

**SOPHOS**

---

simple + secure

# SafeGuard Enterprise Web Helpdesk

Version du produit : 5.60

Date du document : avril 2011



## Table des matières

1 Procédure SafeGuard de challenge/réponse sur le Web.....	3
2 Installation.....	4
3 Authentification.....	7
4 Sélection de l'assistant de Web Help Desk.....	8
5 À propos des types de récupération.....	9
6 Récupération pour les clients SafeGuard Enterprise (administrés).....	10
7 Récupération à l'aide de clients virtuels.....	14
8 Récupération pour les clients Sophos SafeGuard (autonomes).....	18
9 Protection de la configuration SafeGuard.....	20
10 Journalisation des événements de Web Help Desk .....	21
11 Support technique.....	22
12 Mentions légales.....	22

# 1 Procédure SafeGuard de challenge/réponse sur le Web

Pour simplifier le flux de travail dans un environnement d'entreprise et réduire les coûts du support, SafeGuard Enterprise fournit une solution de déblocage basée sur le Web. 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.

En outre, la stratégie de protection de la configuration de SafeGuard peut être suspendue.

## Avantages de la procédure challenge/réponse

Le mécanisme de challenge/réponse est un système d'urgence sécurisé et efficace.

- Tout au long du processus, aucune donnée confidentielle n'est échangée sous une forme autre que chiffrée.
- 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 l'ordinateur d'extrémité. L'assistant de code de réponse du support en ligne s'exécute également sur un ordinateur autonome sans nécessité d'une infrastructure complexe.
- L'utilisateur peut commencer à retravailler rapidement. L'oubli du mot de passe n'entraîne aucune perte de données chiffrées.

## Flux de travail de challenge/réponse

Lors de la procédure challenge/réponse, un code de challenge (chaîne de caractères ASCII) est généré sur l'ordinateur d'extrémité et l'utilisateur fournit ce code à un responsable support. En fonction de ce code, le responsable support génère alors un code de réponse qui autorise l'utilisateur à effectuer une action spécifique sur l'ordinateur.

## Situations d'urgence classiques nécessitant l'intervention du support

- Un utilisateur a oublié le mot de passe de connexion et l'ordinateur a été verrouillé.
- Un utilisateur a oublié ou perdu la clé cryptographique/carte à puce.
- Le cache local de l'authentification au démarrage est partiellement endommagé.
- Si un utilisateur est absent, ses collègues doivent pouvoir 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 l'ordinateur.

SafeGuard Enterprise Web Help Desk propose différents flux de travail de récupération pour ces scénarios d'urgence classiques, ce qui permet aux utilisateurs d'accéder de nouveau à leurs ordinateurs.

## 1.1 Champ d'application de Web Help Desk

Web Help Desk fournit le mécanisme de challenge/réponse de SafeGuard Enterprise via une interface Web. Le contrôle d'accès de cette application Web peut être régi via le protocole SSL

et permet au support de déléguer facilement les tâches dans l'entreprise. Pour ce faire, nul besoin de donner aux employés du support l'accès aux paramètres confidentiels de configuration ou à la gestion centralisée de SafeGuard Enterprise.

Web Help Desk est disponible sur Internet/intranet sans nécessité d'installer le logiciel SafeGuard Enterprise sur l'ordinateur d'extrémité. Les sites Web doivent être hébergés séparément sur un serveur SafeGuard Enterprise IIS (Internet Information Services).

Web Help Desk peut être exécuté en plus de SafeGuard Management Center.

**Remarque :**

Nous vous conseillons de mettre Web Help Desk à disposition uniquement sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, ne donnez pas accès à Web Help Desk sur Internet.

**Web Help Desk fournit la récupération pour les clients suivants :**

- Clients SafeGuard Enterprise
- Clients virtuels
- Clients SafeGuard autonomes

S'il s'agit d'un client SafeGuard Enterprise, le programme détermine de façon dynamique si un client chiffré par volume Enterprise natif ou si un client Enterprise chiffré BitLocker est utilisé et règle le flux de travail de récupération en conséquence.

## 2 Installation

Web Help Desk doit être installé sur un serveur Web IIS équipé du serveur SafeGuard Enterprise. Au cours de l'installation de Web Help Desk, la disponibilité du serveur SafeGuard Enterprise sur le serveur est vérifiée. En cas d'indisponibilité, il est installé automatiquement dans un pool d'applications distinct appelé **SGNWHD-Pool**. Suite à l'installation de Web Help Desk, configurez le serveur Web.

Un seul navigateur doit être installé sur l'ordinateur du responsable de Web Help Desk.

### 2.1 Configuration requise

#### 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.
- Microsoft Internet Information Services (IIS) doit être installé.
- .NET Framework 3.0 Service Pack 1 avec ASP.NET 2.0 doit être installé.

