[SafeGuard® Easy]

[Protection des données par chiffrement]

Version 4.50.3

Windows® Server 2003
Windows® XP
Windows® 2000

utimaco®
safeware

Utimaco Safeware AG
P.O. Box 20 26
DE-61410 Oberursel, Allemagne
Téléphone : +49 (61 71) 88 0
Fax : +49 (61 71) 88-10 10
info.pds@utimaco.com

Assistance technique

Documentation en ligne

Notre base de données en ligne fournit des réponses à de nombreuses questions courantes sur la gamme de produits SafeGuard, notamment sur leurs fonctionnalités, leur mise en œuvre, l'administration et la résolution des problèmes.

Lien vers la rubrique d'assistance :
http://www.utimaco.com/myutimaco

Pour accéder à l'espace public de la base de connaissances, vous pouvez vous connecter en tant qu'utilisateur invité (Guest). Pour accéder à l'espace réservé de la base de connaissances, vous devez être détenteur d'un contrat de maintenance logicielle en cours de validité.

Notre équipe d'assistance enrichit constamment le contenu des deux espaces en les mettant à jour régulièrement.

Services de support et support téléphonique

Notre équipe peut également fournir une assistance par téléphone aux clients possédant un contrat de maintenance logicielle en cours de validité. Pour recevoir une proposition de contrat adaptée à vos besoins, veuillez contacter votre distributeur Utimaco.

Vous comprendrez certainement que nous avons besoin de plusieurs jours pour traiter certaines demandes de nos clients ne disposant pas d'un contrat de maintenance logicielle en cours de validité. En cas d'urgence, veuillez contacter votre distributeur Utimaco qui vous a vendu vos licences ou votre abonnement logiciel.

Table des matières

1 Aperçu

Les ordinateurs individuels contiennent fréquemment des données spécifiques à des personnes, des informations confidentielles relatives à une entreprise ou d'autres données sensibles.

Le vol d'ordinateurs portables, par exemple, est un risque qu'il ne faut pas sous-estimer. Les informations ultra-confidentielles de clients sur l'ordinateur portable de type Notebook d'un collaborateur du service de distribution pourraient, par exemple, tomber entre les mains d'un concurrent et être dommageables à l'entreprise.

SafeGuard Easy permet de se protéger contre de tels risques sans avoir à investir un temps considérable dans l'implémentation de mesures de sécurité.

Comment SafeGuard Easy protège-t-il les postes de travail contre les interventions non autorisées ? Les fonctions de sécurité principales du programme sont le chiffrement de données et la protection contre les attaques par l'intermédiaire d'un support externe.

Les principaux avantages de SafeGuard Easy sont les suivants :

- Sauvegarde simple mais efficace de la confidentialité des données enregistrées ;
- Implémentation rapide du programme ;
- Très grande convivialité.
- Concept de sécurité approprié pour de nombreux domaines d'application

SafeGuard Easy est simple à installer. Il est pour cette raison particulièrement adapté aux systèmes autonomes et aux appareils mobiles, tels que les ordinateurs portables.

1.1 Fonctions de sécurité centrales

Chiffrement

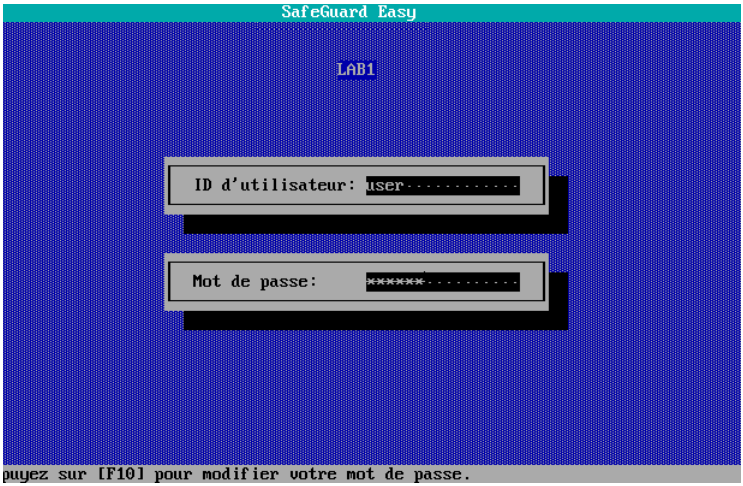
SafeGuard Easy protège de façon simple et efficace la confidentialité des données lors de leur enregistrement sur disque dur, sur disquettes et périphériques amovibles n procédant au chiffrement en ligne. « En ligne », dans ce contexte, signifie que les données sont déchiffrées lors de leur chargement dans la mémoire de travail, puis chifrées à nouveau lors de leur enregistrement. La clé n'est pas enregistrée sur le disque dur ou le PC. Cette caractéristique permet d'échanger des supports de données de façon sécurisée au sein de l'entreprise, tout en protégeant le contenu des supports mobiles de données contre les accès non autorisés. Elle est déterminée à chaque fois à partir du mot de passe SafeGuard Easy de l'utilisateur au moment du démarrage.

