SOPHOS
Security made simple.

SafeGuard Enterprise
Web Helpdesk

Version du produit : 7
Date du document : décembre 2014

Table des matières

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 Web de récupération. 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 de Helpdesk s'exécute également sur un ordinateur autonome sans nécessité d'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 Challenge/Réponse

Au cours 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 du support. En fonction de ce code de challenge, le responsable du support génère alors un code de réponse qui autorise l'utilisateur à effectuer une action spécifique sur l'ordinateur d'extrémité.

Situations d'urgence classiques nécessitant l'assistance du support

- Un utilisateur a oublié le mot de passe de connexion et l'ordinateur d'extrémité a été verrouillé.
- Un utilisateur a oublié ou perdu son token ou sa carte à puce.
- Le cache local de l'authentification au démarrage est partiellement endommagé.
- Un utilisateur est en congé maladie ou en vacances et un de ses collègues doit accéder aux données de son ordinateur.
- Un utilisateur souhaite accéder à un volume chiffré à l'aide d'une clé qui n'est pas disponible sur l'ordinateur d'extrémité.

SafeGuard Enterprise Web Helpdesk propose différents flux de travail de récupération pour ces situations d'urgence classiques, afin de permettre aux utilisateurs d'accéder de nouveau à leur ordinateur d'extrémité.

2 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/intranet et ne nécessite pas l'installation du logiciel SafeGuard Enterprise sur l'ordinateur « helpdesk ». Les sites Web doivent être hébergés séparément sur un serveur SafeGuard Enterprise avec les services Internet (IIS ou Internet Information Services).

Web Helpdesk peut être exécuté avec SafeGuard Management Center.

Remarque : nous vous conseillons de ne mettre Web Helpdesk qu'à disposition sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, il est déconseillé de mettre Web Helpdesk sur Internet.

Web Helpdesk fournit la récupération pour les clients suivants :

- Ordinateurs d'extrémité chiffrés par SafeGuard (clients SafeGuard Enterprise administrés)
- Clients virtuels
- Ordinateurs d'extrémité chiffrés par SafeGuard (clients SafeGuard autonomes non administrés)

3 Installation

Web Helpdesk doit être installé sur un serveur Web avec les services Internet (IIS) équipé du serveur SafeGuard Enterprise. En cas d'indisponibilité du serveur SafeGuard Enterprise, l'utilisateur est invité à l'installer. 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.

3.1 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.
- Les services Internet (IIS) de Microsoft doivent être installés.
- .NET Framework 4 et ASP.NET 4 doivent être installés.
- Pour Windows Server 2012 : le rôle ASP.NET doit être installé (Rôles du serveur > Serveur Web (IIS) > Serveur Web > Développement d'applications > ASP.NET 4.5).

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

Configuration requise pour l'ordinateur d'extrémité

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 et supérieur
- Mozilla Firefox 2 et supérieur

3.2 Installation de Web Helpdesk

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

1. Cliquez deux fois sur SGNWebHelpDesk.msi. Un assistant vous guide tout au long de l'installation. Acceptez les valeurs par défaut selon le cas. Sélectionnez une installation **Complète** si vous y êtes invité.
2. Une fois l'installation terminée, il se peut que vous soyez invité à redémarrer. Cliquez sur **Oui** ou sur **Terminer**.

Le programme d'installation de Web Helpdesk vérifie si le serveur SafeGuard Enterprise est déjà installé sur le serveur Web des services Internet (IIS). En cas d'indisponibilité, vous serez invité à l'installer.

3.2.1 Configuration du serveur Web avec SSL

Pour une sécurité optimale, configurez le serveur Web des services Internet (IIS) de la manière suivante :

1. Déployez Web Helpdesk uniquement sur intranet.

   Veillez à ce que Web Helpdesk soit uniquement disponible sur le réseau intranet de votre entreprise. Pour des raisons de sécurité, n'accordez pas l'accès à Web Helpdesk sur Internet.

2. Établissez une connexion SSL.

   Vous pouvez limiter la disponibilité de Web Helpdesk aux utilisateurs définis en utilisant la configuration des services Internet (IIS) standard fournie avec les des services Internet. Assurez-vous que le certificat de sécurité SSL est installé sur le serveur des services Internet (IIS). Toutes les communications de Web Helpdesk seront prises en charge via le protocole SSL.

   Les tâches générales suivantes doivent être effectuées pour l'installation du 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 des services Internet (IIS) configuré pour utiliser SSL et sélectionner le certificat.

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

   d) Les processus de travail du pool d'applications **`SGNWHD-Pool`** ne doivent pas être supérieurs à 1 (valeur par défaut). Faute de quoi, l'autorisation d'accès à Web Helpdesk est impossible.

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

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

3.2.2 Enregistrement et configuration du serveur SafeGuard Enterprise

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

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

4. Dans **Enregistrement du serveur**, cliquez sur **[...]** pour sélectionner le certificat machine du serveur. Ce dernier est généré lors de l'installation du serveur SafeGuard Enterprise. Par défaut, il se trouve dans le répertoire **`MachCert`** du répertoire d'installation du serveur SafeGuard Enterprise (nom de fichier : **`<nomordinateur>.cer)`**. Si le serveur SafeGuard Enterprise est installé sur un autre ordinateur que SafeGuard Management Center, ce fichier **`.cer`** doit être accessible via une autorisation réseau ou une copie doit être mise à disposition.

