entreprise cible que vous avez exporté dans SafeGuard Management Center cible (étape 1). Assurez-vous qu'il s'agit du certificat désiré.

7. Cliquez sur **Créer** et sélectionnez un répertoire de destination et un nom de fichier pour le fichier .cco. Confirmez que vous voulez passer un **Ordre de changement du certificat d'entreprise**. Sachez qu'un CCO n'est pas relié à des terminaux spécifiques. À l'aide d'un CCO, tout client de l'environnement source peut être déplacé.

8. Dans SafeGuard Management Center cible, importez le CCO créé dans SafeGuard Management Center source.

9. Dans le menu **Outils**, cliquez sur **Outil de package de configuration** et sélectionnez l'onglet **CCO**.

10. Cliquez sur **Importer**.

11. Dans la boîte de dialogue **Importation de l'ordre de changement du certificat d'entreprise (CCO)**, sélectionnez le CCO que vous avez créé dans SafeGuard Management Center source et saisissez un nom de CCO et une description (facultatif). Cliquez sur **OK**.

12. Dans SafeGuard Management Center cible, créez un package de configuration.

13. Dans le menu **Outils**, cliquez sur **Outil de package de configurationPackages du client autonome** et ajoutez un nouveau package de configuration.

14. Sélectionnez le CCO importé dans le menu déroulant dans la colonne **CCO**.

15. Indiquez un emplacement sous **Chemin de sortie du package de configuration**.

16. Cliquez sur **Créer un package de configuration**.
    Le package de configuration est créé dans l'emplacement spécifié.

17. Installez ce package de configuration sur tous les terminaux que vous voulez déplacer de l'environnement source vers l'environnement cible.

3.8.12.3 Gestion des ordres de changement du certificat d'entreprise

Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**. Tous les ordres de changement du certificat d'entreprise (CCO, Company Certificate Change Order) apparaissent dans l'onglet **CCO**.

Des informations détaillées sur le CCO sélectionné apparaissent dans la partie inférieure de la boîte de dialogue.

Si le CCO a été créé pour mettre à jour le certificat d'entreprise, le **Certificat d'entreprise d'origine** doit être renouvelé. Si le CCO a été créé pour déplacer les terminaux, veuillez renouveler le certificat d'entreprise de l'environnement dans lequel les terminaux vont être déplacés.

Le **Certificat d’entreprise de destination** est le nouveau certificat d’entreprise si le CCO a été créé pour mettre à jour le certificat d’entreprise ou le certificat d’entreprise de l’environnement dans lequel les terminaux vont être déplacés.

Au-dessous des détails du certificat sont affichées les tâches pour lesquelles le CCO sélectionné peut être utilisé.

Pour pouvoir gérer les CCO, vous devez disposer du droit de **Gérer les CCO**.

Importation

Lors de la création de packages de configuration, si vous souhaitez sélectionner l’ordre de changement du certificat d’entreprise (CCO) créé par un autre outil d’administration pour changer le certificat d’entreprise, vous devez d’abord l’importer.

Si vous cliquez sur **Importer...**, une boîte de dialogue s’ouvre dans laquelle vous pouvez sélectionner et nommer le CCO. Le nom que vous saisissez ici apparaît sur l’onglet **CCO** de l’**Outil de package de configuration**.

Exporter

À l’aide de la fonctionnalité **Exporter**, les CCO stockés dans la base de données peuvent être exportés et sont alors disponibles sous la forme de fichiers .cco.

3.8.13 Licences

Vous avez besoin d'une licence valide pour utiliser SafeGuard Enterprise avec SafeGuard Management Center. Par exemple, dans la base de données SafeGuard Enterprise, une licence valide est une condition préalable à l'envoi de stratégies aux terminaux. Les licences de token appropriées sont également requises pour la gestion des tokens.

Les fichiers de licence sont disponibles auprès de votre partenaire des ventes. Ces fichiers doivent être importés dans la base de données SafeGuard Enterprise après l'installation.

Le fichier de licence inclut entre autres informations :

- Le nombre de licences achetées par module.
- Le nom du détenteur de la licence.

Si le nombre de licences disponibles ou la limite de tolérance est dépassé, des messages d'avertissement/erreur correspondants s'affichent au démarrage de SafeGuard Management Center.

Dans la zone **Utilisateurs et ordinateurs**, SafeGuard Management Center propose un aperçu de l'état de la licence du système SafeGuard Enterprise installé. L'affichage de l'état de la licence est disponible dans l'onglet **Licences** du nœud racine, des domaines, des OU, des objets conteneurs et

des groupes de travail. C'est là que les responsables de la sécurité peuvent trouver des informations détaillées sur l'état de la licence. S'ils ont les droits suffisants, ils peuvent importer des licences dans la base de données SafeGuard Enterprise.

3.8.13.1 Fichier de licence

Le fichier de licence à importer dans la base de données SafeGuard Enterprise, que vous recevez, est un fichier .XML avec une signature. Le fichier de licence inclut les informations suivantes :

- Nom de la société
- Informations supplémentaires (département, filiale par exemple)
- Date de génération
- Nombre de licences par module
- Informations sur la licence du token
- Date d’expiration de la licence
- Type de licence (démonstration ou complète)
- Signature avec le certificat de signature de licence

3.8.13.2 Licences de token

Pour gérer des tokens ou des cartes à puce, les licences de token appropriées sont requises. Si les licences appropriées ne sont pas disponibles, vous ne pouvez pas créer de stratégies pour les tokens dans SafeGuard Management Center.

3.8.13.3 Licences d’évaluation

Le fichier de licence d’évaluation peut être utilisé à des fins d’évaluation. Ces licences sont uniquement valides pendant une certaine période de temps et ont une date d’expiration. En revanche il n’existe aucune restriction fonctionnelle.

Ces licences ne doivent pas être utilisées dans un environnement de travail normal.

Après avoir installé SafeGuard Management Center et effectué toutes les étapes de l’assistant de configuration, vous pouvez importer la licence d’essai que vous téléchargée comme indiqué à la section Importation de fichiers de licence *(page 192)*.

Si vous n’importez pas un fichier de licence, vous allez être invité à le faire au démarrage de SafeGuard Management Center.

Fichiers de licence d’essai

Lorsque vous téléchargez le produit, vous pouvez également télécharger un fichier de licence d’essai. Cette licence d’évaluation (appelée licence d’évaluation de SafeGuard Enterprise) contient cinq licences pour chaque module et elle est valable pendant deux ans à compter de la date de sortie de la version SafeGuard Enterprise en question.

Fichiers de licence de démonstration individuelle

Si vous avez besoin de plus de licences que celles disponibles dans le fichier de licence par défaut pour l'évaluation, vous pouvez obtenir une licence de démo adaptée à vos besoins. Pour obtenir un fichier de licence de démonstration individuelle, veuillez contacter votre partenaire de ventes. Ce type de démonstration de licence est également limité dans le temps. La licence est également limitée au nombre de licences par module accordé par votre partenaire commercial.

Lorsque vous démarrez SafeGuard Management Center, un message d'avertissement indique que vous utilisez des licences de démonstration. Si le nombre de licences disponibles indiqué dans la licence de démonstration est dépassé ou si la durée limite est atteinte, un message d'erreur s'affiche.

3.8.13.4 Aperçu de l’état de la licence

Pour afficher un aperçu de l’état de la licence :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Dans la fenêtre de navigation à gauche, cliquez sur le nœud racine, le domaine, l’OU, l’objet conteneur ou le groupe de travail.
3. Dans la zone d’action, passez dans l’onglet **Licences**.

L’état de la licence apparaît.

L’écran est divisé en trois zones. La zone supérieure indique le nom du client pour lequel la licence a été générée ainsi que la date de génération.

La zone centrale propose des détails sur la licence. Les colonnes individuelles contiennent les informations suivantes :

Colonne	Explication
État (icône)	Une icône indique le statut de la licence (validité, message d'avertissement, message d'erreur) du module concerné.
Fonction	Indique le module installé.
Licences achetées	Indique le nombre de licences achetées pour le module installé.
Licences utilisées	Indique le nombre de licences utilisées pour le module installé.
Expire	Indique la date d'expiration de la licence.
Type	Indique le type de licence, démonstration ou standard.

Si vous affichez l'onglet **Licences** d'un domaine/OU, l'aperçu indique l'état en fonction de l'ordinateur de la branche concernée.

Des détails sur les modules de token sous licence sont proposés sous cette présentation.

Dans la partie inférieure, un message avec une couleur d'arrière-plan spécifique à l'état (vert = valide, jaune = avertissement, rouge = erreur) et une icône indiquent l'état global de la licence, quel que soit le domaine ou l'UO sélectionnée. En cas de message d'avertissement ou d'erreur, les informations sur la restauration d'un état de licence valide sont également affichées.

Les icônes affichées dans l'onglet **Licences** ont les significations suivantes :

Licence valide

Avertissement

La licence d'un module affiche un état d'avertissement si

- La limite de la licence est dépassée.
- La licence a expiré.

Erreur

La licence d'un module affiche un état d'erreur si

- La licence a expiré il y a plus d'un mois.

Pour actualiser l'aperçu de l'état de la licence, cliquez sur **Recompter les licences utilisées**.

3.8.13.5 Importation de fichiers de licence

Condition préalable : pour importer un fichier de licence dans la base de données SafeGuard Enterprise, un responsable de la sécurité doit disposer du droit « Importer le fichier de licence ».

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.

2. Dans la fenêtre de navigation, à gauche, cliquez sur le nœud racine, le domaine ou l'unité organisationnelle.
3. Dans la zone d'action, passez dans l'onglet **Licences**.
4. Cliquez sur le bouton **Importer le fichier de licence...**.

   Une fenêtre s'ouvre dans laquelle vous pouvez sélectionner le fichier de licence.

5. Sélectionnez le fichier de licence que vous souhaitez importer, puis cliquez sur **Ouvrir**.

   La boîte de dialogue **Application de la licence ?** apparaît avec le contenu du fichier de licence.

6. Cliquez sur **Appliquer la licence**.

Le fichier de licence est importé dans la base de données SafeGuard Enterprise.

Après avoir importé le fichier de licence, les licences de module achetées sont indiquées par le type de licence **standard**. Tous les modules pour lesquels aucune licence n'a été achetée et pour lequel la licence d'évaluation (fichier de licence par défaut) ou des licences de démonstration individuelles sont utilisées sont marqués avec le type de licence **démonstration**.

Lorsqu'un nouveau fichier de licence est importé, seuls les modules inclus dans ce fichier de licence sont affectés. Toute autre information de licence de module est conservée telle que récupérée depuis la base de données. Cette fonctionnalité d'importation simplifie l'évaluation d'autres modules suite à l'achat.

3.8.13.6 Dépassement du nombre de licences

Une valeur de tolérance a été définie dans votre fichier de licence quant au dépassement du nombre de licences achetées et à la période de validité de la licence. Si le nombre de licences disponibles par module ou la période de validité est dépassé, un message d'avertissement s'affiche. Ceci n'affecte pas l'utilisation du système et aucune restriction n'affecte ses fonctionnalités. Vous pouvez réviser l'état de la licence et mettre à niveau ou renouveler votre licence. La valeur de tolérance est généralement de 10 % du nombre de licences achetées (la valeur minimale est 5, la valeur maximale est 5 000).

Un message d'erreur s'affiche si la valeur de tolérance est dépassée. Dans ce cas, les fonctionnalités sont restreintes. Le déploiement des stratégies sur les terminaux est désactivé. Cette désactivation ne peut pas être inversée manuellement dans SafeGuard Management Center. La licence doit être mise à niveau ou renouvelée pour pouvoir de nouveau bénéficier de toutes les fonctions. Outre la désactivation du déploiement des stratégies, la restriction fonctionnelle n'affecte pas les terminaux. Les stratégies affectées restent actives. Les clients peuvent également être désinstallés.

Les sections suivantes décrivent le comportement du système en cas de dépassement du nombre de licences autorisées ainsi que l’action nécessaire pour restaurer la restriction fonctionnelle.

Licence non valide : avertissement

Si le nombre de licences disponibles est dépassé, un avertissement apparaît au démarrage de SafeGuard Management Center.

SafeGuard Management Center s'ouvre et affiche la présentation de l'état de la licence dans la zone **Utilisateurs et ordinateurs** de l'onglet **Licences**.

Un message d'avertissement vous informe que la licence n'est pas valide. À l'aide des informations détaillées sur le fichier de licence, vous pouvez déterminer le module pour lequel le nombre de licences disponibles est dépassé. Cet état de la licence peut être modifié en faisant évoluer, en renouvelant ou en mettant la licence à niveau.

Licence non valide : erreur

Si la valeur de tolérance du nombre de licences ou la période de validité définie dans la licence est dépassée, SafeGuard Management Center affiche un message d’erreur.

Dans SafeGuard Management Center, le déploiement de stratégies sur les terminaux est désactivé.

Un message d’erreur s’affiche dans la zone **Utilisateurs et ordinateurs** de l’onglet **Licences**.

À l’aide des informations détaillées sur le fichier de licence, vous pouvez déterminer le module pour lequel le nombre de licences disponibles est dépassé.

Pour surmonter la restriction de fonctionnalité, vous pouvez :

- Redistribuer des licences

  Pour mettre à disposition les licences, vous pouvez désinstaller le logiciel sur les terminaux non utilisés pour supprimer les ordinateurs de la base de données SafeGuard Enterprise.

- Mettre à niveau/renouveler des licences

  Contactez votre partenaire commercial pour mettre à niveau ou renouveler votre licence. Vous recevrez un nouveau fichier de licence à importer dans la base de données SafeGuard Enterprise.

- Importer un nouveau fichier de licence

Si vous avez renouvelé ou mis à niveau votre licence, veuillez importer le fichier de licence dans la base de données SafeGuard Enterprise. Ce nouveau fichier importé remplace le fichier de licence non valide.

Dès que vous redistribuez des licences ou que vous importez un fichier de licence valide, la restriction fonctionnelle est annulée et le système fonctionne à nouveau normalement.

3.8.14 Tokens et cartes à puce

SafeGuard Enterprise fournit une sécurité optimale en prenant en charge les tokens et cartes à puce pour authentification. Les tokens/cartes à puce peuvent stocker des certificats, signatures numériques et renseignements biométriques.

Remarque :

Les tokens et les cartes à puce ne peuvent pas être configurés sur les terminaux macOS.

L'authentification par token est basée sur le principe d'une authentification en deux étapes : l'utilisateur possède un token (propriété), mais il ne peut l'utiliser que s'il en connaît le mot de passe (connaissance). Lorsqu'un token ou une carte à puce sont utilisés, leur présence et un code confidentiel suffisent à l'utilisateur pour s'authentifier.

Les cartes à puce et les tokens sont traités de la même manière dans SafeGuard Enterprise. Les termes « token » et « carte à puce » recouvrent la même notion dans le produit et le manuel. L'utilisation de tokens et de cartes à puce doit être activée dans la licence comme indiqué à la section Licences de token *(page 190)*.

Windows 8 et version supérieure offre une fonction nommée *carte à puce virtuelle*. Une carte à puce virtuelle simule les fonctionnalités d'une carte à puce physique à l'aide d'une puce TPM. En revanche, elle ne peut pas être utilisée avec SafeGuard Enterprise.

Les tokens sont pris en charge dans SafeGuard Enterprise :

- Dans l'authentification au démarrage SafeGuard (non applicable à Windows 8 et Windows 8.1)
- Au niveau du système d'exploitation
- Pour se connecter à SafeGuard Management Center

Lorsqu'un token est généré pour un utilisateur dans SafeGuard Enterprise, des informations telles que le fabricant, le type, le numéro de série, les données de connexion et les certificats sont stockées dans la base de données SafeGuard Enterprise. Les tokens sont identifiés par un numéro de série, puis reconnues dans SafeGuard Enterprise.

Les avantages sont considérables :

- Vous savez quels tokens sont en circulation et à quels utilisateurs ils ont été assignés.
- Vous connaissez la date et l’heure de leur création.
- En cas de perte d’un token, le responsable de la sécurité peut l’identifier et le bloquer. Ces mesures évitent toute utilisation frauduleuse de données.
- Toutefois, le responsable de la sécurité peut utiliser la procédure Challenge/Réponse pour autoriser temporairement la connexion sans token, par exemple si un utilisateur a oublié son code confidentiel.

  Remarque : Avec le chiffrement de volumes SafeGuard, cette option de récupération n’est pas prise en charge par la connexion par token cryptographique (Kerberos).

3.8.14.1 Types de token

Le terme « token » se rapporte à toutes les technologies utilisées et ne dépend pas d'une forme particulière de périphérique. Il englobe tous les périphériques pouvant stocker et transférer des données à des fins d'identification et d'authentification (cartes à puce ou tokens USB).

SafeGuard Enterprise prend en charge les types suivants de tokens/cartes à puce pour l'authentification :

- **Non cryptographique**

  L'authentification au démarrage SafeGuard et Windows est basée sur les codes d'accès de l'utilisateur (Identifiant utilisateur/Mot de passe) stockés sur le token.
- **Cryptographique - Kerberos**

  L'authentification au démarrage SafeGuard et Windows est basée sur les certificats stockés sur le token. Les tokens cryptographiques ne peuvent pas être utilisés pour les terminaux non administrés.

Tokens cryptographiques - Kerberos

Avec les tokens cryptographiques, l’utilisateur est identifié à l’authentification au démarrage SafeGuard par le certificat stocké sur le token. Pour se connecter au système, il suffit à l’utilisateur de saisir le code confidentiel du token.

Remarque : Les tokens cryptographiques ne peuvent pas être utilisés pour les terminaux non administrés.

Vous devez fournir des tokens aux utilisateurs. Retrouvez plus de renseignements à la section Configuration de l'utilisation d'un token *(page 199)*.

Conditions requises de base pour les certificats :

- Algorithme : RSA
- Longueur de la clé : minimum 1024
- Utilisation de la clé : *chiffrement de données* ou *chiffrement de la clé*.

Remarque : En cas de problèmes de connexion avec un token Kerberos, il n'est pas possible d'utiliser la procédure Challenge/Réponse ou Local Self Help pour la récupération de la connexion. Seule la procédure Challenge/Réponse utilisant les clients virtuels est prise en charge. Elle permet aux utilisateurs de récupérer l'accès aux volumes chiffrés sur leurs terminaux.

3.8.14.2 Composants

Pour utiliser les tokens/cartes à puce avec SafeGuard Enterprise, les composants suivants sont requis :

- Token/carte à puce
- Lecteur de token/carte à puce
- Pilote de token/carte à puce
- Middleware de token/carte à puce (module PKCS#11)

Tokens USB

De même que les cartes à puce, les tokens USB comportent une carte à puce et un lecteur de cartes à puce dans un même boîtier. L'utilisation des tokens USB nécessite la présence d'un port USB.

Lecteurs et pilotes de token/carte à puce

- **Windows**

  Dans le système d'exploitation Windows, les lecteurs de cartes compatibles PC/SC sont pris en charge. L'interface PC/SC régit la communication entre l'ordinateur et la carte à puce. La majorité de ces lecteurs de cartes sont déjà intégrés dans l'installation de Windows. Pour être prises en charge par SafeGuard Enterprise, les cartes à puce requièrent des pilotes compatibles PKCS#11.

- **Authentification au démarrage SafeGuard**

  Avec l'authentification au démarrage SafeGuard, c'est l'interface PC/SC qui régit la communication entre le PC et la carte à puce. Les pilotes de cartes à puce pris en charge sont fixés, de sorte que les utilisateurs ne peuvent pas en ajouter. Les pilotes de cartes à puce appropriés doivent être activés au moyen d'une stratégie dans SafeGuard Enterprise.

  L'interface des lecteurs de cartes à puce est standardisée et un grand nombre de ces lecteurs possèdent une interface USB ou une interface ExpressCard/54 et mettent en œuvre la norme CCID. Dans SafeGuard Enterprise, il s'agit d'une condition préalable à la prise en charge avec l'authentification au démarrage SafeGuard. De plus, du côté du pilote, le module PKCS#11 doit être pris en charge.

Tokens et cartes à puce pris en charge par l'authentification au démarrage SafeGuard

SafeGuard Enterprise prend en charge une large variété de cartes à puce et de lecteurs de carte à puce, de tokens USB et de leurs pilotes respectifs ainsi que de middlewares grâce à l'authentification au démarrage SafeGuard. Avec SafeGuard Enterprise, les tokens/cartes à puce compatibles avec les opérations 2048 bits RSA sont pris en charge.

La prise en charge des tokens et cartes à puce faisant l'objet d'améliorations d'une version à l'autre, les tokens et cartes à puce de la version actuelle de SafeGuard Enterprise sont répertoriés dans les Notes de publication.

Middlewares compatibles

Les middlewares de la liste ci-dessous sont compatibles avec le module PKCS#11 correspondant. PKCS#11 est une interface standard servant à connecter des tokens cryptographiques/cartes à puce à différents logiciels. Elle est utilisée ici pour la communication entre le token cryptographique/carte à puce, le lecteur de carte à puce et SafeGuard Enterprise. Retrouvez plus de renseignements dans l'article 132376 de la base de connaissances Sophos.

Fabricant	Middleware
ActivIdentity	ActivClient, ActivClient (PIV)
AET	SafeSign Identity Client
Aladdin	eToken PKI Client
A-Trust Charismatics	a.sign Client Smart Security Interface
Gemalto	Gemalto Access Client, Gemalto Classic Client, Gemalto .NET Card
IT Solution GmbH	IT Solution trustWare CSP+
Nexus RSA	Nexus Personal RSA Authentication Client 2.x, RSA Smart Card Middleware 3.x

Fabricant	Middleware
Sertifitseerimiskeskus AS	Estonian ID Card
Siemens	CardOS API TC-FNMT
ATOS	CardOS API TC-FNMT
FNMT	Módulo PCKS#11 TC-FNMT TC-FNMT
T-Systems	NetKey 3.0
Unizeto	proCertum

Licences

Sachez que l'utilisation des middlewares respectifs pour le système d'exploitation standard requiert un accord de licence avec le fabricant correspondant. Retrouvez plus de renseignements sur la manière d'obtenir des licences dans l'article 116585 de la base de connaissances Sophos.

Le middleware est défini dans la stratégie SafeGuard Enterprise du type **Paramètres de machine spécifiques** sous **Paramètres PKCS#11 personnalisés** dans le champ **Module PKCS#11 pour Windows** ou **Module PKCS#11 pour l'authentification au démarrage SafeGuard**. Le package de configuration correspondant doit également être installé sur l'ordinateur sur lequel fonctionne SafeGuard Management Center.

3.8.14.3 Configuration de l'utilisation d'un token

Procédez aux étapes suivantes si vous voulez fournir des tokens aux utilisateurs suivants à des fins d'authentification :

- Utilisateurs de terminaux administrés
- Responsables de la sécurité de SafeGuard Management Center

1. Initialisez les tokens vides.
   Retrouvez plus de renseignements à la section Initialisation d'un token *(page 200)*.
2. Installez le middleware.
   Retrouvez plus de renseignements à la section Installation du middleware *(page 201)*.
3. Activez le middleware.
   Retrouvez plus de renseignements à la section Activation du middleware *(page 201)*.
4. Générez des tokens pour les utilisateurs et les responsables de la sécurité.
   Retrouvez plus de renseignements à la section Génération d'un token *(page 202)*.
5. Configurez le mode de connexion.
   Retrouvez plus de renseignements à la section Configuration du mode de connexion *(page 204)*.
6. Configurez d'autres paramètres de token comme par exemple, les règles de syntaxe des codes confidentiels.

Pour plus d’informations, reportez-vous aux sections Gestion des codes confidentiels *(page 210)* et Gestion des tokens et des cartes à puce *(page 212)*.

7. Assignez des certificats et des clés aux tokens/utilisateurs.
   Retrouvez plus de renseignements à la section Assignation de certificats *(page 206)*.

Vous pouvez également utiliser des tokens dont les données proviennent d’une application différente pour l’authentification à condition qu’ils disposent de suffisamment d’espace de stockage pour les certificats et les informations de connexion.

Pour une administration simplifiée des tokens, SafeGuard Enterprise propose les fonctions suivantes :

- Affichage et filtrage des informations du token
- Initialisation, modification, réinitialisation et blocage des codes confidentiels
- Lecture et suppression des données du token
- Blocage des tokens

Remarque : Pour générer et gérer des tokens ou modifier des données sur les tokens générés, vous avez besoin des droits d’**Accès complet** pour les utilisateurs concernés. La vue **Tokens générés** n’affiche que les tokens des utilisateurs pour qui vous avez des droits en **Lecture seule** ou d’**Accès complet**.

3.8.14.4 Préparation à l’utilisation d’un token

Pour préparer la prise en charge d’un token ou d’une carte à puce dans SafeGuard Enterprise, veuillez :

- Initialisez les tokens vides.
- Installez le middleware.
- Activez le middleware.

Initialisation d’un token

Avant qu’un token « vide » non formaté puisse être généré, il doit être préparé pour l’utilisation, c’est-à-dire initialisé, conformément aux instructions fournies par son fabricant. Lorsqu’il est initialisé, des informations de base, par exemple le code confidentiel standard, sont écrites dessus. Cette opération s’effectue avec le logiciel d’initialisation du fabricant de tokens.

Retrouvez plus de renseignements chez le fabricant de tokens concerné.

Installation du middleware

Veuillez installer le middleware qui convient, à la fois sur l'ordinateur sur lequel SafeGuard Management Center est installé et sur le terminal approprié, si vous ne l'avez pas déjà fait. Retrouvez plus de renseignements sur les middlewares compatibles à la section Middlewares compatibles *(page 198)*.

Redémarrez les ordinateurs sur lesquels vous avez installé le nouveau middleware.

Remarque : Si vous installez le middleware **Gemalto .NET Card** ou **Nexus Personal**, vous allez également devoir ajouter leur chemin d'installation à la variable d'environnement PATH des **Propriétés système** de votre ordinateur.

- Le chemin d'installation par défaut pour **Gemalto .NET Card** : `C:\Program Files\Gemalto\PKCS11 for .NET V2 smart cards`
- Le chemin d'installation par défaut pour **Nexus Personal** : `C:\Program Files\Personal\bin`

Activation du middleware

Veuillez assigner le middleware approprié sous la forme du module PKCS#11 en définissant une stratégie dans SafeGuard Management Center. Vous devez le faire à la fois sur l'ordinateur sur lequel SafeGuard Management Center est exécuté et sur le terminal. C'est la condition nécessaire pour que SafeGuard Enterprise communique avec le token. Vous pouvez définir le paramètre du module PKCS#11 en utilisant une stratégie, de la façon suivante.

Condition préalable : le middleware est installé sur l'ordinateur concerné et le token a été initialisé. Le package de configuration du client SafeGuard Enterprise doit également être installé sur l'ordinateur PC sur lequel SafeGuard Management Center est exécuté.

1. Dans SafeGuard Management Center, cliquez sur **Stratégies**.
2. Créez une nouvelle stratégie du type **Paramètres de machine spécifiques** ou sélectionnez une stratégie existante de ce type.
3. Dans la zone de travail côté droit, sélectionnez le middleware approprié sous **Paramètres de prise en charge du token > Nom du module**. Enregistrez les paramètres.
4. Assignez la stratégie.

À présent, SafeGuard Enterprise peut communiquer avec le token.

3.8.14.5 Génération d’un token

Lorsqu’un token est généré dans SafeGuard Enterprise, les données qui sont utilisées pour l’authentification sont écrites sur ce token. Ces données sont constituées de codes d’accès et de certificats.

Dans SafeGuard Enterprise, des tokens peuvent être générés pour les rôles d’utilisateurs suivants :

- Tokens pour les utilisateurs de terminaux administrés
- Tokens pour les responsables de la sécurité

L’utilisateur et les responsables de la sécurité peuvent accéder au token. L’utilisateur est celui qui doit utiliser le token. L’utilisateur n’a accès qu’aux objets et aux clés privés. Le responsable de la sécurité peut uniquement accéder aux objets publics, mais il peut réinitialiser le code confidentiel de l’utilisateur.

Génération d’un token ou d’une carte à puce pour un utilisateur

Conditions préalables :

- Le token doit être initialisé et le module PKCS#11 approprié doit être activé.
- Le package de configuration du client SafeGuard Enterprise doit également être installé sur l’ordinateur PC sur lequel SafeGuard Management Center est exécuté.
- Vous avez besoin des droits d’**Accès complet** pour l’utilisateur correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Connectez le token à l’interface USB. SafeGuard Enterprise lit le token.
3. Sélectionnez l’utilisateur pour lequel un token doit être généré, et ouvrez l’onglet **Données de token** dans la zone de travail du côté droit.
4. Dans l’onglet **Données de token**, procédez comme suit :
   a. Sélectionnez l’**ID utilisateur** et le **Domaine** de l’utilisateur concerné et saisissez votre **Mot de passe** Windows.
   b. Cliquez sur **Générer un token**.

   La boîte de dialogue **Génération d’un token** s’affiche.
5. Sélectionnez le connecteur adapté au token dans la liste déroulante **Connecteurs disponibles**.
6. Générez un nouveau **Code confidentiel utilisateur** et répétez la saisie.

7. Sous **Code confidentiel RS**, saisissez le code PUK standard fourni par le fabricant ou le code confidentiel généré lorsque le token a été initialisé.

   Remarque : Si vous remplissez uniquement le champ **Code confidentiel utilisateur (obligatoire)**, le code confidentiel de l'utilisateur doit correspondre à celui qui a été généré lors de l'initialisation du token. Il est alors inutile de répéter le code confidentiel de l'utilisateur ou de saisir un code confidentiel du responsable de la sécurité.

8. Cliquez sur **Générer un token maintenant**.

Le token est généré, les informations de connexion écrites sur le token et les informations de token enregistrées dans la base de données SafeGuard Enterprise. Vous pouvez afficher les données de la zone **Token** dans l'onglet **Informations sur le token**.

Génération d'un token ou d'une carte à puce pour un responsable de la sécurité

Lorsque SafeGuard Enterprise est installé pour la première fois, le premier responsable de la sécurité (SO) peut générer pour lui-même un token et indiquer le mode de connexion. Pour tous les autres responsables de la sécurité, les tokens sont générés dans SafeGuard Management Center.

Condition préalable :

- Le token doit être initialisé et le module PKCS#11 approprié doit être activé.
- Vous devez disposer des droits nécessaires pour effectuer des sélections pour le responsable de la sécurité.

1. Dans SafeGuard Management Center, cliquez sur **Responsables de la sécurité**.
2. Connectez le token à l'interface USB. SafeGuard Enterprise lit le token.
3. Dans la fenêtre de navigation de gauche, cochez **Responsable de la sécurité** et sélectionnez**Nouveau > Nouveau responsable de la sécurité** dans le menu contextuel.

   La boîte de dialogue **Nouveau responsable de la sécurité** s'affiche.

4. Dans le champ **Connexion au token**, spécifiez le type de connexion pour le responsable de la sécurité :

   - Pour permettre au responsable de la sécurité de s'authentifier avec ou sans token, sélectionnez **Facultatif**.

   - Pour rendre obligatoire la connexion sur la carte à puce pour le responsable de la sécurité, sélectionnez **Obligatoire**.

Avec ce paramètre, la clé privée reste sur le token. Le token doit toujours être connecté, sinon, le système doit être réinitialisé.

5. Veuillez, ensuite, indiquer le certificat du responsable de la sécurité.

   - Pour créer un nouveau certificat, cliquez sur le bouton **Créer** près de la liste déroulante **Certificat**.

     Saisissez un mot de passe pour le certificat deux fois et cliquez sur **OK** pour le confirmer.

     Indiquez l'emplacement d'enregistrement du certificat.

   - Pour importer les certificats, cliquez sur le bouton **Importer** près de la liste déroulante **Certificat** et ouvrez le fichier de certificat correspondant.

     La recherche s'effectue d'abord dans un fichier de certificat, puis sur le token. Les certificats peuvent rester dans l'emplacement de stockage quel qu'il soit.

6. Sous **Rôles**, activez les rôles devant être assignés au responsable de la sécurité.

7. Confirmez les saisies en cliquant sur **OK**.

Le responsable de la sécurité est créé, le token est généré, les informations de connexion sont écrites sur le token (en fonction du paramètre) et les informations du token sont enregistrées dans la base de données SafeGuard Enterprise. Vous pouvez afficher les données de la zone **Token** dans l'onglet **Informations sur le token**.

3.8.14.6 Configuration du mode de connexion

Il existe deux méthodes de connexion à l'aide d'un token. Il est possible de combiner les deux méthodes de connexion.

- Connexion avec identifiant utilisateur/mot de passe
- Connexion avec token

  Lorsque vous vous connectez avec un token ou une carte à puce, vous pouvez sélectionner la méthode non cryptographique ou la méthode Kerberos (cryptographique).

En tant que responsable de la sécurité, vous spécifiez le mode de connexion à utiliser dans une stratégie du type **Authentification**.

Si vous sélectionnez l'option de connexion par token **Kerberos** :

- Vous allez devoir émettre un certificat dans une infrastructure de clé publique (PKI) et la stocker sur le token. Ce certificat est importé sous forme de certificat utilisateur dans la base de données SafeGuard Enterprise. Si un certificat généré automatiquement existe déjà dans une base de données, il est remplacé par le certificat importé.

Activation de la connexion automatique à l'authentification au démarrage SafeGuard avec des codes confidentiels de token par défaut

Un code confidentiel de token par défaut distribué par la stratégie permet la connexion automatique de l'utilisateur à l'authentification au démarrage SafeGuard. Ceci permet d'éviter la génération de chaque token séparément et permet aux utilisateurs de se connecter automatiquement lors de l'authentification au démarrage SafeGuard sans intervention de l'utilisateur.

Lorsqu'un token est utilisée lors de la connexion et qu'un code confidentiel par défaut est assigné à l'ordinateur, l'utilisateur est connecté automatiquement à l'authentification au démarrage SafeGuard sans qu'il ait besoin de saisir un code confidentiel.

En tant que responsable de la sécurité, vous pouvez définir le code confidentiel spécifique dans une stratégie du type **Authentification** et l'assigner à différents ordinateurs ou groupes d'ordinateurs, par exemple à tous les ordinateurs d'un même lieu.

Pour activer la connexion automatique avec un code confidentiel de token par défaut, procédez comme suit :

1. Dans SafeGuard Management Center, cliquez sur **Stratégies**.
2. Sélectionnez une stratégie du type **Authentification**.
3. Sous **Options de connexion**, dans **Mode de connexion**, sélectionnez **Token**.
4. Dans **Code confidentiel utilisé pour la connexion automatique avec token**, spécifiez le code confidentiel par défaut à utiliser pour la connexion automatique. Dans ce cas, il n'est pas nécessaire de suivre les règles relatives au code confidentiel.

   Remarque : Ce paramètre n'est disponible que si vous sélectionnez **Carte à puce** comme **Mode de connexion** possible.

5. Dans **Connexion automatique vers Windows**, définissez **Désactiver la connexion automatique vers Windows**. Si vous ne sélectionnez pas cette option lorsqu'un code confidentiel par défaut est spécifié, vous ne pourrez pas enregistrer la stratégie.

   Si vous souhaitez activer l'option **Connexion automatique vers Windows**, vous pouvez créer ultérieurement une autre stratégie du type **Authentification** dans laquelle cette option est

activée, et l'assigner au même groupe d'ordinateurs afin que les deux stratégies soient actives dans le RSOP.

6. Vous pouvez également spécifier d'autres paramètres de token.
7. Enregistrez vos paramètres et assignez la stratégie aux ordinateurs ou groupes d'ordinateurs concernés.

Windows démarre si la connexion automatique sur le terminal réussit.

En cas d'échec de la connexion automatique sur le terminal, l'utilisateur est invité à saisir le code confidentiel de token lors de l'authentification au démarrage SafeGuard.

3.8.14.7 Assignation de certificats

Les informations de connexion, mais également les certificats peuvent être écrits sur un token. Seule la partie privée du certificat (fichier .p12) peut être enregistrée sur le token. En revanche, les utilisateurs peuvent alors seulement se connecter avec le token. Nous vous recommandons d'utiliser des certificats PKI.

Vous pouvez assigner les données d'authentification à différents types de tokens de la manière suivante :

- En générant des certificats directement sur le token.
- En assignant des données qui sont déjà sur le token.
- En important des certificats d'un fichier.

Remarque : Les certificats de l'AC ne peuvent pas provenir d'un token et être stockés dans la base de données ou dans le magasin de certificats. Si vous utilisez des certificats de l'AC, ces derniers doivent être disponibles sous forme de fichiers et pas seulement sur un token. Ceci s'applique également aux CRL (liste de révocation des certificats). De surcroît, les certificats de l'AC doivent correspondre à la liste de révocation de certificats pour que les utilisateurs puissent se connecter aux ordinateurs concernés. Vérifiez que l'AC et que la liste de révocation de certificats correspondante sont correctes. SafeGuard Enterprise n'effectue pas cette vérification. SafeGuard Enterprise ne peut ensuite communiquer avec les certificats ayant expiré que si les clés nouvelles et anciennes sont présentes sur la même carte.

Génération de certificats à partir de tokens

Pour générer des certificats à partir de tokens, vous avez besoin des droits d'**Accès complet** pour l'utilisateur concerné.

Vous pouvez générer de nouveaux certificats directement à partir du token si, par exemple, aucune structure de certificat n'est présente.

Remarque :

Si seule la partie privée du certificat est écrite sur le token, l'utilisateur peut seulement accéder à sa clé privée avec ce token. La clé privée ne se trouve alors que sur le token. En cas de perte du token, la clé privée devient inaccessible.

Condition préalable : le token a été généré.

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Connectez le token à l'interface USB.

   SafeGuard Enterprise lit le token.

3. Cochez l'utilisateur pour lequel un certificat doit être généré, et ouvrez l'onglet **Certificat** dans la zone de travail du côté droit.
4. Cliquez sur **Générer et assigner un certificat par token**. Notez que la longueur de la clé doit correspondre à la taille du token.
5. Sélectionnez le connecteur et saisissez le code confidentiel du token.
6. Cliquez sur **Créer**.

Le token génère le certificat et l'assigne à l'utilisateur.

Assignation de certificats de token à un utilisateur

Conditions préalables :

- le token a été généré.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

Pour assigner un certificat disponible sur un token à un utilisateur :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.
2. Connectez le token à l'interface USB.

   SafeGuard Enterprise lit le token.

3. Sélectionnez l'utilisateur à qui vous voulez assigner un certificat et ouvrez l'onglet **Certificat** dans la zone de travail à droite.

4. Cliquez sur l’icône **Assigner un certificat à partir d’un token** de la barre d’outils de SafeGuard Management Center.
5. Sélectionnez le certificat concerné dans la liste et saisissez le code confidentiel du token.
6. Cliquez sur **OK**.

Le certificat est assigné à l’utilisateur. Un seul certificat peut être assigné par utilisateur.

Modification du certificat de l’utilisateur

Vous pouvez modifier ou renouveler les certificats requis pour la connexion en assignant un nouveau certificat dans SafeGuard Management Center. Le certificat est assigné sous la forme d’un certificat de veille en compagnie de celui existant. En se connectant avec le nouveau certificat, l’utilisateur change le certificat sur le terminal.

Remarque :

Si les utilisateurs ont perdu leurs tokens ou si ceux-ci ont été compromis. Ne les échangez pas en assignant de nouveaux certificats comme cela est décrit ici. Sinon, vous pourriez rencontrer des problèmes. Par exemple, l’ancien certificat de token peut être encore valide pour la connexion Windows. Tant que l’ancien certificat est encore valide, la connexion à Windows est toujours possible et l’ordinateur peut être déverrouillé. Au lieu de cela, bloquez le token pour empêcher la connexion.

Les certificats de veille peuvent être utilisés dans les cas suivants :

- Modification des certificats générés par token (cryptographique).
- Passage de certificats générés automatiquement à des certificats générés par token.
- Passage d’une authentification par nom utilisateur/mot de passe à une authentification par token cryptographique (Kerberos).

Conditions préalables :

- Le nouveau token a été généré.
- Seul un certificat est assigné à l’utilisateur.
- Vous avez besoin des droits d’**Accès complet** pour l’utilisateur correspondant.

Pour changer le certificat d’un utilisateur pour la connexion par token :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**.

2. Connectez le token à l’interface USB.

   SafeGuard Enterprise lit le token.

3. Sélectionnez l’utilisateur dont vous voulez changer le certificat et ouvrez l’onglet **Certificat** dans la zone de travail à droite.
4. Dans la barre d’outils, cliquez sur l’icône appropriée pour l’action que vous voulez exécuter.
5. Sélectionnez le certificat concerné et saisissez le code confidentiel du token.
6. Cliquez sur **OK**.
7. Fournissez le nouveau token à l’utilisateur.

Le certificat est assigné à l’utilisateur sous la forme d’un certificat de veille. Ceci est indiqué par une coche dans la colonne **Veille** de l’onglet **Certificats** de l’utilisateur.

Après la synchronisation entre le terminal et le serveur SafeGuard Enterprise, la boîte de dialogue d’état du terminal indique que ce dernier est **Prêt pour la modification du certificat**.

L’utilisateur doit maintenant lancer une modification du certificat sur le terminal. Retrouvez plus de renseignements dans le *Manuel d’utilisation de SafeGuard Enterprise*.

Une fois que l’utilisateur a changé le certificat sur le terminal, le certificat est également renouvelé sur le serveur SafeGuard Enterprise lors de la synchronisation suivante. Cela supprime l’ancien token de l’onglet **Certificats** de l’utilisateur dans SafeGuard Management Center. Le nouveau token devient le token standard pour l’utilisateur.

Remarque : Dans SafeGuard Management Center, les deux certificats peuvent être supprimés séparément. Si un seul certificat de veille est disponible, le certificat suivant est assigné sous la forme d’un certificat de veille.

Importation d’un certificat à partir d’un fichier du token

Condition préalable : le token a été généré.

Vous devez sélectionner cette procédure pour un token avec la prise en charge Kerberos. Le certificat doit être reconnu par SafeGuard Enterprise et ajouté au token. S’il existe déjà un certificat généré automatiquement, le certificat importé le remplacera.

Pour ajouter la partie privée du certificat (fichier .p12) sur le token à partir d’une fichier :

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. Connectez le token à l’interface USB.

SafeGuard Enterprise lit le token.

3. Marquez le token auquel vous voulez ajouter la partie privée du certificat et, dans la zone de travail à droite, ouvrez l'onglet **Informations de connexion et certificats**.
4. Cliquez sur l'icône **P12 à token** dans la barre d'outils de SafeGuard Management Center.
5. Sélectionnez le fichier de certificat concerné.
6. Saisissez le code confidentiel du token et le mot de passe du fichier .p12 et confirmez en cliquant sur **OK**.

La partie privée du certificat est ajoutée au token. À présent, vous devez l'assigner à un utilisateur comme indiqué à la section Assignation de certificats de token à un utilisateur *(page 207)*. Les utilisateurs peuvent alors seulement se connecter avec ce token.

3.8.14.8 Gestion des codes confidentiels

En tant que responsable de la sécurité, vous pouvez changer le code confidentiel de l'utilisateur et celui du responsable de la sécurité et aussi forcer le changement du code confidentiel de l'utilisateur. Ceci est généralement nécessaire lors de la génération d'un token. Vous pouvez également initialiser des codes confidentiels, c'est-à-dire les générer comme de nouveaux codes confidentiels, et les bloquer.

Pour initialiser, changer et bloquer les codes confidentiels, vous avez besoin des droits d'**Accès complet** pour les utilisateurs correspondants.

Vous pouvez utiliser des stratégies pour spécifier d'autres options de code confidentiel pour le terminal.

Remarque : Lorsque vous changez un code confidentiel, certains fabricants de tokens spécifient leurs propres règles de code confidentiel qui peuvent contredire celles de SafeGuard Enterprise. C'est la raison pour laquelle il se peut qu'il ne soit pas possible de changer un code confidentiel comme vous le souhaitez, même s'il respecte les règles des codes confidentiels de SafeGuard Enterprise. Vous devez toujours consulter les règles des codes confidentiels du fabricant de tokens. Elles peuvent être affichées dans la zone **Token** sous **Informations sur le token** dans SafeGuard Management Center.

Les codes confidentiels sont gérés dans SafeGuard Management Center sous **Tokens**. Le token est connecté et coché dans la fenêtre de navigation de gauche.

Initialisation du code confidentiel de l'utilisateur

Conditions préalables :

- Le code confidentiel du responsable de la sécurité doit être connu.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

1. Dans la barre d'outils de SafeGuard Management Center, cliquez sur **Initialiser le code confidentiel de l'utilisateur**.
2. Saisissez le code confidentiel du responsable de la sécurité.
3. Saisissez le nouveau code confidentiel de l'utilisateur, répétez la saisie et confirmez en cliquant sur **OK**.

Le code confidentiel de l'utilisateur est initialisé.

Changement du code confidentiel d'un responsable de la sécurité

Condition préalable : Le code confidentiel du responsable de la sécurité précédent doit être connu.

1. Dans la barre d'outils de SafeGuard Management Center, cliquez sur l'icône **Changer le code confidentiel RS**.
2. Saisissez l'ancien code confidentiel du responsable de la sécurité.
3. Saisissez le nouveau code confidentiel du responsable de la sécurité, répétez la saisie et cliquez sur **OK**.

Le code confidentiel du responsable de la sécurité a été modifié.

Changement d'un code confidentiel de l'utilisateur

Condition préalable :

- Le code PIN de l'utilisateur doit être connu.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

1. Dans la barre d'outils de SafeGuard Management Center, cliquez sur l'icône **Changer le code confidentiel de l'utilisateur**.
2. Saisissez l'ancien et le nouveau code confidentiels de l'utilisateur, répétez la saisie du nouveau et confirmez en cliquant sur **OK**.

Le code confidentiel de l'utilisateur est changé. Si vous avez changé le code confidentiel d'un autre utilisateur, informez-le de cette modification.

Changement forcé du code confidentiel

Pour forcer le changement d'un code confidentiel, vous avez besoin des droits d'**Accès complet** pour l'utilisateur concerné.

Dans la barre d’outils de SafeGuard Management Center, cliquez sur **Forcer le changement du code confidentiel**.

Lors de la prochaine connexion de l’utilisateur avec le token, il doit changer son code confidentiel.

Historique des codes confidentiels

L'historique des codes confidentiels peut être supprimé. Pour cela, cliquez sur l'icône **Supprimer l'historique du code confidentiel** de la barre d'outils de SafeGuard Management Center.

3.8.14.9 Gestion des tokens et des cartes à puce

Dans la zone **Tokens** de SafeGuard Management Center, le responsable de la sécurité peut :

- Avoir un aperçu des tokens et des certificats qui ont été générés.
- Filtrer des aperçus.
- Bloquer les tokens pour authentification.
- Lire ou supprimer les données sur un token.

Affichage des informations du token/carte à puce

En tant que responsable de la sécurité, vous pouvez afficher des informations sur tous les tokens ou sur certains tokens ayant été générés. Vous pouvez aussi filtrer les aperçus.

Condition préalable : le token doit être connecté.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. Pour afficher des informations sur un token individuel, sélectionnez le token correspondant dans la zone de navigation sous **Connecteurs de tokens**.

   Le fabricant, le type, le numéro de série, les données matérielles et les règles des codes confidentiels sont affichés sous **Informations sur le token**. Vous pouvez également voir à quel utilisateur le token est assigné.

   Remarque : Sous **Connecteurs de tokens**, les tokens générés apparaissent quels que soient vos droits d’accès aux utilisateurs concernés. Vous pouvez ainsi voir si le token est en cours d’utilisation ou non. Si vous n’avez pas de droits d’accès en **Lecture seule** à l’utilisateur assigné, toutes les données sur les tokens dans les onglets **Informations sur le token** et **Informations d’identification et certificats** sont grisées et vous ne pouvez pas gérer ce token.

3. Pour afficher un aperçu des tokens, sélectionnez **Tokens générés**. Vous pouvez afficher toutes les cartes à puce ayant été générées ou filtrer l’aperçu par utilisateur.

Le numéro de série du token, les utilisateurs assignés et la date de création sont affichés. Vous pouvez également voir si le token est bloqué.

Remarque : La vue **Tokens générés** n'affiche que les tokens des utilisateurs pour qui vous avez des droits en **Lecture seule** ou d'**Accès complet**.

Blocage d'un token ou d'une carte à puce

Si vous êtes responsable de la sécurité, vous pouvez bloquer des tokens. C'est utile, par exemple, si un token a été perdu.

Pour bloquer un token, vous avez besoin des droits d'**Accès complet** pour l'utilisateur concerné.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. Dans la zone de navigation de gauche, sélectionnez **Tokens générés** à gauche de la zone de navigation.
3. Sélectionnez le token à bloquer et cliquez sur l'icône **Bloquer le token** de la barre d'outils de SafeGuard Management Center.

Le token est bloqué pour l'authentification et l'utilisateur assigné ne peut plus l'utiliser pour se connecter. Le token ne peut être débloqué qu'en utilisant le code confidentiel du responsable de la sécurité.

Suppression des informations du token/carte à puce

En tant que responsable de la sécurité, vous pouvez supprimer les informations écrites sur le token par SafeGuard Enterprise.

Condition préalable :

- le token doit être connecté.
- Vous avez besoin des droits d'**Accès complet** pour l'utilisateur correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. Dans la zone de navigation de gauche, sélectionnez la carte à puce concernée sous **Cartes à puce générées**.
3. Dans la barre d'outils de SafeGuard Management Center, cliquez sur **Effacer la clé**.
4. Saisissez le code confidentiel du responsable de la sécurité qui a été assigné au token et confirmez en cliquant sur **OK**.

Toutes les données gérées par SafeGuard Enterprise sont supprimées. Les certificats restent sur le token.

Le code confidentiel de l’utilisateur est réinitialisé à 1234.

les tokens effacés sont ainsi automatiquement supprimées de la liste des tokens générés.

Lecture des informations de token/carte à puce

En tant que responsable de la sécurité, vous pouvez lire les données sur le token à l'aide du code confidentiel de l'utilisateur.

Condition préalable :

- Le token doit être connecté. Le responsable de la sécurité doit connaître le code confidentiel. Ou il doit être initialisé comme indiqué à la section Initialisation du code confidentiel de l’utilisateur *(page 210)*.
- Vous avez besoin des droits en **Lecture seule** ou d’**Accès complet** pour l'utilisateur correspondant.

1. Dans SafeGuard Management Center, cliquez sur **Tokens**.
2. À gauche de la zone de navigation, sélectionnez le token approprié sous **Connecteurs de tokens** et sélectionnez l'onglet **Codes d'accès & certificats**.
3. Cliquez sur l'icône **Obtenir les codes d'accès utilisateur** et saisissez le code confidentiel de l'utilisateur du token.

Les données du token s'affichent.

3.8.15 Planification des tâches

SafeGuard Management Center contient le **Planificateur de tâches** pour créer et planifier des tâches périodiques basées sur des scripts. Les tâches sont automatiquement exécutées par un service sur le serveur SafeGuard Enterprise pour exécuter les scripts spécifiées.

Les tâches périodiques sont, par exemple, utiles pour

- la synchronisation automatique entre Active Directory et SafeGuard Enterprise.
- la suppression automatique des journaux d’événements.

Pour ces deux procédures, des modèles de script prédéfinis sont disponibles avec SafeGuard Enterprise. Vous pouvez utiliser ces scripts tels quels ou les modifier en fonction de vos besoins. Retrouvez plus de renseignements à la section Scripts prédéfinis pour les tâches périodiques *(page 222)*.

En tant que responsable de la sécurité avec les droits nécessaires, vous pouvez indiquer des scripts, des règles et des intervalles pour les tâches dans le **Planificateur des tâches**.

Remarque : Assurez-vous que les autorisations SQL appropriées sont définies pour le compte qui sert à exécuter le **Planificateur de tâches** SafeGuard Enterprise. Retrouvez plus de renseignements dans l'article 113582 de la base de connaissances de Sophos.

Remarque : L'API ne peut pas traiter plus d'une tâche à la fois. L'utilisation de plus d'un compte par tâche entraînera des problèmes de violations d'accès de la base de données.

3.8.15.1 Création d'une nouvelle tâche

Pour créer des tâches dans le **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** s'affiche.

2. Cliquez sur **Créer...**.

   La boîte de dialogue **Nouvelle tâche** apparaît.

3. Dans le champ **Nom**, saisissez un nom de tâche unique.

   Si le nom de tâche n'est pas unique, un avertissement apparaît lorsque vous cliquez sur **OK** pour enregistrer la tâche.

4. Dans la liste déroulante du champ **Serveur SGN**, sélectionnez le serveur sur lequel la tâche doit fonctionner.

   La liste déroulante affiche seulement les serveurs pour lesquels la création de scripts est autorisée. Vous autorisez la création de scripts pour une serveur donné lorsque vous l'enregistrez dans l'**Outil de package de configuration** dans SafeGuard Management Center.

   Si vous sélectionnez **Aucune**, la tâche n'est pas exécutée.

5. Cliquez sur le bouton **Importer...** près du champ **Script**.

   La boîte de dialogue **Sélectionner le fichier de script à importer** apparaît.

   Remarque : Deux scripts prédéfinis sont disponibles dans le répertoire Script Templates de l'installation de votre installation de SafeGuard Management Center. La boîte de dialogue

Sélectionner le fichier script à importer montre automatiquement ce répertoire. Retrouvez plus de renseignements à la section Scripts prédéfinis pour les tâches périodiques *(page 222)*.

Dans le **Planificateur de tâches**, vous pouvez importer, exporter et modifier des scripts. Retrouvez plus de renseignements à la section Utilisation de scripts dans le Planificateur de tâches *(page 220)*.

6. Sélectionnez le script que vous voulez exécuter avec la tâche et cliquez sur **OK**.

   Si le script sélectionné est vide, le bouton **OK** dans la boîte de dialogue reste désactivée et un avertissement apparaît.

7. Dans le champ **Heure de début**, indiquez quand la tâche doit être exécutée sur le serveur sélectionnée.

   L'heure de début affichée est rendue à l'aide de l'heure locale de l'ordinateur sur lequel fonctionne SafeGuard Management Center. En interne, l'heure de début est stockée en temps universel coordonné (UTC, Coordinated Universal Time). Ceci permet l'exécution de tâches au même moment, même si les serveurs sont dans différents fuseaux horaires. Tous les serveurs utilisent l'heure courante du serveur de base de données pour déterminer quand démarrer les tâches. Pour permettre une meilleure surveillance des tâches, l'heure de référence de la base de données apparaît dans la boîte de dialogue **Planificateur de tâches**.

8. Sous **Périodicité**, indiquez à quelle fréquence la tâche doit être exécutée sur le serveur sélectionné.

   - Pour exécuter la tâche une fois, sélectionnez **Une seule fois** et indiquez la **Date** requise.
   - Pour exécuter la tâche tous les jours, sélectionnez **Quotidien** suivi de **Chaque jour (y compris le samedi et le dimanche)** ou **Chaque jour de la semaine (du lundi au vendredi)**.
   - Pour exécuter la tâche de façon hebdomadaire, sélectionnez **Hebdomadaire** et indiquez le jour de la semaine de votre choix.
   - Pour exécuter la tâche de façon mensuelle, sélectionnez **Mensuel** et indiquez le jour requis du mois dans une plage de 1 à 31. Pour exécuter la tâche à la fin de chaque mois, sélectionnez **Dernier** dans la liste déroulante.

   Après avoir rempli tous les champs obligatoires, le bouton **OK** devient disponible.

9. Cliquez sur **OK**.

La tâche est enregistrée dans la base de données et apparaît dans l'aperçu du **Planificateur de tâches**. Elle est exécutée sur le serveur sélectionné en fonction de la planification indiquée.

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

3.8.15.2 Affichage de l’aperçu du Planificateur de tâches

Après avoir créé des tâches à exécuter sur un serveur SafeGuard Enterprise, elles apparaissent dans la boîte de dialogue **Planificateur de tâches** que vous ouvrez en sélectionnant **Outils > Planificateur de tâches**.

Cette boîte de dialogue affiche pour chaque tâche les colonnes suivantes :

Colonne	Description
Nom de la tâche	Affiche le nom unique de la tâche.
Serveur SGN	Indique sur quel serveur la tâche est exécutée.
Planification	Afficher le programme spécifié pour la tâche avec la récurrence et l’heure.
Heure de la prochaine exécution	Affiche quand la prochaine exécution de la tâche aura lieu (date et heure). S’il n’existe plus d’heures d’exécution de cette tâche, cette colonne affiche **Aucune**.
Heure de la dernière exécution	Affiche quand la dernière exécution de la tâche aura lieu (date et heure). Si elle n’a pas encore été exécutée, cette colonne affiche **Aucune**.
Résultat de la dernière exécution	Affiche le résultat de la dernière tâche exécutée : • **Succès** Le script de la tâche a été exécuté avec succès. • **Échec** L’exécution de la tâche a échoué. Un numéro d’erreur apparaît, s’il est disponible. • **En cours d’exécution** Le script est en cours d’exécution. • **Droits insuffisants** La tâche a échoué à cause de droits insuffisants pour l’exécution de scripts. • **Abandonné**

Colonne	Description
	L’exécution de la tâche a été abandonnée car la durée d’exécution a dépassé 24 heures. • **Contrôle perdu** Le contrôle de l’exécution du script de la tâche a été perdu, par exemple parce que le service du planificateur SGN a été arrêté. • **Script corrompu** Le script à exécuter est corrompu. • **Le script a été supprimé entre-temps** Alors que la tâche était placée dans la file d’attente pour exécution, le script correspondant a été supprimé de la base de données SafeGuard Enterprise. • **Erreurs runtime** Une erreur runtime a été détectée lors du traitement du service du planificateur.

Sous les colonnes, les boutons suivants apparaissent :

Bouton	Description
Créer...	Cliquez sur ce bouton pour créer une nouvelle tâche.
Supprimer	Cliquez sur ce bouton pour supprimer une tâche sélectionnée.
Propriétés	Cliquez sur ce bouton pour afficher la boîte de dialogue **Propriétés de <nom de tâche>** d’une tâche sélectionnée. Dans cette boîte de dialogue, vous pouvez modifier la tâche ou importer, exporter et modifier des scripts.
Rafraîchir	Cliquez sur ce bouton pour rafraîchir la liste des tâches dans la boîte de dialogue **Planificateur de tâches**. Si un autre utilisateur a entre-temps ajouté ou supprimé des tâches, la liste est mise à jour.

Tous les serveurs utilisent l’heure courante du serveur de base de données pour déterminer quand démarrer les tâches. Ainsi, pour une meilleure surveillance des tâches, l’heure du serveur de base de données apparaît ici. Il apparaît avec l’heure locale de l’ordinateur sur lequel fonctionne SafeGuard Management Center.

3.8.15.3 Modification de tâches

Pour modifier des tâches dans le **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

   La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Effectuez les changements requis.

   Remarque : Ce nom de tâche doit être unique. Si vous changez le nom en un nom de tâche existant, un message d’erreur apparaît.

4. Cliquez sur **OK**.

Les changements deviennent effectifs.

3.8.15.4 Suppression de tâches

Pour supprimer des tâches du **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise.

   Le bouton **Supprimer** devient disponible.

3. Cliquez sur le bouton **Supprimer** et confirmez que vous voulez supprimer la tâche.

La tâche est supprimée de la boîte de dialogue de l'aperçu du **Planificateur de tâches** et ne sera plus exécutée sur le serveur SafeGuard Enterprise.

Remarque : Si la tâche a été démarrée entre-temps, elle est supprimée de la boîte de dialogue de l'aperçu du **Planificateur de tâches**, mais sera tout de même achevée.

3.8.15.5 Utilisation de scripts dans le Planificateur de tâches

Avec le **Planificateur de tâches**, vous pouvez importer, modifier et exporter des scripts. Pour utiliser les scripts dans le **Planificateur de tâches**, vous avez besoin des droits du responsable de la sécurité **Utiliser le planificateur de tâches** et **Gérer les tâches**.

Importation de scripts

Pour spécifier un script à exécuter par une tâche, le script doit être importé. Vous pouvez importer le script lorsque vous créez la tâche pour la première fois. Vous pouvez aussi importer des scripts pour les tâches existantes.

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

   La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Cliquez sur le bouton **Importer...** près du champ **Script**.

   La boîte de dialogue **Sélectionner le fichier de script à importer** apparaît.

   Remarque : Deux scripts prédéfinis sont disponibles dans le répertoire Script Templates de l'installation de votre installation de SafeGuard Management Center. La boîte de dialogue **Sélectionner le fichier script à importer** montre automatiquement ce répertoire. Retrouvez plus de renseignements à la section Scripts prédéfinis pour les tâches périodiques *(page 222)*.

4. Sélectionnez le script que vous voulez importer et cliquez sur **OK**.

   Le nom du script apparaît dans le champ **Script**.

5. Cliquez sur **OK**.

Si le script a déjà été importé, vous êtes invité à confirmer que vous voulez remplacer l’ancien script.

Si la taille du fichier à importer dépasse 10 Mo, un message d’erreur apparaît et le processus d’importation est rejeté.

Le script est enregistré dans la base de données.

Modification de scripts

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

   La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Cliquez sur le bouton déroulant **Modifier** près du champ **Script**.

   La liste déroulante montre tous les éditeurs disponibles pour la modification du script.

4. Sélectionnez l’éditeur que vous souhaitez utiliser.

   Le script s’ouvre dans l’éditeur sélectionné.

5. Effectuez vos changements et enregistrez-les.

   L’éditeur est fermé et la boîte de dialogue **Propriétés de <nom de tâche>** réapparaît.

6. Cliquez sur **OK**.

Le script changé est enregistré dans la base de données.

Exportation de scripts

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Planificateur de tâches**.

   La boîte de dialogue **Planificateur de tâches** apparaît montrant un aperçu des tâches planifiées.

2. Sélectionnez la tâche requise et cliquez sur le bouton **Propriétés**.

La boîte de dialogue **Propriétés de <nom tâche>** apparaît avec les propriétés de la tâche.

3. Cliquez sur le bouton **Exporter...** près du champ **Script**.

   Une boîte de dialogue **Enregistrer sous** apparaît.

4. Sélectionnez l'emplacement du fichier pour l'enregistrement du script et cliquez sur **Enregistrer**.

   Le script est enregistré à l'emplacement de fichier spécifié.

Scripts prédéfinis pour les tâches périodiques

Les scripts prédéfinis suivants sont disponibles avec SafeGuard Enterprise :

- ActiveDirectorySynchronization.vbs

  Vous pouvez utiliser ce script pour la synchronisation automatique entre Active Directory et SafeGuard Enterprise.

- EventLogDeletion.vbs

  Vous pouvez utiliser ce script pour supprimer automatiquement les journaux d'événements.

Les scripts sont installés automatiquement dans le sous-dossier Script Templates de l'installation de SafeGuard Management Center.

Pour utiliser ces scripts lors de tâches quotidiennes, importez-les dans le **Planificateur de tâches** et apportez les changements de paramètres nécessaires avant de les utiliser.

Script prédéfini pour la synchronisation avec Active Directory

Vous pouvez importer une structure organisationnelle existante dans la base de données SafeGuard Enterprise depuis un Active Directory. Retrouvez plus de renseignements à la section Synchronisation de la structure organisationnelle *(page 164)*.

Après avoir importé la structure du répertoire, vous pouvez planifier une tâche périodique de synchronisation automatique entre l'Active Directory et SafeGuard Enterprise. Pour cette tâche, vous pouvez utiliser le script prédéfini ActiveDirectorySynchronization.vbs.

Le script synchronise tous les conteneurs existants dans la base de données SafeGuard Enterprise avec un Active Directory.

Avant que nous n'utilisiez le script dans une tâche périodique, vous pouvez modifier les paramètres suivants :

Paramètre	Description
logFileName	Indiquez un chemin pour le fichier journal du script. Ce paramètre est obligatoire. S'il est laissé vide ou incorrect, la synchronisation ne fonctionne pas et un message d'erreur apparaît. Par défaut, ce paramètre est vide. Si un fichier journal existe déjà, de nouveaux journaux sont ajoutés à la fin du fichier.
synchronizeMembership	Définissez ce paramètre sur 1 pour également synchroniser les appartenances. Si ce paramètre est défini sur 0, les appartenances ne sont pas synchronisées. Le paramètre par défaut est 1.
synchronizeAccountState	Définissez ce paramètre sur 1 pour également synchroniser l'état activé par l'utilisateur. Si ce paramètre est défini sur 0, l'état activé par l'utilisateur est seulement synchronisé à la première synchronisation. Le paramètre par défaut est 0.

Remarque :

Assurez-vous d'avoir les droits d'accès nécessaires pour la synchronisation Active Directory et que les autorisations SQL appropriées sont définies pour le compte utilisé pour exécuter le **Planificateur de tâches** SafeGuard Enterprise. Retrouvez plus de renseignements à la section Droits d'accès du responsable de la sécurité et importation Active Directory *(page 162)*. Retrouvez plus de renseignements sur la définition des droits d'accès Active Directory dans l'article 107979 de la base de connaissances de Sophos. Retrouvez plus de renseignements sur la définition des autorisations SQL dans l'article 113582 de la base de connaissances de Sophos.

Une fois les droits définis correctement, appliquez les changements et redémarre le service : Passez sur le serveur hébergeant la page Web SafeGuard Enterprise. Ouvrez l'interface **Services** en cliquant sur **Démarrer > Exécuter > Services.msc**. Cliquez avec le bouton droit de la souris sur **Service du planificateur SafeGuard ®** et cliquez sur **Toutes les tâches > Redémarrer**.

Nous vous conseillons de synchroniser l'Active Directory à intervalles modérés, deux fois par jour maximum afin que les performances du serveur ne soient pas trop diminuées. Les nouveaux objets apparaîtront dans SafeGuard Management Center sous .Enregistré automatiquement entre ces intervalles où ils peuvent être administrés normalement.

Script prédéfini pour la suppression automatique des journaux d'événements

Les événements journalisés dans la base de données SafeGuard Enterprise sont stockés dans le tableau EVENT. Pour plus d'informations sur la journalisation, reportez-vous à la section Rapports *(page 228)*.

Avec le **Planificateur de tâches**, vous pouvez créer une tâche périodique pour supprimer automatiquement les journaux d'événements. Pour cette tâche, vous pouvez utiliser le script prédéfini EventLogDeletion.vbs.

Le script supprime les événements du tableau EVENT. Si vous spécifiez le paramètre approprié, il déplace par ailleurs les événements dans le tableau de journalisation de sauvegarde EVENT_BACKUP en laissant un nombre prédéfini d'événements récents dans le tableau EVENT.

Avant que nous n'utilisiez le script dans une tâche périodique, vous pouvez modifier les paramètres suivants :

Paramètre	Description
maxDuration	Avec ce paramètre, indiquez combien de temps (en jours) les événements doivent être conservés dans le tableau EVENT. Le nombre par défaut est 0. Si ce paramètre est défini sur 0, il n'y a pas de délai pour les événements conservés dans le tableau EVENT.
maxCount	Avec ce paramètre, indiquez combien d'événements doivent rester dans le tableau EVENT. Le nombre par défaut est 5000. Si ce paramètre est défini sur 0, il n'y a pas de limite au nombre d'événements à conserver dans le tableau EVENT.
keepBackup	Avec ce paramètre, indiquez si les événements supprimés doivent être sauvegardés dans le tableau EVENT. Le nombre par défaut est 0. Si ce paramètre est défini sur 0, les événements ne sont pas sauvegardés. Définissez ce paramètre sur 1 pour créer une sauvegarde des événements supprimés.

Remarque :

Si vous utilisez le script pour déplacer des événements du tableau EVENT dans le tableau de journalisation de sauvegarde, la connexion des événements ne s'applique plus. Pour activer la connexion aux événements tout en utilisant la procédure enregistrée pour le nettoyage des événements est inutile. Retrouvez plus de renseignements à la section Connexion des événements journalisés *(page 236)*.

3.8.15.6 Restrictions concernant les serveurs enregistrés

Lorsque vous enregistrez des serveurs dans l'**Outil de package de configuration** de SafeGuard Management Center, vous pouvez enregistrer plus d'un modèle de serveur avec le même certificat de machine. Mais vous pouvez seulement installer un modèle à la fois sur la machine réelle.

Si la case à cocher **Scripts autorisés** est sélectionnée pour les deux serveurs, le **Planificateur de tâches** affiche les deux serveurs pour sélection dans la liste déroulante **Serveur SGN** des boîtes de

dialogue **Nouvelle tâche** et **Propriétés de <nom de tâche>**. Le **Planificateur de tâches** ne peut pas déterminer lequel des deux modèles a été installé sur la machine.

Pour éviter cela, ne sélectionnez pas la case à cocher **Scripts autorisés** pour les modèles qui ne sont pas installés sur le serveur. Évitez aussi les modèles dupliqués avec le même certificat de machine.

Retrouvez plus de renseignements sur l'enregistrement des serveurs à la section Enregistrement et configuration du serveur SafeGuard Enterprise *(page 55)*.

3.8.16 Audit

Journalisation des événements pour BitLocker

Les événements signalés par le client BitLocker sont consignés dans le journal de la même manière que pour tout autre client SafeGuard Enterprise. Il n'est pas expressément indiqué que l'événement est lié à un client BitLocker. Les événements signalés sont identiques pour tout client SafeGuard Enterprise.

Journalisation des événements pour la restauration à l'aide de l'ID de la clé de restauration BitLocker

Un événement est journalisé lorsque l'ID de la clé de récupération BitLocker est affichée au responsable de la sécurité (événement 2088).

Journalisation des événements du chiffrement asynchrone

Les événements sont journalisés lorsque :

- Le chiffrement asynchrone a chiffré un fichier (événement 3018)
- Le chiffrement asynchrone a déchiffré un fichier (événement 3019)

Vous pouvez consulter la liste de ces événements dans SafeGuard Management Center sous **Rapports** dans l'observateur d'événements.

Événements de journalisation pour les utilisateurs non confirmés

Les événements sont journalisés lorsque :

- Les utilisateurs sont ajoutés au groupe **.Utilisateurs non confirmés** (événement 2801)
- Les utilisateurs ont été confirmés (événement 2800)

- L'option **Confirmer automatiquement les utilisateurs qui ne peuvent pas être authentifiés par Active Directory** est activée (événement 2802)

- L’option **Confirmer automatiquement les utilisateurs qui ne peuvent pas être authentifiés par Active Directory** est désactivée (événement 2803)

- Les utilisateurs ont été confirmés automatiquement (événement 2804)

Vous pouvez consulter la liste de ces événements dans SafeGuard Management Center sous **Rapports** dans l’observateur d’événements.

Journalisation des événements pour la suppression des domaines, des nœuds UO et des groupes de travail

Les événements sont journalisés lorsque :

- L’option **Empêcher la suppression des domaines, des nœuds UO et des groupes de travail** est activée. Le message affiche le responsable de la sécurité qui l’a activée (événement 2805).

- L’option **Empêcher la suppression des domaines, des nœuds UO et des groupes de travail** est désactivée. Le message affiche le responsable de la sécurité qui l’a désactivée (événement 2806).

Vous pouvez consulter la liste de ces événements dans SafeGuard Management Center sous **Rapports** dans l’observateur d’événements.

Événements de journal pour les utilisateurs, ordinateurs ou groupes de travail

Les inscriptions réussies ou non des utilisateurs, des ordinateurs ou des groupes de travail sont consignées dans le journal. Vous pouvez consulter la liste de ces événements dans SafeGuard Management Center sous **Rapports** dans l’observateur d’événements.

Journalisation des événements pour la désactivation/activation du déploiement de la stratégie

Les événements sont journalisés lorsque :

- Le déploiement de la stratégie est désactivé par le responsable de la sécurité. Le message affiche le responsable de la sécurité qui a désactivé le déploiement de la stratégie (événement 2770).
- Le déploiement de la stratégie est activé par le responsable de la sécurité. Le message affiche le responsable de la sécurité qui a activé le déploiement de la stratégie (événement 2771).
- Le déploiement de la stratégie est désactivé par la gestion des licences (événement 2773). Raisons possibles :
    - Licences non valides

    - Licence expirée
    - Dépassement du nombre de licences
- Le déploiement de la stratégie est activé par la gestion des licences (événement 2771).

Vous pouvez consulter la liste de ces événements dans SafeGuard Management Center sous **Rapports** dans l'observateur d'événements.

Événements de journal pour les listes de compte de service

Les actions accomplies concernant les listes de comptes de service sont signalées par les événements du journal suivants :

SafeGuard Management Center

- Liste de comptes de service <nom> créée
- Liste de comptes de service <nom> modifiée
- Liste de comptes de service <nom> supprimée

Terminaux protégés par SafeGuard Enterprise

- Utilisateur Windows <nom domaine/utilisateur> connecté à <horodatage> sur le poste <nom domaine/poste de travail> avec un compte de service SGN.
- Nouvelle liste de comptes de service <nom> importée.
- Liste de comptes de service <nom> supprimée.

Journalisation des événements pour le Planificateur de tâches

Les événements concernant l'exécution des tâches peuvent être journalisés pour fournir des informations utiles, par exemple pour la résolution des problèmes. Vous pouvez définir les événements suivants à journaliser :

- La tâche du planificateur s'est exécutée avec succès
- La tâche du planificateur a échoué
- Le fil du service du planificateur s'est arrêté à cause d'une exception.

Les événements incluent les résultats de la console de scripts pour faciliter la résolution des problèmes.

Retrouvez plus de renseignements sur la journalisation à la section Rapports *(page 228)*.

Suivi de fichiers dans le stockage Cloud

Vous pouvez suivre l'état des fichiers accédés dans le stockage Cloud à l'aide de la fonction **Rapports** de SafeGuard Management Center. Les fichiers accédés peuvent faire l'objet d'un suivi quelle que soit la stratégie de chiffrement qui leur est appliquées.

Dans une stratégie de type **Journalisation**, vous pouvez définir ce qui suit :

- Consigner dans le journal un événement lorsqu'un fichier ou un répertoire est créé sur un périphérique amovible.
- Consigner dans le journal un événement lorsqu'un fichier ou un répertoire est renommé sur un périphérique amovible.
- Consigner dans le journal un événement lorsqu'un fichier ou un répertoire est supprimé sur un périphérique amovible.

Retrouvez plus de renseignements à la section Rapport d'accès aux fichiers sur les supports amovibles et dans le stockage Cloud *(page 234)*.

Suivi de fichiers sur supports amovibles

Vous pouvez réaliser un suivi des fichiers accessibles sur les supports amovibles à l'aide de la fonction **Rapports** de SafeGuard Management Center. Les fichiers accédés peuvent faire l'objet d'un suivi quelle que soit la stratégie de chiffrement appliquée aux fichiers sur les supports amovibles.

Dans une stratégie de type **Journalisation**, vous pouvez définir ce qui suit :

- Un événement à consigner dans le journal lorsqu'un fichier ou un répertoire est créé sur un support amovible.
- Un événement à consigner dans le journal lorsqu'un fichier ou un répertoire est renommé sur un support amovible.
- Un événement à consigner dans le journal lorsqu'un fichier ou un répertoire est supprimé d'un support amovible.

Retrouvez plus de renseignements à la section Rapport d'accès aux fichiers sur les supports amovibles et dans le stockage Cloud *(page 234)*.

3.8.16.1 Rapports

La possibilité de signaler des incidents liés à la sécurité est une condition préalable à une analyse détaillée du système. Les événements journalisés facilitent le suivi exact des processus sur une station de travail donnée ou dans un réseau. En journalisant les événements, vous pouvez par exemple vérifier les atteintes à la sécurité commises par de tiers. À l'aide des fonctionnalités de

journalisation, les administrateurs et responsables de la sécurité peuvent aussi détecter les erreurs dans l'affectation de droits utilisateur et les corriger.

SafeGuard Enterprise journalise toutes les activités et informations de l'état du terminal, ainsi que les actions de l'administrateur et les événements liés à la sécurité, puis les enregistre de manière centralisée. Les fonctionnalités de journalisation enregistrent les événements déclenchés par les produits SafeGuard installés. Le type de journaux est défini dans les stratégies du type **Journalisation**. C'est aussi où vous spécifiez le résultat et l'emplacement de sauvegarde des événements journalisés : le journal des événements Windows du terminal ou la base de données SafeGuard Enterprise.

En tant que responsable de la sécurité disposant des droits nécessaires, vous pouvez afficher, imprimer et archiver les informations d'état et les rapports de journaux affichés dans SafeGuard Management Center. SafeGuard Management Center propose des fonctions de tri et de filtrage complètes très utiles lors de la sélection d'événements pertinents à partir des informations disponibles.