SafeGuard Easy chiffre non seulement l'ensemble du contenu du disque dur, mais encore celui des supports amovibles, tels que des disquettes, des disques ZIP ou JAZ, voire des clés USB. En outre, il est possible d'empêcher l'importation non autorisée de données de logiciels non licenciés ou de virus, étant donné que les utilisateurs ne peuvent pas utiliser de supports en texte clair sans droit d'accès adéquat.

Pour le chiffrement, divers algorithmes peuvent être sélectionnés pour les disquettes, les périphériques amovibles et le disque dur. Les algorithmes disponibles sont AES, Rijndael, XOR, STEALTH-40, IDEA, BLOWFISH, DES et 3DES.

Contrôle d'accès avec l'authentification avant amorçage (PBA) et la protection des zones d'amorçage

L'authentification avant amorçage (PBA) est une fonction de sécurité centrale de SafeGuard Easy. La PBA n'autorise que l'ouverture de session par les utilisateurs SafeGuard Easy enregistrés sur le système.



Lors de la tentative de démarrage d'un poste de travail dont le disque dur est chiffré depuis un support extérieur (par ex. disquette système, CD-ROM ou autre disque dur), le disque dur reste inaccessible. Ceci signifie que le démarrage du système est possible, mais que les données chiffrées sur le disque dur ne peuvent pas être lues.

Si la PBA est utilisée sur un poste de travail dont les zones d'amorçage sont protégées, il est impossible de démarrer le poste de travail avec un support externe sans connaître les données d'utilisateur de SafeGuard Easy.

1.2 Autres mécanismes de protection

Prise en charge des technologies Thinkvantage de Lenovo (IBM) - Client Security Solution (CSS) 8.10 et Rescue and Recovery 4.20
SafeGuard Easy prend en charge les versions antérieures des technologies Thinkvantage de Lenovo. Avec la version actuelle de SafeGuard Easy, nous sommes entièrement compatibles avec Client Security Solution (CSS) et Rescue et Recovery (RnR) de Lenovo.

Rescue and Recovery : SafeGuard Easy est compatible avec Rescue and Recovery de Lenovo. Ceci permet aux utilisateurs de bénéficier de cette méthode efficace de sauvegarde et de restauration de Lenovo, même si la partition du système d'exploitation est chiffrée avec SafeGuard Easy. SafeGuard Easy offre ici une fonctionnalité unique en son genre parmi les produits de chiffrement de disques durs. Les sauvegardes de systèmes SafeGuard Easy chiffrés peuvent être stockées sur tous les lecteurs proposés par RnR. En cas d'urgence, il est donc possible de restaurer un système endommagé en chargeant une sauvegarde d'un CD/DVD, d'un lecteur réseau, d'un deuxième disque dur interne, ainsi que d'un disque dur ou d'une clé USB.

TCPA / TPM (puce ESS/CSS) : SafeGuard Easy est le premier logiciel de chiffrement de disques durs à intégrer les composants de sécurité, spécifiées par Trusted Computing Group (TCG), dans les ordinateurs portables modernes. SafeGuard Easy utilise, entre autres, ces composants pour sécuriser la connexion entre le client et le serveur d'administration, ainsi que pour générer des nombres aléatoires. La fonction SafeGuard Easy SAL ou SSO reste disponible et représente donc une intégration optimale dans l'infrastructure de composants ESS.