   Ne sélectionnez pas le certificat MSO.

   Le FQDN, par exemple **`serveur.monentreprise.edu`** et les informations de certificat apparaissent.

   Si vous utilisez le chiffrement de transport SSL entre l'ordinateur d'extrémité et le serveur SafeGuard Enterprise, le nom du serveur indiqué ici doit être identique à celui indiqué dans le certificat SSL. Sinon, ils ne pourront pas communiquer.

5. Cliquez sur **OK**.

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

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

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

7. Cliquez sur **OK** pour confirmer le message de succès.
8. Dans l'onglet **Serveurs**, 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 **Serveurs**.

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.

3.3 Mise à jour de Web Helpdesk

Lors de la mise à jour de Web Helpdesk à la dernière version, nous vous conseillons de désinstaller Web Helpdesk puis d'installer la dernière version de Web Helpdesk. Créez uniquement un nouveau package de configuration du serveur si des paramètres du serveur ont été mis à jour.

3.4 Langues prises en charge

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

4 Autorisation de connexion à Web Helpdesk pour les utilisateurs sans client SafeGuard Enterprise

Il est possible d'utiliser Web Helpdesk sans le client SafeGuard Enterprise.

Les droits d'accès peuvent être gérés en ajoutant ou en supprimant les utilisateurs ou groupes Windows.

Remarque :

Cette fonction utilise l'authentification Windows. Lorsque l'authentification Windows est activée, il n'est plus possible de se connecter par le biais d'un utilisateur Active Directory.

4.1 Conditions préalables à la connexion sans client SafeGuard Enterprise

Les conditions préalables suivantes doivent être remplies :

1. Un groupe d'utilisateurs Windows doit être créé et configuré. Il doit contenir des utilisateurs autorisés à accéder à Web Helpdesk. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.
2. L'authentification Windows à Web Helpdesk doit être activée (**Outils - Outil de package de configuration - Serveurs - Win. Auth. WHD**. Retrouvez plus d'informations dans le *Guide d'installation de SafeGuard Enterprise*).

4.2 Activation de l'authentification Windows pour SafeGuard Web Helpdesk

1. Ouvrez le Gestionnaire des services Internet (IIS).
2. Sous **Sites** > **Site Web par défaut**, sélectionnez le nœud de l'utilisateur (par exemple SGNWHD).
3. Sélectionnez **Authentification**.
4. Sélectionnez le nom de l'entrée **Authentification Windows** dans la liste des authentifications.
5. Cliquez sur **Activer** sur la barre **Actions** située sur le côté droit.
6. Sélectionnez ensuite **Règles d'autorisation .NET** pour ajouter trois règles d'autorisation .NET.

   Remarque : Windows 2008 Server n'affiche pas d'icône dans les services Internet (IIS) pour les **Règles d'autorisation .NET**. En revanche, il y a un lien vers les **Règles d'autorisation**. Pour modifier ces règles, le rôle **Autorisation d'URL** doit être installé en allant dans **IIS** > **Sécurité** > **Autorisation d'URL**.

7. Sur la barre **Actions**, cliquez sur **Ajouter une règle de refus...**.
8. Une boîte de dialogue s'ouvre. Refusez l'accès en activant **Utilisateurs anonymes**. Cliquez sur **OK** pour confirmer.

9. Retournez sur la barre **Actions** et cliquez sur **Ajouter une règle d'autorisation...**.
10. Une boîte de dialogue s'ouvre. Activez **Rôles ou groupes d'utilisateurs définis** et saisissez le nom de votre groupe d'utilisateurs en incluant le nom de domaine dans le champ (par exemple <Nom de domaine>\Utilisateurs WHD) pour autoriser l'accès groupe d'utilisateurs au groupe d'utilisateurs que vous avez indiqué.
11. Cliquez sur **OK** pour confirmer.
12. Retournez sur la barre **Actions** et cliquez sur **Ajouter une règle de refus...**.
13. Une boîte de dialogue s'ouvre. Activez **Tous les utilisateurs** pour refuser l'accès à tous les utilisateurs. Cliquez sur **OK** pour confirmer.
14. Assurez-vous que les entrées sont dans l'ordre suivant :
    - Refuser - Utilisateurs anonymes - Local
    - Autoriser - <Nom de domaine\Nom du groupe> - Local
    - Refuser - Tous les utilisateurs - Local
    - Refuser - Tous les utilisateurs - Héritée

Testez la fonctionnalité en vous connectant conformément aux instructions de la section Connexion avec authentification Windows à la page 9. L'écran de bienvenue apparaît.

Si vous devez désactiver l'authentification Windows pour permettre la connexion par le biais d'un utilisateur Active Directory promu, supprimez la règle **Refuser - Tous les utilisateurs anonymes**.

Remarque : vous pouvez également activer l'authentification Windows en modifiant le fichier web.config. Par exemple :

```
<configuration>
  <system.web>
    <authentication mode="Windows" />
     <authorization>
      <allow roles="HelpDesk" />
      <deny users="*" />
     </authorization>
  </system.web>
</configuration>
```

4.3 Connexion avec l'authentification Windows

Veuillez procéder comme suit :

1. Ouvrez le navigateur et saisissez l'URL.
2. Appelez l'application en saisissant son URL : **`https://<ID de l'hôte ou adresse IP>/SGNWHD`**
3. Sélectionnez l'option **Récupération** ou **Approuver la suspension** et procédez conformément aux instructions de la section À propos des types de récupération à la page 13 et des sections suivantes.