Des analyses automatiques de la base de données de journaux, par exemple avec Crystal Reports ou Microsoft System Center Operations Manager, sont également possibles. SafeGuard Enterprise protège les entrées des journaux contre toute manipulation non autorisée à l'aide de signatures sur le client et sur le serveur.

En fonction de la stratégie de journalisation, les événements des catégories suivantes peuvent être journalisés :

- Authentification
- Administration
- Système
- Chiffrement
- Client
- Contrôle d'accès

- Pour **SafeGuard Data Exchange**, vous pouvez avoir un suivi des fichiers accédés sur les supports amovibles en journalisant les événements correspondants. Retrouvez plus de renseignements sur ce type de rapport à la section Rapport d'accès aux fichiers sur les supports amovibles et dans le stockage Cloud *(page 234)*.

- Pour **SafeGuard Cloud Storage**, vous pouvez avoir un suivi des fichiers accédés dans le stockage Cloud en journalisant les événements correspondants. Retrouvez plus de renseignements sur ce type de rapport à la section Rapport d'accès aux fichiers sur les supports amovibles et dans le stockage Cloud *(page 234)*.

Condition préalable

Les événements sont gérés par le serveur SafeGuard Enterprise. Si vous voulez activer les rapports sur les ordinateurs sur lesquels aucun client SafeGuard Enterprise n'est installé (ordinateurs

SafeGuard Management Center ou serveur SafeGuard Enterprise), veuillez-vous assurer que ces événements sont envoyés au serveur SafeGuard Enterprise. Vous allez donc devoir installer un package de configuration client sur l'ordinateur. Ainsi, l'ordinateur est activé en tant que client sur le serveur SafeGuard Enterprise et les fonctionnalités de journalisation Windows ou SafeGuard Enterprise sont activées.

Retrouvez plus de renseignements sur les packages de configuration du client à la section Utilisation des packages de configuration *(page 102)*.

Scénarios d'application

Les fonctionnalités de journalisation de SafeGuard Enterprise constituent une solution conviviale et complète pour l'enregistrement et l'analyse des événements. Les exemples suivants illustrent des scénarios d'application types des **Rapports** de SafeGuard Enterprise.

Contrôle centralisé des ordinateurs d'extrémité d'un réseau

Le responsable de la sécurité souhaite être régulièrement informé des événements critiques (accès non autorisé aux données, nombre d'échecs de tentatives de connexion sur une période spécifiée, par exemple). Grâce à une stratégie de journalisation, le responsable de la sécurité peut configurer la journalisation dans un fichier journal local de processus afin de journaliser tous les événements liés à la sécurité survenus sur les ordinateurs d'extrémité. Ce fichier journal est transféré dans la base de données SafeGuard Enterprise via le serveur SafeGuard Enterprise une fois atteint un certain nombre d'événements. Le responsable de la sécurité peut récupérer, afficher et analyser les événements dans l'**Observateur d'événements** de SafeGuard Management Center. Les processus exécutés sur différents terminaux peuvent ainsi faire l'objet d'un audit sans intervention du personnel sur la journalisation.

Surveillance des utilisateurs mobiles

Les utilisateurs mobiles ne sont généralement pas connectés en permanence au réseau de l'entreprise. Par exemple, les commerciaux déconnectent leur portable pendant une réunion. Dès qu'ils se reconnectent au réseau, les événements SafeGuard Enterprise journalisés pendant la période hors ligne sont transférés. Les fonctionnalités de journalisation proposent une vue d'ensemble précise des activités de l'utilisateur pendant la période de déconnexion de l'ordinateur.

Destinations des événements journalisés

Il y a deux destinations possibles pour les événements journalisés : l'Observateur d'événements Windows ou la base de données SafeGuard Enterprise. Seuls les événements liés à un produit SafeGuard sont inscrits à la destination correspondante.

Les destinations de sortie des événements à journaliser sont spécifiées dans la stratégie de journalisation.

Observateur d’événements Windows

Les événements pour lesquels vous définissez l’Observateur d’événements Windows comme destination dans la stratégie de journalisation sont journalisés dans l’Observateur d’événements Windows. L’Observateur d’événements Windows peut être utilisée pour afficher et gérer les journaux des événements liés au système, à la sécurité et à l’application. Vous pouvez également enregistrer ces journaux d’événements. Un compte administrateur sur l’ordinateur d’extrémité concerné est requis pour ces procédures. Dans l’Observateur d’événements Windows, un code d’erreur s’affiche à la place d’un texte descriptif de l’événement.

Une condition préalable à l’affichage des événements SafeGuard Enterprise dans l’Observateur d’événements Windows consiste à avoir installé un package de configuration client sur le terminal.

Ce chapitre décrit les processus d’affichage, de gestion et d’analyse des journaux d’événements dans SafeGuard Management Center. Retrouvez plus de renseignements sur l’Observateur d’événements Windows dans votre documentation Microsoft.

Base de données SafeGuard Enterprise

Les événements pour lesquels vous définissez la base de données SafeGuard Enterprise comme destination dans la stratégie de journalisation sont collectés dans un fichier journal local dans le cache local de l’ordinateur d’extrémité concerné dans le répertoire suivant : auditing\SGMTranslog. Les fichiers journaux sont soumis à un mécanisme de transport qui les transfère dans la base de données via le serveur SafeGuard Enterprise. Par défaut, le fichier est soumis dès que le mécanisme de transport a établi une connexion avec le serveur. Pour limiter la taille d’un fichier journal, vous pouvez définir un nombre maximal d’entrées du journal dans une stratégie du type **Paramètres généraux**. Le fichier journal est soumis dans la file d’attente de transport du serveur SafeGuard Enterprise une fois le nombre d’entrées spécifié atteint. Les événements journalisés dans la base de données centrale peuvent être affichés dans l’**Observateur d’événements** ou dans l’**Observateur de suivi des fichiers** de SafeGuard Enterprise. En tant que responsable de la sécurité, vous devez disposer des droits appropriés pour afficher, analyser et gérer les événements journalisés dans la base de données.

Configuration des paramètres de journalisation

Les paramètres de rapport sont définis à l’aide de deux stratégies :

- Stratégie **Paramètres généraux**

  Dans une stratégie **Paramètres généraux**, vous pouvez spécifier un nombre maximum d’entrées journalisées au-delà duquel le fichier journal contenant les événements destinés à la base de données centrale doit être transféré dans la base de données de SafeGuard Enterprise. Ceci permet de réduire la taille des fichiers journaux individuels à transférer. Ce paramètre est facultatif.

- Stratégie **Journalisation**

  Les événements à journaliser sont spécifiés dans une stratégie de journalisation. Dans cette stratégie, un responsable de la sécurité avec les droits de stratégie requis définit quels événements seront journalisés et dans quelle destination en sortie.

Définition du nombre d'événements pour commentaires

1. Cliquez sur **Rapports** dans SafeGuard Management Center.
2. Créez une stratégie **Paramètres généraux** ou sélectionnez une stratégie existante.
3. Sous **Journalisation**, dans le champ **Commentaires après un certain nombre d'événements**, spécifiez le nombre maximum d'événements pour un fichier journal.
4. Enregistrez vos paramètres.

Après l'assignation de la stratégie, le nombre d'événements spécifié s'applique.

Sélection des événements

1. Dans SafeGuard Management Center, sélectionnez les **Stratégies**.
2. Créez une nouvelle stratégie **Journalisation** ou sélectionnez une stratégie existante.

   Dans la zone d'action de droite, sous **Journalisation**, tous les événements prédéfinis qui peuvent être journalisés apparaissent. Par défaut, les événements sont regroupés par **Niveau**, par exemple **Avertissement** ou **Erreur**. Vous avez la possibilité de changer la manière de les regrouper. Cliquez sur les en-têtes de colonnes pour trier les événements par **ID**, **Catégorie**, etc.

3. Pour indiquer qu'un événement doit être journalisé dans la base de données SafeGuard Enterprise, sélectionnez l'événement en cliquant sur la colonne contenant l'icône de base de données **Consigner les événements dans une base de données**. Pour les événements à journaliser dans l'Observateur d'événements Windows, cliquez dans la colonne contenant l'icône du journal des événements **Consigner dans le journal des événements**.

   Cliquez plusieurs fois pour dessélectionner l'événement ou le rendre nul. Si vous ne définissez pas de paramètre pour un événement, la valeur par défaut correspondante s'applique.

4. Pour tous les événements sélectionnés, une coche verte s'affiche dans la colonne correspondante. Enregistrez vos paramètres.

Après avoir assigné la stratégie, les événements sélectionnés sont journalisés dans la destination en sortie correspondante.

Remarque : Pour obtenir une liste de tous les événements pouvant être journalisés, reportez-vous à la section Événements disponibles pour les rapports *(page 242)*.

Affichage des événements journalisés

En tant que responsable de la sécurité disposant des droits nécessaires, vous pouvez consulter les événements journalisés dans la base de données centrale de l'**Observateur d'événements** de SafeGuard Management Center.

Pour récupérer les entrées journalisées dans la base de données centrale :

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la zone de navigation **Rapports**, sélectionnez **Observateur d'événements**.
3. Dans la zone d'action **Observateur d'événements** à droite, cliquez sur l'icône de la loupe.

Tous les événements journalisés dans la base de données centrale apparaissent dans l'**Observateur d'événements**.

Les colonnes indiquent les informations suivantes relatives aux événements journalisés :

Colonne	Description
ID	Affiche un numéro identifiant l'événement.
Événement	Affiche un texte d'événement (description de l'événement).
Catégorie	Classification de l'événement selon la source (Chiffrement, Authentification, Système, par exemple).
Application	Affiche la zone logicielle d'où l'événement provient (SGMAuth, SGBaseENc, SGMAS, par exemple).
Ordinateur	Affiche le nom de l'ordinateur sur lequel l'événement journalisé s'est produit.
Domaine de l'ordinateur	Affiche le domaine de l'ordinateur sur lequel l'événement journalisé s'est produit.
Utilisateur	Affiche l'utilisateur connecté lorsque l'événement s'est produit.
Domaine utilisateur	Affiche le domaine de l'utilisateur connecté lorsque l'événement s'est produit.
Heure de connexion	Affiche la date et l'heure système auxquelles l'événement a été journalisé sur le terminal.

Cliquez sur les en-têtes de colonnes pour trier les événements par **Niveau**, **Catégorie**, etc.

Le menu contextuel des colonnes propose également de nombreuses fonctions de tri, de regroupement et de personnalisation de la Visionneuse des événements.

Cliquez deux fois sur une entrée de l'**Observateur d'événements** pour afficher des détails sur l'événement journalisé.

Application de filtres dans l'Observateur d'événements SafeGuard Enterprise

SafeGuard Management Center propose des fonctions de filtrage complètes. Grâce à ces fonctions, vous pouvez récupérer rapidement les événements appropriés parmi ceux affichés.

La zone **Filtre** de l'**Observateur d'événements** offre les champs suivants pour la définition des filtres :

Champ	Description
Catégories	Grâce à ce champ, vous pouvez filtrer l'**Observateur d'événements** en fonction de la classification source (par exemple **Chiffrement**, **Authentification**, **Système**) affichée dans la colonne **Catégorie**. Sélectionnez les catégories souhaitées dans la liste déroulante du champ.
Niveau d'erreur	Grâce à ce champ, vous pouvez filtrer l'**Observateur d'événements** en fonction de la classification des événements Windows (par exemple, avertissement, erreur) indiquée dans la colonne **Niveau**. Sélectionnez les niveaux souhaités dans la liste déroulante du champ.
Afficher dernier	Dans ce champ, vous pouvez définir le nombre d'événements à afficher. Les derniers événements journalisés sont affichés (par défaut, les 100 derniers événements).

Vous pouvez également créer des filtres personnalisés à l'aide de l'éditeur de filtres. Vous pouvez afficher l'éditeur de filtres dans le menu contextuel des colonnes d'un rapport. Dans la fenêtre **Générateur de filtres**, vous pouvez définir des filtres et les appliquer à la colonne concernée.

Rapport d'accès aux fichiers sur les supports amovibles et dans le stockage Cloud

Pour **SafeGuard Data Exchange** et **SafeGuard Cloud Storage**, vous pouvez suivre le nombre de fichiers qui sont accédés sur les supports amovibles ou dans votre stockage Cloud. Quelle que soit la stratégie de chiffrement s'appliquant aux fichiers enregistrés sur les supports amovibles ou dans le stockage Cloud, les événements peuvent être consignés pour ce qui suit :

- Un fichier ou répertoire est créé sur un support amovible ou dans le stockage Cloud.
- Un fichier ou répertoire est renommé sur un support amovible ou dans le stockage Cloud.
- Un fichier ou répertoire est supprimé d'un périphérique amovible ou du stockage Cloud.

Les événements de suivi d'accès aux fichiers peuvent être visualisés dans l'Observateur d'événements Windows ou dans l'**Observateur de suivi des fichiers** de SafeGuard Enterprise en fonction de la destination que vous spécifiez lorsque vous définissez la stratégie de journalisation.

Configuration du suivi d’accès aux fichiers

1. Dans SafeGuard Management Center, sélectionnez **Stratégies**.
2. Créez une nouvelle stratégie **Journalisation** ou sélectionnez une stratégie existante.

   Dans la zone d’action de droite, sous **Journalisation**, tous les événements prédéfinis qui peuvent être journalisés apparaissent. Cliquez sur les en-têtes de colonnes pour trier les événements par **ID**, **Catégorie**, etc.

3. Pour activer le suivi d’accès aux fichiers, sélectionnez les événements de journalisation suivants en fonction de vos besoins :
   - Pour les fichiers sur supports amovibles :
     - ID 3020 Suivi de fichiers pour les supports amovibles : un fichier a été créé.
     - ID 3021 Suivi de fichiers pour les supports amovibles : un fichier a été renommé.
     - ID 3022 Suivi de fichiers pour les supports amovibles : un fichier a été supprimé.
   - Pour les fichiers dans le stockage Cloud :
     - ID 3025 Suivi de fichiers pour le stockage Cloud : un fichier a été créé.
     - ID 3026 Suivi de fichiers pour le stockage Cloud : un fichier a été renommé.
     - ID 3027 Suivi de fichiers pour le stockage Cloud : un fichier a été supprimé.

   Pour indiquer qu’un événement doit être journalisé dans la base de données SafeGuard Enterprise, sélectionnez l’événement en cliquant sur la colonne contenant l’icône de base de données **Consigner les événements dans une base de données**. Pour les événements à journaliser dans l’Observateur d’événements Windows, cliquez dans la colonne contenant l’icône du journal des événements **Consigner dans le journal des événements**.
   Pour tous les événements sélectionnés, une coche verte s’affiche dans la colonne correspondante.

4. Enregistrez vos paramètres.

Après assignation de la stratégie, le suivi d’accès aux fichiers est activé et les événements sélectionnés sont journalisés dans la destination en sortie correspondante.

Remarque : Veuillez noter que l’activation du suivi d’accès aux fichiers augmente la charge sur le serveur.

Affichage des événements de suivi d’accès aux fichiers

Pour afficher les journaux de suivi d’accès aux fichiers, vous avez besoin du droit **Afficher les événements de suivi des fichiers**.

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la zone de navigation **Rapports**, sélectionnez **Observateur de suivi des fichiers**.
3. Dans la zone d’action **Observateur de suivi des fichiers** à droite, cliquez sur la loupe.

Tous les événements journalisés dans la base de données centrale apparaissent dans l'**Observateur de suivi des fichiers**. L'affichage est identique à celui de l'**Observateur d'événements**. Retrouvez plus de renseignements à la section Affichage des événements journalisés *(page 233)*.

Impression de rapports

Vous pouvez imprimer les rapports d'événements affichés dans l'**Observateur d'événements** ou dans l'**Observateur de suivi des fichiers** de SafeGuard Management Center à partir du menu **Fichier** dans la barre de menus de SafeGuard Management Center.

- Pour afficher un aperçu avant l'impression du rapport, sélectionnez **Fichier > Aperçu avant impression**. L'aperçu avant impression propose différentes fonctions comme l'exportation du document dans divers formats de sortie (par exemple, PDF) ou la modification de la mise en page (par exemple, en-tête et pied de page).
- Pour imprimer le document sans afficher l'aperçu, sélectionnez **Fichier > Imprimer**.

Connexion des événements journalisés

Les événements destinés à la base de données centrale sont journalisés dans le tableau EVENT de la base de données de SafeGuard Enterprise. Une protection d'intégrité spécifique peut être appliquée à ce tableau. Les événements peuvent être journalisés sous forme de liste connectée dans le tableau EVENT. En raison de la connexion, chaque entrée de la liste dépend de l'entrée précédente. Si une entrée est supprimée de la liste, ceci apparaît clairement et peut être vérifié à l'aide d'une vérification de l'intégrité.

Pour optimiser les performances, la connexion des événements dans le tableau EVENT est désactivée par défaut. Vous pouvez activer la connexion des événements journalisés pour vérifier l'intégrité. Retrouvez plus de renseignements à la section Vérification de l'intégrité des événements journalisés *(page 237)*.

Remarque : La protection d'intégrité ne s'applique pas au tableau EVENT lorsque la connexion des événements journalisés est désactivée.

Remarque : Un trop grand nombre d'événements peut entraîner des problèmes de performances. Retrouvez plus de renseignements sur la manière d'éviter ces problèmes de performances lors du nettoyage des événements à la section Nettoyage d'événement planifié par script *(page 238)*.

Activation de la connexion des événements journalisés

1. Arrêtez le service Web SGNSRV sur le serveur Web.

2. Supprimez tous les événements de la base de données et créez une sauvegarde lors de la suppression. Retrouvez plus de renseignements à la section Suppression de tous les événements ou d'une sélection d'événements *(page 237)*.

   Remarque : Si vous ne supprimez pas tous les anciens événements de la base de données, la connexion ne fonctionnera pas correctement car elle n'était pas activée pour les anciens événements restants.

3. Définissez la clé de registre suivante sur 0 ou supprimez-la :

   HKEY_LOCAL_MACHINE\SOFTWARE\Utimaco\SafeGuard Enterprise DWORD : DisableLogEventChaining = 0

4. Redémarrez le service Web.

La connexion des événements journalisés est activée.

Remarque : Pour désactiver de nouveau la connexion des événements, définissez la clé de registre sur 1.

Vérification de l'intégrité des événements journalisés

Conditions préalables : pour vérifier l'intégrité des événements journalisés, la concaténation des événements dans le tableau EVENT doit être activée.

1. Dans SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Actions > Vérifier l'intégrité**.

Un message affiche des informations sur l'intégrité des événements journalisés.

Remarque : Si la connexion des événements est désactivée, une erreur est renvoyée.

Suppression de tous les événements ou d'une sélection d'événements

1. Dans SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans l'**Observateur d'événements**, sélectionnez les événements à supprimer.
3. Pour supprimer des événements sélectionnés, sélectionnez **Actions > Supprimer des événements** ou cliquez sur l'icône **Supprimer des événements** dans la barre d'outils. Pour supprimer tous les événements, sélectionnez **Actions > Supprimer tous les événements** ou cliquez sur l'icône **Supprimer tous les événements** dans la barre d'outils.

4. Avant de supprimer les événements sélectionnés, le système affiche la fenêtre **Sauvegarder les événements sous** permettant de créer un fichier de sauvegarde. Retrouvez plus de renseignements à la section Création d’un fichier de sauvegarde *(page 238)*.

Les événements sont supprimés du journal des événements.

Création d’un fichier de sauvegarde

Lorsque vous supprimez des événements, vous pouvez créer un fichier de sauvegarde du rapport affiché dans la visionneuse des événements de SafeGuard Management Center.

1. Lors de la sélection de **Actions > Supprimer les événements** ou **Actions > Supprimer tous les événements**, la fenêtre **Sauvegarder les événements sous** permettant de créer un fichier de sauvegarde apparaît avant la suppression des événements.
2. Pour créer un fichier de sauvegarde .XML du journal des événements, saisissez un nom et un emplacement de fichier, puis cliquez sur **OK**.

Ouverture d'un fichier de sauvegarde

1. Dans SafeGuard Management Center, cliquez sur **Rapports**.
2. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Actions > Ouvrir le fichier de sauvegarde**.

   La fenêtre **Ouvrir une sauvegarde d'événement** apparaît.

3. Sélectionnez le fichier de sauvegarde à ouvrir et cliquez sur **Ouvrir**.

Le fichier de sauvegarde et les événements apparaissent dans l'**Observateur d'événements** de SafeGuard Management Center. Pour revenir à une vue standard de l'**Observateur d'événements**, cliquez de nouveau sur l'icône **Ouvrir le fichier de sauvegarde** dans la barre d'outils.

Nettoyage d’événement planifié par script

Remarque : SafeGuard Management Center contient le **Planificateur de tâches** pour créer et planifier des tâches périodiques basées sur des scripts. Les tâches sont automatiquement exécutées par un service sur le serveur SafeGuard Enterprise pour exécuter les scripts spécifiées.

Quatre scripts SQL sont disponibles dans le répertoire \tools du produit SafeGuard Enterprise livré pour le nettoyage automatique et efficace du tableau EVENT :

- spShrinkEventTable_install.sql

- ScheduledShrinkEventTable_install.sql
- spShrinkEventTable_uninstall.sql
- ScheduledShrinkEventTable_uninstall.sql

Les deux scripts spShrinkEventTable_uninstall.sql et ScheduledShrinkEventTable_uninstall.sql permettent d'installer une procédure enregistrée ainsi qu'une tâche planifiée sur le serveur de la base de données. La tâche planifiée exécuté la procédure enregistrée à des intervalles réguliers définis. La procédure enregistrée déplace des événements du tableau EVENT dans le tableau de sauvegarde EVENT_BACKUP tout en conservant un nombre prédéfini d'événements récents dans le tableau EVENT.

Les deux scripts spShrinkEventTable_uninstall.sql et ScheduledShrinkEventTable_uninstall.sql permettent de désinstaller la procédure enregistrée ainsi que la tâche planifiée. Ces deux scripts suppriment également le tableau EVENT_BACKUP.

Remarque : Si vous utilisez la procédure enregistrée pour déplacer des événements du tableau EVENT dans le tableau de sauvegarde, la connexion des événements ne s'applique plus. L'activation de la connexion tout en utilisant par ailleurs la procédure enregistrée pour le nettoyage des événements est inutile. Retrouvez plus de renseignements à la section Connexion des événements journalisés *(page 236)*.

Création de la procédure enregistrée

Le script spShrinkEventTable_install.sql permet de créer une procédure enregistrée qui déplace des données du tableau EVENT dans un tableau de sauvegarde EVENT_BACKUP. Le tableau EVENT_BACKUP est créé automatiquement s'il n'existe pas.

La première ligne est « USE SafeGuard ». Si vous avez donné un autre nom à votre base de données SafeGuard Enterprise, modifiez le nom en conséquence.

La procédure enregistrée conserve les <n> derniers événements dans le tableau EVENT et déplace les autres événements dans le tableau EVENT_BACKUP. Le nombre d'événements conservés dans le tableau EVENT est défini par un paramètre.

Pour exécuter la procédure stockée, lancez la commande suivante dans SQL Server Management Studio (Nouvelle requête) :

exec spShrinkEventTable 1000

Cet exemple de commande déplace tous les événements sauf les 1000 derniers.

Création d’une tâche planifiée d’exécution de la procédure enregistrée

Pour nettoyer automatiquement le tableau EVENT à intervalles réguliers, vous pouvez créer une tâche sur le serveur SQL. La tâche peut être créée avec le script ScheduledShrinkEventTable_install.sql ou à l’aide de SQL Enterprise Manager.

Remarque : La tâche planifiée ne s’applique pas aux bases de données SQL Express. L’agent SQL Server doit être en cours d’exécution pour que la tâche planifiée soit exécutée. SQL Server Express ne comportant aucun agent SQL Server, cette tâche ne s’applique pas à ces installations.

- Le script doit être exécuté dans msdb. Si vous avez donné un autre nom que SafeGuard à votre base de données SafeGuard Enterprise, modifiez le nom en conséquence.

  /* Default: Database name ’SafeGuard’ change if required*/

  SELECT @SafeGuardDataBase=’SafeGuard’

- Vous pouvez également préciser le nombre d’événements à conserver dans le tableau EVENT. Le nombre par défaut est 100 000.

  /* Default: keep the latest 100000 events, change if required*/

  SELECT @ShrinkCommand=’exec spShrinkEventTable 100000’

- Vous pouvez indiquer si une exécution de tâche doit être journalisée dans le journal des événements NT.

  exec sp_add_job

  @job_name=’AutoShrinkEventTable’,

  @enabled=1,

  @notify_level_eventlog=3

  Les valeurs suivantes sont disponibles pour le paramètre notify_level_eventlog :

Valeur	Résultat
3	Journaliser à chaque exécution de la tâche.
2	Journaliser en cas d’échec de la tâche.
1	Journaliser, si la tâche a été exécutée avec succès.
0	Ne pas journaliser l’exécution de la tâche dans le journal des événements NT.

- Vous pouvez préciser la fréquence de répétition de la tâche en cas d’échec.

  exec sp_add_jobstep

- @retry_attempts=3

  Cet exemple définit 3 tentatives d’exécution de la tâche en cas d’échec.

- @retry_interval=60

  Cet exemple définit un intervalle de 60 minutes.

- Vous pouvez spécifier l’heure d’exécution de la tâche.

exec sp_add_jobschedule

- @freq_type=4

  Cet exemple définit une exécution quotidienne de la tâche.

- @freq_interval=1

  Cet exemple définit une exécution de la tâche une fois par jour.

- @active_start_time=010000

  Cet exemple définit que la tâche est exécutée à 1 heure du matin.

Remarque : Outre les valeurs d’exemple indiquées ci-dessus, vous pouvez définir différentes options de planification avec sp_add-jobschedule. Par exemple, la tâche peut être exécutée toutes les deux minutes ou une fois par semaine seulement. Retrouvez plus de renseignements dans la documentation de Microsoft Transact SQL.

Nettoyage des procédures, des tâches et des tableaux enregistrés

Le script spShrinkEventTable_uninstall.sql permet de supprimer la procédure enregistrée et le tableau EVENT_BACKUP. Le script ScheduledShrinkEventTable_uninstall.sql permet d’annuler l’enregistrement de la tâche planifiée.

Remarque : Lorsque vous exécutez spShrinkEventTable_uninstall.sql, le tableau EVENT_BACKUP est supprimé ainsi que toutes les données qu’il contient.

Modèles de messages de rapport

Les événements ne sont pas journalisés avec leurs textes d'événement complet dans la base de données SafeGuard Enterprise. Seuls l'identifiant et les valeurs de paramètre correspondantes sont inscrits dans le tableau de la base de données. Lors de la récupération des événements journalisés

dans la **Visionneuse des événements** de SafeGuard Management Center, les valeurs de paramètre et les modèles de texte contenus dans le fichier .dll sont convertis en un texte d'événement complet dans la langue du système SafeGuard Management Center courant.

Les modèles utilisés pour les textes d'événement peuvent être modifiés et traités, à l'aide de requêtes SQL par exemple. Pour cela, vous pouvez générer une table contenant tous les modèles de texte des messages d'événement. Vous pouvez ensuite personnaliser les modèles en fonction de vos exigences particulières.

Pour créer une table contenant les modèles de texte des identifiants d'événement individuels :

1. Dans la barre de menus de SafeGuard Management Center, sélectionnez **Outils > Options**.
2. Dans la fenêtre **Options**, accédez à l'onglet **Base de données**.
3. Dans la zone **Modèles de messages de rapport**, cliquez sur **Créer une table**.

La table contenant les modèles de l'identifiant d'événement est créée dans la langue système en cours et peut être personnalisée.

Remarque : La table doit être effacée avant la génération des modèles. Si les modèles ont été générés tel que décrit pour une langue spécifique et si un utilisateur génère les modèles d'une autre langue, les modèles de la première langue sont supprimés.

3.8.16.2 Événements disponibles pour les rapports

Le tableau suivant fournit un aperçu de tous les événements pouvant être sélectionnés pour la journalisation.

Catégorie	Identifiant d'événement	Description
Système	1001	Processus démarré.
Système	1005	Service démarré.
Système	1006	Échec du démarrage du service.
Système	1007	Arrêt du service.
Système	1016	Échec du test d'intégrité des fichiers de données.
Système	1017	Chemin du journal indisponible.
Système	1018	Tentative de désinstallation de SafeGuard Enterprise non autorisée.
Système	1019	impossible de sauvegarder la clé
Système	1020	Impossible d'envoyer la « sauvegarde de la clé est terminée » à Sophos Enterprise Console.
Système	1021	réception de la sauvegarde de la clé non confirmée
Communication	1500	Un email a été envoyé avec des pièces jointes (De, Objet, Méthode de chiffrement)
Communication	1507	Un email a été envoyé avec des pièces jointes (De, Objet, Pièces jointes, Méthode de chiffrement)
Communication	1508	Un email a été envoyé avec des pièces jointes (De, Destinataires, Objet, Pièces jointes, Méthode de chiffrement)

Authentification	2001	GINA externe identifié et intégré.
Authentification	2002	GINA externe identifié ; échec de l’intégration.
Authentification	2003	Authentification au démarrage active.
Authentification	2004	Authentification au démarrage désactivée.
Authentification	2005	Éveil par appel réseau activé.
Authentification	2006	Éveil par appel réseau désactivé.
Authentification	2007	Challenge créé.
Authentification	2008	Réponse créée.
Authentification	2009	Connexion réussie.
Authentification	2010	Connexion impossible.
Authentification	2011	Utilisateur importé lors de la connexion et marqué comme propriétaire.
Authentification	2012	Utilisateur importé par un propriétaire et marqué comme non-propriétaire.
Authentification	2013	Utilisateur importé par un non propriétaire et marqué comme non propriétaire.
Authentification	2014	Utilisateur supprimé en tant que propriétaire.
Authentification	2015	Impossible d’importer l’utilisateur lors de la connexion.
Authentification	2016	L’utilisateur s’est déconnecté.
Authentification	2017	L’utilisateur a été contraint de se déconnecter.
Authentification	2018	Action effectuée sur le périphérique.
Authentification	2019	L’utilisateur a initié une modification de mot de passe/code confidentiel.
Authentification	2020	L’utilisateur a modifié son mot de passe/code confidentiel après la connexion.
Authentification	2021	Qualité du mot de passe/code confidentiel.
Authentification	2022	La stratégie de mot de passe/code confidentiel a été enfreinte.
Authentification	2023	LocalCache était corrompu et a été restauré.
Authentification	2024	Configuration non valide de la liste noire des mots de passe.
Authentification	2025	Le code de réponse permettant à l’utilisateur d’afficher le mot de passe a été reçu.
Authentification	2026	La sauvegarde du cache local a été effectuée.
Authentification	2027	Impossible de sauvegarder le cache local.
Authentification	2028	L’utilisateur connecté est un utilisateur invité.
Authentification	2029	Connexion réussie à Web Helpdesk avec des codes d’accès préconfigurés.
Authentification	2030	L’utilisateur connecté est un compte de service.
Authentification	2031	Connexion impossible à Web Helpdesk avec des codes d’accès préconfigurés.
Authentification	2032	Impossible d’autoriser Web Helpdesk.
Authentification	2033	Web Helpdesk démarré.
Authentification	2035	Liste de comptes de service importée.
Authentification	2036	Liste de comptes de service supprimée.
Authentification	2056	Ajouter un utilisateur Windows de SGN.
Authentification	2057	Tous les utilisateurs Windows de SGN ont été supprimés d’une machine.
Authentification	2058	L’utilisateur de L’Assignation utilisateur/machine a été supprimé manuellement
Authentification	2061	Code de renvoi de vérification Computrace.

Authentification	2062	Impossible d’exécuter la vérification Computrace.
Authentification	2071	L’initialisation du noyau a a réussi.
Authentification	2072	Impossible d’initialiser le noyau.
Authentification	2073	Les clés de la machine ont été générées avec succès sur le client.
Authentification	2074	Les clés de la machine n’ont pas pu être générées sur le client.
Authentification	2075	Impossible d’afficher les propriétés du disque ou d’initialiser le disque Opal.
Authentification	2079	L’importation de l’utilisateur dans le noyau a réussi.
Authentification	2080	La suppression de l’utilisateur du noyau a réussi.
Authentification	2081	Impossible d’importer l’utilisateur dans le noyau.
Authentification	2082	Impossible de supprimer l’utilisateur du noyau.
Authentification	2083	Réponse avec action « afficher le mot de passe utilisateur » créée.
Authentification	2084	Réponse pour les clients virtuels créée.
Authentification	2085	Réponse pour les clients autonomes créée.
Authentification	2086	Un nouveau certificat a été généré pour l’utilisateur du client autonome.
Authentification	2087	Un certificat a été assigné à l’utilisateur du client autonome. Cet événement survient uniquement sur les terminaux non administrés et ne sera donc jamais consigné dans la base de données.
Authentification	2095	Impossible d’activer l’éveil par appel réseau.
Authentification	2096	Impossible de désactiver l’éveil par appel réseau.
Authentification	2097	L’utilisateur a ouvert une session sur le client en utilisant le token de secours pour la première fois. Le token de veille a été défini comme clé standard.
Authentification	2098	L’activation du certificat de veille réussie a été signalée au serveur.
Authentification	2099	L’utilisateur a ouvert une session sur le client en utilisant le token de secours pour la première fois. Le certificat de veille n’a pas pu être activé à cause d’une erreur.
Authentification	2100	L’activation du certificat de secours a échoué sur le serveur
Authentification	2101	Le code confidentiel a été modifié sur le token.
Authentification	2102	Impossible de modifier le code confidentiel sur le token.
Authentification	2103	Impossible d’appliquer la stratégie « Appliquer la connexion au token par certificat »
Authentification	2104	Stratégie « Activer la connexion au token par certificat » appliquée.
Administration	2500	Lancement de SafeGuard Enterprise Administration.
Administration	2501	Impossible de se connecter à SafeGuard Enterprise Administration.
Administration	2502	Autorisation pour SafeGuard Enterprise Administration refusée.
Administration	2502	Autorisation pour SafeGuard Enterprise Administration refusée.
Administration	2503	Autorisation supplémentaire requise.
Administration	2504	Autorisation supplémentaire accordée pour l’action.
Administration	2505	Autorisation supplémentaire refusée.
Administration	2506	Importation de données depuis le répertoire menée à bien.
Administration	2507	Importation de données depuis le répertoire annulée.
Administration	2508	Impossible d’importer des données depuis le répertoire.
Administration	2511	Utilisateur créé.
Administration	2513	Utilisateur modifié.
Administration	2515	Utilisateur supprimé.

Administration	2518	Échec de l’application de l’utilisateur.
Administration	2522	Impossible de supprimer l’utilisateur.
Administration	2525	Machine appliquée.
Administration	2529	Machine supprimée.
Administration	2532	Échec de l’application de la machine.
Administration	2536	Impossible de supprimer la machine.
Administration	2539	OU appliqué.
Administration	2543	OU supprimé.
Administration	2546	Échec de l’application de l’OU.
Administration	2547	Échec de l’importation de l’OU.
Administration	2550	Impossible de supprimer l’OU.
Administration	2553	Groupe appliqué.
Administration	2555	Groupe modifié.
Administration	2556	Groupe renommé.
Administration	2557	Groupe supprimé.
Administration	2560	Échec de l’application du groupe.
Administration	2562	Impossible de modifier le groupe.
Administration	2563	Impossible de renommer le groupe.
Administration	2564	Impossible de supprimer le groupe.
Administration	2573	Membres ajoutés au groupe.
Administration	2575	Membres supprimés du groupe.
Administration	2576	Impossible d’ajouter les membres au groupe.
Administration	2578	Impossible de supprimer les membres du groupe.
Administration	2580	Groupe déplacé d’une OU vers une autre.
Administration	2583	Impossible de passer le groupe d’une OU vers une autre.
Administration	2591	Objets ajoutés au groupe.
Administration	2593	Objets supprimés du groupe.
Administration	2594	Impossible d’ajouter les objets au groupe.
Administration	2596	Impossible de supprimer les objets du groupe.
Administration	2603	Clé générée.
Administration	2603	Clé générée.
Administration	2604	Clé modifiée.
Administration	2607	Clé assignée.
Administration	2608	Assignation de clé annulée.
Administration	2609	Impossible de générer la clé.
Administration	2610	Impossible de modifier la clé.
Administration	2613	Impossible d’assigner la clé.
Administration	2614	Impossible de supprimer l’assignation de la clé.
Administration	2615	Certificat généré.
Administration	2616	Certificat importé.
Administration	2619	Certificat supprimé.
Administration	2621	Certificat assigné à l’utilisateur.
Administration	2622	Annulation de l’assignation de certificat à l’utilisateur.
Administration	2623	Impossible de créer le certificat.
Administration	2624	Impossible d’importer le certificat.
Administration	2627	Impossible de supprimer le certificat.

Administration	2628	Impossible de procéder à l’extension du certificat.
Administration	2629	Impossible d’assigner le certificat à l’utilisateur.
Administration	2630	Impossible de supprimer l’assignation du certificat à l’utilisateur.
Administration	2631	Token connecté.
Administration	2632	Token supprimé.
Administration	2633	Token généré pour l’utilisateur.
Administration	2634	Changer le code confidentiel utilisateur sur le token.
Administration	2635	Changer le code confidentiel SO sur le token.
Administration	2636	Token verrouillé.
Administration	2637	Token déverrouillé.
Administration	2638	Token supprimé.
Administration	2639	Assignation de token supprimé pour l’utilisateur.
Administration	2640	Impossible de générer un token pour l’utilisateur.
Administration	2641	Impossible de modifier le code confidentiel utilisateur sur le token.
Administration	2642	Impossible de modifier le code confidentiel du responsable de la sécurité sur le token.
Administration	2643	Impossible de verrouiller le token.
Administration	2644	Impossible de déverrouiller le token.
Administration	2645	Impossible de supprimer le token.
Administration	2647	Stratégie créée.
Administration	2648	Stratégie modifiée.
Administration	2650	Stratégie supprimée.
Administration	2651	Stratégie assignée et activée sur l’OU.
Administration	2652	Stratégie assignée supprimée de l’OU.
Administration	2653	Impossible de créer la stratégie.
Administration	2654	Impossible de modifier la stratégie.
Administration	2657	Impossible d’assigner et d’activer une stratégie sur l’UO.
Administration	2658	Impossible de supprimer la stratégie assignée par l’UO.
Administration	2659	Groupe de stratégies créé.
Administration	2660	Groupe de stratégies modifié.
Administration	2661	Groupe de stratégies supprimé.
Administration	2662	Impossible de créer le groupe de stratégies.
Administration	2663	Impossible de modifier le groupe de stratégies.
Administration	2665	La stratégie suivante a été ajoutée au groupe de stratégies.
Administration	2667	La stratégie suivante a été supprimée du groupe de stratégies.
Administration	2668	Impossible d’ajouter la stratégie au groupe de stratégies.
Administration	2670	Impossible de supprimer la stratégie du groupe de stratégies.
Administration	2678	Événement enregistré exporté.
Administration	2679	Impossible d’exporter les événements enregistrés.
Administration	2680	Événements enregistrés supprimés.
Administration	2681	Impossible de supprimer les événements enregistrés.
Administration	2684	Le responsable de la sécurité autorise le renouvellement du certificat.
Administration	2685	Le responsable de la sécurité refuse le renouvellement du certificat.
Administration	2686	Impossible de modifier les paramètres de renouvellement du certificat.
Administration	2687	Modification du certificat du responsable.
Administration	2688	Impossible de modifier le certificat du responsable.

Administration	2692	Création de groupes de travail.
Administration	2693	Création de groupes de travail impossible.
Administration	2694	Suppression de groupes de travail.
Administration	2695	Suppression de groupes de travail impossible.
Administration	2696	Création d’utilisateurs.
Administration	2697	Création d’utilisateurs impossible.
Administration	2698	Création de machines.
Administration	2699	Création de machines impossible.
Administration	2700	Violation de licence.
Administration	2701	Création du fichier de clé.
Administration	2702	Suppression de la clé du fichier de clé.
Administration	2703	Le responsable de la sécurité a désactivé l’authentification au démarrage dans la stratégie.
Administration	2704	Sujet de la question LSH créé.
Administration	2705	Sujet de la question LSH modifié.
Administration	2706	Sujet de la question LSH supprimé.
Administration	2707	Question modifiée.
Administration	2708	Package de configuration créé pour le client autonome.
Administration	2709	Package de configuration créé pour le client Enterprise.
Administration	2710	Le CCO a été importé.
Administration	2711	Le CCO a été exporté.
Administration	2712	Le CCO a été supprimé.
Administration	2713	Mise à jour du certificat de l’entreprise.
Administration	2715	Liste de comptes de service créée.
Administration	2716	Liste de comptes de service modifiée.
Administration	2717	Liste de comptes de service supprimée.
Administration	2718	Définition de Cloud Storage créée.
Administration	2719	Définition de Cloud Storage modifiée.
Administration	2720	Définition de Cloud Storage supprimée.
Administration	2721	Liste d’application créée.
Administration	2722	Liste d’application modifiée.
Administration	2723	Liste d’application supprimée.
Administration	2724	Rôle créé.
Administration	2725	Rôle modifié.
Administration	2726	Rôle supprimé.
Administration	2727	Rôle assigné au responsable de la sécurité.
Administration	2728	Annulation de l’assignation du rôle au responsable de la sécurité.
Administration	2729	Responsable principal de la sécurité créé.
Administration	2730	Responsable principal de la sécurité modifié.
Administration	2731	Responsable principal de la sécurité supprimé.
Administration	2732	Certificat du responsable principal de la sécurité modifié.
Administration	2733	Impossible de modifier le certificat du responsable principal de la sécurité.
Administration	2734	Responsable principal de la sécurité activé.
Administration	2735	Responsable principal de la sécurité désactivé.
Administration	2736	Responsable de la sécurité créé.

Administration	2737	Responsable de la sécurité modifié.
Administration	2738	Responsable de la sécurité supprimé.
Administration	2739	Responsable de la sécurité supprimé. Informations supplémentaires sur les enfants.
Administration	2740	Responsable de la sécurité activé.
Administration	2741	Responsable de la sécurité désactivé.
Administration	2742	Responsable de la sécurité déplacé.
Administration	2743	Responsable de la sécurité promu responsable principal de la sécurité.
Administration	2744	Responsable de la sécurité promu responsable principal de la sécurité. Informations supplémentaires sur les enfants.
Administration	2745	Responsable principal de la sécurité rétrogradé.
Administration	2746	Groupe de responsables de la sécurité créé.
Administration	2747	Groupe de responsables de la sécurité modifié.
Administration	2748	Groupe de responsables de la sécurité supprimé.
Administration	2749	Responsable de la sécurité ajouté au groupe de responsables de la sécurité.
Administration	2750	Responsable de la sécurité supprimé du groupe de responsables de la sécurité.
Administration	2753	Accès en lecture au conteneur accordé au responsable de la sécurité.
Administration	2754	Accès en lecture au conteneur accordé au groupe de responsables de la sécurité.
Administration	2755	Accès total au conteneur accordé au responsable de la sécurité.
Administration	2756	Accès total au conteneur accordé au groupe de responsables de la sécurité.
Administration	2757	Accès au conteneur révoqué pour le responsable de la sécurité.
Administration	2758	Accès au conteneur révoqué pour le groupe de responsables de la sécurité.
Administration	2759	Accès en lecture à la stratégie accordé au responsable de la sécurité.
Administration	2760	Accès en lecture à la stratégie accordé au groupe de responsables de la sécurité.
Administration	2761	Accès total à la stratégie accordé au responsable de la sécurité.
Administration	2762	Accès total à la stratégie accordé au groupe de responsables de la sécurité.
Administration	2763	Accès à la stratégie révoqué pour le responsable de la sécurité.
Administration	2764	Accès à la stratégie révoqué pour le groupe de responsables de la sécurité.
Administration	2765	Les paramètres de nombre de questions LSH ont changé.
Administration	2766	Accès au conteneur formellement interdit au responsable de la sécurité
Administration	2767	L’interdiction formelle d’accès au conteneur a été levée pour le responsable de la sécurité.
Administration	2768	L’autorisation d’accès en lecture au conteneur a été levée pour le responsable de la sécurité.
Administration	2769	L’observateur du suivi de fichiers a été ouvert.
Administration	2770	Stratégie de déploiement activée par le responsable de la sécurité.
Administration	2771	Stratégie de déploiement désactivée par le responsable de la sécurité.
Administration	2772	Stratégie de déploiement activée par la gestion de licence.

Administration	2773	Stratégie de déploiement désactivée par la gestion de licence.
Administration	2800	La confirmation de l’utilisateur non confirmé a réussi.
Administration	2801	Un utilisateur n’a pas été confirmé automatiquement.
Administration	2810	Utilisateur de l’authentification au démarrage créé.
Administration	2811	Utilisateur de l’authentification au démarrage modifié.
Administration	2812	Utilisateur de l’authentification au démarrage supprimé.
Administration	2815	Impossible de créer l’utilisateur de l’authentification au démarrage.
Administration	2816	Impossible de modifier l’utilisateur de l’authentification au démarrage.
Administration	2817	Impossible de supprimer l’utilisateur de l’authentification au démarrage.
Administration	2820	Groupe d’utilisateurs de l’authentification au démarrage créé.
Administration	2821	Groupe d’utilisateurs de l’authentification au démarrage modifié.
Administration	2822	Groupe d’utilisateurs de l’authentification au démarrage supprimé.
Administration	2825	Impossible de créer le groupe d’utilisateurs de l’authentification au démarrage.
Administration	2826	Impossible de modifier le groupe d’utilisateurs de l’authentification au démarrage.
Administration	2827	Impossible de supprimer le groupe d’utilisateurs de l’authentification au démarrage.
Administration	2830	Le groupe d’authentification au démarrage est affecté au conteneur.
Administration	2831	Le groupe d’authentification au démarrage a été supprimé du conteneur.
Administration	2832	Les groupes sont activés pour une affectation du groupe d’authentification au démarrage au conteneur.
Administration	2833	Impossible d’assigner le groupe d’authentification au démarrage au conteneur.
Administration	2834	Impossible de supprimer le groupe d’authentification au démarrage affecté du conteneur.
Administration	2835	Impossible d’activer les groupes pour l’assignation du groupe d’authentification au démarrage au conteneur.
Administration	2850	Le service du planificateur s’est arrêté à cause d’une exception.
Administration	2851	La tâche du planificateur s’est exécutée avec succès.
Administration	2852	Échec de la tâche du planificateur.
Administration	2853	Tâche du planificateur créée ou modifiée.
Administration	2854	Tâche du planificateur supprimée.
Administration	2855	L’algorithme de la signature du certificat des nouveaux certificats a été changée.
Administration	2856	La longueur de la clé du certificat a été changée pour les nouveaux certificats.
Administration	2857	La période de validité du certificat a été changée pour les nouveaux certificats.
Administration	2858	La base de données a été mise à niveau.
Administration	2859	Impossible de mettre à niveau la base de données.
Administration	2900	Création de la réponse pour la suspension de la protection de la configuration.
Administration	2905	La clé de récupération BitLocker a été exportée pour la machine.
Client	3003	Sauvegarde du noyau réussie.
Client	3005	Première tentative de restauration du noyau réussie.

Client	3006	Deuxième tentative de restauration du noyau réussie.
Client	3007	Impossible de sauvegarder le noyau.
Client	3008	Impossible de restaurer le noyau.
Client	3009	Impossible de sauvegarder le noyau.
Client	3010	Supprimer le token de sauvegarde à partir de l’authentification au démarrage.
Client	3011	Ajouter le token de sauvegarde à partir de l’authentification au démarrage.
Client	3018	L’opération de chiffrement retardée a chiffré un fichier.
Client	3019	L’opération de chiffrement retardée a déchiffré un fichier.
Client	3020	Suivi de fichiers pour les supports amovibles : un fichier a été créé.
Client	3021	Suivi de fichiers pour les supports amovibles : un fichier a été renommé.
Client	3022	Suivi de fichiers pour les supports amovibles : un fichier a été supprimé.
Client	3025	Suivi de fichiers pour le stockage Cloud : un fichier a été créé.
Client	3026	Suivi de fichiers pour le stockage Cloud : un fichier a été renommé.
Client	3027	Suivi de fichiers pour le stockage Cloud : un fichier a été supprimé.
Client	3028	Suivi de fichier : un fichier a été chiffré manuellement.
Client	3029	Suivi de fichier : un fichier a été déchiffré manuellement.
Client	3030	L’utilisateur a modifié ses secrets LSH après la connexion.
Client	3035	La fonction LSH a été activée.
Client	3040	Désactivation de LSH.
Client	3045	LSH est disponible : client Enterprise
Client	3046	LSH est disponible : client autonome
Client	3050	Désactivation de LSH : client Enterprise
Client	3051	La fonction LSH n’est pas disponible (client autonome).
Client	3055	La liste QST (questions LSH) a été modifiée.
Client	3060	L’utilisateur a modifié ses réponses dans LSH.
Client	3070	Sauvegarde réussie de la clé sur le partage réseau spécifié.
Client	3071	La sauvegarde de clé n’a pas pu être enregistrée sur le partage réseau indiqué.
Client	3072	L’utilisateur a désactivé le chiffrement.
Client	3080	L’entrée de démarrage Sophos UEFI a été réparée.
Client	3081	L’entrée de démarrage Sophos UEFI n’a pas pu être réparée.
Client	3082	Le module Outlook complémentaire a été désactivé alors qu’il est activé dans la stratégie SGN.
Client	3110	L’utilisateur de l’authentification au démarrage a été importé dans l’authentification au démarrage
Client	3111	L’utilisateur de l’authentification au démarrage a été supprimé de l’authentification au démarrage
Client	3116	Impossible d’importer l’utilisateur de l’authentification au démarrage dans l’authentification au démarrage
Client	3117	Impossible de supprimer l’utilisateur de l’authentification au démarrage de l’authentification au démarrage
Client	3200	Protection de la configuration suspendue.
Client	3201	Protection de la configuration non suspendue (mauvaise réponse).

Client	3202	Suspension de la Protection de la configuration interrompue par l’utilisateur.
Client	3203	Suspension de la Protection de la configuration interrompue (temps de suspension dépassé).
Client	3300	Application principale redémarrée.
Client	3301	Interruption inattendue de l’application principale.
Client	3302	Impossible de redémarrer l’application principale
Client	3303	Une exception non prise en charge a entraîné l’arrêt de fonctionnement de l’application principale.
Client	3304	Échec de l’arrêt de l’application principale inconnu.
Client	3405	La désinstallation du client de protection de configuration a échoué.
Client	3406	Une erreur interne s’est produite au niveau du client de protection de configuration.
Client	3407	Le client de protection de configuration a détecté une possible falsification.
Client	3408	Le client de protection de configuration a détecté une possible falsification des fichiers journaux.
Client	3409	Phrase secrète saisie incorrecte.
Chiffrement	3500	Le disque dur a été préparé pour le chiffrement BitLocker.
Chiffrement	3501	Accès refusé au support sur le lecteur.
Chiffrement	3502	Accès refusé au fichier de données.
Chiffrement	3503	Démarrage du chiffrement initial basé sur secteur du lecteur
Chiffrement	3504	Chiffrement initial basé sur secteur du lecteur démarré (mode rapide)
Chiffrement	3505	Fin du chiffrement initial basé sur secteur du lecteur réussie.
Chiffrement	3506	Échec et clôture du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3507	Annulation du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3508	Échec du chiffrement initial basé sur secteur du lecteur.
Chiffrement	3509	Démarrage du déchiffrement basé sur secteur du lecteur.
Chiffrement	3510	Clôture du déchiffrement basé sur secteur du lecteur.
Chiffrement	3511	Échec et clôture du déchiffrement basé sur secteur du lecteur.
Chiffrement	3512	Annulation du déchiffrement basé sur secteur du lecteur.
Chiffrement	3513	Échec du déchiffrement basé sur secteur du lecteur.
Chiffrement	3514	Démarrage du chiffrement initial de fichiers sur le lecteur.
Chiffrement	3515	Succès du chiffrement initial de fichiers sur un lecteur.
Chiffrement	3516	Échec et fermeture du chiffrement initial de fichiers sur un lecteur.
Chiffrement	3517	Annulation du chiffrement initial de fichiers sur le lecteur.
Chiffrement	3519	Démarrage du déchiffrement sur un lecteur.
Chiffrement	3520	Succès de la fermeture du déchiffrement de fichiers sur un lecteur.
Chiffrement	3521	Échec et fermeture du déchiffrement de fichiers sur un lecteur.
Chiffrement	3522	Annulation du déchiffrement de fichiers sur un lecteur.
Chiffrement	3524	Démarrage du chiffrement d’un fichier.
Chiffrement	3525	Succès du chiffrement d’un fichier.
Chiffrement	3526	Échec du chiffrement d’un fichier.
Chiffrement	3540	Démarrage du déchiffrement d’un fichier.
Chiffrement	3541	Succès du déchiffrement du fichier.
Chiffrement	3542	Échec du déchiffrement d’un fichier.

Chiffrement	3543	Sauvegarde de la clé de démarrage réussie.
Chiffrement	3544	Nombre maximum d’algorithmes de démarrage dépassé.
Chiffrement	3545	Erreurs de lecture sur la KSA.
Chiffrement	3546	Désactivation des volumes en fonction des stratégies définies.
Chiffrement	3547	Avertissement ! La sauvegarde du secteur de démarrage NTFS manque sur le volume.
Chiffrement	3548	L’utilisateur a créé de nouveaux codes d’accès de démarrage BitLocker pour cet ordinateur.
Chiffrement	3549	L’utilisateur a tenté de créer de nouveaux codes d’accès de démarrage BitLocker pour cet ordinateur mais l’opération a échoué.
Chiffrement	3552	L’utilisateur a suspendu la protection BitLocker.
Chiffrement	3553	L’utilisateur a repris la protection BitLocker.
Chiffrement	3559	Les éléments de la file d’attente de chiffrement asynchrone sont manquants.
Chiffrement	3560	Contrôle d’accès
Chiffrement	3561	L’état de cet ordinateur est maintenant sécurisé.
Chiffrement	3562	Cet ordinateur est sécurisé. Toutefois, le paramètre « Supprimer les clés des machines compromises » n’est pas activé dans la stratégie. Aucune action effectuée.
Chiffrement	3563	Cet ordinateur n’est pas sécurisé. Toutefois, le paramètre « Supprimer les clés des machines compromises » n’est pas activé dans la stratégie. Aucune action effectuée.
Chiffrement	3570	Clé de chiffrement de support assignée.
Chiffrement	3571	Clé de la phrase secrète des support assignée.
Chiffrement	3572	Clé de la phrase secrète des support créée.
Chiffrement	3573	Clé de la phrase secrète des support importée.
Chiffrement	3574	Table de clés corrompue détectée.
Chiffrement	3600	Erreur de chiffrement générale.
Chiffrement	3601	Erreur de chiffrement - moteur : volume manquant.
Chiffrement	3602	Erreur de chiffrement - moteur : volume hors ligne.
Chiffrement	3603	Erreur de chiffrement - moteur : volume supprimé.
Chiffrement	3604	Erreur de chiffrement - moteur : volume incorrect.
Chiffrement	3605	Cet ordinateur n’est pas sécurisé. Veuillez prendre les mesures nécessaires.
Chiffrement	3607	Erreur de chiffrement - clé de chiffrement manquante.
Chiffrement	3610	Erreur de chiffrement - zone de stockage des clés d’origine endommagée.
Chiffrement	3611	Erreur de chiffrement - zone de stockage des clés de sauvegarde endommagée.
Chiffrement	3612	Erreur de chiffrement - zone ESA d’origine endommagée.
Chiffrement	3700	File Share a ignoré un chemin incorrect dans la stratégie.
Chiffrement	3701	Application sécurisée introuvable.
Chiffrement	3710	Le chiffrement File Share a démarré.
Chiffrement	3711	Le chiffrement File Share a réussi.
Chiffrement	3712	Le chiffrement File Share s’est terminé avec des erreurs.
Chiffrement	3713	Le chiffrement File Share a été annulé.
Chiffrement	3714	Le chiffrement initial est terminé.

Chiffrement	3715	Le chiffrement initial de ce chemin est terminé.
Chiffrement	3800	Cloud Storage a ignoré un chemin incorrect dans la stratégie.
Chiffrement	3900	Le chiffrement du fichier HTML5 à auto-déchiffrement est terminé.
Chiffrement	3999	La préparation du disque dur pour le chiffrement BitLocker a échoué
Contrôle d’accès	4400	Le port autorisé a été approuvé.
Contrôle d’accès	4401	Le périphérique autorisé a été approuvé.
Contrôle d’accès	4402	Le périphérique de stockage autorisé a été approuvé.
Contrôle d’accès	4403	Le réseau local sans fil autorisé a été approuvé.
Contrôle d’accès	4404	Le port autorisé a été retiré avec succès.
Contrôle d’accès	4405	Le périphérique autorisé a été retiré avec succès.
Contrôle d’accès	4406	Le périphérique de stockage autorisé a été retiré avec succès.
Contrôle d’accès	4407	Le réseau local sans fil autorisé a été déconnecté.
Contrôle d’accès	4408	Port restreint.
Contrôle d’accès	4409	Périphérique restreint.
Contrôle d’accès	4410	Périphérique de stockage restreint.
Contrôle d’accès	4411	Réseau local sans fil restreint.
Contrôle d’accès	4412	Port bloqué.
Contrôle d’accès	4413	Périphérique bloqué.
Contrôle d’accès	4414	Périphérique de stockage bloqué.
Contrôle d’accès	4415	Réseau local sans fil bloqué.

3.8.17 Types de stratégie et champs d’application

Les stratégies SafeGuard Enterprise comportent tous les paramètres nécessaires pour mettre en œuvre une stratégie de sécurité à l’échelle de l’entreprise sur les terminaux.

Les stratégies de SafeGuard Enterprise peuvent comporter des paramètres pour les domaines suivants (types de stratégies) :

- **Paramètres généraux**

  Paramètres pour le taux de transfert, la personnalisation, la récupération de connexion, les images d’arrière-plan, etc.

- **Authentification**

  Paramètres de mode de connexion, verrouillage de périphérique, etc.

- **Code confidentiel**

  Définit la configuration minimale des codes confidentiels utilisés.

- **Mot de passe**

Définit la configuration minimale des mots de passe utilisés.

- **Phrase secrète**

  Définit la configuration minimale pour les phrases secrètes utilisées pour SafeGuard Data Exchange.

- **Protection des périphériques**

  Paramètres de chiffrement basé sur volume ou sur fichier (y compris des paramètres pour SafeGuard Data Exchange, SafeGuard Cloud Storage et SafeGuard Portable) : algorithmes, clés, les lecteurs sur lesquels les données doivent être chiffrées, etc.

- **Paramètres de machine spécifiques**

  Paramètres d'authentification au démarrage SafeGuard (activer/désactiver), d'éveil par appel réseau sécurisé, d'options d'affichage, etc.

- **Journalisation**

  Définit les événements à consigner dans le journal et leurs destinations de sortie.

- **Protection de la configuration**

  Remarque : Le paramètre Protection de la configuration n'est disponible que pour les clients SafeGuard Enterprise jusqu'à la version 6.0.

  Paramètres (autoriser/bloquer) pour l'utilisation des ports et des périphériques (lecteurs multimédias amovibles, imprimantes, etc.).

- **Chiffrement de fichiers**

  Paramètres pour un chiffrement basé sur fichier sur les lecteurs locaux et les emplacements réseau, surtout pour les groupes de travail et les partages réseau.

Dans SafeGuard Management Center, les stratégies par défaut sont disponibles pour tous les types de stratégie. Pour les stratégies de **Protection des périphériques** les stratégies de chiffrement intégral du disque (cible : stockage de masse), Cloud Storage (cible : DropBox) et Data Exchange (cible : supports amovibles) sont disponibles. Les options dans ces stratégies par défaut sont définies sur les valeurs adéquates. Vous pouvez modifier les paramètres par défaut en fonction de vos exigences particulières. Les stratégies par défaut sont nommées <type de stratégie> (Par défaut).

Remarque : Les noms de ces stratégies par défaut dépendent du paramètre de langue définit au cours de l'installation. Si vous modifiez la langue de SafeGuard Management Center par la suite, les noms de la stratégie par défaut demeurent dans le paramètre de langue au cours de l'installation.

3.8.17.1 Paramètres généraux

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
Chargement des paramètres	
Mode de récursivité des stratégies	**Répéter les paramètres machine** Si **Répéter les paramètres machine** est sélectionné dans le champ **Mode de récursivité des stratégies** et si la stratégie provient d'une machine (le paramètre **Répéter les paramètres machine** d'une stratégie utilisateur n'entraîne aucun effet), cette stratégie est mise en œuvre une nouvelle fois à la fin. Ceci remplace ensuite les paramètres de l'utilisateur et les paramètres de la machine s'appliquent. **Ignorer l'utilisateur** Si vous sélectionnez **Ignorer l'utilisateur** pour une stratégie (stratégie de machine) dans le champ **Mode de récursivité des stratégies**, et si la stratégie provient d'une machine, seuls les paramètres de la machine sont analysés. Les paramètres de l'utilisateur ne sont pas analysés. **Aucun bouclage** **Aucun blocage** est le comportement standard : Les stratégies de l'utilisateur sont prioritaires sur celles de la machine. **Comment les paramètres « Ignorer l'utilisateur » et « Répéter les paramètres machine » sont-ils analysés?** S'il existe des assignations de stratégies actives, les stratégies de la machine sont analysées et regroupées d'abord. Si le regroupement des différentes stratégies se traduit par l'attribut **Ignorer l'utilisateur** dans le mode de récursivité des stratégies, les stratégies qui auraient été appliquées pour l'utilisateur ne

Paramètre de stratégie	Explication
	sont plus analysées. Cela signifie que les mêmes stratégies s'appliquent à l'utilisateur et à la machine. Si la valeur **Répéter les paramètres machine** est appliquée dans le cas du mode de récursivité des stratégies, lorsque les stratégies individuelles de la machine ont été regroupées, les stratégies de l'utilisateur sont ensuite combinées à celles de la machine. Après le regroupement, les stratégies de la machine sont réécrites et remplacent les paramètres de stratégie de l'utilisateur. Cela signifie que, si un paramètre est présent dans les deux stratégies, la valeur de la stratégie de la machine remplace celle de la stratégie de l'utilisateur. Si le regroupement des stratégies individuelles de la machine indique « Non configuré », les conditions suivantes s'appliquent : Les paramètres de l'utilisateur deviennent prioritaires sur ceux de la machine.
Taux de transfert	
Intervalle de connexion au serveur (minutes)	Détermine la période, en minutes, après laquelle un client SafeGuard Enterprise envoie une demande de stratégie (modifications) au serveur SafeGuard Enterprise. pour éviter qu'un grand nombre de clients ne contactent le serveur simultanément, la communication s'effectue dans une période de +/- 50% de l'intervalle de connexion défini. Exemple : Si vous avez sélectionné « 90 minutes », la communication s'effectue après un intervalle pouvant aller de 45 à 135 minutes.
Commentaires	
Aidez-nous à améliorer Sophos SafeGuard® en envoyant des données d'utilisation anonymes	Sophos s'efforce en permanence d'améliorer SafeGuard Enterprise. Dans ce but, les clients envoient régulièrement des données anonymes à Sophos. Ces données sont exclusivement utilisées dans le but d'améliorer notre produit. Elles ne peuvent pas être utilisées pour identifier les clients ou leurs machines et ne contiennent aucune autre information confidentielle. Toutes les données étant envoyées de manière anonyme, la fonction de récupération des données est activée par défaut. Si vous paramétrez cette option sur **Non**, aucune donnée d'utilisation ne sera envoyée à Sophos.

Paramètre de stratégie	Explication
Journalisation	
Commentaires après un certain nombre d'événements	Le système de journalisation, introduit sous le nom de Win32 Service « SGM LogPlayer », recueille les entrées du journal générées par SafeGuard Enterprise pour la base de données centrale et les stocke dans des fichiers journaux locaux. Elles sont stockées dans le cache local dans le répertoire « Auditing \SGMTransLog ». Ces fichiers sont transférés au mécanisme de transport qui les envoie ensuite à la base de données via le serveur SGN. Le transfert s'effectue dès que le mécanisme de transport a réussi à créer une connexion au serveur. La taille du fichier journal a donc tendance à augmenter jusqu'à ce qu'une connexion ait été établie. Pour limiter la taille de chaque fichier journal, il est possible de spécifier un nombre maximal d'entrées du journal dans la stratégie. Lorsque le nombre d'entrées prédéfini a été atteint, le système de journalisation place le fichier journal dans la file d'attente de transport du serveur SGN et démarre un nouveau fichier journal.
Personnalisation	
Langue utilisée sur le client	Langue dans laquelle les paramètres de SafeGuard Enterprise sont affichés sur le terminal : Vous pouvez sélectionner une langue prise en charge ou le paramètre de langue du système d'exploitation du terminal.
Récupération de connexion	
Activer la récupération de connexion après la corruption du cache local Windows	Le cache local Windows représente le point de départ et de fin de l'échange de données entre le terminal et le serveur. Il stocke la totalité des clés, stratégies, certificats utilisateur et fichiers d'audit. Les données stockées dans le cache local sont signées et ne peuvent pas être modifiées manuellement. Par défaut, la récupération de la connexion est désactivée suite à la corruption du cache local. Ceci signifie que le cache local sera restauré automatiquement à partir de sa sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local Windows. Si le cache local Windows doit être réparé

Paramètre de stratégie	Explication
	explicitement via une procédure Challenge/Réponse, définissez ce champ sur **Oui**.
Local Self Help	
Activer Local Self Help	Détermine si les utilisateurs sont autorisés à se connecter à leurs ordinateurs avec Local Self Help en cas d'oubli de leur mot de passe. Avec Local Self Help, l'utilisateur peut se connecter en répondant à un nombre spécifique de questions prédéfinies dans l'authentification au démarrage SafeGuard. Il peut de nouveau accéder à son ordinateur même si aucune connexion téléphonique ou Internet n'est disponible. La connexion automatique à Windows doit être activée pour que l'utilisateur puisse utiliser Local Self Help. Dans le cas contraire, Local Self Help ne fonctionne pas.
Longueur minimum des réponses	Définit la longueur minimale de caractères pour les réponses Local Self Help.
Texte de bienvenue sous Windows	Indique le texte personnalisé à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur le terminal. Avant de pouvoir indiquer le texte ici, veuillez le saisir et l'enregistrer dans la **zone de navigation des stratégies** sous **Textes**.
L'utilisateur peut définir des questions personnalisées	En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles répondre et les distribuer sur le terminal dans la stratégie. Toutefois, vous pouvez également accorder aux utilisateurs le droit de définir des questions personnalisées. Pour autoriser les utilisateurs à définir leurs propres questions, sélectionnez **Oui**.
Challenge / Réponse (C/R)	
Activer la récupération de la connexion (via C/R)	Détermine si un utilisateur est autorisé à générer un challenge dans l'authentification au démarrage SafeGuard afin de pouvoir accéder de nouveau à son ordinateur avec une procédure Challenge/Réponse.

Paramètre de stratégie	Explication
	Oui : L'utilisateur est autorisé à générer un challenge. Dans ce cas, l'utilisateur peut de nouveau accéder à son ordinateur avec une procédure C/R en cas d'urgence. **Non** : L'utilisateur n'est pas autorisé à générer un challenge. Dans ce cas, l'utilisateur ne peut pas exécuter une procédure C/R pour accéder de nouveau à son ordinateur en cas d'urgence.
Autoriser la connexion automatique vers Windows	Permet à l'utilisateur de se connecter automatiquement à Windows après s'être authentifié avec la procédure Challenge/ Réponse. **Oui** : l'utilisateur est automatiquement connecté à Windows. **Non** : l'écran de connexion Windows apparaît. **Exemple** : un utilisateur a oublié son mot de passe. Après la procédure Challenge/Réponse, SafeGuard Enterprise connecte l'utilisateur à l'ordinateur sans mot de passe SafeGuard Enterprise. Dans ce cas, la connexion automatique à Windows est désactivée et l'écran de connexion Windows s'affiche. L'utilisateur ne peut pas se connecter car il ne connaît pas le mot de passe SafeGuard Enterprise (= mot de passe Windows). Le paramètre **Oui** autorise la connexion automatique ; l'utilisateur n'est pas bloqué au niveau de l'écran de connexion Windows.
Texte d'informations	Affiche un texte d'informations lorsqu'une procédure Challenge/ Réponse est lancée dans l'authentification au démarrage SafeGuard. Par exemple : « Veuillez contacter le bureau de support en appelant le 03 20 90 27 29. » Avant d'insérer un texte ici, veuillez le créer sous forme de fichier texte dans la zone de navigation **Stratégies** sous **Textes**.
Images	
	Condition préalable : Les nouvelles images doivent être enregistrées dans la zone de navigation **Stratégies** de SafeGuard Management Center sous **Images**. Les images ne sont disponibles qu'une fois enregistrées. Formats pris en charge : .BMP, .PNG, .JPEG.

Paramètre de stratégie	Explication
Image d’arrière-plan dans l’authentification au démarrage **Image d’arrière-plan dans l’authentification au démarrage (basse résolution)**	Remplace l’arrière-plan SafeGuard Enterprise bleu par une image d’arrière-plan personnalisée. Par exemple, les clients peuvent utiliser le logo de l’entreprise dans l’authentification au démarrage SafeGuard et lors de la connexion à Windows. Taille de fichier maximale pour toutes les images bitmap d’arrière-plan : 500 Ko. Normal : • Résolution : 1024 x 768 (mode VESA) • Couleurs : illimité Basse : • Résolution : 640 x 480 (mode VGA) • Couleurs : 16 couleurs
Image de connexion dans l’authentification au démarrage **Image de connexion dans l’authentification au démarrage (basse résolution)**	Remplace l’image SafeGuard Enterprise affichée lors de la connexion à l’authentification au démarrage SafeGuard par une image personnalisée, par exemple le logo d’une entreprise. Normal : • Résolution : 413 x 140 pixels • Couleurs : illimité Basse : • Résolution : 413 x 140 pixels • Couleurs : 16 couleurs

Paramètre de stratégie	Explication
Chiffrement de fichiers	
Applications sécurisées	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez indiquer des applications comme sécurisées pour leur accorder l'accès aux fichiers chiffrés. Ceci s'avère utile, par exemple, pour activer le logiciel antivirus afin de contrôler les fichiers chiffrés. Saisissez les applications que vous voulez définir comme fiables dans la zone de liste d'édition de ce champ. Les applications doivent être saisies comme des chemins pleinement qualifiés.
Applications ignorées	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez indiquer des applications comme ignorées pour les exempter du chiffrement/déchiffrement des fichiers transparents. Par exemple, si vous définissez un programme de sauvegarde comme une application ignorée, les données chiffrées sauvegardées par le programme restent chiffrées. Saisissez les applications que vous voulez définir comme ignorées dans la zone de liste d'édition de ce champ. Les applications doivent être saisies comme des chemins pleinement qualifiés.
Périphériques ignorés	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez exclure des périphériques entiers (par exemple, des disques) du chiffrement basé sur fichier. Dans la zone de liste d'édition, sélectionnez **Réseau** pour sélectionner un périphérique prédéfini ou saisissez les noms de périphériques requis pour exclure des périphériques données du chiffrement.
Activer le chiffrement permanent	Pour le chiffrement basé sur fichier par File Encryption et SafeGuard Data Exchange, vous pouvez configurer le chiffrement permanent. Avec le chiffrement permanent, les copies des fichiers chiffrés seront chiffrées, même lorsqu'elles sont enregistrées dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement. Ce paramètre de stratégie est activé par défaut.

Paramètre de stratégie	Explication
L’utilisateur est autorisé à définir les clés par défaut	Pour le chiffrement basé sur fichier par Cloud Storage, vous pouvez décider si l’utilisateur est autorisé ou non à définir une clé par défaut pour le chiffrement. S’il est autorisé, la commande **Définir la clé par défaut** est ajoutée dans le menu contextuel Windows Explorer des dossiers de synchronisation Cloud Storage. Les utilisateurs peuvent utiliser la commande pour spécifier des clés par défaut distinctes à utiliser pour le chiffrement des différents dossiers de synchronisation.
Supprimer les clés sur les machines compromises	Ce paramètre de stratégie s’applique uniquement aux ordinateurs protégés par un produit Sophos Endpoint Security permettant de bénéficier d’un état de bon fonctionnement (par exemple ; les versions Sophos Central de Endpoint Security and Control). Lorsque cette stratégie est appliquée, les clés sont retirées des ordinateurs compromis. Lorsque l’ordinateur est marqué comme étant compromis, aucune clé ne lui est assignée.
L’utilisateur est autorisé à déchiffrer les fichiers	Pour Synchronized Encryption, vous pouvez empêcher les utilisateurs de déchiffrer les fichiers manuellement. Si vous définissez cette option sur **Non**, l’option **Déchiffrer le fichier sélectionné** est supprimée du menu par clic droit des fichiers comme indiqué à la section Chiffrement/Déchiffrement manuel des fichiers *(page 451)*. Les fichiers peuvent ensuite être déchiffrés à l’aide des paramètres de stratégie. Sur macOS, ce paramètre est uniquement appliqué si la stratégie est assignée à la machine. Son assignation à un utilisateur n’a aucun effet.
L’utilisateur est autorisé à créer des fichiers protégés par mot de passe	Pour le chiffrement de fichiers par Synchronized Encryption, File Encryption, Cloud Storage et Data Exchange, vous pouvez décider si les utilisateurs vont pouvoir créer des fichiers protégés par mot de passe ou non lors de la configuration. Si vous définissez cette option sur **Oui**, une option **Créer un fichier protégé par mot de passe** est ajoutée du menu par clic droit des fichiers comme indiqué à la section Chiffrement/Déchiffrement manuel des fichiers *(page 451)*.
Paramètres du module de messagerie complémentaire	

Paramètre de stratégie	Explication
Activer le module de messagerie complémentaire	SafeGuard Enterprise intègre un module complémentaire pour Microsoft Outlook qui facilite le chiffrement des pièces jointes. Si vous paramétrez cette option sur **Oui**, les utilisateurs vont être invités à décider du mode de traitement des pièces jointes à chaque fois qu'ils enverront des emails avec pièces jointes. De plus, vous pouvez établir des listes de domaines et indiquer le mode de traitement des pièces jointes lorsqu'elles sont envoyées à ces domaines.
Comportement des domaines autorisés	
Méthode de chiffrement pour les domaines autorisés	Sélectionnez la façon de gérer les pièces jointes dans la liste déroulante : **Chiffré** : toutes les pièces jointes des emails envoyés à un domaine spécifié seront chiffrées. Les utilisateurs ne recevront aucune demande de confirmation. **Aucun chiffrement** : les pièces jointes des emails envoyés à un domaine spécifié ne seront pas chiffrées. Les utilisateurs ne recevront aucune demande de confirmation. **Inchangé** : les fichiers chiffrés seront envoyés chiffrés tandis que les fichiers en clair seront envoyés en clair. Les utilisateurs ne recevront aucune demande de confirmation. **Toujours demander** : les utilisateurs seront invités à confirmer le mode de traitement des pièces jointes à chaque fois qu'ils enverront des pièces jointes à un domaine spécifié.
Liste de domaines autorisés	Saisissez un ou plusieurs domaines sur lesquels la méthode de chiffrement doit être appliquée. Saisissez plusieurs domaines séparés par des virgules. Les caractères de remplacement et les domaines partiellement spécifiés ne sont pas pris en charge.