Certification suivant FIPS 140-2 Level 1
SafeGuard Easy satisfait aux directives de la certification FIPS 140-2 Level 1 (FIPS=Federal Information Processing Standard) du National Institute of Standards and Technology américain (NIST). Le NIST définit les critères de sécurité prescrits par le gouvernement des États-unis d'Amérique pour les produits chiffrés.

SafeGuard Easy est déjà certifié conformément aux Standard Common Criteria, Evaluation Assurance Level 3 (EAL3).

Authentification 2 facteurs en option dans la phase précédant l'amorçage
SafeGuard Easy peut être configuré de manière à ce que seuls les utilisateurs possédant une clé électronique aient accès à l'ordinateur. La clé électronique peut être utilisée non seulement dans l'authentification avant amorçage (PBA), mais également, bien entendu, au niveau des systèmes d'exploitation pour d'autres applications basées sur certificats, via le standard PKCS#11 ou CSP. L'ouverture de session de l'administrateur SGE dans les programmes d'administration peut également avoir lieu via la clé Aladdin. Une procédure Requête/Réponse permet de mettre en place un centre d'assistance pour les utilisateurs qui ont oublié leur mot de passe ou jeton.

SafeGuard Easy prend en charge

- différents eTokens Aladdin
- Jeton USB Verisign
- RSA SecurID 800 Token

Authentification biométrique avec le lecteur d'empreintes digitales de Lenovo
SafeGuard Easy prend en charge l'authentification par jeton USB (RSA, Aladdin), mais aussi par « empreinte digitale » dans le cadre de l'authentification avant amorçage. L'authentification par empreinte digitale offre à l'utilisateur l'avantage de ne plus avoir à se soucier du mot de passe SafeGuard Easy ou de l'identifiant d'un jeton USB. Il peut ainsi procéder à son authentification en insérant simplement un doigt dans le lecteur intégré d'un ordinateur portable Lenovo.

Prise en charge de la veille prolongée (Suspendre sur disque)
Cette fonctionnalité est particulièrement utile pour les utilisateurs de périphériques mobiles qui contournent la procédure de démarrage en mettant leur session sur « pause », puis en la « restaurant », dans la mesure où ces options sont disponibles sur la plupart des systèmes d'exploitation.

Contrairement à la plupart des autres logiciels de chiffrement de disques durs, SafeGuard Easy permet d'utiliser le mode Veille prolongée et même de chiffrer les données d'image générées afin de les sauvegarder de façon sécurisée sur le disque dur. La sécurité reste ainsi garantie à tout moment, la consommation est réduite et les utilisateurs gagnent du temps par rapport à la procédure d'amorçage usuelle.

Compatibilité avec le logiciel Absolute Computrace
Computrace permet de rouvrir une session sur un ordinateur volé sur le réseau et de dévoiler son emplacement. SafeGuard Easy est compatible avec Computrace. Grâce à la compatibilité, ceci fonctionne à présent aussi avec les disques durs chiffrés.

Une compatibilité intégrale nécessite une version du logiciel Computrace qui, actuellement (12/2008) n'a pas encore été mise sur le marché par Absolute Software.

Auto-assistance Web
La fonctionnalité d'auto-assistance Web de SafeGuard Easy permet à l'utilisateur de se dépanner en cas d'oubli du mot de passe SafeGuard Easy. Ceci entraîne une réduction du nombre d'appels au service d'assistance concernant l'oubli du mot de passe. Le personnel du service d'assistance dispose ainsi de plus de temps pour se concentrer sur des cas plus critiques. Il existe diverses solutions pour la procédure Requête/Réponse dans une variante logicielle normale ou chiffrée.

L'auto-assistance est disponible sous forme de programme complémentaire.

Règles de mots de passe
SafeGuard Easy offre différentes options d'implémentation de règles de mot de passe dans le module PBA, telles qu'une liste configurable de mots de passe interdits, des règles étendues pour les caractères spéciaux, des codes utilisateur, etc., ce qui permet de s'adapter facilement aux directives de l'entreprise.