5 Authentification

Les responsables de la sécurité doivent s'authentifier dans Web Helpdesk et sur le serveur SafeGuard Enterprise afin de pouvoir utiliser l'assistant de récupération basé sur le Web. Les responsables de la sécurité se connectent à Web Helpdesk à l'aide de leurs nom d'utilisateur et mot de passe qui sont les mêmes que leurs codes d'accès Windows.

Les utilisateurs se voient proposer deux cas de figure différents :

- Les utilisateurs qui ont été promus au rang de responsables de la sécurité dans SafeGuard Management Center se connectent conformément aux instructions de la section Connexion à Web Helpdesk sans authentification Windows à la page 10.
- Les utilisateurs qui font partie d'un groupe d'utilisateurs Web Helpdesk spécifique avec « Authentification Windows activée » se connectent conformément aux instructions de la section Connexion avec authentification Windows à la page 9.

5.1 Préparations dans SafeGuard Management Center

Pour pouvoir procéder à l'authentification dans Web Helpdesk sans utiliser l'authentification Windows, les conditions préalables suivantes doivent être remplies et les préparations suivantes doivent être effectuées dans SafeGuard Management Center. Retrouvez plus d'informations dans le *Manuel d'administration 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. Ces certificats (fichier **`.p12`**) doivent être disponibles dans la base de données.
3. Les futurs utilisateurs de Web Helpdesk doivent 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 nom de responsable de la sécurité défini, qui est une combinaison de leur nom d'utilisateur Windows et du nom du domaine qui leur est attribué. Le mot de passe Windows est requis pour assurer la protection des certificats.

4. Les responsables de la sécurité doivent se voir attribuer le rôle de responsable du support afin de pouvoir s'authentifier dans Web Helpdesk.
5. Ils doivent également avoir les droits d'accès sur les objets qu'ils vont utiliser comme, par exemple, les domaines ou les unités organisationnelles. Retrouvez plus d'informations à la section *Attribution d'objets de répertoire à un responsable de la sécurité* du *Manuel d'administration de SafeGuard Enterprise.*

Remarque : les responsables de la sécurité de Web Helpdesk doivent s'authentifier sur le serveur SafeGuard Enterprise. L'authentification via un token n'est pas prise en charge dans Web Helpdesk.

5.2 Connexion à Web Helpdesk sans l'authentification Windows

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 le nom de responsable de la sécurité que vous avez créé dans SafeGuard Management Center au format suivant : **`<nom d'utilisateur>@<DOMAINE>`** par exemple **`ResponsableWHD@MONDOMAINE`**.

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

4. Saisissez votre mot de passe Windows.
5. Cliquez sur **Connexion**.

Vous êtes connecté à Web Helpdesk.

Remarque : si le certificat est créé lors de la promotion d'un utilisateur, ce dernier doit utiliser le mot de passe du certificat pour se connecter à SafeGuard Management Center. Il va devoir saisir le mot de passe du certificat même s'il est invité à saisir le mot de passe Windows.

6 Sélection de l'assistant de Web Helpdesk

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**. Retrouvez plus d'informations à la section À propos des types de récupération à la page 13.
   - Pour autoriser la suspension de la stratégie SafeGuard Configuration Protection, sélectionnez **Approuver la suspension**. Retrouvez plus d'informations à la section Module SafeGuard Configuration Protection à la page 25.

7 À propos des types de récupération

Vous pouvez sélectionner le type de récupération requis. Les types de récupération suivants sont fournis :

- **Client SafeGuard Enterprise (administré)**

  Il s'agit de la récupération de connexion pour les ordinateurs administrés de façon centralisée par SafeGuard Management Center. Les ordinateurs d'extrémité administrés sont répertoriés dans la zone **Utilisateurs et ordinateurs** de 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 lancée 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.

- **Client Sophos SafeGuard (autonome)**

  Il s'agit de la récupération de connexion des ordinateurs d'extrémité administrés localement. Ils ne sont jamais connectés au serveur SafeGuard Enterprise. Pour chaque ordinateur d'extrémité Sophos SafeGuard non administré, 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 clé de récupération est disponible, par exemple sur une carte mémoire USB ou sur 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.

8 Récupération pour les ordinateurs d'extrémité administrés (clients SafeGuard Enterprise administrés)

SafeGuard Enterprise fournit la procédure de récupération aux ordinateurs d'extrémité protégés par le client SafeGuard Enterprise administré dans différentes situations de récupération d'urgence, par exemple la récupération de mots de passe ou l'accès aux données par démarrage à partir d'un support externe.

Le programme détermine de façon dynamique si le chiffrement intégral du disque de SafeGuard Enterprise ou si le Chiffrement de lecteur BitLocker est utilisé et règle le flux de travail de récupération en conséquence.

8.1 Actions de récupération pour les ordinateurs d'extrémité administrés

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

Remarque : pour les ordinateurs d'extrémité chiffrés BitLocker, l'action de récupération consiste à récupérer la clé utilisée pour chiffrer un volume spécifique. La récupération de mots de passe n'est pas proposée.