#### Configuration requise du client

Un navigateur doit être installé sur l'ordinateur du responsable de Web Help Desk. Web Help Desk prend en charge les navigateurs suivants :

- Microsoft Internet Explorer 7 et 8
- Mozilla Firefox 2 et 3

## 2.2 Installation de Web Help Desk

Le fichier SGNWebHelpDesk.msi du package d'installation requis est fourni avec le produit.

1. Démarrez SGNWebHelpDesk.msi.
2. Dans la page **Bienvenue**, cliquez sur **Suivant**.
3. Acceptez le contrat de licence.
4. Sélectionnez un chemin d'installation.
5. Cliquez sur **Terminer** pour terminer l'installation.

Le programme d'installation de Web Help Desk vérifie si le serveur SafeGuard Enterprise est déjà installé sur le serveur Web IIS. S'il ne l'est pas, il est automatiquement installé. Web Help Desk est installé sur le serveur Web IIS, dans un pool d'applications distinct appelé **SGNWHD-Pool**.

### 2.2.1 Configuration du serveur Web avec SSL

Pour une sécurité optimale, configurez le serveur Web IIS de la manière suivante :

1. Déployez Web Help Desk sur le réseau intranet uniquement.  
Veillez à placer Web Help Desk uniquement sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, ne donnez pas accès à Web Help Desk sur Internet.
2. Établissez une connexion SSL.  
Vous pouvez restreindre l'accès de Web Help Desk aux utilisateurs définis à l'aide de la configuration IIS standard fournie avec IIS. Assurez-vous que le certificat de sécurité SSL est installé sur le serveur IIS. L'intégralité de la communication de Web Help Desk sera effectuée via le protocole SSL.  
Les tâches générales suivantes doivent être effectuées pour configurer le serveur Web pour SSL :
  - a) Une autorité de certification doit être installée pour générer des certificats utilisés pour le chiffrement SSL.
  - b) Un certificat doit être généré et le serveur IIS configuré pour utiliser SSL et sélectionner le certificat.
  - c) Le nom du serveur spécifié lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui spécifié dans le certificat SSL. Faute de quoi, la communication entre le client et le serveur est impossible. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.
  - d) Les processus de travail du pool d'applications **SGNWHD-Pool** ne doivent pas être supérieurs à 1 (valeur par défaut), sinon l'autorisation à Web Help Desk échoue.

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

- <http://msdn2.microsoft.com/en-us/library/ms998300.aspx>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;316898>

- [https://blogs.msdn.com/sql\\_protocols/archive/2005/11/10/491563.aspx](https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx)

## 2.2.2 Enregistrement et configuration du serveur SafeGuard Enterprise

Si le serveur SafeGuard Enterprise n'a pas été installé ni enregistré avant l'installation de Web Help Desk, enregistrez-le dans le SafeGuard Management Center.

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

Ne sélectionnez pas le certificat MSO.

Le FQDN, par exemple **server.mycompany.edu** et les informations de certificat apparaissent.

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

5. Cliquez sur **OK**.  
Les informations du serveur sont affichées dans l'onglet **Enregistrer le serveur**.
6. Cliquez sur l'onglet **Créer un package de configuration de serveur**. Les serveurs disponibles sont affichés. Sélectionnez le serveur requis. Spécifiez le chemin de sortie pour le package de configuration du serveur. Cliquez sur **Créer un package de configuration**.  
Un package de configuration (MSI) appelé <Serveur>.msi est créé à l'emplacement spécifié.
7. Cliquez sur **OK** pour confirmer le message de succès.
8. Dans l'onglet **Enregistrer le serveur**, cliquez sur **Fermer**.

Le serveur SafeGuard Enterprise est enregistré et configuré. Installez ensuite le package de configuration du serveur (MSI) sur l'ordinateur exécutant le serveur SafeGuard Enterprise. À tout moment, vous pouvez changer la configuration du serveur dans l'onglet **Enregistrer le serveur**.

### Remarque :

Si vous voulez installer un nouveau package de configuration du serveur (MSI) sur le serveur SafeGuard Enterprise, veillez à désinstaller le package de configuration du serveur obsolète avant d'en installer un nouveau.

## 2.3 Mise à jour de Web Help Desk

Lors de la mise à jour de Web Help Desk à la dernière version, il est conseillé de désinstaller Web Help Desk, puis de procéder à l'installation de la dernière version de Web Help Desk. Créez uniquement un nouveau package de configuration du serveur si des paramètres du serveur doivent être mis à jour.

## 2.4 Prise en charge des langues

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

# 3 Authentification

Le responsable de la sécurité doit s'authentifier dans Web Help Desk et sur le serveur SafeGuard Enterprise afin de pouvoir utiliser l'assistant Web de récupération. Il se connecte à Web Help Desk à l'aide de son nom utilisateur et de son mot de passe qui sont les mêmes que ses codes d'accès Windows.

