

# SOPHOS

## SafeGuard® Enterprise 5.50 Web Helpdesk

Date du document : Avril 2010



# Table des matières

- 1 Procédure challenge/réponse de SafeGuard Enterprise basée sur le Web ..... 2
- 2 Installation ..... 5
- 3 Authentification ..... 10
- 4 Types de récupération ..... 12
- 5 Récupération pour les clients SafeGuard Enterprise..... 14
- 6 Récupération à l'aide de clients virtuels ..... 24
- 7 Récupération pour les clients SafeGuard autonomes ..... 30
- 8 Support technique..... 34
- 9 Copyright ..... 35

# 1 Procédure challenge/réponse de SafeGuard Enterprise basée 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 de SafeGuard Enterprise qui ne peuvent pas se connecter à leurs ordinateurs ou qui ne peuvent pas accéder à des données chiffrées.

## 1.1 Avantages de la procédure challenge/réponse

Le mécanisme de challenge/réponse est un système de déblocage 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 espionnées ne peuvent pas être utilisées ultérieurement ni sur d'autres périphériques.
- Aucune connexion réseau en ligne n'est nécessaire pour l'ordinateur de l'utilisateur. L'assistant de code de réponse de Helpdesk 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.

## 1.2 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 de l'utilisateur 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.

## 1.3 Situations d'urgence classiques nécessitant l'assistance 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 Helpdesk 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.

## 1.4 Portée de Web Helpdesk

Web Helpdesk 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 aux employés du 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 Helpdesk est disponible sur Internet/l'intranet sans pour autant qu'il soit nécessaire d'installer le logiciel SafeGuard Enterprise sur la machine de l'utilisateur. Les sites Web doivent être hébergés séparément sur un serveur SafeGuard Enterprise IIS (Internet Information Services).

Web Helpdesk peut être exécuté en sus de SafeGuard Management Center.

**Remarque:** Nous vous recommandons de ne fournir Web Helpdesk que sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, il est déconseillé de placer Web Helpdesk sur Internet.

### **1.4.1 Web Helpdesk 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 Helpdesk doit être installé sur un serveur Web IIS équipé de SafeGuard Enterprise Server. Lors de l'installation de Web Helpdesk, le système vérifie si SafeGuard Enterprise Server est déjà installé sur le serveur. S'il ne l'est pas, il est automatiquement installé dans un pool d'applications distinct, appelé SGNWHD-Pool. Après l'installation de Web Helpdesk, vous devez configurer le serveur Web.

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

### 2.1 Configuration minimale

#### 2.1.1 Configuration minimale du serveur

La configuration minimale détaillée du serveur est décrite dans les Notes de version.

- Vous devez 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.

#### 2.1.2 Configuration minimale du client

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

- Microsoft Internet Explorer 7.0
- Mozilla Firefox 2 et Firefox 3

**Remarque:** Nous vous recommandons de ne fournir Web Helpdesk que sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, il est déconseillé de placer Web Helpdesk sur Internet.

## 2.2 Installation de Web Helpdesk

Le fichier SGNWebHelpDesk.msi du package d'installation requis se trouve sur le CD du produit.

1. Démarrez SGNWebHelpDesk.msi à partir du CD du produit.
2. Cliquez sur **Suivant** dans la fenêtre de bienvenue.
3. Acceptez le contrat de licence.
4. Sélectionnez un chemin d'installation.
5. Confirmez la réussite de l'installation.

Le programme d'installation de Web Helpdesk vérifie si SafeGuard Enterprise Server est déjà installé sur le serveur Web IIS. S'il ne l'est pas, il est automatiquement installé. Web Helpdesk 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 renforcer la sécurité, vous devez configurer le serveur Web IIS de la manière suivante :

1. Déployez Web Helpdesk uniquement sur le réseau intranet.

Veillez à placer Web Helpdesk uniquement sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, il est déconseillé de placer Web Helpdesk sur Internet.

2. Établissez une connexion SSL.

Vous pouvez limiter la disponibilité de Web Helpdesk aux utilisateurs définis en utilisant la configuration IIS standard fournie avec IIS. Vérifiez que vous avez installé un certificat de sécurité SSL sur le serveur IIS. L'intégralité de la communication de Web Helpdesk sera prise en charge 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. Sinon, le client et le serveur ne peuvent pas communiquer. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.

Pour plus d'informations sur la configuration de SSL, consultez les liens suivants ou contactez le support technique (en anglais) :

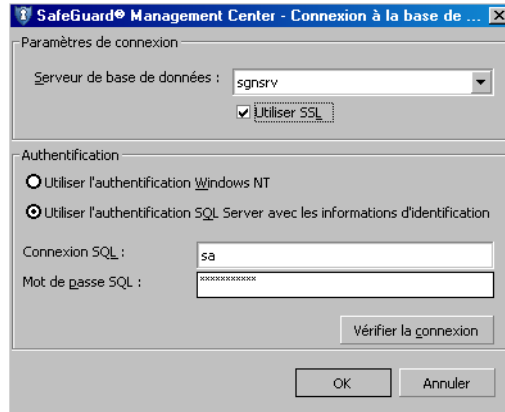
- <http://msdn2.microsoft.com/en-us/library/ms998300.aspx>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;316898>
- [https://blogs.msdn.com/sql\\_protocols/archive/2005/11/10/491563.aspx](https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx)

## 2.2.2 Configuration et enregistrement de SafeGuard Enterprise Server

Si SafeGuard Enterprise Server n'a pas été installé ni enregistré avant l'installation de Web Helpdesk, vous devez l'enregistrer dans SafeGuard Management Center, une fois l'installation de Web Helpdesk terminée.

1. Lancez Management Center, puis sélectionnez **Outils > Outil de package de configuration** dans la barre de menus.
2. Sélectionnez **Enregistrer le serveur**, puis cliquez sur **Ajouter**.
3. Sélectionnez le certificat machine du serveur qui est généré lors de l'installation de SafeGuard Enterprise Server. Par défaut, il est situé dans le répertoire MachCert du répertoire d'installation de SafeGuard Enterprise Server. Son nom de fichier est <Nomordinateur>.cer. Si SafeGuard Enterprise Server est installé sur un autre ordinateur que SafeGuard Management Center, ce fichier .cer doit être accessible sous la forme d'une copie ou d'une autorisation réseau.
4. Le serveur et ses propriétés sont affichés dans l'onglet **Enregistrer le serveur**.
5. Activez **Scripts autorisés** pour utiliser l'API de script.