8.1.1 Récupération du mot de passe à l'authentification au démarrage

L'une des situations les plus courantes est l'oubli du mot de passe par l'utilisateur. Par défaut, SafeGuard Enterprise est installé avec l'authentification au démarrage (POA) activée. Le mot de passe à l'authentification au démarrage permettant d'accéder à l'ordinateur d'extrémité est identique au mot de passe Windows.

Si l'utilisateur a oublié le mot de passe au niveau de l'authentification au démarrage, le responsable du support peut générer une réponse pour **Démarrer le client SGN avec une connexion utilisateur**, mais sans afficher le mot de passe de l'utilisateur. Cependant, dans ce cas, après la saisie du code de réponse, l'ordinateur d'extrémité démarre le système d'exploitation. L'utilisateur doit donc changer son mot de passe Windows conformément aux conditions définies sur le domaine. L'utilisateur peut alors se connecter à Windows ainsi qu'à l'authentification au démarrage à l'aide du nouveau mot de passe.

Bon usage de récupération du mot de passe à l'authentification au démarrage

Si l'utilisateur a oublié son mot de passe, nous vous conseillons d'utiliser les méthodes suivantes afin d'éviter d'avoir à réinitialiser le mot de passe de manière centralisée :

- **Utilisation de Local Self Help :** Local Self Help permet à l'utilisateur d'afficher son mot de passe et de continuer à l'utiliser. Ceci évite d'avoir à réinitialiser le mot de passe ou de demander de l'aide au support technique. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.

- **Utilisation de la procédure Challenge/Réponse pour les clients SafeGuard Enterprise (administrés) :** nous déconseillons la réinitialisation du mot de passe dans Active Directory

avant la procédure Challenge/Réponse. En effet, ceci vous donne la garantie que le mot de passe demeure synchronisé entre Windows et SafeGuard Enterprise. Assurez-vous que le support technique de Windows est bien informé.

En tant que responsable du support de SafeGuard Enterprise, générez une réponse pour **Démarrer le client SGN avec une connexion utilisateur** à l'aide de l'option **Afficher le mot de passe utilisateur**. Vous évitez de cette manière d'avoir à réinitialiser le mot de passe de l'utilisateur dans Active Directory. L'utilisateur peut continuer à travailler avec le mot de passe actuel et le modifier localement par la suite, s'il le souhaite.

8.1.2 Affichage du mot de passe de l'utilisateur

SafeGuard Enterprise offre une option permettant aux utilisateurs d'afficher leur mot de passe lors de la procédure Challenge/Réponse. De cette manière, il n'est pas nécessaire de réinitialiser le mot de passe dans Active Directory. Cette option est uniquement disponible si l'action **Démarrer le client SGN avec une connexion utilisateur** est demandée.

8.1.3 Accès aux données par démarrage de l'ordinateur d'extrémité à partir d'un support externe

Il est également possible d'utiliser la procédure Challenge/Réponse pour autoriser le démarrage d'un ordinateur d'extrémité à partir d'un support externe, par exemple WinPE. Pour ce faire, l'utilisateur doit sélectionner **Poursuivre le démarrage à partir de : Disquette/Support externe** dans la boîte de dialogue de connexion de l'authentification au démarrage et lancer le challenge. À la réception de la réponse, l'utilisateur saisit comme d'habitude les codes d'accès dans l'authentification au démarrage et poursuit le démarrage à partir du support externe.

Les conditions suivantes doivent être remplies pour pouvoir accéder à un volume chiffré :

- Le périphérique à utiliser doit contenir le pilote du filtre SafeGuard Enterprise. Retrouvez plus d'informations sur la manière d'obtenir ce CD-ROM pilote sur : http://www.sophos.com/fr-fr/support/knowledgebase/108805.aspx
- L'utilisateur doit démarrer l'ordinateur d'extrémité à partir d'un support externe. Vous pouvez lui octroyer ce droit en définissant une stratégie dans SafeGuard Management Center et en l'affectant à l'ordinateur d'extrémité (l'option de stratégie **Authentification > Accès : L'utilisateur peut uniquement démarrer à partir du disque dur interne** doit être définie sur **Non**).
- L'ordinateur d'extrémité doit autoriser le démarrage à partir du support externe.
- Seuls les volumes chiffrés avec la clé machine définie sont accessibles. Ce type de chiffrement de clés peut être défini dans une stratégie de chiffrement des périphériques dans SafeGuard Management Center et affecté à l'ordinateur d'extrémité.

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

8.1.4 Restauration du cache de la stratégie SafeGuard Enterprise

Si la mémoire cache de la stratégie SafeGuard Enterprise est endommagée, l'utilisateur est invité automatiquement à lancer une procédure Challenge/Réponse lors de la connexion à l'authentification au démarrage.

8.2 Création d'une réponse pour les ordinateurs d'extrémité administrés

Pour créer une réponse pour les ordinateurs administrés (clients SafeGuard Enterprise), le nom de l'ordinateur et le nom de domaine sont nécessaires.