Audit dans la PBA et le système d'exploitation
SafeGuard Easy conserve également une trace des problèmes affectant la sécurité, tels que les échecs de connexion, lors de la phase de préparation du démarrage.

Ces entrées sont ensuite insérées dans le journal des événements de Windows afin d'être évaluées. Une autre solution consiste à ajouter un composant facultatif et à transférer ces entrées vers un serveur local, où elles pourront ensuite être évaluées. Ceci permet de déceler plus rapidement les effractions et de diagnostiquer plus simplement les situations.

Base de données d'administration centrale en option
En supplément de ces fonctions de distribution fiable des fichiers de configuration, SafeGuard Easy inclut un logiciel centralisé d'administration. Ce dernier prend en charge la sauvegarde des noyaux système, la distribution des données de configuration et l'intégration des clients hors connexion.

SafeGuard Easy utilise par défaut les bases de données Microsoft Access et Microsoft SQL Server pour enregistrer des informations sur les clients SGE. La module « Remote Administration » (administration à distance), également disponible, permet en outre une configuration ciblée d'un seul client via le réseau.

Mot de passe utilisateur commun pour SafeGuard Easy et Windows (synchronisation des mots de passe)
Les appels pour oubli du mot de passe sont des événements quotidiens pour les collaborateurs du service d'assistance. La règle d'or est : moins l'utilisateur doit mémoriser de mots de passe, moins le personnel de support sera sollicité. La fonctionnalité de mot de passe de SafeGuard Easy permet de réduire le nombre d'appels utilisateur, dans la mesure où le logiciel peut être configuré pour appliquer le même mot de passe pour Windows et SafeGuard Easy (« synchronisation ») en un simple clic. Une fois la synchronisation effectuée, les utilisateurs ouvrent leur session avec le même mot de passe en mode authentification avant amorçage de SafeGuard Easy et dans le système d'exploitation.

Support Wake On LAN sécurisé
L'authentification avant amorçage de SafeGuard Easy offre une protection optimale contre les attaques des pirates informatiques. Cependant, pour garantir le plus sûrement possible la distribution de logiciels via l'activation à distance quand le chiffrement de disque dur est actif, SafeGuard Easy propose de nouvelles fonctions.

Télé-assistance sûre (Requête/Réponse)
Le personnel d'assistance aide les utilisateurs quand ceux-ci ont oublié leur mot de passe. La procédure Requête/Réponse est sûre et idéale pour les utilisateurs d'ordinateurs portables, car ces derniers ne requièrent pas de connexion en ligne directe avec le service d'assistance.

Requête / Réponse pour PDA
Les utilisateurs SafeGuard Easy ayant oublié leur mot de passe ou leur jeton (clé électronique) redeviennent rapidement opérationnels grâce au service d'assistance centralisé. Les collaborateurs du service d'assistance sont à présent en mesure de réaliser leurs tâches au moyen d'un PDA (Pocket PC) et ne sont plus contraints à la présence d'un ordinateur standard.

Installation avec Windows Installer
L'installation entièrement basée sur le mode Windows Installer (MSI) standard peut être répartie et exécutée de façon simple et effective sur les réseaux Windows.

Gestionnaire d'amorçage intégré (Double amorçage)
Il est fréquemment nécessaire de subdiviser le disque dur d'un ordinateur portable en une partition privée, non protégée et administrée par l'utilisateur et une partition chiffrée et administrée par l'entreprise. A cet effet, SafeGuard Easy fournit à présent un gestionnaire d'amorçage qui permet de réaliser de tels scénarios de façon simple et sûre, administrés de manière centralisée. Les données de l'entreprise restent ainsi protégées et l'utilisateur est entièrement libre d'utiliser sa partition privée, y compris le choix du système d'exploitation.

Chiffrement de périphériques amovibles possible à présent pour les supports USB
SafeGuard Easy étend la palette des périphériques amovibles pris en charge à la génération actuelle des cartes mémoire Plug&Play (supports USB), ceux-ci étant ainsi disponibles pour un échange de données sécurisé. Le chiffrement d'un lecteur de disquettes ou de disques amovibles peut être en outre activé et désactivé séparément pour chaque lecteur.