6. Cliquez sur **Connexion à la base de données** puis sur [...] pour configurer la connexion à la base de données :



- a) Sélectionnez le serveur de base de données requis auquel le serveur Web Helpdesk doit se connecter.
- b) Activez **Utiliser SSL** pour protéger via SSL la connexion entre cette base de données et le serveur Web sélectionné.
- c) Dans **Authentification**, définissez les informations d'identification de base de données à utiliser pour la base de données sélectionnée : **Utiliser l'authentification Windows NT** ou **Utiliser l'authentification SQL**.

Choisissez l'option **Utiliser l'authentification SQL** pour les ordinateurs qui ne font partie d'aucun domaine. Dans le cas contraire, utilisez une authentification Windows NT qui exige une configuration supplémentaire. Si vous utilisez l'option **Utiliser l'authentification SQL**, nous vous recommandons fortement de protéger la connexion à la base de données via SSL afin de chiffrer le transport des informations d'identification SQL.

- d) Vérifiez la connexion à la base de données. Un nouveau package du serveur peut être créé même si la vérification échoue.

Vous pouvez modifier, à tout moment, les propriétés et paramètres d'un quelconque serveur enregistré et de sa connexion à la base de données. Veillez simplement à créer un nouveau package du serveur ensuite et à le distribuer au serveur concerné. La nouvelle connexion à la base de données peut être utilisée une fois le package du serveur à jour installé sur le serveur.

7. Ouvrez l'onglet **Créer un package serveur**.
8. Sélectionnez le serveur requis.
9. Spécifiez le chemin de sortie.

10. Cliquez sur **Créer un MSI serveur**. Un fichier .msi appelé <Serveur>.msi est alors créé au niveau du chemin de sortie.

11. Exécutez ce nouveau fichier de configuration .msi sur le serveur SafeGuard Enterprise.

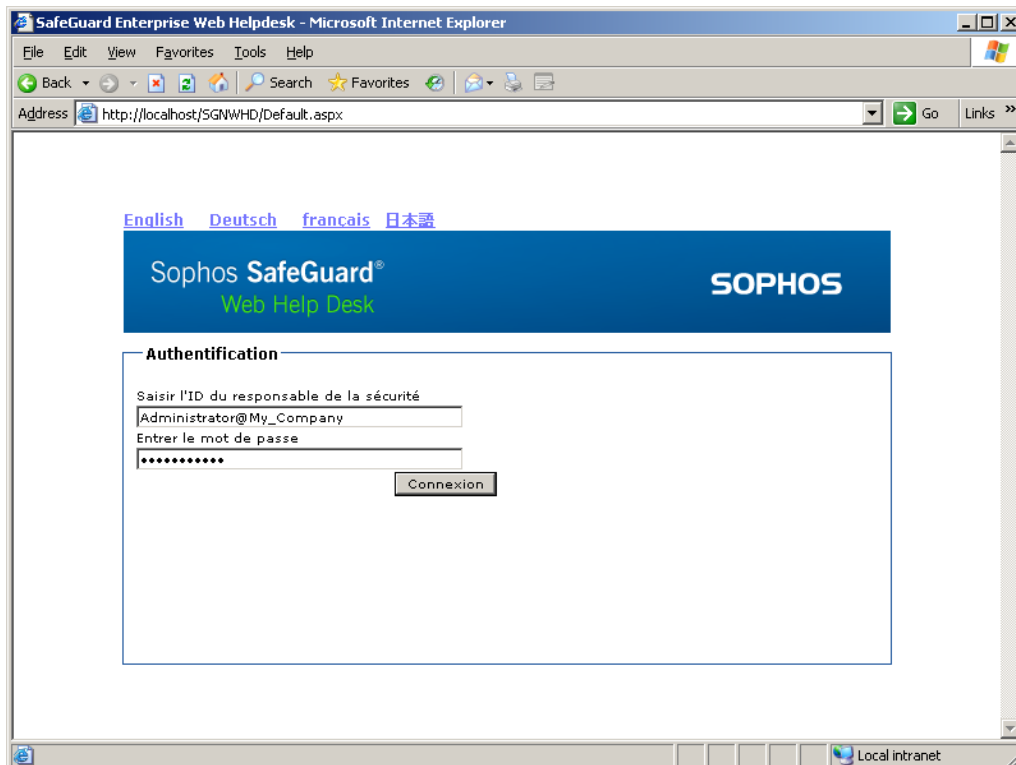
L'ordinateur est enregistré comme serveur SafeGuard Enterprise.

## 2.3 Mise à jour de Web Helpdesk

Lors de la mise à jour de Web Helpdesk vers la dernière version, il est recommandé de désinstaller Web Helpdesk, puis d'installer de zéro la dernière version de Web Helpdesk. Le package de configuration du serveur doit être créé de zéro si des paramètres du serveur doivent être mis à jour.

## 2.4 Prise en charge des langues

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.



## 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. Ils se connectent à Web Helpdesk en utilisant leur ID de responsable de la sécurité et leur mot de passe, qui équivalent à leurs informations d'identification Windows.

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

### 3.1 Préparations dans SafeGuard Management Center

Pour octroyer un accès à Web Helpdesk, les conditions préalables suivantes doivent être remplies et les préparations suivantes doivent être effectuées dans SafeGuard Management Center. Pour plus d'informations, reportez-vous au manuel de l'administrateur de SafeGuard Enterprise.

1. Vous devez avoir importé les utilisateurs de Web Helpdesk 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 Helpdesk doivent ensuite être promus au rang de responsables de la sécurité.

Les responsables de la sécurité peuvent alors se connecter à Web Helpdesk à l'aide de leur ID de responsable de la sécurité défini, qui est une combinaison de leur nom d'utilisateur Windows et du nom du domaine qui leur est attribué. Le mot de passe requis est le mot de passe Windows, qui protège leurs certificats.

4. Les responsables de la sécurité doivent posséder le rôle de responsable support afin de pouvoir s'authentifier dans Web Helpdesk.