1. Sur la page **Type de récupération**, sélectionnez **Client SafeGuard Enterprise**.
2. Dans la liste, sélectionnez le domaine requis.
3. Saisissez le nom de l'ordinateur requis. Vous pouvez procéder de plusieurs façons :
   - Sélectionnez un nom en cliquant sur **[...]**, puis sur **Rechercher** dans la fenêtre contextuelle. Une liste des ordinateurs s'affiche. Sélectionnez l'ordinateur requis, puis cliquez sur **OK**. Le nom de l'ordinateur s'affiche désormais dans la fenêtre **Type de récupération** sous **Domaine**.
   - Saisissez le nom abrégé de l'ordinateur. Lorsque vous cliquez sur **Suivant**, ce nom est recherché dans la base de données. S'il est trouvé, le nom d'ordinateur unique s'affiche.
   - Saisissez directement le nom de l'ordinateur au format de nom unique, par exemple :

     `CN=Poste1,OU=Développement,OU=Siège,DC=Utimaco,DC=com`

4. Cliquez sur **Suivant**.

Le programme détermine ensuite de façon dynamique si c'est le chiffrement intégral du disque de SafeGuard Enterprise ou le Chiffrement de lecteur BitLocker qui est utilisé et ajuste le flux de travail de récupération en conséquence.

- S'il s'agit d'un ordinateur protégé par SafeGuard Enterprise, l'étape suivante requiert la sélection des informations de l'utilisateur.
- S'il s'agit d'un ordinateur chiffré avec BitLocker, un volume qui n'est plus accessible peut être récupéré. L'étape suivante nécessite la sélection du volume à déchiffrer.

8.2.1 Création d'une réponse pour les ordinateurs protégés par le chiffrement intégral du disque de SafeGuard Enterprise

1. Dans **Domaine**, sélectionnez le domaine requis de l'utilisateur. S'il s'agit d'un utilisateur local, sélectionnez **Utilisateur local sur <nom de l'ordinateur>**.
2. Recherchez le nom de l'utilisateur requis. Procédez de l'une des manières suivantes :
   - Cliquez sur **Rechercher par Nom affiché**. Sélectionnez le nom requis dans la liste et cliquez sur **OK**.
   - Cliquez sur **Rechercher par Nom de connexion**. Sélectionnez le nom requis dans la liste et cliquez sur **OK**.
   - Saisissez directement le nom de l'utilisateur. Assurez-vous d'orthographier le nom correctement.
3. Cliquez sur **Suivant**. Une fenêtre s'affiche, dans laquelle vous pouvez saisir le code de challenge.
4. Saisissez le code de challenge que l'utilisateur vous a 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, si **Token cryptographique demandé** est requis, les actions disponibles pour la réponse sont **Démarrer le client SGN avec une connexion utilisateur** et **Démarrer le client SGN sans connexion utilisateur**.
6. Sélectionnez l'action que l'utilisateur doit exécuter.
7. Si l'action **Démarrer le client SGN avec une connexion utilisateur** a été sélectionnée comme réponse, vous pouvez également sélectionner **Afficher le mot de passe utilisateur** afin d'afficher le mot de passe sur l'ordinateur d'extrémité cible.
8. Cliquez sur **Suivant**. Un code de réponse est généré.
9. Lisez ou envoyez le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

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

8.2.2 Création d'une réponse pour les ordinateurs protégés par le Chiffrement de lecteur BitLocker

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

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

9 Récupération à l'aide de clients virtuels

L'utilisation des clients virtuels pour la récupération de l'accès à des volumes chiffrés dans SafeGuard Enterprise permet la récupération même dans des situations d'urgence complexes.

Ce type de récupération peut être appliquée dans les situations classiques suivantes :

- L'authentification au démarrage est corrompue.
- Un volume est chiffré avec une clé différente de celle de la clé machine définie sur l'ordinateur. La clé nécessaire n'est pas disponible dans l'environnement de l'utilisateur. Par conséquent, elle doit être identifiée dans la base de données, puis transférée vers l'ordinateur d'extrémité de façon sécurisée.

Remarque : la récupération à l'aide d'un client virtuel doit uniquement être utilisée pour résoudre des situations de récupération complexes. Si les problèmes mentionnés ci-dessus ont lieu, l'utilisation d'un client virtuel est appropriée. Cependant, si seule la clé nécessaire manque pour la récupération d'un volume, la meilleure solution consiste à affecter tout simplement la clé manquante au jeu de clés de l'utilisateur approprié.

Dans ces situations, SafeGuard Enterprise propose la solution suivante :

Pour activer une procédure Challenge/Réponse dans cette situation, vous pouvez créer des fichiers spécifiques, appelés clients virtuels, dans SafeGuard Management Center et les distribuer à l'utilisateur avant le démarrage de la session de Challenge/Réponse. La procédure de Challenge/Réponse peut ensuite être lancée sur 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 Helpdesk, la récupération à l'aide des clients virtuels n'est pas prise en charge pour les ordinateurs d'extrémité non administrés (clients Sophos SafeGuard autonomes). Utilisez plutôt SafeGuard Management Center.

9.1 Flux de travail de récupération à l'aide de clients virtuels

Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.

1. Le responsable du support crée le client virtuel dans la zone **Clés et certificats** de SafeGuard Management Center et l'exporte dans un fichier. Ce fichier, appelé **`recoverytoken.tok`**, doit être distribué aux utilisateurs et mis à leur disposition avant la session de Challenge/Réponse.
2. L'utilisateur doit ensuite démarrer un CD-ROM de récupération de SafeGuard Enterprise ou tout autre CD-ROM à l'aide d'un environnement WinPE modifié de SafeGuard Enterprise sur son ordinateur, à partir du BIOS, sans aucune authentification au démarrage, puis lancer une session de Challenge/Réponse à l'aide d'un outil de récupération de clé de SafeGuard Enterprise.