3.8.17.2 Authentification

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
Accès	
L’utilisateur peut uniquement démarrer à partir du disque dur interne	Ce paramètre est uniquement pris en charge par les terminaux sur lesquels une version antérieure à la version 6.1 de SafeGuard Enterprise est installée. Il était utilisé pour permettre la récupération et autoriser l’utilisateur à démarrer le terminal à partir d’un support externe. Ce paramètre n’est plus appliqué sur les terminaux à partir de la version 6.1. Pour le scénario de récupération concerné, vous pouvez utiliser la récupération avec des clients virtuels comme indiqué dans le Manuel d’administration de SafeGuard Enterprise. Détermine si les utilisateurs peuvent démarrer l’ordinateur à partir du disque dur et/ou d’un autre support. **OUI** : les utilisateurs peuvent démarrer à partir du disque dur uniquement. L’authentification au démarrage SafeGuard n’offre pas la possibilité de démarrer l’ordinateur avec une disquette ou d’autres supports externes. **NON** : les utilisateurs peuvent démarrer l’ordinateur à partir du disque dur, d’une disquette ou d’un support externe (USB, CD, etc.).
Options de connexion	
Mode de connexion	Détermine comment les utilisateurs doivent s’authentifier à l’authentification au démarrage SafeGuard. • **Identifiant utilisateur/Mot de passe** les utilisateurs doivent se connecter avec leurs noms d’utilisateur et leurs mots de passe. • **Token**

Paramètre de stratégie	Explication
	L’utilisateur peut uniquement se connecter à l’authentification au démarrage SafeGuard à l’aide d’un token ou d’une carte à puce. Ce processus offre un niveau de sécurité plus élevé. L’utilisateur doit insérer sa clé lors de la connexion. L’identité de l’utilisateur est vérifiée par la possession de la clé et la présentation du code confidentiel. Après la saisie d’un code confidentiel correct, SafeGuard Enterprise lit automatiquement les données pour la connexion de l’utilisateur. Vous pouvez combiner les paramètres **Identifiant utilisateur/ Mot de passe** et **Token**. Pour vérifier si la connexion fonctionne en utilisant un token, sélectionnez tout d’abord les deux paramètres. Dessélectionnez seulement le mode de connexion **Identifiant utilisateur/Mot de passe** si l’authentification à l’aide du token a réussi. Pour passer d’un mode de connexion à l’autre, veuillez autoriser les utilisateurs à se connecter dès que les deux paramètres sont combinés. Autrement, il se peut qu’ils ne puissent pas se connecter du tout. Vous devez aussi combiner les deux paramètres, si vous voulez autoriser Local Self Help pour la connexion avec le token. • **Empreinte digitale** sélectionnez ce paramètre pour permettre la connexion à l’aide du lecteur d’empreintes digitales Lenovo. Les utilisateurs auxquels cette stratégie s’applique peuvent alors se connecter à l’aide d’une empreinte digitale ou d’un nom d’utilisateur et d’un mot de passe. Cette procédure offre le niveau de sécurité maximal. Lors de la connexion, les utilisateurs font glisser leurs doigts sur le lecteur d’empreintes digitales. Lorsque l’empreinte digitale est correctement reconnue, le processus d’authentification au démarrage SafeGuard lit les codes d’accès de l’utilisateur et connecte l’utilisateur à l’authentification au démarrage. Le système transfère alors les codes d’accès vers Windows et connecte l’utilisateur à l’ordinateur. Après avoir sélectionné ce mode de connexion, l’utilisateur peut se connecter uniquement à l’aide

Paramètre de stratégie	Explication
	d’une empreinte digitale préenregistrée ou d’un nom d’utilisateur et d’un mot de passe. Vous ne pouvez pas utiliser conjointement les procédures de connexion par token et par empreinte digitale sur le même ordinateur.
Afficher les échecs de connexion pour cet utilisateur	**Oui** : suite à la connexion à l’authentification au démarrage SafeGuard et Windows, une boîte de dialogue indique les informations relatives au dernier échec de connexion (nom d’utilisateur/date/heure).
Afficher la dernière connexion utilisateur	**Oui** : suite à la connexion à partir de l’authentification au démarrage SafeGuard et Windows, une boîte de dialogue affiche les informations suivantes concernant la dernière connexion réussie : • Nom d’utilisateur • Date de connexion • Heure de connexion • Codes d’accès de l’utilisateur
Désactiver la déconnexion forcée dans le verrouillage du poste de travail	ce paramètre ne s’applique que sous Windows XP. Windows XP n’est plus pris en charge à partir de SafeGuard Enterprise 6.1. Ce paramètre de stratégie est toujours disponible dans SafeGuard Management Center afin de prendre en charge les clients SafeGuard Enterprise 6 administrés par la version 7.0 du Management Center. Si l’utilisateur souhaite quitter le terminal pendant une courte durée, il peut cliquer sur **Verrouiller le poste de travail** pour empêcher d’autres utilisateurs de l’utiliser et le déverrouiller avec le mot de passe utilisateur. **Non** : l’utilisateur qui a verrouillé l’ordinateur, ainsi qu’un administrateur, peuvent le déverrouiller. Si un administrateur déverrouille l’ordinateur, l’utilisateur connecté est automatiquement déconnecté. **Oui** : seul l’utilisateur peut déverrouiller l’ordinateur. L’administrateur ne pourra pas le déverrouiller et l’utilisateur ne sera pas déconnecté automatiquement.

Paramètre de stratégie	Explication
Activer la présélection utilisateur/ domaine	**Oui** : l'authentification au démarrage SafeGuard enregistre le nom et le domaine du dernier utilisateur connecté. Il n'est donc pas nécessaire que les utilisateurs saisissent leur nom d'utilisateur chaque fois qu'ils se connectent. **Non** : l'authentification au démarrage SafeGuard n'enregistre pas le nom et le domaine du dernier utilisateur connecté.
Liste de comptes de service	Pour éviter que les opérations d'administration sur un ordinateur protégé par SafeGuard Enterprise n'activent l'authentification au démarrage et n'entraînent l'ajout des opérateurs en charge du déploiement comme autant d'utilisateurs possibles de l'ordinateur, SafeGuard Enterprise vous permet de créer des listes de comptes de service pour la connexion Windows sur les terminaux SafeGuard Enterprise. Les utilisateurs de la liste sont traités comme des utilisateurs invités SafeGuard Enterprise. Avant de sélectionner une liste, vous devez créer les listes dans la zone de navigation **Stratégies** sous **Listes de comptes de service**.
Connexion automatique vers Windows	Pour que l'utilisateur puisse autoriser d'autres utilisateurs à accéder à son ordinateur, il doit pouvoir désactiver la connexion automatique vers Windows. • **Laisser l'utilisateur choisir** En sélectionnant/dessélectionnant cette option dans la boîte de dialogue de connexion à l'authentification au démarrage SafeGuard, l'utilisateur peut choisir d'exécuter ou non la connexion automatique à Windows. • **Désactiver la connexion automatique vers Windows** Après la connexion à l'authentification au démarrage SafeGuard, la boîte de dialogue de connexion Windows s'affiche. L'utilisateur doit se connecter manuellement à Windows. • **Appliquer la connexion automatique vers Windows**

Paramètre de stratégie	Explication
	L’utilisateur se connecte toujours automatiquement à Windows.
Options BitLocker	
Mode de connexion BitLocker pour les volumes de démarrage	Les options suivantes sont disponibles : • **Mot de passe** : l’utilisateur doit saisir un mot de passe. • **TPM** : la clé de connexion est stockée sur la puce du TPM (Module de plate-forme sécurisée). • **TPM + PIN** : la clé de connexion est stockée sur la puce du TPM et un code confidentiel est également nécessaire pour la connexion. • **Clé de démarrage** : la clé de connexion est stockée sur une carte mémoire USB. • **TPM + Clé de démarrage** : la clé de connexion est stockée sur la puce du TPM et sur une carte mémoire USB. Les deux sont requises pour établir la connexion. Si vous voulez utiliser **TPM + PIN**, **TPM + Clé de démarrage** ou **Clé de démarrage**, veuillez activer la Stratégie de groupe **Demander une authentification supplémentaire au démarrage** soit dans Active Directory, soit localement sur les ordinateurs. Dans l’Éditeur d’objets de stratégie de groupe (**gpedit.msc**), la Stratégie de groupe se trouve à l’emplacement suivant : **Stratégie Ordinateur local\Configuration ordinateur \Modèles d’administration\Composants Windows \Chiffrement de lecteur BitLocker\Lecteur du système d’exploitation.** Pour utiliser la méthode **Clé de démarrage**, veuillez également activer **Autoriser BitLocker sans un module de plateforme sécurisée compatible** dans la Stratégie de groupe.

Paramètre de stratégie	Explication
	Si le mode de connexion de secours est activé sur le système, le mode de connexion défini ici ne sera pas appliqué.
Mode de connexion de secours BitLocker pour volumes de démarrage	S'il est impossible d'utiliser le paramètre **Mode de connexion BitLocker pour les volumes de démarrage**, SafeGuard Enterprise offre les alternatives de connexion suivantes : • **Mot de passe** : l'utilisateur doit saisir un mot de passe. • **Clé de démarrage** : la clé de connexion est stockée sur une carte mémoire USB. • **Mot de passe ou clé de démarrage** : les cartes mémoire USB seront uniquement utilisées si les mots de passe sont pris en charge sur le système d'exploitation client. • **Erreur** : un message d'erreur s'affiche et le volume n'est pas chiffré. Pour les clients à la version 6.1 ou antérieure, les valeurs **Mot de passe ou clé de démarrage** et **Mot de passe** seront reliés aux anciens paramètres **Carte mémoire USB** et **Erreur**. Les mots de passe sont uniquement pris en charge sur Windows 8 ou version supérieure.
Mode de connexion BitLocker pour volumes non démarrables	Pour les volumes non démarrables (lecteurs de données fixes), les options suivantes sont disponibles : • **Auto-déverrouiller** : si le volume de démarrage est chiffré, une clé externe est créée et stockée sur le volume de démarrage. Le ou les volumes non démarrables seront ensuite déchiffrés automatiquement. Ils seront déverrouillés automatiquement à l'aide de la fonctionnalité Auto-déverrouiller de BitLocker. L'auto-

Paramètre de stratégie	Explication
	déverrouillage fonctionne uniquement si le volume de démarrage est chiffré. Autrement, c'est le mode de connexion de secours qui est utilisé. • **Mot de passe** : l'utilisateur est invité à saisir son mot de passe pour chaque volume non démarrable. • **Clé de démarrage** : les clés de déverrouillage des volumes non démarrables sont stockées sur une clé USB. Les clients à la version 6.1 ou antérieure ignorent ce paramètre de stratégie et utilisent plutôt les valeurs définies pour le mode de connexion des volumes de démarrage. Le module de plate-forme sécurisée (TPM) ne peut pas être utilisé sur les volumes non démarrables. Une carte mémoire USB ou un message d'erreur seront utilisés dans ce cas. Les mots de passe sont uniquement pris en charge sur Windows 8 ou version supérieure. Si le mode de connexion de secours est activé sur le système, le mode de connexion défini ici ne sera pas appliqué.
Mode de connexion de secours BitLocker pour volumes non démarrables	S'il est impossible d'utiliser le paramètre **Mode de connexion BitLocker pour volumes non démarrables**, SafeGuard Enterprise offre les alternatives de connexion suivantes : • **Mot de passe** : l'utilisateur est invité à saisir son mot de passe pour chaque volume non démarrable. • **Clé de démarrage** : les clés sont stockées sur une carte mémoire USB. • **Mot de passe ou clé de démarrage** : les cartes mémoire USB seront uniquement utilisées si les mots de passe sont pris en charge sur le système d'exploitation client. Les clients à la version 6.1 ou antérieure ignorent ce paramètre de stratégie. Ils utilisent plutôt les valeurs

Paramètre de stratégie	Explication
	définies pour le mode de connexion de secours des volumes de démarrage. Comme ils ne peuvent pas gérer les mots de passe, une carte mémoire USB ou un message d'erreur sera utilisé. Les mots de passe sont uniquement pris en charge sur Windows 8 ou version supérieure.
Échecs de connexion	
Nombre maximal d'échecs de connexion	Détermine le nombre de tentatives de connexion d'un utilisateur avec un nom d'utilisateur ou un mot de passe non valide. Par exemple, après trois tentatives successives de saisie d'un nom d'utilisateur ou d'un mot de passe incorrect, une quatrième tentative verrouille l'ordinateur.
Messages d'échec de connexion dans l'authentification au démarrage (POA)	Définit le niveau de détail des messages d'échec de connexion: • **Standard** : affiche une brève description. • **Détaillé** : affiche des informations plus détaillées.
Options de token	
Action si l'état de connexion du token est perdu	Définit le comportement après suppression du token de l'ordinateur : Les actions possibles sont les suivantes : • **Verrouiller l'ordinateur** • **Ouvrir la boîte de dialogue du code confidentiel** • **Aucune action**
Autoriser le déblocage du token	Détermine si le token peut être débloqué lors de la connexion.

Paramètre de stratégie	Explication
Options de verrouillage	
Verrouiller l’écran après X minutes d’inactivité	Détermine la durée après laquelle un poste de travail non utilisé est automatiquement verrouillé. La valeur par défaut est 0 minutes. Le poste de travail ne sera pas verrouillé si cette valeur reste inchangée.
Verrouiller l’écran au retrait du token	Détermine si l’écran est verrouillé lorsqu’un token est retiré au cours d’une session.
Verrouiller l’écran après mise en veille	Détermine si l’écran est verrouillé lors de la réactivation de l’ordinateur du mode veille.

3.8.17.3 Règles de syntaxe des codes confidentiels

Dans les stratégies du type **Code confidentiel**, vous définissez les paramètres des codes confidentiels du token. Ces paramètres ne s’appliquent pas aux codes confidentiels utilisés pour la connexion aux terminaux chiffrés par BitLocker. Retrouvez plus de renseignements sur les codes confidentiels BitLocker à la section Codes confidentiels et mots de passe *(page 323)*.

Les codes confidentiels peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau code confidentiel, n’utilisez pas de caractère avec la combinaison ALT + <caractère> car ce mode de saisie n’est pas disponible dans l’authentification au démarrage SafeGuard.

Remarque : Définissez des règles de code confidentiel dans SafeGuard Management Center ou dans Active Directory, mais pas dans les deux.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
Code confidentiel	
Longueur minimum du code confidentiel	Indique le nombre de caractères que doit contenir un code confidentiel lorsqu’il est modifié par l’utilisateur. La valeur requise peut être saisie directement ou augmentée/réduite à l’aide des boutons en forme de flèche.
Longueur maximale du code confidentiel	Indique le nombre maximum de caractères que peut contenir un code confidentiel lorsqu’il est modifié par l’utilisateur. La valeur

Paramètre de stratégie	Explication
	requise peut être saisie directement ou augmentée/réduite à l'aide des boutons en forme de flèche.
Nombre minimum de lettres **Nombre minimum de chiffres** **Nombre minimum de caractères spéciaux**	Ces paramètres spécifient qu'un code confidentiel ne doit pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais une combinaison de ces 2 au moins (par exemple, 15fleur). Ce paramètre n'est pratique que si la longueur minimale définie pour le code confidentiel est supérieure à 2.
Interdire l'utilisation consécutive de touches horizontales	Concerne les touches disposées successivement sur les rangées du clavier. Par exemple, « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire l'utilisation consécutive de touches verticales	Concerne les touches disposées successivement sur les colonnes du clavier. Par exemple « wqa1 », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme codes confidentiels. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire l'utilisation de trois caractères consécutifs ou plus	L'activation de cette option interdit les séquences de touches • qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ou « cba »). • constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).
Interdire l'utilisation du nom d'utilisateur en tant que code confidentiel	Détermine si le nom d'utilisateur et le code confidentiel peuvent être identiques. **Oui** : le nom d'utilisateur Windows et le code confidentiel doivent être différents. **Non** : l'utilisateur peut utiliser son nom d'utilisateur Windows comme code confidentiel.
Utiliser la liste des codes confidentiels interdits	Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les codes confidentiels. Les séquences de caractères sont stockées dans la **Liste de codes confidentiels interdits** (par exemple, un fichier .txt).

Paramètre de stratégie	Explication
Liste de codes confidentiels interdits	Définit les séquences de caractères à ne pas utiliser pour les codes confidentiels. Si un utilisateur utilise un code confidentiel non autorisé, un message d'erreur s'affiche. **Condition préalable :** Une liste (fichier) de codes confidentiels interdits doit être enregistrée dans SafeGuard Management Center, dans la zone de navigation de stratégie sous **Textes**. Retrouvez plus de renseignements à la section Création de listes de codes confidentiels interdits à utiliser dans les stratégies *(page 276)*. La liste n'est disponible qu'après l'enregistrement. • Taille de fichier maximale : 50 Ko • Format pris en charge : Unicode **Définition des codes confidentiels interdits** Dans la liste, les codes confidentiels interdits sont séparés par un saut de ligne. *Caractère générique :* Le caractère générique « * » peut représenter tout caractère et tout nombre de caractères dans un code confidentiel. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme code confidentiel. **Remarque :** • Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. • Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier. • L'option **Utiliser la liste des codes confidentiels interdits** doit être activée.

Paramètre de stratégie	Explication
Respecter la casse	Ce paramètre ne s'applique qu'avec **Utiliser la liste des codes confidentiels interdits** et **Interdire l'utilisation du nom d'utilisateur en tant que code confidentiel**. **Exemple 1 :** vous avez saisi « tableau » dans la liste des codes confidentiels interdits. Si l'option **Respecter la casse** est définie sur **OUI**, les variantes supplémentaires du code confidentiel telles que TABLEAU, TablEAU ne seront pas acceptées et la connexion sera refusée. **Exemple 2 :** le nom d'utilisateur « ROussos » est saisi. Si l'option **Respecter la casse** est définie sur **Oui** et si l'option **Interdire l'utilisation du nom d'utilisateur en tant que code confidentiel** est définie sur **Non**, l'utilisateur ROussos ne peut pas utiliser de variante du nom d'utilisateur (par exemple, roussos ou rOussOS) en tant que code confidentiel.
Modifications	
Changer le code confidentiel après un min. de (jours)	Détermine la période pendant laquelle un code confidentiel ne peut pas être modifié. Ce paramètre empêche l'utilisateur de changer trop souvent de code confidentiel au cours d'une période donnée. **Exemple :** L'utilisateur Bertrand définit un nouveau code confidentiel (par exemple, « 13jk56 »). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de changer le code confidentiel par « 13jk56 ». Le changement de code confidentiel est refusé car Madame Bertrand ne peut définir un nouveau code confidentiel qu'après un délai de cinq jours.
Changer de code confidentiel après un max. de (jours)	L'utilisateur doit définir un nouveau code confidentiel une fois la période définie expirée. Si la période est définie sur 999 jours, aucun changement de code confidentiel n'est requis.
Avertir d'un changement obligatoire avant (jours)	Un message d'avertissement s'affiche « n » jours avant l'expiration du code confidentiel pour rappeler à l'utilisateur de changer son code confidentiel dans « n » jours. L'utilisateur peut également le changer immédiatement.
Paramètres généraux	
Masquer le code confidentiel dans l'authentification au démarrage	Indique si les chiffres sont masqués lors de la saisie des mots de passe. Si cette option est activée, vous ne verrez rien s'afficher lors de la saisie du code confidentiel à l'authentification au démarrage. En cas contraire, les codes confidentiels sont cachés par des astérisques.

Paramètre de stratégie	Explication
Longueur de l’historique du code confidentiel	Détermine à quel moment des codes confidentiels déjà utilisés peuvent l’être à nouveau. Il convient de définir la longueur d’historique avec le paramètre **Changer de code confidentiel après un max. de (jours)**. **Exemple :** La longueur d’historique du code confidentiel pour l’utilisateur Bertrand est définie à 4 et le nombre de jours à l’issue desquels l’utilisateur doit changer son code confidentiel est de 30. M. Bertrand se connecte actuellement en utilisant le code confidentiel « Informatique ». Lorsque la période de 30 jours expire, il est invité à changer son code confidentiel. M. Bertrand saisit « Informatique » comme nouveau code confidentiel et reçoit un message d’erreur indiquant que ce code confidentiel a déjà été utilisé et qu’il doit en sélectionner un nouveau. M. Bertrand ne peut pas utiliser le code confidentiel « Informatique » avant la quatrième invitation de changement du code confidentiel (en d’autres termes, longueur d’historique du code confidentiel = 4).

Création de listes de codes confidentiels interdits à utiliser dans les stratégies

Pour les stratégies de type **Code confidentiel**, une liste de codes confidentiels interdits peut être créée afin de définir les séquences de caractères à ne pas utiliser dans les codes confidentiels. Les codes confidentiels sont utilisés pour la connexion avec le token. Retrouvez plus de renseignements à la section Tokens et cartes à puce *(page 195)*.

Les fichiers texte contenant les informations requises doivent être créés avant de pouvoir les enregistrer dans SafeGuard Management Center. La taille maximale de ces fichiers texte est de **50 Ko**. SafeGuard Enterprise utilise les textes codés en Unicode UTF-16 uniquement. Si vous créez les fichiers texte dans un autre format, ils seront automatiquement convertis lorsqu’ils seront enregistrés.

Remarque : Dans les listes, les codes confidentiels interdits sont séparés par un saut de ligne.

Pour enregistrer les fichiers texte :

1. Dans la zone de navigation Stratégies, cliquez avec le bouton droit de la souris sur **Textes** et sélectionnez **Nouveau > Texte**.
2. Saisissez le nom du texte à afficher dans le champ **Nom de l’élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte créé auparavant. Un message s’affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Textes** dans la zone de navigation des stratégies. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque : Grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

3.8.17.4 Règles de syntaxe des mots de passe

Dans les stratégies du type **Mot de passe**, vous définissez les règles des mots de passe utilisés pour vous connecter au système. Ces paramètres ne s'appliquent pas aux mots de passe utilisés pour la connexion aux terminaux chiffrés par BitLocker. Retrouvez plus de renseignements sur les mots de passe BitLocker à la section Codes confidentiels et mots de passe *(page 323)*.

Les mots de passe peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau mot de passe, n'utilisez pas de caractère avec la combinaison ALT + <caractère> car ce mode de saisie n'est pas disponible dans l'authentification au démarrage SafeGuard. Les règles relatives aux mots de passe utilisés pour se connecter au système sont définies dans des stratégies du type **Mot de passe**.

Remarque : Retrouvez plus de renseignements sur l'application d'une stratégie de mot de passe fort à la section Recommandations en matière de sécurité *(page 456)* ainsi que dans le *Manuel SafeGuard Enterprise pour une utilisation conforme à la certification*.

L'application de règles de mots de passe et l'historique des mots de passe peuvent seulement être garantis si le fournisseur de codes d'accès SGN est utilisé en permanence. Définissez des règles de mots de passe soit dans le SafeGuard Management Center, soit dans Active Directory, pas dans les deux.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
Mot de passe	
Longueur minimum du mot de passe	Indique le nombre maximum de caractères que doit contenir un mot de passe lorsqu'il est modifié par l'utilisateur. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des boutons en forme de flèche.
Longueur maximale du mot de passe	Indique le nombre maximum de caractères que peut contenir un mot de passe lorsque l'utilisateur en change. La valeur requise

Paramètre de stratégie	Explication
	peut être saisie directement ou augmentée/réduite à l'aide des boutons en forme de flèche.
Nombre minimum de lettres **Nombre minimum de chiffres** **Nombre minimum de caractères spéciaux**	Ces paramètres spécifient qu'un mot de passe ne doit pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais une combinaison de ces 2 au moins (par exemple, 15fleur). Ce paramètre n'est pratique que si la longueur minimale définie pour le mot de passe est supérieure à 2.
Interdire l'utilisation consécutive de touches horizontales	Concerne les touches disposées successivement sur les rangées du clavier. Par exemple, « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire l'utilisation consécutive de touches verticales	Concerne les touches disposées successivement sur les colonnes du clavier. Par exemple « wqa1 », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mot de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire l'utilisation de trois caractères consécutifs ou plus	L'activation de cette option interdit les séquences de touches • qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ou « cba »). • constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).
Interdire l'utilisation du nom d'utilisateur en tant que mot de passe	Indique qu'un nom d'utilisateur ne doit pas être utilisé en tant que mot de passe. **Oui** : le nom d'utilisateur Windows et le mot de passe doivent être différents. **Non** : l'utilisateur peut utiliser son nom d'utilisateur Windows comme mot de passe.
Utiliser la liste des mots de passe interdits	Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les mots de passe. Les séquences de caractères sont stockées dans la **Liste des mots de passe interdits** (par exemple, un fichier .txt).

Paramètre de stratégie	Explication
Liste des mots de passe interdits	Définit les séquences de caractères à ne pas utiliser pour les mots de passe. Si un utilisateur utilise un mot de passe non autorisé, un message d'erreur s'affiche. Une liste (fichier) de mots de passe interdits doit être enregistrée dans SafeGuard Management Center, dans la zone de navigation des stratégies sous **Textes**. Retrouvez plus de renseignements à la section Création d'une liste de mots de passe interdits à utiliser dans les stratégies *(page 282)*. La liste n'est disponible qu'après l'enregistrement. Taille de fichier maximale : 50 Ko Format pris en charge : Unicode **Définition de mots de passe interdits** Dans la liste, les mots de passe interdits sont séparés par un saut de ligne. *Caractère générique* : Le caractère générique « * » peut représenter tout caractère et tout nombre de caractères dans un mot de passe. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme mot de passe. **Remarque :** • Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. • Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier. • L'option **Utiliser la liste des mots de passe interdits** doit être activée.
Respecter la casse	Ce paramètre ne s'applique qu'avec **Utiliser la liste des mots de passe interdits** et **Interdire l'utilisation du nom d'utilisateur en tant que mot de passe**. **Exemple 1 :** vous avez saisi « tableau » dans la liste des mots de passe interdits. Si l'option **Respecter la casse** est définie sur **Oui**, les variantes supplémentaires du mot de passe telles que

Paramètre de stratégie	Explication
	TABLEAU, TablEAU ne seront pas acceptées et la connexion sera refusée. **Exemple 2 :** le nom d'utilisateur « ROussos » est saisi. Si l'option **Respecter la casse** est définie sur **Oui** et si l'option **Interdire l'utilisation du nom d'utilisateur en tant que mot de passe** est définie sur **Non**, l'utilisateur ROussos ne peut pas utiliser de variante du nom d'utilisateur (par exemple, roussos ou rOussOS) en tant que mot de passe.
Modifications	
Autoriser le changement de mot de passe autorisée après un min. de (jours)	Détermine la période pendant laquelle un mot de passe ne peut être modifié. Ce paramètre empêche l'utilisateur de changer trop souvent de mot de passe au cours d'une période donnée. Si l'utilisateur est forcé à changer son mot de passe par Windows ou s'il modifie son mot de passe après l'affichage du message d'avertissement indiquant que le mot de passe expirera dans X jours, ce paramètre ne sera pas évalué. **Exemple :** L'utilisateur Bertrand définit un nouveau mot de passe (par exemple, « 13jk56 »). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de changer le mot de passe en « 13jk56 ». Le changement de mot de passe est refusé car l'utilisateur Bertrand ne peut définir un nouveau mot de passe qu'après un délai de cinq jours.
Le mot de passe expire après (jours)	Si vous paramétrez cette option, l'utilisateur doit définir un nouveau mot de passe une fois la période définie expirée.
Avertir d'un changement obligatoire avant (jours)	Un message d'avertissement s'affiche «n» jours avant l'expiration du mot de passe pour rappeler à l'utilisateur de changer son mot de passe dans «n» jours. L'utilisateur peut également le changer immédiatement.
Paramètres généraux	
Masquer le mot de passe à l'authentification au démarrage	Indique si les caractères sont masqués lors de la saisie des mots de passe. Si cette option est activée, vous ne verrez rien s'afficher lors de la saisie du mot de passe à l'authentification au démarrage. En cas contraire, les mots de passe sont cachés par des astérisques.
Longueur de l'historique de mot de passe	Détermine à quel moment des mots de passe déjà utilisés peuvent l'être à nouveau. Il est judicieux de définir la longueur d'historique conjointement au paramètre **Expiration du mot de passe après (jours)**.

Paramètre de stratégie	Explication
	Exemple : La longueur d'historique du mot de passe pour l'utilisateur Bertrand est définie à 4 et le nombre de jours à l'issue desquels l'utilisateur doit changer son mot de passe est de 30. M. Bertrand se connecte actuellement en utilisant le mot de passe « Informatique ». Lorsque la période de 30 jours expire, il est invité à modifier son mot de passe. M. Bertrand saisit « Informatique » comme nouveau mot de passe et reçoit un message d'erreur indiquant que ce mot de passe a déjà été utilisé et qu'il doit en sélectionner un nouveau. M. Bertrand ne peut pas utiliser le mot de passe « Informatique » avant la quatrième invitation de changement du mot de passe (en d'autres termes, longueur d'historique du mot de passe = 4). **Remarque :** Si vous définissez la longueur de l'historique de mot de passe sur 0, l'utilisateur peut utiliser son ancien mot de passe comme nouveau mot de passe. Ceci n'est pas la bonne marche à suivre et doit être évité autant que possible.
Synchronisation du mot de passe de l'utilisateur avec les autres clients SGN	Ce champ détermine la procédure de synchronisation des mots de passe lorsque des utilisateurs se servant de plusieurs terminaux SafeGuard Enterprise, et définis comme les utilisateurs de ces ordinateurs, changent leurs mots de passe. Les options suivantes sont disponibles : • Lent (attendre que l'utilisateur se connecte) Si un utilisateur change son mot de passe sur un terminal SafeGuard Enterprise et s'il tente de se connecter à un autre ordinateur sur lequel il est également enregistré, il doit tout d'abord se connecter avec son ancien mot de passe à l'authentification au démarrage. La synchronisation du mot de passe n'est effectuée qu'après la connexion avec l'ancien mot de passe. • Rapide (attendre la connexion de la machine) Si un utilisateur change son mot de passe sur un terminal SafeGuard Enterprise, la synchronisation du mot de passe avec d'autres ordinateurs, sur lesquels l'utilisateur est également enregistré, est effectuée dès que l'autre ordinateur a établi une connexion avec le serveur. C'est

Paramètre de stratégie	Explication
	le cas, par exemple, lorsqu'un autre utilisateur, également enregistré en tant qu'utilisateur de l'ordinateur, se connecte simultanément à l'ordinateur.

Création d'une liste de mots de passe interdits à utiliser dans les stratégies

Pour les stratégies de type **Mot de passe**, vous pouvez créer une liste de mots de passe interdits pour définir les séquences de caractères qui ne doivent pas être utilisées dans les mots de passe.

Remarque : Dans les listes, les mots de passe non autorisés sont séparés par un saut de ligne.

Les fichiers texte contenant les informations requises doivent être créés avant de pouvoir les enregistrer dans SafeGuard Management Center. La taille maximale de ces fichiers texte est de **50 Ko**. SafeGuard Enterprise utilise les textes codés en Unicode UTF-16 uniquement. Si vous créez les fichiers texte dans un autre format, ils seront automatiquement convertis lorsqu'ils seront enregistrés.

Si un fichier est converti, un message apparaît.

Pour enregistrer les fichiers texte :

1. Dans la zone de navigation Stratégies, cliquez avec le bouton droit de la souris sur **Textes** et sélectionnez **Nouveau > Texte**.
2. Saisissez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur **[...]** pour sélectionner le fichier texte créé auparavant. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Textes** dans la zone de navigation des stratégies. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

Remarque : Utilisez le bouton **Modifier le texte** pour ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

3.8.17.5 Phrase secrète pour SafeGuard Data Exchange

L'utilisateur doit entrer une phrase secrète qui est utilisée pour générer des clés locales pour un échange sécurisé des données avec SafeGuard Data Exchange. Les clés générées sur les terminaux

sont également stockées dans la base de données SafeGuard Enterprise. Dans les stratégies du type **Phrase secrète**, vous définissez les conditions requises correspondantes.

Retrouvez plus de renseignements sur SafeGuard Data Exchange à la section SafeGuard Data Exchange *(page 358)*.

Retrouvez plus de renseignements sur SafeGuard Data Exchange et sur SafeGuard Portable sur le terminal dans le *Manuel d'utilisation de SafeGuard Enterprise*, au chapitre *SafeGuard Data Exchange*.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
Phrase secrète	
Longueur minimum de la phrase secrète	Définit le nombre minimum de caractères de la phrase secrète à partir de laquelle la clé est générée. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Longueur maximale de la phrase secrète	Définit le nombre maximum de caractères de la phrase secrète. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Nombre minimum de lettres **Nombre minimum de chiffres** **Nombre minimum de caractères spéciaux**	Ce paramètre spécifie qu'une phrase secrète ne peut pas contenir seulement des lettres, des nombres ou des symboles mais doit comporter une combinaison de ces 2 au moins (par exemple, 15 fleur). Ces paramètres ne sont utiles que si la longueur minimale définie pour la phrase secrète est supérieure à 2.
Interdire l'utilisation consécutive de touches horizontales	Concerne les touches disposées successivement sur les rangées du clavier. Par exemple, « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire l'utilisation consécutive de touches verticales	Concerne les touches disposées successivement sur les colonnes du clavier. Par exemple « wqa1 », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux caractères adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mots de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire l'utilisation de trois caractères consécutifs ou plus	L'activation de cette option interdit les séquences de touches • qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ou « cba »).

Paramètre de stratégie	Explication
	• constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).
Interdire l’utilisation du nom d’utilisateur en tant que phrase secrète	Détermine si le nom d’utilisateur et la phrase secrète peuvent être identiques. **Oui** : le nom d’utilisateur Windows et la phrase secrète doivent être différents. **Non** : l’utilisateur peut utiliser son nom d’utilisateur Windows comme phrase secrète.
Respecter la casse	Ce paramètre est effectif lorsque l’option **Interdire l’utilisation du nom d’utilisateur en tant que phrase secrète** est active. **Exemple :** le nom d’utilisateur « ROussos » est saisi. Si l’option **Respecter la casse** est définie sur OUI et si **Interdire l’utilisation du nom d’utilisateur en tant que phrase secrète** est définie sur NON, l’utilisateur ROussos ne peut pas utiliser de variante du nom d’utilisateur (par exemple, roussos ou rOussOS) en tant que phrase secrète.

3.8.17.6 Listes d’autorisation pour les stratégies de protection des périphériques pour le chiffrement basé sur fichier

Dans SafeGuard Management Center, vous pouvez sélectionner des listes d’autorisation comme cibles pour les stratégies du type **Protection des périphériques** pour le chiffrement basé sur fichier. Ceci vous permet de créer des stratégies de chiffrement pour des modèles de périphériques spécifiques ou même pour des périphériques distincts.

Avant de sélectionner une liste d’autorisation comme cible pour une stratégie **Protection des périphériques**, vous devez la créer et l’enregistrer dans SafeGuard Management Center. Vous pouvez définir des listes d’autorisation pour des modèles de périphériques de stockage spécifiques (par exemple, un iPod, des périphériques USB provenant d’un fournisseur particulier) ou pour des périphériques de stockage distincts en fonction du numéro de série. Vous pouvez ajouter manuellement les périphériques aux listes d’autorisation ou utiliser les résultats d’un contrôle Safend Auditor. Retrouvez plus de renseignements dans la *documentation de Safend Auditor*.

Ensuite, vous pouvez sélectionner la liste d’autorisation en tant que cible lorsque vous créez la stratégie **Protection des périphériques**.

Remarque : Si vous sélectionnez une liste d’autorisation comme cible pour une stratégie du type **Protection des périphériques**, vous pouvez seulement sélectionner **Basé sur fichier** ou **Aucun chiffrement** comme **Mode de chiffrement du support**. Si vous sélectionnez **Aucun chiffrement** pour une stratégie **Protection des périphériques** avec une liste d’autorisation, cette

stratégie n’exclut aucun périphérique du chiffrement, si une autre stratégie est appliquée qui spécifie le chiffrement basé sur volume.

Remarque : Concernant les périphériques SafeStick de BlockMaster, des conditions requises particulières s’appliquent. Ces périphériques ont des identifications différentes pour les administrateurs et les utilisateurs sans droits administrateur. Pour une gestion cohérente dans SafeGuard Enterprise, vous devez ajouter les deux identifications aux listes d’autorisation. SafeGuard PortAuditor détecte les deux identifications, si un périphérique SafeStick a été ouvert au moins une fois sur l’ordinateur contrôlé par SafeGuard PortAuditor.

Création de listes d’autorisation pour les stratégies de protection des périphériques pour le chiffrement basé sur fichier

1. Dans la zone de navigation **Stratégies**, sélectionnez **Liste d’autorisation**.
2. Dans le menu contextuel **Liste d’autorisation**, cliquez sur **Nouvelle > Liste d’autorisation**.
3. Sélectionnez le type de liste d’autorisation :

   - Pour créer une liste d’autorisation pour des modèles de périphériques spécifiques, sélectionnez **Modèles de périphériques de stockage**.

   - Pour créer une liste d’autorisation pour des périphériques spécifiques en fonction du numéro de série, sélectionnez **Périphériques de stockage distincts**.

4. Sous **Source de liste d’autorisation**, indiquez comment vous voulez créer la liste d’autorisation :

   - Pour saisir manuellement les périphériques, sélectionnez **Créer manuellement une liste d’autorisation**.

     Lorsque vous cliquez sur **OK**, une liste d’autorisation vide s’ouvre dans SafeGuard Management Center. Dans cette liste d’autorisation vide, vous pouvez créer manuellement des entrées. Pour ajouter une nouvelle entrée, cliquez sur l’icône verte **Ajouter (Insérer)** dans la barre d’outils de SafeGuard Management Center.

     Remarque : Pour récupérer les chaînes correspondantes d’un périphérique dans le Gestionnaire de périphériques Windows, ouvrez la fenêtre **Propriétés** du périphérique et observez les valeurs des propriétés **Numéros d’identification du matériel** et **Chemin d’accès à l’instance du périphérique**. Seules les interfaces suivantes sont prises en charge : USB, 1394, PCMCIA et PCI.

   - Si vous voulez utiliser le résultat d’un contrôle des terminaux par Safend Auditor comme source, sélectionnez **Importer le résultat de Safend Auditor**.

Les résultats de l’analyse Safend Auditor doivent être disponibles (fichier XML) si vous voulez créer la liste d’autorisation avec cette source. Pour sélectionner le fichier, cliquez sur le bouton **[...]**.

Retrouvez plus de renseignements dans la *documentation de Safend Auditor*.

Cliquez sur **OK** pour afficher le contenu du fichier importé dans SafeGuard Management Center.

La liste d’autorisation apparaît sous **Listes d’autorisation** dans la zone de navigation **Stratégies**. Vous pouvez la sélectionner lorsque vous créez des stratégies du type **Protection des périphériques** pour le chiffrement basé sur fichier.

Sélection des listes d’autorisation comme cibles des stratégies de protection des périphériques pour le chiffrement basé sur fichier

Condition préalable : La liste d’autorisation requise doit avoir été créée dans SafeGuard Management Center.

1. Dans la zone de navigation de SafeGuard Management Center, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis sélectionnez **Nouveau**.
3. Sélectionnez **Protection des périphériques**.

   Une boîte de dialogue permettant de nommer la nouvelle stratégie s’affiche.

4. Saisissez un nom et éventuellement une description de la nouvelle stratégie.
5. Sous **Cible de protection de périphérique**, sélectionnez la liste d’autorisation correspondante :

   - Si vous avez créé une liste d’autorisation pour les modèles de périphériques de stockage, elle apparaît sous **Modèles de périphériques de stockage**.

   - Si vous avez créé une liste d’autorisation pour les périphériques de stockage distincts, elle apparaît sous **Périphériques de stockage distincts**.

6. Cliquez sur **OK**.

La liste d’autorisation a été sélectionnée comme cible pour la stratégie de **Protection des périphériques**. Une fois que la stratégie a été transférée sur le terminal, le mode de chiffrement sélectionné dans la stratégie s’applique.

3.8.17.7 Protection des périphériques

Les stratégies du type **Protection des périphériques** couvrent les paramètres pour le chiffrement des données sur différents périphériques de stockage des données. Le chiffrement peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents. Les stratégies de type **Protection des périphériques** incluent également des paramètres pour SafeGuard Data Exchange, SafeGuard Cloud Storage et SafeGuard Portable. Retrouvez plus de renseignements aux sections SafeGuard Data Exchange *(page 358)* et Stockage Cloud *(page 351)*. Retrouvez plus de renseignements sur SafeGuard Data Exchange, SafeGuard Cloud Storage et SafeGuard Portable sur le terminal dans le *Manuel d'utilisation de SafeGuard Enterprise*.

Lors de la création d'une stratégie de protection des périphériques, vous devez d'abord spécifier la cible de la protection des périphériques. Les cibles possibles sont les suivantes :

- Stockage de masse (volumes de démarrage ou non démarrables)
- Supports amovibles sur les terminaux Windows

  Sur macOs, une stratégie de type **Chiffrement de fichiers** avec l'espace réservé **<Amovibles>** en tant que **Chemin** est nécessaire pour chiffrer les fichiers sur les supports amovibles. Retrouvez plus de renseignements à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.
- Lecteurs optiques
- Lettres de lecteur
- Modèles de périphériques de stockage
- Périphériques de stockage distincts
- Définitions Cloud Storage

Pour chaque cible, créez une stratégie distincte.

Remarque : Supports amovibles : une stratégie qui spécifie le chiffrement basé sur volume des lecteurs amovibles et qui permet à l'utilisateur de choisir une clé dans une liste (par exemple, **Toute clé du jeu de clés utilisateur**) peut être contournée par l'utilisateur en ne choisissant aucune clé. Pour s'assurer que les lecteurs amovibles sont toujours chiffrés, utilisez une stratégie de chiffrement basée sur fichier ou définissez explicitement une clé dans la stratégie de chiffrement basée sur volume.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
Mode de chiffrement des supports	Permet de protéger les périphériques (ordinateurs de bureau et portables, etc.) ainsi que tous types de supports amovibles.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
	Ce paramètre est obligatoire. L’objectif essentiel consiste à chiffrer toutes les données stockées sur des périphériques de stockage locaux ou externes. La méthode de fonctionnement transparente permet aux utilisateurs de continuer à utiliser leurs applications courantes, par exemple Microsoft Office. Le chiffrement transparent signifie que toutes les données chiffrées (dans des répertoires ou dans des volumes chiffrés) sont automatiquement déchiffrées dans la mémoire principale dès qu’elles sont ouvertes dans un programme. Un fichier est automatiquement chiffré de nouveau lorsqu’il est enregistré. Les options suivantes sont disponibles : • **Aucun chiffrement** • **Basé sur le volume** (= chiffrement transparent basé sur secteur) Garantit que toutes les données sont chiffrées (y compris les fichiers de démarrage, les fichiers d’échange, les fichiers inactifs/de mise en veille prolongée, les fichiers temporaires, les informations de répertoire, etc.) sans que l’utilisateur ait à modifier ses habitudes de travail ou tenir compte de problèmes de sécurité. • **Basé sur fichier** (= chiffrement transparent basé sur fichier, Chiffrement Smart Media) Garantit que toutes les données sont chiffrées (à l’exception du support de démarrage et des informations de répertoire) avec l’avantage que même les supports optiques tels que les CD/DVD peuvent être chiffrés et que les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard Enterprise n’est pas installé (si les stratégies l’autorisent).

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
	Pour les stratégies avec listes d'autorisation, vous pouvez uniquement sélectionner **Aucun chiffrement** ou **Basé sur fichier**.
Paramètres généraux	
Algorithme à utiliser pour le chiffrement	Définit l'algorithme de chiffrement. Liste des algorithmes utilisables avec les normes respectives : AES256 : 32 octets (256 bits) AES128 : 16 octets (128 bits)
Clé à utiliser pour le chiffrement	Définit la clé utilisée pour le chiffrement. Vous pouvez définir des clés spécifiques (clé machine ou une clé définie par ex.) ou vous pouvez autoriser l'utilisateur à sélectionner une clé. Vous pouvez également limiter les clés qu'un utilisateur est autorisé à utiliser. Les options suivantes sont disponibles : • **Toute clé du jeu de clés utilisateur** Toutes les clés du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. Cette option doit être sélectionnée si vous définissez une stratégie de chiffrement basé sur fichier pour un terminal non administré protégé par SafeGuard Enterprise (autonome). • **Toute clé du jeu de clés utilisateur sauf la clé utilisateur** Toutes les clés sauf celles du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles. • **Toute clé de groupe du jeu de clés utilisateur** Toutes les clés de groupe du jeu de clés d'un utilisateur sont affichées et celui-ci peut sélectionner l'une d'entre elles.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
	• **Clé machine définie** La clé de la machine est utilisée et l’utilisateur ne peut pas sélectionner de clé. Elle est uniquement disponible sur un terminal sur lequel le chiffrement par volume est installé (BitLocker ou SafeGuard Full Disk Encryption). Une stratégie définissant la **Clé machine définie** en tant que clé à utiliser pour le chiffrement de fichiers (par exemple pour SafeGuard Data Exchange) ne sera pas appliquée sur un terminal sur lequel le chiffrement par volume n’est pas installé. Les données ne peuvent pas être chiffrées. Cette option doit être sélectionnée si vous définissez une stratégie de chiffrement basé sur volume pour un terminal non administré protégé par SafeGuard Enterprise (mode autonome). Si vous sélectionnez néanmoins **Toute clé du jeu de clés utilisateur** et si l’utilisateur sélectionne une clé créée localement pour le chiffrement basé sur volume, l’accès à ce volume sera refusé. • **Toute clé du jeu de clés utilisateur sauf les clés créées localement** Toutes les clés sauf les clés générées localement à partir d’un jeu de clés sont affichées et l’utilisateur peut sélectionner l’une d’entre elles. • **Clé définie dans la liste** L’administrateur peut sélectionner toutes les clés disponibles lorsqu’il définit des stratégies dans Management Center. La clé doit être sélectionnée sous **Clé définie pour le chiffrement**.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
	Stratégies pour le terminal non administré protégé par SafeGuard Enterprise (autonome) : Seule l'option **Toute clé du jeu de clés utilisateur** peut être utilisée lors de la création de stratégies pour des terminaux non administrés. La création de clés locales doit en outre être autorisée pour ce type de terminal. Si la fonction de phrase secrète des supports est activée pour des terminaux non administrés, la clé de chiffrement de support est utilisée automatiquement comme **Clé définie pour le chiffrement**. en effet, aucune clé de groupe n'est disponible sur les terminaux non administrés. La sélection d'une autre clé sous **Clé définie pour le chiffrement** lors de la création d'une stratégie de support amovible pour des clients autonomes n'a aucun effet.
Clé définie pour le chiffrement	Cliquez sur **[...]** pour afficher la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour rechercher des clés et en sélectionner une dans la liste qui apparaît. Dans le cas d'une stratégie de type **Protection des périphériques** avec la cible **Supports amovibles**, cette clé sert à chiffrer la clé de chiffrement de support lorsque la fonction de phrase secrète des supports est activée (**L'utilisateur peut définir une phrase secrète des supports pour les périphériques** définie sur **Oui**). Pour ce type de stratégie, veuillez configurer les paramètres **Clé à utiliser pour le chiffrement** et **Clé définie pour le chiffrement**. **Stratégies pour les terminaux non administrés protégés par SafeGuard Enterprise (autonome) :** Si la fonction de phrase secrète des supports est activée pour des terminaux non administrés, la clé de chiffrement de support est utilisée automatiquement comme **Clé définie pour le chiffrement**. en effet, aucune clé de groupe n'est disponible sur les terminaux non administrés.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
L’utilisateur est autorisé à créer une clé locale	Ce paramètre détermine si les utilisateurs peuvent générer ou non une clé locale sur leurs ordinateurs. Le paramètre par défaut est **Oui** et les utilisateurs sont autorisés à créer des clés locales. Une stratégie qui interdit aux utilisateurs de créer des clés locales (**L’utilisateur est autorisé à créer une clé locale** définie sur **Non**) sera uniquement appliquée aux terminaux Windows. Les clés locales sont générées sur le terminal selon une phrase secrète saisie par l’utilisateur. La configuration minimale de la phrase secrète est définie dans des stratégies du type **Phrase secrète**. Ces clés sont également enregistrées dans la base de données. L’utilisateur peut les utiliser sur n’importe quel ordinateur auquel il est connecté. Des clés locales peuvent être utilisées pour l’échange de données sécurisé avec SafeGuard Data Exchange (SG DX). Retrouvez plus de renseignements à la section Clés locales *(page 365)*.
Paramètres basés sur le volume	
L’utilisateur peut ajouter ou supprimer des clés d’un volume chiffré	**Oui** : les utilisateurs du terminal peuvent ajouter ou supprimer des clés d’un jeu de clés. La boîte de dialogue s’affiche dans l’onglet **Propriétés/Chiffrement** de la commande du menu contextuel. **Non** : les utilisateurs du terminal ne peuvent pas ajouter de clés.
Réaction aux volumes non chiffrés	Définit de quelle manière SafeGuard Enterprise gère les supports non chiffrés. Les options suivantes sont disponibles : • **Rejeter** (= le support en texte n’est pas chiffré) • **Accepter uniquement les supports vierges et chiffrer**

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
	• **Accepter tous les supports et chiffrer**
L'utilisateur peut déchiffrer le volume	Permet à l'utilisateur de déchiffrer le volume avec une commande du menu contextuel dans l'Explorateur Windows.
Chiffrement initial rapide	Sélectionnez ce paramètre pour activer le mode de chiffrement initial rapide pour le chiffrement basé sur volume. Ce mode réduit le temps nécessaire pour le chiffrement initial sur les terminaux. Ce mode peut conduire à un état moins sécurisé. Retrouvez plus de renseignements dans le Manuel d'administration de SafeGuard Enterprise.
Poursuivre sur les secteurs incorrects	Indique si le chiffrement doit se poursuivre ou être arrêté si des secteurs incorrects sont détectés. Le paramètre par défaut est **Oui**.
Paramètres basés sur le fichier	
Chiffrement initial de tous les fichiers	Démarre automatiquement le chiffrement initial d'un volume après la connexion de l'utilisateur. Il se peut que l'utilisateur doive sélectionner une clé du jeu de clés au préalable.
L'utilisateur peut annuler le chiffrement initial	Permet à l'utilisateur d'annuler le chiffrement initial.
L'utilisateur est autorisé à accéder aux fichiers non chiffrés	Définit si un utilisateur peut accéder aux données non chiffrées d'un volume.
L'utilisateur peut déchiffrer des fichiers	Permet à l'utilisateur de déchiffrer des fichiers individuels ou des répertoires entiers (avec l'extension de l'Explorateur Windows <clic droit>).

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
L’utilisateur peut définir une phrase secrète des supports pour les périphériques	Permet à l’utilisateur de définir une phrase secrète des supports sur son ordinateur. La phrase secrète des supports permet d’accéder facilement à l’aide de SafeGuard Portable à toutes les clés locales utilisées sur des ordinateurs sur lesquels SafeGuard Data Exchange n’est pas installé.
Copier SafeGuard Portable sur la cible	Si cette option est sélectionnée, SafeGuard Portable est copié sur tous les supports amovibles connectés au terminal et dans tous les dossiers de synchronisation définis par une définition Cloud Storage pour SafeGuard Cloud Storage dès l’écriture de contenu sur le support ou le dossier chiffré. SafeGuard Portable permet l’échange des données chiffrées avec les supports amovibles ou le stockage dans le Cloud sans que SafeGuard Enterprise ne soit installé sur le destinataire. Le destinataire peut déchiffrer et chiffrer de nouveau les fichiers chiffrés en utilisant SafeGuard Portable et le mot de passe correspondant. Le destinataire peut chiffrer de nouveau les fichiers avec SafeGuard Portable ou utiliser la clé d’origine pour le chiffrement. Il n’est pas nécessaire que SafeGuard Portable soit installé ou copié sur l’ordinateur du destinataire, il peut être utilisé directement à partir du support amovible ou du dossier de synchronisation du stockage Cloud.
Clé de chiffrement initial par défaut	Ce champ propose une boîte de dialogue de sélection d’une clé utilisée pour le chiffrement initial basé sur fichier. Si vous sélectionnez une clé ici, l’utilisateur ne peut pas sélectionner de clé au démarrage du chiffrement initial. Le chiffrement initial démarre sans interaction de l’utilisateur. La clé sélectionnée est toujours utilisée pour le chiffrement initial. **Exemple :** **Condition préalable :** Une clé par défaut a été définie pour le chiffrement initial.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
	Le chiffrement initial démarre automatiquement lorsque l'utilisateur connecte un périphérique USB à l'ordinateur. La clé définie est utilisée. L'utilisateur ne doit pas intervenir. Si l'utilisateur souhaite chiffrer de nouveau les fichiers ou enregistrer de nouveaux fichiers sur le périphérique USB, il peut sélectionner la clé de son choix (s'il y est autorisé et si disponible). Si l'utilisateur connecte un autre périphérique USB, la clé définie pour le chiffrement initial est de nouveau utilisée. Cette clé est également utilisée pour tous les processus de chiffrement ultérieurs jusqu'à ce que l'utilisateur sélectionne explicitement une autre clé. Si la phrase secrète des supports est activée, cette option sera désactivée. La **Clé définie pour le chiffrement** sera utilisée.
Dossier en texte brut	Le dossier spécifié ici sera créé sur tous les supports amovibles, périphériques de stockage de masse et dans le dossier de synchronisation de stockage dans le Cloud. Les fichiers copiés dans ce dossier restent au format brut.
L'utilisateur est autorisé à décider de l'opération de chiffrement	Vous pouvez autoriser l'utilisateur à décider du chiffrement des fichiers sur les supports amovibles (Windows uniquement) et sur les périphériques de stockage de masse. • Si vous définissez cette option sur **Oui**, les utilisateurs sont invités à décider si les données doivent être chiffrées. Pour les périphériques de stockage en masse, l'invite apparaît après chaque connexion tandis que pour les supports amovibles, l'invite apparaît lorsqu'ils sont connectés. • Si vous définissez cette option sur **Oui, mémoriser les paramètres de l'utilisateur**, les utilisateurs peuvent utiliser l'option **Mémoriser le paramètre et ne plus afficher cette boîte de dialogue** pour que leurs choix soient conservés pour le périphérique correspondant. Dans ce cas, la boîte de dialogue ne réapparaîtra pas pour le périphérique correspondant.

Paramètre de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
	Si l’utilisateur sélectionne **Non** dans la boîte de dialogue sur le terminal, aucun chiffrement initial ou transparent n’a lieu.

3.8.17.8 Paramètres de machine spécifiques - Paramètres de base

Paramètres de stratégie	Explication
Les paramètres sont affichés de la même manière que dans SafeGuard Enterprise Management Center.	
Authentification au démarrage (POA)	
Activer l’authentification au démarrage	Définit si l’authentification au démarrage SafeGuard est activée ou désactivée. ⚠ **Important :** Pour des raisons de sécurité, nous vous conseillons fortement de conserver l’authentification au démarrage SafeGuard activée. La désactivation de l’authentification au démarrage SafeGuard réduit la sécurité du système de connexion Windows et accroît le risque d’accès non autorisés aux données chiffrées.
Refuser l’accès en cas d’absence de connexion au serveur (jours) (0=pas de vérification)	Refuse la connexion à l’authentification au démarrage SafeGuard si le terminal n’a pas été connecté au serveur pendant une période supérieure à la période définie.
Éveil par appel réseau (WOL) sécurisé	Grâce aux paramètres d’**Éveil par appel réseau sécurisé (WOL)**, vous pouvez préparer les terminaux aux déploiements de logiciels. Si les paramètres d’Éveil par appel réseau sécurisé s’appliquent aux terminaux, les paramètres nécessaires (par exemple, la désactivation de l’authentification au démarrage SafeGuard et un intervalle d’éveil par appel réseau) sont transférés directement sur les terminaux sur lesquels les paramètres sont analysés. ⚠ **Important :** La désactivation de l’authentification au démarrage SafeGuard (même pour un nombre limité de processus de

Paramètres de stratégie	Explication
	démarrage) réduit le niveau de sécurité de votre système. Retrouvez plus de renseignements sur l'éveil par appel réseau sécurisé dans le Manuel d'administration de SafeGuard Enterprise.
Nombre de connexions automatiques	Définit le nombre de redémarrages lorsque l'authentification au démarrage SafeGuard est inactive pour l'éveil par appel réseau. Ce paramètre remplace temporairement le paramètre **Activer l'authentification au démarrage** jusqu'à ce que le nombre prédéfini de connexions automatiques soit atteint. L'authentification au démarrage SafeGuard est ensuite réactivée. Si vous définissez le nombre de connexions automatiques sur deux et si **Activer l'authentification au démarrage** est actif, le terminal démarre deux fois sans authentification via l'authentification au démarrage SafeGuard. Pour le mode Éveil par appel réseau, nous vous conseillons d'autoriser **trois redémarrages de plus que nécessaire pour vos opérations de maintenance** pour faire face aux problèmes imprévus.
Autoriser la connexion à Windows pendant l'éveil par réseau	Détermine si les connexions Windows locales sont autorisées durant un éveil par appel réseau.
Début de la plage horaire pour le lancement du WOL externe **Fin de la plage horaire pour le lancement du WOL externe**	La date et l'heure peuvent être sélectionnées ou saisies pour le début et la fin de l'éveil par appel réseau (WOL). Format de date : *MM/JJ/AAAA* Format d'heure : *HH:MM* Les combinaisons suivantes de saisie sont possibles : • début et fin de l'éveil par appel réseau définis ;

Paramètres de stratégie	Explication
	• fin de l’éveil par appel réseau définie, début ouvert. • aucune entrée : aucun intervalle n’a été défini. Pour un déploiement planifié de logiciels, le responsable de la sécurité doit définir la plage de l’éveil par appel réseau de sorte que le script de programmation puisse démarrer suffisamment tôt pour que les terminaux aient le temps de démarrer. WOLstart (Début WOL) : le point de départ de l’éveil par appel réseau dans le script de programmation doit se trouver dans l’intervalle défini dans la stratégie. Si aucun intervalle n’est défini, l’éveil par appel réseau n’est pas activé localement sur le terminal protégé par SafeGuard Enterprise. WOLstop (Fin WOL) : cette commande s’effectue quel que soit le point d’extrémité défini pour l’éveil par appel réseau.
Assignation utilisateur/machine (AUM)	
Interdire la connexion à l’utilisateur invité SGN	**Remarque :** Ce paramètre s’applique uniquement aux terminaux administrés. Définit si les utilisateurs invités peuvent se connecter à Windows sur le terminal. **Remarque :** Les comptes Microsoft sont toujours considérés comme des utilisateurs invités de SafeGuard Enterprise.
Autoriser l’enregistrement de nouveaux utilisateurs SGN pour	Définit qui peut importer un autre utilisateur SGN dans l’authentification au démarrage SafeGuard et/ou AUM (en désactivant la connexion automatique vers le système d’exploitation). **Remarque :** Pour les terminaux sur lesquels le module Protection des périphériques n’est pas installé, le paramètre **Autoriser l’enregistrement de nouveaux utilisateurs**

Paramètres de stratégie	Explication
	SGN pour doit être défini sur **Tout le monde** s'il est possible d'ajouter plusieurs utilisateurs à l'Assignation utilisateur/machine avec accès à leur jeu de clés. Autrement, les utilisateurs peuvent uniquement être ajoutés dans SafeGuard Management Center. Ce paramètre est uniquement évalué sur les terminaux administrés. Retrouvez plus de renseignements dans l'article 110659 de la base de connaissances de Sophos. Si le paramètre est défini sur **Personne**, l'authentification au démarrage n'est pas activée. Les utilisateurs devront être assignés manuellement dans SafeGuard Management Center.
Activer l'enregistrement des utilisateurs Windows de SGN	Définit si les utilisateurs Windows de SGN peuvent être enregistrés sur le terminal. Un utilisateur Windows de SGN n'est pas ajouté à l'authentification au démarrage SafeGuard. En revanche, il dispose d'un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur SGN. Si vous sélectionnez ce paramètre, tous les utilisateurs, qui seraient autrement devenus des utilisateurs invités, deviennent des utilisateurs Windows de SGN. Les utilisateurs sont ajoutés à l'Assignation utilisateur/machine dès qu'ils se connectent à Windows.
Activer le nettoyage manuel de l'AUM pour les terminaux autonomes	**Remarque :** Ce paramètre s'applique uniquement aux terminaux non administrés. Définit si les utilisateurs peuvent supprimer les utilisateurs SGN et les utilisateurs Windows de SGN de l'assignation utilisateur/machine. Si vous sélectionnez **Oui**, la commande **Assignations utilisateur/machine** est disponible dans le menu de l'icône de la barre d'état système sur le terminal. Cette commande affiche une liste des utilisateurs pouvant se connecter à l'authentification au démarrage SafeGuard en tant qu'utilisateurs SGN et à Windows en tant qu'utilisateurs Windows de SGN. Dans la boîte de dialogue qui s'affiche, il est possible de

Paramètres de stratégie	Explication
Nombre maximal d’utilisateurs Windows de SGN avant nettoyage automatique	retirer des utilisateurs de la liste. Une fois que les utilisateurs SGN ou que les utilisateurs Windows de SGN ont été supprimés, ils ne peuvent plus se connecter à l’authentification au démarrage SafeGuard où à Windows. **Remarque :** Ce paramètre s’applique uniquement aux terminaux administrés. Ce paramètre vous permet d’activer le nettoyage automatique des utilisateurs Windows de SafeGuard Enterprise sur les terminaux administrés. Dès que le seuil que vous avez fixé est dépassé par un utilisateur Windows de SafeGuard Enterprise, tous les utilisateurs Windows de SafeGuard Enterprise sont supprimés de l’Assignation utilisateur/machine à l’exception du nouveau. La valeur par défaut est de **10**.
Options d’affichage	
Afficher l’identification de la machine	Affiche le nom de l’ordinateur ou un texte défini dans la barre de titre de l’authentification au démarrage SafeGuard. Si les paramètres réseau de Windows incluent le nom de l’ordinateur, ce dernier est automatiquement intégré aux paramètres de base.
Texte d’identification de la machine	Le texte à afficher dans la barre de titre de l’authentification au démarrage SafeGuard. Si vous avez sélectionné **Nom défini** dans le champ **Afficher l’identification de la machine**, vous pouvez saisir le texte dans ce champ de saisie.
Afficher la mention légale	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît avant l’identification dans l’authentification au démarrage SafeGuard. Dans certains pays, la loi exige l’affichage d’une zone de texte ayant un certain contenu. L’utilisateur doit confirmer la zone de texte avant que le système ne continue.

Paramètres de stratégie	Explication
	Avant d’indiquer un texte, veuillez l’enregistrer en tant qu’élément de texte sous **Textes** dans la zone de navigation **Stratégies**.
Texte de la mention légale	Le texte à afficher en tant que mention légale. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré sous **Textes** dans la zone de navigation **Stratégies**.
Afficher des informations supplémentaires	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît après la mention légale (si elle est activée). Vous pouvez définir si les informations supplémentaires sont affichées : • Jamais • À chaque démarrage système • À chaque connexion Avant d’indiquer un texte, veuillez l’enregistrer en tant qu’élément de texte sous **Textes** dans la zone de navigation **Stratégies**.
Texte des informations supplémentaires	Le texte à afficher en tant qu’informations supplémentaires. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré sous **Textes** dans la zone de navigation **Stratégies**.
Afficher les informations pendant une période supplémentaire	Dans ce champ, vous pouvez définir la durée (en secondes) pendant laquelle les informations supplémentaires doivent être affichées. Vous pouvez indiquer le nombre de secondes après lesquelles la zone de texte d’informations supplémentaires est fermée automatiquement. L’utilisateur peut fermer la zone de texte à tout moment en cliquant sur **OK**.

Paramètres de stratégie	Explication
Activer et afficher l’icône de la barre d’état système	L’icône de la barre d’état système de SafeGuard Enterprise permet à l’utilisateur d’accéder rapidement et facilement à l’ensemble des fonctions du terminal. En outre, des informations concernant l’état du terminal (nouvelles stratégies reçues, etc.) peuvent être affichées dans des infobulles. **Oui :** l’icône de la barre d’état système est affichée dans la zone d’information de barre des tâches et l’utilisateur est continuellement informé via l’infobulle concernant l’état de le terminal protégé par SafeGuard Enterprise. **Non :** l’icône de la barre d’état système n’est pas affichée. Aucune information d’état n’est affichée par les infobulles. **Muet :** l’icône de la barre d’état système est affichée dans la zone d’information de barre des tâches mais aucune information d’état n’est affichée via les infobulles.
Afficher les icônes en chevauchement dans l’Explorateur	Définit si des symboles de clé Windows s’affichent pour indiquer l’état de chiffrement des volumes, périphériques, dossiers et fichiers.
Clavier virtuel en POA	Définit si un clavier virtuel peut être affiché sur demande dans la boîte de dialogue de l’authentification au démarrage SafeGuard pour la saisie du mot de passe.
Options d’installation	
Désinstallation autorisée	Détermine si la désinstallation de SafeGuard Enterprise est autorisée sur les ordinateurs client. Lorsque l’option **Désinstallation autorisée** est définie sur **Non**, SafeGuard Enterprise ne peut pas être désinstallé, même par un utilisateur avec les droits administrateur, lorsque ce paramètre est actif au sein d’une stratégie.
Activer la protection antialtération Sophos	Active/désactive la protection antialtération Sophos. Si vous avez autorisé la désinstallation

Paramètres de stratégie	Explication
	de SafeGuard Enterprise dans le paramètre de stratégie **Désinstallation autorisée**, vous pouvez définir ce paramètre de stratégie sur **Oui**, pour garantir que les tentatives de désinstallation sont vérifiées par la protection antialtération Sophos pour empêcher la suppression accidentelle du logiciel. Si la protection antialtération Sophos n'autorise pas la désinstallation, les tentatives de désinstallation seront annulées. Si l'option **Activer la protection antialtération Sophos** est définie sur **Non**, la désinstallation de SafeGuard Enterprise ne sera pas vérifiée ou empêchée par la protection antialtération Sophos. **Remarque :** Ce paramètre ne s'applique qu'aux terminaux sur lesquels la version 9.5 ou ultérieure de Sophos Endpoint Security and Control est installée
Paramètres du fournisseur des codes d'accès	
Enveloppement du fournisseur de codes d'accès	Vous pouvez configurer SafeGuard Enterprise pour utiliser un fournisseur de codes d'accès différents de ceux du fournisseur de codes d'accès Windows. Les modèles des fournisseurs de codes d'accès pris en charge peuvent être téléchargés sur www.sophos.com. Pour obtenir une liste des modèles de fournisseurs de codes d'accès éprouvés et savoir où les télécharger, veuillez contacter le support Sophos. Vous pouvez importer un modèle et le déployer sur les terminaux en utilisant le paramètre de la stratégie **Fournisseur de codes d'accès**. Veuillez cliquer sur **Importer le modèle** et naviguez jusqu'au fichier de modèles. Le modèle importé et son contenu sont affichés dans le champ **Fournisseur de codes d'accès** et défini en tant que stratégie. Pour supprimer un modèle, veuillez cliquer sur **Effacer le modèle**.

Paramètres de stratégie	Explication
	Remarque : Veuillez ne pas modifier les fichiers de modèles fournis. Si la structure XML de ces fichiers est modifiée, les paramètres ne seront pas reconnus sur le terminal et le fournisseur de codes d'accès Windows par défaut sera utilisé à la place. La configuration nécessite généralement l'aide de Sophos Professional Services. Veuillez contacter le support Sophos.
Paramètres de prise en charge du token	
Nom du module middleware du token	Enregistre le module PKCS#11 d'un token. Les options suivantes sont disponibles : • ActiveIdentity ActivClient • ActiveIdentity ActivClient (PIV) • AET SafeSign Identity Client • Aladdin eToken PKI Client • a.sign Client • ATOS CardOS API • Charismathics Smart Security Interface • Estonian ID-Card • Gemalto Access Client • Gemalto Classic Client • Gemalto .NET Card • IT Solution trustWare CSP+ • Módulo PKCS#11 TC-FNMT

Paramètres de stratégie	Explication
	• Nexus Personal • RSA Authentication Client 2.x • RSA Smart Card Middleware 3.x • Siemens CardOS API • T-Systems NetKey 3.0 • Unizeto proCertum • Paramètres PKCS#11 personnalisés... • Si vous sélectionnez **Paramètres PKCS#11 personnalisés...**, les **Paramètres PKCS#11 personnalisés** sont activés. Vous pouvez saisir les noms de module à utiliser : ◦ Module PKCS#11 pour Windows ◦ Module PKCS#11 pour l'authentification au démarrage SafeGuard **Remarque :** Si vous installez le middleware **Nexus Personal** ou **Gemalto .NET Card**, vous allez également devoir ajouter leur chemin d'installation à la variable d'environnement PATH des **Propriétés système** de votre ordinateur. • Le chemin d'installation par défaut pour **Gemalto .NET Card** : `C:\Program Files \ Gemalto\PKCS11 for .NET V2 smart cards` • Le chemin d'installation par défaut pour **Nexus Personal** : `C:\Program Files \Personal\bin` **Licences :**

Paramètres de stratégie	Explication
	Sachez que l'utilisation des middlewares respectifs pour le système d'exploitation standard requiert un accord de licence avec le fabricant correspondant. Retrouvez plus de renseignements dans l'article 116585 de la base de connaissances de Sophos. Pour les licences Siemens, contactez : Atos IT Solutions and Services GmbH Otto-Hahn-Ring 6 D-81739 Muenchen Allemagne
Services en attente de	Ce paramètre permet de résoudre les problèmes de certaines cartes à puce. Notre support fournira les paramètres correspondants requis.

3.8.17.9 Journalisation pour les terminaux Windows

Les événements SafeGuard Enterprise peuvent être journalisés dans l'Observateur d'événements Windows ou dans la base de données SafeGuard Enterprise. Pour indiquer les événements à journaliser et leur destination, créez une stratégie du type **Journalisation**, puis sélectionnez les événements souhaités d'un simple clic.

Vous pouvez sélectionner plusieurs types d'événements, de catégories différentes (par exemple authentification, chiffrement, etc.). Nous vous conseillons de définir une stratégie pour la journalisation et de déterminer quels sont les événements nécessaires, en fonction de vos exigences en matière de rapports et d'audits.

Retrouvez plus de renseignements à la section Rapports *(page 228)*.

3.8.18 Réparation d'une installation corrompue de SafeGuard Management Center

Une installation corrompue de SafeGuard Management Center peut être réparée facilement si la base de données est toujours intacte. Dans ce cas, veuillez réinstaller SafeGuard Management Center et utiliser la base de données existantes ainsi que la sauvegarde du certificat du responsable principal de la sécurité.

- 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. Les données doivent être disponibles et valides.

- Vous devez également connaître les mots de passe de ce fichier .p12, ainsi que ceux du magasin de certificats.

Pour réparer une installation corrompue de SafeGuard Management Center :

1. Réinstallez le package d’installation de SafeGuard Management Center. Ouvrez SafeGuard Management Center. L’assistant de configuration démarre automatiquement.
2. 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 authentification préalable au démarrage 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 SafeGuard Management Center.

    - Si le fichier de certificat sauvegardé est introuvable sur l’ordinateur, cliquez sur **Importer**. Recherchez le fichier de certificat sauvegardé et cliquez sur **Ouvrir**. Saisissez le mot de passe du fichier de certificat sélectionné. Cliquez sur **Oui**. Saisissez et confirmez le mot de passe d’authentification dans SafeGuard Management Center.
5. Cliquez sur **Suivant**, puis sur **Terminer** pour achever la configuration de SafeGuard Management Center.

L’installation corrompue de SafeGuard Management Center est réparée.

3.8.19 Résolution des problèmes

3.8.19.1 Codes d'erreur

Codes SGMERR du journal des événements de Windows

Le message suivant s’affichera dans le journal des événements de Windows :

« Autorisation pour l’administration de SafeGuard Enterprise refusée pour l’utilisateur... Raison : SGMERR[536870951] ».

Consultez le tableau ci-dessous pour connaître la définition du numéro « 536870951 ». Le numéro « 536870951 » signifie par exemple « Saisie incorrecte du code confidentiel ». Authentification impossible de l’utilisateur.

Identifiant de l’erreur	Affichage
0	OK
21	Erreur interne détectée
22	Module non initialisé
23	Erreur d’E/S de fichier détectée
24	Le cache ne peut pas être assigné
25	Erreur de lecture d’E/S de fichier
26	Erreur d’écriture d’E/S de fichier
50	Aucune opération n’a été effectuée
101	Erreur générale
102	Accès refusé
103	Le fichier existe déjà
1201	Impossible d’ouvrir l’entrée du registre.
1202	Impossible de lire l’entrée du registre.
1203	Impossible d’écrire l’entrée du registre.
1204	Impossible de supprimer l’entrée du registre.
1205	Impossible de créer l’entrée du registre.
1206	Accès impossible à un pilote ou un service système.
1207	Impossible d’ajouter un pilote ou un service système dans le registre.
1208	Impossible de supprimer un pilote ou un service système du registre.
1209	Une entrée est déjà présente dans le registre pour un pilote ou un service système.
1210	Aucun accès au Service Control Manager.
1211	Impossible de trouver une entrée dans le registre pour une session.
1212	Une entrée du registre est non valide ou erronée.
1301	Échec de l’accès à un lecteur.
1302	Aucune information n’est disponible sur un volume.
1303	Échec de l’accès à un volume.
1304	Option non valide définie.
1305	Type de système de fichiers non valide.
1306	Le système de fichiers existant sur un volume et le système de fichiers défini diffèrent.
1307	La taille du cluster existant utilisée par un système de fichiers et la taille du cluster définie diffèrent.
1308	Taille de secteur non valide utilisée par un système de fichiers défini.
1309	Secteur de départ non valide défini.

Identifiant de l’erreur	Affichage
1310	Type de partition non valide défini.
1311	Impossible de trouver une zone non utilisée et défragmentée de la taille requise sur un volume.
1312	Impossible de marquer le cluster du système de fichiers comme étant utilisé.
1313	Impossible de marquer le cluster du système de fichiers comme étant utilisé.
1314	Impossible de marquer le cluster du système de fichiers comme étant CORRECT.
1315	Impossible de marquer le cluster du système de fichiers comme étant INCORRECT.
1316	Aucune information disponible sur les clusters d’un système de fichiers.
1317	Impossible de trouver une zone marquée comme MAUVAISE sur un volume.
1318	Taille incorrecte définie pour une zone de volume.
1319	Le secteur MBR d’un disque dur n’a pas pu être remplacé.
1330	Une commande erronée a été définie pour une allocation ou une désallocation.
1351	Algorithme non valide défini.
1352	Échec de l’accès au noyau système.
1353	Aucun noyau système n’est installé.
1354	Une erreur s’est produite lors de l’accès au noyau système.
1355	Modification non valide des paramètres système.
1401	Échec de l’écriture de données sur un lecteur.
1402	Échec de la lecture de données d’un lecteur.
1403	Échec de l’accès à un lecteur.
1404	Lecteur non valide défini.
1405	Échec du changement de position sur un lecteur.
1406	Le lecteur n’est pas prêt.
1407	Échec du démontage d’un lecteur.
1451	Impossible d’ouvrir le fichier.
1452	Le fichier est introuvable.
1453	Le chemin d’accès défini pour le fichier est non valide.
1454	Impossible de créer le fichier.
1455	Impossible de copier le fichier.
1456	Aucune information n’est disponible sur un volume.
1457	Impossible de modifier la position dans un fichier.
1458	Échec de la lecture de données d’un fichier.
1459	Échec de l’écriture de données dans un fichier.
1460	Impossible de supprimer un fichier.
1461	Système de fichiers non valide.
1462	Impossible de fermer le fichier.
1463	L’accès à un fichier a été refusé.
1501	Mémoire disponible insuffisante.
1502	Paramètre non valide ou erroné défini.