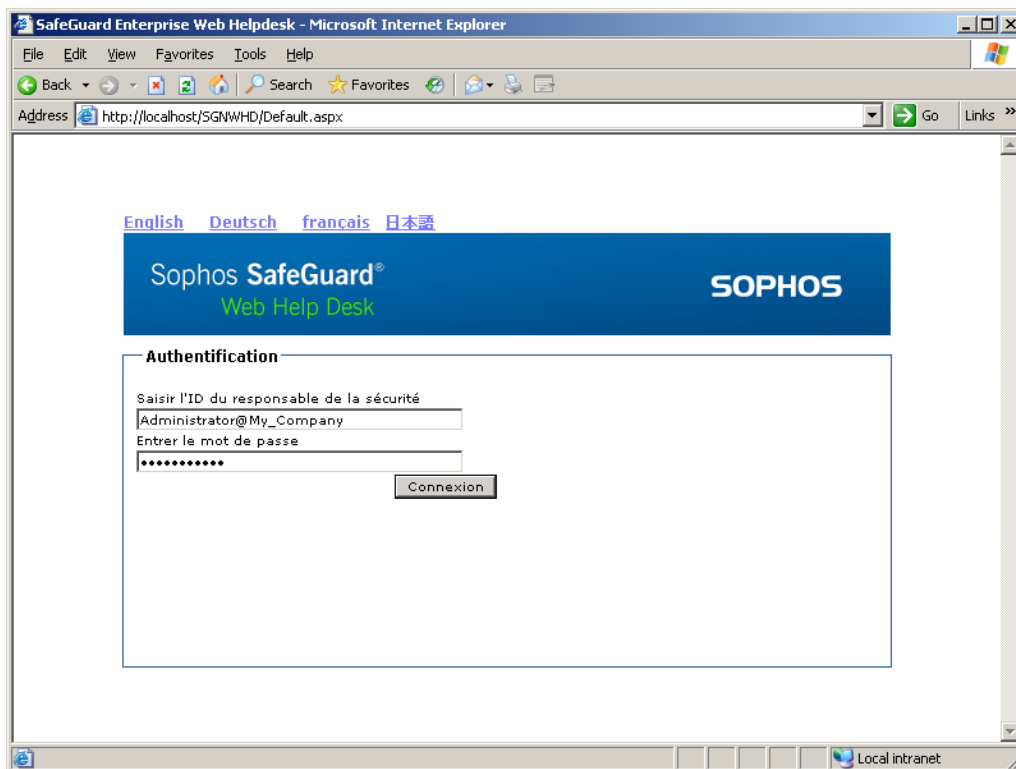
Les conditions préalables à la réussite de l'authentification dans Web Helpdesk sont remplies.

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

## 3.2 Connexion à Web Helpdesk

Procédez comme suit :

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



3. Dans l'écran de bienvenue, saisissez votre ID de responsable de la sécurité tel qu'il est défini dans SafeGuard Management Center, de la manière suivante : <nom d'utilisateur>@<DOMAINE>, par exemple Responsable\_WHD@MONDOMAINE.  
Étant donné que la saisie respecte la casse, veillez à orthographier correctement le nom d'utilisateur. Aucune liste de noms d'utilisateur n'est fournie afin de masquer ces informations aux utilisateurs non autorisés.
4. Saisissez votre mot de passe. Le mot de passe requis correspond à votre mot de passe Windows.
5. Cliquez sur **Connexion**.

L'assistant de récupération de Web Helpdesk est démarré.

## 4 Types de récupération

Les types de récupérations suivants sont fournis :

### ■ Clients SafeGuard Enterprise

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

### ■ Clients virtuels

Les volumes chiffrés peuvent être récupérés facilement même dans les cas où la procédure challenge/réponse n'est habituellement pas prise en charge, par exemple lorsque l'authentification au démarrage est corrompue.

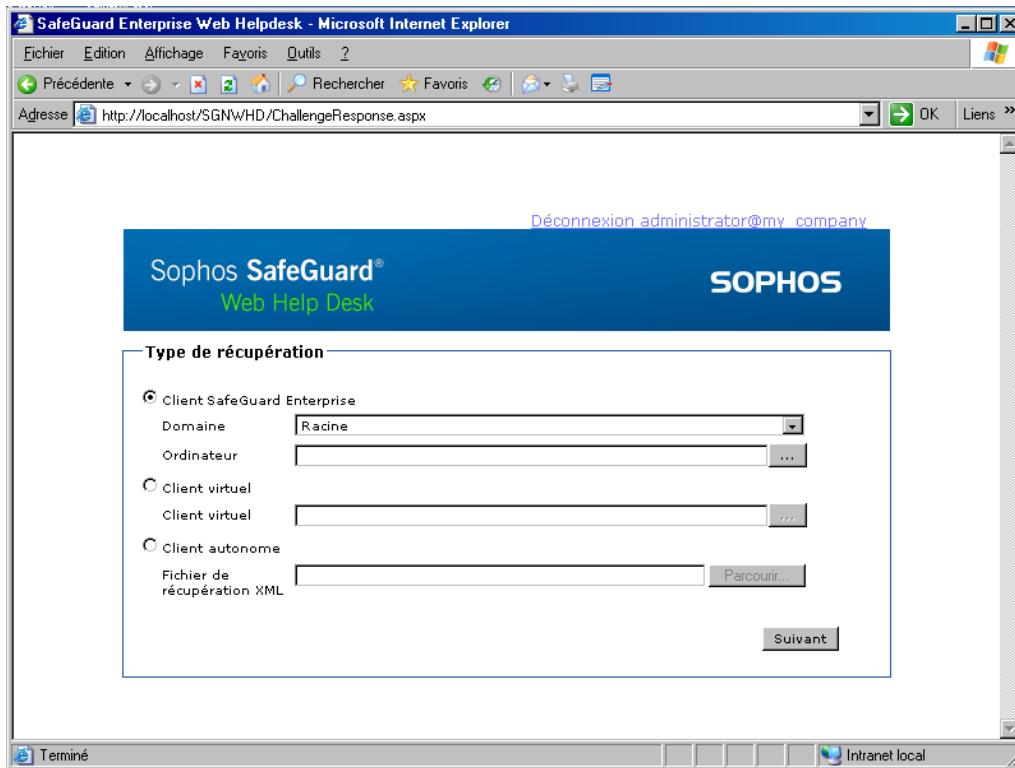
Pour activer une procédure challenge/réponse dans cette situation, vous pouvez créer des fichiers spécifiques, appelés clients virtuels, et les distribuer à l'utilisateur avant la session de challenge/réponse. La procédure de challenge/réponse peut ensuite être initiée sur l'ordinateur client à l'aide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

### ■ Clients SafeGuard autonomes

Ordinateurs d'utilisateur gérés localement. Ils ne sont jamais connectés au serveur SafeGuard Enterprise. Pour chaque client 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 récupération est disponible, par exemple sur une carte mémoire ou via un chemin réseau partagé afin que le responsable support puisse y accéder, la procédure challenge/réponse pour un client SafeGuard autonome est prise en charge.