   Dans la base de données SafeGuard Enterprise, le fichier du client virtuel est utilisé et indiqué dans le challenge au lieu du nom de l'utilisateur/de l'ordinateur qui n'est pas disponible dans ce cas.

3. L'outil de récupération de clé de l'utilisateur indique alors à ce dernier les volumes qui sont chiffrés et les clés qui sont utilisées pour chacun de ces volumes. L'utilisateur fournit ensuite ces informations au responsable du support.
4. Le responsable du support identifie le client virtuel dans la base de données et sélectionne la clé requise pour accéder aux volumes chiffrés : soit une clé unique, soit plusieurs clés exportées vers un fichier de clé. Le responsable du support génère alors le code de réponse.
5. L'utilisateur saisit le code de réponse, dans lequel les clés requises sont transportées. Pour accéder de nouveau aux volumes chiffrés, l'utilisateur saisit le code de réponse et redémarre l'ordinateur.

9.2 Actions de récupération à l'aide de clients virtuels

Pour que l'utilisateur puisse accéder aux volumes chiffrés à l'aide des clés qui ne sont pas à sa disposition, les clés de chiffrement correctes doivent être transférées de la base de données vers l'environnement de l'utilisateur.

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

- Transfert d'une seule clé
- Transfert de plusieurs clés dans un fichier de clé chiffré

9.2.1 Transfert d'une seule clé

Un Challenge/Réponse peut être lancé pour récupérer une seule clé afin d'accéder à un volume chiffré. Le responsable du support doit sélectionner la clé nécessaire dans la base de données, puis générer un code de réponse. Cette clé est chiffrée et transférée vers 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.

9.2.2 Transfert de plusieurs clés dans un fichier de clé chiffré

Une procédure Challenge/Réponse peut être lancée en vue de récupérer plusieurs clés afin d'accéder aux volumes chiffrés. Les clés sont stockées dans un fichier, qui est chiffré par mot de passe. Pour ce faire, le responsable du support doit avoir exporté une ou plusieurs clés requises à stocker dans un fichier. Ce fichier est chiffré à l'aide d'un mot de passe aléatoire, qui est stocké dans la base de données. Ce mot de passe est exclusif à chaque fichier de clé créé.

Le fichier de clé chiffré doit être transféré vers l'environnement de l'utilisateur et mis à la disposition de l'utilisateur. Pour déchiffrer ce fichier de clé, l'utilisateur doit alors lancer une session Challenge/Réponse via l'outil de récupération de clé **`RecoverKeys.exe`**. Au cours de cette session, le mot de passe est transféré vers l'ordinateur d'extrémité cible. Le responsable du support génère alors une réponse, puis sélectionne le mot de passe approprié pour déchiffrer le fichier de clé. Le mot de passe est transféré à l'ordinateur d'extrémité cible dans le code de réponse. Le fichier de clé peut alors être déchiffré à l'aide du mot de passe.

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

Remarque : avec Web Helpdesk, un fichier de clé et le mot de passe correspondant sont supprimés de la base de données dès qu'ils ont été utilisés dans une session de

Challenge/Réponse. Veuillez donc créer un nouveau fichier de clé et un mot de passe après chaque session de Challenge/Réponse réussie.

9.3 Réponse à l'aide de clients virtuels

9.3.1 Conditions préalables

- Le client virtuel doit avoir été créé dans la zone **Clés et certificats** de SafeGuard Management Center. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.
- Le responsable du support doit être en mesure de localiser le client virtuel dans la base de données. Les clients virtuels sont identifiés de façon unique par leur nom.
- Le fichier du client virtuel, **recoverytoken.tok**, doit être à la disposition de l'utilisateur. Ce fichier doit être stocké dans le même dossier que l'outil de récupération de clé. Nous vous conseillons de stocker ce fichier sur une carte mémoire.
- Lorsque la récupération de plusieurs clés est demandée, le responsable du support doit d'abord créer un fichiers de clé contenant les clés de récupération nécessaires dans le champ **Clés et certificats** de SafeGuard Management Center. Le fichier de clé doit être à la disposition de l'utilisateur pour qu'une récupération puisse être effectuée. Le mot de passe de chiffrement de ce fichier de clé doit être indiqué dans la base de données. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.
- L'utilisateur doit avoir démarré l'outil de récupération de clé et lancé la session de Challenge/Réponse.
- Une réponse ne peut être lancée que pour des clés 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.