Identifiant de l’erreur	Affichage
1503	Dépassement de la taille de la mémoire tampon de données.
1504	Un module DLL n’a pas pu être chargé.
1505	Une fonction ou un processus a été annulé.
1506	Aucun accès autorisé.
1510	Aucun noyau système n’est installé.
1511	Impossible de lancer un programme.
1512	Une fonction, un objet ou une donnée est indisponible.
1513	Entrée non valide détectée.
1514	Un objet existe déjà.
1515	Appel de fonction non valide.
1516	Une erreur interne s’est produite.
1517	Une violation d’accès s’est produite.
1518	La fonction ou le mode n’est pas pris en charge.
1519	Échec de la désinstallation.
1520	Une erreur d’exception s’est produite.
1550	Le secteur MBR du disque dur n’a pas pu être remplacé.
2850	Arrêt du service Planificateur de tâches en raison d’une exception.
2851	Succès de l’exécution de la tâche du Planificateur de tâches.
2852	Échec de la tâche du planificateur.
2853	La tâche du Planificateur de tâches a été créée ou modifiée.
2854	La tâche du Planificateur de tâches a été supprimée.
20001	Inconnu
20002	Processus terminé
20003	Fichier non vérifié
20004	Stratégie non valide
30050	Impossible d’ouvrir la commande
30051	Mémoire insuffisante
30052	Échec général de la communication de traitement
30053	Une ressource est temporairement indisponible. Cet état est temporaire. Des tentatives d’accès ultérieures peuvent fonctionner normalement.
30054	Échec général de communication
30055	Valeur renvoyée inattendue
30056	Aucun lecteur de carte n’est connecté.
30057	Dépassement de mémoire tampon
30058	La carte n’est pas alimentée
30059	Un dépassement de délai s’est produit
30060	Type de carte incorrect
30061	La fonctionnalité demandée n’est pas prise en charge à l’heure actuelle / par ce SE / dans cette situation, etc.
30062	Pilote non valide
30063	Ce logiciel ne peut pas utiliser le microprogramme du matériel connecté

Identifiant de l’erreur	Affichage
30064	Impossible d’ouvrir le fichier
30065	Fichier introuvable
30066	La carte n’est pas insérée
30067	Argument non valide
30068	Le sémaphore est en cours d’utilisation
30069	Le sémaphore est temporairement en cours d’utilisation
30070	Échec général
30071	Actuellement, vous ne disposez pas des droits permettant d’effectuer l’opération demandée. Généralement, un mot de passe doit être fourni au préalable.
30072	Actuellement, le service n’est pas disponible
30073	Un élément (par ex. une clé portant un nom spécifique) est introuvable.
30074	Le mot de passe fourni est incorrect.
30075	Le mot de passe fourni plusieurs fois est incorrect, l’accès est par conséquent verrouillé. Il est généralement possible d’utiliser un outil d’administration approprié pour le déverrouiller.
30076	L’identité ne correspond pas à une identité définie ayant fait l’objet d’un contrôle croisé
30077	Plusieurs erreurs se sont produites. Utilisez ce code d’erreur si c’est le seul moyen d’obtenir un code d’erreur lorsque des erreurs différentes se sont produites.
30078	Il reste des éléments, par conséquent la structure du répertoire ne peut par ex. pas être supprimée.
30079	Erreur lors du contrôle de cohérence
30080	L’ID se trouve sur une liste noire, par conséquent, l’opération demandée n’est pas autorisée.
30081	Identificateur non valide
30082	Fichier de configuration non valide
30083	Secteur introuvable.
30084	Entrée introuvable.
30085	Plus de sections
30086	Fin du fichier atteinte.
30087	L’élément spécifié existe déjà
30088	Le mot de passe fourni est trop court.
30089	Le mot de passe fourni est trop long.
30090	Un élément (par ex. un certificat) a expiré.
30091	Le mot de passe n’est pas verrouillé.
30092	Chemin introuvable.
30093	Le répertoire n’est pas vide.
30094	Aucune donnée supplémentaire
30095	Le disque est plein.
30096	Une opération a été annulée.

Identifiant de l’erreur	Affichage
30097	Données en lecture seule ; une opération d’écriture a échoué
12451840	La clé n’est pas disponible.
12451842	La clé n’est pas définie.
12451842	Accès refusé au support non chiffré.
12451843	Accès refusé au support non chiffré sauf s’il est vide.
352321637	Le fichier n’est pas chiffré.
352321638	La clé n’est pas disponible.
352321639	La clé correcte n’est pas disponible.
352321640	Erreur de la somme de contrôle dans l’en-tête du fichier.
352321641	Erreur de la fonction CBI.
352321642	Nom de fichier non valide.
352321643	Erreur de lecture/écriture du fichier temporaire.
352321644	L’accès aux données non chiffrées n’est pas autorisé.
352321645	Zone de stockage des clés (KSA) saturée.
352321646	Le fichier est déjà chiffré avec un autre algorithme.
352321647	Le fichier est compressé avec NTFS et ne peut pas être chiffré.
352321648	Le fichier est chiffré avec EFS.
352321649	Propriétaire du fichier non valide
352321650	Mode de chiffrement du fichier non valide
352321651	Erreur d’opération CBC.
385875969	Intégrité rompue.
402653185	Le token ne contient pas de codes d’accès.
402653186	Impossible d’écrire les codes d’accès sur le token.
402653187	Impossible de créer la balise TDF.
402653188	La balise TDF ne contient pas les données requises.
402653189	L’objet existe déjà sur le token.
402653190	Aucun connecteur valide trouvé
402653191	Lecture impossible du numéro de série
402653192	Le chiffrement du token a échoué.
402653193	Le déchiffrement du token a échoué.
536870913	Le fichier de clé ne contient pas de données valides.
536870914	Des parties de la paire de clés RSA sont incorrectes
536870915	Impossible d’importer la paire de clés.
536870916	Le format du fichier de clés n’est pas valide.
536870917	Aucune donnée disponible
536870918	Échec de l’importation du certificat.
536870919	Le module a déjà été initialisé
536870920	Le module n’a pas encore été initialisé
536870921	Le chiffrement ASN.1 est corrompu.
536870922	Longueur des données incorrecte
536870923	Signature incorrecte.

Identifiant de l’erreur	Affichage
536870924	Mécanisme de chiffrement appliqué incorrect.
536870925	Cette version n’est pas prise en charge.
536870926	Erreur de remplissage.
536870927	Indicateurs non valides.
536870928	Le certificat a expiré et n’est plus valide
536870929	Heure saisie incorrecte. Le certificat n’est pas encore valide.
536870930	Le certificat a été retiré.
536870931	La chaîne de certificat est non valide.
536870932	Impossible de créer la chaîne de certificat.
536870933	Impossible de contacter CDP.
536870934	Un certificat pouvant être utilisé uniquement comme unité de donnée finale a été utilisé comme CA ou réciproquement.
536870935	Problèmes de validité de la longueur du certificat dans la chaîne.
536870936	Erreur d’ouverture d’un fichier.
536870937	Erreur de lecture d’un fichier.
536870938	Un ou plusieurs paramètres assignés à la fonction sont incorrects.
536870939	Le résultat de la fonction dépasse la taille du cache.
536870940	Problème de token et/ou de connecteur rompu.
536870941	Le token n’a pas suffisamment de mémoire pour effectuer la fonction demandée.
536870942	Le token a été retiré du connecteur alors que la fonction était en cours.
536870943	La fonction demandée n’a pas pu être réalisée, mais aucune information concernant la cause de cette erreur n’est disponible.
536870945	L’ordinateur sur lequel la compilation CBI s’effectue n’a pas suffisamment de mémoire pour effectuer la fonction demandée. Il se peut que cette fonction ne soit que partiellement exécutée.
536870946	Une opération demandée n’est pas prise en charge par la compilation CBI.
536870947	Tentative de définition d’une valeur pour un objet qui ne peut pas être paramétré ou modifié.
536870948	Valeur non valide pour l’objet.
536870949	Échec d’obtention de la valeur d’un objet car celui-ci est sensible ou inaccessible.
536870950	Le code confidentiel saisi a expiré. (Le fait que le code confidentiel d’un utilisateur classique fonctionne ou non sur un token générée dépend de cette dernière).
536870951	Le code confidentiel fourni est incorrect. Authentification impossible de l’utilisateur.
536870952	Le code confidentiel saisi contient des caractères non valides. Ce code de réponse ne s’applique qu’aux opérations qui tentent de définir un code confidentiel.
536870953	Le code confidentiel saisi est trop long ou trop court. Ce code de réponse ne s’applique qu’aux opérations qui tentent de définir un code confidentiel.

Identifiant de l’erreur	Affichage
536870954	Le code confidentiel sélectionné est bloqué et ne peut pas être utilisé. Ceci se produit lorsqu’un certain nombre de tentatives ont été faites pour authentifier un utilisateur et lorsque le token refuse toute tentative supplémentaire.
536870955	Identifiant de connecteur non valide.
536870956	Le token n’était pas dans le connecteur lors de la requête.
536870957	L’archive CBI et/ou le connecteur n’ont pas reconnu le token qui s’y trouve.
536870958	L’opération demandée n’a pas pu être effectuée car le token est protégé en écriture.
536870959	L’utilisateur saisi ne peut pas être connecté car il a déjà ouvert une session.
536870960	L’utilisateur saisi ne peut pas se connecter car un autre utilisateur est déjà connecté à cette session.
536870961	L’opération demandée n’a pas pu être effectuée car aucun utilisateur correspondant n’est connecté. Par exemple, il n’est pas possible de quitter une session lorsqu’un utilisateur est encore connecté.
536870962	Le code confidentiel de l’utilisateur normal n’a pas été initialisé avec CBIInitPin
536870963	Une tentative de connexion effectuée par plusieurs utilisateurs simultanément sur le même token a été autorisée.
536870964	Une valeur incorrecte a été spécifiée en tant que CBIUser. Les types valides sont définis dans les types d’utilisateurs.
536870965	Un objet ayant l’identifiant spécifié est introuvable sur le token.
536870966	Dépassement de délai de l’opération.
536870967	Cette version d’IE n’est pas prise en charge
536870968	Authentification impossible.
536870969	Le certificat de base n’est pas sécurisé.
536870970	Aucune CRL trouvée
536870971	Aucune connexion Internet active.
536870972	Erreur de valeur de temps du certificat.
536870973	Impossible de vérifier le certificat sélectionné.
536870974	Le statut d’expiration du certificat est inconnu.
536870975	Le module s’est fermé. Aucune autre demande.
536870976	Une erreur s’est produite pendant la requête d’une fonction réseau.
536870977	Une requête de fonction non valide a été reçue.
536870978	Impossible de trouver un objet.
536870979	Une session Terminal Server a été interrompue.
536870980	Opération non valide.
536870981	L’objet est en cours d’utilisation
536870982	Le générateur de nombres aléatoire n’a pas été initialisé. (CBIRNDInit ( ) non requis.)
536870983	Commande inconnue (voir CBIControl ( ))
536870984	UNICODE n’est pas pris en charge

Identifiant de l’erreur	Affichage
536870985	Davantage de valeurs de départ sont nécessaires pour le générateur de nombres aléatoire
536870986	L’objet existe déjà
536870987	Combinaison d’algorithme incorrecte. (Voir CBIRecrypt ( )).
536870988	Le module Cryptoki (PKCS#11) n’a pas été initialisé.
536870989	Le module Cryptoki (PKCS#11) a été initialisé.
536870990	Impossible de charger le module Cryptoki (PKCS#11).
536870991	Certificat introuvable
536870992	Non approuvé
536870993	Clé non valide
536870994	La clé ne peut pas être exportée.
536870995	L’algorithme spécifié n’est pas pris en charge temporairement.
536870996	Le mode de déchiffrement saisi n’est pas pris en charge.
536870997	Erreur de compilation GSENC.
536870998	Le format de requête de données n’est pas reconnu.
536870999	Le certificat n’a pas de clé privée.
536871000	Paramètre système incorrect.
536871001	Une opération est active.
536871002	Un certificat de la chaîne n’est pas correctement imbriqué.
536871003	La CRL n’a pas pu être remplacée.
536871004	Le code confidentiel de l’utilisateur a déjà été initialisé.
805306369	Vous ne disposez pas des droits permettant d’effectuer cette opération. Accès refusé.
805306370	Opération non valide
805306371	Paramètre utilisé non valide
805306372	L’objet existe déjà
805306373	L’objet est introuvable.
805306374	Exception de la base de données
805306375	L’opération a été annulée par l’utilisateur
805306376	Le token n’est pas assigné à un utilisateur spécifique
805306377	Le token est assigné à plusieurs utilisateurs
805306378	Le token est introuvable dans la base de données
805306379	Le token a été supprimé et retiré de la base de données
805306380	Impossible d’identifier le token dans la base de données.
805306381	La stratégie est assignée à un groupe de stratégies. Supprimez l’assignation avant de supprimer la stratégie.
805306382	La stratégie est assignée à une OU. Supprimez d’abord l’assignation.
805306383	Le certificat n’est pas valide pour ce responsable.
805306384	Le certificat a expiré pour ce responsable.
805306385	Le responsable est introuvable dans la base de données.
805306386	Le responsable sélectionné n’est pas unique.

Identifiant de l’erreur	Affichage
805306387	Le responsable est bloqué et ne peut pas être authentifié.
805306388	Le responsable n’est plus ou n’est pas encore valide.
805306389	Impossible d’autoriser le responsable - requête en dehors des heures de bureau.
805306390	Une partie responsable ne peut pas se supprimer.
805306391	Le responsable principal de la sécurité ne peut pas être supprimé car un second responsable principal de la sécurité est nécessaire pour une authentification supplémentaire.
805306392	Le responsable de la sécurité ne peut pas être supprimé car un second responsable de la sécurité est requis pour une authentification supplémentaire.
805306393	Le responsable de la vérification ne peut pas être supprimé car un second responsable de la vérification est requis pour une authentification supplémentaire.
805306394	Le responsable de la récupération ne peut pas être supprimé car un second responsable récupération est requis pour une authentification supplémentaire.
805306395	Le conseiller principal ne peut pas être supprimé car un second conseiller principal est requis pour une authentification supplémentaire.
805306396	La fonction de responsable principal de la sécurité ne peut pas être supprimée car un second responsable principal de la sécurité est nécessaire pour une authentification supplémentaire.
805306397	La fonction de responsable de la sécurité ne peut pas être supprimée car un second responsable de la sécurité est nécessaire pour une authentification supplémentaire.
805306398	La fonction de responsable de la vérification ne peut pas être supprimée car un second responsable de la vérification est nécessaire pour une authentification supplémentaire.
805306399	La fonction de responsable récupération ne peut pas être supprimée car un second responsable récupération est nécessaire pour une authentification supplémentaire.
805306400	La fonction de responsable récupération ne peut pas être supprimée car un second responsable récupération est nécessaire pour une authentification supplémentaire.
805306401	Aucun responsable supplémentaire ayant la fonction requise n’est disponible pour une authentification supplémentaire.
805306402	Journal des événements
805306403	L’intégrité du journal des événements central a été vérifiée.
805306404	Intégrité enfreinte. Un ou plusieurs événements ont été supprimés du début de la chaîne.
805306405	Intégrité enfreinte. Un ou plusieurs événements ont été supprimés de la chaîne. Le message indiquant la détection du point de rupture de la chaîne a été mis en surbrillance.
805306406	Intégrité enfreinte. Un ou plusieurs événements ont été supprimés de la fin de la chaîne.
805306407	Impossible d’exporter les événements dans le fichier. Raison :

Identifiant de l’erreur	Affichage
805306408	L’affichage actuel comprend des données non enregistrées. Voulez-vous enregistrer les modifications avant de quitter cet affichage?
805306409	Le fichier n’a pas pu être chargé ou est endommagé. Raison :
805306410	L’intégrité du journal a été enfreinte. Un ou plusieurs événements ont été supprimés.
805306411	Voulez-vous enregistrer les événements dans un fichier avant de les supprimer ?
805306412	Affichage des tâches
805306413	Plusieurs CRL trouvées dans la base de données : Impossible de supprimer les CRL.
805306414	CRL non trouvée dans la base de données :
805306415	L’utilisateur auquel le certificat devrait avoir été assigné est introuvable dans la base de données.
805306416	Un blob P7 est requis en urgence pour l’assignation d’un certificat.
805306417	L’utilisateur auquel le certificat devrait avoir été assigné n’a pas un nom unique.
805306418	Il est malheureusement impossible de trouver l’assignation du certificat.
805306419	L’assignation du certificat n’est pas unique. Le certificat devant être supprimé n’est pas clair.
805306420	L’utilisateur pour lequel le certificat doit être produit est introuvable dans la base de données.
805306421	L’utilisateur auquel le certificat doit être assigné ne peut pas avoir un nom unique.
805306422	Le certificat a déjà été assigné à un autre utilisateur. Un certificat ne peut être assigné qu’à un seul utilisateur.
805306423	La machine à laquelle le certificat doit être assigné est introuvable dans la base de données.
805306424	La machine à laquelle le certificat doit être assigné n’a pas pu être identifiée de façon unique.
805306425	Les certificats importés ne peuvent pas être étendus par SGN.
805306426	Données de certificat incohérentes
805306427	L’extension du certificat n’a pas été approuvée par un responsable de la sécurité.
805306428	Erreur de suppression du token
805306429	Le certificat ne peut pas être supprimé par le token car il a été autorisé par l’utilisateur présent.
805306430	Un accès système du même nom existe déjà. Sélectionnez un autre nom.
805306431	Aucun rôle n’est affecté au responsable de la sécurité. La connexion est impossible.
805306432	La licence a été violée.
805306433	Aucune licence trouvée.
805306435	Chemin du fichier journal manquant ou incorrect.

Identifiant de l’erreur	Affichage
2415919104	Aucune stratégie trouvée.
2415919105	Aucun fichier de configuration n’est disponible.
2415919106	Aucune connexion au serveur.
2415919107	Aucune donnée supplémentaire.
2415919108	Priorité non valide utilisée pour l’envoi au serveur.
2415919109	Données supplémentaires en attente.
2415919110	Enregistrement automatique en attente.
2415919111	Échec de l’authentification de la base de données.
2415919112	Identifiant de session erroné.
2415919113	Paquet de données ignoré.
3674210305	Domaine introuvable.
3674210306	Machine introuvable.
3674210307	Utilisateur introuvable.
3758096385	Le mot de passe ne contient pas assez de lettres
3758096386	Le mot de passe ne contient pas assez de chiffres
3758096387	Le mot de passe ne contient pas assez de caractères spéciaux
3758096388	Le mot de passe est identique au nom d’utilisateur
3758096389	Le mot de passe contient des caractères consécutifs
3758096390	Le mot de passe ressemble trop au nom d’utilisateur
3758096391	Le mot de passe figure dans la liste des mots de passe interdits
3758096392	Le mot de passe ressemble trop à l’ancien mot de passe
3758096393	Le mot de passe comporte une séquence clavier de plus de deux caractères
3758096394	Le mot de passe comporte une colonne clavier de plus de deux caractères
3758096395	Le mot de passe n’est pas encore valide
3758096396	Un mot de passe a expiré
3758096397	La période de validité minimum du mot de passe n’est pas expirée
3758096398	La période de validité maximum du mot de passe est expirée
3758096399	Les informations concernant un changement de mot de passe imminent doivent être affichées
3758096400	Doit être changé lors de la première connexion
3758096401	Le mot de passe a été trouvé dans l’historique
3758096402	Erreur lors de la vérification par rapport à la liste noire spécifiée.
4026531840	Aucune "plate-forme" trouvée.
4026531841	Aucun document.
4026531842	Erreur d’analyse XML.
4026531843	Erreur Document Object Model (XML).
4026531844	Aucune balise <DATAROOT> trouvée.
4026531845	Balise XML introuvable.
4026531846	Erreur "nostream".
4026531847	Erreur "printtree".

Codes d’erreur BitLocker

Les erreurs BitLocker sont signalées par les événements SafeGuard suivants :

- Impossible d’initialiser le noyau. Code interne : <*code d’erreur*>.
- échec et clôture du chiffrement initial du secteur pour le lecteur <*lettre du lecteur*>. Raison : <*code d’erreur*>.

Le tableau suivant est une liste des codes d’erreur pour BitLocker :

Code d’erreur (Hex)	**Code d’erreur (Déc)**	**Description**
0x00000000 – 0x000032C8	0 – 15999	Retrouvez plus de renseignements dans les Codes d’erreurs système de Microsoft
0x00BEB001	12496897	Chiffrement impossible en raison d’une erreur pendant l’initialisation du noyau.
0x00BEB002	12496898	Le gestionnaire de démarrage ne doit pas se trouver sur le volume du système à chiffrer.
0x00BEB003	12496899	Version de Windows non prise en charge sur le disque dur. La version minimum est Windows Vista.
0x00BEB004	12496900	La méthode d’authentification configurée n’est pas prise en charge.
0x00BEB005	12496901	La boîte de dialogue du code confidentiel ne s’est pas terminée correctement.
0x00BEB006	12496902	La boîte de dialogue de chemin d’accès ne s’est pas terminée correctement.
0x00BEB007	12496903	Erreur de communication entre processus dans la boîte de dialogue du code confidentiel ou de chemin d’accès.
0x00BEB008	12496904	Exception non prise en charge dans la boîte de dialogue du code confidentiel ou de chemin d’accès. La boîte de dialogue s’est affichée mais l’utilisateur s’est déconnecté ou l’a terminée à l’aide du Gestionnaire des tâches.
0x00BEB009	12496905	L’algorithme de chiffrement défini dans la stratégie ne correspond pas à celui du lecteur chiffré. Par défaut (s’il n’a pas été modifié), un volume BitLocker natif utilise AES-128 tandis que les stratégies SGN définissent AES-256.
0x00BEB00A	12496906	Le volume est un volume dynamique. Les volumes dynamiques ne sont pas pris en charge.
0x00BEB00B	12496907	Le test matériel a échoué en raison d’un problème matériel.
0x00BEB00C	12496908	Une erreur est survenue pendant l’initialisation et l’activation du TPM.

0x00BEB00D	12496909	Il y a un conflit entre l’algorithme de chiffrement dans la stratégie SGN et les paramètres de l’algorithme de chiffrement dans l’objet de stratégie de groupe (GPO).
0x00BEB00E	12496910	Échec du chiffrement initial du secteur pour le lecteur <lettre du lecteur>.
0x00BEB00F	12496911	La sauvegarde Active Directory des clés de secours est requise mais aucun contrôleur de domaine n’est disponible.
0x00BEB010	12496912	La sauvegarde Active Directory des clés de secours est incompatible avec le challenge/réponse BitLocker.
0x00BEB102	12497154	La version UEFI n’a pas pu être validée et BitLocker va donc être exécuté en mode hérité.
0x00BEB202	12497410	Le package de configuration client n’a pas encore été installé.
0x00BEB203	12497411	La version UEFI n’est pas prise en charge et BitLocker va donc être exécuté en mode hérité. La configuration minimum requise est 2.3.1.
0x80280006	-2144862202	Module de plate-forme sécurisée inactif.
0x80280007	-2144862201	Module de plate-forme sécurisée désactivé.
0x80280014	-2144862188	Le module de plate-forme sécurisée a déjà un propriétaire.
0x80310037	-2144272329	Le paramètre de stratégie de groupe qui exige la compatibilité FIPS empêche la génération du mot de passe de récupération locale et son écriture sur le fichier de sauvegarde de la clé. Le chiffrement va tout de même se poursuivre.
0x8031005B	-2144272293	La stratégie de groupe pour la méthode d’authentification spécifiée n’est pas définie. Veuillez activer la stratégie de groupe « Demander une authentification supplémentaire au démarrage ».
0x8031005E	-2144272290	La stratégie de groupe pour le chiffrement sans module de plate-forme sécurisée n’est pas définie. Veuillez activer la stratégie de groupe « Demander une authentification supplémentaire au démarrage » et sélectionner la case « Autoriser BitLocker sans un module de plateforme sécurisée compatible ».
0x80280000 – 0x803100CF	-2144862208 – -2144272177	Retrouvez plus de renseignements dans les Codes d’erreur COM (TPM, PLA, FVE) de Microsoft.

4. Administration des terminaux Windows

Restrictions générales

Notez les restrictions générales suivantes pour SafeGuard Enterprise sur les terminaux :

- SafeGuard Enterprise pour Windows ne prend pas en charge le matériel d'Apple et ne peut pas être installé dans un environnement Boot Camp. Veuillez plutôt utiliser un client Windows virtuel.
- Les modules de chiffrement intégral du disque SafeGuard (chiffrement de volumes SafeGuard et prise en charge de BitLocker) ne sont pas compatibles avec les systèmes équipés de disques durs reliés par un bus SCSI.
- La fonction de **Changement rapide d'utilisateur** n'est pas prise en charge.
- L'utilisation de SafeGuard Enterprise dans un environnement Terminal Server n'est pas prise en charge.
- Lors de l'utilisation de l'interface AHCI (Intel Advanced Host Controller Interface) sur les terminaux avec l'authentification au démarrage, nous vous conseillons d'utiliser le port de connexion 0 pour le disque dur de démarrage.
- Sur les terminaux avec l'authentification au démarrage, le chiffrement par volume de SafeGuard pour les volumes se trouvant sur les disques dynamiques et sur les disques de table de partition GUID (GPT) n'est pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur le terminal, ils ne sont pas pris en charge.
- Si vous voulez utiliser le chiffrement par volume SafeGuard sur des terminaux avec plusieurs disques physiques, veuillez installer le logiciel de chiffrement sur le premier disque.

- SafeGuard Full Disk Encryption est uniquement disponible sur les terminaux Windows 7 BIOS. Si vous utilisez Windows 7 UEFI ou une version plus récente de Windows, veuillez utiliser la fonctionnalité intégrée de Chiffrement de lecteur BitLocker de Windows. Retrouvez plus de renseignements à la section Gestion du Chiffrement de lecteur BitLocker *(page 321)*.

  Retrouvez plus de renseignements sur SafeGuard Enterprise Full Disk Encryption dans le Manuel d'administration de SafeGuard Enterprise.

4.1 Gestion du Chiffrement de lecteur BitLocker

Pour un chiffrement des disques rapide, facile et fiable, SafeGuard Enterprise utilise la technologie intégrée au système d'exploitation. Vous pouvez donc administrer en toute simplicité les clés et fonctions de récupération sur les lecteurs BitLocker chiffrés à partir de SafeGuard Management Center.

Le Chiffrement de lecteur BitLocker est une fonction de chiffrement de disque complet avec authentification préalable au démarrage incluse dans les systèmes d'exploitation Microsoft Windows. Elle est conçue pour protéger les données en permettant le chiffrement des volumes de démarrage et de données. À partir de Windows 8, le Chiffrement de lecteur BitLocker doit être utilisé à la place de SafeGuard Full Disk Encryption pour procéder au chiffrement intégral des disques.

SafeGuard Enterprise gère le chiffrement BitLocker sur un ordinateur. Le chiffrement BitLocker peut être activé et la gestion des lecteurs déjà chiffrés par BitLocker peut être prise en charge.

Pendant l'installation sur le terminal et pendant le premier redémarrage, SafeGuard Enterprise détermine si le matériel satisfait aux conditions requises pour BitLocker avec le Challenge/Réponse SafeGuard. S'il ne satisfait pas aux conditions, la gestion de SafeGuard Enterprise BitLocker s'effectue sans Challenge/Réponse. Dans ce cas, la clé de récupération BitLocker peut être récupérée à l'aide de SafeGuard Management Center.

4.1.1 Authentification avec le Chiffrement de lecteur BitLocker

Le Chiffrement de lecteur BitLocker offre différentes options d'authentification pour les volumes de démarrage et pour les volumes non démarrables.

Le responsable de la sécurité peut définir les différents modes de connexion dans une stratégie dans SafeGuard Management Center et la distribuer aux terminaux BitLocker.

Les modes de connexion suivants sont proposés aux utilisateurs SafeGuard Enterprise BitLocker :

- **TPM** : la clé de connexion est stockée sur la puce du TPM (Module de plate-forme sécurisée).
- **TPM + PIN** : la clé de connexion est stockée sur la puce du TPM et un code confidentiel est également nécessaire pour la connexion.
- **Clé de démarrage** : la clé de connexion est stockée sur une carte mémoire USB.
- **TPM + Clé de démarrage** : la clé de connexion est stockée sur la puce du TPM et sur une carte mémoire USB. Les deux sont requises pour établir la connexion.
- **Mot de passe** : l'utilisateur doit saisir un mot de passe.
- **Mot de passe ou clé de démarrage** : les cartes mémoire USB seront uniquement utilisées si les mots de passe sont pris en charge sur le système d'exploitation client.
- **Auto-déverrouiller** : si le volume de démarrage est chiffré, une clé externe est créée et stockée sur le volume de démarrage. Le ou les volumes non démarrables seront ensuite déchiffrés

automatiquement. Ils seront déverrouillés automatiquement à l'aide de la fonctionnalité Auto-déverrouiller de BitLocker.

Retrouvez plus de renseignements sur le paramétrage des modes de connexion à la section Authentification *(page 263)*.

4.1.1.1 Module de plate-forme sécurisée (Trusted Platform Module ou TPM)

TPM est un module semblable à une carte à puce sur la carte mère qui exécute des fonctions cryptographiques et des opérations de signature numérique. Il permet de créer, stocker et gérer des clés utilisateur. Il est protégé contre les attaques.

4.1.1.2 Codes confidentiels et mots de passe

Les conditions requises pour les codes confidentiels et mots de passe BitLocker sont définies par les Stratégies de groupes Windows et non pas par les paramètres de SafeGuard Enterprise.

Les mots de passe sont uniquement pris en charge à partir de Windows 8.

Les paramètres à respecter pour les mots de passe se trouvent dans l'Éditeur de stratégie de groupe locale (**gpedit.msc**) :

Stratégie Ordinateur local > Configuration ordinateur > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs du système d'exploitation > Configurer l'utilisation des mots de passe pour les lecteurs du système d'exploitation et

Stratégie Ordinateur local > Configuration ordinateur > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs de données fixes > Configurer l'utilisation des mots de passe pour les lecteurs de données fixes.

Ces paramètres peuvent également être appliqués à l'aide d'objets de stratégie de groupe basés sur Active Directory.

Par défaut, SafeGuard Enterprise permet l'utilisation de codes confidentiels améliorés. Ceci signifie que ces utilisateurs peuvent utiliser toutes les touches du clavier comme les chiffres, les lettres et les caractères spéciaux ou symboles.

BitLocker prend uniquement en charge la disposition du clavier EN-US. Par conséquent, les utilisateurs pourraient rencontrer des problèmes lors de la saisie de leurs codes confidentiels améliorés ou de leurs mots de passe complexes. Il est conseillé aux utilisateurs de passer en disposition du clavier EN-US avant de créer leur code confidentiel ou mot de passe BitLocker. Ils devront probablement appuyer sur une touche différente de celle de leur clavier pour saisir le caractère voulu. Par conséquent, avant le chiffrement du volume de démarrage, l'ordinateur est

redémarré afin de garantir que l'utilisateur sera en mesure de saisir son code confidentiel ou son mot de passe correctement au démarrage.

À partir de Windows 10 RS2, la longueur minimale requise du code confidentiel est de 6 caractères.

4.1.2 Bon usage : paramètres des stratégies et expérience utilisateur

Le responsable de la sécurité configure les stratégies de chiffrement pour les lecteurs à chiffrer ainsi que pour la stratégie d'authentification. Le module de plate-forme sécurisée (TPM) doit être utilisé à chaque fois que cela est possible. Toutefois, même sans TPM, le volume de démarrage doit être chiffré. L'intervention de l'utilisateur doit être minimale.

Selon ces conditions, le responsable de la sécurité choisit les paramètres d'authentification suivants (il s'agit des paramètres par défaut) :

- **Mode de connexion BitLocker pour les volumes de démarrage** : **TPM + PIN**
- **Mode de connexion de secours BitLocker pour volumes de démarrage** : **Mot de passe ou clé de démarrage**
- **Mode de connexion BitLocker pour volumes non démarrables** : **Auto-déverrouiller**
- **Mode de connexion de secours BitLocker pour volumes non démarrables** : **Mot de passe ou clé de démarrage**

Le responsable de la sécurité crée une stratégie de protection des périphériques ayant pour objet le **Stockage interne** et règle le mode de chiffrement sur **Basé sur le volume**. Les deux stratégies vont être appliquées aux terminaux à chiffrer.

Pour les utilisateurs SafeGuard Enterprise BitLocker, les cas de figure suivants sont possibles :

Cas de figure 1 : un utilisateur se connecte à un terminal à l'aide d'un TPM.

1. L'utilisateur est invité à saisir son code confidentiel pour le volume de démarrage (par exemple, lecteur C:).
2. L'utilisateur saisit le code confidentiel et clique sur **Redémarrer et chiffrer**.
3. Le système teste le matériel et s'assure que l'utilisateur peut saisir correctement son code confidentiel. Il redémarre et invite l'utilisateur à saisir son code confidentiel.
    - Si l'utilisateur saisit son code confidentiel correctement, le terminal démarre.
    - Si l'utilisateur ne saisit pas son code confidentiel correctement, (en raison d'une disposition du clavier incorrecte par exemple), l'utilisateur peut appuyer sur la touche **Echap** dans l'environnement de prédémarrage pour annuler le test et démarrer le terminal.
    - En cas de problème matériel (par exemple, le non fonctionnement du TPM), le test est interrompu et le terminal démarre.
4. L'utilisateur se connecte de nouveau.
5. Si le test matériel réussi (l'utilisateur a saisi son code confidentiel correctement et aucun problème n'a été rencontré avec le TPM), le chiffrement du volume de démarrage commence.

Dans le cas contraire (en cas d'échec du test), une erreur est signalée et le volume n'est pas chiffré. Si le test échoue parce que l'utilisateur a appuyé sur **Echap** dans l'environnement de prédémarrage, l'utilisateur est invité à saisir de nouveau son code confidentiel et à redémarrer l'ordinateur (comme à l'étape 2, les étapes 3, 4 et 5 seront répétées).

6. Le chiffrement du volume de démarrage commence.
7. Le chiffrement des volumes de données commence également sans qu'aucune intervention de l'utilisateur ne soit nécessaire.

Cas de figure 2 : un utilisateur se connecte à un terminal Windows 8 sans TPM.

1. L'utilisateur est invité à saisir son mot de passe pour le volume de démarrage.
2. L'utilisateur saisit le mot de passe et clique sur **Redémarrer et chiffrer**.
3. Le système redémarre, teste le matériel et l'utilisateur se connecte de nouveau comme décrit dans le cas de figure précédent (précisément comme aux étapes 3 à 6 du cas de figure 1. Les références au TPM peuvent être ignorées et un mot de passe est nécessaire plutôt qu'un code confidentiel).
4. Le chiffrement du volume de démarrage commence.
5. Le chiffrement des volumes de données commence également sans qu'aucune intervention de l'utilisateur ne soit nécessaire.

Cas de figure 3 : un utilisateur se connecte à un terminal Windows 7 sans TPM.

1. L'utilisateur est invité à sauvegarder la clé de chiffrement du volume de démarrage sur une carte mémoire USB.
2. L'utilisateur connecte une carte mémoire ou clé USB et appuie sur **Enregistrer et redémarrer**.
3. Le système redémarre, teste le matériel et l'utilisateur se connecte de nouveau. (il s'agit de la même procédure que dans les cas de figure précédents. En revanche, l'utilisateur doit fournir la carte mémoire USB au moment du démarrage. Une autre erreur matériel pouvant survenir serait l'impossibilité de lire la carte mémoire USB à partir de l'environnement de prédémarrage).
4. Le chiffrement du volume de démarrage commence.
5. Le chiffrement des volumes de données commence également sans qu'aucune intervention de l'utilisateur ne soit nécessaire.

Cas de figure 4 : le responsable de la sécurité change le paramètre de la stratégie **Mode de connexion de secours BitLocker pour volumes de démarrage** sur **Mot de passe**. un utilisateur se connecte à un terminal Windows 7 sans TPM.

1. Le terminal n'ayant pas de TPM et Windows 7 n'autorisant pas l'utilisation de mots de passe pour les volumes de démarrage, le volume de démarrage ne sera pas chiffré.
2. Pour chaque volume non démarrable, l'utilisateur est invité à enregistrer la clé externe sur une carte mémoire USB. Le chiffrement du volume respectif commence dès que l'utilisateur clique sur **Enregistrer**.

3. Lorsque l’utilisateur redémarre le terminal, la clé USB doit être connectée afin de permettre le déverrouillage des volumes non démarrables.

4.1.3 Conditions préalables à la gestion de BitLocker sur les terminaux

- Si vous voulez utiliser les méthodes de connexion **TPM + PIN**, **TPM + Clé de démarrage**, **Clé de démarrage** ou **Mot de passe**, veuillez activer la Stratégie de groupe **Demander une authentification supplémentaire au démarrage** soit dans Active Directory, soit localement sur les ordinateurs. Dans l’Éditeur d’objets de stratégie de groupe (gpedit.msc), la Stratégie de groupe se trouve à l’emplacement suivant :

  Stratégie Ordinateur local > Configuration ordinateur > Modèles d’administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteur du système d’exploitation.

  Pour utiliser la méthode **Clé de démarrage**, veuillez également activer **Autoriser BitLocker sans un module de plateforme sécurisée compatible** dans la Stratégie de groupe.
- Pour utiliser **TPM + PIN** sur les tablettes, veuillez activer la Stratégie de groupe **Activer l’utilisation de l’authentification BitLocker exigeant une saisie au clavier préalable au démarrage sur tablettes tactiles**.

  Remarque :

  Ces Stratégies de groupe sont automatiquement activées lors de l’installation sur le terminal. Assurez-vous que les paramètres ne sont pas remplacés par différentes Stratégies de groupe.

- Une stratégie de protection des périphériques BitLocker qui déclenche la configuration d’un mécanisme d’authentification (par exemple **TPM**, **TPM + PIN**, **TPM + Clé de démarrage**) va automatiquement déclencher l’activation TPM. L’utilisateur est informé que le TPM doit être activé et si le système doit être redémarré ou arrêté selon le TPM utilisé.

  Remarque :

  Si la gestion de SafeGuard BitLocker est installée sur un terminal, il se peut que l’état de chiffrement d’un lecteur indique **Non préparé**. Retrouvez plus de renseignements à la section Onglet Lecteurs *(page 138)*. Ceci signifie que le lecteur ne peut actuellement pas être chiffré avec BitLocker car les préparations d’usage n’ont pas encore été effectuées. Ceci s’applique uniquement aux terminaux administrés. En effet, les terminaux non administrés ne sont pas en mesure de créer des rapports sur les données d’inventaire.

Avec l’outil de ligne de commande SGNState (nécessitant les droits administratifs), vous pouvez vérifier si le terminal est correctement préparé pour le chiffrement BitLocker. Dans certains cas, les Outils de préparation de lecteur Windows BitLocker doivent être exécutés.

4.1.3.1 Challenge/Réponse SafeGuard pour BitLocker

L’utilisation du Challenge/Réponse SafeGuard Enterprise pour BitLocker nécessite de satisfaire aux conditions ci-dessous :

- Windows 64 bits
- Version UEFI 2.3.1 ou plus récente
- Certificat UEFI de Microsoft activé ou Démarrage sécurisé désactivé
- Entrées de démarrage NVRAM accessibles à partir de Windows
- Windows installé en mode GPT
- Le matériel ne doit pas être répertorié dans le fichier POACFG.xml.

  Sophos fournit un fichier POACFG.xml par défaut intégré dans le programme d’installation. Nous vous conseillons de télécharger le fichier le plus récent et de le mettre à disposition du programme d’installation.

Pendant l’installation sur le terminal et pendant le premier redémarrage, SafeGuard Enterprise détermine si le matériel satisfait aux conditions requises pour BitLocker avec le Challenge/Réponse SafeGuard. S’il ne satisfait pas aux conditions, la gestion de SafeGuard Enterprise BitLocker s’effectue sans Challenge/Réponse. Dans ce cas, la clé de récupération BitLocker peut être récupérée à l’aide de SafeGuard Management Center.

4.1.4 Gestion du Chiffrement de lecteur BitLocker avec SafeGuard Enterprise

La gestion centralisée et totalement transparente de BitLocker via SafeGuard Enterprise peut être utilisée au sein d’environnements informatiques hétérogènes. SafeGuard Enterprise améliore de manière considérable les fonctions BitLocker. Les stratégies de sécurité de BitLocker peuvent être appliquées de manière centralisée via SafeGuard Enterprise. Même des processus critiques, comme

la gestion et la récupération des clés, sont disponibles lorsque BitLocker est géré par l'intermédiaire de SafeGuard Enterprise.

SafeGuard Enterprise vous permet de gérer le Chiffrement de lecteur BitLocker à partir de SafeGuard Management Center. En tant que responsable de la sécurité, vous pouvez créer des stratégies de chiffrement et d'authentification et les distribuer sur les terminaux BitLocker.

Lorsqu'un terminal BitLocker est enregistré dans SafeGuard Management Center, les informations concernant l'utilisateur, l'ordinateur, le mode de connexion et l'état du chiffrement apparaissent. Les événements sont également consignés dans le journal pour les terminaux BitLocker.

Les terminaux chiffrés avec BitLocker proposent les mêmes fonctionnalités d'administration que les terminaux chiffrés avec SafeGuard Full Disk Encryption. Vous pouvez vérifier le type d'un ordinateur dans la section **Inventaire** sous section in **Utilisateurs et ordinateurs**. La colonne **Type de chiffrement** vous indique s'il s'agit d'un terminal BitLocker.

Remarque : Lors de l'installation du client SafeGuard Enterprise sur Windows 7, la fonction **BitLocker** doit être explicitement sélectionnée pour activer la gestion de BitLocker.

Retrouvez plus de renseignements sur BitLocker To Go et SafeGuard Enterprise, à la section BitLocker To Go *(page 332)*.

4.1.5 Chiffrement avec BitLocker géré par SafeGuard Enterprise

La prise en charge du Chiffrement de lecteur BitLocker dans SafeGuard Enterprise vous permet de chiffrer les volumes de démarrage ainsi que les volumes non démarrables à l'aide du chiffrement et des clés BitLocker. De plus, toutes les données se trouvant, par exemple, sur les supports amovibles peuvent être chiffrées avec le chiffrement de fichiers de SafeGuard Enterprise et les clés SafeGuard Enterprise. Il ne s'agit pas d'une fonction BitLocker mais bien d'une fonction offerte par SafeGuard Enterprise.

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

4.1.5.1 Clés de chiffrement pour BitLocker

Lors d'un chiffrement du volume de démarrage ou d'autres volumes avec BitLocker via SafeGuard Enterprise, les clés de chiffrement sont toujours générées par BitLocker. Une clé est générée par BitLocker pour chaque volume et ne peut pas être réutilisée.

Lors de l'utilisation de BitLocker avec SafeGuard Enterprise, une clé de sauvegarde est stockée dans la base de données SafeGuard Enterprise. Ceci permet de définir un mécanisme d'assistance et de récupération similaire au mécanisme de Challenge/Réponse de SafeGuard Enterprise.

Il n'est cependant pas possible de sélectionner globalement des clés et de les réutiliser avec des clients SafeGuard Enterprise natifs. Les clés n'apparaissent pas dans SafeGuard Management Center.

Remarque : BitLocker vous permet également de sauvegarder les clés de récupération dans Active Directory. Si cette option est activée dans les objets de stratégie de groupe (GPO), l'opération est effectuée automatiquement lorsqu'un volume est chiffré avec BitLocker. Si un volume est déjà chiffré, l'administrateur peut sauvegarder les clés de récupération manuellement à l'aide de l'outil Manage-BDE de Windows (voir « manage-bde -protectors -adbackup -? »).

4.1.5.2 Algorithmes BitLocker dans SafeGuard Enterprise

BitLocker prend en charge les algorithmes AES (Advanced Encryption Standard) suivants:

- AES-128
- AES-256

AES-128 avec diffuseur et AES-256 avec diffuseur ne sont plus pris en charge. Les lecteurs déjà chiffrés utilisant un algorithme avec un diffuseur peuvent être gérés par SafeGuard Enterprise.

4.1.5.3 Stratégies de chiffrement pour le Chiffrement de lecteur BitLocker

Le responsable de la sécurité peut créer une stratégie de chiffrement (initial) dans SafeGuard Management Center et la distribuer aux terminaux BitLocker lors de l'exécution. Elle déclenche le chiffrement BitLocker des lecteurs indiqués dans la stratégie.

Les clients BitLocker étant administrés de manière transparente dans SafeGuard Management Center, le responsable de la sécurité ne doit procéder à aucun paramétrage BitLocker spécifique pour le chiffrement. SafeGuard Enterprise connait l'état du client et sélectionne en conséquence le chiffrement BitLocker. Lorsqu'un client BitLocker est installé avec SafeGuard Enterprise et que le chiffrement de volumes est activé, les volumes sont chiffrés par le Chiffrement de lecteur BitLocker.

Un terminal BitLocker traite les stratégies de type **Protection des périphériques** et **Authentification**.

Les paramètres suivants sont évalués sur le terminal :

- Paramètres d'une stratégie de type **Protection des périphériques** :
  - **Cible : Périphériques de stockage locaux | Volumes internes | Volumes de démarrage | Volumes non démarrables | Lettres des lecteurs A: - Z:**
  - **Mode de chiffrement des supports : Chiffrement basé sur volume** | **Aucun chiffrement**
  - **Algorithme à utiliser pour le chiffrement : AES128** | **AES256**
  - **Chiffrement initial rapide : Oui** | **Non**

Retrouvez plus de renseignements à la section Protection des périphériques *(page 286)*.

- Paramètres d'une stratégie de type **Authentification** :
  - **Mode de connexion BitLocker pour les volumes de démarrage : TPM** | **TPM + PIN** | **TPM + Clé de démarrage** | **Clé de démarrage**
  - **Mode de connexion de secours BitLocker pour volumes de démarrage : Mot de passe** | **Clé de démarrage** | **Mot de passe ou clé de démarrage** | **Erreur**
  - **Mode de connexion BitLocker pour volumes non démarrables** : **Auto-déverrouiller** | **Mot de passe** | **Clé de démarrage**
  - **Mode de connexion de secours BitLocker pour volumes non démarrables** : **Mot de passe** | **Mot de passe ou clé de démarrage** | **Clé de démarrage**

Retrouvez plus de renseignements à la section Authentification *(page 263)*.

Tous les autres paramètres sont ignorés par le terminal BitLocker.

4.1.5.4 Chiffrement sur un ordinateur protégé par BitLocker

Avant toute opération de chiffrement, les clés de chiffrement sont générées par BitLocker. Le comportement est légèrement différent selon le système utilisé.

Terminaux avec TPM

Si le responsable de la sécurité définit un mode de connexion à BitLocker avec le module TPM (TPM, TPM + PIN, ou TPM + Clé de démarrage), l'activation du TPM est automatiquement initiée.

Le TPM (Module de plate-forme sécurisée) est un périphérique matériel utilisé par BitLocker pour stocker ses clés de chiffrement. Les clés ne sont pas stockées sur le disque dur de l'ordinateur. Le module TPM doit être accessible par le BIOS au cours du démarrage. Lorsque l'utilisateur démarre son ordinateur, BitLocker récupère ces clés automatiquement à partir du TPM.

Terminaux sans TPM

Si un terminal n'est pas équipé d'un TPM, une clé de démarrage BitLocker (sous Windows 8 ou version supérieure) ou un mot de passe peut être utilisé comme mode de connexion.

Une clé de démarrage BitLocker peut être créée à l'aide d'une carte mémoire USB pour stocker les clés de chiffrement. L'utilisateur doit insérer la carte mémoire à chaque démarrage de l'ordinateur.

Lorsque SafeGuard Enterprise active BitLocker, les utilisateurs sont invités à procéder à l'enregistrement de la clé de démarrage BitLocker. Une boîte de dialogue affiche les lecteurs cible valides dans lesquels vous pouvez stocker la clé de démarrage.

Pour les **volumes de démarrage**, la clé de démarrage doit être disponible au démarrage du terminal. La clé de démarrage peut donc uniquement être stockée sur des supports amovibles.

Pour les volumes de données, la clé de démarrage BitLocker peut être conservée sur un volume de démarrage chiffré. Cette opération est effectuée automatiquement si l'option **Auto-déverrouiller** est sélectionnée dans la stratégie.

Clés de récupération BitLocker

Pour la récupération BitLocker, SafeGuard Enterprise offre une procédure Challenge/Réponse permettant d'échanger des informations en toute confidentialité et d'obtenir la clé de récupération BitLocker auprès du support technique. Retrouvez plus de renseignements à la section Récupération des terminaux chiffrés avec BitLocker *(page 333)*.

Pour permettre la récupération par Challenge/Réponse ou l'obtention de la clé de récupération, le support technique doit avoir les données nécessaires à disposition. Ces données nécessaires à la récupération sont enregistrées dans des fichiers de récupération de clé spécifiques.

Remarque : Si la gestion de SafeGuard BitLocker sans Challenge/Réponse en mode autonome est utilisée, la clé de récupération ne change pas suite à la procédure de récupération.

Remarque : Si un disque dur chiffré BitLocker sur un ordinateur est remplacé par un nouveau disque dur chiffré BitLocker et que celui-ci prend la même lettre de lecteur que le précédent, SafeGuard Enterprise n'enregistre que la clé de récupération du nouveau disque.

Gestion des lecteurs déjà chiffrés avec BitLocker

Si des lecteurs déjà chiffrés avec BitLocker sont présents sur votre ordinateur, ils seront gérés par SafeGuard Enterprise dès que le logiciel sera installé.

Lecteurs de démarrage chiffrés

- Selon la prise en charge SafeGuard Enterprise BitLocker utilisée, il se peut que vous deviez redémarrer l'ordinateur. Veuillez redémarrer l'ordinateur aussitôt que possible.
- Si une stratégie de chiffrement SafeGuard Enterprise s'applique au lecteur chiffré :
  - Le **Challenge/Réponse SafeGuard Enterprise BitLocker** est installé : la gestion est prise en charge et il est possible d'utiliser le Challenge/Réponse SafeGuard Enterprise.
  - **SafeGuard Enterprise BitLocker** est installé : la gestion est prise en charge et il est possible d'utiliser la récupération.
- Si aucune stratégie de chiffrement SafeGuard Enterprise ne s'applique au lecteur chiffré :
  - Le **Challenge/Réponse SafeGuard Enterprise BitLocker** est installé : la gestion n'est pas prise en charge et il n'est pas possible d'utiliser le Challenge/Réponse SafeGuard Enterprise.
  - **SafeGuard Enterprise BitLocker** est installé : il est possible d'utiliser la récupération.

Lecteurs de données chiffrés

- Si une stratégie de chiffrement SafeGuard Enterprise s'applique au lecteur chiffré :

la gestion est prise en charge et il est possible d'utiliser la récupération.

- Si aucune stratégie de chiffrement SafeGuard Enterprise ne s'applique au lecteur chiffré :

  il est possible d'utiliser la récupération SafeGuard Enterprise.

4.1.5.5 Déchiffrement avec BitLocker

Les ordinateurs chiffrés avec BitLocker ne peuvent pas être déchiffrés automatiquement. Le déchiffrement peut être effectué soit à l'aide du **Chiffrement de lecteur BitLocker** depuis le **Panneau de configuration** soit en utilisant l'outil de ligne de commande « manage-bde » de Microsoft.

Pour permettre aux utilisateurs de déchiffrer les lecteurs chiffrés avec BitLocker manuellement, une stratégie sans règle de chiffrement pour le lecteur chiffré par BitLocker doit être appliquée sur le terminal. L'utilisateur peut alors déclencher le déchiffrement en désactivant BitLocker pour le lecteur de son choix dans le **Panneau de configuration** du **Chiffrement de lecteur BitLocker** ou via « manage-bde ».

4.1.6 BitLocker To Go

BitLocker To Go peut être utilisé pour chiffrer des volumes sur des supports amovibles lorsque les composants du client de prise en charge de SafeGuard Enterprise BitLocker sont installés. Toutefois, BitLocker To Go ne peut pas être administré par SafeGuard Enterprise.

Retrouvez plus de renseignements sur la désactivation de BitLocker To Go à la section Désactivation du chiffrement BitLocker To Go *(page 332)*.

BitLocker To Go est incompatible avec SafeGuard Full Disk Encryption (chiffrement intégral des disques par volume). Lorsque vous installez SafeGuard Full Disk Encryption, BitLocker To Go est désactivé. Les volumes et supports amovibles déjà chiffrés avec BitLocker To Go demeurent accessibles.

4.1.6.1 Désactivation du chiffrement BitLocker To Go

1. Dans l'Éditeur de stratégie de groupe Windows, sélectionnez **Stratégie Ordinateur local > Configuration ordinateur > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs de données amovibles**.
2. Cliquez avec le bouton droit de la souris sur **Contrôler l'utilisation de BitLocker sur les lecteurs amovibles** et sélectionnez **Modifier**.
3. Sélectionnez **Activé**.
4. Sous **Options**, dessélectionnez **Autoriser les utilisateurs à protéger les lecteurs de données amovibles avec BitLocker**.

5. Sous **Options**, sélectionnez **Autoriser les utilisateurs à suspendre et supprimer la protection BitLocker sur les lecteurs de données amovibles**.
6. Cliquez sur **OK**.

Le chiffrement BitLocker To Go est désactivé sur les terminaux. Les utilisateurs ne peuvent plus chiffrer les nouveaux volumes avec BitLocker To Go. Les volumes et supports amovibles déjà chiffrés avec BitLocker To Go demeurent accessibles.

4.1.7 Récupération des terminaux chiffrés avec BitLocker

Selon le système utilisé, SafeGuard Enterprise offre une procédure Challenge/Réponse pour la récupération ou la possibilité d'obtenir une clé de récupération de la part du support. Retrouvez plus de renseignements sur la configuration requise du Challenge/Réponse SafeGuard Enterprise à la section Challenge/Réponse SafeGuard pour BitLocker *(page 327)*.

4.1.7.1 Récupération par l'ID de clé de récupération BitLocker

S'il s'agit d'ordinateurs chiffrés par BitLocker, un volume qui n'est plus accessible peut être récupéré à l'aide de l'ID de clé de récupération BitLocker.

Les utilisateurs doivent fournir ce numéro d'ID. Lorsque du processus de récupération, l'ID de la clé de récupération BitLocker du lecteur du système d'exploitation est affichée sur l'écran de récupération BitLocker. Pour les lecteurs de données, l'ID de la clé de récupération BitLocker s'affiche lorsque les utilisateurs cliquent sur **Plus d'options** puis sur **Saisir la clé de récupération** dans l'assistant pour déverrouiller un lecteur chiffré par BitLocker.

⚠ **Important :** Les clés de récupération sont uniquement affichées si le responsable de la sécurité dispose des autorisations requises pour gérer l'ordinateur. Si l'ordinateur a été supprimé de SafeGuard Management Center, l'autorisation **Utiliser l'outil de récupération** est requise pour accéder aux clés de récupération.

1. Pour ouvrir l'**Assistant de récupération** dans SafeGuard Management Center, cliquez sur **Outils > Récupération**.

2. Sur la page **Type de récupération**, sélectionnez **ID de la clé de récupération BitLocker (administré)** et cliquez sur **Suivant**.

3. Cliquez sur **[...]** pour rechercher l'ID d'une clé de récupération.

4. Sur la page **Rechercher la clé de récupération BitLocker**, saisissez au moins les quatre premiers chiffres de l'ID de la clé de récupération BitLocker dans le champ **Rechercher le nom** et cliquez sur **Rechercher maintenant**.
   Toutes les clés correspondant à votre demande sont affichées.

Les clés actives et inactives sont affichées. Les clés de récupération sont affichées même si l'ordinateur assigné a été supprimé du SafeGuard Management Center. Dans ce cas, le nom de l'ordinateur ne peut pas être déterminé et **N/A** est affiché dans la colonne **Ordinateur**.

5. Sélectionnez la clé désirée et cliquez sur **OK**.
   Les informations sur la clé sont affichées sur la page **Rechercher la clé de récupération BitLocker**.
6. Cliquez sur **Suivant**.
   Sur la page **Récupération BitLocker**, la clé de récupération BitLocker à 48 chiffres est affichée.
7. Fournissez cette clé à l'utilisateur.

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

4.1.7.2 Clé de restauration des terminaux SafeGuard Enterprise sous une version inférieure à la version 7

S'il s'agit d'ordinateurs chiffrés avec BitLocker, un volume qui n'est plus accessible peut être restauré.

Les utilisateurs doivent fournir le nom de l'ordinateur puis récupérer la clé de restauration à saisir sur l'écran de restauration.

1. Pour ouvrir l'**Assistant de restauration** dans SafeGuard Management Center, cliquez sur **Outils > Restauration**.
2. Sur la page **Type de restauration**, sélectionnez **Client SafeGuard Enterprise (administré)**.
3. Sous **Domaine**, sélectionnez le domaine requis dans la liste.
4. Sous **Ordinateur**, saisissez ou sélectionnez le nom d'ordinateur requis. Vous pouvez procéder de plusieurs façons :

   - Pour sélectionner un nom, cliquez sur **[...]**. Cliquez ensuite sur **Rechercher maintenant**. Une liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur s'affiche dans la fenêtre **Type de restauration** sous **Domaine**.

   - Saisissez le nom abrégé de l'ordinateur directement dans le champ. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.

   - Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

     CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae
5. Cliquez sur **Suivant**.

6. Sélectionnez le volume auquel accéder dans la liste et cliquez sur **Suivant**.
7. L’assistant de récupération affiche la clé de récupération à 48 chiffres correspondante.
8. Fournissez cette clé à l’utilisateur.

L’utilisateur peut la saisir afin de récupérer le volume chiffré BitLocker sur le terminal.

4.1.7.3 Challenge/Réponse pour BitLocker

Pour les terminaux UEFI satisfaisant à certaines conditions requises, SafeGuard Enterprise offre la procédure Challenge/Réponse pour la récupération.

Les utilisateurs doivent fournir le code de challenge affiché sur l’écran de récupération BitLocker et en retour, ils recevront une réponse à saisir sur l’écran de récupération.

Sur les terminaux UEFI qui ne remplissent pas ces conditions requises, la gestion SafeGuard BitLocker sans procédure Challenge/Réponse est installée automatiquement. Retrouvez plus de renseignements sur la récupération de ces terminaux aux sections Récupération par l’ID de clé de récupération BitLocker *(page 333)* et Clé de restauration des terminaux SafeGuard Enterprise sous une version inférieure à la version 7 *(page 334)*.

1. Pour ouvrir l’**Assistant de récupération** dans SafeGuard Management Center, cliquez sur **Outils** > **Récupération**.
2. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise (administré)**.
3. Sous **Domaine**, sélectionnez le domaine requis dans la liste.
4. Sous **Ordinateur**, saisissez ou sélectionnez le nom d’ordinateur requis. Vous pouvez procéder de plusieurs façons :
   - Pour sélectionner un nom, cliquez sur **[...]**. Cliquez ensuite sur **Rechercher maintenant**. Une liste des ordinateurs s’affiche. Sélectionnez l’ordinateur requis, puis cliquez sur **OK**. Le nom de l’ordinateur apparaît sur la page **Type de récupération**.
   - Saisissez le nom abrégé de l’ordinateur directement dans le champ. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S’il est trouvé, le nom d’ordinateur unique s’affiche.
   - Saisissez directement le nom de l’ordinateur au format de nom unique, par exemple :

     CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae
5. Cliquez sur **Suivant**.
6. Sélectionnez le volume auquel accéder dans la liste et cliquez sur **Suivant**.

7. Cliquez sur **Suivant**.

   Une fenêtre apparaît où vous pouvez saisir le code de challenge.

8. Saisissez le code de challenge que l’utilisateur vous a transmis et cliquez sur **Suivant**.

9. Un code de réponse est généré. Fournissez le code de réponse à l’utilisateur. Une aide à l’épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L’utilisateur peut saisir le code de réponse et accède au terminal.

4.2 Chiffrement de fichiers par emplacement

Le module Chiffrement de fichiers de SafeGuard Enterprise offre un chiffrement de fichiers par emplacement des lecteurs locaux et des emplacements réseau, surtout pour les groupes de travail et les partages réseau.

Dans SafeGuard Management Center, vous définissez les règles du chiffrement basé sur fichier dans les stratégies **Chiffrement de fichiers**. Dans ces règles de Chiffrement de fichiers, vous indiquez les dossiers qui doivent être gérés par le Chiffrement de fichiers, le mode de chiffrement et la clé à utiliser pour le chiffrement. Dans les stratégies **Paramètres généraux**, vous pouvez définir comment des applications et des systèmes de fichiers spécifiques sont gérés sur les terminaux dans le contexte du Chiffrement de fichiers. Vous pouvez indiquer les applications ignorées et fiables ainsi que les périphériques ignorés. Vous pouvez aussi activer le chiffrement permanent pour le Chiffrement de fichiers.

Pour le chiffrement, des clés personnelles peuvent être utilisées. Une clé personnelle activée pour un utilisateur particulier s’applique uniquement à cet utilisateur et ne peut pas être partagée avec d’autres utilisateurs ou assignées à ces derniers. Vous pouvez créer des clés personnelles dans SafeGuard Management Center sous **Utilisateurs et ordinateurs**.

Après assignation d’une stratégie **Chiffrement de fichiers** sur vos terminaux, les fichiers présents dans les emplacements couverts par la stratégie sont chiffrés de manière transparente sans intervention de l’utilisateur :

- Les nouveaux fichiers dans les emplacements correspondants sont chiffrés automatiquement.
- Si les utilisateurs ont la clé d’un fichier chiffré, ils peuvent lire et modifier le contenu.
- S’ils n’ont pas la clé du fichier chiffré, l’accès est refusé.
- Si un utilisateur accède à un fichier chiffré sur un terminal sur lequel le Chiffrement de fichiers n’est pas installé, le contenu chiffré apparaît.

Les fichiers déjà présents dans les emplacements couverts par la stratégie de chiffrement ne sont pas chiffrés automatiquement. Les utilisateurs doivent procéder au chiffrement initial dans l'**Assistant de chiffrement de fichiers SafeGuard** sur le terminal. Retrouvez plus de renseignements dans le *Manuel d'utilisation de SafeGuard Enterprise*.

Remarque :

SafeGuard File Encryption n'est pas compatible avec le chiffrement EFS intégré et la compression de fichiers de Windows. Si EFS est activé, il est prioritaire sur toute règle de chiffrement de fichiers applicable et les fichiers créés dans le dossier en question ne peuvent pas être chiffrés par le Chiffrement de fichiers. Si la compression est activée, le Chiffrement de fichiers a une priorité plus haute et les fichiers sont chiffrés mais pas compressés. Pour chiffrer les fichiers avec le Chiffrement de fichiers, veuillez d'abord supprimer le chiffrement EFS ou la compression des données. L'opération peut être effectuée manuellement ou en exécutant l'assistant de chiffrement initial de SafeGuard Enterprise.

SafeGuard File Encryption n'est pas compatible avec la fonctionnalité de fichiers à la demande depuis Windows 10.

Retrouvez plus de renseignements sur l'utilisation des terminaux Mac avec SafeGuard File Encryption pour Mac à la section *À propos de Sophos SafeGuard File Encryption pour Mac (page 385)* et dans le *Manuel d'utilisation de SafeGuard Enterprise pour Mac*.

4.2.1 Configuration des règles de chiffrement dans les stratégies de chiffrement de fichiers par emplacement

Vous définissez les règles du chiffrement de fichiers sur les emplacements réseau dans une stratégie du type **Chiffrement de fichiers**.

Remarque : Lorsqu'ils sont chiffrés, certains dossiers (par exemple, C:\Program Files) peuvent empêcher l'exécution du système d'exploitation ou d'applications. Lorsque vous définissez des règles de chiffrement, assurez-vous que ces dossiers ne sont pas chiffrés.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Chiffrement de fichiers** ou sélectionnez-en une.
   L'onglet **Chiffrement de fichiers** apparaît.

2. Sélectionnez **Par emplacement** dans la liste déroulante **Type de chiffrement**.
   Le tableau des emplacements sur lesquels le chiffrement de fichiers par emplacement est appliqué sur l'ordinateur apparait.

   Remarque : Le paramètre **Type de chiffrement** est disponible à partir de la version 8.0 de SafeGuard Enterprise. Si vous avez mis à jour la console SafeGuard Management Center, les stratégies de chiffrement de fichiers déjà existantes seront converties en stratégies de chiffrement de fichiers **Par emplacement**. Retrouvez plus de renseignements sur le **Type de**

chiffrement > Aucun chiffrement à la section Stratégies de type Aucun chiffrement *(page 133)*.

3. Dans la colonne **Chemin**, définissez le chemin (c'est-à-dire le dossier) à gérer par le Chiffrement de fichiers :
   - Cliquez sur le bouton déroulant et sélectionnez un espace réservé de nom de dossier dans la liste des espaces réservés disponibles.

     En faisant passer votre curseur sur les entrées de la liste, vous pouvez afficher des infobulles qui vous indiquent comment un espace réservé est généralement présenté sur un terminal. Vous pouvez seulement saisir des espaces réservés valides. Retrouvez une description de tous les espaces réservés disponibles à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.

     ⚠ **Important :** Le chiffrement intégral du profil utilisateur à l'aide de l'espace réservé `<Profil utilisateur>` peut entraîner une instabilité du bureau Windows sur le terminal.

   - Cliquez sur le bouton Parcourir pour naviguer dans le système de fichiers et sélectionnez le dossier requis.
   - Sinon, saisissez simplement un nom de chemin.

   Retrouvez plus de renseignements utiles sur la configuration des chemins dans les règles de chiffrement de fichiers à la section Informations supplémentaires sur la configuration des chemins dans les règles de chiffrement de fichiers par emplacement *(page 339)*.

4. Dans la colonne **Étendue**, sélectionnez :
   - **Ce dossier uniquement** pour appliquer la règle seulement au dossier indiqué par la colonne **Chemin**.
   - **Inclure les sous-dossiers** pour appliquer aussi la règle à tous ses sous-dossiers.

5. Dans la colonne **Mode**, définissez comment le Chiffrement de fichiers doit gérer le dossier indiqué dans la colonne **Chemin** :
   - Sélectionnez **Chiffrer** pour chiffrer de nouveaux fichiers dans le dossier. Le contenu des fichiers chiffrés existants est déchiffré de manière transparente lorsqu'un utilisateur y accède avec la clé requise. Si l'utilisateur n'a pas la clé requise, l'accès est refusé.
   - Si vous sélectionnez **Exclure**, les nouveaux fichiers du dossier ne sont pas chiffrés. Vous pouvez utiliser cette option pour exclure un sous-dossier du chiffrement si le dossier parent est déjà couvert par une règle avec l'option **Chiffrer**.
   - Si vous sélectionnez **Ignorer**, les fichiers du dossier ne sont pas gérés du tout par le Chiffrement de fichiers. Les nouveaux fichiers sont enregistrés en texte brut. Si un utilisateur accède déjà aux fichiers chiffrés dans ce dossier, le contenu chiffré apparaît, que l'utilisateur ait la clé requise ou pas.

6. Dans la colonne **Clé**, sélectionnez la clé à utiliser pour le mode **Chiffrer**. Vous pouvez utiliser des clés créées et appliquées dans **Utilisateurs et ordinateurs** :

- Cliquez sur le bouton Parcourir pour ouvrir la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour afficher une liste de toutes les clés disponibles et sélectionnez la clé requise.

  Remarque : Les clés machine ne sont pas montrées dans la liste. Elles ne peuvent pas être utilisées par le Chiffrement de fichiers car elles sont uniquement disponibles sur une seule machine et ne peuvent donc pas être utilisées pour permettre à des groupes d'utilisateurs d'accéder aux mêmes données.

- Clique sur le bouton **Clé personnelle** avec l'icône de la clé, pour insérer l'espace réservé **Clé personnelle** dans la colonne **Clé**. Sur le terminal, cet espace réservé sera résolu sur la clé personnelle active de l'utilisateur SafeGuard Enterprise connecté. Si les utilisateurs correspondants n'ont pas encore de clés personnelles actives, elles sont créées automatiquement. Vous pouvez créer des clés personnelles pour un ou plusieurs utilisateurs dans **Utilisateurs et ordinateurs**. Retrouvez plus de renseignements à la section Clés personnelles pour le chiffrement de fichiers par File Encryption *(page 177)*.

7. Le type de **Système** (**Windows**, **macOS** ou **Tous les systèmes** pour les systèmes Windows et macOS) sera assigné automatiquement.

8. Ajoutez d'autres règles de chiffrement selon vos besoins et enregistrez vos changements.

   Remarque : Toutes les règles de Chiffrement de fichiers assignées par des stratégies et activées pour les utilisateurs/ordinateurs à des nœuds différents dans **Utilisateurs et ordinateurs** sont cumulées. L'ordre des règles de chiffrement dans une stratégie **Chiffrement de fichiers** n'a pas d'importance pour leur évaluation sur le terminal. Dans une stratégie **Chiffrement de fichiers**, vous pouvez déplacer les règles pour avoir une meilleur visibilité.

4.2.1.1 Informations supplémentaires sur la configuration des chemins dans les règles de chiffrement de fichiers par emplacement

Lors de la configuration des chemins dans les règles de chiffrement de fichiers, veuillez prendre en compte ce qui suit.

- Un chemin peut seulement contenir des caractères qui peuvent aussi être utilisés dans des systèmes de fichiers. Les caractères comme <, >, * et $ ne sont pas autorisés.
- Vous pouvez seulement saisir des espaces réservés valides. Retrouvez une liste de tous les espaces réservés pris en charge à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.

  Les noms des variables d'environnement ne sont pas vérifiés par SafeGuard Management Center. Ils doivent seulement être présents sur le terminal.

- Le champ **Chemin** indique toujours un dossier. Vous ne pouvez pas spécifier de fichier unique ou utiliser de caractères joker pour les noms de dossiers, de fichiers ou pour les extensions de fichiers.
- **Règles absolues et relatives**

  Vous pouvez définir des règles absolues et relatives. Une règle absolue définit exactement un dossier spécifique, par exemple C:\encrypt. Une règle relative n'inclut pas d'informations sur le serveur/partage UNC, d'informations sur la lettre du lecteur ou sur le dossier parent. encrypt_sub est un exemple de chemin utilisé dans une règle relative. Dans ce cas, tous les fichiers présents sur tous les lecteurs (y compris les emplacements réseau) qui résident dans un dossier encrypt_sub (ou l'un de ses sous-dossiers) sont couverts par la règle.

  Remarque : Les chemins relatifs sont uniquement autorisés sur les ordinateurs Windows.

- **Noms de dossiers longs et notation 8.3**

  Saisissez toujours les noms de dossiers longs pour les règles File Encryption car les noms 8.3 pour les noms de dossiers longs peuvent varier d'un ordinateur à un autre. Les règles des noms 8.3 sont détectées automatiquement par le terminal protégé par SafeGuard Enterprise lorsque les stratégies correspondantes sont appliquées. Que les applications utilisent des noms de dossiers longs ou des noms 8.3 pour l'accès aux fichiers, le résultat devrait être identique. Pour les règles relatives, utilisez des noms de dossiers courts pour vous assurer que la règle peut être appliquée, que l'application utilise ou non des noms de dossiers longs ou une notation 8.3.

- **Notation UNC et/ou lettres des lecteurs connectés**

  Que l'administration des règles soit basée sur une notation UNC ou sur des lettres de lecteurs connectés dépend de vos conditions requises :

  - Utilisez la notation UNC si vos noms de serveur et de partage ne sont pas susceptibles de changer, mais si les mappages des lettres de lecteurs varient entre les utilisateurs.
  - Utilisez des lettres de lecteurs connectés, si les lettres restent les mêmes et si les noms des serveurs peuvent changer.

  Si vous utilisez UNC, spécifiez un nom de serveur et un nom de partage, par exemple \\serveur \partage.

  File Encryption fait correspondre en interne les noms UNC et les lettres de lecteurs connectés. Dans une règle, un chemin a donc besoin d'être défini soit en tant que chemin UNC, soit avec des lettres de lecteurs connectés.

  Remarque : Les utilisateurs ayant la possibilité de changer le mappage des lettres de leurs lecteurs, nous conseillons d'utiliser les chemins UNC dans les règles File Encryption pour des raisons de sécurité.

- **Dossiers hors ligne**

  Si la fonction Windows **Rendre disponible hors connexion** est utilisée, vous n'avez pas à créer de règles spéciales pour les copies (hors ligne) locales des dossiers. Les nouveaux fichiers dans

la copie locale du dossier qui a été rendue disponible pour une utilisation hors ligne sont chiffrés d'après la règle pour l'emplacement (réseau) d'origine.

Retrouvez plus de renseignements sur les noms de fichiers et de chemins sur http://msdn.microsoft.com/fr-fr/library/aa365247.aspx.

4.2.1.2 Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement

Les espaces réservés suivants peuvent être utilisés lors de la spécification des chemins dans les règles de chiffrement des stratégies **Chiffrement de fichiers**. Vous pouvez sélectionner ces espaces réservés en cliquant sur le bouton du menu déroulant du champ **Chemin**.

Utilisez toujours des barres obliques inverses pour séparer les chemins même lors de la création de règles de chiffrement de fichiers pour macOS. De cette manière, vous pouvez appliquer les règles aux deux systèmes d'exploitation (Windows et macOS). Sur les terminaux macOS, les barres obliques inverses sont automatiquement transformées en barres obliques afin de correspondre aux conditions requises du système d'exploitation macOS. Toutes les erreurs dans les espaces réservés sont consignées dans le journal. Les règles de chiffrement de fichiers incorrectes sont consignées dans le journal, puis ignorées sur le terminal.

Exemple : Le chemin Windows `<Profil utilisateur>\Dropbox\personnel` est converti sur Mac en `/Utilisateurs/<NomUtilisateur>/Dropbox/personnel`.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et macOS)	Résultats dans la valeur suivante sur le terminal
`<%nom_variable_environnement%>`	Tous	Valeur de la variable d'environnement. Exemple : <%NOMUTILISATEUR%>. **Remarque :** Si des variables d'environnement contiennent plusieurs emplacements (par exemple, la variable PATH), les chemins ne seront pas divisés en plusieurs règles. Ceci entraîne une erreur et la règle de chiffrement est non valide.
`<Poste de travail>`	Tous	Dossier virtuel représentant le bureau de l'ordinateur.
`<Documents>`	Tous	Dossier virtuel représentant l'élément du bureau Mes documents (équivalent à CSIDL_MYDOCUMENTS). Chemin type : C:\Documents and Settings\<nom d'utilisateur>\Mes Documents.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et macOS)	Résultats dans la valeur suivante sur le terminal
`<Téléchargements>`	Tous	Dossier dans lequel les téléchargements sont stockés par défaut. Le chemin habituel Windows est C:\Utilisateurs\nom d'utilisateur\Téléchargements.
`<Musique>`	Tous	Répertoire du système de fichiers qui sert de dépôt de données pour les fichiers musique. Chemin type : C:\Documents and Settings \Utilisateur\Mes Documents\Ma Musique.
`<Partages réseau>`	Tous	
`<Images>`	Tous	Répertoire du système de fichiers qui sert de dépôt de données pour les fichiers image. Chemin type : C:\Documents and Settings \nom d'utilisateur\Mes Documents\Mes Images. **Remarque :** Sur les Macs, le chiffrement de tout le dossier `<Images>` n'est pas pris en charge. Toutefois, vous pouvez chiffrer les sous-dossiers, par exemple `<Images>\enc`.
`<Public>`	Tous	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers document de tous les utilisateurs. Chemin type : C: \Utilisateurs\nom d'utilisateur.
`<Amovibles>`	Tous	Dirige vers les dossiers racine de tous les supports amovibles.
`<Profil utilisateur>`	Tous	Dossier du profil de l'utilisateur. Chemin type : C:\Utilisateurs\nom d'utilisateur. **Remarque :** Le chiffrement de tout le profil d'utilisateur n'est pas pris en charge. Toutefois, vous pouvez chiffrer les sous-dossiers, par exemple `<Profil d'utilisateur>\enc`.
`<Vidéos>`	Tous	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers vidéo de tous les utilisateurs. Chemin type : C:\Documents and Settings\All Users \Documents\My Videos.
`<Cookies>`	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les cookies Internet.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et macOS)	Résultats dans la valeur suivante sur le terminal
		Chemin type : C:\Documents and Settings \nom d'utilisateur\Cookies.
<Favoris>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les éléments préférés de l'utilisateur. Chemin type : \Documents and Settings\nom d'utilisateur\Favoris.
<Données des applications locales>	Windows	Répertoire du système de fichiers qui sert de dépôt de données pour les applications locales (non itinérantes). Chemin type : C: \Documents and Settings\nom d'utilisateur \Local Settings\Application Data.
<Données des programmes>	Windows	Répertoire du système de fichier contenant les données d'application de tous les utilisateurs. Chemin type : C:\Documents and Settings\All Users\Application Data.
<Program Files>	Windows	Dossier Program Files. Chemin type : \Program Files. Pour les systèmes 64 bits, celui-ci sera étendu en deux règles : une pour les applications 32 bits et une pour les applications 64 bits.
<Musique publique>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers musique de tous les utilisateurs. Chemin type : C:\Documents and Settings\All Users \Documents\My Music.
<Images publiques>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers image de tous les utilisateurs. Chemin type : C:\Documents and Settings\Tous les utilisateurs\Documents\Mes Images.
<Vidéos publiques>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers vidéo de tous les utilisateurs. Chemin type : C:\Documents and Settings\All Users \Documents\Mes Vidéos.
<Itinérant>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les données spécifiques aux applications. Chemin type : C:\Documents and Settings\nom d'utilisateur\Application Data.
<Système>	Windows	Dossier système Windows. Chemin type : C: \Windows\System32. Pour les systèmes 64

Espace réservé au chemin	Système d'exploitation (Tous=Windows et macOS)	Résultats dans la valeur suivante sur le terminal
		bits, celui-ci sera étendu en deux règles : une pour le 32 bits et une pour le 64 bits.
<Dossier de gravure temporaire>	Windows	Répertoire du système de fichiers qui sert de zone de transit pour les fichiers en attente d'écriture sur un CD-ROM. Chemin type : C:\Documents and Settings\nom d'utilisateur\Local Settings\Application Data\Microsoft\CD Burning.
<Fichiers Internet temporaires>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers temporaires Internet. Chemin type : C:\Documents and Settings\nom d'utilisateur\Local Settings\Temporary Internet Files.
<Windows>	Windows	Répertoire Windows ou SYSROOT. Ceci correspond aux variables d'environnement %windir% ou %SYSTEMROOT%. Chemin type : C:\Windows.
<Racine>	macOS	Le dossier racine macOS. Il est déconseillé d'appliquer des stratégies au dossier racine même si ceci est techniquement possible.