Seuls les utilisateurs promus auparavant au rang de responsable de la sécurité dans SafeGuard Management Center peuvent accéder à Web Help Desk.

## 3.1 Préparations dans le SafeGuard Management Center

Pour pouvoir procéder à l'authentification dans Web Help Desk, les conditions préalables suivantes doivent être remplies et les préparations suivantes doivent être effectuées dans le SafeGuard Management Center. Pour plus d'informations, consultez l'aide de l'administrateur.

1. Vous devez avoir importé les utilisateurs de Web Help Desk à partir d'Active Directory dans la base de données SafeGuard Enterprise.
2. Vous devez avoir affecté des certificats utilisateur à ces utilisateurs ou les avoir importés pour eux, et ces certificats (fichier .p12) doivent être disponibles dans la base de données.
3. Les futurs utilisateurs de Web Help Desk doivent ensuite être promus au rang de responsables de la sécurité.

Les responsables de la sécurité peuvent alors se connecter à Web Help Desk 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 a été attribué. Le mot de passe requis est le mot de passe Windows, qui protège leurs certificats.

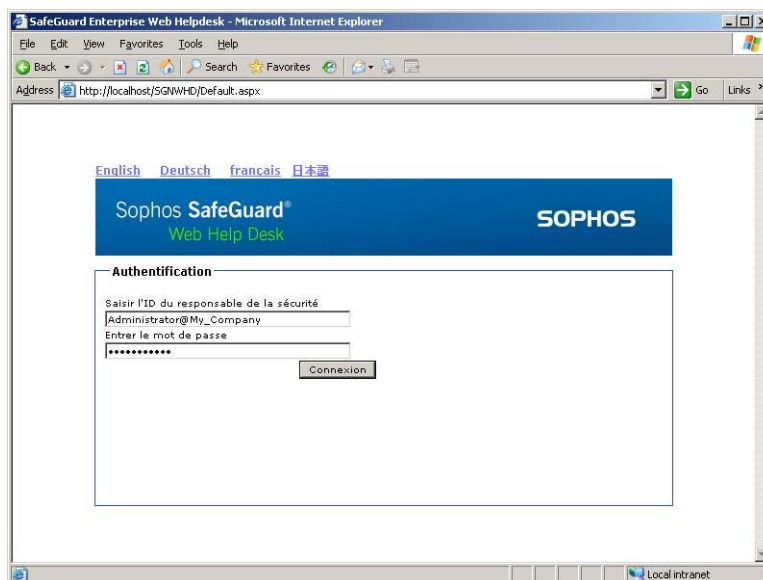
4. Les responsables de la sécurité doivent se voir attribuer le rôle de responsable du support afin de pouvoir s'authentifier dans Web Help Desk.

Les conditions préalables à la réussite de l'authentification dans Web Help Desk sont remplies.

**Remarque :** les responsables de la sécurité de Web Help Desk doivent s'authentifier sur le serveur SafeGuard Enterprise, par conséquent l'authentification via une clé cryptographique n'est pas prise en charge dans Web Help Desk.

## 3.2 Connexion à Web Help Desk

1. Démarrez votre navigateur.
2. Appelez l'application en saisissant son URL : **https://<ID de l'hôte ou adresse IP>/SGNWHD**



3. Sur la page de **Bienvenue**, saisissez votre nom de responsable de la sécurité exactement de la même manière qu'il est défini dans le SafeGuard Management Center : **<nom d'utilisateur>@<DOMAINE>** par exemple **ResponsableWHD@MONDOMAINE**.

Cette entrée est sensible aux majuscules. Assurez-vous d'orthographier le nom utilisateur correctement.

4. Saisissez votre mot de passe. Le mot de passe requis correspond à votre mot de passe Windows.
5. Cliquez sur **Connexion**.

Vous êtes connecté à Web Help Desk.

## 4 Sélection de l'assistant de Web Help Desk

1. Sur la page d'**Accueil**, effectuez l'une des actions suivantes :
  - Pour autoriser les actions de récupération sur les ordinateurs d'extrémité, sélectionnez **Récupération**, reportez-vous à la section [À propos des types de récupération](#) à la page 9.
  - Pour autoriser la suspension de la stratégie de protection de la configuration SafeGuard, sélectionnez **Approuver la suspension** reportez-vous à la section [Protection de la configuration SafeGuard](#) à la page 20.

## 5 À propos des types de récupération

Les types de récupérations suivants sont fournis :

### ■ Clients SafeGuard Enterprise (administrés)

Ordinateurs d'extrémité gérés de façon centralisée par le SafeGuard Management Center. Ils sont répertoriés dans la zone Utilisateurs & ordinateurs du SafeGuard Management Center.

### ■ Clients virtuels

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.