## 4.1 Sélection du type de récupération

Une fois que vous vous êtes connecté à Web Helpdesk, vous pouvez sélectionner le type de récupération demandé.



## 5 Récupération pour les clients SafeGuard Enterprise

SafeGuard Enterprise fournit la procédure de récupération aux clients 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 via l'initialisation 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. Lors de cette procédure, le système détermine, de façon dynamique, le type de client Enterprise utilisé. Le flux de travail de récupération est réglé en conséquence.

### 5.1 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.

#### 5.1.1 Récupération du mot de passe au niveau 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 POA 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 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 initialise le système d'exploitation. L'utilisateur doit donc changer le mot de passe au niveau 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.

##### **Pratique recommandée de récupération de mot de passe au niveau de l'authentification au démarrage**

**Remarque:** nous recommandons d'utiliser principalement 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 :

**Utilisez Local Self Help.** Avec la récupération via Local Self Help, le mot de passe actuel peut être affiché et l'utilisateur peut continuer à l'utiliser sans devoir le réinitialiser et sans requérir l'assistance du support. Pour plus d'informations, consultez l'aide de l'administrateur.

**Lors de l'utilisation de la procédure Challenge/Réponse :** il est recommandé d'éviter la réinitialisation centralisée du mot de passe dans Active Directory avant la procédure de Challenge/Réponse. Cela garantit que le mot de passe reste 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 l'ancien mot de passe et le modifier localement par la suite, s'il le souhaite.

### 5.1.2 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.

### 5.1.3 Récupération du mot de passe au niveau Windows

L'accès risque également d'être refusé aux utilisateurs au niveau Windows, par exemple après le verrouillage d'un poste ou la déconnexion et le rétablissement du système d'exploitation. Le cas échéant, le responsable support génère une réponse pour **Initialiser le client SGN sans connexion utilisateur**.

Le mot de passe doit également être réinitialisé dans Active Directory.

1. Le support du domaine doit réinitialiser le mot de passe utilisateur au niveau Windows.
2. L'utilisateur se connecte à Windows avec ce nouveau mot de passe.
3. À la prochaine réinitialisation, l'utilisateur n'est pas en mesure de se connecter à l'authentification au démarrage à l'aide des nouvelles informations d'identification.
4. L'utilisateur doit ensuite initier une procédure challenge/réponse informant le responsable support du nouveau mot de passe.

5. Le responsable support doit effectuer les tâches suivantes dans SafeGuard Management Center :
  - a) Supprimer le certificat utilisateur dans l'onglet **Certificats** de la zone **Utilisateurs & ordinateurs**.
  - b) Supprimer l'ordinateur auquel l'utilisateur essaie de se connecter dans l'onglet **Utilisateurs** de la zone **Utilisateurs & ordinateurs**.
6. Le responsable support génère une réponse pour l'initialisation sans connexion utilisateur.
7. L'utilisateur saisit le code de réponse et se connecte à Windows à l'aide des nouvelles informations d'identification.
8. L'utilisateur doit réinitialiser l'ordinateur pour exécuter la modification du mot de passe au niveau de l'authentification au démarrage.

#### 5.1.4 Accès aux données via l'initialisation à partir d'un support externe

Il est également possible d'utiliser la procédure challenge/réponse pour autoriser la réinitialisation 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 peut saisir les informations d'identification dans POA, de façon habituelle, et poursuivre l'initialisation à partir d'un support externe.

Les conditions suivantes doivent être remplies pour que vous puissiez accéder à un volume chiffré :

- Le périphérique à utiliser doit contenir le pilote du filtre SafeGuard Enterprise. Consultez la base de connaissances pour savoir comment obtenir un tel CD de pilote :  
<http://www.sophos.com/support/knowledgebase/article/108805.html>.
- L'utilisateur doit exécuter l'initialisation à partir d'un support externe et doit disposer de l'autorisation appropriée. Vous pouvez lui octroyer ce droit en définissant une stratégie dans SafeGuard Management Center et en l'affectant au client (l'option de stratégie **Authentification > Accès : Les utilisateurs peuvent uniquement booter à partir du disque dur** doit être définie sur **Non**). Par défaut, le droit d'initialisation à partir d'un support externe n'est pas affecté.

- En général, l'ordinateur de l'utilisateur doit prendre en charge l'initialisation 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 Management Center et affecté au client.

**Remarque:** Notez que l'utilisation de supports externes, par exemple WinPE, pour accéder à un lecteur chiffré autorise uniquement un accès partiel au volume.

### 5.1.5 Restauration du cache de stratégies SafeGuard Enterprise

Cette procédure est nécessaire si le cache de stratégies SafeGuard est endommagé. Le cas échéant, l'utilisateur est invité automatiquement à initier une procédure challenge/réponse lors de la connexion à l'authentification au démarrage.