4.2.2 Configuration des paramètres de chiffrement des fichiers par emplacement dans les stratégies Paramètres généraux

En plus des règles de chiffrement définies dans les stratégies **Chiffrement de fichiers** suivantes : **Type de chiffrement** > **Par emplacement**, vous pouvez configurer les paramètres **Chiffrement de fichiers** dans des stratégies du type **Paramètres généraux** :

- **Applications sécurisées**
- **Applications ignorées**
- **Périphériques ignorés**
- **Activer le chiffrement permanent**

4.2.2.1 Configuration des applications sécurisées et ignorées pour le chiffrement de fichiers

Vous pouvez définir des applications comme sécurisées pour leur accorder l'accès aux fichiers chiffrés. Ceci s'avère utile, par exemple, pour activer le logiciel antivirus afin de contrôler les fichiers chiffrés.

Vous pouvez définir des applications comme ignorées pour les exempter du chiffrement/déchiffrement transparent des fichiers. Par exemple, si vous définissez un programme de sauvegarde comme une application ignorée, les données chiffrées sauvegardées par le programme restent chiffrées.

Remarque : Les processus enfants ne seront pas sécurisés/ignorés.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.

2. Sous **Chiffrement de fichiers**, cliquez sur la liste déroulante du champ **Applications sécurisées** ou **Application ignorées**.

3. Dans la zone de liste de l'éditeur, saisissez les applications à définir comme sécurisées/ignorées.
   - Vous pouvez définir plusieurs applications sécurisées/ignorées dans une stratégie. Chaque ligne de la zone de liste de l'éditeur définir une application.
   - Les noms des applications doivent se terminer par .exe.
   - Les noms des applications doivent être indiqués comme des chemins pleinement qualifiés avec informations sur le lecteur/répertoire, par exemple "c:\dir\example.exe". La saisie d'un nom de fichier seulement (par exemple, « exemple.exe ») n'est pas suffisante. Pour une meilleure utilisation, la vue sur une ligne de la liste des applications n'affiche que les noms de fichiers séparés par des points-virgules.
   - Les noms d'applications peuvent contenir les mêmes noms d'espaces réservés pour les dossiers d'environnement Windows et variables d'environnement que les règles de chiffrement dans les stratégies de chiffrement de fichiers. Retrouvez une description de tous les espaces réservés disponibles à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.

4. Enregistrez vos modifications.

Remarque : Les paramètres de stratégie **Applications sécurisées** et **Applications ignorées** sont les paramètres de la machine. La stratégie doit donc être assignée aux machines, pas aux utilisateurs. Sinon, les paramètres ne sont pas activés.

4.2.2.2 Configuration des périphériques ignorés

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.

2. Sous **Chiffrement de fichiers**, cliquez sur la liste déroulante du champ **Périphériques ignorés**.

3. Dans la zone de liste de l'éditeur :

a. Sélectionnez **Réseau** si vous ne voulez pas chiffrer les données sur le réseau.

b. Saisissez les noms de périphériques requis pour exclure des périphériques donnés du chiffrement. Ceci peut être utile lorsque vous avez besoin d'exclure les systèmes des fournisseurs tiers.
Vous pouvez afficher les noms des appareils actuellement utilisés dans le système à l'aide du programme de contrôle Fltmc.exe (fltmc volumes, fltmc instances) à partir de Microsoft. Retrouvez plus de renseignements à la section https://docs.microsoft.com/fr-fr/windows-hardware/drivers/ifs/development-and-testing-tools.

Vous pouvez exclure des lecteurs de disque (réseau) individuels du chiffrement en créant une règle de Chiffrement de fichiers dans une stratégie **Chiffrement de fichiers** et en paramétrant le **Mode** de chiffrement sur **Ignorer**. Vous pouvez uniquement appliquer ce paramètre aux lecteurs administrés par Windows et pas aux volumes macOS.

4.2.2.3 Configuration du chiffrement permanent pour le Chiffrement de fichiers

Le contenu des fichiers chiffrés par File Encryption est déchiffré instantanément si l'utilisateur possède la clé requise. Lorsque le contenu est enregistré sous la forme d'un nouveau fichier dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement, le fichier obtenu ne sera pas chiffré.

Avec le chiffrement permanent, les copies des fichiers chiffrés seront chiffrées, même lorsqu'elles sont enregistrées dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement.

Vous pouvez configurer le chiffrement permanent dans des stratégies du type **Paramètres généraux**. Le paramètre de stratégie **Activer le chiffrement permanent** est activé par défaut.

Remarque :

Si des fichiers sont copiés ou déplacés sur un périphérique ignoré ou dans un dossier auquel s'applique une stratégie avec un mode de chiffrement **Ignorer**, le paramètre **Activer le chiffrement permanent** n'a aucun effet.

Les archives Zip sont ignorées par le chiffrement permanent.

4.2.3 Complément Outlook pour le chiffrement par emplacement

À partir de la version 8.1, le complément Outlook pour Windows de SafeGuard Enterprise est disponible pour le chiffrement par emplacement. Il est disponible sur les terminaux lorsque vous installez un module de Chiffrement de fichiers par emplacement.

En général, la fonctionnalité d'envoi d'emails externes est la même que pour le chiffrement par application. Toutefois, l'envoi d'email avec pièces jointes à des domaines autorisés doit être

effectués avec une grande prudence en raison de la nature du chiffrement par emplacement et des fonctions à plusieurs clés de Synchronized Encryption.

Dans la stratégie **Paramètres généraux par défaut**, vous pouvez configurer ce qui va se passer lorsque des pièces jointes d'emails sont envoyés à des domaines (généralement internes) autorisés. Les options disponibles pour le **Comportement des domaines autorisés** sont :

- **Chiffré**
- **Aucun chiffrement**
- **Toujours demander**
- **Inchangé (Synchronized Encryption)**

Aucun chiffrement et **Toujours demander** se comportent de la même façon pour tous les modules de Chiffrement de fichiers.

Les options **Chiffré** et **Inchangé (Synchronized Encryption)** se comportent différemment lorsqu'elles sont utilisés avec Synchronized Encryption ou avec le chiffrement par emplacement.

Chiffré

- Synchronized Encryption

  Les fichiers chiffrés restent chiffrés et la clé de chiffrement est inchangée. Les fichiers non chiffrés sont chiffrés par la **Clé Synchronized Encryption** uniquement si l'extension de fichier est définie dans la liste des apps intégrées.

- Chiffrement basé sur l'emplacement

  Tous les fichiers joints sont chiffrés avec la **Clé Synchronized Encryption** quelles que soient leurs extensions de fichier et quel que soit leur état de chiffrement.

Inchangé (Synchronized Encryption)

- Synchronized Encryption

  les fichiers chiffrés seront envoyés chiffrés tandis que les fichiers en clair seront envoyés en clair.

- Chiffrement basé sur l'emplacement

  Tous les fichiers sont chiffrés avec la **Clé Synchronized Encryption**.

4.2.3.1 Création de stratégies pour l’activation du complément Outlook de SafeGuard Enterprise

Pour activer le complément Outlook de SafeGuard Enterprise pour le chiffrement de fichiers par emplacement :

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.
   L’onglet **Paramètres généraux** apparaît.

2. Rendez-vous sous la section **Paramètres du module de messagerie complémentaire**.

3. Dans la liste déroulante **Activer le module de messagerie complémentaire**, sélectionnez **Oui**.
   Le module complémentaire est maintenant activé. Les utilisateurs vont être invités à décider du mode de traitement des pièces jointes à chaque fois qu’ils enverront des emails avec pièces jointes.

   De plus, vous pouvez établir des listes de domaines et indiquer le mode de traitement des pièces jointes lorsqu’elles sont envoyées à ces domaines.

4. Procédez en sélectionnant le mode de traitement des pièces jointes dans la liste déroulante **Méthode de chiffrement pour les domaines autorisés** :
   - **Chiffré** : Tous les fichiers joints sont chiffrés avec la **Clé Synchronized Encryption** quelles que soient leurs extensions et quels que soient leurs état de chiffrement.
   - **Aucun chiffrement** : les pièces jointes des emails envoyés à un domaine spécifié sont chiffrées. Les utilisateurs ne reçoivent aucune demande de confirmation.
   - **Inchangé (Synchronized Encryption)** Tous les fichiers sont chiffrés avec la **Clé Synchronized Encryption**.
   - **Toujours demander** : les utilisateurs sont invités à confirmer le mode de traitement des pièces jointes à chaque fois qu’ils envoient des pièces jointes à un domaine spécifié.

5. Saisissez un ou plusieurs domaines sur lesquels la méthode de chiffrement doit être appliquée. Saisissez plusieurs domaines séparés par des virgules. Les caractères de remplacement et les domaines partiellement spécifiés ne sont pas pris en charge.

6. Lorsque vous quittez l’onglet **Paramètres généraux**, le système vous demande si vous voulez enregistrer vos modifications.

7. Cliquez sur **Oui**.

8. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la nouvelle stratégie à vos groupes d’utilisateurs.

4.2.4 Utilisation de plusieurs stratégies de chiffrement de fichiers par emplacement

Toutes les règles de chiffrement de fichiers assignées par des stratégies et activées pour les utilisateurs/ordinateurs à des nœuds différents dans **Utilisateurs et ordinateurs** dans SafeGuard Management Center sont cumulées.

Vous pouvez assigner une stratégie **Chiffrement de fichiers** au nœud racine qui inclut des règles adaptées à tous les utilisateurs et des stratégies plus spécifiques à des sous-nœuds spécifiques. Toutes les règles de toutes les stratégies assignées à des utilisateurs/ordinateurs sont cumulées et appliquées sur le terminal.

4.2.4.1 Stratégies de chiffrement de fichiers par emplacement dans le RSOP

Si plusieurs stratégies **Chiffrement de fichiers** s'appliquent à un utilisateur ou à un ordinateur, l'onglet **RSOP** (Resulting Set of Policies, série obtenue de stratégies) dans **Utilisateurs et ordinateurs** affiche la somme de toutes les règles de chiffrement de fichiers de toutes les stratégies **Chiffrement de fichiers**. Les règles sont triées dans l'ordre d'évaluation des règles de chiffrement sur le terminal. Retrouvez plus de renseignements à la section Évaluation des règles de chiffrement de fichiers par emplacement sur les terminaux *(page 349)*.

La colonne **Nom de la stratégie** indique d'où les règles individuelles proviennent.

Pour les règles en double, la seconde (et la troisième, etc.) règle est marquée d'une icône. Cette icône fournit aussi une infobulle vous informant que la règle sera ignorée sur le terminal car il s'agit du double d'une règle avec une priorité supérieure.

4.2.5 Évaluation des règles de chiffrement de fichiers par emplacement sur les terminaux

Sur les terminaux, les règles de chiffrement de fichiers sont triées d'une telle façon que les emplacements plus spécifiquement définis sont évalués en premier :

- Si deux règles avec les mêmes paramètres **Chemin** et **Étendue** proviennent de stratégies assignées à des nœuds différents, la règle de la stratégie la plus proche de l'objet utilisateur dans **Utilisateurs et ordinateurs** est appliquée.
- Si deux règles avec les mêmes paramètres **Chemin** et **Étendue** proviennent de stratégies assignées au même nœud, la règle de la stratégie ayant la priorité la plus élevée est appliquée.
- Les règle absolues sont évaluées avant les règles relatives, par exemple c:\encrypt avant encrypt. Retrouvez plus de renseignements à la section Informations supplémentaires sur la configuration des chemins dans les règles de chiffrement de fichiers par emplacement *(page 339)*.

- Les règles avec un chemin contenant plus de sous-répertoires sont évaluées avant celles avec un chemin contenant moins de sous-répertoires.
- Les règles définies avec UNC sont évaluées avant celles avec des informations sur la lettre du lecteur.
- Les règles dont l'option **Ce dossier uniquement** est activée sont évaluées avant celles sans cette option.
- Les règles utilisant le mode **Ignorer** sont évaluées avant celles utilisant le mode **Chiffrer** ou **Exclure**.
- Les règles utilisant le mode **Exclure** sont évaluées avant celles utilisant le mode **Chiffrer** ou Exclure.
- Si deux règles sont identiques en ce qui concerne les critères indiquées, celle qui vient en premier dans l'ordre alphabétique est évaluée avant l'autre.

4.2.6 Conflit entre les règles de chiffrement de fichiers par emplacement

Étant donné que plusieurs stratégies de chiffrement de fichiers peuvent être assignées à un utilisateur ou un ordinateur, des conflits sont possibles. Deux règles sont considérées comme étant en conflit, si elles ont les mêmes valeurs pour le chemin, le mode et le sous-répertoire, mais si la clé à utiliser est différente. Dans ce cas, la règle issue de la stratégie de chiffrement de fichiers ayant la priorité la plus élevée s'applique. L'autre règle est abandonnée.

4.2.7 Chiffrement de fichiers par emplacement et SafeGuard Data Exchange

SafeGuard Data Exchange est utilisé pour chiffrer des données stockées sur des supports amovibles connectés à un ordinateur afin d'échanger ces données avec d'autres utilisateurs. Le chiffrement de fichiers est utilisé pour SafeGuard Data Exchange.

Si SafeGuard Data Exchange et le chiffrement de fichiers par emplacement sont installés sur un terminal, il peut arriver qu'une stratégie de chiffrement SafeGuard Data Exchange soit définie pour un lecteur présent sur l'ordinateur et que les stratégies de chiffrement de fichiers par emplacement soient définies pour des dossiers présents sur le même lecteur. Dans ce cas, la stratégie de chiffrement SafeGuard Data Exchange remplace les stratégies **File Encryption**. Les nouveaux fichiers sont chiffrés en fonction de la stratégie de chiffrement de SafeGuard Data Exchange.

Retrouvez plus de renseignements sur SafeGuard Data Exchange à la section SafeGuard Data Exchange *(page 358)*.

4.3 Stockage Cloud

Le module Stockage Cloud de SafeGuard Enterprise offre le chiffrement de fichiers des données stockées dans le Cloud.

Il ne change pas la façon dont les utilisateurs exploitent les données stockées dans le Cloud. Les utilisateurs se servent des mêmes applications de synchronisation spécifiques aux fournisseurs pour envoyer des données dans le Cloud ou en recevoir depuis celui-ci. Le but du Stockage Cloud est de s'assurer que les copies locales des données stockées dans le Cloud sont chiffrées de manière transparente et qu'elles seront donc toujours stockées dans le Cloud sous une forme chiffrée.

Dans SafeGuard Management Center, créez des **Définitions Stockage Cloud (CSD, Cloud Storage Definitions)** et utilisez-les dans les stratégies **Protection des périphériques**. Les définitions Stockage Cloud prédéfinies de différents fournisseurs de stockage dans le Cloud sont disponibles. Par exemple, Dropbox ou Egnyte.

Après assignation d'une stratégie Stockage Cloud aux terminaux, les fichiers présents dans les emplacements couverts par la stratégie sont chiffrés de manière transparente sans interaction avec l'utilisateur :

- Les fichiers chiffrés seront synchronisés dans le Cloud.
- Les fichiers chiffrés reçus du Cloud peuvent comme d'habitude être modifiés par les applications.

Pour accéder aux fichiers chiffrés Stockage Cloud sur les terminaux sans SafeGuard Enterprise Cloud Storage, SafeGuard Portable peut être utilisé pour lire les fichiers chiffrés.

Remarque : Le Stockage Cloud chiffre uniquement les nouvelles données stockées dans le Cloud. Si les données sont déjà stockées dans le Cloud avant l'installation de Stockage Cloud, ces données ne seront pas automatiquement chiffrées. Si vous voulez chiffrer ces données, veuillez d'abord les supprimer du Cloud et les ajouter de nouveau.

Retrouvez plus de renseignements sur le suivi de fichiers dans le stockage Cloud à la section Audit *(page 225)*.

4.3.1 Conditions requises pour le logiciel de stockage Cloud

Pour activer le chiffrement des données stockées dans le Cloud, le logiciel fourni par le fournisseur de stockage Cloud doit :

- Fonctionner sur l'ordinateur sur lequel le stockage Cloud est installé.
- Avoir une application (ou un service système) stockée dans le système de fichiers local et synchroniser les données entre le Cloud et le système local.

- Stocker les données synchronisées dans le système de fichiers local.

4.3.2 Création de définitions de stockage Cloud

SafeGuard Management Center inclut des définitions de stockage Cloud prédéfinies de différents fournisseurs de stockage dans le Cloud comme, par exemple, Dropbox ou Egnyte. Vous pouvez modifier les chemins des définitions de stockage Cloud prédéfinies selon vos besoins ou créer une nouvelle définition à partir des valeurs prédéfinies. Ceci s'avère particulièrement utile, par exemple, si vous souhaitez uniquement chiffrer une partie des données de votre stockage dans le Cloud. Vous pouvez également créer vos propres définitions de stockage Cloud.

Remarque : Lorsqu'ils sont chiffrés, certains dossiers (par exemple, le dossier d'installation Dropbox) peut empêcher l'exécution du système d'exploitation ou d'applications. Lorsque vous créez des définitions de stockage Cloud pour les stratégies de **Protection des périphériques**, assurez-vous que ces dossiers ne sont pas chiffrés.

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Définitions de stockage Cloud**.
2. Sélectionnez **Nouveau > Définition de stockage Cloud**.
3. La boîte de dialogue **Nouvelle définition de stockage Cloud** apparaît. Saisissez un nom de définition de stockage Cloud.
4. Cliquez sur **OK**. La définition de stockage Cloud apparaît avec le nom saisi sous le nœud racine **Définitions de stockage Cloud** dans la zone de navigation **Stratégies**.
5. Sélectionnez la définition de stockage Cloud. Dans la zone de travail à droite, le contenu d'une définition de stockage Cloud apparaît :

   - **Nom de la cible :**

     Il s'agit du nom que vous avez saisi initialement. Il sert à référencer la définition de stockage Cloud comme cible dans une stratégie de type **Protection des périphériques**.

   - **Application de synchronisation :**

     Saisissez le chemin et l'application qui synchronise les données avec le Cloud (par exemple : <Bureau>\dropbox\dropbox.exe). L'application doit résider sur un lecteur local.

   - **Dossiers de synchronisation :**

     Saisissez le ou les dossiers qui seront synchronisés avec le Cloud. Seuls les chemins locaux sont pris en charge.

     Remarque : Pour les chemins dans les paramètres **Application de synchronisation** et **Dossiers de synchronisation**, les mêmes espaces réservés que ceux utilisés pour le

Chiffrement de fichiers sont pris en charge comme indiqué à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.

4.3.2.1 Espaces réservés pour les fournisseurs de stockage dans le Cloud

En tant que responsable de la sécurité, vous pouvez utiliser des espaces réservés pour les fournisseurs du stockage dans le Cloud afin de définir des applications de synchronisation et des dossiers de synchronisation. Ces espaces réservés représentent les applications tierces de stockage dans le Cloud prises en charge. Vous pouvez utiliser l'espace réservé pour spécifier une certaine application tierce comme application de synchronisation et même utiliser le même espace réservé pour qu'il pointe vers les dossiers de synchronisation que l'application tierce utilise véritablement pour la synchronisation.

Les espaces réservés pour les fournisseurs de stockage dans le Cloud sont encapsulés par `<!` et `!>`.

Fournisseur	Espace réservé	Utilisable dans le paramètre CSD	Résultat
Box	**`<!Box!>`**	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Box. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisée par le logiciel Box.
Dropbox	**`<!Dropbox!>`**	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Dropbox. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de

Fournisseur	Espace réservé	Utilisable dans le paramètre CSD	Résultat
			synchronisation utilisé par le logiciel Dropbox.
Egnyte **Windows** uniquement	**<!Egnyte!>**	**Application de synchronisation**	Le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Egnyte.
	<!EgnytePrivate!>	**Dossiers de synchronisation**	Tous les dossiers confidentiels du stockage Cloud d'Egnyte. Pour les utilisateurs Egnyte classiques, il s'agit généralement d'un seul dossier. Pour les administrateurs Egnyte, cet espace réservé consiste généralement en plusieurs dossiers.
	<!EgnyteShared!>	**Dossiers de synchronisation**	Tous les dossiers partagés du stockage Cloud d'Egnyte.
	Remarque : Les modifications de la structure du dossier Egnyte (y compris, l'ajout ou la suppression de dossiers confidentiels ou partagés) sont détectées automatiquement. Les stratégies affectées sont mises à jour automatiquement.		
	Remarque : Les dossiers de synchronisation peuvent se trouver sur des emplacements du réseau. Vous pouvez donc saisir les chemins réseau dans le paramètre **Dossiers de synchronisation**. Le module Stockage Cloud de SafeGuard Enterprise se connecte donc par défaut aux systèmes de fichiers réseau. Si cette opération n'est pas nécessaire, vous pouvez désactiver ce comportement en définissant une stratégie **Paramètres généraux** et en sélectionnant **Réseau** sous **Périphériques ignorés**.		
Google Drive	**<!GoogleDrive!>**	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Google Drive. Pour les dossiers de synchronisation : Le

Fournisseur	Espace réservé	Utilisable dans le paramètre CSD	Résultat
			chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel Google Drive.
OneDrive	`<!OneDrive!>`	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel OneDrive. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel OneDrive.
	Remarque : SafeGuard Enterprise ne prend pas en charge les comptes Microsoft. Sous Windows 8.1, OneDrive peut uniquement être utilisé si l'utilisateur Windows est un utilisateur de domaine. Sous Windows 8.1, SafeGuard Enterprise ne prend pas en charge OneDrive pour les utilisateurs locaux.		
OneDrive Entreprise	`<!OneDriveForBusiness!>`	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel OneDrive. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel OneDrive.
	Remarque : OneDrive Entreprise prend uniquement en charge le stockage des fichiers chiffrés dans les dossiers locaux et leur synchronisation dans le Cloud. Le stockage des fichiers chiffrés à partir des applications Microsoft Office 2013 directement dans le Cloud OneDrive Entreprise ou sur le serveur SharePoint n'est pas pris en charge. Ces fichiers ne sont pas chiffrés et sont stockés dans le Cloud.		

Fournisseur	Espace réservé	Utilisable dans le paramètre CSD	Résultat
	Les fichiers chiffrés par SafeGuard Enterprise dans le Cloud OneDrive Entreprise ne peuvent pas être ouverts par Microsoft Office 365.		
SkyDrive **Windows** uniquement	**`<!SkyDrive!>`**	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel OneDrive. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel OneDrive.
	Microsoft a changé le nom de SkyDrive pour OneDrive. Cependant, l'espace réservé **`<!SkyDrive!>`** est toujours disponible. De cette manière, les anciennes stratégies utilisant cet espace réservé et les terminaux utilisant une version de SafeGuard Enterprise antérieure à la version 7 ne pouvant pas gérer l'espace réservé **`<!OneDrive!>`** peuvent continuer à être utilisé sans qu'aucun changement ne soit nécessaire. Les terminaux utilisant la version 7 de SafeGuard Enterprise peuvent gérer les deux espaces réservés.		

Exemple

Si vous utilisez Dropbox comme fournisseur de stockage dans le Cloud, vous pouvez simplement saisir **`<!Dropbox!>`** dans **Application de synchronisation**. Si vous n'indiquez pas explicitement de dossier de synchronisation, **`<!Dropbox!>`** est aussi copié dans la liste des dossiers sous **Dossiers de synchronisation**.

En supposant que

- Vous avez utilisé les espaces réservés `<!Dropbox!>` comme application de synchronisation et `<!Dropbox!>\encrypt` comme dossier de synchronisation dans la définition de stockage Cloud (DSC).
- Dropbox est installé sur le terminal.
- L'utilisateur dispose de `d:\dropbox` configuré en tant que dossier à synchroniser avec Dropbox :

Lorsque le terminal SafeGuard Enterprise reçoit une stratégie avec une DSC comme celle-ci, il interprète automatiquement les espaces réservés de la DSC pour qu'ils s'accordent avec le chemin de Dropbox.exe pour l'application de synchronisation, puis il lit la configuration Dropbox et définit la stratégie de chiffrement dans le dossier `d:\dropbox\encrypt`.

4.3.2.2 Exportation et importation des définitions Stockage Cloud

En tant que responsable de la sécurité, vous pouvez exporter et importer des définitions Stockage Cloud (CSD, Cloud Storage Definitions). Une CSD sera exportée sous la forme d'un fichier XML.

- Pour exporter une CSD, cliquez sur **Exporter une définition de Stockage Cloud...** dans le menu contextuel de la définition Stockage Cloud désirée dans la zone **Stratégie**.
- Pour importer une CSD, cliquez sur **Importer une définition Stockage Cloud...** dans le menu contextuel du nœud de la définition Stockage Cloud dans la zone **Stratégie**.

Les deux commandes sont également disponibles dans le menu **Actions** de SafeGuard Management Center.

4.3.3 Création d'une stratégie de protection des périphériques avec une définition Stockage Cloud

Des définitions Stockage Cloud doivent avoir été créées auparavant. Les définitions Stockage Cloud prédéfinies de différents fournisseurs de stockage dans le Cloud sont disponibles. Par exemple, Dropbox ou Egnyte.

Vous définissez les paramètres pour chiffrer les données de stockage dans le Cloud dans une stratégie du type **Protection des périphériques**.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Protection des périphériques**.
2. Sélectionnez une définition Stockage Cloud comme cible.
3. Cliquez sur **OK**. La nouvelle stratégie s'affiche dans la fenêtre de navigation sous **Éléments de stratégie**. Dans la zone d'action, tous les paramètres de la stratégie **Protection du périphérique** s'affichent et peuvent être changés.
4. Pour le **Mode de chiffrement du support**, sélectionnez **Basé sur fichier**. Le chiffrement basé sur volume n'est pas pris en charge.

5. Sous **Algorithme à utiliser pour le chiffrement**, sélectionnez l'algorithme à utiliser pour le chiffrement des données dans les dossiers de synchronisation définis dans la CSD.

6. Les paramètres **Clé à utiliser pour le chiffrement** et **Clé définie pour le chiffrement** servent à définir la clé ou les clés qui seront utilisées pour le chiffrement. Retrouvez plus de renseignements à la section Protection des périphériques *(page 286)*.

7. Si vous activez le paramètre **Copier SG Portable sur la cible**, SafeGuard Portable est copié dans chaque dossier de synchronisation à chaque fois que du contenu est écrit. SafeGuard Portable est une application qui peut être utilisée pour lire les fichiers chiffrés sur les ordinateurs Windows sur lesquels SafeGuard Enterprise n'est pas installé.

   Remarque : Pour partager les données chiffrées conservées dans le Cloud avec les utilisateurs ne disposant pas de SafeGuard Enterprise, les utilisateurs doivent être autorisés à créer des clés locales comme indiqué à la section Clés locales *(page 365)*.

8. Le paramètre **Dossier en texte brut** vous permet de définir un dossier qui sera exclu du chiffrement. Les données stockées dans les sous-dossiers du dossier en texte brut défini seront également exclues du chiffrement. SafeGuard Cloud Storage crée automatiquement des dossiers en texte brut vides dans tous les dossiers de synchronisation définis dans la **Définition de Cloud Storage**.

4.4 SafeGuard Data Exchange

SafeGuard Data Exchange est utilisé pour chiffrer des données stockées sur des supports amovibles connectés à un ordinateur afin d'échanger ces données avec d'autres utilisateurs. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une intervention minimale de l'utilisateur.

Seuls les utilisateurs disposant des clés appropriées peuvent lire le contenu des données chiffrées. Tout processus de chiffrement ultérieur est exécuté de manière transparente.

Dans le cadre d'une administration centralisée, vous définissez la gestion des données de supports amovibles.

En tant que responsable de la sécurité, vous définissez les paramètres spécifiques dans une stratégie du type **Protection des périphériques** avec **Supports amovibles** comme **Cible de protection de périphérique**.

Pour SafeGuard Data Exchange, le chiffrement **basé sur fichier** doit être utilisé comme **Mode de chiffrement des supports**.

Retrouvez plus de renseignements sur le suivi de l’accès des fichiers sur des supports amovibles à la section Audit *(page 225)*.

4.4.1 Bon usage

Cette section décrit des études de cas classiques de SafeGuard Data Exchange et comment les mettre en œuvre en créant les stratégies appropriées.

Bob et Alice sont deux employés de la même société et disposent de SafeGuard Data Exchange. Joe est un partenaire externe et ne dispose pas de SafeGuard Enterprise sur son ordinateur.

4.4.1.1 Utilisation interne uniquement

Bob souhaite partager des données chiffrées sur un support amovible avec Alice. Ils font partie du même groupe et disposent donc de la clé de groupe appropriée dans leur jeu de clés SafeGuard Enterprise. Étant donné qu’ils utilisent la même clé de groupe, ils peuvent accéder en toute transparence aux fichiers chiffrés sans saisir de phrase secrète.

Vous devez définir les paramètres dans une stratégie du type **Protection des périphériques** > **Supports amovibles** :

- **Mode de chiffrement des supports : Basé sur fichier**
- **Clé à utiliser pour le chiffrement : Clé définie dans la liste**
  - Clé définie dans la liste : <clé de groupe/domaine > (par exemple, groupe_utilisateurs_Bob_Alice@DC=...) pour s’assurer qu’ils partagent la même clé

Si les stratégies de l’entreprise stipulent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers : Oui**

  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.

- **L’utilisateur peut annuler le chiffrement initial : Non**

  L’utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.

- **L’utilisateur est autorisé à accéder aux fichiers non chiffrés : Non**

Si des fichiers au format brut sont détectés sur les supports amovible, leur accès est refusé.

- **L’utilisateur peut déchiffrer des fichiers : Non**

  L’utilisateur n’est pas autorisé à déchiffrer des fichiers de supports amovibles.

- **Copier SG Portable sur la cible : Non**

  SafeGuard Portable n’est pas nécessaire tant que les données de supports amovibles sont partagées dans un groupe de travail. SafeGuard Portable permet également d’autoriser le déchiffrement de fichiers sur des ordinateurs sur lesquels SafeGuard Enterprise n’est pas installé.

Les utilisateurs peuvent partager des données en échangeant simplement leurs périphériques. Lorsqu’ils connectent les périphériques à leurs ordinateurs, ils accèdent en toute transparence aux fichiers chiffrés.

Remarque : Cette étude de cas est possible grâce à la fonction de chiffrement de périphérique de SafeGuard Enterprise permettant de chiffrer tous les supports amovibles par secteur.

4.4.1.2 Utilisation à domicile ou personnelle sur des ordinateurs tiers

- **À domicile :**

  Bob souhaite utiliser son support amovible chiffré sur son ordinateur personnel, sur lequel SafeGuard Enterprise n’est pas installé. Sur son ordinateur personnel, Bob déchiffre les fichiers avec SafeGuard Portable. En définissant une phrase secrète des supports pour tous les supports amovibles de Bob, il ouvre simplement SafeGuard Portable et saisit la phrase secrète du support. Il a ensuite accès de manière transparente à tous les fichiers chiffrés, quelle que soit la clé locale utilisée pour les chiffrer.

- **Utilisation personnelle sur des ordinateurs tiers :**

  Bob connecte le support amovible à l’ordinateur de Joe (partenaire externe) et saisit la phrase secrète des supports pour accéder aux fichiers chiffrés stockés sur le périphérique. Bob peut alors copier les fichiers (chiffrés ou non) sur l’ordinateur de Joe.

Comportement sur le terminal :

- Bob connecte pour la première fois le support amovible.

- La clé de chiffrement de support, unique à chaque périphérique, est créée automatiquement.
- Bob est invité à saisir la phrase secrète des supports pour l'utiliser hors ligne via SafeGuard Portable.
- L'utilisateur n'a pas besoin de connaître les clés utilisées ou le jeu de clés. La clé de chiffrement de support est toujours utilisée pour le chiffrement de données sans aucune interaction de l'utilisateur. La clé de chiffrement de support n'est pas visible, y compris pour l'utilisateur. Seule la clé de groupe/domaine définie de manière centralisée est visible.
- Bob et Alice, du même groupe ou domaine, accèdent de manière transparente car ils partagent la même clé de groupe/domaine.
- Si Bob souhaite accéder à des fichiers chiffrés d'un support amovible sur un ordinateur sur lequel SafeGuard Data Exchange n'est pas installé, il peut utiliser la phrase secrète des supports dans SafeGuard Portable.

Vous devez définir les paramètres dans une stratégie du type **Protection des périphériques > Supports amovibles** :

- **Mode de chiffrement des supports : Basé sur fichier**
- **Clé à utiliser pour le chiffrement : Clé définie dans la liste**
  - Clé définie dans la liste : <clé de groupe/domaine > (par exemple, groupe_utilisateurs_Bob_Alice@DC=...) pour s'assurer qu'ils partagent la même clé
- **L'utilisateur peut définir une phrase secrète des supports pour les périphériques : Oui**

  L'utilisateur définit une phrase secrète des supports sur son ordinateur qui s'applique à tous les supports amovibles.
- **Copier SG Portable sur la cible : Oui**

  SafeGuard Portable permet à l'utilisateur d'accéder à tous les fichiers chiffrés du support amovible en saisissant une phrase secrète des supports unique sur un système sur lequel SafeGuard Data Exchange n'est pas installé.

Si les stratégies de l'entreprise définissent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers : Oui**

  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.

- **L’utilisateur peut annuler le chiffrement initial : Non**

  L’utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.

- **L’utilisateur est autorisé à accéder aux fichiers non chiffrés : Non**

  Si des fichiers au format brut sont détectés sur les supports amovible, leur accès est refusé.

- **L’utilisateur peut déchiffrer des fichiers : Non**

  L’utilisateur n’est pas autorisé à déchiffrer des fichiers de supports amovibles.

Au bureau, Bob et Alice accèdent de manière transparente aux fichiers chiffrés du support amovible. À domicile ou sur les ordinateurs tiers, ils peuvent utiliser SafeGuard Portable pour ouvrir des fichiers chiffrés. Les utilisateurs saisissent seulement la phrase secrète des supports et peuvent accéder à tous les fichiers chiffrés. Cette méthode simple mais fiable permet de chiffrer des données sur tous les supports amovibles. Cette configuration vise à réduire au maximum l’interaction de l’utilisateur tout en chiffrant chaque fichier d’un support amovible et en permettant aux utilisateurs d’accéder hors ligne aux fichiers chiffrés. L’utilisateur n’est pas autorisé à déchiffrer des fichiers de supports amovibles.

Remarque : Dans cette configuration, les utilisateurs ne sont pas autorisés à créer des clés locales car elles sont inutiles dans ce cas de figure. Ceci doit être indiqué dans une stratégie de type **Protection des périphériques > Périphériques de stockage locaux** (**Paramètres généraux > L’utilisateur est autorisé à créer une clé locale > Non**).

- **Copier SG Portable vers support amovible : Non.**

  SafeGuard Portable n’est pas nécessaire tant que les données de supports amovibles sont partagées dans un groupe de travail. SafeGuard Portable permet également d’autoriser le déchiffrement de fichiers sur des ordinateurs sur lesquels SafeGuard Enterprise n’est pas installé.

Au bureau, l’utilisateur accède de manière transparente aux fichiers chiffrés d’un support amovible. À son domicile, il utilise SafeGuard Portable pour ouvrir des fichiers chiffrés. L’utilisateur saisit simplement la phrase secrète des supports et accède à tous les fichiers chiffrés, quelle que soit la clé de chiffrement utilisée.

4.4.1.3 Partage d’un support amovible avec un tiers externe

Remarque : Cet exemple s’applique uniquement aux terminaux Windows.

Bob souhaite partager un périphérique chiffré avec Joe (tiers externe) qui ne dispose pas de SafeGuard Data Exchange et qui doit donc utiliser SafeGuard Portable. Si on suppose que Bob ne souhaite pas que Joe accède à tous les fichiers chiffrés du support amovible, il peut créer une clé locale et chiffrer les fichiers avec cette clé. Joe peut alors utiliser SafeGuard Portable et ouvrir les fichiers chiffrés à l’aide de la phrase secrète de la clé locale et Bob peut toujours utiliser la phrase secrète des supports pour accéder aux fichiers chiffrés du support amovible.

Comportement sur l’ordinateur

- Bob connecte pour la première fois le support amovible. La clé de chiffrement de support, unique à chaque périphérique, est créée automatiquement.
- Bob est invité à saisir la phrase secrète des supports pour l’utiliser hors ligne.
- La clé de chiffrement de support est utilisée pour le chiffrement de données sans aucune intervention de l’utilisateur, mais...
- Bob peut maintenant créer ou sélectionner une clé locale (par exemple, JoeClé) pour chiffrer des fichiers spécifiques à échanger avec Joe.
- Bob et Alice, du même groupe ou domaine, accèdent de manière transparente car ils partagent la même clé de groupe/domaine.
- Si Bob souhaite accéder à des fichiers chiffrés d’un support amovible sur un ordinateur sur lequel SafeGuard Data Exchange n’est pas installé, il peut utiliser la phrase secrète des supports dans SafeGuard Portable.
- Joe peut accéder aux fichiers spécifiques en saisissant la phrase secrète de la clé (JoeClé) sans accéder à l’ensemble des fichiers du support amovible.

Vous devez définir les paramètres dans une stratégie du type **Protection des périphériques** > **Supports amovibles** :

- **Mode de chiffrement des supports : Basé sur fichier**
- **Clé à utiliser pour le chiffrement : Toute clé du jeu de clés utilisateur**

Permet à l’utilisateur de choisir différentes clés pour chiffrer des fichiers de son support amovible.

- **Clé définie pour le chiffrement :** <clé de groupe/domaine> (par exemple groupe_utilisateurs_Bob_Alice@DC=...) L’utilisateur peut partager des données dans son groupe de travail et permettre à un autre utilisateur d’accéder de manière transparente au support amovible lorsqu’il le connecte à son ordinateur professionnel.

- **L’utilisateur peut définir une phrase secrète des supports pour les périphériques : Oui**

  L’utilisateur définit une phrase secrète des supports sur son ordinateur qui s’applique à tous les supports amovibles.

- **Copier SG Portable sur la cible : Oui**

  SafeGuard Portable permet à l’utilisateur d’accéder à tous les fichiers chiffrés du support amovible en saisissant une phrase secrète des supports unique sur un système sur lequel SafeGuard Data Exchange n’est pas installé.

Si les stratégies de l’entreprise définissent également que tous les fichiers des supports amovibles doivent toujours être chiffrés, ajoutez les paramètres suivants :

- **Chiffrement initial de tous les fichiers : Oui**

  Vérifie que les fichiers des supports amovibles sont chiffrés lors de la première connexion du support au système.

- **L’utilisateur peut annuler le chiffrement initial : Non**

  L’utilisateur ne peut pas annuler le chiffrement initial, pour le différer par exemple.

- **L’utilisateur est autorisé à accéder aux fichiers non chiffrés : Non**

  Si des fichiers au format brut sont détectés sur les supports amovible, leur accès est refusé.

- **L’utilisateur peut déchiffrer des fichiers : Non**

  L’utilisateur n’est pas autorisé à déchiffrer des fichiers de supports amovibles.

Au bureau, Bob et Alice accèdent de manière transparente aux fichiers chiffrés du support amovible. À leur domicile, ils peuvent utiliser SafeGuard Portable pour ouvrir des fichiers chiffrés en saisissant la phrase secrète des supports. Si Bob ou Alice souhaite partager le support amovible sur un ordinateur tiers sur lequel SafeGuard Data Exchange n’est pas installé, ils peuvent utiliser des clés locales pour s’assurer que le tiers externe n’accède qu’à certains fichiers. Cette configuration avancée

implique une interaction plus importante de l’utilisateur en l’autorisant à créer des clés locales sur son ordinateur.

Remarque : Pour ce faire, l’utilisateur doit au préalable être autorisé à créer des clés locales (paramètre par défaut dans SafeGuard Enterprise).

4.4.2 Clés de groupe

Pour échanger des données chiffrées entre utilisateurs, des clés de groupe SafeGuard Enterprise doivent être utilisées. Si la clé de groupe se trouve dans les jeux de clés des utilisateurs, ces derniers peuvent accéder en toute transparence aux supports amovibles connectés à leurs ordinateurs.

Sur les ordinateurs sur lesquels SafeGuard Enterprise n'est pas installé, il est impossible d'accéder aux données chiffrées de supports amovibles, à l'exception de la clé de domaine/groupe définie de manière centralisée qui peut être utilisée avec la phrase secrète des supports.

Remarque : SafeGuard Portable peut être utilisé pour utiliser/partager des données chiffrées de supports amovibles sur/avec des ordinateurs/utilisateurs ne disposant pas de SafeGuard Enterprise. SafeGuard Portable nécessite l'utilisation de clés locales ou d'une phrase secrète des supports.

4.4.3 Clés locales

SafeGuard Data Exchange prend en charge le chiffrement à l’aide de clés locales. Des clés locales sont créées sur les ordinateurs et peuvent être utilisées pour chiffrer des données de supports amovibles. Elles sont créées en saisissant une phrase secrète et sauvegardées dans la base de données de SafeGuard Enterprise.

Remarque : Par défaut, l’utilisateur est autorisé à créer des clés locales. Si des utilisateurs n’y sont pas autorisés, vous devez désactiver cette option de manière explicite. Ceci doit être effectué dans une stratégie de type **Protection des périphériques** avec **Périphériques de stockage locaux** comme **Cible de protection de périphérique** (**Paramètres généraux > L’utilisateur est autorisé à créer une clé locale > Non**).

Si des clés locales sont utilisées pour chiffrer des fichiers sur des supports amovibles, ces fichiers peuvent être déchiffrés à l’aide de SafeGuard Portable sur un ordinateur sur lequel SafeGuard Data Exchange n’est pas installé. À l’ouverture des fichiers avec SafeGuard Portable, l’utilisateur est invité à saisir la phrase secrète spécifiée lors de la création de la clé. L’utilisateur peut ouvrir le fichier s’il connaît la phrase secrète.

Grâce à SafeGuard Portable, chaque utilisateur connaissant la phrase secrète peut accéder à un fichier chiffré sur un support amovible. Il est ainsi également possible de partager des données chiffrées avec des partenaires ne disposant pas de SafeGuard Enterprise. SafeGuard Portable et la phrase secrète des fichiers auxquels ils doivent accéder doivent leur être fournis.

Si différentes clés locales sont utilisées pour chiffrer des fichiers de supports amovibles, vous pouvez également restreindre l'accès aux fichiers. Par exemple : vous chiffrez les fichiers présents sur une carte mémoire USB à l'aide d'une clé avec la phrase secrète *ma_clélocale* et chiffrez un fichier nommé *PourMonPartenaire.doc* à l'aide de la phrase secrète *partenaire_clélocale*. Si vous confiez la carte mémoire USB à un partenaire et fournissez la phrase secrète *partenaire_clélocale* à ce dernier, il aura uniquement accès au fichier *PourMonPartenairedoc*.

Remarque : Par défaut, SafeGuard Portable est copié automatiquement sur les supports amovibles connectés au système dès l'écriture de contenu sur les supports couverts par une règle de chiffrement. Si vous ne souhaitez pas que SafeGuard Portable soit copié sur les supports amovibles, désactivez l'option **Copier SG Portable sur la cible** dans une stratégie du type **Chiffrement de périphériques**.

4.4.4 Phrase secrète des supports

SafeGuard Data Exchange vous permet de spécifier qu'une seule phrase secrète des supports pour tous les supports amovibles (sauf les supports optiques) doit être créée sur les terminaux. La phrase secrète des supports permet d'accéder à la clé de domaine/groupe définie de manière centralisée et à toutes les clés locales utilisées dans SafeGuard Portable. L'utilisateur ne saisit qu'une seule phrase secrète et peut accéder à tous les fichiers chiffrés dans SafeGuard Portable, quelle que soit la clé locale utilisée pour le chiffrement.

Sur chaque terminal et pour chaque périphérique, une clé de chiffrement de support unique pour le chiffrement de données est créée automatiquement. Cette clé est protégée par la phrase secrète des supports et une clé de domaine/groupe définie de manière centralisée. Sur un ordinateur sur lequel SafeGuard Data Exchange est installé, il n'est donc pas nécessaire de saisir la phrase secrète des supports pour accéder aux fichiers chiffrés contenus sur le support amovible. L'accès est accordé automatiquement si la clé appropriée se trouve dans le jeu de clés de l'utilisateur.

La clé de domaine/groupe à utiliser doit être spécifiée sous **Clé définie pour le chiffrement**.

La fonction de phrase secrète des supports est disponible lorsque l'option **L'utilisateur peut définir une phrase secrète des supports pour les périphériques** est activée dans une stratégie de type **Protection des périphériques**.

Lorsque ce paramètre est activé sur l'ordinateur, l'utilisateur est invité automatiquement à saisir une phrase secrète des supports lorsqu'il connecte des supports amovibles pour la première fois. La phrase secrète des supports est valide sur chaque terminal Windows auquel l'utilisateur peut se connecter. L'utilisateur peut également changer la phrase secrète des supports. La synchronisation est alors automatique lorsque la phrase secrète reconnue sur l'ordinateur et la phrase secrète des supports amovibles ne correspondent pas.

En cas d'oubli de la phrase secrète des supports l'utilisateur peut la récupérer sans recourir au support.

Remarque :

Pour activer la phrase secrète des supports, activez l'option **L'utilisateur peut définir une phrase secrète des supports pour les périphériques** dans une stratégie de type **Chiffrement de périphérique**. Cette option n'est disponible que si vous avez sélectionné **Supports amovibles** comme **Cible de protection de périphérique**.

Sur les Macs la phrase secrète des supports n'est pas prise en charge.

4.4.4.1 Phrase secrète des supports et terminaux non administrés

Sur un terminal non administré, autrement dit un ordinateur fonctionnant en mode autonome, sur lequel la fonction de phrase secrète des supports est désactivée, aucune clé n'est disponible une fois l'installation terminée, car les terminaux non administrés utilisent des clés locales uniquement. Avant de pouvoir utiliser le chiffrement, l'utilisateur doit créer une clé.

Si la fonction de phrase secrète des supports est activée dans une stratégie de support amovible pour ces ordinateurs, la clé de chiffrement de support est créée automatiquement sur l'ordinateur client et peut être utilisée pour un chiffrement immédiatement après l'installation. Il s'agit d'une clé prédéfinie du jeu de clés de l'utilisateur qui s'affiche sous la forme d'un <nom utilisateur> dans les boîtes de dialogue de sélection de clé.

Le cas échéant, les clés de chiffrement de support sont également utilisées pour toutes les tâches de chiffrement initial.

4.4.5 Configuration des applications fiables et ignorées pour SafeGuard Data Exchange

Vous pouvez définir des applications comme sécurisées pour leur accorder l'accès aux fichiers chiffrés. Ceci s'avère utile, par exemple, pour activer le logiciel antivirus afin de contrôler les fichiers chiffrés.

Vous pouvez définir des applications comme ignorées pour les exempter du chiffrement/déchiffrement transparent des fichiers. Par exemple, si vous définissez un programme de sauvegarde comme une application ignorée, les données chiffrées sauvegardées par le programme restent chiffrées.

Remarque : Les processus enfants ne seront pas fiables/ignorés.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.

2. Sous **Chiffrement de fichiers**, cliquez sur la liste déroulante du champ **Applications sécurisées** ou **Application ignorées**.

3. Dans la zone de liste de l'éditeur, saisissez les applications à définir comme sécurisées/ignorées.
   - Vous pouvez définir plusieurs applications sécurisées/ignorées dans une stratégie. Chaque ligne de la zone de liste de l'éditeur définir une application.
   - Les noms des applications doivent se terminer par .exe.
   - Les noms des applications doivent être spécifiés comme des chemins pleinement qualifiés avec informations sur le lecteur/répertoire. La saisie d'un nom de fichier seulement (par exemple, « exemple.exe ») n'est pas suffisante. Pour une meilleure utilisation, la vue sur une ligne de la liste des applications n'affiche que les noms de fichiers séparés par des points-virgules.

4. Enregistrez vos modifications.

Remarque : Les paramètres de stratégie **Applications sécurisées** et **Applications ignorées** sont les paramètres de la machine. La stratégie doit donc être assignée aux machines, pas aux utilisateurs. Sinon, les paramètres ne deviennent pas actifs.

4.4.6 Configuration des périphériques ignorés pour SafeGuard Data Exchange

Vous pouvez définir des périphériques comme ignorés pour les exclure du processus de chiffrement des fichiers. Vous pouvez seulement exclure des périphériques entiers.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.

2. Sous **Chiffrement de fichiers**, cliquez sur la liste déroulante du champ **Périphériques ignorés**.

3. Dans la zone de liste de l'éditeur, saisissez les noms de périphériques requis pour exclure des périphériques donnés du chiffrement. Ceci peut être utile lorsque vous avez besoin d'exclure les systèmes des fournisseurs tiers.

   Remarque : Vous pouvez afficher les noms des appareils actuellement utilisés dans le système à l'aide du programme de contrôle Fltmc.exe (fltmc volumes, fltmc instances) à partir de Microsoft. Retrouvez plus de renseignements à la section https://docs.microsoft.com/fr-fr/windows-hardware/drivers/ifs/development-and-testing-tools.

4.4.7 Configuration du chiffrement permanent pour SafeGuard Data Exchange

Avec le chiffrement permanent, les copies des fichiers chiffrés seront chiffrées, même lorsqu'elles sont enregistrées dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement.

Vous pouvez configurer le chiffrement permanent dans des stratégies du type **Paramètres généraux**. Le paramètre de stratégie **Activer le chiffrement permanent** est activé par défaut.

Lorsqu'un utilisateur enregistre un fichier chiffré avec **Enregistrer sous** sous un nom de fichier différent dans un emplacement non couvert par une règle de chiffrement, le fichier sera en texte brut.

Le paramètre **Activer le chiffrement permanent** n'a aucun effet si les fichiers sont copiés ou déplacés sur un appareil ou un emplacement ignoré. Vous définissez les emplacements ignorés dans une stratégie de type **Chiffrement de fichiers > Par emplacement > Mode > Ignorer**.

4.4.8 SafeGuard Data Exchange et File Encryption

Le module File Encryption de SafeGuard Enterprise permet un chiffrement basé sur fichier sur les emplacements réseau, surtout pour les groupes de travail et les partages réseau.

Si SafeGuard Data Exchange et SafeGuard File Encryption sont installés sur un terminal, il peut arriver qu'une stratégie de chiffrement SafeGuard Data Exchange soit définie pour un lecteur présent sur l'ordinateur et que les stratégies de chiffrement de fichiers soient définies pour des dossiers présents sur le même lecteur. Dans ce cas, la stratégie de chiffrement SafeGuard Data Exchange remplace les stratégies File Encryption. Les nouveaux fichiers sont chiffrés en fonction de la stratégie de chiffrement de SafeGuard Data Exchange.

Retrouvez plus de renseignements à la section Chiffrement de fichiers par emplacement *(page 336)*.

4.5 SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique

Les disques durs à chiffrement automatique offrent un chiffrement de type matériel des données lorsqu'ils sont écrits sur le disque dur. Trusted Computing Group (TCG) a publié la norme Opal indépendante des fournisseurs pour les disques durs à chiffrement automatique. Différents fournisseurs de matériels proposent des disques durs compatibles Opal. SafeGuard Enterprise prend en charge la norme Opal et permet la gestion des terminaux avec disques durs compatibles Opal

à chiffrement automatique. Retrouvez plus de renseignements dans l'article 113366 de la base de connaissances de Sophos.

4.5.1 Comment SafeGuard Enterprise intègre-t-il les disques durs compatibles Opal ?

SafeGuard Enterprise permet de gérer les terminaux avec disques durs compatibles Opal à chiffrement automatique depuis SafeGuard Management Center, comme tout autre terminal protégé par SafeGuard Enterprise.

La gestion centralisée et pleinement transparente des disques durs compatibles Opal par SafeGuard Enterprise permet l'utilisation d'environnements informatiques hétérogènes. En prenant en charge la norme Opal, nous offrons la série complète des fonctions SafeGuard Enterprise aux utilisateurs professionnels des disques durs compatibles Opal à chiffrement automatique. Associé à SafeGuard Enterprise, les disques durs compatibles Opal offrent des fonctions de sécurité renforcées.

4.5.2 Amélioration des disques durs compatibles Opal avec SafeGuard Enterprise

En combinaison avec les disques durs compatibles Opal à chiffrement automatique, SafeGuard Enterprise offre les avantages suivants :

- Administration centralisée des terminaux
- Authentification au démarrage SafeGuard avec interface graphique utilisateur
- Prise en charge multi-utilisateurs
- Prise en charge de la connexion par token/carte à puce
- Prise en charge de la connexion par empreintes digitales
- Récupération (Local Self Help, Challenge/Réponse)
- Audit centralisé
- Chiffrement des supports amovibles (par exemple, les clés de mémoire USB) avec SafeGuard Data Exchange

4.5.3 Administration avec SafeGuard Enterprise des terminaux équipés de disques durs compatibles Opal

Dans SafeGuard Management Center, vous pouvez administrer les terminaux équipés de disques durs compatibles Opal à chiffrement automatique comme tout autre poste protégé par SafeGuard Enterprise. En tant que responsable de la sécurité, vous pouvez définir des stratégies de sécurité, par exemple des stratégies d'authentification, et les déployer sur les terminaux.

Une fois qu'un terminal équipé d'un disque dur compatible Opal est enregistré dans SafeGuard Enterprise, des informations concernant l'utilisateur, l'ordinateur, le mode de connexion et l'état du chiffrement sont affichées. En outre, les événements sont consignés dans le journal.

Dans SafeGuard Enterprise, l'administration des terminaux équipés de disques durs compatibles Opal est transparente, ce qui signifie que les fonctions d'administration en général fonctionnent de la même façon que pour les autres terminaux protégés par SafeGuard Enterprise. Le type d'un ordinateur apparaît dans l'**Inventaire** d'un conteneur dans **Utilisateurs et ordinateurs**. La colonne **Type de POA** vous indique si l'ordinateur correspondant est chiffré par SafeGuard Enterprise ou utilise un disque dur compatible Opal à chiffrement automatique.

4.5.4 Chiffrement de disques durs compatibles Opal

Les disques durs compatibles Opal sont à chiffrement automatique. Les données sont chiffrées automatiquement lorsqu'elles sont écrites sur le disque dur.

Les disques durs sont verrouillés par une clé AES 128/256 utilisée comme mot de passe Opal. Ce mot de passe est géré par SafeGuard Enterprise via une stratégie de chiffrement. Reportez-vous à la section Verrouillage des disques durs compatibles Opal *(page 371)*.

4.5.5 Verrouillage des disques durs compatibles Opal

Pour verrouiller les disques durs compatibles Opal, la clé de la machine doit être définie pour au moins un volume sur le disque dur dans une stratégie de chiffrement. Au cas où la stratégie de chiffrement inclut un volume de démarrage, la clé de la machine est définie automatiquement.

1. Dans SafeGuard Management Center, créez une stratégie du type **Protection des périphériques**.
2. Dans le champ **Mode de chiffrement des supports**, sélectionnez **Basé sur volume**.
3. Dans le champ **Clé à utiliser pour le chiffrement**, sélectionnez **Clé machine définie**.
4. Enregistrez vos changements dans la base de données.
5. Déployez la stratégie sur le terminal correspondant.

Le disque dur compatible Opal est verrouillé et est seulement accessible en se connectant sur l'ordinateur à l'authentification au démarrage SafeGuard.

4.5.6 Autorisation de déverrouillage des disques durs compatibles Opal aux utilisateurs

En tant que responsable de la sécurité, vous pouvez permettre aux utilisateurs de déverrouiller les disques durs compatibles Opal sur les terminaux à l'aide de la commande **Déchiffrer** du menu contextuel Windows Explorer.

Condition préalable : Dans la stratégie Protection des périphériques, ceci s'applique au disque dur Opal. L'option **L'utilisateur peut déchiffrer le volume** doit être définie sur **Oui**.

1. Dans SafeGuard Management Center, créez une stratégie du type **Protection des périphériques** et incluez tous les volumes présents sur le disque dur compatible Opal.
2. Dans le champ **Mode de chiffrement des supports**, sélectionnez **Aucune chiffrement**.
3. Enregistrez vos changements dans la base de données.
4. Déployez la stratégie sur le terminal correspondant.

L'utilisateur peut déverrouiller le disque dur compatible Opal sur le terminal. Le disque dur demeure verrouillé.

4.5.7 Journalisation des événements pour les terminaux équipés de disques durs compatibles Opal

Les événements signalés par les terminaux équipés de disques durs compatibles Opal à chiffrement automatique sont consignés dans le journal, comme pour tout autre terminal protégé par SafeGuard Enterprise. Les événements ne mentionnent pas particulièrement le type d'ordinateur. Les événements signalés sont identiques à tout autre terminal protégé par SafeGuard Enterprise.

Retrouvez plus de renseignements à la section Rapports *(page 228)*.

4.6 SafeGuard Configuration Protection

Le module SafeGuard Configuration Protection n'est plus disponible dans SafeGuard Enterprise 6.1. La stratégie correspondante ainsi que l'assistant de suspension sont toujours disponibles dans la version 8.3 de SafeGuard Management Center afin de prendre en charge les versions 6 et 5.60 des clients SafeGuard Enterprise sur lesquels sont installés et administrés SafeGuard Configuration Protection avec la version 8.3 de Management Center.

Retrouvez plus de renseignements sur SafeGuard Configuration Protection dans l'*Aide de l'administrateur de SafeGuard Enterprise 6*. http://www.sophos.com/fr-fr/medialibrary/PDFs/documentation/sgn_60_h_eng_admin_help.pdf.

4.7 À propos de la désinstallation

La désinstallation du logiciel de chiffrement SafeGuard Enterprise des terminaux implique les étapes suivantes :

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

Les stratégies appropriées doivent être effectives sur les terminaux pour permettre le déchiffrement et la désinstallation.

Lorsqu'un utilisateur avec les droits administrateur se connecte au terminal après la désinstallation, un outil de nettoyage démarre en tâche de fond. Un message informe l'utilisateur que l'opération de nettoyage nécessite le redémarrage de l'ordinateur.

L'outil de nettoyage se trouve ici : `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\SGNCleanUp.exe`

4.7.1 Désinstallation

Les conditions préalables suivantes doivent être remplies :

- Les données chiffrées doivent être déchiffrées correctement pour qu'elles deviennent accessibles par la suite. Le processus de déchiffrement doit être terminé. Un véritable déchiffrement est particulièrement important lorsque la désinstallation est déclenchée par Active Directory.
  - Par ailleurs, tous les supports amovibles chiffrés doivent être déchiffrés avant la désinstallation du dernier terminal protégé par SafeGuard Enterprise accessible. Sinon, les utilisateurs pourraient ne plus pouvoir accéder à leurs données. Tant que la base de données SafeGuard Enterprise est disponible, les données présentes sur les supports amovibles peuvent être récupérées.
- Pour désinstaller le chiffrement intégral du disque SafeGuard, tous les volumes chiffrés basé sur volume doivent disposer d'une lettre de lecteur qui leur est assignée.

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

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

4.7.2 Interdiction de la désinstallation sur les terminaux

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

5. Administration des terminaux Mac

Les Macs sur lesquels les produits Sophos suivants sont installés peuvent être administrés par SafeGuard Enterprise et/ou créer des rapports d’informations sur leur état. Les informations d’état apparaissent dans SafeGuard Management Center :

- À partir de la version 6.1 de Sophos SafeGuard File Encryption pour Mac
- À partir de la version 7.0 de Sophos SafeGuard Native Device Encryption
- Sophos SafeGuard Disk Encryption pour Mac 6.1

5.1 Création d’un package de configuration pour les Macs

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

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Assignez un serveur SafeGuard Enterprise principal (le serveur secondaire n’est pas nécessaire).
6. Sélectionnez **SSL** comme **Chiffrement du transport** pour la connexion entre le terminal et le serveur SafeGuard Enterprise. **Sophos** en tant que **Chiffrement de transport** n’est pas pris en charge pour Mac.
7. Indiquez un chemin de sortie pour le package de configuration (ZIP).
8. Cliquez sur **Créer un package de configuration**.

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

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

5.2 À propos de SafeGuard Native Device Encryption pour Mac

Sophos SafeGuard Native Device Encryption pour Mac fait bénéficier aux utilisateurs macOS du même niveau de protection des données que la fonction de chiffrement de disque de SafeGuard Enterprise offre déjà aux utilisateurs Windows.

SafeGuard Native Device Encryption pour Mac est basé sur la technologie de chiffrement intégral du disque intégrée à macOS. Le logiciel a recours à FileVault 2 pour chiffrer l’intégralité du disque dur afin que vos données soient en sécurité même en cas de perte ou de vol de votre ordinateur. Vous avez également la possibilité d’appliquer et de gérer le chiffrement du disque sur des réseaux tout entier.

Le chiffrement fonctionne de manière transparente. L’utilisateur n’a pas besoin de chiffrer ou de déchiffrer les fichiers lors de leur ouverture, modification ou enregistrement.

SafeGuard Management Center vous permet de sélectionner les ordinateurs (Windows et Macs) à chiffrer, de suivre l’état de leur chiffrement et de fournir des outils de récupération aux utilisateurs ayant oublié leur mot de passe.

5.2.1 Gestion des terminaux FileVault 2 avec SafeGuard Management Center

Dans SafeGuard Management Center, les terminaux FileVault 2 peuvent être gérés exactement comme tout terminal natif de SafeGuard Enterprise. En tant que responsable de la sécurité, vous pouvez définir des stratégies de chiffrement pour les terminaux FileVault 2 et les distribuer.

Lorsque le terminal FileVault 2 est enregistré dans SafeGuard Enterprise, les informations concernant l’utilisateur, l’ordinateur, le mode de connexion et l’état du chiffrement apparaissent. Les événements sont également consignés dans le journal pour les clients FileVault 2.

La gestion des clients FileVault 2 dans SafeGuard Enterprise est transparente, ce qui signifie que les fonctions de gestion fonctionnent en général de façon identique pour les clients FileVault 2 et SafeGuard Enterprise natifs. Vous pouvez retrouver le type d’un ordinateur dans l’**Inventaire** d’un conteneur dans **Utilisateurs et ordinateurs**. La colonne **Type de POA** vous indique si l’ordinateur correspondant est un client FileVault 2.

5.2.2 Stratégies de chiffrement pour le chiffrement intégral du disque FileVault 2

Le responsable de la sécurité peut créer une stratégie de chiffrement dans SafeGuard Management Center et la distribuer aux terminaux FileVault 2 sur lesquels elle sera appliquée.

Les terminaux FileVault 2 étant administrés de manière transparente dans SafeGuard Management Center, le responsable de la sécurité n’a pas besoin de procéder à un paramétrage spécifique de FileVault 2 pour le chiffrement. SafeGuard Enterprise connait l’état du client et sélectionne en conséquence le chiffrement FileVault 2.

Un terminal FileVault 2 traite uniquement les stratégies de type **Protection des périphériques** avec des **Volumes de démarrage** cibles et le **Mode de chiffrement du support** défini sur **Volume** ou sur **Aucun chiffrement**. Tous les autres paramètres de stratégie sont ignorés.

- **Volume** active FileVault 2 sur le terminal.
- **Aucun chiffrement** permet à l’utilisateur de déchiffrer le Mac.

5.2.3 Stratégies

SafeGuard Native Device Encryption pour Mac utilise uniquement les stratégies de type **Protection des périphériques** et **Paramètres généraux** et ignore tous les paramètres de stratégie à l’exception de **Cible**, **Mode de chiffrement des supports** et **Intervalle de connexion au serveur (minutes)**.

5.2.3.1 Options de configuration administrées centralement

Les stratégies sont configurées de manière centralisée dans SafeGuard Management Center. Pour commencer à utiliser le chiffrement intégral du disque, les paramètres doivent être choisi comme suit :

1. Créez une nouvelle stratégie de type **Protection des périphériques**. Pour **Cible de protection des périphériques**, sélectionnez **Périphériques de stockage locaux**, **Stockage interne** ou **Volumes de démarrage**. Saisissez un nom pour la stratégie et cliquez sur **OK**.
2. Pour le **Mode de chiffrement des supports**, sélectionnez **Par volume**.

Une nouvelle stratégie de protection des périphériques est créée et configurée pour le chiffrement intégral du disque des Macs.

Remarque :

Assurez-vous que la stratégie est assignée aux terminaux que vous voulez chiffrer. Vous pouvez assigner la stratégie au niveau principal de votre domaine ou groupe de travail. Si votre équipe du

service informatique effectue l'installation, n'assignez pas la stratégie avant que les terminaux aient été distribués aux utilisateurs. En effet, il y a un risque que le terminal soit chiffré trop tôt et que le technicien du service informatique soit enregistré dans FileVault 2 à la place des utilisateurs.

5.2.4 Fonctionnement du chiffrement

FileVault 2 maintient toutes les données sécurisées sur le disque dur grâce au chiffrement de données XTS-AES-128 opérant au niveau du disque. L'algorithme a été optimisé pour les blocs de 512 octets. La conversion du texte brut en texte crypté et vice versa est effectuée instantanément et a peu d'impact sur l'activité de l'utilisateur étant donné sa priorité peu élevée.

L'un des obstacles classiques à l'utilisation du chiffrement intégral du disque était que l'utilisateur devait s'authentifier par deux fois : une fois pour déverrouiller le volume de démarrage chiffré (authentification au démarrage) et une seconde fois pour se connecter à son ordinateur.

Ces opérations ne sont, à présent, plus nécessaires. L'utilisateur saisit son mot de passe à la connexion avant le démarrage et le système déclenche le transfert du mot de passe lorsque le système d'exploitation est en route et demande les codes d'accès de connexion. Le transfert de mot de passe évite à l'utilisateur d'avoir à se connecter deux fois après un démarrage à froid.

L'utilisateur peut réinitialiser son mot de passe à tout moment sans avoir à chiffrer de nouveau le volume. Ceci est rendu possible par le système de clé multi-niveaux qui est utilisé. Les clés affichées à l'utilisateur (par exemple, des clés de connexion et des clés de récupération) sont des clés de chiffrement dérivées pouvant être remplacées. L'authentique clé de chiffrement de volume n'est jamais transmise à l'utilisateur.

Retrouvez plus de renseignements sur FileVault 2 dans le *Livre blanc technique d'Apple - Bon usage pour le déploiement de FileVault 2 (Août 2012)*, disponible au téléchargement sur le site Web d'Apple.

5.2.5 Chiffrement initial

Lorsque vous définissez le chiffrement par volume du disque système à l'aide d'une stratégie, le chiffrement des disques démarre automatiquement dès que l'utilisateur redémarre son terminal. L'utilisateur doit effectuer les actions suivantes :

1. Saisir le mot de passe macOS.
2. Patienter pendant le redémarrage du Mac.

> **Remarque :** En cas d'échec de l'activation du chiffrement, un message d'erreur apparaît. Retrouvez plus de renseignements dans les fichiers d'historique. L'emplacement par défaut est `/var/log/system.log` Rechercher le mot clé fdesetup.

3. Le chiffrement du disque commence et s’effectue en tâche de fond. L’utilisateur peut continuer à travailler.

L’utilisateur est ajouté en tant que premier utilisateur FileVault 2 du terminal.

5.2.6 Déchiffrement

Il n’est généralement pas nécessaire de déchiffrer. Si vous définissez une règle stipulant qu’**aucun chiffrement** n’est nécessaire pour vos clients Mac déjà chiffrés, ceux-ci resteront chiffrés. Par contre, dans ce cas, les utilisateurs ont la possibilité de le déchiffrer. Le bouton se trouve sous l’onglet Chiffrement de fichiers dans le panneau des préférences.

Les utilisateurs disposant des droits d’administrateur local pourront déchiffrer manuellement leur disque dur à l’aide de la fonctionnalité FileVault 2 intégrée. Toutefois, ils seront invités à redémarrer pour terminer l’opération de déchiffrement. Dès que le Mac aura redémarré, SafeGuard Native Device Encryption pour Mac appliquera le chiffrement si une règle a été définie dans ce sens.

5.2.7 Ajout d’un utilisateur FileVault 2

Sur les terminaux macOS à partir de la version 10.13, tous les utilisateurs existants d’un terminal sont ajoutés automatiquement dans FileVault.

Sur les terminaux macOS jusqu’à la version 10.12, chaque utilisateur doit se connecter séparément pour être ajouté dans FileVault. Pour ajouter un utilisateur à FileVault, procédez de la manière suivante :

1. Lorsque le Mac est en cours de fonctionnement, connectez-vous sous le nom d’utilisateur que vous souhaitez enregistrer dans FileVault.
2. Saisissez les codes d’accès de cet utilisateur dans la boîte de dialogue **Activation de votre compte**.

Les utilisateurs pourront se connecter comme s’il n’y avait aucun logiciel de chiffrement du disque installé sur leur ordinateur.

Vous pouvez assigner les utilisateurs aux terminaux dans SafeGuard Management Center afin de leur permettre d’utiliser FileVault 2.

5.2.8 Suppression d’un utilisateur FileVault 2

Il est possible de supprimer un utilisateur de la liste des utilisateurs affectés à un Mac dans SafeGuard Management Center. À la prochaine synchronisation, l’utilisateur sera également retiré de la liste des utilisateurs FileVault 2 sur le terminal. En revanche, ceci ne signifie pas que l’utilisateur ne sera plus en mesure de se connecter au Mac. Comme pour tout autre nouvel utilisateur, il lui suffira de se connecter à un Mac afin d’être à nouveau autorisé d’accès.

Si vous voulez vraiment empêcher un utilisateur de démarrer un Mac, indiquez que cet utilisateur est bloqué dans Management Center. L’utilisateur sera supprimé de la liste des utilisateurs FileVault 2 du client et aucune nouvelle autorisation ne sera possible.

Il est possible de supprimer les utilisateurs FileVault 2 à l’exception du dernier d’entre eux. Si le propriétaire est supprimé, l’utilisateur suivant dans la liste est indiqué comme étant le propriétaire. SafeGuard Native Device Encryption pour Mac ne fait aucune différence entre un utilisateur et un propriétaire.

5.2.9 Synchronisation avec le serveur backend

Pendant le processus de synchronisation, l’état des clients est signalé au serveur backend de SafeGuard Enterprise. Les règles sont mises à jour et l’assignation utilisateur/machine est vérifiée.

Les informations suivantes sont donc envoyées à partir des clients et apparaissent dans SafeGuard Management Center :

- Dès que le terminal est chiffré, l’authentification au démarrage est vérifiée. Les autres informations affichées incluent le nom du lecteur, l’intitulé, le type, l’état, l’algorithme et le système d’exploitation.
- Les nouveaux utilisateurs FileVault 2 sont également ajoutés dans Management Center.

Remarque : Si le logiciel client SafeGuard Enterprise est supprimé d’un terminal, cet ordinateur ainsi que ses utilisateurs demeurent visibles dans SafeGuard Management Center. En revanche, la date et l’heure auxquelles le serveur a été contacté pour la dernière fois ne changent plus.

Les modifications ci-dessous ont lieu sur le client :

- Les règles modifiées dans Management Center sont modifiées sur le client.
- Les utilisateurs supprimés ou bloqués dans Management Center sont également supprimés de la liste des utilisateurs FileVault 2 sur le client.

5.2.10 Options de ligne de commande

L'application Terminal vous permet de saisir les commandes et les options de ligne de commande. Les options de ligne de commande suivantes sont disponibles :

Nom de la commande	Définition	Paramètres additionnels (facultatif)
sgdeadmin	Répertorie toutes les commandes disponibles y compris les conseils d'utilisation.	--help
sgdeadmin --version	Affiche la version et le copyright du produit installé.	
sgdeadmin --status	Renvoie des informations sur l'état du système telle que la version, le serveur et le certificat.	
sgdeadmin --list-user-details	Renvoie des informations sur l'utilisateur connecté.	--all affiche les informations sur tous les utilisateurs (commande sudo requise) --xml renvoie un fichier généré au format xml.
sgdeadmin --list-policies	Affiche des informations relatives à la règle. Les GUID de clé sont résolus en noms de clé si possible. Une clé personnelle sera affichée en caractères gras.	--all affiche les informations sur tous les utilisateurs (commande sudo requise) --xml renvoie un fichier généré au format xml.
sgdeadmin --synchronize	Force l'établissement d'un contact immédiat avec le serveur (une connexion au serveur est nécessaire).	
sgdeadmin --import-recoverykey ["recoverykey"]	Importe la clé de récupération FileVault 2 et remplace la clé de récupération déjà existante.	--force remplace la clé de récupération déjà existante sans demander de confirmation supplémentaire

Nom de la commande	Définition	Paramètres additionnels (facultatif)
		"recoverykey" demande à l'utilisateur de saisir la clé de récupération s'il ne l'a pas fait.
sgdeadmin --import-config "/path/to/target/file"	Importe le fichier ZIP de configuration indiqué. Cette commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Utilisez l'opération glisser-déplacer pour déplacer, par exemple, un chemin complet du Finder à l'application Terminal.	
sgdeadmin --enable-server-verify	Active la vérification du serveur SSL pour la communication avec le serveur SafeGuard Enterprise. Suite à l'installation, la vérification du serveur SSL est activée. Cette commande nécessite de disposer des droits administratifs (sudo).	
sgdeadmin --disable-server-verify	Désactive la vérification du serveur SSL pour la communication avec le serveur SafeGuard Enterprise. Cette commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Nous déconseillons l'utilisation de cette option car elle risque de créer une faille de sécurité.	
sgdeadmin --update-machine-info [--domain "domain"]	Met à jour les informations de la machine qui sont utilisées pour enregistrer ce client sur le serveur SafeGuard Enterprise. Cette	--domain "domain" Le domaine que le client doit utiliser pour s'enregistrer sur le serveur SafeGuard Enterprise. Ce paramètre est uniquement nécessaire si l'ordinateur est

Nom de la commande	Définition	Paramètres additionnels (facultatif)
	commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Utilisez uniquement cette commande après avoir changé le domaine ou le groupe de travail auquel appartient l'ordinateur. Si l'ordinateur est membre de plusieurs domaines ou groupes de travail et que vous exécutez cette commande, il se peut que l'enregistrement du domaine soit modifié et que les clés personnelles et/ou les utilisateurs FileVault 2 soient supprimés.	membre de plusieurs domaines. Si l'ordinateur n'est pas relié à ce domaine, la commande échouera.
sgdeadmin --enable-systemmenu	Active le menu système sur le terminal.	
sgdeadmin --disable-systemmenu	Désactive le menu système sur le terminal.	
sgdeadmin --synchronize	Synchronise les informations de la base de données (stratégies, clés, etc.) à partir du serveur backend SafeGuard Enterprise.	

5.2.11 Clé de secours pour terminaux Mac

L'accès aux clients SafeGuard Enterprise chiffrés à l'aide de FileVault 2 est possible si vous suivez la procédure ci-dessous :

1. Pour ouvrir l'**Assistant de récupération** dans SafeGuard Management Center, cliquez sur **Outils > Récupération**.
2. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise (administré)**.
3. Sous **Domaine**, sélectionnez le domaine requis dans la liste.
4. Sous **Ordinateur**, saisissez ou sélectionnez le nom d'ordinateur requis. Vous pouvez procéder de plusieurs façons :

    - Pour sélectionner un nom, cliquez sur **[...]**. Cliquez ensuite sur **Rechercher maintenant**. Une liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur s'affiche dans la fenêtre **Type de récupération** sous **Domaine**.

- Saisissez le nom abrégé de l'ordinateur directement dans le champ. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.

- Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

  CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=uae

5. Cliquez sur **Suivant**.
6. L'assistant de récupération affiche la clé de récupération à 24 chiffres correspondante.
7. Fournissez cette clé à l'utilisateur.

L'utilisateur peut saisir la clé de secours pour se connecter au terminal Mac et réinitialiser le mot de passe.