Pour activer une procédure challenge/réponse dans cette situation, vous pouvez créer des fichiers spécifiques, appelés clients virtuels, et les distribuer à l'utilisateur avant la session de challenge/réponse. La procédure de challenge/réponse peut ensuite être initiée sur l'ordinateur d'extrémité à l'aide de ces clients virtuels et de l'outil de récupération de clé **RecoveryKeys.exe** disponible dans le produit. Il suffit ensuite à l'utilisateur d'informer le responsable du support des clés requises et de saisir le code de réponse afin de pouvoir accéder à nouveau aux volumes chiffrés.

### ■ Clients Sophos SafeGuard (autonomes)

Ordinateurs d'extrémité gérés localement. Ils ne sont jamais connectés au serveur SafeGuard Enterprise. Pour chaque client Sophos SafeGuard autonome, un fichier de récupération (au format .xml) est généré lors de la configuration. Il contient la clé machine définie, qui est chiffrée avec le certificat de l'entreprise. Si ce fichier de clés de récupération est disponible, par exemple sur un lecteur flash USB ou via un chemin réseau partagé afin que le responsable du support puisse y accéder, la procédure challenge/réponse pour un ordinateur non administré protégé par Sophos SafeGuard est prise en charge.

Déconnexion administrator@my\_company

Sophos SafeGuard® Web Help Desk SOPHOS

Type de récupération

Client SafeGuard Enterprise  
Domaine: Racine  
Ordinateur: [input]

Client virtuel  
Client virtuel: [input]

Client autonome  
Fichier de récupération XML: [input] Parcourir

Suivant

Terminé Intranet local

## Sélection du type de récupération

Après avoir sélectionné **Récupération** sur la page d'**Accueil**, sélectionnez le type de récupération requis.

# 6 Récupération pour les clients SafeGuard Enterprise (administrés)

SafeGuard Enterprise fournit la procédure de récupération aux clients SafeGuard Enterprise enregistrés dans la base de données, dans différents scénarios d'urgence, par exemple la récupération de mots de passe ou l'accès aux données par démarrage à partir d'un support externe.

La procédure challenge/réponse est prise en charge pour les clients natifs SafeGuard Enterprise et les clients chiffrés BitLocker. Au cours de la procédure challenge/réponse, le type de client Enterprise utilisé est déterminé de façon dynamique et la tâche de récupération est réglée en conséquence.

## 6.1 Actions de récupération pour les clients SafeGuard Enterprise

Le flux de travail de récupération dépend du type de client Enterprise pour lequel une récupération est demandée.

### Remarque :

S'il s'agit d'ordinateurs chiffrés BitLocker, la seule action de récupération consiste à récupérer la clé utilisée pour chiffrer un volume spécifique. La récupération de mots de passe n'est pas proposée.

### 6.1.1 Récupération du mot de passe de l'authentification au démarrage

L'un des scénarios les plus courants 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 de l'authentification au démarrage permettant d'accéder à l'ordinateur 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 **Initialiser le client SGN avec une connexion utilisateur**, mais sans afficher le mot de passe utilisateur. Cependant, dans ce cas, après la saisie du code de réponse, l'ordinateur démarre le système d'exploitation. L'utilisateur doit donc changer son mot de passe Windows, à condition que le domaine soit accessible. 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 de l'authentification au démarrage

#### Remarque :

Nous vous conseillons d'utiliser les méthodes suivantes pour récupérer un mot de passe oublié par l'utilisateur afin d'éviter que ce mot de passe ne soit réinitialisé de manière centralisée :

**Utilisation de Local Self Help :** Local Self Help permet à l'utilisateur d'afficher le mot de passe actuel et de continuer à l'utiliser. Ainsi, il n'a pas besoin de réinitialiser le mot de passe ou de recourir à l'assistance technique. Pour plus d'informations, consultez l'aide de l'administrateur.

**Utilisation de la procédure challenge/réponse pour les clients SafeGuard Enterprise (gérés) :** nous vous conseillons d'éviter la réinitialisation du mot de passe dans Active Directory avant la procédure challenge/réponse. Ainsi, vous garanzissez que le mot de passe demeure synchronisé entre Windows et SafeGuard Enterprise. Assurez-vous que le support Windows en a bien connaissance.

En tant que responsable support SafeGuard Enterprise, générez une réponse pour **Initialiser le client SGN avec une connexion utilisateur** avec l'option **Afficher le mot de passe utilisateur**. Ainsi, ils ne sont pas tenus de réinitialiser le mot de passe 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.

### 6.1.2 Affichage du mot de passe utilisateur

SafeGuard Enterprise permet aux utilisateurs d'afficher leur mot de passe lors de la procédure challenge/réponse. Ainsi, ils ne sont pas tenus de réinitialiser le mot de passe dans Active Directory. Cette option est disponible uniquement si l'action **Initialiser le client SGN avec une connexion utilisateur** est demandée.