9.3.2 Création d'une réponse à l'aide de clients virtuels

1. En tant que responsable du support, sélectionnez **Client virtuel** dans la fenêtre **Type de récupération**.
2. Saisissez le nom du client virtuel que l'utilisateur vous a indiqué. Pour ce faire, vous pouvez procéder de plusieurs façons :
   - Saisissez directement le nom unique.
   - Sélectionnez un nom en cliquant sur **[...]**, puis sur **Rechercher** dans la fenêtre contextuelle. La liste des clients virtuels s'affiche. Sélectionnez le client virtuel requis, puis cliquez sur **OK**. Le nom du client virtuel s'affiche alors dans la fenêtre **Type de récupération** dans **Client virtuel**.
3. Cliquez sur **Suivant**. La page dans laquelle vous pouvez sélectionner l'action de récupération s'affiche.
4. Sélectionnez l'action de récupération que l'utilisateur doit effectuer, puis cliquez sur **Suivant**.
   - Si vous devez transférer une seule clé de récupération, sélectionnez **Clé requise**. Dans la liste, sélectionnez la clé nécessaire. Cliquez sur **[...]**. Vous pouvez afficher les clés en fonction de leur ID ou de leur nom symbolique. Cliquez sur **Rechercher**, sélectionnez la clé, puis cliquez sur **OK**.

- Si l'utilisateur a besoin d'un fichier de clé contenant plusieurs clés de récupération, sélectionnez **Mot de passe du fichier de clé requis** afin de transmettre à l'utilisateur le mot de passe du fichier de clé chiffré. Sélectionnez le fichier de clé requis. Cliquez sur **[...]**, puis sur **Rechercher**. Sélectionnez le fichier de clé et cliquez sur **OK**.

Vous pouvez sélectionner l'option **Mot de passe du fichier de clé demandé** uniquement si un fichier de clé a été créé dans la zone **Clés et certificats** de SafeGuard Management Center et si le mot de passe de chiffrement du fichier de clé est stocké dans la base de données. Avec Web Helpdesk, les fichiers de clés et les mots de passe correspondants sont supprimés de la base de données dès qu'ils ont été utilisés dans une session de Challenge/Réponse. Veuillez donc créer un nouveau fichier de clé et un mot de passe après chaque session de Challenge/Réponse réussie.

5. Cliquez sur **Suivant**. La page dans laquelle vous devez saisir le code de challenge s'affiche.
6. Saisissez le code de challenge que l'utilisateur vous a 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 à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.
   - Si une seule clé est demandée, la clé générée est transférée dans le code de réponse.
   - Si un mot de passe est demandé pour le fichier de clé chiffré, il est transféré dans le code de réponse. Ce fichier de clé est ensuite supprimé.
8. L'utilisateur doit saisir le code de réponse sur l'ordinateur d'extrémité.
9. L'utilisateur doit redémarrer l'ordinateur et se reconnecter pour accéder aux volumes.

Les volumes sont à nouveau accessibles.

10 Récupération pour les ordinateurs d'extrémité non administrés (clients Sophos SafeGuard autonomes)

SafeGuard Enterprise inclut également des procédures Challenge/Réponse pour les ordinateurs d'extrémité non administrés (clients Sophos SafeGuard autonomes). Ils 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, leur identification pendant une procédure Challenge/Réponse est impossible.

La procédure Challenge/Réponse des ordinateurs d'extrémité autonomes est donc basée sur le fichier de clé de récupération créé lors de la configuration de l'ordinateur d'extrémité. Le fichier de récupération (au format .xml) est généré pour chaque ordinateur d'extrémité non administré 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 carte mémoire ou via un chemin réseau partagé, une réponse peut être générée.

10.1 Actions de récupération pour les ordinateurs d'extrémité non administrés

La procédure Challenge/Réponse pour les ordinateurs d'extrémité non administrés (client Sophos SafeGuard autonome) doit être lancée dans les situations suivantes :

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

Aucune clé utilisateur n'est disponible dans la base de données pour les ordinateurs d'extrémité non administrés. Par conséquent, la seule action de récupération possible dans une session de Challenge/Réponse est **Démarrer le client Sophos SafeGuard sans connexion utilisateur**.

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

10.1.1 L'utilisateur a saisi un mot de passe incorrect un trop grand nombre de fois

Dans ce cas de figure, la réinitialisation du mot de passe n'est pas nécessaire. En effet, la procédure Challenge/Réponse permet à l'utilisateur de se connecter à l'authentification au démarrage. L'utilisateur peut ensuite saisir le mot de passe Windows approprié et réutiliser l'ordinateur d'extrémité.

10.1.2 L'utilisateur a oublié le mot de passe

Remarque : nous vous conseillons d'utiliser Local Self Help pour récupérer un mot de passe oublié. Grâce à Local Self Help, vous pouvez afficher le mot de passe actuel et continuer à l'utiliser. Ceci vous évite d'avoir à réinitialiser le mot de passe ou de demander de l'aide au support technique. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.

Lors de la récupération d'un mot de passe oublié via la procédure Challenge/Réponse, la réinitialisation de mot de passe est requise.

1. La procédure Challenge/Réponse permet à l'ordinateur de démarrer à partir de l'authentification au démarrage.
2. Dans la boîte de dialogue de connexion Windows, l'utilisateur ne connaît pas le mot de passe et doit par conséquent le modifier au niveau Windows. D'autres actions de récupération doivent être effectuées via des moyens Windows standard. En effet, elles sont hors du champ d'application de SafeGuard Enterprise. Nous vous conseillons d'utiliser les méthodes de réinitialisation de mot de passe Windows.
   - À l'aide d'un compte de service ou administrateur disponible sur votre ordinateur avec les droits Windows requis.
   - À l'aide d'un disque de réinitialisation de mot de passe Windows.