Gestion souple de l'utilisateur lors de l'authentification avant amorçage
Les possibilités de guidage de l'utilisateur dans la PBA ont été améliorées à différents niveaux. Il est notamment possible d'afficher une remarque relative aux droits d'accès, au propriétaire de l'appareil, etc., prescrits par l'administrateur.

Réutilisation de fichiers de configuration de versions SafeGuard Easy antérieures
(à partir de SafeGuard Easy 3.20)
Les entreprises utilisent les fichiers de configuration SafeGuard Easy lorsque de nombreux clients doivent posséder un fichier de configuration identique. SafeGuard importe les « vieux » fichiers de configuration et reprend ainsi de façon simple les paramètres et la clé en cas de mise à niveau, sans avoir à les saisir de nouveau.

Démarrage d'urgence possible à partir d'une disquette ou d'un CD
Au lieu de lecteurs de disquettes, les systèmes informatiques ont aujourd'hui plutôt des lecteurs de CD/DVD. SafeGuard Easy s'adapte à ces développements dans le domaine du matériel informatique et prend en charge autant les disquettes que les CD et clés USB comme supports de secours. Les supports de démarrage sont pris en charge sous MS DOS et Windows PE.

Connexion Windows standard sans boîte de dialogue SafeGuard
Suite à l'installation de SafeGuard Easy, la boîte de dialogue Windows n s'affiche que lorsque vous vous connectez au système d'exploitation. Cependant, les clients peuvent personnaliser la connexion par défaut et utiliser une boîte de dialogue de connexion de type Utimaco et non plus Windows.

Module d'extension SafeGuard pour le TMS (Token Management System) d'Aladdin
Le système de gestion de jetons d'Aladdin est un outil basé sur Active Directory qui permet d'initialiser les jetons électroniques (eToken). A partir de la version 1.1, le TMS d'Aladdin offre la possibilité d'intégrer des modules d'extension d'autres concepteurs. Utimaco fournit ainsi un module d'extension permettant de charger des données SafeGuard Easy (PBA) et des données d'ouverture de session Windows sur le jeton électronique. La combinaison du TMS d'Aladdin et du module d'extension d'Utimaco permettent de contourner la fonctionnalité d'administration de jetons de SafeGuard Token lors de l'initialisation du jeton électronique, mais les deux programmes peuvent également fonctionner en parallèle. Le module d'extension SafeGuard pour le TMS est une option à commander séparément. Une licence de démonstration pour 10 utilisateurs est livrée avec SafeGuard Easy et est disponible pour le téléchargement.

Changement d'utilisateur « plus rapide » avec jeton
Les utilisateurs qui ont recours à la connexion par jeton de SafeGuard disposent également d'une autre fonctionnalité : s'il est nécessaire de modifier le profil des droits de SafeGuard Easy sur un PC multi-utilisateur (par exemple, pour annuler le droit de chiffrement des supports amovibles), les utilisateurs de jetons doivent simplement se déconnecter de Windows. Il n'est plus nécessaire de redémarrer le PC ou se connecter au module PBA, comme c'était le cas auparavant.

Remarque : Le changement rapide d'utilisateurs SafeGuard Easy ne doit pas être confondu avec la fonctionnalité Microsoft de même nom !

Compatibilité avec le service de copie d'instantané de volume de Windows XP
Le service de cliché instantané des volumes de Windows XP effectue une « sauvegarde immédiate » des fichiers ou des bases de données ouverts. Le personnel peut donc continuer son travail pendant que l'administrateur sauvegarde ses données. SafeGuard Easy prend maintenant complètement en charge le service de copie d'instantané de volume, les configurations manuelles du système n'étant plus nécessaires.

Remarque : En remplacement de la fonction de copie de Windows XP, les utilisateurs peuvent également se servir d'autres outils compatibles SafeGuard Easy, par exemple Rescue and Recovery de Lenovo (disponible également pour les plates-formes non Lenovo).

1.3 Nouveautés de SafeGuard Easy

La version 4.50 de SafeGuard Easy corrige les problèmes apparus dans les versions précédentes. Ces modifications sont consignées dans le fichier `lisezmoi.txt`.