### 6.1.3 Accès aux données par démarrage de l'ordinateur à partir d'un support externe

Il est également possible d'utiliser la procédure challenge/réponse pour autoriser le démarrage d'un ordinateur à partir d'un support externe, par exemple WinPE. Pour ce faire, l'utilisateur doit sélectionner **Poursuivre l'initialisation à partir de : Disquette/Support externe** dans la boîte de dialogue de connexion de l'authentification au démarrage et initier le challenge. Lors de 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 d'un support externe.

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. Pour plus d'informations sur la manière d'obtenir ce CD-ROM pilote, consultez :  
<http://www.sophos.fr/support/knowledgebase/article/108805.html>.
- L'utilisateur doit démarrer l'ordinateur à partir d'un support externe et doit disposer du droit approprié. Vous pouvez lui octroyer ce droit en définissant une stratégie dans le SafeGuard Management Center et en l'affectant au client (l'option de stratégie **Authentification > Accès: L'utilisateur peut uniquement démarrer à partir du disque dur** doit être définie sur **Non**). Par défaut, le droit de démarrer à partir d'un support externe n'est pas affecté.
- En général, l'ordinateur d'extrémité doit prendre en charge le démarrage à partir de supports autres qu'un disque dur fixe.

- 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 du périphérique dans le SafeGuard Management Center et être affecté à l'ordinateur.

**Remarque :**

Lorsque vous utilisez un support externe tel que WinPE pour accéder au lecteur chiffré, vous accédez uniquement à une partie du volume.

### 6.1.4 Restauration de la mémoire cache de la stratégie SafeGuard Enterprise

Cette procédure est utilisée si la mémoire cache de la stratégie SafeGuard est endommagée. Le cas échéant, l'utilisateur est invité automatiquement à initier une procédure challenge/réponse lors de la connexion à l'authentification au démarrage.

## 6.2 Création d'une réponse pour les clients SafeGuard Enterprise

Pour créer une réponse lors de la procédure challenge/réponse pour un client SafeGuard Enterprise, les noms de l'ordinateur d'extrémité et du domaine sont requis.

**Remarque :** ce nom doit toujours correspondre au nom unique de l'ordinateur.

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. Pour ce faire, vous pouvez procéder de plusieurs façons :
  - Sélectionnez un nom en cliquant sur [...], puis sur **Rechercher** dans la fenêtre contextuelle. La 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=Postel,OU=Développement,OU=Siège,DC=Utimaco,DC=uae**
4. Cliquez sur **Suivant**.

Le programme détermine alors de façon dynamique si un ordinateur SafeGuard Enterprise natif ou si un ordinateur chiffré BitLocker est utilisé et règle le flux de travail de récupération en conséquence. S'il s'agit d'un ordinateur SafeGuard Enterprise natif, l'étape suivante requiert la sélection des informations utilisateur. S'il s'agit d'un ordinateur chiffré BitLocker, l'étape suivante nécessite la sélection du volume à déchiffrer.

### 6.2.1 Création d'une réponse pour les clients SafeGuard Enterprise natifs

S'il s'agit d'un client SafeGuard Enterprise natif, une recherche portant sur l'ordinateur approprié doit être effectuée dans la base de données.

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 indiqué, puis 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 l'ordinateur d'extrémité s'affichent. Les actions disponibles pour la réponse dépendent des actions demandées sur l'ordinateur d'extrémité lors de l'appel du challenge. Par exemple, en cas de **Demande de clé cryptographique**, les actions disponibles pour la réponse sont **Initialiser le client SGN avec une connexion utilisateur** et **Initialiser le client SGN sans connexion utilisateur**.
6. Sélectionnez l'action que l'utilisateur doit exécuter.
7. Si l'action **Initialiser 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 l'ordinateur cible.
8. Cliquez sur **Suivant**. Un code de réponse est généré.
9. Lisez ou envoyez le code de réponse à l'utilisateur. Une aide orthographique est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L'utilisateur peut ensuite saisir le code de réponse sur l'ordinateur d'extrémité et exécuter l'action autorisée.

## 6.2.2 Création d'une réponse pour les clients SafeGuard Enterprise protégés par BitLocker

S'il s'agit de clients SafeGuard Enterprise protégés par BitLocker, un volume devenu inaccessible peut être récupéré. Une recherche portant sur l'ordinateur approprié est effectuée dans la base de données. Le volume requis doit ensuite être sélectionné pour récupérer un ordinateur chiffré BitLocker.

1. Sélectionnez le volume auquel accéder, puis cliquez sur **Suivant**. Web Help Desk affiche alors la clé de récupération à 48 chiffres correspondante.
2. Lisez cette clé à l'utilisateur.

L'utilisateur peut alors la saisir, afin de pouvoir accéder au volume chiffré BitLocker sur son ordinateur.