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

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

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

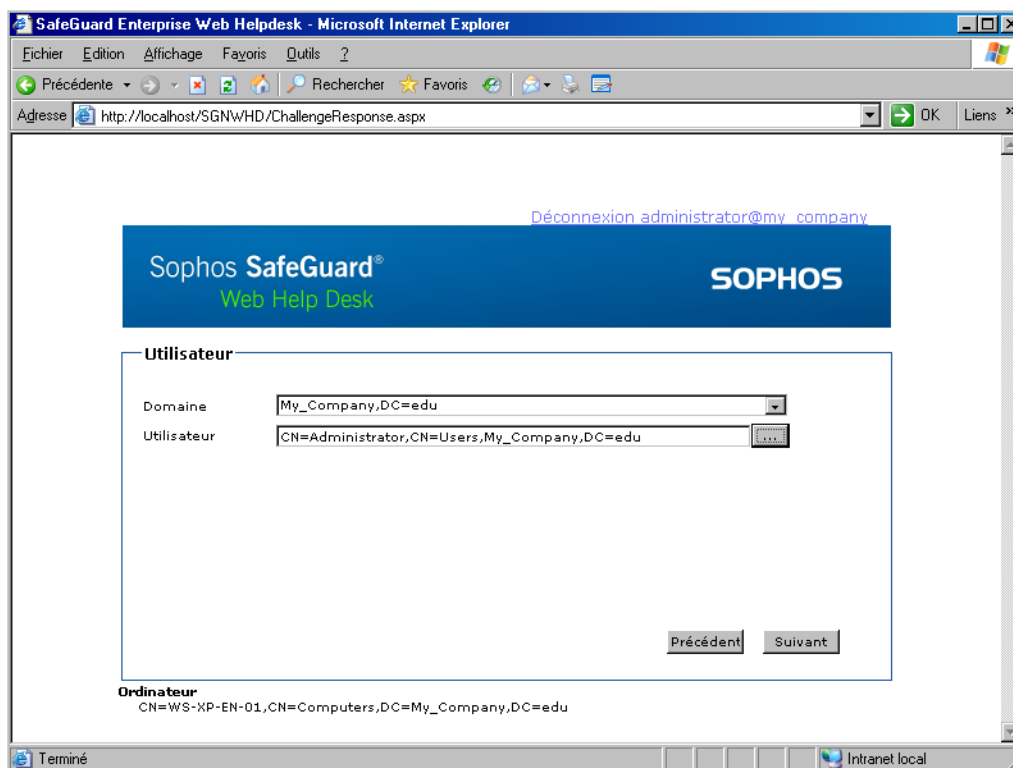
1. Dans la fenêtre **Type de récupération**, sélectionnez **Client SafeGuard Enterprise**.
2. Dans la liste, sélectionnez le domaine requis.
3. Saisissez le nom de l'ordinateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
  - Sélectionnez un nom en cliquant sur [...], puis sur **Rechercher** 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 alors 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=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.

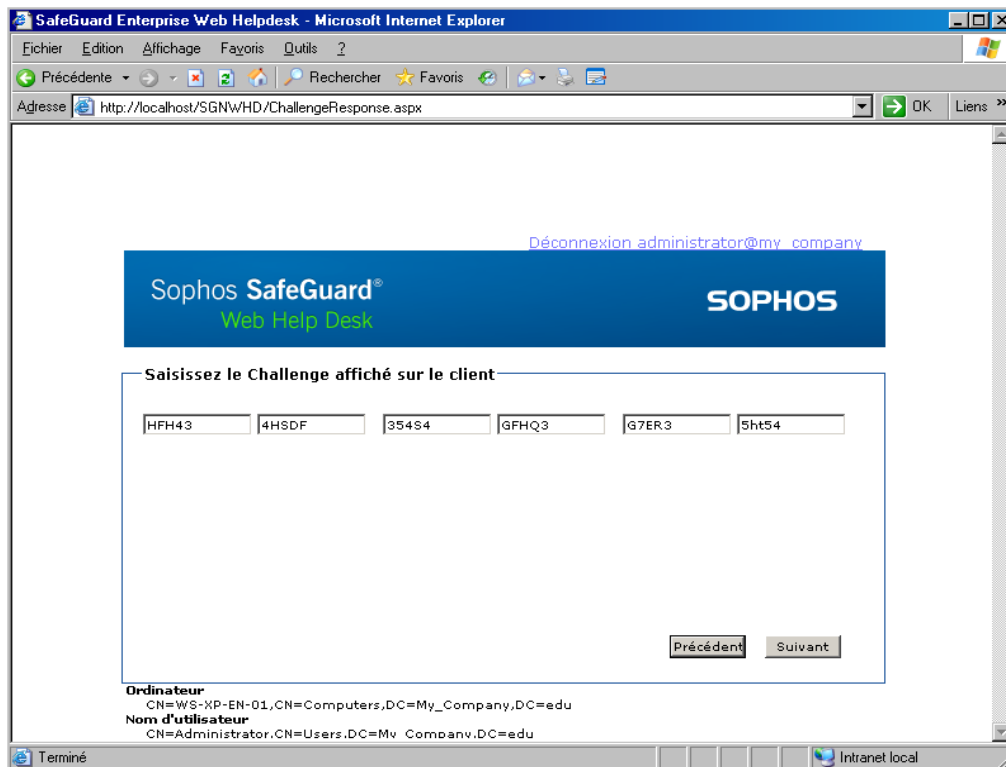
## 5.2.1 Création d'une réponse pour les clients SafeGuard Enterprise natifs

S'il s'agit d'un client SafeGuard Enterprise natif, une recherche portant sur l'ordinateur approprié est effectuée dans la base de données. Puis, le nom d'utilisateur et le domaine correspondants doivent être sélectionnés afin d'effectuer la récupération d'un client SafeGuard Enterprise.

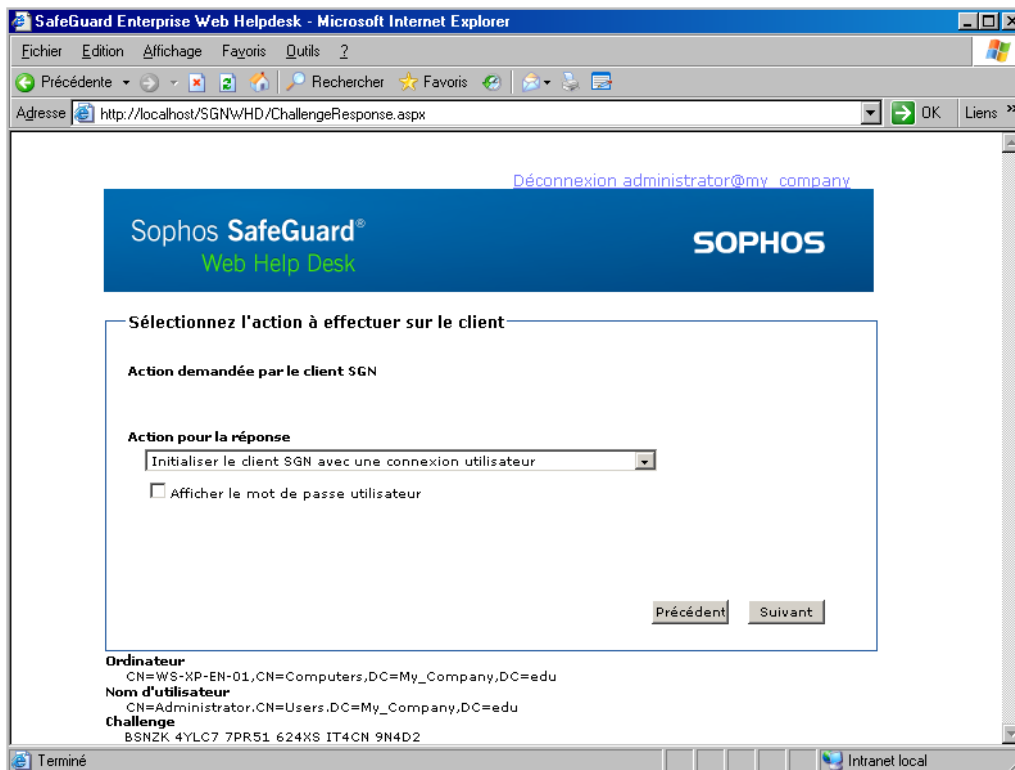
1. Dans **Domaine**, sélectionnez le domaine requis de l'utilisateur. S'il s'agit d'un utilisateur local, sélectionnez **Utilisateur local sur <nom de l'ordinateur>**.
2. Saisissez le nom de l'utilisateur requis. Pour ce faire, vous pouvez procéder de plusieurs façons :
  - Sélectionnez le nom d'utilisateur en cliquant sur [...], puis sur **Rechercher** dans la fenêtre contextuelle. La liste des noms d'utilisateur s'affiche. Sélectionnez le nom requis, puis cliquez sur **OK**.
  - Saisissez directement le nom de l'utilisateur. Assurez-vous de l'orthographier 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.