5.2.12 Gestion de la clé de récupération

Si tous les utilisateurs FileVault d'un système particulier oublient leur mot de passe, si les autres codes d'accès ne sont pas disponibles et si aucune clé de secours n'est disponible, le volume chiffré ne peut pas être déverrouillé et les données sont inaccessibles. Il se peut que les données soient définitivement perdues. Par conséquent, il est essentiel de préparer un programme de récupération correct.

Une nouvelle clé de secours est générée à chaque activation du chiffrement du disque. Si Sophos SafeGuard Native Device Encryption n'est pas installé au moment de l'opération de chiffrement, elle est visible par l'utilisateur qui en est, par conséquent, responsable et doit veiller à ne pas la perdre. Si Sophos SafeGuard Native Device Encryption est installé, elle est envoyée par un canal sécurisé au serveur backend de SafeGuard Enterprise et archivée de manière centralisée. Le responsable de la sécurité peut la récupérer à chaque fois qu'il en a besoin. Retrouvez plus de renseignements à la section Réinitialisation en cas d'oubli du mot de passe *(page 399)*.

SafeGuard Management Center change automatiquement la clé de récupération de FileVault après avoir été récupérée.

Même si SafeGuard Native Device Encryption n'a pas été installé lorsque le disque a été chiffré, la clé de secours peut être gérée de manière centralisée. Il est donc nécessaire de l'importer. L'option de ligne de commande adéquate est sgdeadmin --import-recoverykey. Retrouvez plus de renseignements à la section Options de ligne de commande *(page 381)*. La clé de secours sera envoyée en lettre majuscule.

En cas de présence d'une clé de secours institutionnelle, elle peut également être utilisée à des fins de récupération. Retrouvez plus de renseignements sur support.apple.com/kb/HT5077.

5.2.13 Gestion des mots de passe

Le jeu de clés Sophos SafeGuard est sécurisé à l'aide d'un certificat d'utilisateur. La clé privée correspondante est protégée par le mot de passe macOS.

Le mot de passe permet de générer un certificat si l'utilisateur n'a pas été créé dans SafeGuard Enterprise.

Changement local de mot passe

Les utilisateurs ont la possibilité de changer localement leur mot de passe dans **Préférences Système > Utilisateurs et groupes**. Aucune autre étape supplémentaire n'est requise.

Le mot de passe a été changé sur un autre terminal

Remarque : Les mots de passe peuvent être changés sur les terminaux Windows et Mac.

Le mot de passe n'étant plus connu sur ce terminal, les étapes suivantes doivent être effectuées :

1. Connectez-vous à macOS avec votre nouveau mot de passe.
2. Le message **Le système n'a pas réussi à déverrouiller votre trousseau de session** apparaît.
3. Sélectionnez **Mettre à jour le mot de passe du trousseau**.
4. Saisissez l'ancien mot de passe.

Retrouvez plus de renseignements sur la réinitialisation d'un mot de passe oublié à la section Réinitialisation en cas d'oubli du mot de passe *(page 399)*.

5.3 À propos de Sophos SafeGuard File Encryption pour Mac

Sophos SafeGuard File Encryption pour Mac étend la protection des données offerte par Sophos SafeGuard Enterprise sur Windows aux utilisateurs de Macs. Il offre le chiffrement des fichiers sur les lecteurs locaux, les partages réseaux, les lecteurs amovibles et dans le Cloud.

SafeGuard File Encryption pour Mac vous permet de chiffrer et de déchiffrer les fichiers puis d'échanger ces fichiers avec d'autres utilisateurs sur les ordinateurs Macs ou Windows.

Pour lire les fichiers chiffrés par SafeGuard Enterprise sur des appareils mobiles, veuillez utiliser Sophos Secure Workspace pour iOS ou Android.

Configurer les règles de chiffrement

Dans SafeGuard Management Center, vous définissez les règles du chiffrement basé sur fichier dans les règles File Encryption. Dans les stratégies de chiffrement de fichiers, vous indiquez les dossiers qui doivent être gérés par le chiffrement de fichiers, le mode de chiffrement et la clé à utiliser pour le chiffrement. Grâce à cette administration centralisée, vous pouvez être sûr que les mêmes dossiers et clés de chiffrement sont traités sur des plates-formes différentes. Retrouvez plus de renseignements à la section Configuration des règles de chiffrement dans les stratégies de chiffrement de fichiers par emplacement *(page 337)*.

Dossiers exclus

Les dossiers ci-dessous sont exclus du chiffrement :

- **Dossiers exclus et sous-dossiers non exclus :**
  - <Racine>/
  - <Racine>/Volumes/
  - <Profil utilisateur>/
- **Dossiers et sous-dossiers exclus :**
  - <Racine>/bin/
  - <Racine>/sbin/
  - <Racine>/usr/
  - <Racine>/private/
  - <Racine>/dev/
  - <Racine>/Applications/
  - <Racine>/Système/
  - <Racine>/Bibliothèque/
  - <Profil utilisateur>/Bibliothèque/
  - /<Amovibles>/SGPortable/
  - /<Amovibles>/Informations sur le volume système/

Ceci signifie, par exemple, qu'une règle de chiffrement pour la racine d'une partition supplémentaire (<Racine>/Volumes/) n'a aucun effet même si elle signalée comme ayant reçue une règle.

Une règle de chiffrement sur <Racine>/abc aura un effet tandis qu'une règle de chiffrement sur <Racine>/private/abc n'en aura aucun.

Réduction de la charge administrative

- Essayez d'avoir le moins de points de montage (ou Dossiers sécurisés) possibles.
- Désactivez l'option **Exiger une confirmation avant de créer un compte mobile**.

  Si vous créez ou utilisez des comptes mobiles pour les terminaux Mac, assurez-vous que l'option **Exiger une confirmation avant de créer un compte mobile** est désactivée. Lorsque

cette option est activée, l'utilisateur peut sélectionner **Ne pas créer**. Ceci peut entraîner la création d'un utilisateur macOS incomplet. Par exemple un utilisateur qui n'a pas de répertoire de départ local.

Pour désactivez cette option, procédez aux étapes suivantes :

1. Ouvrez les **Préférences Système** et cliquez sur **Utilisateurs et groupes**.
2. Cliquez sur le cadenas et saisissez votre mot de passe.
3. Sélectionnez l'utilisateur.
4. Cliquez sur **Options d'ouverture de session**.
5. Dans **Compte serveur réseau**, cliquez sur **Modifier....** .
6. Sélectionnez le domaine Active Directory.
7. Cliquez sur **Ouvrir Utilitaire d'annuaire....** .
8. Cliquez sur le cadenas et saisissez votre mot de passe, puis cliquez sur **Modifier la configuration**.
9. Sélectionnez Active Directory et cliquez sur l'icône Modifier.
10. Cliquez sur la flèche se trouvant à côté de **Afficher les options avancées**.
11. Sélectionnez **Créer un compte mobile lors de l'ouverture de session** et dessélectionnez l'option **Exiger une confirmation avant de créer un compte mobile**.
12. Cliquez sur **OK**.

Restrictions

- **Nombre maximal de dossiers sécurisés (points de montage) sur un client**

  Chaque client macOS contient un nombre maximal de 24 dossiers sécurisés (points de montage). Si plusieurs utilisateurs sont connectés à la même machine, vous devez ajouter les points de montage de tous les utilisateurs connectés.

- **Recherche de fichiers**
  - **Spotlight**

    Par défaut, la recherche de fichiers dans les Dossiers sécurisés avec Spotlight n'est pas possible.

    Pour activer la recherche Spotlight, veuillez exécuter la commande du Terminal suivante : `sgfsadmin --enable-spotlight`

    Pour désactiver la recherche Spotlight, veuillez exécuter la commande du Terminal suivante : `sgfsadmin --disable-spotlight`

    Remarque : L'utilisation de Spotlight avec Sophos SafeGuard risque de ralentir la vitesse de recherche.

  - **Fichiers identifiés**

    La recherche des fichiers identifiés ne fonctionne pas dans les Dossiers sécurisés.

- **Déplacement de fichiers chiffrés à partir des Dossiers sécurisés**

  Lorsque vous déplacez un fichier chiffré d'un Dossier sécurisé vers un dossier non sécurisé, le fichier demeure chiffré mais vous n'êtes pas en mesure de voir son contenu. Vous devez d'abord le déchiffrer manuellement.

  Lorsque vous ouvrez un fichier chiffré dans un Dossier sécurisé et que vous l'enregistrez dans un Dossier non sécurisé, le fichier est déchiffré automatiquement.

- **Stockage permanent des versions indisponibles dans les Dossiers sécurisés**

  Pour les fichiers dans les Dossiers sécurisés, la fonctionnalité de base **Parcourir toutes les versions...** n'est pas disponible.

- **Partage des Dossiers sécurisés**

  Un dossier sécurisé ne peut pas être partagé sur le réseau.

- **Gravure de CD**

  Il n'est pas possible de graver un CD chiffré.

- **Suppression de fichiers**

  Lorsque vous supprimez des fichiers à partir d'un Dossier sécurisé (point de montage), vous voyez apparaître un message vous demandant de confirmer l'opération de suppression. Les fichiers supprimés ne sont pas déplacés dans le dossier Corbeille et ne peuvent donc pas être restaurés.

- **SafeGuard Portable**

  SafeGuard Portable n'est pas disponible sur les Macs.

- **Utilisation d'AirDrop**

  Les fichiers chiffrés peuvent être transférés avec AirDrop. Assurez-vous que l'appareil de destination peut gérer les fichiers chiffrés. En cas contraire, les applications pourraient fonctionner de manière inattendue.

- **Handoff**

  Il n'est pas possible d'utiliser Handoff sur les fichiers chiffrés.

- **Montage de partages de fichier réseau avec `autofs`**

  Les partages de fichier réseau sur lesquels une règle est appliquée et qui sont automatiquement montés au démarrage ne seront pas détectés par Sophos SafeGuard File Encryption. La gestion

de ces points de montage est impossible car le point de montage d’origine ne peut pas être remplacé.

5.3.1 Options de configuration administrées centralement

Les options suivantes sont configurées de manière centralisée dans Management Center :

- **Stratégies**
- **Clés**

- **Certificats**

  Le serveur SafeGuard Enterprise fournit le certificat X.509 à l'utilisateur. Un certificat est généré à la première connexion. Le certificat sécurise le jeu de clés de l'utilisateur.

- **Intervalle de connexion au serveur**

5.3.2 Stratégies

SafeGuard File Encryption pour Mac utilise uniquement les stratégies **Chiffrement de fichiers** et **Paramètres généraux**. Ainsi, vous avez uniquement besoin d’utiliser la stratégie **Chiffrement de fichiers** pour administrer le chiffrement des données sur le système de fichiers local, les supports amovibles, les partages réseau et le stockage Cloud.

Les stratégies **Protection des périphériques** (notamment **Stockage Cloud** et **Chiffrement des supports amovibles**) seront ignorées pour SafeGuard File Encryption pour macOS. Veuillez toujours assigner les stratégies de **Chiffrement de fichiers** aux objets des utilisateurs. Les stratégies **Chiffrement de fichiers** assignées aux terminaux n’auront aucun effet sur les terminaux macOS.

Remarque : Dans SafeGuard Management Center, veuillez saisir les chemins en utilisant des barres obliques inverses. Elles sont automatiquement converties en barres obliques sur le terminal Mac.

5.3.3 Chiffrement de fichiers dans le stockage Cloud

SafeGuard Entreprise offre un chiffrement de fichier des données stockées dans le Cloud.

Il ne change pas la façon dont les utilisateurs exploitent les données stockées dans le Cloud. Les utilisateurs se servent des mêmes applications de synchronisation spécifiques aux fournisseurs pour

envoyer des données dans le Cloud ou en recevoir depuis celui-ci. Les copies locales des données stockées dans le Cloud sont chiffrées de manière transparente et seront donc toujours stockées dans le Cloud sous une forme chiffrée.

Sur les Macs, SafeGuard Enterprise offre la détection automatique des fournisseurs de stockage Cloud suivants :

- Box
- Dropbox (inclut Dropbox Business)
- Google Drive
- OneDrive
- OneDrive Entreprise

Pour ces fournisseurs, veuillez uniquement indiquer le chemin des dossiers de synchronisation dans une stratégie par emplacement du type **Chiffrement de fichiers**.

Pour le chiffrement par application des fichiers dans le stockage Cloud, vous pouvez utiliser les espaces réservés prédéfinis comme indiqué à la section Configuration du chiffrement de fichiers par application dans le Cloud *(page 431)*

Après assignation de la stratégie aux terminaux, les fichiers présents dans les emplacements couverts par la stratégie sont chiffrés de manière transparente sans interaction avec l'utilisateur :

- Les fichiers chiffrés seront synchronisés dans le Cloud.
- Les fichiers chiffrés reçus du Cloud peuvent comme d'habitude être traités par les applications.

Les données stockées dans le Cloud avant que vous n'ayez activé le chiffrement ne sont pas chiffrés automatiquement. Pour garantir que les fichiers sensibles sur votre ordinateur soient chiffrés, les utilisateurs peuvent procéder au chiffrement initial comme indiqué à la section Chiffrement initial *(page 392)*.

5.3.3.1 Configuration du chiffrement de fichiers par emplacement dans le Cloud

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Chiffrement de fichiers** ou sélectionnez-en une.
   L'onglet **Chiffrement de fichiers** apparaît.

2. Sélectionnez **Par emplacement** dans la liste déroulante **Type de chiffrement**.
   Le tableau des emplacements sur lesquels le chiffrement de fichiers par emplacement est appliqué sur l'ordinateur apparait.

3. Dans la colonne **Chemin**, indiquez le chemin du dossier de synchronisation du stockage Cloud. Par exemple ; `<Profil utilisateur>\Dropbox`.

- Cliquez sur le bouton déroulant et sélectionnez un espace réservé de nom de dossier dans la liste des espaces réservés disponibles.

  En faisant passer votre curseur sur les entrées de la liste, vous pouvez afficher des infobulles qui vous indiquent comment un espace réservé est généralement présenté sur un terminal. Vous pouvez seulement saisir des espaces réservés valides. Retrouvez une description de tous les espaces réservés disponibles à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.

- Vous avez également la possibilité de saisir le nom du chemin et du dossier.

Remarque :

Le dossier de synchronisation local ne doit pas être modifié par les utilisateurs. Par exemple, en cas de déplacement du dossier, le chiffrement des fichiers dans le Cloud ne fonctionnera plus.

Si le dossier de synchronisation sur les terminaux change d'emplacement, veuillez mettre à jour le chemin dans la règle de chiffrement.

4. Dans la colonne **Étendue**, sélectionnez :
   - **Ce dossier uniquement** pour appliquer la règle seulement au dossier indiqué par la colonne **Chemin**.
   - **Inclure les sous-dossiers** pour appliquer aussi la règle à tous ses sous-dossiers.
5. Dans la colonne **Mode**, sélectionnez **Chiffrer**.
6. Dans la colonne **Clé**, sélectionnez la clé à utiliser pour le mode **Chiffrer**. Vous pouvez utiliser des clés créées et appliquées dans **Utilisateurs et ordinateurs** :

   - Cliquez sur le bouton **Parcourir** pour ouvrir la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour afficher une liste de toutes les clés disponibles et sélectionnez la clé requise.

     Remarque : Les clés machine ne sont pas montrées dans la liste. Elles ne peuvent pas être utilisées par le Chiffrement de fichiers car elles sont uniquement disponibles sur une seule machine et ne peuvent donc pas être utilisées pour permettre à des groupes d'utilisateurs d'accéder aux mêmes données.

   - Cliquez sur le bouton **Clé personnelle** avec l'icône de la clé pour insérer l'espace réservé **Clé personnelle** dans la colonne **Clé**. Sur le terminal, cet espace réservé sera résolu sur la clé personnelle active de l'utilisateur SafeGuard Enterprise connecté. Si les utilisateurs correspondants n'ont pas encore de clés personnelles actives, elles sont créées automatiquement. Vous pouvez créer des clés personnelles pour un ou plusieurs utilisateurs dans **Utilisateurs et ordinateurs**. Retrouvez plus de renseignements à la section Clés personnelles pour le chiffrement de fichiers par File Encryption *(page 177)*.

7. Pour ajouter d’autres chemins :

8. Enregistrez vos modifications.

9. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la nouvelle stratégie à vos groupes d’utilisateurs.

5.3.3.2 Résolution des problèmes et prise en charge des fournisseurs de stockage Cloud supplémentaires

Sophos SafeGuard détecte normalement les dossiers de synchronisation Cloud automatiquement. Toutefois, su les fournisseurs de stockage Cloud publient une nouvelle version de leur logiciel et modifient certains des paramètres par défaut, il se peut que la détection automatique échoue.

Dans ce cas, demandez au support Sophos de vous fournir un fichier de configuration. Retrouvez plus de renseignements dans l’article 126321 de la base de connaissances de Sophos.

Vous pouvez également ajouter de nouveaux fournisseurs de stockage Cloud dans ce fichier de configuration afin qu’ils puissent être aussi détectés automatiquement.

5.3.4 Chiffrement initial

Le premier chiffrement de fichiers peut être lancé à partir du volet des préférences ou depuis l’outil de ligne de commandes. Les administrateurs et les utilisateurs peuvent déclencher le premier chiffrement des fichiers sur les lecteurs locaux et sur les lecteurs multimédia amovibles. Seuls les administrateurs peuvent chiffrer les partages réseau.

Une stratégie définit si le chiffrement initial est lancé automatiquement et si les dossiers locaux, amovibles ou les fournisseurs de stockage Cloud doivent être chiffrés.

Pour démarrer manuellement le chiffrement sur le terminal :

1. Ouvrez les **Préférences Système**.

2. Cliquez sur l’icône Sophos SafeGuard.

3. Sélectionnez l’onglet **Stratégies**.

4. Passez dans la vue **Chemin converti localement** si elle n’est pas déjà ouverte. Vous pouvez soit

    a. appliquer toutes les stratégies en cliquant sur le bouton **Appliquer toutes les stratégies** au bas de la fenêtre.
    soit

b. sélectionner une seule stratégie et cliquez sur le bouton **Appliquer la stratégie**.

Remarque : Ne déconnectez pas les appareils pendant l’opération de chiffrement.

Remarque : Si vous souhaitez voir les détails et le contenu du chemin converti localement, sélectionnez ce chemin dans le tableau et cliquez sur **Afficher dans le Finder**.

5.3.5 Permutation rapide d'utilisateur

SafeGuard File Encryption pour Mac prend également en charge la permutation rapide d'utilisateur. Le logiciel vous permet de permuter entre les comptes d'utilisateur à partir d'un seul terminal sans avoir à quitter les applications ou à fermer la session sur l'ordinateur.

5.3.6 Utilisation de clés locales

Remarque : Les clés locales ne peuvent pas être utilisée par SafeGuard Synchronized Encryption.

Les clés locales servent à chiffrer les fichiers dans les dossiers spécifiques sur un périphérique amovible ou chez un fournisseur de stockage Cloud. Ces emplacements doivent déjà être inclus dans une stratégie de chiffrement.

Pour créer une clé locale :

1. Cliquez avec le bouton droit de la souris sur un fichier ou sur une série de fichiers et sélectionnez **Créer une nouvelle clé**.

2. Choisissez un nom et une phrase secrète pour votre clé et cliquez sur **OK**.
   Le nom de la clé sera préfixé par « Local_ » et suivi de la date et de l’heure.

La clé locale est créée et affichée dans le panneau des préférences. L’utilisateur peut à présent appliquer la clé locale à un périphérique amovible ou à un répertoire Cloud.

5.3.7 Options de ligne de commande

L’application Terminal vous permet de saisir les commandes et les options de ligne de commande. Les options de ligne de commande suivantes sont disponibles :

Nom de la commande	Définition	Paramètres additionnels (facultatif)
sgfsadmin	Répertorie toutes les commandes disponibles y compris les conseils d'utilisation.	--help
sgfsadmin --version	Affiche la version et le copyright du produit installé.	
sgfsadmin --status	Renvoie des informations sur l'état du système telle que la version, le serveur et le certificat.	
sgfsadmin --list-user-details	Renvoie des informations sur l'utilisateur connecté.	--all affiche les informations sur tous les utilisateurs (commande sudo requise) --xml renvoie un fichier généré au format xml.
sgfsadmin --list-keys	Répertorie les GUID existants et les noms de toutes les clés dans le magasin de clés.	--all affiche les informations sur tous les utilisateurs (commande sudo requise) --hidden-keys affiche uniquement les clés marquées comme masquées --xml renvoie un fichier généré au format xml.
sgfsadmin --list-policies	Affiche des informations relatives à la règle. Les GUID de clé sont résolus en noms de clé si possible. Une clé personnelle sera affichée en caractères gras.	--all affiche les informations sur tous les utilisateurs (commande sudo requise) --xml renvoie un fichier généré au format xml. --raw affiche les règles brutes, c'est-à-dire les règles paramétrées sur le serveur SafeGuard Management Center.

Nom de la commande	Définition	Paramètres additionnels (facultatif)
sgfsadmin --enforce-policies	Applique la règle de chiffrement.	--all applique la règle à tous les répertoires auxquels les règles s'appliquent. "directoryname" applique la règle au répertoire indiqué.
sgfsadmin --file-status "filename1" ["filename2"..."filenameN"]	Renvoie les informations de chiffrement d'un fichier ou d'une liste de fichiers. Les caractères de remplacement sont acceptés.	--xml renvoie un fichier généré au format xml.
sgfsadmin --import-config "/path/to/target/file"	Importe le fichier ZIP de configuration indiqué. Cette commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Utilisez l'opération glisser-déplacer pour déplacer, par exemple, un chemin complet du Finder à l'application Terminal.	
sgfsadmin --enable-server-verify	Active la vérification du serveur SSL pour la communication avec le serveur SafeGuard Enterprise. Suite à l'installation, la vérification du serveur SSL est activée. Cette commande nécessite de disposer des droits administratifs (sudo).	
sgfsadmin --disable-server-verify	Désactive la vérification du serveur SSL pour la communication avec le serveur SafeGuard Enterprise. Cette commande nécessite de disposer des droits administratifs (sudo).	

Nom de la commande	Définition	Paramètres additionnels (facultatif)
	Remarque : Nous déconseillons l'utilisation de cette option car elle risque de créer une faille de sécurité.	
sgfsadmin --update-machine-info [--domain "domaine"]	Met à jour les informations de la machine qui sont utilisées pour enregistrer ce client sur le serveur SafeGuard Enterprise. Cette commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Utilisez uniquement cette commande après avoir changé le domaine ou le groupe de travail auquel appartient l'ordinateur. Si l'ordinateur est membre de plusieurs domaines ou groupes de travail et que vous exécutez cette commande, il se peut que l'enregistrement du domaine soit modifié et que les clés personnelles et/ou les utilisateurs FileVault 2 soient supprimés.	--domain "domain" Le domaine que le client doit utiliser pour s'enregistrer sur le serveur SafeGuard Enterprise. Ce paramètre est uniquement nécessaire si la machine est membre de plusieurs domaines. Si l'ordinateur n'est pas relié à ce domaine, la commande échouera.
sgfsadmin --dump-unprivileged-applications [chemin]	Collecte les chemins des applications qui ne sont pas autorisées à accéder aux fichiers chiffrés. Vous pouvez utiliser ces informations pour ajouter des applications à la liste d'application. Vous pouvez	

Nom de la commande	Définition	Paramètres additionnels (facultatif)
	restreindre les résultats à un chemin spécifique. **Remarque :** Cette fonction concerne uniquement Synchronized Encryption.	
sgfsadmin --synchronize	Synchronise les informations de la base de données (stratégies, clés et certificats) à partir du serveur backend SafeGuard Enterprise.	
sgfsadmin --enable-spotlight	Active la recherche Spotlight.	
sgfsadmin --disable-spotlight	Désactive la recherche Spotlight.	

5.3.8 Utilisation de Time Machine

Remarque : Cette section s'applique uniquement si une règle de chiffrement est configurée pour <Amovibles>.

Si vous voulez utiliser un nouveau disque pour effectuer une sauvegarde de Time Machine et si le système d'exploitation ne vous suggère pas automatiquement de l'utiliser, veuillez utiliser la commande suivante dans l'application Terminal :

```
sudo tmutil setdestination -a "/Volumes/.sophos_safeguard_{NOM DU DISQUE}/"
```

Si vous utilisez Time Machine pour un dossier chiffré, les fichiers sauvegardés ne sont pas affichés. Ces sauvegardes sont conservées dans un emplacement caché et contiennent uniquement les données chiffrées. Pour restaurer les fichiers, veuillez procéder comme suit :

1. Ouvrez Time Machine.
   Le contenu de votre dossier racine s'affiche.

2. Appuyez sur **Maj - Commande - G** (pour « Aller au dossier : ») et saisissez le chemin masqué du dossier chiffré que vous souhaitez restaurer.
   Si le dossier chiffré que vous utilisez habituellement est nommé /Utilisateurs/admin/Documents, veuillez saisir `/Utilisateurs/admin/.sophos_safeguard_Documents/`.

3. Naviguez jusqu'au fichier que vous souhaitez restaurer, puis, cliquez sur l'icône en forme de roue de la barre de menu de Time Machine et sélectionnez **Restaurer <nom de fichier> dans...**.

4. Naviguez jusqu'au fichier restauré dans le Finder et vérifiez son état de chiffrement.

5. Chiffrez le fichier manuellement si nécessaire.

Remarque : La première copie de sauvegarde Time Machine suite à une nouvelle installation de SafeGuard File Encryption est plus longue à effectuer et nécessite plus d'espace disque que d'habitude. Ceci est dû au fait que macOS n'autorise pas les systèmes de fichiers empilés. Tous les répertoires locaux pour lesquels des points de montage sécurisés ont été créés (Documents, Musique, Vidéos, etc.) seront donc copiés sur le disque de sauvegarde.

5.3.9 Utilisation des supports multimédia amovibles

Pour activer le chiffrement de fichiers sur les supports multimédia amovibles, une stratégie de **Chiffrement de fichiers** avec l'espace réservé **<Amovibles>** comme **Chemin** est requise. Retrouvez plus de renseignements à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.

Pour pouvoir échanger et modifier des données présentes sur les périphériques amovibles entre deux personnes, ces deux personnes doivent disposer de la règle correspondante et être affectées à une clé. Aucune clé personnelle ne peut être utilisée.

Échange de données sur les supports multimédia amovibles entre macOs et Windows

Pour l'échange de données entre les terminaux Windows et macOS, le support multimédia amovible doit impérativement être formaté à l'aide de FAT32. Les utilisateurs Mac peuvent vérifier le format de stockage du disque à l'aide de l'Utilitaire du disque.

Sur le terminal Windows, une stratégie d'échange de données **Protection des périphériques** avec **Supports amovibles** comme **Cible de protection de périphérique** comme indiqué à la section Protection des périphériques *(page 286)* ou une stratégie **Chiffrement de fichiers** avec l'espace réservé **<Amovibles>** comme **Chemin** est requise.

La stratégie d'échange de données vous permet de laisser à l'utilisateur la liberté de décider s'il veut chiffrer les données ou pas et de mémoriser ce paramètre à l'aide d'un paramètre de stratégie. Ce paramètre de stratégie est uniquement évalué sur les machines Windows. S'il utilise les supports multimédia amovibles sur un Mac et revient sur son terminal Windows, il sera invité une nouvelle fois à faire un choix. La phrase secrète des supports multimédia est uniquement disponible sur Windows.

Bon usage :

La définition d'un type de stratégie **Chiffrement de fichiers** peut être un meilleur choix car vous pouvez utiliser une seule stratégie pour les terminaux Macs et Windows.

Sous Windows, les utilisateurs n'ont pas la possibilité de décider si les supports multimédia amovibles doivent être chiffrés ou pas car l'option **L'utilisateur est autorisé à décider de l'opération de chiffrement** n'est pas disponible dans les stratégies **Chiffrement de fichiers**.

Sur les supports amovibles en lecture seule (par exemple ; les cartes SD protégées en écriture), les points de montage sécurisés ne peuvent pas être créés correctement. En pratique, utilisez uniquement les supports amovibles sur lesquels vous avez les droits en lecture et en écriture.

5.4 Résolution des problèmes

5.4.1 Réinitialisation en cas d'oubli du mot de passe

Remarque : Ces instructions supposent que l'utilisateur a installé SafeGuard Disk Encryption et SafeGuard File Encryption ou Synchronized Encryption sur son Mac. S'il utilise uniquement l'un des logiciels ci-dessus, les étapes à suivre peuvent être différentes.

Si un utilisateur oublie son mot de passe de connexion à macOS, procédez de la manière suivante :

1. Demandez à l'utilisateur d'ouvrir la boîte de dialogue de connexion et cliquez sur **?**.
   L'indice de mot de passe apparaît et l'utilisateur est invité à réinitialiser son mot de passe avec la clé de récupération.

2. Demandez à l'utilisateur de cliquer sur le triangle se trouvant à côté du message afin de passer à l'étape suivante.

3. Dans SafeGuard Management Center, sélectionnez **OutilsRécupération** pour afficher la clé de récupération de la machine spécifique.

4. Communiquez à l'utilisateur la clé de récupération à saisir sur la boîte de dialogue de connexion.
   La clé de récupération est remplacée dès sa première utilisation pour démarrer le système.
   La nouvelle clé de récupération est générée automatiquement et envoyée au serveur backend SafeGuard Enterprise sur lequel elle va être archivée et mise à disposition pour la prochaine opération de récupération.

5. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs** et supprimez le certificat de l'utilisateur.

6. Pour les utilisateurs locaux, effectuez les opérations suivantes :
   a. Demandez à l'utilisateur de créer un nouveau mot de passer et un indice de mot de passe.
   b. Dans SafeGuard Management Center, sélectionnez **Utilisateurs et ordinateurs > .Utilisateurs non confirmés** et confirmez l'utilisateur.

c. Demandez à l’utilisateur d’ouvrir l’onglet **Serveur** dans la Fenêtre de préférences et de cliquer sur **Synchroniser**.

7. Pour les utilisateurs Active Directory, effectuez les opérations suivantes :
   a. Réinitialisez le mot de passe déjà existant dans votre environnement d’administration des utilisateurs et générez un mot de passe préliminaire. Sélectionnez l’option correspondante pour obliger l’utilisateur à modifier son mot de passe après sa première connexion.
   b. Contactez l’utilisateur et communiquez lui son mot de passe préliminaire.
   c. Demandez à l’utilisateur de cliquer sur **Annuler** dans la boîte de dialogue **Réinitialisation du mot de passe** et de saisir le mot de passe préliminaire.
   d. Demandez à l’utilisateur de créer un nouveau mot de passer et un indice de mot de passe et de cliquer sur **Réinitialiser le mot de passe**.

8. Demandez à l’utilisateur de cliquer sur **Créer un nouveau jeu de clés** dans la boîte de dialogue suivante.

9. Demandez à l’utilisateur de saisir le nouveau mot de passe afin de créer le certificat d’utilisateur SafeGuard.

Les clés de l’utilisateur vont être chargées automatiquement dans le nouveau jeu de clés afin que tous les documents soient accessibles comme auparavant.

Remarque : Veuillez uniquement communiquer la clé de récupération à une personne de confiance. En effet, une clé de récupération est toujours spécifique à une machine et pas à un utilisateur. Assurez-vous que la clé de récupération n’est pas utilisée pour accéder de manière non autorisée aux données sensibles d’un autre utilisateur sur la même machine.

5.4.2 Problèmes d'accès aux données

Un utilisateur peut rencontrer des problèmes d'accès aux données pour les raisons suivantes :

- L'utilisateur n'a pas encore été confirmé.

  Retrouvez plus de renseignements sur les utilisateurs non confirmés à la section Authentification renforcée : le groupe .Utilisateurs non confirmés *(page 107)*.

  Remarque : Les utilisateurs locaux sont toujours des utilisateurs non confirmés.

- L'utilisateur n'a pas la clé nécessaire dans son jeu de clés.

  Retrouvez plus de renseignements sur l’assignation de clés aux utilisateurs à la section Assignation de clés dans Utilisateurs et ordinateurs *(page 176)*.

- Les clés ont été temporairement révoquées pour des raisons de sécurité. Le terminal est considéré comme compromis.

5.4.3 Problèmes d'utilisation des machines virtuelles

Les applications de virtualisation telles que VMware Fusion ou Parallels ne peuvent pas être utilisées avec un point de montage SafeGuard Enterprise. Nous vous conseillons de démarrer la machine virtuelle à partir d'un dossier caché.

Exemple :

Plutôt que de démarrer la machine virtuelle à partir de `~/Documents/Virtual Machines/`, utilisez le chemin `~/.sophos_safeguard_documents/Virtual Machines`.

5.4.4 Fichiers récupérés par SafeGuard

Dans certaines circonstances, un dossier nommé **Fichiers récupérés par Sophos SafeGuard** peut être présent dans un dossier. Ceci arrive si SafeGuard File Encryption essaye de créer un nouveau Dossier sécurisé (point de montage) et que le dossier caché qui doit être créé pour le stockage du contenu chiffré (par exemple /Utilisateurs/admin/.sophos_safeguard_Documents/) existe déjà et contient des fichiers. Le contenu du dossier d'origine (par exemple /Utilisateurs/admin/Documents) est donc déplacé dans le dossier **Fichiers récupérés par Sophos SafeGuard** et seul le contenu du dossier caché est affiché comme d'habitude.

5.4.5 Token sécurisé manquant

Les utilisateurs sans token sécurisé ne peuvent pas activer FileVault.

Si un utilisateur se connecte sans token sécurisé et que la stratégie exige l'activation de FileVault, un message apparaît indiquant que FileVault ne peut pas être activé en raison de l'absence d'un token sécurisé. L'utilisateur est invité à contacter l'administrateur système.

Retrouvez plus de renseignements sur la résolution de ce problème dans l'article 128052 de la base de connaissances Sophos.

5.5 Données d'inventaire et d'état des Mac

Pour les Macs, l'**Inventaire** fournit les données suivantes sur chaque machine. Les données affichées peuvent varier selon le produit Sophos installé :

- Le nom du Mac
- Le système d'exploitation
- Le type de l'authentification au démarrage
- Le nombre de lecteurs chiffrés
- Le nombre de lecteurs déchiffrés
- Le dernier contact du serveur
- La date de modification
- Si le certificat d'entreprise en cours est utilisé ou non

5.6 Désinstallation du Chiffrement de périphériques des terminaux Mac

Si vous devez désinstaller le logiciel à partir d’un ordinateur client, procédez de la manière suivante :

1. Sur le client Mac, allez dans */Bibliothèque*.
2. Sélectionnez le dossier */Sophos SafeGuard DE*.
3. Sélectionnez et cliquez deux fois sur le fichier *Sophos SafeGuard DE Uninstaller.pkg*
4. Un assistant vous guide tout au long de la désinstallation.

Dès que le dernier produit Sophos SafeGuard est supprimé, la configuration du client l’est également.

Il n’est pas nécessaire de déchiffrer le disque avant de désinstaller le logiciel.

Tout utilisateur avec les droits administratifs sera en mesure de désinstaller le logiciel. (Une règle empêchant d’effectuer cette opération sur les clients Windows n’a aucun effet sur les clients Mac).

Le package du programme de désinstallation est signé et macOS va essayer de valider cette signature. Cette procédure peut prendre plusieurs minutes.

5.7 Désinstallation du Chiffrement de fichiers des terminaux Mac

Si vous devez désinstaller le logiciel à partir d'un ordinateur client, procédez de la manière suivante :

1. Sur le client Mac, allez dans */Bibliothèque*.
2. Ouvrez le dossier *Sophos SafeGuard FS*.
3. Sélectionnez et cliquez deux fois sur le fichier *Sophos SafeGuard FS Uninstaller.pkg*
4. Un assistant vous guide tout au long de la désinstallation.
5. Redémarrez le système avant de continuer à utiliser votre Mac.

Dès que le dernier produit Sophos SafeGuard est supprimé, la configuration du client l'est également.

Remarque : Le package du programme de désinstallation est signé et macOS va essayer de valider cette signature. Cette procédure peut prendre plusieurs minutes.

6. Synchronized Encryption

Cette section s’applique à Windows et macOS. Lorsque les informations concernent uniquement l’une des plates-formes, ceci sera clairement indiqué.

Modules

- **Chiffrement de fichiers à base d’application**

  SafeGuard Enterprise Synchronized Encryption chiffre tous les fichiers créés par une application indiquée dans une stratégie quel que soit l’emplacement du fichier. Pour ces applications, le chiffrement est automatique. Elles sont également appelées Apps intégrées.

  Si, par exemple, vous indiquez que Microsoft Word est une application sur laquelle le chiffrement de fichiers est activé, tous les fichiers que vous créez et/ou enregistrez avec Microsoft Word sont automatiquement chiffrés. Toute personne dont le jeu de clés contient la clé utilisée pour chiffrer le fichier peut y accéder.

  Par défaut, SafeGuard Enterprise chiffre les fichiers avec la clé Synchronized Encryption comme indiqué à la section Clé Synchronized Encryption *(page 415)*.

De plus, vous pouvez :

- Définir les emplacement sur lesquels une autre clé que la **Clé Synchronized Encryption** est utilisée pour le chiffrement, comme par exemple, la **Clé personnelle**.

- Exclure des dossiers du chiffrement.

- Utiliser uniquement des emplacements définis sur lesquels des applications définies chiffrent leurs données.

- **Complément Outlook pour Windows**

  Pour rendre les choses plus simples à l’utilisateur, Synchronized Encryption inclut un complément Outlook qui détecte automatiquement l’envoi d’emails avec pièce jointe à l’extérieur de l’entreprise. Il demandera ensuite à l’utilisateur quelle option il souhaite utiliser (**Protégé par mot de passe**, **Non protégé**). Si nécessaire, l’utilisateur peut créer un mot de passe dans la boîte de dialogue affichée. Vous avez également la possibilité d’utiliser une

stratégie pour définir l’action par défaut à effectuer automatiquement sans intervention de l’utilisateur.

- **Intégration à Sophos Central Endpoint Protection - Supprimer les clés des machines compromises**

  Sophos Central Endpoint Protection permet de supprimer les clés automatiquement en cas de détection d’une activité malveillante sur les terminaux.

  Cette fonction est uniquement disponible si vous utilisez Sophos Central Endpoint Protection avec SafeGuard Enterprise.

- **Partage du jeu de clés entre SafeGuard Enterprise et Sophos Mobile**

  Les clés de chiffrement du jeu de clés SafeGuard Enterprise peuvent être mises à disposition dans l’app Sophos Secure Workspace (SSW) administrée par Sophos Mobile. Les utilisateurs de l’app peuvent alors utiliser les clés pour déchiffrer et consulter les documents ou pour chiffrer des documents. Ces fichiers peuvent être partagés en toute sécurité entre tous les utilisateurs de SafeGuard Enterprise et de Sophos Secure Workspace.

6.1 Bon usage : support multi-clés pour Synchronized Encryption

SafeGuard Enterprise vous permet de configurer des clés de chiffrement supplémentaires pour des emplacements spécifiques lors de l’utilisation de Synchronized Encryption.

Retrouvez ci-dessous des instructions en contexte :

- Votre entreprise a sélectionné **Par application (Synchronized Encryption)** pour chiffrer tous les fichiers créés par des applications usuelles avec la **clé Synchronized Encryption**.
- Les fichiers sont chiffrés dans le dossier Documents des utilisateurs avec leur **Clé personnelle**.
  - Le dossier Documents des utilisateurs doit contenir le dossier /unencrypted dans lequel les utilisateurs peuvent conserver leurs fichiers non chiffrés.
- Pour garantir que tous les fichiers sur les terminaux sont chiffrés conformément à la stratégie de sécurité de votre entreprise, veuillez activer le chiffrement initial.

6.1.1 Création d’une stratégie de chiffrement de fichiers à plusieurs clés

1. Dans SafeGuard Management Center, sélectionnez la stratégie **Chiffrement de fichiers (par défaut)** et sélectionnez **Par application (Synchronized Encryption)** sous **Type de chiffrement**.

2. Sous **Liste d'application**, sélectionnez **Modèle**.
   La liste d'application par défaut est appelée **Modèle**. Elle contient les applications les plus communément utilisées.

3. Sous **Portée du chiffrement**, sélectionnez **Partout**. Il s'agit de l'option la plus sûre généralement utilisée sur les terminaux Windows.
   Une règle de chiffrement des fichiers sur tous les emplacements va être créée à l'aide de la **Clé Synchronized Encryption**. Cette règle est ajoutée à la liste des emplacements sur lesquels le chiffrement par application est appliqué.

   Vous pouvez à présent ajouter des règles spécifiques pour les emplacements que vous voulez chiffrer avec d'autres clés de chiffrement. Ces emplacements peuvent être locaux ou sur le réseau. Vous pouvez utiliser des valeurs prédéfinies pour les indiquer.

   Dans notre exemple, nous voulons chiffrer le dossier Documents des utilisateurs.

4. Pour ajouter une règle, cliquez sur le champ de modification du **Chemin** et sélectionnez **<Documents>** dans le menu déroulant.

   Remarque : Vous ne pouvez pas modifier la portée du chiffrement.

   La **Clé Synchronized Encryption** est utilisée par défaut mais vous pouvez choisir une autre clé de chiffrement. Par exemple, la clé de domaine ou la clé d'une unité organisationnelle. Vous pouvez également sélectionner la **Clé personnelle** qui est unique à chaque utilisateur.

5. Cliquez sur le symbole de la **Clé personnelle** dans le champ **Clé** pour sélectionner les clés personnelles des utilisateurs et chiffrer le dossier Documents. Vous pouvez placer le curseur de la souris sur les symboles de clé pour afficher leur fonction.

   Pour utiliser un dossier non chiffré, vous devez définir une règle d'exception pour ce dossier spécifique.

6. Cliquez sur le champ **Chemin** et sélectionnez **<Documents>** dans le menu déroulant. Saisissez \unencrypted après l'espace réservé **<Documents>**.

7. Dans la colonne **Mode**, sélectionnez **Exclure** dans le menu déroulant.

8. Pour activer le chiffrement initial sur les terminaux, paramétrez l'option **Sur les disques locaux** sous **Chiffrement initial : chiffrer automatiquement les fichiers existants** sur **Oui**.

9. Enregistrez la stratégie et déployez-la.

Remarque : Lorsque vous assignez une stratégie, avec des règles spécifiques pour les emplacements et des clés différentes, aux terminaux sur lesquels SafeGuard Enterprise 8.0 est installé, ces règles s'appliquent correctement. Tous les emplacements indiqués sont chiffrés avec les clés sélectionnées. Toutefois, si une règle dont la **Portée du chiffrement** est définie sur **Partout** fait partie de la stratégie, seule la **Clé Synchronized Encryption** est utilisée. Les fichiers dans les emplacements spécifiques sont également chiffrés avec la **Clé Synchronized Encryption**.

6.2 Configuration requise

Pour pouvoir utiliser les fonctions de Synchronized Encryption, les conditions suivantes doivent être remplies :

- Le serveur et la base de données SafeGuard Enterprise ainsi que la console SafeGuard Management Center doivent être configurés correctement.
- Le composant **Synchronized Encryption** doit être installé sur les terminaux Windows tandis que **SafeGuard File Encryption** doit être installé sur les terminaux macOS.
    - Sur les terminaux Windows, Synchronized Encryption remplace tous les autres modules de SafeGuard Enterprise File Encryption. Il ne peut pas être installé en plus des modules Data Exchange, File Encryption ou Cloud Storage. Les stratégies de chiffrement de fichiers utilisées par ces modules de chiffrement par emplacement sont incompatibles avec les nouvelles stratégies de chiffrement Synchronized Encryption par application. Si vous procédez à la migration du module SafeGuard Enterprise File Encryption vers le module Synchronized Encryption et que vous conservez les stratégies de chiffrement par emplacement, le RSOP (série obtenue de stratégies) dans SafeGuard Management Center continuera à afficher les deux. En revanche, seule la stratégie de chiffrement par application sera valable. En effet, le calcul RSOP ne prend pas en compte les modules installés sur un terminal.
    - Le module Synchronized Encryption est incompatible avec SafeGuard LAN Crypt.

- Pour activer les fonctions dont vous avez besoin, procédez de la manière suivante :
    - Créez une liste d'application.
    - Créez des stratégies de chiffrement de fichiers par application (Synchronized Encryption).
    - Créez des stratégies pour activer le complément Outlook (chiffre les pièces jointes d'email conformément aux paramètres de la stratégie).
    - Créez des stratégies pour activer l'intégration à Sophos Endpoint Protection (suppression de clés en cas de détection d'une activité malveillante sur les terminaux).
    - Configurez le partage du jeu de clés SafeGuard Enterprise avec les appareils mobiles administrés par Sophos Mobile.
    - Déployez les stratégies.

Seules les stratégies d’utilisateur sont appliquées sur les Macs. Les stratégies d’ordinateur sont ignorées.

6.2.1 Installation des terminaux

Exécutez le programme d’installation du client correspondant à votre plate-forme :

- Sur les terminaux Windows, sélectionnez le composant **Synchronized Encryption**.
- Sur les Macs, installez **SafeGuard File Encryption**.

6.2.2 Mise à niveau des terminaux

- **Windows**

  pour mettre à niveau les terminaux à partir de la version 8.0 de SafeGuard Enterprise et installer le module Synchronized Encryption, veuillez exécuter le programme d’installation du client correspondant à votre plate-forme et suivez les instructions à l’écran. Cette opération met à niveau les modules installés à la version 8.30. Pour installer le module Synchronized Encryption, veuillez recommencer l’installation en sélectionnant **Changer** dans la boîte de dialogue **Changer, réparer ou supprimer l’installation** et en sélectionnant **Synchronized Encryption**. S’il est déjà installé, supprimez tout chiffrement de fichiers par emplacement.
- **macOS**

  exécutez le programme d’installation du client et suivez les instructions à l’écran.

6.2.3 Migration à partir du module de Chiffrement de fichiers sur Windows

Les utilisateurs peuvent migrer du module SafeGuard Enterprise File Encryption au module Synchronized Encryption. Les fichiers chiffrés demeurent chiffrés et accessibles. Les fichiers sont modifiés et enregistrés après l’opération de migration et sont chiffrés de nouveau avec la clé Synchronized Encryption. Le paramétrage d’un chiffrement initial dans la stratégie permet de chiffrer de nouveau les fichiers avec la clé Synchronized Encryption.

Conditions préalables

Veuillez-vous assurer que toutes les clés requises (anciennes clés utilisées pour le chiffrement de fichiers avec l’ancien module de **Chiffrement de fichiers** et la nouvelle clé Synchronized Encryption) sont disponibles sur les jeux de clés des utilisateurs.

- Si nécessaire, vous pouvez assigner les clés aux utilisateurs dans SafeGuard Management Center.
- Si nécessaire, les utilisateurs doivent importer les clés locales sur leur jeu de clés sur les terminaux. Retrouvez plus de renseignements à la section *Importation des clés à partir d'un fichier* dans le Manuel d'utilisation de SafeGuard Enterprise. Les clés locales seront ensuite disponibles dans SafeGuard Management Center. Elles peuvent être assignées aux utilisateurs comme prévu.

Opération de migration

Veuillez suivre les étapes ci-dessous :

1. Installez le module Synchronized Encryption sur les terminaux. Le module remplace le module de Chiffrement de fichiers existant.
2. Assurez-vous que toutes les clés disponibles sur les jeux de clés des utilisateurs qui se servaient du Chiffrement de fichiers soient toujours disponibles dans leurs jeux de clés. De cette manière, les utilisateurs ont accès aux fichiers qui sont déjà chiffrés à l'aide de Synchronized Encryption.
3. Dans SafeGuard Management Center, créez les nouvelles stratégies Synchronized Encryption.
    - Toutes les applications en mesure d'accéder aux fichiers chiffrés doivent figurer sur la **Liste d'application** utilisée dans les stratégies Synchronized Encryption.
    - La **Portée du chiffrement** des stratégies Synchronized Encryption doit être la même que celle définie dans les stratégies de chiffrement de fichiers par emplacement.
    - Indiquez les paramètres du chiffrement initial. Le chiffrement initial démarre immédiatement après l'application de la stratégie sur le terminal. Il chiffre ou chiffre de nouveau tous les fichiers à l'aide de la clé Synchronized Encryption. De cette manière, tous les fichiers sont chiffrés conformément aux stratégies en vigueur.

      Remarque : Le chiffrement initial peut également être déclenché à partir du menu contextuel de l'Explorateur Windows (**Chiffrement de fichiers SafeGuard > Chiffrer en fonction de la stratégie**).
4. Déployez les stratégies.

Résultat

- Les fichiers chiffrés faisant l'objet de stratégies Synchronized Encryption sont de nouveau chiffrés avec la clé Synchronized Encryption.

- Les fichiers créés ou modifiés par les applications figurant dans la liste d'application Synchronized Encryption sont chiffrés avec la clé Synchronized Encryption.

- Les fichiers chiffrés ne faisant pas l'objet de stratégies Synchronized Encryption demeurent chiffrés avec l'ancienne clé de Chiffrement des fichiers. Les utilisateurs qui ont la clé requise sur leur jeu de clés peuvent toujours déchiffrer les fichiers manuellement, même si les fichiers ne font plus l'objet des stratégies de chiffrement.

6.2.4 Migration à partir du module de Chiffrement de fichiers sur macOS

Les terminaux macOS sur lesquels est installé Sophos SafeGuard Enterprise sont en mesure de traiter les stratégies de chiffrement **Par application (Synchronized Encryption)** et les stratégies de chiffrement des fichiers **Par emplacement**. Selon les stratégies reçues, les terminaux utilisent soit Synchronized Encryption, soit le Chiffrement de fichiers.

Si vous procédez à la mise à niveau à partir de la version 7, les terminaux continuent à fonctionner en mode de Chiffrement de fichiers par emplacement comme dans la version précédente.

Pour passer au mode de chiffrement par application de Synchronized Encryption, procédez de la manière suivante :

Opération de migration

1. Dans SafeGuard Management Center, créez les nouvelles stratégies Synchronized Encryption.
   - Toutes les applications en mesure d'accéder aux fichiers chiffrés doivent figurer sur la **Liste d'application** utilisée dans les stratégies Synchronized Encryption.
   - La **Portée du chiffrement** des stratégies Synchronized Encryption doit être la même que celle définie dans les stratégies de chiffrement de fichiers par emplacement.
   - Indiquez les paramètres du chiffrement initial. Le chiffrement initial démarre immédiatement après l'application de la stratégie sur le terminal. Il chiffre ou chiffre de nouveau tous les fichiers à l'aide de la clé Synchronized Encryption. De cette manière, tous les fichiers sont chiffrés conformément aux stratégies en vigueur.

     Remarque : Les utilisateurs peuvent également démarrer le chiffrement initial à partir de l'onglet **Stratégies** du volet de préférences (**Appliquer toutes les stratégies**) ou exécutez la commande du Terminal pour le chiffrement initial.
2. Déployez les stratégies.
3. Lorsque les utilisateurs reçoivent les stratégies, ils sont invités à se déconnecter et à se reconnecter.

Résultat

- Les fichiers chiffrés faisant l’objet de stratégies Synchronized Encryption sont de nouveau chiffrés avec la clé Synchronized Encryption.

- Les fichiers créés ou modifiés par les applications figurant dans la liste d’application Synchronized Encryption sont chiffrés avec la clé Synchronized Encryption.

- Les fichiers chiffrés ne faisant pas l’objet de stratégies Synchronized Encryption demeurent chiffrés avec la clé de Chiffrement des fichiers. Les utilisateurs qui ont la clé requise sur leur jeu de clés peuvent toujours déchiffrer les fichiers manuellement, même si les fichiers ne font plus l’objet des stratégies de chiffrement.

6.2.5 Déploiement partiel de Synchronized Encryption

Dans le cas d’un déploiement partiel de SafeGuard Enterprise Synchronized Encryption, veuillez-vous assurer que tous vos utilisateurs ont accès aux données chiffrées partagées.

Si vous voulez activer le chiffrement dans votre entreprise de manière progressive, vous pouvez, par exemple, commencer à déployer les stratégies Synchronized Encryption avec le chiffrement activé sur les terminaux de votre service *Marketing* uniquement. Ces terminaux chiffreront les fichiers conformément aux stratégies Synchronized Encryption. Les terminaux des utilisateurs de vos autres services ne seront pas en mesure d'accéder à ces fichiers puisque les stratégies Synchronized Encryption ne leur sont pas appliquées. Pour éviter cette situation, déployez des stratégies en lecture seule qui autoriseront l'accès en lecture aux fichiers chiffrés. Ces terminaux ne chiffrent aucune donnée mais sont en mesure de lire les fichiers chiffrés.

Condition préalable :

- Le serveur et la base de données SafeGuard Enterprise ainsi que la console SafeGuard Management Center doivent être configurés correctement.
- Le module Synchronized Encryption est installé sur **tous** les terminaux et se connecte à SafeGuard Management Center (le package de configuration est installé).

- Vous avez créé une liste d'application et une stratégie Synchronized Encryption pour les terminaux sur lesquels les données doivent être chiffrées.

6.2.5.1 Déploiement partiel progressif

1. Créez une stratégie Synchronized Encryption (chiffrement par application) dans SafeGuard Management Center.

2. Déployez la stratégie sur les terminaux des utilisateurs sur lesquels les données doivent être chiffrées. Dans l'exemple ci-dessus, il s'agit des terminaux du service *Marketing*.

3. Créez des stratégies en lecture seule.

   Remarque : Vous devez créer des stratégies distinctes pour les terminaux Windows et Mac.

4. Déployez les stratégies en lecture seule sur tous les terminaux Windows et Mac. Dans l'exemple ci-dessus, il s'agit de tous terminaux à l'exception de ceux du service *Marketing*.

6.2.5.2 Création d'une stratégie de lecture seule pour les terminaux Windows

1. Dans SafeGuard Management Center, allez dans **Stratégies**.

2. Cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis cliquez sur **Nouveau** et sur **Chiffrement de fichiers**.

3. Saisissez un nom pour la nouvelle stratégie et cliquez sur **OK**.

4. Sur l'onglet **Chiffrement de fichiers**, sélectionnez **Par application (Synchronized Encryption)** dans la liste déroulante **Type de chiffrement**.
   Les options **Liste d'application** et **Portée du chiffrement** apparaissent.

5. Sélectionnez la **Liste d'application** que vous avez créée dans la liste déroulante.

6. Dans la liste déroulante **Portée du chiffrement**, sélectionnez **Emplacements définis**.

7. Lorsque vous quittez l'onglet **Chiffrement de fichiers**, le système vous demande si vous voulez enregistrer vos modifications.

8. Cliquez sur **Oui**.

9. Dans **Utilisateurs et ordinateurs**, assignez et activez la nouvelle stratégie aux utilisateurs de terminaux Windows qui devraient être autorisés à lire les données chiffrées mais pas à chiffrer les données.

   Remarque : Cette stratégie ne doit pas être assignée aux terminaux macOS. Il vous suffit simplement d’activer la stratégie uniquement pour les .**Ordinateurs authentifiés**. En effet, les terminaux macOS interprètent uniquement les paramètres de l'utilisateur. Faites glisser le groupe **.Utilisateurs authentifiés** de la zone d'activation des stratégies à la liste **Groupes disponibles**.

6.2.5.3 Création d’une stratégie de lecture seule pour les terminaux Mac

1. Dans SafeGuard Management Center, allez dans **Stratégies**.
2. Cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis cliquez sur **Nouveau** et sur **Chiffrement de fichiers**.
3. Saisissez un nom pour la nouvelle stratégie et cliquez sur **OK**.
4. Sur l’onglet **Chiffrement de fichiers**, sélectionnez **Par emplacement** dans la liste déroulante **Type de chiffrement**.
   La liste des chemins pour le chiffrement par emplacement apparaît.
5. Indiquez les chemins suivants et excluez-les du chiffrement.
   - Partages réseau : Utilisez l’espace réservé <Partages réseau> pour diriger vers les dossiers racine de tous les partages réseau macOS.
   - Supports amovibles : Utilisez l’espace réservé <Supports amovibles> pour diriger vers les dossiers racine de tous les supports amovibles macOS.
   - Dossier(s) de synchronisation du fournisseur Cloud : Saisissez le ou les dossiers qui seront synchronisés avec un service Cloud. Seuls les chemins locaux sont pris en charge.
   - Le chemin suivant est uniquement nécessaire si Microsoft Outlook pour Mac 2011 est utilisé :

     <Profil Utilisateur>\Library\Caches\TemporaryItems\Outlook Temp\
   - Le chemin suivant est uniquement nécessaire si Microsoft Outlook pour Mac 2016 est utilisé :

     <%RPTTMP%>\com.microsoft.Outlook\Outlook Temp\
   - Les chemins suivants sont uniquement nécessaires si Apple Mail est utilisé :

     <Profil Utilisateur>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads\

     <%RPTDIR%>\com.apple.mail\com.apple.mail\
6. Assurez-vous que tous les chemins sont exclus du chiffrement : **Exclure** est sélectionné dans la colonne **Mode** pour chaque chemin.
7. Lorsque vous quittez l’onglet **Chiffrement de fichiers**, le système vous demande si vous voulez enregistrer vos modifications.
8. Cliquez sur **Oui**.
9. Dans **Utilisateurs et ordinateurs**, assignez la nouvelle stratégie aux utilisateurs de terminaux Mac qui devraient être autorisés à lire les données chiffrées mais pas à les chiffrer.

6.3 Chiffrement des données

SafeGuard Enterprise Synchronized Encryption intègre un module de chiffrement de fichiers polyvalent. SafeGuard Synchronized Encryption vous permet de chiffrer les données sensibles selon l'application avec laquelle elles ont été créées ou modifiées. Ce chiffrement étant permanent, vos données sont sécurisées même lorsqu'elles sont déplacées dans un autre emplacement, téléchargées chez un fournisseur de stockage Cloud ou envoyées par email. Selon les paramètres de stratégie, certains types de fichiers sont généralement chiffrés automatiquement. Toutefois, dans certains cas, il pourrait être nécessaire de déchiffrer ou de chiffrer chaque fichier manuellement. Dans l'Explorateur Windows et dans le Finder macOS, les fichiers chiffrés sont identifiés par un verrou de couleur verte.

Retrouvez plus de renseignements sur la façon d'empêcher les utilisateurs de déchiffrer les fichiers manuellement à la section Interdiction aux utilisateurs de déchiffrer les fichiers manuellement *(page 452)*.

Chiffrer les données avec différentes clés de chiffrement

Vous pouvez spécifier l'utilisation de différentes clés pour chiffrer les fichiers à des emplacements spécifiques comme indiqué à la section Création de stratégies pour le chiffrement de fichiers par application *(page 422)*.

Stratégies

- Les stratégies Synchronized Encryption ne sont pas fusionnées. La stratégie correspondant le plus à l'objet cible (utilisateur ou ordinateur) dans la hiérarchie est toujours appliquée. La stratégie en vigueur pour un utilisateur ou un ordinateur est affichée sur l'onglet **Responsables de la sécurité** sous la vue **Utilisateurs et ordinateurs**.

Chiffrement permanent

Windows

- Lorsque vous déplacez un fichier chiffré d'un dossier chiffré vers un dossier non chiffré, le fichier demeure chiffré. Vous pouvez ouvrir ce fichier et le modifier. Lorsque vous le modifiez et l'enregistrez, le fichier demeure chiffré.

macOS

- **Déplacement de fichiers chiffrés à partir des Dossiers sécurisés**

En tant que responsable de la sécurité, vous définissez les dossiers de votre Mac à classer comme Dossiers sécurisés. Si vous utilisez Synchronized Encryption, tous les fichiers dans les Dossiers sécurisés sont automatiquement chiffrés.

Lorsque vous déplacez un fichier chiffré d'un dossier sécurisé vers un dossier non sécurisé, le fichier demeure chiffré. Vous pouvez l'ouvrir mais seul le contenu fichier sera affiché. Vous devez d'abord le déchiffrer manuellement.

Lorsque vous ouvrez un fichier chiffré dans un Dossier sécurisé et que vous l'enregistrez dans un Dossier non sécurisé, le fichier est déchiffré automatiquement.

Sauvegardes

Si vous utilisez un outil de sauvegarde tel que l'Historique des fichiers dans Windows 8.x et Windows 10 ou Time Machine dans macOS, il se peut que vous ayez des sauvegardes d'anciennes versions des fichiers que vous voulez chiffrer. Synchronized Encryption ne peut pas chiffrer ces fichiers. Veuillez supprimer ou chiffrer les sauvegardes déjà existantes et désactiver les sauvegardes automatiques.

6.3.1 Clé Synchronized Encryption

Par défaut, SafeGuard Enterprise Synchronized Encryption a recours à la clé Synchronized Encryption pour chiffrer les fichiers : `Root_Synchronized_Encryption@SGN`. Le clé est assignée automatiquement est elle est disponible pour tous les utilisateurs.

La clé Synchronized Encryption est utilisée tant que vous n'indiquez pas d'emplacements sur lesquels une autre clé doit être utilisée. Pour ces emplacements, toutes les clés disponibles peuvent être utilisées comme indiqué à la section Clés et certificats *(page 173)*.

6.3.2 Chiffrement automatique des fichiers conformément à la stratégie de chiffrement asynchrone

Pour garantir que les fichiers sont toujours chiffrés conformément à la stratégie s'appliquant à un emplacement particulier, Synchronized Encryption permet d'effectuer un chiffrement asynchrone.

Le chiffrement asynchrone est appliqué lorsque les utilisateurs effectuent les opérations suivantes :

- Copier ou déplacer des fichiers, par exemple dans l'Explorateur Windows ou dans le Finder macOS.
- Créer des fichiers dont les extensions sont spécifiées dans les **Listes d'applications** avec des applications pour lesquelles le chiffrement de fichiers n'est pas activé.

Résultats :

- Les fichiers sont copiés ou déplacés à partir d'un dossier non chiffrés dans un dossier sur lequel une règle de chiffrement s'applique.
- Les fichiers copiés ou déplacé d'un dossier chiffré vers un dossier non chiffré sont déchiffrés.

  SafeGuard Enterprise déchiffre automatiquement les fichiers si les utilisateurs mettent un ou plusieurs fichiers dans un emplacement sans chiffrement. Si les utilisateurs déplacent un dossier vers un dossier exclus du chiffrement ou s'ils renomment un dossier du même nom qu'un dossier exclus du chiffrement, les fichiers ne sont pas déchiffrés automatiquement pour éviter tout déchiffrement accidentel. Ils peuvent ensuite déchiffrer les fichiers manuellement ou utiliser l'option **Chiffrer en fonction de la stratégie** à partir du menu contextuel **Chiffrement de fichiers SafeGuard**.
- Les fichiers qui sont copiés ou déplacés d'un dossier chiffré vers un dossier sur lequel une règle de chiffrement différente s'applique sont chiffrés conformément à la règle appliquée au dossier cible.
- Lorsque les fichiers sont créés par des applications pour lesquelles le chiffrement de fichiers n'est pas activé et que l'extension du fichier est indiquée dans les **Listes d'application**, le fichier est chiffré et ne peut pas être ouvert par l'application qui l'a créé. Par exemple, si les utilisateurs créent un fichier .doc avec OpenOffice et qu'OpenOffice ne figure pas dans les **Listes d'application**.

⚠ **Important :** En cas d'interruption de la copie ou du déplacement des fichiers, en raison, par exemple du redémarrage de l'ordinateur ou si les utilisateurs ferment la boîte de dialogue ou se déconnectent de leur ordinateur ou l'éteignent, l'opération ne reprendra pas automatiquement. Par conséquent, il se peut que des fichiers ne soient pas chiffrés involontairement.

Recommandation

Pour vous assurer que les fichiers sont toujours chiffrés conformément aux stratégies de l'entreprise :

- Activez le chiffrement initial des terminaux (chiffrement local) avec une stratégie conformément aux instructions de la section Création de stratégies pour le chiffrement de fichiers par application *(page 422)*.
- Pour les partages réseau, utilisez l'outil de ligne de commande SGFileEncWizard.exe pour vérifier et rétablir l'état de chiffrement des fichiers comme indiqué à la section Chiffrement initial sur les partages réseau *(page 421)*.

Journalisation des événements du chiffrement asynchrone

Retrouvez plus de renseignements sur les événements journalisés à la section Audit *(page 225)*.

6.3.3 Listes d’application

L’utilisation du chiffrement de fichiers à base d’application nécessite la création de **Listes d’application**. Ces listes contiennent les applications dans lesquelles les fichiers sont chiffrés dès leur création ou leur enregistrement. Seules les applications figurant dans les **Listes d’application** peuvent accéder aux données chiffrées. Toutes les autres applications afficheront du contenu chiffré et illisible. SafeGuard Enterprise inclut un modèle de liste d’application que vous pouvez facilement adapté en fonction de vos besoins. Il contient les applications usuelles sur lesquelles vous pouvez utiliser le chiffrement de fichiers à base d’application. Vous pouvez choisir d’activer ou de désactiver les applications dans un groupe ou d’activer ou de désactiver le groupe tout entier.

Remarque : La création de stratégies **Par application (Synchronized Encryption)** n’est pas possible si les **Listes d’application** n’ont pas été créées auparavant.

Listes d’application pour Macs

Pour certaines applications macOS, vous devez exclure certains emplacements du chiffrement afin de garantir un fonctionnement correct. Par exemple, pour Microsoft Office 2011 `<Documents>\Microsoft User Data` doit être exclus. Ce chemin est déjà spécifié dans le modèle fourni.

6.3.3.1 Création d’une liste d’application

1. Dans SafeGuard Management Center, allez dans **Stratégies**.
2. Recherchez l’entrée **Listes d’application** dans la vue **Stratégies**.
3. Cliquez avec le bouton droit de la souris sur **Modèle** et cliquez sur **Dupliquer la liste d’application**.
   Modèle_1 apparaît.

   Vous avez également la possibilité de créer une nouvelle liste d’applications.
4. Cliquez avec le bouton droit de la souris sur *Modèle_1*, puis cliquez sur **Propriétés** et saisissez un nouveau nom.
5. Cliquez sur **OK**.
6. Cliquez sur la nouvelle liste d’application.
   Le volet de droite affiche le contenu du modèle.
7. Pour créer des **Listes d’application** pour Macs, cliquez sur l’onglet **OS X**.

8. Vérifiez la liste et désactivez les applications sur lesquelles vous ne voulez pas appliquer le chiffrement. La dessélection de la case **Active** sur la droite du champ **Nom du groupe d'applications** désactive toutes les applications du groupe. La dessélection de la case Active à droite d'une application spécifique présente dans le groupe désactive uniquement cette application.

9. Pour ajouter d'autres applications aux groupes existants :

    a. Cliquez avec le bouton droit de la souris sur le groupe auquel vous voulez ajouter une application, cliquez sur **Nouveau** puis sur **Application**.

    b. Dans le champ **Nom de l'application**, saisissez un nom pour l'application.

    c. Sous **Emplacement du processus**, indiquez le chemin en incluant le programme exécutable, par exemple ; `<Program Files>\Adobe\Reader 11.0\Reader \AcroRd32.exe`. Vous pouvez soit saisir le chemin manuellement soit utiliser les emplacements prédéfinis dans la liste déroulante.
    Vous pouvez indiquer toutes les versions d'une application sous un **Nom d'application**. Par exemple, Acrobat Reader 11.0 et Acrobat Reader DC sous **Nom d'application** : *Reader*

    d. **Extension de fichier** : Les extensions de fichier que vous indiquez ici concernent le chiffrement initial des fichiers déjà existants et le chiffrement asynchrone mais n'ont aucun impact sur le chiffrement de fichiers **Par application (Synchronized Encryption)**.
        - Chiffrement initial

          Les fichiers déjà existants couverts par la stratégie de chiffrement ne sont pas chiffrés automatiquement. Pour chiffrer ces fichiers, le chiffrement initial doit être effectué sur les terminaux. Les fichiers, dont les extensions ont été indiquées ici, seront chiffrés à l'aide de la clé Synchronized Encryption lors de l'opération de chiffrement initial. Vous pouvez saisir les extensions de fichier avec ou sans point (par exemple « .txt » ou « txt »). Les caractères de remplacement ne sont pas pris en charge.

          L'emplacement sur lequel aura lieu le chiffrement initial doit être indiqué à la création de la stratégie pour le chiffrement de fichiers **Par application (Synchronized Encryption)**. Il peut être appliqué aux disques locaux, aux périphériques amovibles et aux fournisseurs de stockage Cloud détectés automatiquement.

        - Chiffrement asynchrone

          Assurez-vous que les fichiers sont toujours chiffrés conformément à la stratégie s'appliquant à un emplacement particulier. Il est appliqué lorsque les utilisateurs vont :
            - Copier ou déplacer des fichiers, par exemple dans l'Explorateur Windows ou dans le Finder macOS.

◦ Créer des fichiers dont les extensions sont spécifiées dans les **Listes d’applications** avec des applications pour lesquelles le chiffrement de fichiers n’est pas activé.

Retrouvez plus de renseignements à la section Chiffrement automatique des fichiers conformément à la stratégie de chiffrement asynchrone *(page 415)*.

Si vous désactivez un groupe d’applications, les extensions de fichier que vous avez indiqué pour le chiffrement initial dans le groupe seront également désactivés

10. **Listes d’applications** pour macOS (onglet **OS X**) : Si nécessaire, veuillez ajouter les emplacements à exclure du chiffrement dans le tableau **Emplacement exclu** afin d’assurer un fonctionnement correct.

11. Pour ajouter d’autres groupes d’applications :
    Vous pouvez, par exemple, utiliser des groupes d’applications pour placer toutes les parties d’une suite logicielle sous un seul nœud. Ainsi, la seule désactivation du groupe suffira à désactiver toutes ces parties.
    a. Cliquez avec le bouton droit de la souris sur l’arborescence **Modèle** et cliquez sur **Nouveau** puis sur **Groupe d’applications**.
    b. Dans le champ **Nom du groupe d’applications**, saisissez un nom pour le groupe.
    c. Pour ajouter d’autres applications aux groupes :

12. Lorsque vous quittez la vue Modèle, le système vous demande si vous voulez enregistrer vos modifications. Cliquez sur **Oui**.

La nouvelle liste d’applications apparaît sous **Listes d’application** dans la vue **Stratégies**. Vous pouvez créer d’autres listes d’application et les utiliser dans différentes stratégies pour le chiffrement de fichiers par application.

⚠ **Important :** Nous vous conseillons d’ajouter toutes les applications capables de traiter les mêmes types de fichier (par exemple .docx) à la liste d’application. N’ajoutez pas d’applications partageant des données sur Internet (par exemple, les clients de messagerie ou les navigateurs).

6.3.4 Chiffrement initial

Le chiffrement initial garantit le chiffrement des nouveaux fichiers mais aussi de toutes les données déjà existantes. Les fichiers sont chiffrés conformément aux stratégies de l’entreprise. Ceci permet d’éviter que les données de l’entreprise demeurent déchiffrées involontairement.

Le chiffrement initial traite les fichiers en fonction des :

- Extensions de fichier indiquées dans les **Listes d’application**. Retrouvez plus de renseignements à la section Création d’une liste d’application *(page 417)*.

- Paramètres indiqués dans les stratégies Synchronized Encryption. Retrouvez plus de renseignements à la section Création de stratégies pour le chiffrement de fichiers par application *(page 422)*.

Il peut être déclenché automatiquement par un paramètre de stratégie ou manuellement par les utilisateurs. Il est appliqué sur tous les emplacements définis dans la stratégie.

Remarque : Le chiffrement initial sur les partages réseau peut uniquement être exécuté à l'aide de l'outil de ligne de commande SGFileEncWizard.exe. Retrouvez plus de renseignements à la section Chiffrement initial sur les partages réseau *(page 421)*.

En cas de déclenchement automatique, le chiffrement initial s'exécute en tâche de fond. Lorsque l'opération est terminée, un événement est consigné dans le journal.

En cas de nécessité de traiter une grande quantité de données, le chiffrement initial peut affecter les performances des terminaux.

Le chiffrement initial commence dès que l'un de ces événements se produit :

- Un utilisateur se connecte.
- Une nouvelle stratégie ou une stratégie mise à jour est appliquée au terminal
- Un support amovible est connecté
- Un point de montage est créé (macOS)

Le chiffrement initial procède comme suit :

- Les fichiers en clair sont chiffrés conformément aux paramètres de la stratégie.
- Les fichiers chiffrés avec une autre clé que celle définie dans la stratégie sont de nouveau chiffrés avec la clé définie dans la stratégie. Ceci à condition que les deux clés se trouvent sur le jeu de clés de l'utilisateur.
- Les fichiers chiffrés avec une clé non disponible dans le jeu de clés de l'utilisateur demeurent inchangés.
- Les fichiers chiffrés ne sont jamais déchiffrés.

Sur Windows, les utilisateurs peuvent démarrer manuellement le chiffrement initial en cliquant avec le bouton droit de la souris sur le nœud **Ce PC** dans l'Explorateur Windows et en sélectionnant **Chiffrement de fichiers SafeGuard > Chiffrer en fonction de la stratégie**. L'assistant SafeGuard File Encryption affiche des informations sur la quantité de données à traiter, la progression et les résultats de l'opération.

Sur les Macs, les utilisateurs ouvrent les **Préférences Système** et cliquent sur l'icône Sophos SafeGuard, puis ils sélectionnent l'onglet **Stratégies** et passent à la vue **Chemin converti localement** puis cliquent sur **Appliquer toutes les stratégies**.

6.3.4.1 Chiffrement initial sur les partages réseau

Le chiffrement initial ne peut pas être déclenché automatiquement à l'aide d'un paramètre de stratégie sur les partages réseau. En tant que responsable de la sécurité, vous pouvez lancer le chiffrement initial des partages réseau à partir d'un ordinateur sur lequel SafeGuard Enterprise est installé et qui a accès à ces partages à l'aide de la ligne de commande SGFileEncWizard.exe.

Sur un ordinateur sur lequel SafeGuard Enterprise est installé, l'utilitaire se trouve sous `<SYSTÈME>:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\`

Avant de lancer le chiffrement initial sur les partages réseau, veuillez prendre en compte ce qui suit :

- Cette opération peut entraîner des problèmes pour les utilisateurs de terminaux sur lesquels le module Synchronized Encryption n'est pas installé ou sur lesquels aucune stratégie Synchronized Encryption n'est appliquée. Ces utilisateurs ne peuvent pas déchiffrer les fichiers chiffrés à l'aide de Synchronized Encryption. Assurez-vous que les utilisateurs des terminaux censés pouvoir accéder à ces fichiers ont bien installé le module Synchronized Encryption et qu'une stratégie est bien appliquée sur ces terminaux.
- Si vous voulez chiffrer de nouveau les fichiers sur les partages réseau déjà chiffrés, vous devez avoir toutes les clés qui ont été utilisées pour chiffrer ces fichiers sur votre jeu de clés lorsque vous déclenchez le chiffrement initial. Les fichiers pour lesquels vous n'avez pas de clé demeurent chiffrer avec « l'ancienne » clé.

Conditions requises au chiffrement initial des partages réseau

- Le chiffrement initial doit être effectué sur un ordinateur sur lequel le logiciel SafeGuard Enterprise est installé.
- Le terminal doit avoir accès à tous les partages réseau à chiffrer.
- Une stratégie Synchronized Encryption couvrant tous les partages réseau à chiffrer doit être appliquée sur le terminal.
- Toutes les clés utilisées pour chiffrer les fichiers déjà existants dans les partages réseau doivent être disponibles sur votre jeu de clés.

Chiffrement initial avec SGFileEncWizard

Vous pouvez appeler SGFileEncWizard.exe avec les paramètres suivants :

SGFileEncWizard.exe [<chemindémarrage>] [%POLICY] [/V0 | /V1 | /V2 | /V3] [/X] [/L<fichierjournal>]

- <chemindémarrage> : traite les chemins indiqués ainsi que leurs sous-dossiers. Veuillez séparer les différents chemins par un espace.

Remarque : Pour procéder au chiffrement initial des partages réseau, veuillez indiquer explicitement chaque partage réseau à chiffrer. Seuls ces chemins seront traités. Indiquez les chemins dans la notation UNC afin d'éviter tous problèmes avec les différentes lettres de lecteur des partages réseau mappés. Seuls les chemins absolus sont autorisés.

- **%POLICY** : appliquez la stratégie Synchronized Encryption aux chemins indiqués et chiffrez de nouveau les fichiers si nécessaire. La stratégie appliquée au terminal sur lequel est exécuté SGFileEncWizard.exe est utilisée.

  Remarque : Ce paramètre peut être ignoré pour le chiffrement initial des partages réseau.