## 7 Récupération à l'aide de clients virtuels

Grâce à la récupération des clients virtuels, SafeGuard Enterprise permet de récupérer des volumes chiffrés 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 l'ordinateur de façon sécurisée.

### Remarque :

La récupération des clients virtuels doit uniquement être utilisée pour résoudre des situations d'urgence complexes : si les deux problèmes mentionnés ci-dessus existent, la récupération des clients virtuels est appropriée. Cependant, si une seule clé 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 le 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 initiée sur l'ordinateur d'extrémité 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 Help Desk, la récupération à l'aide des clients virtuels n'est pas prise en charge pour les clients Sophos SafeGuard autonomes.

### 7.1 Flux de travail de récupération à l'aide de clients virtuels

#### Remarque :

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

1. Le responsable du support doit créer le client virtuel dans la zone **Clés et certificats** du SafeGuard Management Center et l'exporter 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 peut 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.  
L'identification dans la base de données SafeGuard Enterprise s'effectue en utilisant le fichier du client virtuel et en le mentionnant dans le challenge à la place du nom de l'utilisateur/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 présente 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.

## 7.2 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, la ou les clés de chiffrement correctes doivent être transférées de la base de données vers l'environnement de l'utilisateur.

La procédure challenge/réponse utilise donc deux actions à l'aide des clients virtuels :

- Le transfert d'une seule clé.
- Le transfert de plusieurs clés dans un fichier de clés chiffré.

### 7.2.1 Transfert d'une seule clé

Un challenge peut être initié 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 l'ordinateur d'extrémité, 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.

### 7.2.2 Transfert de plusieurs clés dans un fichier de clés chiffré

Un challenge peut être initié 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 propre à chaque fichier de clés créé.

Le fichier de clés chiffré doit être transféré vers l'environnement de l'utilisateur et mis à la disposition de l'utilisateur. Pour déchiffrer ce fichier de clés, l'utilisateur doit alors initier 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 l'ordinateur cible. Le responsable du support génère alors une réponse, puis sélectionne le mot de passe approprié pour déchiffrer le fichier de clés. Le mot de passe est transféré à l'ordinateur cible dans le code de réponse. Le fichier de clés peut alors être déchiffré à l'aide du mot de passe.

Les clés contenues dans le fichier de clés sont importées dans la zone de stockage des clés sur l'ordinateur d'extrémité et tous les volumes chiffrés à l'aide des clés disponibles sont à nouveau accessibles.

**Remarque :**

Grâce à Web Help Desk, un fichier de clés 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. Dans ce cas, créez un nouveau fichier de clés et un mot de passe après chaque session de challenge/réponse réussie.

## 7.3 Réponse à l'aide de clients virtuels

Pour créer une réponse à l'aide de clients virtuels, les conditions préalables suivantes doivent être remplies.

### 7.3.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Le client virtuel doit avoir été créé dans la zone **Clés et certificats** du SafeGuard Management Center. Pour plus d'informations, consultez l'aide de l'administrateur.
- Le responsable du support doit être à même 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 clé USB.
- Lorsque la récupération de plusieurs clés est demandée, le responsable du support doit d'abord créer un fichier de clés contenant les clés de récupération nécessaires dans la zone **Clés et certificats** du SafeGuard Management Center. Le fichier de clés 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 clés doit être indiqué dans la base de données. Pour plus d'informations, consultez l'aide de l'administrateur.
- L'utilisateur doit avoir démarré l'outil de récupération de clé et initié la session de challenge/réponse.
- Une réponse ne peut être initiée que pour des clés attribuées. Si une clé est inactive, c'est-à-dire qu'elle n'est pas attribuée à au moins un utilisateur, une réponse pour client virtuel est impossible. Dans ce cas, la clé inactive peut être attribuée de nouveau à un autre utilisateur et une réponse pour cette clé peut être de nouveau générée.

### 7.3.2 Création d'une réponse à l'aide de clients virtuels

1. En votre qualité de 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 fenêtre dans laquelle vous pouvez sélectionner l'action de récupération s'affiche.
4. Sélectionnez l'action de récupération que l'utilisateur doit entreprendre, puis cliquez sur **Suivant**.
  - Si vous devez transférer une seule clé de récupération, sélectionnez **Clé requise**. Dans la liste, sélectionnez la clé respective. 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 clés contenant plusieurs clés de récupération, sélectionnez **Mot de passe du fichier de clés requis** afin de transmettre à l'utilisateur le mot de passe du fichier de clés chiffré. Sélectionnez le fichier de clés requis. Cliquez sur [...], puis sur **Rechercher**. Sélectionnez le fichier de clés, puis cliquez sur **OK**.

Vous pouvez sélectionner l'option **Mot de passe du fichier de clés requis** uniquement si un fichier de clés a été créé dans la zone **Clés et certificats** du SafeGuard Management Center et si le mot de passe de chiffrement du fichier de clés est stocké dans la base de données. Grâce à Web Help Desk, les fichiers de clés et le mot de passe correspondant sont supprimés de la base de données dès qu'ils ont été utilisés avec succès dans une session de challenge/réponse. Dans ce cas, vous devez donc créer un fichier de clés et un mot de passe après chaque session de challenge/réponse aboutie.