   En tant que responsable du support, vous pouvez informer l'utilisateur de la procédure à appliquer et lui fournir les codes d'accès Windows supplémentaires ou le disque requis.
3. L'utilisateur saisit le nouveau mot de passe dans la boîte de dialogue de connexion Windows fourni par le support. L'utilisateur modifie ensuite ce mot de passe immédiatement en choisissant une valeur connue de lui seul.
4. SafeGuard Enterprise détecte que le nouveau choix de mot de passe ne correspond pas au mot de passe SafeGuard Enterprise utilisé actuellement au niveau de l'authentification au démarrage. L'utilisateur est invité à saisir son ancien mot de passe SafeGuard Enterprise et, puisqu'il a oublié son mot de passe, il doit cliquer sur **Annuler**.
5. Dans SafeGuard Enterprise, un nouveau certificat est nécessaire afin de pouvoir définir un nouveau mot de passe sans avoir à fournir l'ancien.
6. Un nouveau certificat d'utilisateur est créé en fonction du nouveau choix de mot de passe Windows. L'utilisateur peut donc se reconnecter à l'ordinateur ainsi qu'à l'authentification au démarrage à l'aide du nouveau mot de passe.

   Clés pour SafeGuard Data Exchange

   Si l'utilisateur a oublié son mot de passe Windows et que celui-ci a été réinitialisé, les clés déjà créées pour SafeGuard Data Exchange ne pourront pas être utilisées sans la phrase secrète correspondante. Pour continuer à utiliser les clés utilisateur déjà générées pour SafeGuard Data Exchange, l'utilisateur doit se souvenir des phrase secrètes SafeGuard Data Exchange afin de les réactiver.

10.2 Création d'une réponse pour les ordinateurs d'extrémité non administrés

Pour générer une réponse pour un ordinateur non administré, indiquez le nom du fichier de récupération (au format .xml).

1. Dans Web Helpdesk, sur le menu **Outils**, cliquez sur **Récupération**.
2. Dans **Type de récupération**, sélectionnez **Client autonome**.

3. Cliquez sur **Parcourir** pour localiser le fichier (.xml) de récupération de clé requis.
4. Saisissez le code de challenge que l'utilisateur vous a indiqué.
5. Sélectionnez l'action que l'utilisateur doit entreprendre, puis cliquez sur **Suivant**.
6. Un code de réponse est généré. Lisez le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L'utilisateur peut saisir le code de réponse, exécuter l'action requise, puis reprendre son travail.

11 Module SafeGuard Configuration Protection

Le module SafeGuard Configuration Protection n'est plus disponible dans SafeGuard Enterprise 6.1. La stratégie correspondante est toujours disponible dans la version 6.1 de SafeGuard Management Center afin de prendre en charge les versions 6.x des clients SafeGuard Enterprise sur lesquels la fonction de Protection de la configuration est installée et administrée avec la version 6.1 de Management Center.

Retrouvez plus d'informations sur SafeGuard Configuration Protection dans le *Manuel Web Helpdesk pour SafeGuard Enterprise 6 :* http://www.sophos.com/fr-fr/medialibrary/PDFs/documentation/sgn_60_m_eng_web_helpdesk.pdf.

12 Journalisation des événements de Web Helpdesk

Les événements Web Helpdesk peuvent être journalisés dans l'Observateur d'événements Windows ou dans la base de données SafeGuard Enterprise. Les événements de toutes les activités du support peuvent être journalisés. Il est ainsi possible de savoir qui s'est connecté à Web Helpdesk, quel utilisateur a demandé un challenge ou quelles actions de récupération ont été requises.

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

Les événements consignés dans la base de données centrale de SafeGuard Enterprise peuvent être consultés à l'aide de l'Observateur d'événements de SafeGuard Management Center.

12.1 Activation de la journalisation des événements de Web Helpdesk

La journalisation pour Web Helpdesk est configurée dans SafeGuard Management Center.

Vous devez disposer des droits appropriés pour créer des stratégies et consulter des événements.

1. Dans SafeGuard Management Center, dans la zone de navigation **Stratégie**, créez une stratégie de type **Journalisation**. Sélectionnez les événements à consigner dans le journal. Enregistrez vos modifications.
2. Créez un nouveau **Groupe de stratégies**. Ajoutez la stratégie de type **Journalisation** à ce groupe. Enregistrez vos modifications.
3. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**. Sélectionnez **Packages du client administré** et cliquez sur **Ajouter un package de configuration**. Sélectionnez le groupe de stratégies à inclure dans le package de configuration. Sélectionnez un emplacement de stockage et cliquez sur **Créer un package de configuration**.
4. Dans SafeGuard Management Center, affectez le groupe de stratégies au domaine contenant le serveur Web Helpdesk. Activez-le. Retrouvez plus d'informations à la section *Attribution de stratégies* du *Manuel d'administration de SafeGuard Enterprise.*
5. Sur le serveur Web Helpdesk, installez le package de configuration créé auparavant. Redémarrez le service.

   La journalisation des événements de Web Helpdesk a été activée.
6. Connectez-vous à Web Helpdesk et lancez une procédure Challenge/Réponse.
7. Dans SafeGuard Management Center, cliquez sur l'onglet **Rapports**. Dans la zone d'action de l'**Observateur des événements**, sur le côté droit, cliquez sur l'icône en forme de loupe pour voir les événements journalisés de Web Helpdesk.

13 Support technique

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

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

14 Mentions légales