- Paramètre /V0 : ne pas signaler de messages.
- Paramètre /V1 : consigner uniquement les erreurs dans le journal.
- Paramètre /V2 : consigner les fichiers modifiés dans le journal.
- Paramètre /V3 : consigner tous les fichiers traités dans le journal.
- Paramètre /L<chemin+fichierjournal> : écrire la sortie dans le fichier journal indiqué.
- Paramètre /X : masquer la fenêtre de l'assistant.

Exemple :

SGFileEncWizard.exe \\mon-filer-1\data1\utilisateurs \\mon-filer-1\data2 %POLICY /V3 /X /LC:\Journal\monfichierjournal.xml

Le chiffrement initial est effectué sur les fichiers dans \\mon-filer-1\data1\utilisateurs et dans \\mon-filer-1\data2. L'assistant ne s'ouvre pas et les informations concernant tous les fichiers traités sont consignées dans monfichierjournal.xml.

6.3.5 Création de stratégies pour le chiffrement de fichiers par application

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Chiffrement de fichiers**.

L’onglet **Chiffrement de fichiers** apparaît.

2. Sélectionnez **Par application (Synchronized Encryption)** dans la liste déroulante **Type de chiffrement**.
   Les options **Liste d’application** et **Portée du chiffrement** apparaissent.

   Retrouvez plus de renseignements sur le type de chiffrement **Aucun chiffrement** à la section Stratégies de type Aucun chiffrement *(page 133)*.

3. Dans la liste déroulante, sélectionnez la **Liste d’application**que vous avez créée auparavant.

4. Dans la liste déroulante **Portée du chiffrement**, sélectionnez l’une des options suivantes :

   - **Partout** : le chiffrement est appliqué au lecteurs locaux, amovibles, de stockage dans le Cloud et réseau.

     Une règle de chiffrement des fichiers sur tous les emplacements va être créée à l’aide de la **Clé Synchronized Encryption**. Vous pouvez définir les exemptions où le chiffrement de fichiers par application n’est pas appliqué ou lorsqu’une clé de chiffrement différente est utilisée.

     Remarque : Pour macOS, l’option **Partout** signifie que tous les fichiers se trouvant à certains emplacement prédéfinis seront chiffrés et pourront donc être utilisés uniquement par les applications figurant dans votre liste d’application. Ces emplacements sont :
     - dossier `<Bureau>`
     - dossier `<Documents>`
     - dossier `<Téléchargements>`
     - dossier `<Musique>`
     - dossier `<Vidéos>`
     - tous les partages réseau
     - tous les périphériques amovibles
     - tous les fournisseurs de stockage dans le Cloud
     - dossiers temporaires dans lesquels Microsoft Outlook et Apple Mail conservent les pièces jointes aux emails

     Important : L’application de Synchronized Encryption aux partages réseau peut entraîner des problèmes pour certains utilisateurs. Si les fichiers sur les partages réseau ont été chiffrés par les utilisateurs disposant de la clé Synchronized Encryption dans leur jeu de clés, les utilisateurs ne disposant pas de cette clé ne seront pas en mesure de les déchiffrer. Pour éviter une telle situation, veuillez d’abord exclure les partages réseau du chiffrement et supprimer cette exemption après vous être assuré que tous les utilisateurs disposent bien de la clé Synchronized Encryption. Les utilisateurs reçoivent leur clé lorsqu’une stratégie Synchronized Encryption est appliquée à leur terminal. Vous avez également la possibilité de leur assigner manuellement les clés dans le SafeGuard Management Center.

- **Emplacements définis** : vous permet d'indiquer les emplacements sur lesquels le chiffrement doit être appliqué. Des espaces réservés pour définir les chemins sont disponibles. Vous pouvez choisir d'inclure un chemin au chiffrement ou de l'exclure.

5. Selon la **Portée du chiffrement** que vous sélectionnez, vous pouvez indiquer des chemins sur lesquels le chiffrement par application sera appliqué (**Emplacements définis**) ou les exemptions du chiffrement par application (**Partout**).

   Remarque : Vous pouvez définir les chemins pour Windows et macOS dans la même stratégie. Les espaces réservés pour les différents systèmes sont disponibles dans la liste **Chemin**. La colonne **Système** indique le système d'exploitation pour lequel le chemin est valide (**Tous les systèmes**, **Windows**, **macOS**). Lorsque vous placez votre curseur sur les espaces réservés **Stockage Cloud**, des infobulles apparaissent vous indiquant sur quel système d'exploitation vous pouvez utiliser l'espace réservé.

6. Dans la colonne **Chemin**, indiquez le chemin sur lequel le chiffrement de fichier **Par application (Synchronized Encryption)** sera appliqué :
   - Cliquez sur le bouton déroulant et sélectionnez un espace réservé de nom de dossier dans la liste des espaces réservés disponibles.

     En faisant passer votre curseur sur les entrées de la liste, vous pouvez afficher des infobulles qui vous indiquent comment un espace réservé est généralement présenté sur un terminal. Vous pouvez uniquement saisir des espaces réservés valides pour chaque système d'exploitation. Retrouvez une description de tous les espaces réservés disponibles à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par application *(page 425)*.

     Important : Le chiffrement intégral du profil utilisateur à l'aide de l'espace réservé `<Profil utilisateur>` peut entraîner une instabilité du bureau Windows sur le terminal.

   - Cliquez sur le bouton Parcourir pour naviguer dans le système de fichiers et sélectionnez le dossier requis.
   - Sinon, saisissez simplement un nom de chemin.

7. Sélectionnez le **Mode** de chiffrement :
   - Pour **Portée du chiffrement** > **Emplacements définis**, sélectionnez **Chiffrer** afin de permettre aux applications dans la liste d'application de chiffrer les fichiers présents sous ce chemin ou **Exclure** si ces applications ne doivent pas chiffrer leurs fichiers présents sous ce chemin. Par exemple, vous pouvez chiffrer `D:\Documents` et exclure `D:\Documents\Clair`.
   - Pour la **Portée du chiffrement** > **Partout**, vous pouvez **Exclure** les chemins du chiffrement ou indiquer les emplacements dans lesquels une autre clé que la **Clé Synchronized Encryption** est utilisée.

8. Dans la colonne **Clé**, sélectionnez la clé à utiliser pour le mode **Chiffrer** :

- Cliquez sur le symbole de la **Clé Synchronized Encryption** dans le champ **Clé** pour utiliser la **Clé Synchronized Encryption** pour cet emplacement. Vous pouvez placer le curseur de la souris sur les symboles de clé pour afficher leur fonction.
- Cliquez sur le symbole de la **Clé personnelle** dans le champ **Clé** pour utiliser les clés personnelles des utilisateurs. Sur le terminal, cet espace réservé est résolu sur la **Clé personnelle** de l'utilisateur SafeGuard Enterprise connecté.
- Cliquez sur le bouton Parcourir pour ouvrir la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour afficher une liste de toutes les clés disponibles et sélectionnez la clé requise.

  Remarque : Les clés machine ne sont pas montrées dans la liste. Elles ne peuvent pas être utilisées par le Chiffrement de fichiers car elles sont uniquement disponibles sur une seule machine et ne peuvent donc pas être utilisées pour permettre à des groupes d'utilisateurs d'accéder aux mêmes données.

9. Pour ajouter d'autres chemins :
10. Indiquez les paramètres du **Chiffrement initial**. Sélectionnez l'emplacement dans lequel les fichiers existants seront chiffrés conformément aux chemins indiqués **(Stockés sur les disques locaux**, **Stockés sur les périphériques amovibles**, **Stockés chez les fournisseurs de stockage Cloud détectés automatiquement**). Le chiffrement initial commence lorsque la stratégie est appliquée sur le terminal, à chaque fois que l'utilisateur se connecte ou lorsqu'un périphérique amovible est connecté.
11. Enregistrez vos modifications.

    Lorsque vous quittez l'onglet **Chiffrement de fichiers**, le système vous demande si vous voulez enregistrer vos modifications.

12. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la nouvelle stratégie à vos groupes d'utilisateurs.

6.3.5.1 Espaces réservés des chemins dans les règles de chiffrement de fichiers par application

Les espaces réservés suivants peuvent être utilisés lors de la spécification des chemins dans les règles de chiffrement des stratégies **Chiffrement de fichiers**. Vous pouvez sélectionner ces espaces réservés en cliquant sur le bouton du menu déroulant du champ **Chemin**.

Utilisez toujours des barres obliques inverses pour séparer les chemins même lors de la création de règles de chiffrement de fichiers pour macOS. De cette manière, vous pouvez appliquer les règles aux deux systèmes d'exploitation (Windows et macOS). Sur les terminaux macOS, les barres obliques inverses sont automatiquement transformées en barres obliques afin de correspondre aux conditions requises du système d'exploitation macOS. Toutes les erreurs dans les espaces réservés

sont consignées dans le journal. Les règles de chiffrement de fichiers incorrectes sont consignées dans le journal, puis ignorées sur le terminal.

Exemple : Le chemin Windows `<Profil utilisateur>\Dropbox\personnel` est converti sur Mac en `/Utilisateurs/<NomUtilisateur>/Dropbox/personnel`.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et macOS)	Résultats dans la valeur suivante sur le terminal
`<%nom_variable_environnement%>`	Tous	Valeur de la variable d'environnement. Exemple : <%NOMUTILISATEUR%>. Si des variables d'environnement contiennent plusieurs emplacements (par exemple, la variable PATH), les chemins ne seront pas divisés en plusieurs règles. Ceci entraîne une erreur et la règle de chiffrement est non valide.
`<Poste de travail>`	Tous	Dossier virtuel représentant le bureau de l'ordinateur.
`<Documents>`	Tous	Dossier virtuel représentant l'élément du bureau **Mes documents** (équivalent à CSIDL_MYDOCUMENTS). Chemin type : C:\Utilisateurs\Nom d'utilisateur\Documents.
`<Téléchargements>`	Tous	Le dossier dans lequel les téléchargements sont stockés par défaut. Le chemin habituel Windows est C:\Utilisateurs\nom d'utilisateur\Téléchargements.
`<Musique>`	Tous	Répertoire du système de fichiers qui sert de dépôt de données pour les fichiers musique. Chemin type : C:\Utilisateurs\Nom d'utilisateur\Musique.
`<Partages réseau>`	Tous	
`<Images>`	Tous	Répertoire du système de fichiers qui sert de dépôt de données pour les fichiers image. Chemin type : C:\Utilisateurs\Nom d'utilisateur\Images. **Remarque :** Sur les Macs, le chiffrement de tout le dossier `<Images>` n'est pas pris en charge. Toutefois, vous pouvez chiffrer les sous-dossiers, par exemple `<Images>\enc`.

Espace réservé au chemin	Système d'exploitation (Tous=Windows et macOS)	Résultats dans la valeur suivante sur le terminal
`<Public>`	Tous	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers document de tous les utilisateurs. Chemin type : C:\Utilisateurs\Public.
`<Amovibles>`	Tous	Dirige vers les dossiers racine de tous les supports amovibles.
`<Profil utilisateur>`	Tous	Dossier du profil de l'utilisateur. Chemin type : C:\Utilisateurs\<nom d'utilisateur>. **Remarque :** Le chiffrement de tout le profil d'utilisateur n'est pas pris en charge. Toutefois, vous pouvez chiffrer les sous-dossiers, par exemple `<Profil d'utilisateur>\enc`.
`<Vidéos>`	Tous	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers vidéo des utilisateurs. Chemin type : C:\Utilisateurs\Nom d'utilisateur\Vidéos.
`<Cookies>`	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les cookies Internet.
`<Favoris>`	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les éléments préférés de l'utilisateur. Chemin type : C:\Utilisateurs\Nom d'utilisateur\Favoris.
`<Données des applications locales>`	Windows	Répertoire du système de fichiers qui sert de dépôt de données pour les applications locales (non itinérantes). Chemin type : C:\Utilisateurs\Nom d'utilisateur\AppData\Local.
`<Données des programmes>`	Windows	Répertoire du système de fichier contenant les données d'application de tous les utilisateurs. Chemin type : C:\ProgramData
`<Program Files>`	Windows	Dossier Program Files. Chemin type : \Program Files. Pour les systèmes 64 bits, deux règles sont disponibles : une pour les applications 32 bits et une pour les applications 64 bits.
`<Musique publique>`	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers musique

Espace réservé au chemin	Système d'exploitation (Tous=Windows et macOS)	Résultats dans la valeur suivante sur le terminal
		de tous les utilisateurs. Chemin type : C:\Utilisateurs\Public\Musique.
<Images publiques>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers image de tous les utilisateurs. Chemin type : C:\Utilisateurs\Public\Images.
<Vidéos publiques>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers vidéo de tous les utilisateurs. Chemin type : C:\Utilisateurs\Public\Vidéos.
<Itinérant>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les données spécifiques aux applications. Chemin type : C:\Utilisateurs\Nom d'utilisateur\AppData\Roaming.
<Système>	Windows	Dossier système Windows. Chemin type : C:\Windows\System32. Pour les systèmes 64 bits, deux règles sont disponibles : une pour les applications 32 bits et une pour les applications 64 bits.
<Dossier de gravure temporaire>	Windows	Répertoire du système de fichiers qui sert de zone de transit pour les fichiers en attente d'écriture sur un CD-ROM. Chemin type : C:\Utilisateurs\Nom d'utilisateur\AppData\Local\Microsoft\Windows\CD Burning.
<Fichiers Internet temporaires>	Windows	Répertoire du système de fichiers qui sert de dépôt commun pour les fichiers temporaires Internet.
<Windows>	Windows	Répertoire Windows ou SYSROOT. Ceci correspond aux variables d'environnement %windir% ou %SYSTEMROOT%. Chemin type : C:\Windows.
<Racine>	macOS	Le dossier racine macOS. Nous vous déconseillons d'appliquer des stratégies au dossier racine même si ceci est techniquement possible.

Espaces réservés au stockage Cloud

Fournisseur	Espace réservé au stockage Cloud	Utilisable dans le paramètre CSD	Résultat
Box	`<!Box!>`	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Box. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisée par le logiciel Box.
Dropbox	`<!Dropbox!>`	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Dropbox. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel Dropbox.
Egnyte **Windows** uniquement	`<!Egnyte!>`	**Application de synchronisation**	Le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Egnyte.
	`<!EgnytePrivate!>`	**Dossiers de synchronisation**	Tous les dossiers confidentiels du stockage Cloud d'Egnyte. Pour les utilisateurs Egnyte classiques, il s'agit généralement d'un seul dossier. Pour les administrateurs Egnyte, cet espace réservé consiste généralement en plusieurs dossiers.

Fournisseur	Espace réservé au stockage Cloud	Utilisable dans le paramètre CSD	Résultat
	`<!EgnyteShared!>`	**Dossiers de synchronisation**	Tous les dossiers partagés du stockage Cloud d'Egnyte. Les modifications de la structure du dossier Egnyte (y compris, l'ajout ou la suppression de dossiers confidentiels ou partagés) sont détectées automatiquement. Les stratégies adéquates sont mises à jour automatiquement. Les dossiers de synchronisation peuvent se trouver sur des emplacements du réseau. Vous pouvez donc saisir les chemins réseau dans le paramètre **Dossiers de synchronisation**. Le module SafeGuard Enterprise Cloud Storage se connecte donc par défaut aux systèmes de fichiers réseau. Si cette opération n'est pas nécessaire, vous pouvez désactiver ce comportement en définissant une stratégie **Paramètres généraux** et en sélectionnant **Réseau** sous **Périphériques ignorés**.
Google Drive	`<!GoogleDrive!>`	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel Google Drive. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel Google Drive.
OneDrive	`<!OneDrive!>`	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel OneDrive. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel OneDrive.

Remarque : SafeGuard Enterprise ne prend pas en charge les comptes Microsoft. Sous Windows 8.1, OneDrive peut uniquement être utilisé si l'utilisateur Windows est un utilisateur de domaine. Sous Windows 8.1,

Fournisseur	Espace réservé au stockage Cloud	Utilisable dans le paramètre CSD	Résultat
	SafeGuard Enterprise ne prend pas en charge OneDrive pour les utilisateurs locaux.		
OneDrive Entreprise	`<!OneDriveForBusiness>`	**Application de synchronisation**, **Dossiers de synchronisation**	Pour les applications de synchronisation : le chemin pleinement qualifié de l'application de synchronisation utilisée par le logiciel OneDrive. Pour les dossiers de synchronisation : le chemin pleinement qualifié du dossier de synchronisation utilisé par le logiciel OneDrive.

Remarque : OneDrive Entreprise prend uniquement en charge le stockage des fichiers chiffrés dans les dossiers locaux et leur synchronisation dans le Cloud. Le stockage des fichiers chiffrés à partir des applications Microsoft Office 2013 directement dans le Cloud OneDrive Entreprise ou sur le serveur SharePoint n'est pas pris en charge. Ces fichiers ne sont pas chiffrés et sont stockés dans le Cloud.

Les fichiers chiffrés par SafeGuard Enterprise dans le Cloud OneDrive Entreprise ne peuvent pas être ouverts par Microsoft Office 365.

6.3.5.2 Configuration du chiffrement de fichiers par application dans le Cloud

SafeGuard Enterprise offre la détection automatique des fournisseurs de stockage Cloud suivants :

- Box
- Dropbox (inclut Dropbox Business)
- Google Drive
- OneDrive
- OneDrive Entreprise
- Egnyte (Windows uniquement)

Des espaces réservés prédéfinis sont disponibles. Les chemins des dossiers de synchronisation sont définis automatiquement.

Le dossier de synchronisation local peut être modifié par les utilisateurs. Par exemple, en cas de déplacement, SafeGuard Enterprise suit les modifications et continue de chiffrer les fichiers dans le nouvel emplacement.

Remarque : Les stratégies **Par application (Synchronized Encryption)** ne sont pas fusionnées. Si une stratégie de ce type existe, veuillez l'ajouter aux règles de chiffrement pour le stockage Cloud à la stratégie déjà existante.

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Chiffrement de fichiers** ou sélectionnez-en une.
   L'onglet **Chiffrement de fichiers** apparaît.

2. Sélectionnez **Par application (Synchronized Encryption)** dans la liste déroulante **Type de chiffrement**.
   Les options **Liste d'application** et **Portée du chiffrement** apparaissent.

3. Dans la liste déroulante, sélectionnez la **Liste d'application**que vous avez créée auparavant.

4. Dans la liste déroulante **Portée du chiffrement**, sélectionnez **Emplacements définis**.

5. Indiquez les paramètres du **Chiffrement initial**. Sélectionnez **Dans les stockages Cloud détectés automatiquement** pour chiffrer les fichiers existants dans les dossiers de synchronisation. Le chiffrement initial commence lorsque la stratégie est appliquée sur le terminal, à chaque fois que l'utilisateur se connecte ou lorsqu'un périphérique amovible est connecté.

6. Dans la colonne **Chemin**, cliquez sur le bouton déroulant et sélectionnez un espace réservé au **Stockage Cloud**.
   Retrouvez une liste de tous les espaces réservés au stockage Cloud à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par application *(page 425)*.

   Sélectionnez **<!Tous les fournisseurs de stockage Cloud compatibles!>** pour activer le chiffrement de chaque fournisseur pris en charge.

   Lorsque vous placez votre curseur sur les espaces réservés **Stockage Cloud**, des infobulles apparaissent vous indiquant sur quel système d'exploitation vous pouvez utiliser l'espace réservé.

7. Dans la colonne **Étendue**, sélectionnez :
   - **Ce dossier uniquement** pour appliquer la règle seulement au dossier indiqué par la colonne **Chemin**.
   - **Inclure les sous-dossiers** pour appliquer aussi la règle à tous ses sous-dossiers.

8. Dans la colonne **Mode**, sélectionnez **Chiffrer**.

9. Dans la colonne **Clé**, sélectionnez la clé à utiliser pour le mode **Chiffrer**. Vous pouvez utiliser des clés créées et appliquées dans **Utilisateurs et ordinateurs** :

- Cliquez sur le bouton **Parcourir** pour ouvrir la boîte de dialogue **Rechercher des clés**. Cliquez sur **Rechercher maintenant** pour afficher une liste de toutes les clés disponibles et sélectionnez la clé requise.

  Remarque : Les clés machine ne sont pas montrées dans la liste. Elles ne peuvent pas être utilisées par le Chiffrement de fichiers car elles sont uniquement disponibles sur une seule machine et ne peuvent donc pas être utilisées pour permettre à des groupes d'utilisateurs d'accéder aux mêmes données.

- Cliquez sur le bouton **Clé personnelle** avec l'icône de la clé pour insérer l'espace réservé **Clé personnelle** dans la colonne **Clé**. Sur le terminal, cet espace réservé sera résolu sur la clé personnelle active de l'utilisateur SafeGuard Enterprise connecté. Si les utilisateurs correspondants n'ont pas encore de clés personnelles actives, elles sont créées automatiquement. Vous pouvez créer des clés personnelles pour un ou plusieurs utilisateurs dans **Utilisateurs et ordinateurs**. Retrouvez plus de renseignements à la section Clés personnelles pour le chiffrement de fichiers par File Encryption *(page 177)*.

10. Pour ajouter d'autres chemins :

11. Enregistrez vos modifications.

12. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la nouvelle stratégie à vos groupes d'utilisateurs.

6.4 Complément Outlook pour Synchronized Encryption

Remarque : Le complément Outlook est uniquement disponible sur les terminaux Windows.

Les pièces jointes envoyées aux destinataires utilisant Synchronized Encryption sont chiffrées automatiquement. Vous n'avez pas à vous soucier du chiffrement et du déchiffrement. Lors de l'envoi d'emails aux destinataires extérieurs à votre réseau d'entreprise, vous pouvez chiffrer vos pièces jointes pour protéger vos données sensibles. SafeGuard Enterprise intègre un module complémentaire pour Microsoft Outlook qui facilite le chiffrement des pièces jointes. Lorsque vous envoyez un email avec un ou plusieurs fichiers joints, le système vous invite à choisir la méthode d'envoi des pièces jointes. Les options disponibles varient en fonction de l'état du chiffrement des fichiers que vous avez joint à votre email.

6.4.1 Création de stratégies pour l'activation du complément Outlook de SafeGuard Enterprise

Pour activer le complément Outlook de SafeGuard Enterprise Synchronized Encryption :

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.
   L'onglet **Paramètres généraux** apparaît.

2. Rendez-vous sous la section **Paramètres du module de messagerie complémentaire**.

3. Dans la liste déroulante **Activer le module de messagerie complémentaire**, sélectionnez **Oui**.
   Le module complémentaire est maintenant activé. Les utilisateurs vont être invités à décider du mode de traitement des pièces jointes à chaque fois qu'ils enverront des emails avec pièces jointes.

   De plus, vous pouvez établir des listes de domaines et indiquer le mode de traitement des pièces jointes lorsqu'elles sont envoyées à ces domaines.

4. Procédez en sélectionnant le mode de traitement des pièces jointes dans la liste déroulante **Méthode de chiffrement pour les domaines autorisés** :
   - **Chiffré** : toutes les pièces jointes des emails envoyés à un domaine spécifié seront chiffrées. Les utilisateurs ne recevront aucune demande de confirmation.

     Les fichiers chiffrés restent chiffrés et la clé de chiffrement est inchangée. Les fichiers non chiffrés sont chiffrés par la **Clé Synchronized Encryption** uniquement si l'extension de fichier est définie dans la liste des apps intégrées.
   - **Aucun chiffrement** : les pièces jointes des emails envoyés à un domaine spécifié ne seront pas chiffrées. Les utilisateurs ne recevront aucune demande de confirmation.
   - **Inchangé (Synchronized Encryption)** les fichiers chiffrés seront envoyés chiffrés tandis que les fichiers en clair seront envoyés en clair. Les utilisateurs ne recevront aucune demande de confirmation.
   - **Toujours demander** : les utilisateurs seront invités à confirmer le mode de traitement des pièces jointes à chaque fois qu'ils enverront des pièces jointes à un domaine spécifié.

5. Saisissez un ou plusieurs domaines sur lesquels la méthode de chiffrement doit être appliquée. Saisissez plusieurs domaines séparés par des virgules. Les caractères de remplacement et les domaines partiellement spécifiés ne sont pas pris en charge.

6. Lorsque vous quittez l'onglet **Paramètres généraux**, le système vous demande si vous voulez enregistrer vos modifications.

7. Cliquez sur **Oui**.

8. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la nouvelle stratégie à vos groupes d'utilisateurs.

6.5 Intégration avec Sophos Central Endpoint Protection

SafeGuard Enterprise Synchronized Encryption protège vos données en supprimant les clés en cas d'activité malveillante détectée sur un terminal.

⚠ **Important :** Cette fonction est uniquement disponible si vous utilisez Sophos Central Endpoint Protection avec SafeGuard Enterprise.

Elle s'assure que Sophos SafeGuard communique avec Sophos Central Endpoint Protection. SafeGuard Enterprise et Sophos Central Endpoint Protection partagent l'état de fonctionnement de votre système. En cas d'infection de votre système, SafeGuard Enterprise protège les fichiers sensibles. Lorsque les clés ne sont pas disponibles, l'accès aux données chiffrées est impossible.

Dans ce cas, les utilisateurs seront informés du mauvais état de fonctionnement de leur système, que SafeGuard a protégé leurs fichiers chiffrés et qu'ils ne seront plus en mesure de les ouvrir pendant une certaine période de temps. Les terminaux demeureront à cet état jusqu'à leur retour à un bon état de fonctionnement. SafeGuard Enterprise mettra de nouveau les clés à disposition. Les utilisateurs seront informés que leur terminal est sécurisé et qu'ils peuvent de nouveau accéder à leurs fichiers chiffrés.

Dans les situations où vous considérez que l'état de mauvais fonctionnement des terminaux n'est plus justifié et que ces terminaux sont toujours à cet état, vous pouvez autoriser les utilisateurs à accéder à leur jeu de clé en définissant l'option **Supprimer les clés sur les machines compromises** sur **Non** et en assignant la stratégie modifiée à vos groupes d'utilisateurs. Retrouvez plus de renseignements à la section Création de stratégies pour supprimer les clés sur les machines compromises *(page 436)*.

⚠ **Important :** La désactivation de l'option **Supprimer les clés des machines compromises** représente un risque potentiel à la sécurité. Veuillez analyser et évaluer attentivement la situation avant de procéder de la sorte.

L'état de sécurité de l'ordinateur est affiché dans la boîte de dialogue **État du client Sophos SafeGuard** sur le terminal.

Conditions préalables

- Le module **Synchronized Encryption** doit être installé sur les terminaux Windows,.
- Le module **SafeGuard File Encryption** doit être installé sur les terminaux macOS.
- Sophos Central Endpoint Protection 1.0.3 ou version supérieure doit être installé sur les terminaux.
- Une stratégie de type **Paramètres généraux** avec l'option **Supprimer les clés des machines compromises** doit être assignée.

6.5.1 Création de stratégies pour supprimer les clés sur les machines compromises

Pour protéger les données en cas de détection d'une activité malveillante sur les terminaux :

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.
   L'onglet **Paramètres généraux** apparaît.

2. Rendez-vous dans la section **Chiffrement de fichiers**.

3. Dans la liste déroulante **Supprimer les clés sur les machines compromises**, sélectionnez **Oui**. Les clés vont être supprimées des terminaux en cas de détection d'une activité malveillante. Un message sera consigné dans le journal.

   Remarque : Les comportements malveillants seront toujours consignés dans la base de données SafeGuard Enterprise quels que soient les paramètres de l'option **Supprimer les clés sur les machines compromises**.

4. Lorsque vous quittez l'onglet **Paramètres généraux**, le système vous demande si vous voulez enregistrer vos modifications.

5. Cliquez sur **Oui**.

6. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la nouvelle stratégie à vos groupes d'utilisateurs.

6.6 Partage du jeu de clés SafeGuard Enterprise avec les appareils mobiles administrés par Sophos Mobile

Les clés de chiffrement disponibles dans les jeux de clés SafeGuard Enterprise peuvent également être mises à disposition dans l'app Sophos Secure Workspace. Les utilisateurs de l'app peuvent alors utiliser les clés pour déchiffrer et consulter les documents ou pour chiffrer des documents.

Les jeux de clés sont synchronisés entre SafeGuard Enterprise et Sophos Mobile. Aucune clé n'est stockée sur le serveur Sophos Mobile. Seule l'app Sophos Secure Workspace peut déchiffrer les appareils.

Configuration requise

Les conditions suivantes doivent être remplies pour la synchronisation du jeu de clés :

- Vous avez configuré l'intégration dans SafeGuard Management Center.
- Vous utilisez Sophos Mobile 6.1 ou une version supérieure.
- Vous avez configuré la gestion des utilisateurs externes pour le Portail libre-service Sophos Mobile conformément aux instructions de la documentation Sophos Mobile en utilisant la même base de données d'utilisateurs Active Directory que celle configurée dans SafeGuard Enterprise.
- Sophos Secure Workspace est administrée par Sophos Mobile.
- Vous avez configuré l'intégration dans Sophos Mobile.
- Pour pouvoir disposer du jeu de clés dans Sophos Mobile, les utilisateurs doivent se connecter au moins une fois à SafeGuard Enterprise.

Fonctions sur les appareils mobiles

La synchronisation du jeu de clés inclut les fonctions suivantes :

- Les clés disponibles dans le jeu de clés SafeGuard Enterprise de l'utilisateur sont disponibles dans le jeu de clés de Sophos Secure Workspace (jeu de clés SSW).
- Les utilisateurs peuvent continuer à utiliser les clés locales qui étaient disponibles dans leur jeu de clés SSW même après que vous ayez configuré la synchronisation du jeu de clés.
- Après avoir configuré la synchronisation du jeu de clés, les utilisateurs ne peuvent pas créer de nouvelles clés locales.
- Pour des raisons de sécurité, les clés dans le jeu de clés SafeGuard Enterprise sont supprimées d'un appareil lorsque le conteneur Sophos est verrouillé.

Retrouvez plus de renseignements à la section Affichage des clés de récupération et Gestion des clés de l'Aide de Sophos Secure Workspace.

6.6.1 Configuration de la synchronisation du jeu de clés

Lorsque vous configurez la synchronisation du jeu de clés, les utilisateurs SafeGuard Enterprise peuvent utiliser leur jeu de clés dans l'app Sophos Secure Workspace.

Pour établir la connexion entre Sophos Mobile et Sophos SafeGuard Enterprise :

Remarque : Vous mettez actuellement les jeux de clés à disposition sur les appareils mobiles. Si ces appareils mobiles sont en conformité avec les règles Sophos Mobile, ils sont autorisés à accéder aux fichiers chiffrés. Veuillez contacter l'administrateur Sophos Mobile pour définir les règles de conformité qui empêcheront tout accès non autorisé.

1. Dans la console Sophos Mobile, téléchargez le fichier de certificat du serveur Sophos Mobile. Dans la console Sophos Mobile, sur le menu latéral, sous **PARAMÈTRES**, cliquez sur **Configuration > Configuration du système**, puis sur l'onglet **SGN**.

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

3. Sélectionnez **Serveurs**.

4. Cliquez sur **Ajouter**.
   La boîte de dialogue **Enregistrement du serveur** apparaît.

5. Cliquez sur le bouton Parcourir et naviguez jusqu'au certificat du serveur Sophos Mobile que vous avez téléchargé.

   ⚠ **Important :** Ne modifiez pas le champ **Nom du serveur :**.

6. Cliquez sur **OK**.
   Le serveur Sophos Mobile apparaît sur l'onglet **Serveur** de l'**Outil de package de configuration**.

7. Vous pouvez également sélectionner la case **Récupération par mobile**.
   Cette option va envoyer les clés de récupération BitLocker et FileVault 2 sur le serveur Sophos Mobile. Les utilisateurs de Sophos Secure Workspace administrée par Sophos Mobile peuvent alors afficher ces clés sur leur appareil mobile à des fins de récupération. Retrouvez plus de renseignements à la section Récupération par appareils mobiles *(page 479)*.

   Remarque : Sophos Secure Workspace prend en charge la récupération par mobile à partir de la version 6.2.

   Seuls les appareils mobiles conformes seront en mesure de recevoir les informations sur la clé de récupération. Aussi, pour une sécurité optimale, veuillez vérifier ces paramètres de conformité avec votre administrateur Sophos Mobile.

8. Sélectionnez **Packages du client administré**.

9. Cliquez sur **Ajouter un package de configuration**.

10. Donnez un nom au package de configuration.

11. Dans la colonne **Serveur principal**, sélectionnez le serveur Sophos Mobile dans la liste déroulante. Il n'est pas nécessaire de sélectionner un **Serveur secondaire**.

12. Dans la colonne **Chiffrement du transport**, sélectionnez **SSL**.

13. Indiquez un chemin de sortie pour le package de configuration (MSI).

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

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Veuillez à présent télécharger le package de configuration dans Sophos Mobile.

6.7 Configuration des applications sécurisées et des appareils ignorés

En plus des règles de chiffrement définies dans les stratégies **Chiffrement de fichiers** suivantes : **Type de chiffrementPar application**, vous pouvez configurer les paramètres **Chiffrement de fichiers** dans des stratégies du type **Paramètres généraux** :

- **Applications sécurisées** (généralement le logiciel antivirus)

  Vous pouvez définir des applications comme sécurisées pour leur accorder l'accès aux fichiers chiffrés. Ceci s'avère utile, par exemple, pour activer le logiciel antivirus afin de contrôler les fichiers chiffrés.

  Les processus enfants ne seront pas sécurisés.
- **Périphériques ignorés**

  Vous pouvez définir des périphériques comme ignorés pour les exclure du processus de chiffrement des fichiers. Vous pouvez seulement exclure des périphériques entiers.

6.7.1 Configuration des applications sécurisées pour le chiffrement de fichiers par application

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.

2. Sous **Chiffrement de fichiers**, cliquez sur la liste déroulante du champ **Applications sécurisées**.

3. Dans la zone de liste de l'éditeur, saisissez les applications à définir comme sécurisées.
   - Vous pouvez définir plusieurs applications sécurisées dans une stratégie. Chaque ligne de la zone de liste de l'éditeur définir une application.
   - Les noms des applications doivent se terminer par .exe.
   - Les noms des applications doivent être indiqués comme des chemins pleinement qualifiés avec informations sur le lecteur/répertoire, par exemple `c:\dir\exemple.exe`. La saisie du nom de fichier lui-même (`exemple.exe`) n'est pas suffisante. Pour un meilleur confort d'utilisation, la vue sur une ligne de la liste des applications n'affiche que les noms de fichiers séparés par des points-virgules.
   - macOS : la saisie d'un groupe d'applications (par exemple `/Applications/Scanner.app`) n'est pas suffisante. L'application doit être indiquée comme par exemple, `/Applications/Scanner.app/Contents/MacOS/Scanner`.
   - Les noms d'applications peuvent contenir les mêmes noms d'espaces réservés pour les dossiers d'environnement Windows et variables d'environnement que les règles de chiffrement dans les stratégies de chiffrement de fichiers. Retrouvez une description de tous les espaces réservés disponibles à la section Espaces réservés des chemins dans les règles de chiffrement de fichiers par emplacement *(page 341)*.

4. Enregistrez vos modifications.

Remarque : Les paramètres de stratégie **Applications sécurisées** sont les paramètres de la machine. La stratégie doit donc être assignée aux machines, pas aux utilisateurs. Sinon, les paramètres ne sont pas activés.

6.7.2 Configuration des périphériques ignorés

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie du type **Paramètres généraux** ou sélectionnez-en une.

2. Sous **Chiffrement de fichiers**, cliquez sur la liste déroulante du champ **Périphériques ignorés**.

3. Dans la zone de liste de l'éditeur :

   a. Sélectionnez **Réseau** si vous ne voulez pas chiffrer les données sur le réseau.

   b. Saisissez les noms de périphériques requis pour exclure des périphériques donnés du chiffrement. Ceci peut être utile lorsque vous avez besoin d'exclure les systèmes des fournisseurs tiers.
   Vous pouvez afficher les noms des appareils actuellement utilisés dans le système à l'aide du programme de contrôle Fltmc.exe (fltmc volumes, fltmc instances) à partir de Microsoft. Retrouvez plus de renseignements à la section https://docs.microsoft.com/fr-fr/windows-hardware/drivers/ifs/development-and-testing-tools.

Vous pouvez exclure des lecteurs de disque (réseau) individuels du chiffrement en créant une règle de Chiffrement de fichiers dans une stratégie **Chiffrement de fichiers** et en paramétrant le **Mode** de chiffrement sur **Ignorer**. Vous pouvez uniquement appliquer ce paramètre aux lecteurs administrés par Windows et pas aux volumes macOS.

6.8 Stratégies de Chiffrement de fichiers par application dans le RSOP

Les stratégies Synchronized Encryption n'étant pas fusionnées, le contenu de la stratégie appliquée à un utilisateur ou à un ordinateur est toujours affichée dans l'onglet **Chiffrement de fichiers** sous l'onglet **RSOP** de la vue **Utilisateurs et ordinateurs**.

7. Gestion avancée

7.1 Conseils pratiques

7.1.1 Déploiement

Suggestions générales

- Essayez d'éviter un déploiement simultané du nouveau module Synchronized Encryption et de l'ancien module File Encryption de SafeGuard Enterprise.
- Un déploiement par phase nécessite la vérification de chaque étape, tout particulièrement pour les membres de groupes Active Directory imbriqués d'une grande complexité.
- La formation des utilisateurs est essentielle à un déploiement et à un fonctionnement sans problème.
- Une communication claire sur les participants et sur les conséquences d'une telle opération est également primordiale.
- Les équipes des services informatique et du support doivent être en mesure de répondre de manière adéquate.

Conditions préalables

- L'utilisation de SafeGuard Enterprise Server et de SafeGuard Management Center nécessite l'installation de .NET 4.5.

- SafeGuard Enterprise doit être installé sur tous les terminaux. Autrement, le partage des fichiers chiffrés ne sera pas transparent et les procédures de travail habituelles seront affectées.

- Si vous voulez lire les fichiers chiffrés sur les appareils mobiles (une nouvelle fonction de SafeGuard Enterprise 8), veuillez également déployer l'app Sophos Secure Workspace.

  Remarque : Pour lire les fichiers chiffrés sur les appareils mobiles, veuillez utiliser Sophos Secure Workspace administrée par Sophos Mobile.

- Assurez-vous que les utilisateurs en déplacement se connectent régulièrement au serveur backend de SafeGuard Enterprise via VPN ou par « Accès direct » (Windows) afin que les stratégies de chiffrement les plus récentes soient appliquées.

7.1.1.1 Déploiement partiel

Dans la majorité des situations, le nouveau module **Synchronized Encryption** ne peut pas être déployé et activé en une seule fois et rapidement pour tous les employés. Dans ce genre de situations, il est important de donner aux utilisateurs l'accès en lecture seule aux fichiers chiffrés même s'ils se trouvent sur des terminaux SafeGuard Enterprise sans que le module **Synchronized Encryption** ne soit activé. Par conséquent, une stratégie en lecture seule est requise.

Pour donner les droits en lecture seule aux utilisateurs, veuillez procéder de la manière suivante :

- La clé **Synchronized Encryption**.

  Elle est assignée au nœud racine de SafeGuard Management Center par défaut et tous les employés d'une entreprise doivent obtenir automatiquement cette clé.
- Une **Liste d'applications** et une stratégie en lecture seule spécifique.

  Retrouvez plus de renseignements à la section Déploiement partiel de Synchronized Encryption *(page 411)*.

7.1.1.2 Utilisation de Synchronized Encryption et de SafeGuard Enterprise File Encryption dans le même environnement

Remarque : Si votre environnement nécessite l'utilisation de SafeGuard Synchronized Encryption et de SafeGuard File Encryption, envisagez la procédure suivante afin de bénéficier d'une intégration harmonieuse.

Synchronized Encryption prend en charge une clé de chiffrement pour toute l'entreprise. L'administration et le déploiement sont donc plus faciles à effectuer. Certains services comme les Ressources Humaines ou les Finances pourraient avoir besoin d'une protection cryptographique différente des autres services afin que leurs documents soient uniquement accessibles au sein de leur service.

Dans ce cas de figure, les modules SafeGuard Enterprise File Encryption (File Share, Cloud Storage, Data Exchange) doivent être utilisés. Ces modules permettent d'utiliser différentes clés pour le chiffrement de fichiers. Vous ne pouvez pas installer le module Synchronized Encryption et les modules SafeGuard Enterprise File Encryption sur la même machine.

Pour utiliser les modules Synchronized Encryption et SafeGuard Enterprise File Encryption, vous allez devoir effectuer des tâches administratives supplémentaires :

1. Le déploiement de SafeGuard Enterprise doit prendre en compte les différents modules à installer pour certains services.
2. Les services avec des besoins spéciaux, doivent récupérer d'autres stratégies que celles assignées sur les terminaux **Synchronized Encryption**. Pour que ceci soit possible, la structure AD importée doit autoriser une assignation de ces stratégies aux utilisateurs et machines concernés.
3. La procédure de déploiement/d'installation des modules SafeGuard Enterprise doit être effectuée conformément aux stratégies assignées : les bonnes machines doivent récupérer les bonnes stratégies.

Remarque : Le module complémentaire Outlook n'est pas disponible sur les modules SafeGuard Enterprise File Encryption. Par conséquent, les terminaux Synchronized Encryption et File Encryption ne peuvent pas partager les pièces jointes chiffrées de manière transparente.

Conseils d'utilisation

- Les utilisateurs des modules SafeGuard Enterprise File Encryption doivent récupérer la clé **Synchronized Encryption**. Les utilisateurs peuvent ensuite lire les fichiers chiffrés à l'aide de la clé **Synchronized Encryption** de manière transparente.
- Partage des fichiers chiffrés :

  Pour les utilisateurs des modules SafeGuard Enterprise File Encryption, nous conseillons de créer une stratégie qui définit la clé **Synchronized Encryption** à utiliser pour un partage de « transfert ». Tous les fichiers créés ou déplacés dans ce partage devront être chiffrés avec la clé **Synchronized Encryption**. Les utilisateurs **Synchronized Encryption** sont en mesure de lire ces fichiers.

- Partage des fichiers clairs :

  Pour les utilisateurs des modules SafeGuard Enterprise File Encryption, une stratégie qui exclut un dossier du chiffrement peut être utilisée (**Type de chiffrement** : **Par emplacement**, **Mode** : **Exclure**).

- Lorsque les utilisateurs des modules SafeGuard Enterprise File Encryption veulent partager des fichiers avec les utilisateurs **Synchronized Encryption**, ils doivent d'abord les déchiffrer. Ils peuvent ensuite décider d'envoyer les fichiers déchiffrés ou de les chiffrer à l'aide de la clé Synchronized Encryption.

7.1.1.3 Vérification de la validité des certificats d’utilisateur

La vérification de la validité des certificats d’utilisateur est particulièrement importante pour les entreprises qui utilisent uniquement l’administration SafeGuard Enterprise BitLocker et qui souhaitent ajouter la fonction de chiffrement synchronisé **Synchronized Encryption**.

Vous pouvez vérifier les certificats dans SafeGuard Management Center sous **Clés et certificats > Certificats > Certificats assignés**.

Le certificats ayant expiré ou arrivant bientôt à échéance sont marqués en rouge dans la colonne **Expire le**. Pour renouveler un certificat arrivant bientôt à échéance, veuillez cocher la case dans la colonne **Renouveler**. Les utilisateurs dont les certificats ont déjà expiré doivent en obtenir de nouveaux. Veuillez supprimer les certificats expirés. Les utilisateurs affectés en obtiendront des nouveaux automatiquement la prochaine fois qu'ils se connecteront à SafeGuard Enterprise.

SafeGuard Enterprise met à disposition un script de base de données UserCertficateRenewal.vbs pour automatiser ces tâches. Le script peut être utilisé dans le **Gestionnaire de tâches** de SafeGuard Enterprise ou de Windows pour effectuer ces vérifications régulièrement et renouveler les certificats si nécessaire comme indiqué dans l'article 118878 de la base de connaissances de Sophos.

7.1.1.4 Confirmation de tous les utilisateurs

Dans SafeGuard Enterprise, les nouveaux utilisateurs doivent être confirmés dans SafeGuard Management Center ou authentifiés dans Active Directory. La majorité des utilisateurs seront des utilisateurs Active Directory qui seront confirmés automatiquement. Toutefois, certains utilisateurs, comme par exemple, les utilisateurs locaux, doivent être confirmés manuellement. Les utilisateurs non confirmés ne deviendront pas des **Utilisateurs SGN** et n'obtiendront donc pas les clés de chiffrement pour Synchronized Encryption. Ceci s'applique aux terminaux Windows et macOS.

Nous vous conseillons de paramétrer la première stratégie pour qu'elle soit déployée en **lecture seule**. Dès que tous les terminaux/utilisateurs ont reçu leurs clés, veuillez activer les stratégies de chiffrement. De cette manière, vous êtes sûr que tous les utilisateurs sont confirmés avant qu'ils ne reçoivent leurs stratégies de chiffrement. Vous évitez également de rencontrer des problèmes d'utilisateurs non confirmés.

7.1.1.5 Stratégies pour les terminaux macOS

Pour le chiffrement de fichiers, nous conseillons l'utilisation du type de stratégie **Par application (Synchronized Encryption)** avec la **Portée du chiffrement** définie sur **Emplacements définis** et commencez uniquement avec quelques emplacements sur lesquels les fichiers sont chiffrés automatiquement. De cette manière, vous réduisez l'impact sur les utilisateurs et sur leurs procédures de travail habituelles.

Pour faire la distinction entre les terminaux Windows et macOS en matière de gestion des stratégies, veuillez utiliser un groupe Active Directory ou SafeGuard Enterprise séparé pour les utilisateurs et machines macOS. Activez la stratégie macOS uniquement pour les utilisateurs et machines macOS.

7.1.1.6 Suggestions de stratégie de chiffrement synchronisé sur macOS

Apps intégrées

Les applications qui chiffrent leurs données à ajouter à la **Liste des applications** :

- Email

  Remarque : Pour macOS, aucun module complémentaire Outlook n'est disponible. Toutefois, vous pouvez ajouter Outlook et Apple Mail à la liste des applications pour vous assurer qu'aucune donnée chiffrée ne soit malencontreusement envoyée à des utilisateurs ne pouvant pas y accéder. Veuillez noter que les apps de messagerie que vous incluez dans la liste enverront toutes les pièces jointes déchiffrées et enregistreront toutes les pièces jointes sous forme chiffrée et tous les fichiers clairs en texte clair.

  - /Applications/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - /Applications/Microsoft Office 2011/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - Applications/Mail.app/Contents/MacOS/Mail
- Pour activer l'aperçu dans macOS et la fonctionnalité d'aperçu dans le Finder et dans Apple Mail, les processus suivants doivent être ajoutés :
  - /Applications/Preview.app/Contents/MacOS/Preview
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/

    Contents/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite
  - /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/

    QuickLookUI.framework/Versions/A/Resources/QuickLookUIHelper.app/Contents/MacOS/

    QuickLookUIHelper
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/

    Contents/MacOS/quicklookd

Chemins de Portée du chiffrement : Emplacements définis

- Chiffrer :
  - <Documents>\Encrypted

- Si vous voulez que vos utilisateurs puissent cliquer deux fois sur les documents chiffrés dans leurs clients de messagerie pour les ouvrir, veuillez ajouter ces applications (par exemple Messagerie) à la liste des apps intégrées et leurs dossiers temporaires à la liste des emplacements définis.

  Les emplacements que vous devez définir pour les clients de messagerie sur Mac sont :

  - <%TMPDIR%>\com.apple.mail\com.apple.mail
  - <Profil Utilisateur>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads

  Ajoutez les emplacements suivants pour Outlook pour macOS :

  - <Profil Utilisateur>\Library\Caches\TemporaryItems\Outlook Temp\
  - <%TMPDIR%>com.microsoft.Outlook\Outlook Temp\

7.1.2 Serveur backend

Utilisateur avec accès en lecture seule pour la synchronisation Active Directory

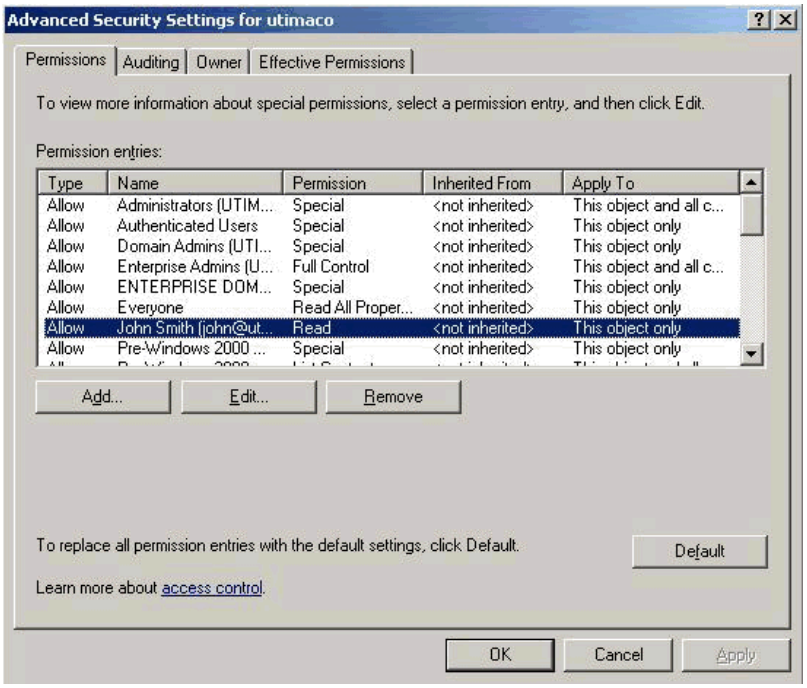
Remarque : Renforcez la sécurité de la connexion en utilisant le chiffrement SSL pour la synchronisation Active Directory.

Le compte utilisé pour l'importation et la synchronisation Active Directory doit être un compte d'utilisateur en **lecture seule**. L'utilisateur doit avoir l'accès en lecture au domaine et à tous les objets enfant.

Pour assigner les droits :

1. Ouvrez la fenêtre d'administration **Utilisateurs et ordinateurs Active Directory** et allez sur **Fonctionnalités avancées**.
2. Cliquez avec le bouton droit de la souris sur le domaine, puis cliquez sur **Propriétés**.
3. Ajoutez un utilisateur (ou un groupe) et sélectionnez la case **Autoriser** pour accorder l'autorisation **Lire**.
4. Cliquez sur **Paramètres avancés** et sélectionnez l'utilisateur (ou le groupe) et cliquez sur **Modifier**.
5. Dans le volet **Liste des autorisations pour <domaine>**, sélectionnez **Cet objet et tous les objets enfants** dans la liste déroulante **Appliquer à :**.

   Vous devriez obtenir le résultat suivant :



Affichage des utilisateurs avec « # » dans SafeGuard Management Center

Les utilisateurs enregistrés dans SafeGuard Enterprise lorsqu'aucun contrôleur de domaine n'était disponible sont identifiés par « # » dans SafeGuard Management Center.

7.1.3 Stratégies

7.1.3.1 Dossiers à exclure du chiffrement

Assurez-vous d'exclure les chemins suivants du chiffrement lorsque vous utilisez **Synchronized Encryption** :

Windows

- <Données des applications locales\Temp>

  Raison : certaines applications créent de nombreux fichiers temporaires de petite taille. S'ils ne sont pas exclus, tous ces fichiers temporaires seront chiffrés conformément à la stratégie. Veuillez exclure le dossier pour éviter tout problème de performances.

- <Données des applications locales>\Microsoft et sous-répertoires

Raison : certaines applications appellent d’autres applications (par exemple, une vidéo imbriquée dans Microsoft PowerPoint). Si l’application d’appel est une application qui chiffre les fichiers, le fichier temporaire (par exemple, la vidéo) sera chiffré. Si l’application appelée (par exemple, le navigateur) est une application qui ne chiffre pas les fichiers (elle ne figure pas sur la liste d’applications), elle ne pourra pas exécuter le fichier chiffré.

- <Program Files>

  Raison : l’accès à ce dossier nécessite les droits administrateur. Le chiffrement initial de SafeGuard ne peut pas chiffrer ces fichiers en raison des droits d’accès. L’exclusion de ce dossier évite de saturer la base de données SafeGuard de messages d’événements d’échec de chiffrement de fichiers.

Tous les systèmes

- <!Fournisseurs de stockage Cloud!>

  En général, nous conseillons de chiffrer l’emplacement de stockage Cloud. Toutefois, vous pouvez exclure certains fournisseurs de stockage Cloud utilisés pour partager des données avec des tierces parties. De cette manière, vous évitez de chiffrer les fichiers dans les dossiers de synchronisation de stockage Cloud local connus. De plus, vous évitez tout problème d’échange de fichiers avec des tierces parties par le biais de la synchronisation Cloud. Il n’est pas nécessaire d’exclure ces dossiers si vous n’utilisez pas les dossiers Cloud pour échanger les fichiers avec des tierces parties.

- <Musique>

  Raison : généralement, ces fichiers n’ont pas besoin d’être chiffrés. Si vous ne voulez pas exclure ce dossier du chiffrement, les applications requises pour ouvrir ces fichiers doivent faire partie de la **Liste des applications**.

- <Profil Utilisateur>\AppData\Roaming\AppleComputer

  Raison : il s’agit du dossier de synchronisation local pour Apple iCloud sur les terminaux Windows. Il doit être exclus pour les mêmes raisons s’appliquant aux <!fournisseurs de stockage cloud!>.

7.1.3.2 Conseils pour le paramétrage de stratégie

Créez un dossier « Unencrypted »

Ce dossier peut être utilisé pour partager des fichiers en clair, par exemple avec les terminaux Linux de l’entreprise ou en cas de procédure de déploiement partiel. Retrouvez plus de renseignements à la section Déploiement partiel de Synchronized Encryption *(page 411)*.

- **Windows**

  Pour exclure le dossier « Unencrypted » du chiffrement sur tous les terminaux, veuillez ajouter le dossier Unencrypted (chemin relatif) en tant qu'exemption dans une stratégie dont la **Portée du chiffrement** est définie sur **Partout**. En procédant ainsi, tous les fichiers dans les dossiers de ce nom, peu importe l'emplacement du dossier, ne seront pas chiffrés.

- **macOS**

  Les chemins relatifs ne sont pas pris en charge sur macOS. Nous vous conseillons de définir <Documents>\Unencrypted en tant qu'exemption dans une stratégie dont la **Portée du chiffrement** est définie sur **Partout**.

Complément Outlook

Nous vous conseillons de paramétrer l'option **Méthode de chiffrement pour les domaines autorisés** dans une stratégie de type **Paramètres généraux** sur **Inchangé**.

Supprimer les clés sur les machines compromises

Les terminaux SafeGuard Enterprise **Synchronized Encryption** sont informés par Sophos Central Endpoint Protection de l'état compromis de la machine.

Nous vous conseillons de définir l'option **Supprimer les clés sur les machines compromises** sur **Non**. Veuillez vérifier les commentaires à propos des terminaux affectés sous **Rapports** dans SafeGuard Management Center pour les détections à l'état de fonctionnement Rouge. Vérifiez puis procédez au nettoyage des terminaux si nécessaire. Enfin, nous conseillons de paramétrer l'option **Supprimer les clés des machines compromises** sur **Oui**.

7.1.3.3 Utilisateur invité

Sur les terminaux sur lesquels l'administration SafeGuard Enterprise BitLocker est uniquement installée, les entreprises continueront peut-être à avoir l'option **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** définie sur **Propriétaire**.

Pour les terminaux sans l'authentification au démarrage SafeGuard Enterprise et équipés de l'administration BitLocker ou des modules de chiffrement de fichiers, l'option **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** doit être définie sur **Tout le monde**. Si vous ne paramétrez pas cette option sur **Tout le monde**, d'autres utilisateurs ne bénéficieront que de l'état **Invité SGN**. Ils ne recevront pas de certificats et ne pourront pas chiffrer les fichiers suite à l'installation d'un module de chiffrement comme **Synchronized Encryption**.

7.1.3.4 Stratégies pour macOS et RSOP

Sur macOS, seules les stratégies assignées aux utilisateurs sont évaluées. Si vous les assignez aux machines, les terminaux macOS ne récupéreront pas les stratégies.

Toutefois, l'onglet RSOP dans SafeGuard Management Center affiche la stratégie actuellement assignée au Mac même si elle n'est pas activée.

7.1.3.5 Suivi de fichiers

Veuillez noter que la fonctionnalité de suivi de fichiers de SafeGuard Enterprise est soumise aux lois en vigueur dans chaque pays d'utilisation. Veuillez vérifier que vous êtes légalement autorisés à procéder au suivi.

7.1.3.6 Rappel de changement de mot de passe

Si vous utilisez le fournisseur de codes d'accès de SafeGuard Enterprise, la fenêtre Windows informant les utilisateurs que leur mot de passe va bientôt expirer ne s'affiche plus.

Pour rappeler aux utilisateurs qu'ils doivent changer leurs mots de passe, veuillez créer et assigner une stratégie SafeGuard Enterprise de type **Mot de passe** avec les paramètres requis. Retrouvez plus de renseignements à la section Règles de syntaxe des mots de passe *(page 277)*.

7.1.4 Terminaux : toutes les plates-formes

7.1.4.1 Chiffrement/Déchiffrement manuel des fichiers

Synchronized Encryption vous permet de chiffrer ou de déchiffrer chaque fichier manuellement. Cliquez avec le bouton droit de la souris sur un fichier et sélectionnez **Chiffrement de fichiers SafeGuard**. Les fonctions suivantes sont disponibles :

- **Afficher l'état du chiffrement** : indique si le fichier est chiffré ou non ainsi que la clé utilisée.
- **Chiffrer en fonction de la stratégie** : chiffre votre fichier avec la clé Synchronized Encryption à condition que le type de fichier soit inclus dans la liste des applications et que l'emplacement du fichier n'ait pas été exclu du chiffrement.
- **Déchiffrer le fichier sélectionné** (uniquement pour les fichiers chiffrés) : vous permet de déchiffrer votre fichier et de l'archiver en texte clair. Nous vous conseillons de déchiffrer votre fichier uniquement s'il ne contient aucune donnée sensible. Vous pouvez désactiver cette option dans une stratégie **Paramètres généraux** comme indiqué à la section Paramètres généraux *(page 255)*.
- **Chiffrer le fichier sélectionné** (uniquement pour les fichiers déchiffrés) : vous permet de chiffrer manuellement votre fichier avec la clé Synchronized Encryption.

- **Créer un fichier protégé par mot de passe** : vous permet de définir un mot de passe pour chiffrer manuellement votre fichier. Ceci est particulièrement utile si vous voulez partager votre fichier en toute sécurité avec une personne de votre entreprise n'ayant pas la clé Synchronized Encryption. Votre fichier est chiffré et enregistré en tant que fichier HTML. Vos destinataires peuvent ouvrir le fichier avec leur navigateur Web dès que vous leur avez communiqué le mot de passe.
  - Vous pouvez désactiver cette option dans une stratégie **Paramètres généraux** comme indiqué à la section Paramètres généraux *(page 255)*.
  - Cette option est uniquement disponible pour les fichiers qui sont soit en texte clair, soit chiffré avec une clé disponible dans votre jeu de clés. Si les fichiers sont chiffrés, ils vont être déchiffrés automatiquement avant d'être protégés par mot de passe.
  - La protection par mot de passe utilise l'encodage « base64 ». Les fichiers sont par conséquent de plus grande taille que le fichier original. La taille de fichier maximale prise en charge est de 50 Mo.
  - Il est uniquement possible de protéger les fichiers individuels par mot de passe et non les dossiers ou les répertoires. Toutefois, vous pouvez sélectionner plus d'un fichier pour afficher leur état de chiffrement et pour les chiffrer/déchiffrer.

Si vous cliquez avec le bouton droit de la souris sur des dossiers ou lecteurs, les fonctions suivantes sont disponibles :

- **Afficher l'état du chiffrement** : affiche une liste de fichiers inclus avec des icônes indiquant l'état du chiffrement et la clé utilisée.
- **Chiffrer en fonction de la stratégie** : le système détecte automatiquement tous les fichiers déchiffrés et les chiffre avec la clé Synchronized Encryption par défaut à condition que le type de fichier soit inclus dans la liste des applications et que l'emplacement du fichier n'ait pas été exclu du chiffrement. Selon votre stratégie, les fichiers chiffrés avec d'autres clés peuvent être chiffrés de nouveau avec la clé Synchronized Encryption.

7.1.4.2 Interdiction aux utilisateurs de déchiffrer les fichiers manuellement

Vous pouvez utiliser un paramètre de stratégie pour interdire aux utilisateurs de déchiffrer les fichiers manuellement.

L'interdiction aux utilisateurs de déchiffrer des fichiers manuellement peut être nécessaire pour des raisons de conformité ou incluses dans la stratégie de sécurité de votre organisation. Pour cela :

1. Dans la zone de navigation **Stratégies**, créez une nouvelle stratégie **Paramètres généraux** ou sélectionnez-en une.
   L'onglet **Paramètres généraux** apparaît.

2. Rendez-vous à la section **Chiffrement de fichiers**.

3. Définissez l'option **L'utilisateur est autorisé à déchiffrer les fichiers** sur **Non**.

4. Lorsque vous quittez l’onglet **Paramètres généraux**, le système vous demande si vous voulez enregistrer vos modifications.

5. Cliquez sur **Oui**.

6. Rendez-vous sur la vue **Utilisateurs et ordinateurs** et assignez la nouvelle stratégie à vos groupes d’utilisateurs.

   ⚠ **Important :** Sur macOS, ce paramètre est uniquement appliqué si la stratégie est assignée à la machine. Son assignation à un utilisateur n’a aucun effet.

L’option **Déchiffrer le fichier sélectionné** est supprimée du menu par clic droit des fichiers. Le chiffrement et le déchiffrement sont uniquement contrôlés par le biais des paramètres de stratégie.

Remarque :

Les utilisateurs peuvent toujours déchiffrer les fichiers lorsque vous avez exclus les dossiers du chiffrement dans votre stratégie de chiffrement. Si les utilisateurs déplacent ou copient les fichiers dans ces dossiers, les fichiers sont déchiffrés.

7.1.4.3 Le terminal ne revient pas à un bon état de fonctionnement : échec de l’opération d’élimination des menaces

La protection des données de nouvelle génération garantit la communication entre Sophos SafeGuard et Sophos Endpoint Protection, si elle est disponible. Il s’agit d’une extension du message de Synchronized Security. Sophos SafeGuard et Sophos Endpoint partagent l’état de bon fonctionnement d’un système en s’envoyant une pulsation sur son état de fonctionnement via Security Hearbeat.

Si un système est gravement infecté par un malware, il sera verrouillé pour protéger tous les fichiers sensibles.

Dans l’éventualité d’une telle situation, les utilisateurs sont informés par Sophos Endpoint Protection que leur système ne fonctionne pas normalement via l’affichage en rouge de l’état de fonctionnement. De plus, Sophos SafeGuard les informe qu’ils ne seront plus en mesure d’accéder aux fichiers chiffrés. Cet état demeurera ainsi (impossibilité d’accéder aux fichiers chiffrés) tant que l’état de fonctionnement du système ne sera pas revenu à la normale (vert). Lorsque le système revient à son état normal de fonctionnement, Sophos SafeGuard se synchronise avec le serveur backend et permet aux utilisateurs d’accéder de nouveau aux fichiers chiffrés.

Si les utilisateurs reçoivent ces notifications et que leur système ne revient pas à un état normal dans les plus brefs délais, ils doivent immédiatement contacter leur service informatique.

Si un terminal n’est pas en mesure de revenir à un état de fonctionnement normal, ceci signifie que l’opération d’élimination des menaces de Sophos Anti-Virus a échoué (cette opération d’élimination s’effectue automatiquement dans Sophos Central). Si l’opération d’élimination échoue, l’intervention du service informatique est nécessaire afin d’éliminer le malware. Retrouvez plus de renseignements sur https://www.sophos.com/fr-fr/support/knowledgebase/112129.aspx.

7.1.5 Terminaux Windows

7.1.5.1 Déchiffrement des fichiers avec SGFileEncWizard.exe

L’utilitaire de ligne de commande SGFileEncWizard.exe permet aux utilisateurs de déclencher le déchiffrement automatique des fichiers.

Sur un ordinateur sur lequel SafeGuard Enterprise est installé, l’utilitaire se trouve sous `<SYSTÈME>:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\`

Configuration requise

- SafeGuard File Encryption à partir de la version 8.20 ou SafeGuard Synchronized Encryption à partir de la version 8.20 doit être installé.
- Les dossiers dans lesquels les fichiers seront déchiffrés doivent être inclus dans des règles d’exclusion dans une stratégie de chiffrement des fichiers existante. Toutes règles permettant de chiffrer ou d’ignorer ces dossiers doivent être retirées. Il est également possible de créer une nouvelle stratégie et de l’assigner aux utilisateurs correspondants comme indiqué dans les sections Configuration des règles de chiffrement dans les stratégies de chiffrement de fichiers par emplacement *(page 337)* et Création de stratégies pour le chiffrement de fichiers par application *(page 422)*.
- SGFileEncWizard.exe doit être lancé par les utilisateurs sur leur propre ordinateur afin que toutes les clés soient disponibles. Aucun droit d’administration n’est requis.
- Le déchiffrement n’aura pas lieu si vous cliquez deux fois sur le fichier SGFileEncWizard.exe pour l’exécuter ou si vous n’avez pas défini de chemin.
- Aucun espace réservé ne peut être utilisé dans l’appel « command-line ».
- Aucun rapport ou résumé de déchiffrement n’est généré.

Procédez au déchiffrement avec SGFileEncWizard.exe

Les utilisateurs doivent exécuter SGFileEncWizard.exe avec le chemin à déchiffrer et le paramètre **/X**. Tous les fichiers se trouvant aux emplacements exclus seront déchiffrés.

SGFileEncWizard.exe" <CHEMIN> /X

Exemples :

```
C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\SGFileEncWizard.exe
D:\ /X

C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\SGFileEncWizard.exe
\\hostname\share\ /X

C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client\SGFileEncWizard.exe
\\hostname\share\ C:\ D:\ /X
```

7.1.5.2 Emails envoyés par la règle de transfert automatique

Lorsque vous créez une règle de transfert automatique ou de redirection sur le **client**, l'envoi automatique de ces emails n'est pas journalisé.

7.1.6 Terminaux macOS

Position des icônes sur le poste de travail

Lors de l’utilisation de SafeGuard Enterprise pour Mac, les positions des icônes sur votre poste de travail ne seront peut-être pas enregistrées correctement. Lorsque vous changez la position d’une icône, elle est replacée à sa position d’origine après chaque redémarrage ou connexion.

Pour enregistrer les positions de vos icônes, procédez comme suit :

1. Démarrez l’application Terminal sur votre Mac.
2. Saisissez la commande suivante :

   defaults write com.sophos.encryption MountDesktopAsNetworkVolume 1
3. Déconnectez-vous et rouvrez une session sur votre Mac.

⚠ **ATTENTION :** Lorsque vous exécutez cette commande, la fonctionnalité de la Corbeille change. Lorsque les fichiers sont supprimés, ils ne sont pas déplacer dans la Corbeille. Leur suppression est définitive. Pour désactiver ce paramètre, saisissez la commande suivante dans l’application Terminal :

defaults remove com.sophos.encryption MountDesktopAsNetworkVolume.

Changement du nom d’ordinateur d’un Mac

Si vous changez le nom d’ordinateur d’un Mac, veuillez ensuite exécuter sgfsadmin --update-machine-info et synchroniser le Mac avec le serveur SafeGuard Enterprise.

7.2 Recommandations en matière de sécurité

En suivant les étapes simples mentionnées ci-dessous, vous pourrez écarter les risques et conserver les données de votre entreprise sécurisées et protégées à tout moment.

Bon usage en matière de chiffrement

- **Assurez-vous qu’une lettre a été assignée à tous les lecteurs.**

  Seuls les lecteurs auxquels une lettre a été assignée sont pris en compte pour le chiffrement/déchiffrement du disque. Les lecteurs sans lettre sont susceptibles d’entraîner des fuites de données confidentielles en texte brut.

  Pour écarter ce type de menace : ne permettez pas aux utilisateurs de changer les assignations de lettres au lecteur. Définissez leurs droits utilisateurs en conséquence. Les utilisateurs standard de Windows n’ont pas ce droit par défaut.

- **Appliquer un chiffrement initial rapide avec précaution.**

  SafeGuard Enterprise propose le chiffrement initial rapide pour réduire le temps du chiffrement initial des volumes en accédant seulement à l’espace véritablement utilisé. Ce mode conduit à un état moins sécurisé si un volume a été utilisé avant son chiffrement avec SafeGuard Enterprise. À cause de leur architecture, les SSD (Solid State Disks) sont plus affectés que les disques durs standard. Ce mode est désactivé par défaut. Retrouvez plus de renseignements dans l’article 113334 de la base de connaissances de Sophos.

- **Utiliser seulement l’algorithme AES-256 pour le chiffrement des données.**
- **Utiliser SSL/TLS (SSL version 3 ou supérieure) pour la protection de la communication client/serveur.**

  Retrouvez plus de renseignements à la section Sécurisation des connexions de transport avec SSL *(page 49)*.

- **Empêcher toute désinstallation.**

  Pour renforcer la protection des terminaux, vous pouvez empêcher la désinstallation locale de SafeGuard Enterprise dans une stratégie **Paramètres de machine spécifiques**. Définissez l’option **Désinstallation autorisée** sur **Non** et déployez cette stratégie sur les terminaux. Les tentatives de désinstallation sont annulées et les tentatives non autorisées sont journalisées.

Si vous utilisez une version de démonstration, assurez-vous que vous paramétrez **Désinstallation autorisée** sur **Oui** avant que la version de démonstration n'expire.

Appliquez la protection antialtération Sophos sur les terminaux utilisant Sophos Endpoint Security and Control.

Évitez le mode veille

Sur les ordinateurs protégés par SafeGuard Enterprise, il est possible que certains individus malintentionnés accèdent aux clés de chiffrement dans certains modes de veille. Tout particulièrement lorsque le système d'exploitation de l'ordinateur n'est pas arrêté correctement et que les processus en tâche de fond restent en cours d'exécution. La protection est renforcée lorsque le système d'exploitation est complètement arrêté ou mis en veille prolongée.

Formez les utilisateurs en conséquence ou considérez la désactivation centrale du mode veille sur les terminaux sans surveillance ou qui ne sont pas en cours d'utilisation :

- Évitez le mode veille (attente/veille prolongée) ainsi que le mode de veille Hybride. Le mode de veille Hybride allie la mise en hibernation et la mise en veille. La définition d'un mot de passe supplémentaire après la reprise d'une session n'assure pas de protection complète.

- Évitez de verrouiller les ordinateurs de bureau et de mettre hors tension les moniteurs ou de fermer les couvercles des portables en guide de protection si ce n'est pas suivi par une véritable mise hors tension ou en hibernation. La demande d'un mot de passe supplémentaire après la reprise d'une session ne fournit pas une protection suffisante.

- Arrêtez vos ordinateurs ou mettez-les en hibernation. L'authentification au démarrage SafeGuard est toujours activée jusqu'à la prochaine utilisation de l'ordinateur. Ce dernier est ainsi totalement protégé.

  Remarque : Il est important que le fichier de mise en veille prolongée soit sur le volume chiffré. Généralement, il se trouve sur C:\.

  Vous pouvez configurer les paramètres d'alimentation appropriés de manière centralisée à l'aide d'Objets de stratégie de groupe ou localement via la boîte de dialogue **Options d'alimentation** du **Panneau de configuration** de l'ordinateur. Définissez l'action du bouton **Veille** sur **Mettre en veille prolongée** ou **Arrêter**.

Mettez en place d'une stratégie de mot de passe forte

Mettez en place une stratégie de mot de passe forte et imposez des changements de mot de passe à intervalles réguliers, surtout pour la connexion au terminal.

Les mots de passe ne doivent être partagés avec quiconque ni écrits.

Formez vos utilisateurs pour choisir des mots de passe forts. Un mot de passe fort suit les règles suivantes :

- Il est assez long pour être sûr : il est conseillé d'utiliser au moins 10 caractères.
- Il contient un mélange de lettres (majuscules et minuscules) ainsi que des caractères spéciaux ou des symboles.
- Il ne contient pas de mot ou de nom fréquemment utilisé.
- Il est difficile à deviner mais simple à se rappeler et à saisir correctement.

Ne désactivez pas l'authentification au démarrage SafeGuard

L'authentification au démarrage SafeGuard fournit une protection de connexion supplémentaire sur le terminal. Avec SafeGuard Full Disk Encryption, elle est installée et activée par défaut. Pour une protection complète, ne la désactivez pas.

Protégez-vous contre l'injection de code

L'injection de code, par exemple à travers une attaque par chargement préalable de fichiers DLL, est possible lorsqu'un attaquant parvient à placer du code malveillant (comme des exécutables) dans des répertoires qui peuvent faire l'objet de recherches pour trouver du code légitime par le logiciel de chiffrement SafeGuard Enterprise. Pour écarter ce type de menace :

- Installez le middleware chargé par le logiciel de chiffrement, par exemple un middleware de token, dans des répertoires inaccessibles aux attaquants externes. Il s'agit généralement de tous des sous-dossiers des répertoires **Windows** et **Program Files**.

- La variable d'environnement PATH ne doit pas contenir de composants qui pointent vers des dossiers accessibles aux attaquants externes (voir ci-dessus).

- Les utilisateurs standard ne doivent pas avoir de droits administratifs.

7.3 Réplication de la base de données SafeGuard Enterprise

La réplication de la base de données SafeGuard Enterprise n'est plus prise en charge à partir de SafeGuard Enterprise 8.1.

7.4 Web Helpdesk

Pour simplifier le flux de travail dans un environnement d'entreprise et réduire les coûts du support, SafeGuard Enterprise fournit une solution Web de récupération pour les clients administrés. Grâce à un mécanisme de Challenge/Réponse convivial, Web Helpdesk aide les utilisateurs qui ne peuvent pas se connecter ou qui ne peuvent pas accéder aux données chiffrées de SafeGuard Enterprise.

Avantages de la procédure Challenge/Réponse

Le mécanisme de Challenge/Réponse est un système d'urgence sécurisé et efficace.

- Aucune donnée confidentielle n'est transmise déchiffrée pendant toute l'opération car Web Helpdesk est uniquement accessible par HTTPS. Les connexions HTTP sont redirigées automatiquement vers HTTPS.
- Cette procédure ne peut être reproduite par un tiers, car les données ne peuvent pas être utilisées ultérieurement ni sur d'autres périphériques.
- Aucune connexion réseau en ligne n'est nécessaire pour le terminal.
- L'utilisateur peut commencer à retravailler rapidement. L'oubli du mot de passe n'entraîne aucune perte de données chiffrées.

Flux de travail Challenge/Réponse

Au cours de la procédure Challenge/Réponse, un code de challenge (chaîne de caractères ASCII) est généré sur le terminal et l'utilisateur communique ce code à un responsable du support. En fonction de ce code de challenge, le responsable du support génère alors un code de réponse qui autorise l'utilisateur à effectuer une action spécifique sur le terminal.

Situations d'urgence classiques nécessitant l'assistance du support

- Un utilisateur a oublié le mot de passe de connexion et le terminal est verrouillé.
- Un utilisateur a oublié ou perdu son token ou sa carte à puce.
- Le cache local de l'authentification au démarrage est partiellement endommagé.
- Un utilisateur est en congé maladie ou en vacances et un de ses collègues doit accéder aux données de son ordinateur.
- Un utilisateur souhaite accéder à un volume chiffré à l'aide d'une clé qui n'est pas disponible sur le terminal.

SafeGuard Enterprise Web Helpdesk propose différents flux de travail de récupération pour ces situations d’urgence classiques, afin de permettre aux utilisateurs d’accéder de nouveau à leur terminal.

7.4.1 Portée de Web Helpdesk

Web Helpdesk fournit le mécanisme de Challenge/Réponse de SafeGuard Enterprise via une interface Web accessible par HTTPS. Il permet au service d’assistance de déléguer les tâches plus facilement dans l’entreprise. Pour ce faire, nul besoin de donner aux employés du support l’accès aux paramètres confidentiels de configuration ou à SafeGuard Management Center.

Le site Web doit être hébergé sur un serveur SafeGuard Enterprise avec les services Internet (IIS ou Internet Information Services).

Remarque : Nous vous conseillons de ne mettre Web Helpdesk qu’à disposition sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, il est déconseillé de mettre Web Helpdesk sur Internet.