5. Cliquez sur **Suivant**. La fenêtre dans laquelle vous devez saisir le code de challenge s'affiche.
6. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis 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 orthographique 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 clés chiffré, il est transféré dans le code de réponse. Ce fichier de clés est ensuite supprimé.
8. L'utilisateur doit saisir le code de réponse sur l'ordinateur d'extrémité.
9. L'utilisateur doit redémarrer l'ordinateur, puis se reconnecter pour accéder aux volumes appropriés.

Les volumes sont à nouveau accessibles.

## 8 Récupération pour les clients Sophos SafeGuard (autonomes)

SafeGuard Enterprise fournit également la procédure challenge/réponse aux clients Sophos SafeGuard autonomes. Les clients Sophos SafeGuard autonomes ne sont jamais connectés au serveur SafeGuard Enterprise. Ils fonctionnent en mode autonome et sont gérés localement. Comme ils ne sont pas enregistrés dans la base de données SafeGuard Enterprise, aucune information sur leur identification nécessaire à une procédure challenge/réponse n'est disponible.

La procédure challenge/réponse des clients Sophos SafeGuard autonomes est donc basée sur le fichier de clés de récupération créé lors de la configuration du client autonome. Le fichier de récupération (au format .xml) est généré pour chaque client Sophos SafeGuard autonome et contient la clé machine définie, chiffrée à l'aide du certificat de l'entreprise. Ce fichier doit être stocké à un emplacement accessible à un responsable du support lors de la procédure challenge/réponse. Si le responsable du support peut accéder au fichier de récupération approprié, par exemple sur une clé USB ou via un chemin réseau partagé, une réponse peut être générée.

### 8.1 Actions de récupération pour les clients Sophos SafeGuard (autonomes)

La procédure challenge/réponse pour un client Sophos SafeGuard autonome doit être initiée dans les situations suivantes :

- L'utilisateur a saisi trop fréquemment le mot de passe de façon incorrecte.
- L'utilisateur a oublié le mot de passe.
- Une mémoire cache endommagée doit être réparée.

Aucune clé utilisateur n'est disponible dans la base de données lorsqu'il s'agit de clients Sophos SafeGuard autonomes. Par conséquent, la seule action de récupération possible dans une session de challenge/réponse est **Initialisation du client SGN 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.

#### 8.1.1 L'utilisateur a saisi trop fréquemment le mot de passe de façon incorrecte

Dans ce cas de figure, la réinitialisation du mot de passe n'est pas nécessaire, 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 l'ordinateur.

## 8.1.2 L'utilisateur a oublié le mot de passe

### Remarque :

Nous vous conseillons d'utiliser Local Self Help pour récupérer un mot de passe oublié. Dans Local Self Help, le mot de passe actuel peut être affiché et l'utilisateur peut continuer à l'utiliser. Ainsi, il n'a pas besoin de réinitialiser le mot de passe ou de recourir à l'assistance technique. Pour plus d'informations, consultez l'aide de l'administrateur.

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 correct et doit par conséquent le modifier au niveau Windows. Cela nécessite d'autres actions de récupération qui sont hors du champ d'application de SafeGuard Enterprise, via des moyens Windows standard. 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 conseiller à l'utilisateur 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 utilisateur est créé en fonction du nouveau choix de mot de passe Windows. Cela permet à l'utilisateur de 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 de passe correspondante. Pour continuer à utiliser les clés utilisateur déjà générées pour SafeGuard Data Exchange, l'utilisateur doit se souvenir des phrases de passe SafeGuard Data Exchange afin de les réactiver.

## 8.2 Création d'une réponse pour clients Sophos SafeGuard (autonomes)

Pour générer une réponse lors d'une session de challenge/réponse pour un client autonome, vous devez indiquer le nom du fichier de récupération (au format .xml).

1. Dans Web Help Desk, 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.

## 9 Protection de la configuration SafeGuard

Associé à SafeGuard PortAuditor (consultez le guide utilisateur de SafeGuard PortAuditor), la protection de la configuration SafeGuard est une solution complète qui permet aux entreprises d'identifier les ports et périphériques utilisés en leur sein (visibilité) et ainsi de définir une stratégie de contrôle de leur utilisation afin de protéger les données transférées.

La protection de la configuration SafeGuard contrôle chaque ordinateur d'extrémité et chaque périphérique, quel que soit le réseau ou l'interface. Elle contrôle le trafic en temps réel et applique des stratégies de sécurité personnalisées et très précises sur toutes les interfaces physiques, sans fil ainsi que sur les périphériques de stockage.