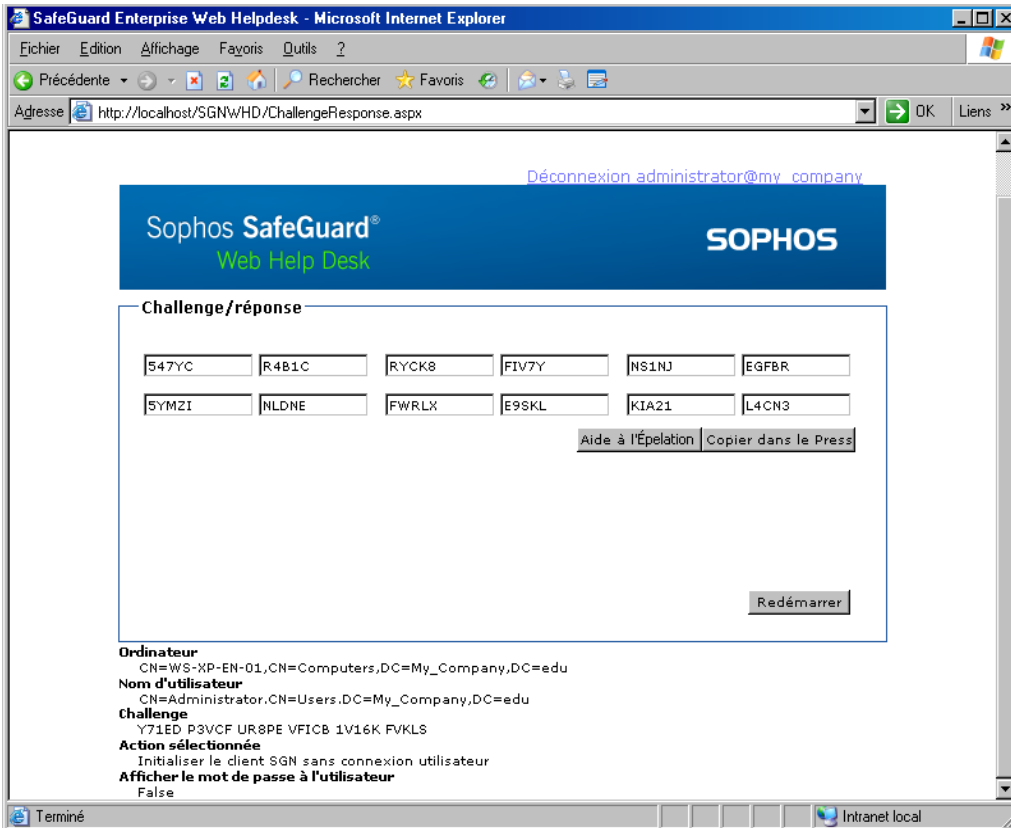


5. Si le code de challenge a été saisi correctement, l'action de récupération demandée par le client SafeGuard Enterprise, ainsi que les actions de récupération possibles sur ce client s'affichent. Les actions possibles pour la réponse dépendent des actions demandées côté client lors de l'appel du challenge. Par exemple, si l'action **Carte à puce crypto** nécessaire est requise côté client, 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-le 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 l'ordinateur de l'utilisateur et exécuter l'action autorisée.

## 5.2.2 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. Dans la liste, sélectionnez le volume auquel accéder, puis cliquez sur **Suivant**. Web Helpdesk 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.

## 6 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.

La récupération à l'aide de clients virtuels peut être appliquée dans les situations classiques suivantes :

- L'authentification au démarrage est corrompue.
- Un volume est chiffré à l'aide d'une clé autre que 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 SafeGuard Management Center et les distribuer à l'utilisateur avant la session de challenge/réponse. La procédure de challenge/réponse peut ensuite être initiée sur l'ordinateur client à l'aide des fichiers du client virtuel, via l'outil de récupération de clé RecoveryKeys.exe à partir du CD du produit et d'un CD d'environnement WinPE modifié de SafeGuard Enterprise. Le responsable 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, les clés requises étant transférées dans la réponse.

## 6.1 Récupération à l'aide de clients virtuels : Flux de travail

**Remarque:** Pour obtenir une description détaillée du flux de travail, consultez le manuel de l'administrateur de SafeGuard Enterprise.

Procédez comme suit :

1. Le responsable support doit créer le client virtuel dans la zone **Clés et certificats** de 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 de récupération de SafeGuard Enterprise ou tout autre CD à l'aide d'un environnement WinPE modifié de SafeGuard Enterprise sur son ordinateur, à partir du BIOS, sans aucune connexion POA, puis initier une session de challenge/réponse à l'aide d'un outil de récupération de clé.

Comme référence 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/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 support.
4. Le responsable support identifie le client virtuel dans la base de données et sélectionne la clé requise pour accéder aux volumes chiffrés : soit une clé, soit plusieurs clés exportées dans un fichier de clés. Le responsable 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.