Web Helpdesk offre les options suivantes :

- Récupération pour les terminaux administrés (clients SafeGuard Enterprise administrés) *(page 466)*

  Il s’agit de la récupération de connexion pour les ordinateurs administrés de façon centralisée par SafeGuard Management Center. Les terminaux administrés sont répertoriés dans la zone Utilisateurs et ordinateurs de SafeGuard Management Center.
- Récupération à l’aide de clients virtuels *(page 470)*

  Les volumes chiffrés peuvent être récupérés facilement même lorsque la procédure Challenge/Réponse n’est habituellement pas prise en charge, par exemple lorsque l’authentification au démarrage est corrompue.
- Récupération pour les terminaux non administrés (clients Sophos SafeGuard autonomes) *(page 474)*

  Il s’agit de la récupération de connexion des terminaux administrés localement.

7.4.2 Autorisation de connexion à Web Helpdesk pour les utilisateurs sans SafeGuard Enterprise

Il est possible d'utiliser Web Helpdesk sans le client SafeGuard Enterprise.

Les droits d'accès peuvent être gérés en ajoutant ou en supprimant les utilisateurs ou groupes Windows.

Remarque : Cette fonction utilise l'authentification Windows. Lorsque l'authentification Windows est activée, il n'est plus possible de se connecter par le biais d'un utilisateur Active Directory.

7.4.2.1 Conditions préalables

En cas de connexion sans client SafeGuard Enterprise, les conditions préalables suivantes doivent être remplies :

- HTTPS doit être activé sur votre serveur IIS.
- Un groupe d'utilisateurs Windows contenant les utilisateurs autorisés d'accès à Web Helpdesk doit être créé et configuré comme indiqué à la section Configuration d'un groupe d'utilisateur Windows pour SafeGuard Web Helpdesk *(page 461)*.
- L'authentification Windows à Web Helpdesk doit être activée dans SafeGuard Management Center (**Outils** > **Outil de package de configuration** > **Serveurs** > **Win**. **Auth. WHD**).
- Le compte exécutant le pool d'applications doit avoir accès à la base de données.

7.4.2.2 Configuration d'un groupe d'utilisateur Windows pour SafeGuard Web Helpdesk

Pour créer et configurer un groupe d'utilisateur Windows pour accéder à SafeGuard Web Helpdesk, procédez de la manière suivante :

1. Ouvrez l'outil **Utilisateurs et ordinateurs Active Directory** et sélectionnez votre domaine.
2. Cliquez sur votre domaine avec le bouton droit de la souris et sélectionnez **Nouvelle** > **Unité Organisationnelle**.
3. Nommez l'unité organisationnelle et cliquez sur **OK** pour confirmer son nom.
4. Développez votre domaine et cliquez avec le bouton droit de la souris sur **Comptes de service administré**.
5. Sélectionnez **Nouveau** > **Groupe** et saisissez un nom de groupe (par exemple, `Utilisateurs WHD`) et cliquez sur **OK**.

6. Cliquez avec le bouton droit de la souris sur l’unité organisationnelle que vous avez créée à l’étape 3 et sélectionnez **Nouveau > Utilisateur**.
7. Saisissez un nom et un nom de connexion pour l’utilisateur et cliquez sur **Suivant**.
8. Créez un mot de passe et indiquez si l’utilisateur doit changer ce mot de passe à la prochaine connexion.
   Un nouvel utilisateur a été créé dans la nouvelle unité organisationnelle.
9. Ajoutez l’utilisateur au groupe que vous avez créé à l’étape 5.
10. Ouvrez Microsoft SQL Server Management Studio et sélectionnez votre serveur dans l’**Explorateur d’objets** sur la gauche.
11. Sélectionnez **Sécurité** et cliquez avec le bouton droit de la souris sur **Connexions** puis sur **Nouvelle connexion...**.
12. Dans le champ **Nom de connexion**, cliquez sur le bouton **Rechercher**.
13. Dans la boîte de dialogue suivante, cliquez sur le bouton **Types d’objet...** et sélectionnez toutes les cases à cocher.
14. Dans le champ de texte en bas de la boîte de dialogue, saisissez le nom du groupe que vous avez créé à l’étape 5 et cliquez sur **Vérifier les noms**.
15. Si le nom du groupe affiché est correct, cliquez sur **OK** pour le confirmer.
    Le champ **Nom de connexion** de la boîte de dialogue **Nouvelle connexion** est rempli avec le nom du domaine et celui du groupe.
16. Dans le champ **Sélectionner une page** dans le coin supérieur gauche, sélectionnez **Mappages des utilisateurs**.
17. Dans le champ **Utilisateurs mappés à cette connexion**, sélectionnez **SafeGuard**.
18. Définissez **db_datareader** et **db_datawriter** comme membres de rôles de base de données et cliquez sur **OK** pour confirmer.

7.4.2.3 Activation de l’authentification Windows pour SafeGuard Web Helpdesk

1. Ouvrez le Gestionnaire des services Internet (IIS).
2. Sur le volet **Connexions** sur la gauche, sélectionnez **Sites > Site Web par défaut > SGNWHD**.
3. Dans l’espace de travail sous **IIS**, cliquez deux fois sur **Authentification** et sélectionnez **Authentification Windows**.

4. Sur la barre d'**Actions** à droite, cliquez sur **Activer**. Assurez-vous que l'état est défini sur **Activé**.

5. Retournez sur la vue générale et sous **ASP.NET**, cliquez deux fois sur **Règles d'autorisation .NET** pour ajouter trois règles d'autorisation .NET.

   Remarque : indows Server 2008 R2 n'affiche pas d'icône dans les services Internet (IIS) pour les **Règles d'autorisation .NET**. En revanche, il y a un lien vers les **Règles d'autorisation**. Pour modifier ces règles, le rôle **Autorisation d'URL** doit être installé en allant dans **IIS > Sécurité > Autorisation d'URL**.

6. Sur la barre **Actions**, cliquez sur **Ajouter une règle de refus...**.

7. Sélectionnez **Tous les utilisateurs anonymes** et cliquez sur **OK** pour confirmer.

8. Sur la barre **Actions**, cliquez sur **Ajouter une règle d'autorisation...**.

9. Sélectionnez **Rôles ou groupes d'utilisateurs définis** et saisissez le nom de votre groupe d'utilisateurs dans le champ (par exemple : <Nom de domaine>\Utilisateurs WHD) afin d'autoriser l'accès au groupe d'utilisateurs à votre groupe d'utilisateurs spécifiques. Retrouvez plus de renseignements à la section Configuration d'un groupe d'utilisateur Windows pour SafeGuard Web Helpdesk *(page 461)*.

10. Cliquez sur **OK** pour confirmer.

11. Sur la barre **Actions**, cliquez sur **Ajouter une règle de refus...**.

12. Sélectionnez **Tous les utilisateurs** et cliquez sur **OK** pour confirmer.

13. Assurez-vous que les entrées sont dans l'ordre suivant :
    - Refuser - Utilisateurs anonymes - Local
    - Autoriser - <Nom de domaine>\<Nom du groupe> - Local
    - Refuser - Tous les utilisateurs - Local
    - Refuser - Tous les utilisateurs - Héritée

Pour tester la fonctionnalité, veuillez-vous connecter comme indiqué à la section Connexion avec authentification Windows *(page 464)*. Pour vérifier la connexion au serveur, sélectionnez **SGNWHD** sur le volet **Connexions** et cliquez sur **Parcourir*:443 (https)** sur le volet **Actions** sur la gauche.

Si vous devez désactiver l'authentification Windows pour permettre la connexion par le biais d'un utilisateur Active Directory promu, supprimez la règle **Refuser - Tous les utilisateurs anonymes**.

Remarque : Vous pouvez activer l'Authentification Windows en modifiant le fichier web.config sous C:\Program Files (x86)\Sophos\SafeGuard Enterprise\SGNWHD. Par exemple :

```
<configuration>
  <system.web>
    <authentication mode="Windows" />
     <authorization>
      <allow roles="HelpDesk" />
      <deny users="*" />
     </authorization>
  </system.web>
</configuration>
```

7.4.2.4 Connexion avec authentification Windows

Veuillez procéder comme suit :

1. Ouvrez le navigateur et saisissez l'URL.
2. Appelez l'application en saisissant son URL : https://<ID de l'hôte ou adresse IP>/SGNWHD
3. Sélectionnez **Récupération** et procédez comme décrit dans la section appropriée ci-dessous :
   - Récupération pour les terminaux administrés (clients SafeGuard Enterprise administrés) *(page 466)*
   - Récupération à l'aide de clients virtuels *(page 470)*
   - Récupération pour les terminaux non administrés (clients Sophos SafeGuard autonomes) *(page 474)*

7.4.3 Authentification

Les responsables de la sécurité doivent s'authentifier dans Web Helpdesk et sur le serveur SafeGuard Enterprise afin de pouvoir utiliser l'assistant de récupération basé sur le Web. Les responsables de la sécurité se connectent à Web Helpdesk à l'aide de leurs nom d'utilisateur et mot de passe.

Deux cas de figure d'authentification sont possibles :

- Les utilisateurs qui ont été promus au rang de responsables de la sécurité dans SafeGuard Management Center se connectent comme indiqué à la section Connexion à Web Helpdesk sans authentification Windows *(page 465)*.
- Les utilisateurs qui ont été assignés à un groupe d'utilisateurs Web Helpdesk spécifiques avec l'option « Authentification Windows activée » se connecteront comme indiqué à la section Connexion avec authentification Windows *(page 464)*.

7.4.3.1 Préparations dans SafeGuard Management Center

Pour pouvoir procéder à l'authentification dans Web Helpdesk sans utiliser l'authentification Windows, les étapes de préparation suivantes doivent être effectuées dans SafeGuard Management Center.

1. Importez les utilisateurs Web Helpdesk à partir d'Active Directory dans la base de données SafeGuard Enterprise.

2. Assignez les certificats d'utilisateur à ces utilisateurs. Les certificats (fichier .p12) doivent être disponibles dans la base de données.

3. Cliquez avec le bouton droit de la souris sur l'utilisateur et sélectionnez **Faire de cet utilisateur un responsable de la sécurité** afin de promouvoir les futurs utilisateurs de Web Helpdesk en responsables de la sécurité.

4. Assignez le rôle de **Responsable du support** aux responsables de la sécurité afin de les autoriser à s'authentifier dans Web Helpdesk.
   Les responsables de la sécurité peuvent alors se connecter à Web Helpdesk à l'aide de leur nom de responsable de la sécurité défini, qui est une combinaison de leur nom d'utilisateur Windows et du nom du domaine qui leur est assigné. Le mot de passe Windows est requis pour assurer la protection des certificats.

   Remarque : Si le certificat est créé lors de la promotion d'un utilisateur, ce dernier doit utiliser le mot de passe du certificat pour se connecter à SafeGuard Management Center. Il va devoir saisir le mot de passe du certificat même s'il est invité à saisir le mot de passe Windows.

5. Accordez leur les droits d'accès sur les objets qu'ils vont utiliser comme, par exemple, les domaines ou les unités organisationnelles.
   Si votre domaine n'apparaît pas dans Web Helpdesk, procédez de la manière suivante :

6. Ouvrez SafeGuard Management Center et cliquez sur **Utilisateurs et ordinateurs**.

7. Sur l'arborescence apparaissant sur la gauche, sélectionnez votre domaine.

8. Dans l'onglet **Accès**, assurez-vous que l'utilisateur auquel vous voulez accorder l'accès apparaît dans la liste.

Remarque : Les responsables de la sécurité de Web Helpdesk doivent s'authentifier sur le serveur SafeGuard Enterprise. L'authentification via un token n'est pas prise en charge dans Web Helpdesk.

7.4.3.2 Connexion à Web Helpdesk sans authentification Windows

1. Démarrez votre navigateur.

2. Appelez l'application en saisissant l'URL suivante : https://<ID de l'hôte ou adresse IP>/SGNWHD

3. Sur la page **Bienvenue**, saisissez le nom du responsable de la sécurité que vous avez créé dans SafeGuard Management Center au format suivant : <nom d'utilisateur>@<DOMAINE> par exemple ResponsableWHD@MONDOMAINE.

4. Saisissez votre mot de passe Windows.

   Remarque : Si le certificat est créé lors de la promotion d'un utilisateur, ce dernier doit utiliser le mot de passe du certificat pour se connecter à SafeGuard Management Center. Il va devoir saisir le mot de passe du certificat même s'il est invité à saisir le mot de passe Windows.

5. Cliquez sur **Connexion**.

Vous êtes connecté à Web Helpdesk.

7.4.4 Récupération pour les terminaux administrés (clients SafeGuard Enterprise administrés)

SafeGuard Enterprise fournit la procédure de récupération aux terminaux protégés par le client SafeGuard Enterprise administré dans différentes situations de récupération d'urgence, par exemple la récupération de mots de passe ou l'accès aux données par démarrage à partir d'un support externe.

Le programme détermine de façon dynamique si le chiffrement intégral du disque de SafeGuard Enterprise ou si le Chiffrement de lecteur BitLocker est utilisé et règle le flux de travail de récupération en conséquence.

7.4.4.1 Actions de récupération pour les terminaux administrés

Le flux de travail de récupération dépend du type de client SafeGuard Enterprise pour lequel une récupération est demandée.

Remarque : Pour les terminaux chiffrés BitLocker, l'action de récupération consiste à récupérer la clé utilisée pour chiffrer un volume spécifique. La récupération de mots de passe n'est pas proposée.

Récupération du mot de passe à l'authentification au démarrage

L'une des situations les plus courantes est l'oubli du mot de passe par l'utilisateur. Par défaut, SafeGuard Enterprise est installé avec l'authentification au démarrage (POA) activée. Le mot de passe à l'authentification au démarrage permettant d'accéder au terminal est identique au mot de passe Windows.

Si l’utilisateur a oublié le mot de passe au niveau de l’authentification au démarrage, le responsable du support peut générer une réponse pour **Démarrer le client SGN avec une connexion utilisateur**, mais sans afficher le mot de passe de l’utilisateur. Cependant, dans ce cas, après la saisie du code de réponse, le terminal démarre le système d’exploitation. L’utilisateur doit donc changer son mot de passe Windows conformément aux conditions définies sur le domaine. L’utilisateur peut alors se connecter à Windows ainsi qu’à l’authentification au démarrage à l’aide du nouveau mot de passe.

Bon usage de récupération du mot de passe à l’authentification au démarrage

Si l’utilisateur a oublié son mot de passe, nous vous conseillons d’utiliser les méthodes suivantes afin d’éviter d’avoir à réinitialiser le mot de passe de manière centralisée :

- **Utilisation de Local Self Help :** Local Self Help permet à l’utilisateur d’afficher son mot de passe et de continuer à l’utiliser. Ceci évite d’avoir à réinitialiser le mot de passe ou de demander de l’aide au support technique.

- **Utilisation de la procédure Challenge/Réponse pour les clients SafeGuard Enterprise (administrés) :** nous déconseillons la réinitialisation centralisée du mot de passe dans Active Directory avant la procédure Challenge/Réponse. En effet, ceci vous donne la garantie que le mot de passe demeure synchronisé entre Windows et SafeGuard Enterprise. Assurez-vous que le support technique de Windows est bien informé.

  Remarque : La réinitialisation du mot de passe par Challenge/Réponse est uniquement disponible sur les terminaux Windows.

En tant que responsable du support de SafeGuard Enterprise, générez une réponse pour **Démarrer le client SGN avec une connexion utilisateur** à l’aide de l’option **Afficher le mot de passe utilisateur**. Vous évitez de cette manière d’avoir à réinitialiser le mot de passe de l’utilisateur dans Active Directory. L’utilisateur peut continuer à travailler avec le mot de passe actuel et le modifier localement par la suite, s’il le souhaite.

Remarque : Cette option n’est pas disponible sur les terminaux protégés par BitLocker ou FileVault2.

Accès aux données par démarrage du terminal à partir d’un support externe

Il est également possible d’utiliser la procédure Challenge/Réponse pour autoriser le démarrage d’un terminal à partir d’un support externe, par exemple WinPE. Pour ce faire, l’utilisateur doit sélectionner **Poursuivre le démarrage à partir de : Disquette/Support externe** dans la boîte de dialogue de connexion de l’authentification au démarrage et lancer le challenge. À la réception de la réponse, l’utilisateur saisit comme d’habitude les codes d’accès dans l’authentification au démarrage et poursuit le démarrage à partir du support externe.

Remarque : Cette option n’est pas disponible sur les terminaux protégés par BitLocker ou FileVault2.

Les conditions suivantes doivent être remplies pour pouvoir accéder à un volume chiffré :

- Le périphérique à utiliser doit contenir le pilote du filtre SafeGuard Enterprise. Retrouvez plus de renseignements dans l’article 108805 de la base de connaissances de Sophos.

- L’utilisateur doit démarrer le terminal à partir d’un support externe. Vous pouvez lui octroyer ce droit en définissant une stratégie dans SafeGuard Management Center et en l’affectant au terminal (**Stratégie > Authentification > Accès > L’utilisateur peut uniquement démarrer à partir du disque dur interne > Non**).
- Le terminal doit autoriser le démarrage à partir du support externe.
- Seuls les volumes chiffrés avec la clé machine définie sont accessibles. Ce type de chiffrement de clés peut être défini dans une stratégie de chiffrement des périphériques dans SafeGuard Management Center et assigné au terminal.

Remarque : Lorsque vous utilisez un support externe tel que WinPE pour accéder au lecteur chiffré, vous accédez uniquement à une partie du volume.

Restauration du cache de la stratégie SafeGuard Enterprise

Si la mémoire cache de la stratégie SafeGuard Enterprise est endommagée, l'utilisateur est invité automatiquement à lancer une procédure Challenge/Réponse lors de la connexion à l'authentification au démarrage.

7.4.4.2 Création d’une réponse pour les terminaux administrés

Pour créer une réponse pour les ordinateurs administrés (clients SafeGuard Enterprise), le nom de l’ordinateur et le nom de domaine sont nécessaires.

1. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise**.
2. Dans la liste, sélectionnez le domaine requis.
3. Saisissez le nom de l’ordinateur requis. Vous pouvez procéder de plusieurs façons :
    - Sélectionnez un nom en cliquant sur **[...]**, puis sur **Rechercher** dans la fenêtre contextuelle. Une liste des ordinateurs s’affiche. Sélectionnez l’ordinateur requis, puis cliquez sur **OK**. Le nom de l’ordinateur s’affiche désormais dans la fenêtre **Type de récupération** sous **Domaine**.
    - Saisissez le nom abrégé de l’ordinateur. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S’il est trouvé, le nom d’ordinateur unique s’affiche.

- Saisissez directement le nom de l’ordinateur au format de nom unique, par exemple :

  CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=com

4. Cliquez sur **Suivant**.

Le programme détermine ensuite de façon dynamique si c’est le chiffrement intégral du disque de SafeGuard Enterprise ou le Chiffrement de lecteur BitLocker qui est utilisé et ajuste le flux de travail de récupération en conséquence.

- S’il s’agit d’un ordinateur protégé par SafeGuard Enterprise, l’étape suivante requiert la sélection des informations de l’utilisateur.
- S’il s’agit d’un ordinateur chiffré avec BitLocker, un volume qui n’est plus accessible peut être récupéré. L’étape suivante nécessite la sélection du volume à déchiffrer.

Création d’une réponse pour les ordinateurs protégés par le chiffrement intégral du disque de SafeGuard Enterprise

1. Dans **Domaine**, sélectionnez le domaine requis de l’utilisateur. S’il s’agit d’un utilisateur local, sélectionnez **Utilisateur local sur <nom de l’ordinateur>**.
2. Recherchez le nom de l’utilisateur requis. Procédez de l’une des manières suivantes :
   - Cliquez sur **Rechercher par Nom affiché**. Sélectionnez le nom requis dans la liste et cliquez sur **OK**.
   - Cliquez sur **Rechercher par Nom de connexion**. Sélectionnez le nom requis dans la liste et cliquez sur **OK**.
   - Saisissez directement le nom de l’utilisateur. Assurez-vous d’orthographier le nom correctement.
3. Cliquez sur **Suivant**. Une fenêtre s’affiche, dans laquelle vous pouvez saisir le code de challenge.
4. Saisissez le code de challenge que l’utilisateur vous a transmis et cliquez sur **Suivant**. Ce code est vérifié. S’il a été saisi de façon incorrecte, le terme **Non valide** s’affiche au-dessous du bloc contenant l’erreur.
5. Si le code de challenge a été saisi correctement, l’action de récupération demandée par le client SafeGuard Enterprise, ainsi que les actions de récupération disponibles sur le terminal s’affichent. Les actions disponibles pour la réponse dépendent des actions demandées sur le terminal lors de l’appel du challenge. Par exemple, si **Token cryptographique demandé** est requis, les actions disponibles pour la réponse sont **Démarrer le client SGN avec une connexion utilisateur** et **Démarrer le client SGN sans connexion utilisateur**.
6. Sélectionnez l’action que l’utilisateur doit exécuter.
7. Si l’action **Démarrer le client SGN avec une connexion utilisateur** a été sélectionnée comme réponse, vous pouvez également sélectionner **Afficher le mot de passe utilisateur** afin d’afficher le mot de passe sur le terminal cible.
8. Cliquez sur **Suivant**. Un code de réponse est généré.

9. Lisez ou envoyez le code de réponse à l’utilisateur. Une aide à l’épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L’utilisateur peut ensuite saisir le code de réponse sur le terminal et exécuter l’action autorisée.

Création d’une réponse pour les ordinateurs protégés par le Chiffrement de lecteur BitLocker

1. Sélectionnez le volume auquel accéder, puis cliquez sur **Suivant**. Web Helpdesk affiche alors la clé de récupération à 48 chiffres correspondante.
2. Fournissez cette clé à l’utilisateur.

L’utilisateur peut alors la saisir, afin de pouvoir accéder au volume chiffré BitLocker sur son ordinateur.

7.4.5 Récupération à l’aide de clients virtuels

L’utilisation des clients virtuels pour la récupération de l’accès à des volumes chiffrés dans SafeGuard Enterprise permet la récupération même dans des situations d’urgence complexes.

Ce type de récupération peut être appliquée dans les situations classiques suivantes :

- L’authentification au démarrage est corrompue.
- Un volume est chiffré avec une clé différente de celle de la clé machine définie sur l’ordinateur. La clé nécessaire n’est pas disponible dans l’environnement de l’utilisateur. Par conséquent, elle doit être identifiée dans la base de données, puis transférée vers le terminal de façon sécurisée.

Remarque : La récupération à l’aide d’un client virtuel doit uniquement être utilisée pour résoudre des situations de récupération complexes. Si les problèmes mentionnés ci-dessus ont lieu, l’utilisation d’un client virtuel est appropriée. Cependant, si seule la clé nécessaire manque pour la récupération d’un volume, la meilleure solution consiste à affecter tout simplement la clé manquante au jeu de clés de l’utilisateur approprié.

Dans ces situations, SafeGuard Enterprise propose la solution suivante :

Pour activer une procédure Challenge/Réponse dans cette situation, vous pouvez créer des fichiers spécifiques, appelés clients virtuels, dans SafeGuard Management Center et les distribuer à l’utilisateur avant le démarrage de la session de Challenge/Réponse. La procédure de Challenge/Réponse peut ensuite être lancée sur le terminal à l’aide des fichiers du client virtuel, de l’outil de récupération de clé RecoveryKeys.exe et d’un CD-ROM d’environnement WinPE modifié de SafeGuard Enterprise. Le responsable du support sélectionne alors les clés requises et génère un code de réponse. L’accès aux volumes chiffrés est autorisé lorsque l’utilisateur saisit le code de réponse tandis que les clés requises sont transférées dans la réponse.

Remarque : Dans Web Helpdesk, la récupération à l'aide des clients virtuels n'est pas prise en charge pour les terminaux non administrés (clients Sophos SafeGuard autonomes). Utilisez plutôt SafeGuard Management Center.

7.4.5.1 Flux de travail de récupération à l'aide de clients virtuels

Retrouvez plus de renseignements dans le *Manuel d'administration de SafeGuard Enterprise*.

1. Le responsable du support crée le client virtuel dans la zone **Clés et certificats** de SafeGuard Management Center et l'exporte dans un fichier. Ce fichier, appelé recoverytoken.tok, doit être distribué aux utilisateurs et mis à leur disposition avant la session de Challenge/Réponse.

2. L'utilisateur doit ensuite démarrer un CD-ROM de récupération de SafeGuard Enterprise ou tout autre CD-ROM à l'aide d'un environnement WinPE modifié de SafeGuard Enterprise sur son ordinateur, à partir du BIOS, sans aucune authentification au démarrage, puis lancer une session de Challenge/Réponse à l'aide d'un outil de récupération de clé de SafeGuard Enterprise.
   Dans la base de données SafeGuard Enterprise, le fichier du client virtuel est utilisé et indiqué dans le challenge au lieu du nom de l'utilisateur ou de l'ordinateur qui n'est pas disponible dans ce cas.

3. L'outil de récupération de clé de l'utilisateur indique alors à ce dernier les volumes qui sont chiffrés et les clés qui sont utilisées pour chacun de ces volumes. L'utilisateur fournit ensuite ces informations au responsable du support.

4. Le responsable du support identifie le client virtuel dans la base de données et sélectionne la clé requise pour accéder aux volumes chiffrés : soit une clé unique, soit plusieurs clés exportées vers un fichier de clé. Le responsable du support génère alors le code de réponse.

5. L'utilisateur saisit le code de réponse, dans lequel les clés requises sont transportées. Pour accéder de nouveau aux volumes chiffrés, l'utilisateur saisit le code de réponse et redémarre l'ordinateur.

7.4.5.2 Actions de récupération à l'aide de clients virtuels

Pour que l'utilisateur puisse accéder aux volumes chiffrés à l'aide des clés qui ne sont pas à sa disposition, les clés de chiffrement correctes doivent être transférées de la base de données vers l'environnement de l'utilisateur.

La procédure Challenge/Réponse applique donc deux actions à l'aide des clients virtuels :

- Transfert d'une seule clé

- Transfert de plusieurs clés dans un fichier de clé chiffré

Transfert d’une seule clé

Un Challenge/Réponse peut être lancé pour récupérer une seule clé afin d’accéder à un volume chiffré. Le responsable du support doit sélectionner la clé nécessaire dans la base de données, puis générer un code de réponse. Cette clé est chiffrée et transférée vers le terminal, une fois le code de réponse saisi. Si ce code de réponse est correct, la clé transférée est importée dans la banque de clés locales. Ensuite, tous les volumes chiffrés à l’aide de cette clé sont accessibles.

Transfert de plusieurs clés dans un fichier de clé chiffré

Une procédure Challenge/Réponse peut être lancée en vue de récupérer plusieurs clés afin d’accéder aux volumes chiffrés. Les clés sont stockées dans un fichier, qui est chiffré par mot de passe. Pour ce faire, le responsable du support doit avoir exporté une ou plusieurs clés requises à stocker dans un fichier. Ce fichier est chiffré à l’aide d’un mot de passe aléatoire, qui est stocké dans la base de données. Ce mot de passe est exclusif à chaque fichier de clé créé.

Le fichier de clé chiffré doit être transféré vers l’environnement de l’utilisateur et mis à la disposition de l’utilisateur. Pour déchiffrer ce fichier de clé, l’utilisateur doit alors lancer une session Challenge/Réponse via l’outil de récupération de clé RecoverKeys.exe. Au cours de cette session, le mot de passe est transféré vers le terminal cible. Le responsable du support génère alors une réponse, puis sélectionne le mot de passe approprié pour déchiffrer le fichier de clé. Le mot de passe est transféré au terminal cible dans le code de réponse. Le fichier de clé peut alors être déchiffré à l’aide du mot de passe.

Les clés contenues dans le fichier de clé sont importées dans la zone de stockage des clés sur le terminal et tous les volumes chiffrés à l’aide des clés disponibles sont à nouveau accessibles.

Remarque : Avec Web Helpdesk, un fichier de clé et le mot de passe correspondant sont supprimés de la base de données dès qu’ils ont été utilisés dans une session de Challenge/Réponse. Veuillez donc créer un nouveau fichier de clé et un mot de passe après chaque session de Challenge/Réponse réussie.

7.4.5.3 Réponse à l'aide de clients virtuels

Conditions préalables

- Le client virtuel doit avoir été créé dans la zone **Clés et certificats** de SafeGuard Management Center.
- Le responsable du support doit être en mesure de localiser le client virtuel dans la base de données. Les clients virtuels sont identifiés de façon unique par leur nom.

- Le fichier du client virtuel, **recoverytoken.tok**, doit être à la disposition de l’utilisateur. Ce fichier doit être stocké dans le même dossier que l’outil de récupération de clé. Nous vous conseillons de stocker ce fichier sur une carte mémoire.
- Lorsque la récupération de plusieurs clés est demandée, le responsable du support doit d’abord créer un fichiers de clé contenant les clés de récupération nécessaires dans le champ **Clés et certificats** de SafeGuard Management Center. Le fichier de clé doit être à la disposition de l’utilisateur pour qu’une récupération puisse être effectuée. Le mot de passe de chiffrement de ce fichier de clé doit être indiqué dans la base de données.
- L’utilisateur doit avoir démarré l’outil de récupération de clé et lancé la session de Challenge/ Réponse.
- Une réponse ne peut être lancée que pour des clés assignées. Si une clé est inactive, c’est-à-dire qu’elle n’est pas assignée à au moins un utilisateur, une réponse pour client virtuel est impossible. Dans ce cas, la clé inactive peut être assignée de nouveau à un autre utilisateur et une réponse pour cette clé peut être de nouveau générée.

Création d’une réponse à l’aide de clients virtuels

1. En tant que responsable du support, sélectionnez **Client virtuel** dans la fenêtre **Type de récupération**.

2. Saisissez le nom du client virtuel que l’utilisateur vous a indiqué. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Saisissez directement le nom unique.
   - Sélectionnez un nom en cliquant sur **[...]**, puis sur **Rechercher** dans la fenêtre contextuelle. La liste des clients virtuels s’affiche. Sélectionnez le client virtuel requis, puis cliquez sur **OK**. Le nom du client virtuel s’affiche alors dans la fenêtre **Type de récupération** dans **Client virtuel**.

3. Cliquez sur **Suivant**. La page dans laquelle vous pouvez sélectionner l’action de récupération s’affiche.

4. Sélectionnez l’action de récupération que l’utilisateur doit effectuer, puis cliquez sur **Suivant**.
   - Si vous devez transférer une seule clé de récupération, sélectionnez **Clé requise**. Dans la liste, sélectionnez la clé nécessaire. Cliquez sur **[...]**. Vous pouvez afficher les clés en fonction de leur ID ou de leur nom symbolique. Cliquez sur **Rechercher**, sélectionnez la clé, puis cliquez sur **OK**.
   - Si l’utilisateur a besoin d’un fichier de clé contenant plusieurs clés de récupération, sélectionnez **Mot de passe du fichier de clé requis** afin de transmettre à l’utilisateur le mot de passe du fichier de clé chiffré. Sélectionnez le fichier de clé requis. Cliquez sur **[...]**, puis sur **Rechercher**. Sélectionnez le fichier de clé et cliquez sur **OK**.

   Vous pouvez sélectionner l’option **Mot de passe du fichier de clé demandé** uniquement si un fichier de clé a été créé dans la zone **Clés et certificats** de SafeGuard Management Center et si le mot de passe de chiffrement du fichier de clé est stocké dans la base de données. Avec Web Helpdesk, les fichiers de clés et les mots de passe correspondants sont supprimés de la base

de données dès qu'ils ont été utilisés dans une session de Challenge/Réponse. Veuillez donc créer un nouveau fichier de clé et un mot de passe après chaque session de Challenge/Réponse réussie.

5. Cliquez sur **Suivant**. La page dans laquelle vous devez saisir le code de challenge s'affiche.
6. Saisissez le code de challenge que l'utilisateur vous a transmis et cliquez sur **Suivant**. Ce code est vérifié. S'il a été saisi de façon incorrecte, le terme **Non valide** s'affiche au-dessous du bloc contenant l'erreur.
7. Si le code de challenge a été saisi correctement, le code de réponse est généré. Lisez le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.
   - Si une seule clé est demandée, la clé générée est transférée dans le code de réponse.
   - Si un mot de passe est demandé pour le fichier de clé chiffré, il est transféré dans le code de réponse. Ce fichier de clé est ensuite supprimé.
8. L'utilisateur doit saisir le code de réponse sur le terminal.
9. L'utilisateur doit redémarrer l'ordinateur et se reconnecter pour accéder aux volumes.

Les volumes sont à nouveau accessibles.

7.4.6 Récupération pour les terminaux non administrés (clients Sophos SafeGuard autonomes)

SafeGuard Enterprise inclut également des procédures Challenge/Réponse pour les terminaux non administrés (clients Sophos SafeGuard autonomes). Ceux-ci n'ont aucune connexion au serveur SafeGuard Enterprise et sont administrés localement. Comme ils ne sont pas enregistrés dans la base de données SafeGuard Enterprise, leur identification pendant une procédure Challenge/Réponse est impossible. La procédure Challenge/Réponse des terminaux autonomes est donc basée sur le fichier de clé de récupération (XML) créé lors de la configuration du terminal. Retrouvez plus de renseignements à la section Création d'un package de configuration pour les terminaux non administrés *(page 105)*. Le fichier de récupération de clé est généré pour chaque terminal non administré et contient la clé machine définie, qui est chiffrée à l'aide du certificat de l'entreprise. Pendant la procédure Challenge/Réponse, le fichier de récupération de clé doit être mis à disposition du responsable du support, par exemple sur un lecteur flash USB ou sur un partage réseau. Lorsque le responsable du support est en mesure d'accéder au fichier de récupération, une réponse peut être générée. Si le fichier n'est pas accessible, la procédure de récupération ne peut pas être effectuée.

7.4.6.1 Actions de récupération pour les terminaux non administrés

La procédure Challenge/Réponse pour les terminaux non administrés (client Sophos SafeGuard autonome) doit être lancée dans les situations suivantes :

- L’utilisateur a saisi un mot de passe incorrect un trop grand nombre de fois.
- L’utilisateur a oublié le mot de passe.
- Un cache local endommagé doit être réparé.

Aucune clé utilisateur n’est disponible dans la base de données pour les terminaux non administrés. Par conséquent, la seule action de récupération possible dans une session de Challenge/Réponse est **Démarrer le client Sophos SafeGuard sans connexion utilisateur**.

La procédure Challenge/Réponse permet à l’utilisateur de se connecter à partir de l’authentification au démarrage. L’utilisateur peut également se connecter à Windows, même si le mot de passe Windows doit être réinitialisé.

L’utilisateur a saisi un mot de passe incorrect un trop grand nombre de fois

Dans ce cas de figure, la réinitialisation du mot de passe n’est pas nécessaire. En effet, la procédure Challenge/Réponse permet à l’utilisateur de se connecter à l’authentification au démarrage. L’utilisateur peut ensuite saisir le mot de passe Windows approprié et réutiliser le terminal.

L’utilisateur a oublié le mot de passe

Remarque : Nous vous conseillons d’utiliser Local Self Help pour récupérer un mot de passe oublié. Grâce à Local Self Help, vous pouvez afficher le mot de passe actuel et continuer à l’utiliser. Ceci évite d’avoir à réinitialiser le mot de passe ou de demander de l’aide au support technique.

Lors de la récupération d’un mot de passe oublié via la procédure Challenge/Réponse, la réinitialisation de mot de passe est requise.

1. La procédure Challenge/Réponse permet à l’ordinateur de démarrer à partir de l’authentification au démarrage.
2. Dans la boîte de dialogue de connexion Windows, l’utilisateur ne connaît pas le mot de passe et doit par conséquent le modifier au niveau Windows. D’autres actions de récupération doivent être effectuées via des moyens Windows standard. En effet, elles sont hors du champ d’application de SafeGuard Enterprise. Nous vous conseillons d’utiliser les méthodes de réinitialisation de mot de passe Windows.
    - À l’aide d’un compte de service ou administrateur disponible sur votre ordinateur avec les droits Windows requis.
    - À l’aide d’un disque de réinitialisation de mot de passe Windows.

En tant que responsable du support, vous pouvez informer l’utilisateur de la procédure à appliquer et lui fournir les codes d’accès Windows supplémentaires ou le disque requis.

3. L’utilisateur saisit le nouveau mot de passe dans la boîte de dialogue de connexion Windows fourni par le support. L’utilisateur modifie ensuite ce mot de passe immédiatement en choisissant une valeur connue de lui seul.

4. SafeGuard Enterprise détecte que le nouveau choix de mot de passe ne correspond pas au mot de passe SafeGuard Enterprise utilisé actuellement au niveau de l’authentification au démarrage. L’utilisateur est invité à saisir son ancien mot de passe SafeGuard Enterprise et, puisqu’il a oublié son mot de passe, il doit cliquer sur **Annuler**.

5. Dans SafeGuard Enterprise, un nouveau certificat est nécessaire afin de pouvoir définir un nouveau mot de passe sans avoir à fournir l’ancien.

6. Un nouveau certificat d’utilisateur est créé en fonction du nouveau choix de mot de passe Windows. L’utilisateur peut donc se reconnecter à l’ordinateur ainsi qu’à l’authentification au démarrage à l’aide du nouveau mot de passe.

   Clés pour SafeGuard Data Exchange

   Si l’utilisateur a oublié son mot de passe Windows et que celui-ci a été réinitialisé, les clés déjà créées pour SafeGuard Data Exchange ne pourront pas être utilisées sans la phrase secrète correspondante. Pour continuer à utiliser les clés utilisateur déjà générées pour SafeGuard Data Exchange, l’utilisateur doit se souvenir des phrase secrètes SafeGuard Data Exchange afin de les réactiver.

7.4.6.2 Création d’une réponse pour les terminaux non administrés

Pour générer une réponse pour un ordinateur non administré, indiquez le nom du fichier de récupération (au format .xml).

1. Dans Web Helpdesk, sur le menu **Outils**, cliquez sur **Récupération**.
2. Dans **Type de récupération**, sélectionnez **Client autonome**.
3. Cliquez sur **Parcourir** pour localiser le fichier (.xml) de récupération de clé requis.
4. Saisissez le code de challenge que l’utilisateur vous a indiqué.
5. Sélectionnez l’action que l’utilisateur doit entreprendre, puis cliquez sur **Suivant**.
6. Un code de réponse est généré. Lisez le code de réponse à l’utilisateur. Une aide à l’épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L’utilisateur peut saisir le code de réponse, exécuter l’action requise, puis reprendre son travail.

7.4.7 Journalisation des événements de Web Helpdesk

Les événements Web Helpdesk peuvent être journalisés dans l'Observateur d'événements Windows ou dans la base de données SafeGuard Enterprise. Les événements de toutes les activités du support peuvent être journalisés. Il est ainsi possible de savoir qui s'est connecté à Web Helpdesk, quel utilisateur a demandé un challenge ou quelles actions de récupération ont été requises.

La journalisation des événements de Web Helpdesk est activée dans SafeGuard Management Center par une stratégie qui doit être publiée dans un package de configuration et déployée sur le service Web Helpdesk.

Les événements consignés dans la base de données centrale de SafeGuard Enterprise peuvent être consultés à l'aide de l'Observateur d'événements de SafeGuard Management Center.

7.4.7.1 Activation de la journalisation des événements de Web Helpdesk

La journalisation pour Web Helpdesk est configurée dans SafeGuard Management Center.

Vous devez disposer des droits appropriés pour créer des stratégies et consulter des événements.

1. Dans SafeGuard Management Center, dans la zone de navigation **Stratégie**, créez une stratégie de type **Journalisation**. Sélectionnez les événements à consigner dans le journal. Enregistrez vos modifications.

2. Créez un nouveau **Groupe de stratégies**. Ajoutez la stratégie de type **Journalisation** à ce groupe. Enregistrez vos modifications.

3. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**. Sélectionnez **Packages du client administré** et cliquez sur **Ajouter un package de configuration**. Sélectionnez le groupe de stratégies à inclure dans le package de configuration. Sélectionnez un emplacement de stockage et cliquez sur **Créer un package de configuration**.

4. Dans SafeGuard Management Center, affectez le groupe de stratégies au domaine contenant le serveur Web Helpdesk. Activez-le. Retrouvez plus de renseignements à la section Assignation des stratégies *(page 100)*.

5. Sur le serveur Web Helpdesk, installez le package de configuration créé auparavant. Redémarrez le service.

   La journalisation des événements de Web Helpdesk a été activée.

6. Connectez-vous à Web Helpdesk et lancez une procédure Challenge/Réponse.

7. Dans SafeGuard Management Center, cliquez sur l'onglet **Rapports**. Dans la zone d'action de l'**Observateur des événements**, sur le côté droit, cliquez sur l'icône en forme de loupe pour voir les événements journalisés de Web Helpdesk.

7.5 Récupération

SafeGuard Enterprise offre les procédures de récupération pour les cas de figure suivants :

- Récupération par appareils mobiles *(page 479)*
- Récupération des terminaux chiffrés avec BitLocker *(page 333)*
- Clé de secours pour terminaux Mac *(page 383)*
- Récupération de SafeGuard Full Disk Encryption avec l'authentification au démarrage. Retrouvez plus de renseignements dans le Manuel d'administration de SafeGuard Enterprise.

7.5.1 Flux de travail Challenge/Réponse

La procédure Challenge/Réponse repose sur les deux composants suivants :

- le terminal sur lequel le code de challenge est généré.
- SafeGuard Management Center où, en tant que responsable du support possédant les droits correspondants, vous créez un code de réponse qui autorisera l'utilisateur à effectuer l'action requise sur l'ordinateur.

  Remarque : Pour une procédure Challenge/Réponse, vous avez besoin des droits d'**Accès complet** pour les ordinateurs/utilisateurs concernés.

1. Sur le terminal, l'utilisateur demande le code de challenge. En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage SafeGuard, soit dans l'outil de récupération de clé KeyRecovery.

   Un code de challenge sous la forme d'une chaîne de caractères ASCII est généré puis affiché.

2. L'utilisateur contacte le support technique et leur fournit l'identification nécessaire et le code de challenge.
3. Le support lance l'assistant de récupération dans SafeGuard Management Center.

4. Le support technique sélectionne le type de récupération approprié, confirme les informations d'identification et le code de challenge, puis sélectionne l'action de récupération souhaitée.

   Un code de réponse sous la forme d'une chaîne de caractères ASCII est généré et s'affiche.

5. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou SMS.

6. L'utilisateur saisit le code de réponse, En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage SafeGuard, soit dans l'outil de récupération de clé KeyRecovery.

   L'utilisateur est ensuite autorisé à effectuer l'action convenue, par exemple à réinitialiser le mot de passe et à reprendre son travail.

7.5.2 Lancement de l'assistant de récupération

Pour pouvoir effectuer une procédure de récupération, assurez-vous de disposer des droits et des autorisations requis.

1. Connectez-vous à SafeGuard Management Center.
2. Cliquez sur **Outils > Récupération** dans la barre de menus.

L'**Assistant de récupération** démarre. Vous pouvez sélectionner le type de récupération que vous souhaitez utiliser.

7.5.3 Récupération par appareils mobiles

Les clés de récupération BitLocker et FileVault 2 peuvent être envoyées au serveur Sophos Mobile. Elles seront ajoutées au jeu de clés SafeGuard Enterprise. Les utilisateurs de Sophos Secure Workspace administrés par Sophos Mobile peuvent alors afficher ces clés sur leurs appareils mobiles conformes à des fins de récupération. Sophos Secure Workspace prend en charge la récupération par mobile à partir de la version 6.2. Retrouvez plus de renseignements dans l'Aide à l'utilisation de Sophos Secure Workspace 6.2.

Conditions requises :

- Le partage du jeu de clés entre SafeGuard Enterprise et Sophos Mobile doit être configuré. L'option **Récupération par mobile** doit être activée comme indiqué à la section Partage du jeu de clés SafeGuard Enterprise avec les appareils mobiles administrés par Sophos Mobile *(page 436)*.
- Sophos Secure Workspace 6.2 doit être utilisé sur les appareils mobiles.

- Les utilisateurs doivent être des utilisateurs SGN sur les terminaux. Ils doivent se trouver dans la liste des assignations utilisateur machine des terminaux concernés.
- Les utilisateurs doivent s'être connecté à un ordinateur particulier à partir duquel ils récupèreront les clés du chiffrement de disque intégral.

Remarque : Pour limiter la quantité de données transmises, seules les clés de dix terminaux sont ajoutées au jeu de clés SafeGuard Enterprise. Ces dix ordinateurs sont ceux qui ont eu le plus de contacts récents avec le serveur.

7.5.3.1 Affichage des clés de récupération sur les appareils mobiles

Remarque : Sophos Secure Workspace doit être installé dans le conteneur Sophos.

Pour voir la clé de récupération d'un ordinateur :

1. Appuyez sur **Clés de récupération** dans le menu pour afficher une liste des ordinateurs qui vous sont assignés.
2. Appuyez sur le nom d'un ordinateur pour afficher sa clé de récupération.
3. Pour déverrouiller votre ordinateur, suivez les instructions affichées sur l'écran BitLocker (Windows) ou FileVault (macOS) de votre ordinateur.

7.6 Outils

Cette section aborde l'utilisation des outils offerts par SafeGuard Enterprise.

Retrouvez les outils dans le répertoire « Tools » de votre logiciel client SafeGuard Enterprise.

À qui s'adresse ce guide ?

Ce guide s'adresse aux administrateurs utilisant SafeGuard Enterprise et agissant en tant que responsables de la sécurité.

7.6.1 Outil « Client/Server Connectivity Check » pour Windows

Si les utilisateurs rencontrent des problèmes de synchronisation de leur terminal avec le serveur, utilisez l'outil de vérification de la connexion client/serveur (Client/Server Connectivity Check) pour obtenir plus de renseignements sur les raisons de l'échec de la communication entre le terminal et le serveur SafeGuard Enterprise. Il vérifie toutes les connexions et affiche les résultats.

Si l’outil détecte un problème de communication, veuillez consulter l’article 109662 de la base de connaissances de Sophos pour obtenir plus de renseignements sur la résolution des problèmes.

7.6.1.1 Vérification de la connexion au serveur

Windows

Ouvrez `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client` et exécutez l’application `SGNCSCC.exe`.

Mac

Ouvrez `/Library/Application Support/Sophos Encryption/` et exécutez l’application `SGNConnectivityTool`.

7.6.2 Affichage des stratégies Synchronized Encryption sur les terminaux

SafeGuard Enterprise offre l’outil de ligne de commande ShowSyncEncPolicyn.exe pour afficher les stratégies Synchronized Encryption actuellement appliquées sur un terminal.

Vous devez toujours exécuter l’outil dans un contexte d’utilisation adéquat. Par exemple, l’exécution de l’outil en tant qu’administrateur sur le terminal de l’utilisateur A n’affichera pas les bonnes stratégies pour l’utilisateur A.

Il affiche :

- La liste des applications Elle contient toutes les applications pour lesquelles le chiffrement de fichiers est exécuté automatiquement (apps intégrées).
- Une liste des extensions de fichiers qui sont considérées par le chiffrement initial et le chiffrement asynchrone.
- Les règles de chiffrement pour Synchronized Encryption. Elles contiennent les chemins des emplacements dans lesquels les fichiers sont chiffrés ou exclus du chiffrement et les clés appropriées.

Paramètres

Vous pouvez appeler ShowSyncEncPolicyn.exe avec les paramètres suivants :

ShowSyncEncpolicyn.exe [-h] [-A] [-a] [-e] [- d]

- La paramètre -h affiche l’aide.
- Le paramètre -A affiche la liste des applications, les extensions de fichiers et les règles de chiffrement.
- Le paramètre -a affiche la liste des applications.
- Le paramètre -e affiche les extensions de fichiers.
- La paramètre -d affiche les règles de chiffrement.

Exemple

```
ShowSyncEncPolicyn.exe -A
```

Les informations suivantes apparaissent :

- Un rappel d’exécution de l’outil dans un contexte d’utilisation adéquat.
- Le champ d’application du chiffrement défini dans la stratégie. Par exemple : **Partout**.
- Les chemins des fichiers chiffrés et de la clé de chiffrement de chaque chemin.
- Les répertoires exclus du chiffrement.
- La liste des extensions de fichiers qui sont considérées par le chiffrement initial et le chiffrement asynchrone.
- La liste des apps intégrées.

7.6.3 Affichage de l’état du système avec SGNState

SafeGuard Enterprise met à disposition l’outil de ligne de commande SGNState pour afficher des informations sur l’état actuel (état du chiffrement et autres informations détaillées sur l’état) de l’installation SafeGuard Enterprise sur un terminal.

Rapports

SGNState peut également être utilisé comme suit :

- Le code renvoyé par SGNState peut être évalué sur le serveur à l’aide d’outils de gestion tiers.
- SGNState /LD renvoie un résultat formaté pour LANDesk pouvant être enregistré dans un fichier.

Paramètres

Vous pouvez appeler l’outil SGNState avec les paramètres suivants :

SGNState [/?] [/H/Type|Status] [/L] [/LD] [/USERLIST]

- Le paramètre /? renvoie des informations sur les paramètres de ligne de commande SGNState disponibles.
- Le paramètre /H Type renvoie des informations supplémentaires sur les types de lecteur.
- Le paramètre /H Status renvoie des informations supplémentaires sur l’état des lecteurs.
- Le paramètre /L affiche les informations suivantes :

  Système d’exploitation

  Version du produit

  Type de chiffrement [SGN | Opal | BitLocker | C/R BitLocker | unknown or earlier version of SGN]

  Authentification au démarrage [yes | no | n/a]

  WOL (état de l’éveil par appel réseau) [yes | no | n/a]

Nom du serveur

Nom du second serveur

Mode de connexion [SGN, no automatic logon | UID/PW | TOKEN/PIN | FINGERPRINT | BL (BitLocker)]

État d'activation du client [ENTERPRISE | OFFLINE]

Dernière réplication de données [date, time]

Connexion au token par certificat appliquée à l'authentification au démarrage [yes | no | n/a]

Mode FIPS activé [yes | no]

Type de certificat d'utilisateur [0 | 1 | 2 | 3|n/a|?]

Code renvoyé [return code]

Versions du pilote de chiffrement de fichier [driver versions]

Informations sur le volume :

Nom	Type	État	Méthode de chiffrement
<nom>	[HD-Part | ...]	[encrypted | not encrypted | ...]	[<nom de l'algorithme> | n/a | ...]
	FLOPPY	Inaccessible	
	REMOV.PART	Interrompu en raison d'un échec	
	REM_PART	Démarrage du chiffrement	
	HD-PART	Chiffrement en cours	
	UNKNOWN	Démarrage du déchiffrement	
		Déchiffrement en cours	
		Non préparé	

- Le paramètre /LD renvoie ces informations formatées pour LANDesk

  La sortie est semblable à la sortie /L, mais chaque ligne commence par « Sophos SafeGuard » :

  Exemple :

  Sophos SafeGuard - Système d'exploitation = Windows 10 Enterprise

  Sophos SafeGuard - Version du produit = 8.20.0.64

  Sophos SafeGuard - Type de chiffrement = BitLocker

...

- Si vous appelez SGNState avec le paramètre /USERLIST, une liste de tous les utilisateurs dans l’assignation utilisateur/machine et les types de certificats qui leur sont assignés s’affiche.

  Type de certificat :

0	Aucun certificat assigné à l’utilisateur.
1	Certificat P7 (par exemple ; connexion du token avec P12 sur carte à puce)
2	Certificat P12
3	Certificat P7+P12 (utilisateur SGN normal)
s/o	Impossible de déterminer le type de certificat.
?	Combinaison de certificat inconnue.

- Code renvoyé

0	aucun volume n’a été chiffré.
1	il y a au moins un volume chiffré.
-1	une erreur s’est produite (par exemple, le chiffrement de périphériques SafeGuard Enterprise n’est pas installé).

7.6.4 Annulation d’une installation en échec avec SGNRollback

Remarque : L’outil SGNRollback doit uniquement être utilisé avec Windows 7 sans BitLocker.

En cas d’échec d’installation de SafeGuard Enterprise sur un terminal, il se peut que l’ordinateur ne soit pas en mesure de démarrer et que son administration à distance soit impossible.

SGNRollback peut réparer une installation SafeGuard Enterprise infructueuse sur un terminal si les conditions suivantes s’appliquent :

- L’authentification au démarrage se bloque au premier démarrage et l’ordinateur ne peut plus être démarré.
- Le disque dur n’est pas chiffré.

SGNRollback permet d’annuler automatiquement les effets de l’échec d’une installation de SafeGuard Enterprise en :

- Permettant le démarrage de l’ordinateur bloqué.

- Supprimant SafeGuard Enterprise.
- Annulant les modifications des autres composants du système d’exploitation.

Démarrez SGNRollback à partir d’un système de récupération Windows (soit WindowsPE, soit BartPE).

7.6.4.1 Conditions préalables

Conditions préalables à l'utilisation de SGNRollback :

- SGNRollback fonctionne avec les systèmes de récupération WinPE et BartPE. Pour pouvoir utiliser SGNRollback à des fins de récupération, veuillez l'intégrer au système de récupération requis. Retrouvez plus de renseignements dans la documentation du système de récupération correspondant.

  Si SGNRollback doit être exécuté par le programme de démarrage automatique, l'administrateur utilisant SGNRollback doit définir les paramètres correspondants dans WinPE comme indiqué à la section Activation du programme de démarrage automatique de SGNRollback pour Windows PE *(page 486)* ou dans BartPE comme indiqué à la section Activation du programme de démarrage automatique de SGNRollback pour BartPE *(page 486)*.

- Le chiffrement intégral du disque de SafeGuard Enterprise est installé.

Remarque : La migration de SafeGuard Easy vers SafeGuard Enterprise n'est pas prise en charge.

7.6.4.2 Démarrage de SGNRollback dans le système de récupération

Vous pouvez démarrer SGNRollback manuellement ou l'ajouter au programme de démarrage automatique du système de récupération.

Activation du programme de démarrage automatique de SGNRollback pour Windows PE

Pour activer le programme de démarrage automatique de SGNRollback pour Windows PE, installez le kit d’installation automatisée (Windows AIK). Retrouvez plus de renseignements sur la création d’un environnement Windows PE et l’exécution automatique d’une application dans le guide de l’utilisateur de l’environnement de préinstallation Windows.

Activation du programme de démarrage automatique de SGNRollback pour BartPE

1. Utilisez la version 3.1.3 ou supérieure de BartPEBuilder pour créer une image PE. Retrouvez plus de renseignements dans la documentation BartPE.
2. Dans BartPE Builder, ajoutez le dossier de l'outil de récupération dans le champ **Custom**.
3. Créez l'image.
4. Copiez le fichier AutoRun0Recovery.cmd à partir du support SafeGuard Enterprise dans le dossier i386 de la version BartPE pour Windows.
5. Créez une commande AutoRun0Recovery.cmd à l'aide des deux lignes de texte suivantes :

   \Recovery\recovery.exe

   exit

6. Exécutez l'outil PEBuilder depuis la ligne de commande :

   Pebuilder -buildis

   Une nouvelle image iso est créée qui intègre le fichier de démarrage automatique.

7. Enregistrez l'image obtenue sur un support de récupération.

Au moment de démarrer cette image, SGNRollback démarre automatiquement.

7.6.4.3 Paramètres

SGNRollback peut être démarré à l'aide du paramètre suivant :

-drv WinDrive	Indique la lettre du lecteur sur lequel l'installation SafeGuard Enterprise devant faire l'objet d'une réparation est installée. Ce paramètre ne peut être utilisé qu'en mode récupération. Il doit être utilisé sur des systèmes à démarrage multiple pour indiquer le bon lecteur.

7.6.4.4 Annulation d'une installation non réussie

Pour annuler les effets d'une installation non réussie de SafeGuard Enterprise sur un terminal, procédez comme suit :

1. Démarrez l'ordinateur à partir du support de récupération contenant le système de récupération, notamment SGNRollback.

2. Démarrez SGNRollback dans le système de récupération. Si le programme de démarrage automatique est présent, SGNRollback démarrera automatiquement. SGNRollback prépare le système d'exploitation pour la désinstallation de SafeGuard Enterprise.
3. Le système vous demande de retirer le support de récupération. Après avoir retiré le support, le système d'exploitation de l'ordinateur est redémarré en mode sans échec.

Toutes les modifications effectuées sont supprimées et SafeGuard Enterprise est désinstallé.

7.6.5 Récupération de l'accès aux ordinateurs à l'aide de l'outil KeyRecovery

L'outil KeyRecovery sert à récupérer l'accès à l'ordinateur dans des situations complexes de récupération d'urgence, par exemple lorsque l'authentification au démarrage est corrompue et que l'ordinateur doit être démarré à partir du disque de récupération SafeGuard. L'outil est démarré dans le contexte d'une procédure de Challenge/Réponse.

Remarque : Retrouvez une description détaillée de cet outil dans le *Manuel d'administration de SafeGuard Enterprise* à la section *Challenge/Réponse à l'aide de clients virtuels*.

7.6.6 Restauration des systèmes de chiffrement intégral du disque SafeGuard Windows BIOS

Remarque : La description suivante se rapporte aux terminaux BIOS Windows protégés par le chiffrement intégral du disque SafeGuard Enterprise à l'aide de l'authentification au démarrage SafeGuard.

SafeGuard Enterprise chiffre les fichiers et les lecteurs de façon transparente. Les volumes de démarrage peuvent également être chiffrés et les fonctions de déchiffrement (code, algorithmes de chiffrement et clé de chiffrement) doivent être disponibles très tôt au cours de la phase de démarrage. C'est la raison pour laquelle les informations chiffrées ne sont pas accessibles si les modules essentiels de SafeGuard Enterprise ne sont pas disponibles ou ne fonctionnent pas.

7.6.6.1 Restauration d'un MBR corrompu

La fonction d'authentification au démarrage de SafeGuard Enterprise est chargée à partir du MBR du disque dur d'un ordinateur. Lorsque l'installation est terminée, SafeGuard Enterprise enregistre une copie de l'original (tel qu'il était avant l'installation de SafeGuard Enterprise) dans son noyau, et modifie le chargeur de PBR à partir de LBA 0. Dans son LBA 0, le MBR modifié contient l'adresse du premier secteur du noyau SafeGuard Enterprise et sa taille totale.

Les problèmes associés au MBR peuvent être résolus avec l'outil de restauration de SafeGuard Enterprise, be_restore.exe. Cet outil est une application Win32 qui doit être exécutée sous Windows et non sous DOS.

Un chargeur MBR défectueux signifie que le système ne peut pas être démarré. Il existe deux manières de le restaurer :

- Restauration du MBR à partir d'une sauvegarde.
- Réparation du MBR.

Pour restaurer un MBR corrompu, procédez comme suit :

1. Nous vous conseillons de créer un CD-ROM Windows PE (environnement préinstallé).
2. Pour utiliser l'outil de restauration be_restore.exe, plusieurs fichiers supplémentaires sont nécessaires. L'outil et les fichiers nécessaires sont disponibles dans le répertoire Tools \KeyRecovery and restore de votre logiciel SafeGuard Enterprise. Copiez tous les fichiers de ce dossier sur une carte mémoire. Veillez à enregistrer tous les fichiers dans **le même** dossier sur votre carte mémoire. Cette condition est nécessaire au démarrage correct de l'outil de restauration.

   Remarque : Pour démarrer be_restore.exe dans un environnement Windows PE, le fichier Windows OLEDLG.dll est requis. Ce fichier n'est pas inclus dans le dossier Tools\KeyRecovery and restore. Ajoutez ce fichier depuis une installation Windows dans le dossier des outils de récupération sur votre CD-ROM de récupération.

3. Si nécessaire, modifiez la séquence de démarrage dans le BIOS et sélectionnez le CD-ROM en priorité.

Remarque : L'outil be_restore.exe peut uniquement restaurer ou réparer le MBR sur le disque 0. Si vous utilisez deux disques durs et que le système est démarré à partir de l'autre disque dur, le MBR ne pourra ni être restauré ni être réparé. Cette condition s'applique également lors de l'utilisation d'un disque dur amovible.

7.6.6.2 Restauration d'une sauvegarde MBR précédemment enregistrée

Chaque ordinateur d'extrémité SafeGuard Enterprise enregistre le secteur de démarrage principal (MBR) SafeGuard Enterprise de son **propre ordinateur** (LBA 0 du disque dur de démarrage après

avoir été modifié par SafeGuard Enterprise) dans la base de données SafeGuard Enterprise. Il peut être exporté dans un fichier à partir de SafeGuard Management Center.

Pour restaurer une sauvegarde du secteur de démarrage principal (MBR) précédemment enregistrée :

1. Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**, puis sélectionnez l'ordinateur approprié dans la zone de navigation.
2. Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés > Paramètres machine > Sauvegarder > Exporter** pour exporter le secteur de démarrage principal (MBR). Cette action génère un fichier de 512 octets portant l'extension .BKN, qui contient le secteur de démarrage principal (MBR).
3. Copiez ce fichier dans le dossier de la carte mémoire dans lequel se trouvent les autres fichiers SafeGuard Enterprise.
4. Insérez maintenant le CD-ROM de démarrage Windows PE dans le lecteur, connectez la carte mémoire contenant les fichiers SafeGuard Enterprise et démarrez l'ordinateur à partir du CD-ROM.
5. Lorsque l'ordinateur est prêt, lancez cmd-box, naviguez jusqu'au répertoire de la carte mémoire contenant les fichiers SafeGuard Enterprise et exécutez be_restore.exe.
6. Sélectionnez **Restore MBR** pour restaurer à partir d’une sauvegarde et sélectionnez le fichier .BKN.

L'outil vérifie à présent si le fichier .BKN sélectionné correspond à l'ordinateur, puis restaure le MBR sauvegardé.

7.6.6.3 Réparation du MBR sans sauvegarde

Même si aucun fichier de sauvegarde MBR n'est disponible localement, be_restore.exe peut réparer un chargeur MBR corrompu. be_restore.exe - **Repair MBR** recherche le noyau SafeGuard Enterprise sur le disque dur, utilise son adresse et recrée le chargeur MBR.

Cette procédure présente de très grands avantages. En effet, aucun fichier de sauvegarde local du MBR spécifique à l'ordinateur n'est nécessaire. Toutefois, elle dure un peu plus longtemps en raison de la recherche effectuée sur le noyau SafeGuard Enterprise se trouvant sur le disque dur.

Pour utiliser la fonction de réparation, procédez selon les instructions de la section Restauration d'un MBR corrompu *(page 488)*, mais sélectionnez **Repair MBR** à l’exécution de be_restore.exe.

Si plusieurs noyaux existent, be_restore.exe – **Repair MBR** utilise celui dont l'estampille temporelle est la plus récente.

7.6.6.4 Table de partition

SafeGuard Enterprise permet de créer de nouvelles partitions principales ou étendues. Cette action modifie la table de partition du disque dur sur lequel se trouve la partition.

Lors de la récupération d'une sauvegarde MBR, l'outil sait si le MBR actuel contient des tables de partition différentes pour le LBA 0 et quel fichier de sauvegarde MBR (*.BKN) doit être récupéré. Dans une boîte de dialogue, l'utilisateur peut sélectionner la table à utiliser.

Réparation d'un MBR avec une table de partition corrompue

Une table de partition corrompue peut empêcher le démarrage du système d'exploitation après une connexion d'authentification au démarrage réussie.

Vous pouvez résoudre ce problème en utilisant be_restore.exe pour récupérer un secteur de démarrage (MBR) précédemment enregistré ou réparer le MBR sans sauvegarde MBR.

Si vous avez une sauvegarde, procédez tel que décrit pour l'option **Restore MBR**.

Si vous n'avez pas de sauvegarde, procédez comme suit :

1. Insérez le CD-ROM de démarrage Windows PE dans le lecteur, connectez la carte mémoire contenant les fichiers SafeGuard Enterprise et démarrez l'ordinateur à partir du CD-ROM.
2. Lorsque l'ordinateur est prêt, à partir de l'invite de commandes, naviguez jusqu'au répertoire de la carte mémoire contenant les fichiers SafeGuard Enterprise et exécutez be_restore.exe.
3. Sélectionnez **Repair MBR**. Si be_restore.exe détecte une différence entre la table de partition du MBR actuel et celle du MBR en miroir, une boîte de dialogue permettant de sélectionner la table de partition à utiliser s'affiche.

   Le MBR en miroir correspond au MBR Microsoft d'origine enregistré durant la configuration du client SafeGuard Enterprise afin de vous permettre de le restaurer, par exemple, en cas de désinstallation du client. La table de partition de ce MBR en miroir est mise à jour par SafeGuard Enterprise si un changement survient dans Windows au niveau de la partition.

4. Sélectionnez **From Mirrored MBR**.

   ⚠ **Important :** Ne sélectionnez pas **From Current MBR**. Si vous le faites, la table de partition corrompue à partir du MBR en cours sera utilisée. Non seulement le système ne pourra toujours pas être démarré, mais le MBR en miroir sera mis à jour et par conséquent corrompu.

7.6.6.5 Signature de disque Windows

Chaque fois que Windows crée un système de fichiers pour la première fois sur un disque dur, il l'associe à une signature. Cette signature est enregistrée dans le MBR du disque dur (offsets 0x01B – 0x01BB). Notez que, par exemple, les lettres de lecteurs logiques du disque dur dépendent de la signature de disque Windows.

Veuillez ne pas changer la signature du disque. Par exemple, en utilisant (« FDISK/MBR »). Autrement, Windows entrera dans un mode de contrôle du disque dur très long au prochain démarrage et récupérera la liste des lecteurs.

Chaque fois que cela se produit sous SafeGuard Enterprise, le pilote du filtre SafeGuard Enterprise « BEFLT.sys » n'est pas chargé. Le démarrage du système est ainsi impossible : l'ordinateur affiche un écran bleu « STOP 0xED Unmountable Boot Volume ».

Pour effectuer les réparations sous SafeGuard Enterprise, la signature de disque Windows originale doit être restaurée sur le secteur de démarrage principal (MBR) du disque dur.

L'utilitaire be_restore.exe effectue cette tâche.

Remarque : N'utilisez surtout pas d'autres outils pour réparer le secteur de démarrage principal (MBR). Par exemple, un ancien MS DOS FDISK.exe que vous utilisez pour réécrire le chargeur MBR (« FDISK /MBR ») peut créer un autre chargeur du secteur de démarrage principal (MBR) sans signature de disque Windows. De même que pour la suppression de la signature du disque Windows, le « nouveau » chargeur du secteur de démarrage principal (MBR) créé par un ancien outil ne sera probablement pas compatible avec les différentes tailles de disque dur généralement utilisées aujourd'hui. Utilisez toujours les versions les plus récentes des outils de réparation.

7.6.6.6 Secteur de démarrage

Au cours du processus de chiffrement, le secteur de démarrage d'un volume est remplacé par le secteur de démarrage de SafeGuard Enterprise. Le secteur de démarrage de SafeGuard Enterprise contient des informations sur l'emplacement et la taille du KSA principal et de sa sauvegarde. L'emplacement est identifié dans les clusters et les secteurs correspondant au début de la partition. Même si le secteur de démarrage de SafeGuard Enterprise est endommagé, les volumes chiffrés sont inaccessibles. L'utilitaire be_restore peut récupérer le secteur de démarrage endommagé.

7.6.7 Restauration des systèmes de Challenge/Réponse Windows UEFI BitLocker

Pour restaurer les systèmes Windows UEFI BitLocker, Sophos met à disposition l’outil de restauration BLCRBackupRestoren.exe. Cet outil vous permet de :

- Sauvegarder les données Challenge/Réponse de BitLocker :

  Cette opération est uniquement nécessaire en cas d’échec de la sauvegarde automatique (événement du journal 3071 : « La sauvegarde de clé n’a pas pu être enregistrée sur le partage réseau indiqué. »)
- Restaurer manuellement une ancienne sauvegarde et réparer l’ordre de démarrage de NVRAM :

Cette opération est uniquement nécessaire si vous pensez que les données Challenge/Réponse de BitLocker sont corrompues ou ont été supprimées.

BLCRBackupRestoren.exe doit être redémarré à partir d'un environnement Windows PE. Il est disponible sur le CD-ROM du client virtuel Sophos.

7.6.7.1 Démarrage de l'outil de ligne de commande

Syntaxe

blcrbackuprestoren [-?] [-B [-T <CheminFichier>]] [-R [-K <NomFichier>] [-S <NomFichier>]] [-I] [-D]

Options

- -?

  Afficher l'aide

- -B

  Sauvegarder

- -T <CheminFichier>

  Chemin cible existant en option

- -R

  Restaurer

- -K <NomFichier>

  Chemin\Nom du fichier de clé en option

  Le fichier de clé en option est le fichier .BKN qui doit être exporté à partir de SafeGuard Management Center.

  Procédez à l'exportation de la manière suivante :

  - Dans SafeGuard Management Center, cliquez sur **Utilisateurs et ordinateurs**, puis sélectionnez l'ordinateur approprié dans la zone de navigation.
  - Cliquez avec le bouton droit de la souris et sélectionnez **Propriétés > Paramètres machine > Sauvegarder > Exporter**.

  Si les données de Challenge/Réponse BitLocker ont été sauvegardées avec succès, l'utilisation de l'option -R est suffisante.

- -S <NomFichier>

  Chemin\Nom de fichier de la source en option

- -I

  Installer l’entrée de démarrage.

- -D

  Supprimer l’entrée de démarrage.

Remarque : Si la restauration automatique échoue et que vous soulez utiliser un fichier de sauvegarde disponible sur une partition de récupération sans lettre de lecteur, vous allez devoir :

- Assigner une lettre de lecteur à cette partition de récupération
- Fournir le chemin pleinement qualifié du fichier de sauvegarde.

Il s’agit toujours d’un seul fichier : <lettre-lecteur>:\SOPHOS\<Nom fichier>.cps.

Exemples

- **Sauvegarder**
  - blcrbackuprestoren -b crée une archive à l’emplacement par défaut.
  - blcrbackuprestoren -b -T <USBStick:\Backup\ crée une archive sur un lecteur externe.

- **Restaurer**
  - blcrbackuprestoren -r extrait l’archive à l’emplacement par défaut.
  - blcrbackuprestoren -r -k X:\exemple\exemple.BKN extrait l’archive de l’emplacement par défaut et reconstruit le fichier de clé.

7.6.8 Mise hors service de volumes chiffrés

Pour les ordinateurs protégés par SafeGuard Enterprise, notre outil de ligne de commande beinvvol.exe peut être utilisé pour mettre hors service en toute sécurité les volumes chiffrés (disques durs, clés USB, etc.). Cet outil de ligne de commande est basé sur la norme DoD 5220.22-M et peut être utilisé pour supprimer des magasins de clés en toute sécurité. Cette norme comporte sept cycles de remplacement avec des modèles aléatoires et alternatifs.

Cet outil de ligne de commande est conçu pour être utilisé sur des ordinateurs sur lesquels :

- SafeGuard Enterprise est installé.

- Certains volumes de disque dur ont été chiffrés.

Vous devez exécuter cet outil sur un système sur lequel le pilote de chiffrement SafeGuard Enterprise n'est pas actif. De cette manière, vous évitez que des données soient mises hors service par accident. Sinon, l'outil ne fonctionne pas et un message d'erreur apparaît.

Remarque : Nous vous conseillons de démarrer votre système à partir d'un support externe comme un CD-ROM Windows PE et d'utiliser l'outil en fonction des instructions disponibles dans l'aide de la ligne de commande.

Une fois que les volumes cibles correspondants ont été mis hors service, ils ne sont plus lisibles.

Conformément à la norme DoD 5220.22-M, l'outil de ligne de commande vide en permanence les secteurs de démarrage et les zones de stockage des clés de SafeGuard Enterprise (KSA d'origine et sauvegarde) de chaque volume chiffré en les remplaçant sept fois. Les clés de chiffrement de données (DEK) aléatoires de chaque volume n'étant pas sauvegardées dans la base de données centrale des clients SafeGuard Enterprise, les volumes sont alors parfaitement sécurisés. Même un responsable de sécurité ne peut y accéder.

L'outil de ligne de commande affiche également des informations sur les volumes disponibles. Par exemple, le nom du volume, la taille du volume et les informations concernant les secteurs de démarrage et les KSA. Ces informations peuvent également être stockées dans un fichier. Le chemin de ce fichier doit, bien sûr, diriger vers un volume qui n'a pas été mis hors service.

Remarque : Les données ne peuvent pas être récupérées après suppression.

7.6.8.1 Démarrage de l'outil de ligne de commande

Syntaxe

- xl[volume]

  Répertorier les informations du ou des volumes cibles. Répertorier les informations concernant tous les volumes si aucun volume cible n'est spécifié.

- xi<volume>

  Invalider le(s) volume(s) cible(s), en cas de chiffrement SGN complet. Le <volume> cible doit être spécifié pour cette commande.

- <volume>

Indiquer le volume cible = {a, b, c, ..., z, *}, <*> correspondant à l’ensemble des volumes.

Options

- -g0

  Désactiver le mécanisme de journalisation.

- -ga[fichier]

  Mode journalisation -append. Ajouter les entrées du journal à la fin du fichier journal cible ou le crée s’il n’existe pas.

- -gt[fichier]

  Mode journalisation -truncate. Tronquer le fichier journal cible s’il existe ou le créer s’il n’existe pas.

- [fichier]

  Indiquer le fichier journal cible. S’il n’est pas indiqué, le fichier journal cible par défaut est « BEInvVol.log » dans le chemin en cours. N’indiquez pas le fichier journal sur le volume qui va être invalidé !

- -?, -h

  Afficher l’aide.

Exemples

> beinvvol -h

> beinvvol xld

> beinvvol xle -ga"c:\sous-répert\fichier.log"

> beinvvol xl* -gt"c:\sous-répert\fichier.log"

> beinvvol xif -gt"c:\mon sous-répert\fichier.log"

> beinvvol xig -g0

> beinvvol xi*

7.6.9 Mise hors service de disques durs à chiffrement automatique compatibles Opal

Les disques durs à chiffrement automatique offrent un chiffrement de type matériel des données lorsqu'ils sont écrits sur le disque dur. Trusted Computing Group (TCG) a publié la norme Opal indépendante des fournisseurs pour les disques durs à chiffrement automatique. SafeGuard Enterprise prend en charge la norme Opal et permet la gestion des terminaux avec disques durs compatibles Opal à chiffrement automatique.

Retrouvez plus de renseignements sur les disques durs compatibles Opal dans le *Manuel d'administration de SafeGuard Enterprise*, à la section *SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique*.

Pour les ordinateurs protégés par SafeGuard Enterprise, vous pouvez utiliser notre outil de ligne de commande opalinvdisk.exe.

7.6.9.1 Conditions préalables et conseils d’utilisation

Pour l’utilisation de opalinvdisk.exe, les conditions préalables et les conseils suivants s’appliquent :

- Avant d’utiliser opalinvdisk.exe, le disque dur compatible Opal doit être déchiffré avec la commande **Déchiffrer** de SafeGuard Enterprise disponible dans le menu contextuel de l’Explorateur Windows sur le terminal. Retrouvez plus de renseignements dans le *Manuel d’administration de SafeGuard Enterprise*, à la section *Autorisation de déverrouillage des disques durs compatibles Opal aux utilisateurs* et dans le *Manuel d’utilisation de SafeGuard Enterprise*, à la section *Extensions des icônes de la barre d’état et de l’Explorateur sur les terminaux avec disques durs compatibles Opal.*

- Vous avez besoin des droits d’administrateur.

- Nous vous conseillons d’utiliser opalinvdisk.exe dans un environnement Windows PE.

- L’outil opalinvdisk.exe lance le service facultatif RevertSP avec le paramètre KeepGlobalRangeKey défini sur False. La véritable procédure de mise hors service exécutée par RevertSP dépend du lecteur de disque dur spécifique. Retrouvez plus de renseignements à la section 5.2.3 du document Opal standard TCG Storage Security Subsystem Class : Opal, Specification Version 1.00, Revision 3.00 disponible sur www.trustedcomputinggroup.org.

7.6.9.2 Utilisation de opalinvdisk.exe

1. Ouvrez une invite de commande et démarrez opalinvdisk.exe avec les droits administrateur.

   Des informations sur les outils et sur son utilisation apparaissent.

2. Sur l’invite de commande, saisissez opalinvdisk.exe <PériphériqueCible>.

   Par exemple : opalinvdisk.exe PhysicalDrive0

Si les conditions préalables nécessaires sont remplies, RevertSP est lancé sur le disque dur indiqué dans <PériphériqueCible>. Si les conditions préalables ne sont pas remplies ou si le disque dur ne prend pas en charge RevertSP, un message d’erreur apparaît.

8. Support technique

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

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

9. Mentions légales