La stratégie de protection de la configuration actuelle peut être suspendue temporairement à l'aide de Sophos SafeGuard Web Help Desk.

### 9.1 Suspension de la stratégie de protection de la configuration

- L'utilisateur doit disposer du droit de suspendre la stratégie de protection de la configuration (stratégie de protection de la configuration, paramètre **Options d'affichage L'utilisateur est autorisé à suspendre la protection de la configuration** défini sur **Oui**).
- Il doit avoir été attribué le droit suivant au support technique : **Utiliser l'outil de suspension**.

Pour suspendre la stratégie :

1. Sur l'ordinateur d'extrémité, l'utilisateur clique sur l'icône de la barre d'état système et sélectionne **Suspendre la protection de la configuration**.
2. Dans **Suspendre la protection de la configuration**, l'utilisateur sélectionne la période de suspension désirée. Le code de challenge est généré automatiquement. Il est valide pendant 30 minutes. L'utilisateur fournit les informations utilisateur, le code de challenge et la période de suspension au support.
3. Dans Web Help Desk, sur la page d'**Accueil**, sélectionnez **Approuver la suspension**.

4. Sur la page **Utilisateur**, sélectionnez ou saisissez le domaine et les informations utilisateur que l'utilisateur a fourni et cliquez sur **Suivant**. Les informations utilisateur sont confirmées.
5. Sur la page **Challenge**, saisissez le code du challenge fourni par l'utilisateur. Sélectionnez la période de suspension telle que fournie par l'utilisateur. La période doit correspondre à celle que l'utilisateur a saisie sur l'ordinateur d'extrémité. Cliquez sur **Suivant**.

Le code de challenge est confirmé et le code de réponse est généré.

6. Sur la page **Réponse**, le code de réponse, l'action accordée et la période de suspension sont affichés. Remettez ces informations à l'utilisateur. Vous pouvez utiliser l'aide à l'épellation. Pour retourner sur la page **Utilisateur**, cliquez sur **Redémarrer**. Pour retourner sur la page de sélection des assistants, cliquez sur **Accueil** en haut à droite de la page.
7. Sur l'ordinateur d'extrémité, dans **Suspendre la protection de la configuration**, l'utilisateur saisit ou copie la réponse qui lui a été fournie par le support. L'utilisateur doit s'assurer que la période correspond à celle qui lui a été fournie par le support. L'utilisateur clique sur **OK**.

La stratégie de protection de la configuration est suspendue pour la période spécifiée. Elle peut être relancée de deux manières :

- Lors de la période de suspension spécifiée, sur l'ordinateur d'extrémité, l'utilisateur clique sur l'icône de la barre d'état système et sélectionne **Reprendre la protection de la configuration**.
- Une fois que la période de suspension spécifiée s'est écoulée, la stratégie de protection de la configuration est reprise automatiquement.

## 10 Journalisation des événements de Web Help Desk

Les événements de SafeGuard Web Help Desk 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 pour savoir par exemple qui s'est connecté à Web Help Desk, quel utilisateur a demandé un challenge ou quelles actions de récupération ont été requises.

La journalisation des événements de Web Help Desk est activée dans le SafeGuard Management Center par une stratégie qui doit être publiée dans un package de configuration et déployée sur le service Web Help Desk.

Les événements qui sont consignés dans la base de données centrale de SafeGuard Enterprise peuvent être consultés à l'aide de la Visionneuse des événements du SafeGuard Management Center.

### 10.1 Activation de la journalisation des événements de Web Help Desk

La journalisation pour Web Help Desk est configurée dans le SafeGuard Management Center. Vous devez disposer des droits appropriés pour créer des stratégies et voir des événements.

1. Dans le 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 **Créer un package de configuration géré** 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 le SafeGuard Management Center, affectez le groupe de stratégies au domaine contenant le serveur Web Help Desk. Activez-le. Pour plus d'informations, consultez le chapitre *Attribution de stratégies* de l'aide de l'administrateur.
5. Sur le service Web Help Desk, installez le package de configuration créé auparavant. Redémarrez le service.

La journalisation des événements de Web Help Desk a été activée.

6. Connectez-vous à Web Help Desk et lancez une procédure challenge/réponse.
7. Dans le SafeGuard Management Center, cliquez sur l'onglet **Rapports**. Dans la zone d'action **Visionneuse des événements**, sur le côté droit, cliquez sur l'icône en forme de loupe pour voir les événements journalisés de Web Help Desk.

## 11 Support technique

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

- Rendez-vous sur le forum SophosTalk (anglais) à l'adresse <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos à l'adresse <http://www.sophos.fr/support/>
- Téléchargez la documentation des produits à l'adresse <http://www.sophos.fr/support/docs/>
- Envoyez un courriel à [support@sophos.fr](mailto:support@sophos.fr), y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

## 12 Mentions légales

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

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

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence

valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

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