## 6.2 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.

### 6.2.1 Transfert d'une seule clé

Un challenge peut être initié pour récupérer une seule clé afin d'accéder à un volume chiffré. Le responsable 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 de l'utilisateur, une fois le code de réponse saisi. Si ce code est correct, la clé transférée est importée dans le magasin de clés locales. Après quoi, tous les volumes chiffrés à l'aide de cette clé sont accessibles.

### 6.2.2 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 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 pouvoir déchiffrer ce fichier de clés, l'utilisateur doit alors initier une procédure challenge/réponse via l'outil de récupération de clé RecoverKeys.exe. Au cours de cette procédure, le mot de passe est transféré vers l'ordinateur cible. Le responsable support génère alors une réponse, puis sélectionne le mot de passe approprié pour déchiffrer le fichier de clés. Le mot de passe est transmis à l'ordinateur cible dans le code de réponse. Le fichier de clés peut alors être déchiffré à l'aide de ce mot de passe.

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

**Remarque:** Avec Web Helpdesk, 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, vous devez donc créer un fichier de clés et un mot de passe après chaque session de challenge/réponse aboutie.

## 6.3 Réponse à l'aide de clients virtuels

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

### 6.3.1 Conditions préalables

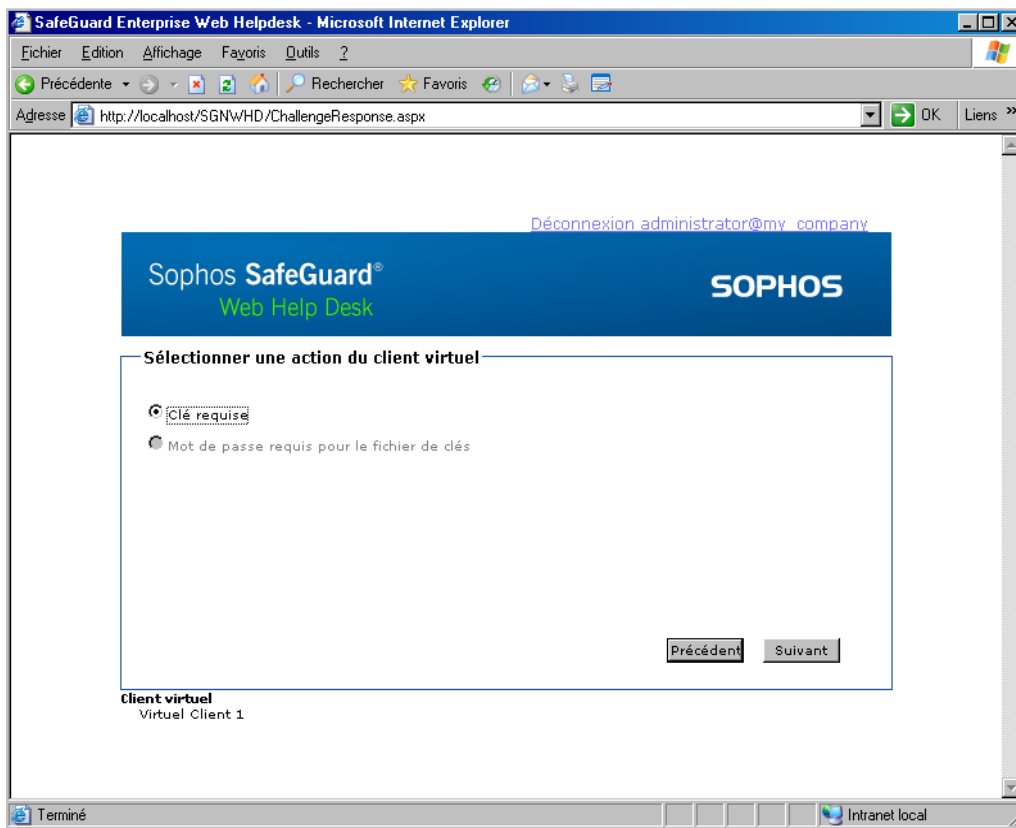
Les conditions préalables suivantes doivent être remplies :

- Le client virtuel doit avoir été créé dans la zone **Clés et certificats** de SafeGuard Management Center. Pour plus d'informations, reportez-vous au manuel de l'administrateur.
- Le responsable 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 recommandons de stocker ce fichier sur une carte mémoire.
- Lorsque la récupération de plusieurs clés est demandée, le responsable support doit tout d'abord créer un fichier de clés contenant les clés de récupération nécessaires dans la zone **Clés et certificats** de 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, reportez-vous au manuel de l'administrateur de SafeGuard Enterprise.
- 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, à savoir qu'elle n'est pas attribuée à un utilisateur au moins, une réponse pour client virtuel est impossible. Dans ce cas, la clé inactive peut être réattribuée à un autre utilisateur et une réponse pour cette clé peut être de nouveau générée.

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

Procédez comme suit :

1. En votre qualité de responsable 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 clé de récupération uniquement, sélectionnez **Clé requise**. Sélectionnez ensuite la clé appropriée dans la liste. 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** de SafeGuard Management Center et si le mot de passe de chiffrement du fichier de clés 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. 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 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 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 de l'utilisateur.
9. L'utilisateur doit redémarrer l'ordinateur, puis se reconnecter pour accéder aux volumes appropriés.

Les volumes sont à nouveau accessibles.

## 7 Récupération pour les clients SafeGuard autonomes

SafeGuard Enterprise fournit également la procédure challenge/réponse aux clients SafeGuard autonomes. Les clients 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 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 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 support lors de la procédure challenge/réponse. Si le responsable support peut accéder au fichier de récupération approprié, par exemple sur une carte mémoire ou via un chemin réseau partagé, une réponse peut être générée.

### 7.1 Actions de récupération pour les clients SafeGuard autonomes

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

- L'utilisateur a saisi le mot de passe de façon incorrecte un trop grand nombre de fois.
- L'utilisateur a oublié le mot de passe.
- Un cache endommagé doit être réparé.

Aucune clé utilisateur n'est disponible dans la base de données lorsqu'il s'agit d'un client SafeGuard autonome. Par conséquent, la seule action de récupération possible dans une session de Challenge/Réponse est **Initialiser le client SGN sans connexion utilisateur**.

La procédure Challenge/Réponse permettra à l'utilisateur de se connecter à partir de l'authentification au démarrage. L'utilisateur pourra également se connecter à Windows, même si le mot de passe Windows doit être réinitialisé.

#### 7.1.1 L'utilisateur a saisi le mot de passe de façon incorrecte un trop grand nombre de fois

Comme dans ce cas, 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 approprié au niveau Windows et réutiliser l'ordinateur.

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

**Remarque:** Nous recommandons d'utiliser en priorité Local Self Help pour récupérer un mot de passe oublié. Avec la récupération via Local Self Help, le mot de passe actuel de l'utilisateur peut être affiché de manière confidentielle dans l'authentification au démarrage et l'utilisateur peut continuer d'utiliser ce mot de passe. Cela évitera la réinitialisation du mot de passe et le recours à l'assistance du support. 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, une 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 davantage le mot de passe correct et doit par conséquent le modifier au niveau Windows. Cela nécessite d'autres actions de récupération sortant du périmètre de SafeGuard Enterprise, via des moyens Windows standard. Nous recommandons l'utilisation des méthodes de réinitialisation de mot de passe Windows suivantes.
  - Via un compte de service ou administrateur disponible sur votre ordinateur avec les droits Windows requis.
  - Via un disque de réinitialisation de mot de passe Windows.

En tant que responsable support, vous pouvez conseiller à l'utilisateur la procédure à appliquer et lui fournir les informations d'identification Windows supplémentaires ou le disque requis.

3. L'utilisateur saisit le nouveau mot de passe 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 alors 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, la définition d'un nouveau mot de passe sans donner l'ancien requiert un nouveau certificat. L'utilisateur doit confirmer cette procédure.
6. Un nouveau certificat utilisateur sera 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.

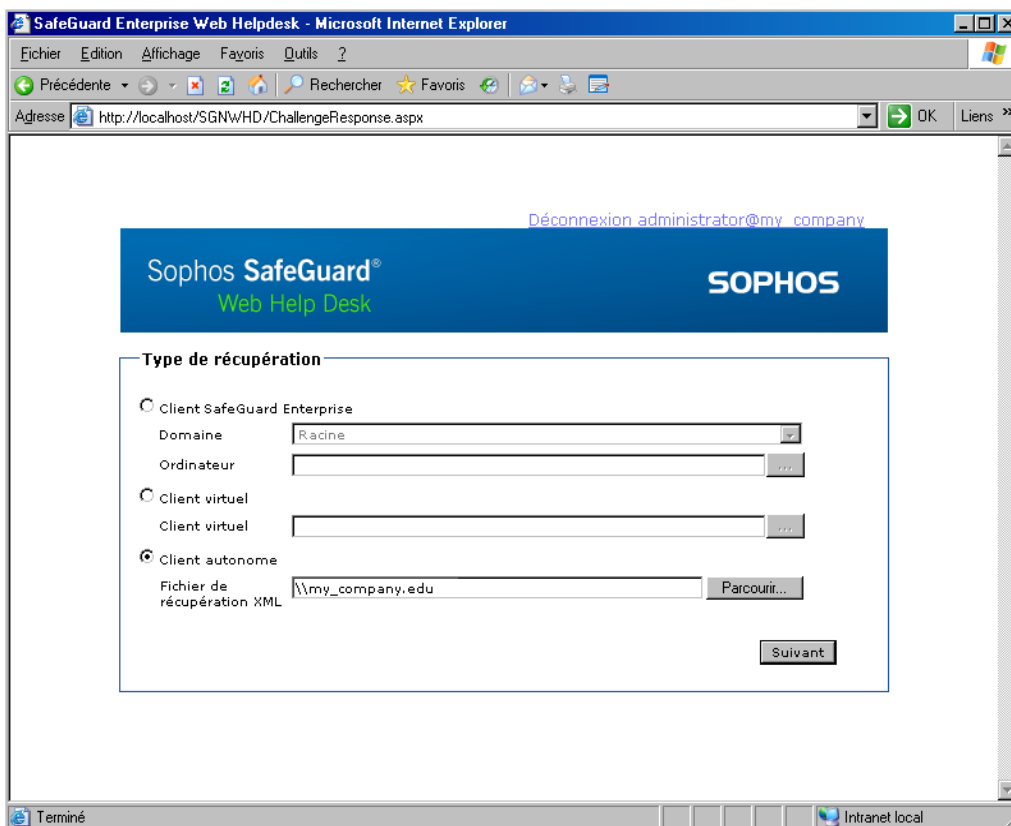
### Clés pour SafeGuard Data Exchange

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 passphrase correspondante. Pour continuer à utiliser les clés utilisateur déjà générées pour SafeGuard Data Exchange, l'utilisateur doit se souvenir des passphrases SafeGuard Data Exchange afin de les réactiver.

## 7.2 Création d'une réponse pour les clients 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. En votre qualité de responsable support, sélectionnez **Client autonome** dans la fenêtre **Type de récupération..**
2. Cliquez sur **Parcourir** pour sélectionner le fichier de récupération requis (au format .xml).



3. Le système vous demande de saisir le code de challenge que l'utilisateur vous a transmis.

4. Sélectionnez l'action que l'utilisateur doit entreprendre, puis cliquez sur **Suivant**.
5. Un code de réponse est généré. Lisez-le 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 accéder de nouveau à l'ordinateur.

## 8 Support technique

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

- Visitez le forum SophosTalk à l'adresse <http://community.sophos.com/> et recherchez d'autres utilisateurs qui connaissent le même problème.
- Visitez la base de connaissances du support technique 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.com](mailto:support@sophos.com), y compris le(s) numéro(s) de version du ou des logiciels Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tout message d'erreur.

## 9 Copyright

Copyright © 1996 - 2010 Sophos Group et Utimaco Safeware AG. Tous droits réservés.

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.

Sophos est une marque déposée de Sophos Plc et de Sophos Group. SafeGuard est une marque déposée de Utimaco Safeware AG - a member of the Sophos Group. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Tous les produits SafeGuard sont sous le copyright d'Utimaco Safeware AG - a member of the Sophos Group, ou, le cas échéant, des concédants de la licence. Tous les autres produits Sophos sont sous copyright de Sophos Plc, ou, le cas échéant, des concédants de la licence.

Vous trouverez des informations de copyright des fournisseurs tiers dans le fichier Disclaimer and Copyright for 3rd Party Software.rtf de votre répertoire d'installation.