Nouveautés de SafeGuard Easy 4.50

Prise en charge des dernières versions des services de système d'exploitation
Le fonctionnement du client SafeGuard Easy a été testé avec la dernière version des plates-formes prises en charge, notamment Windows XP Service Pack 3 et Windows Server 2003 Service Pack 2.

Prise en charge de dernier matériel et intergiciel des jetons
SafeGuard Easy a été actulaisé de prendre en charge le dernier matériel et le dernienr intergiciel des jetons d'Aladdin (CardOS) et de RSA (SID800).

SafeGuard Easy permet désormais d'intégrer le jeton USB NG Flash d'Aladdin. Le jeton permet d'identifier l'utilisateur pour le service PBA de SafeGuard (Easy Pre-Boot Authentication) et les applications de gestion, de la même façon que les autres jetons d'Aladdin, Verisign et RSA.

SafeGuard Easy 4.50 est toujours compatible avec le format de données SID800 de RSA.

Installation en option de l'audit de SafeGuard Easy
La fonctionnalité SafeGuard Easy Logging (l'audit de SafeGuard Easy) n'est plus installée par défaut pendant l'installation de SafeGuard Easy Client. Il est désormais possible de sélectionner cette fonctionnalité en option dans le programme d'installation de SafeGuard Easy Client sous Utilitaires d'administration.

Diverses améliorations mineures
Plusieurs améliorations mineures ont été apportées, notamment les suivantes :

Le programme d'installation recherche le système d'exploitation et ne poursuit pas l'installation si Windows Vista est le système d'exploitation utilisé. Sous Windows Vista, la solution de sécurité privilégiée consiste à déployer SafeGuard Enterprise.

L'outil RepPBA.exe est désormais fourni sur le CD du produit SafeGuard Easy. Cet outil permet de changer de méthode de connexion dans PBA, par exemple, de passer d'une connexion avec un clavier à une connexion avec une clé cryptographique.

La liste exhaustive des améliorations figure dans le fichier `Lizemoi.txt`.

1.4 Modifications par rapport aux versions antérieures

Réinitialisation du jeton USB
Les jetons USB créés avec les versions SafeGuard Easy **antérieures à la version 4.11** ne peuvent pas être automatiquement réutilisés dans la version actuelle, car le format de données du jeton a changé. Ces « anciens » jetons doivent être réinitialisés pour pouvoir ouvrir comme d'habitude une session dans la PBA.

En règle générale, l'utilisateur se charge lui-même de la réinitialisation (s'il dispose du droit SafeGuard Easy correspondant). Lors de la première ouverture de session avec le jeton dans le nouveau SafeGuard Easy, la PBA affiche alors le message « Pas de données SafeGuard Easy sur le jeton, veuillez initialiser d'abord le jeton ». Les utilisateurs « d'anciens » jetons ne doivent cependant pas s'inquiéter : il leur suffit de saisir les données SafeGuard Easy dans les champs prévus à cet effet. Si les données sont correctes, elles sont écrites sur le jeton et la saisie du code PIN suffit à nouveau pour la prochaine ouverture de session.

Au cas d'oubli des données SafeGuard Easy, l'utilisateur peut contacter un interlocuteur le service d'assistance. Celui-ci écrit les données sur le jeton via le nouveau module d'extension SafeGuard Easy.

Le module d'extension SafeGuard Easy pour la gestion de jetons se trouve sur le CD produit dans le répertoire \TOOLS (SCAdmin_SGEasy.msi).

SGEInteg remplace CheckArea/MigHelp
A partir de la version 4.30, « SGEInteg » désigne la fonction de réparation lors d'une mise à jour du noyau système de SafeGuard Easy. SGEInteg reprend les fonctions de CheckArea/MigHelp. Vous le trouverez dans le répertoire \TOOLS du CD du programme.

1.5 Configuration système requise

Systèmes d'exploitation (minimum)

- Windows 2000 Professional (Service Pack 4)
- Windows XP Édition Familiale
- Windows XP Édition Professionnelle
- Windows 2000 Server (Standard)
- Windows Server 2003 (Standard)

Les Service packs actuels sont conseillés.

SafeGuard Easy n'a pas été testé avec Windows XP Media Edition.

Remarque sur Windows XP
SafeGuard Easy, versions 4.50, peut être utilisé aussi sous Windows XP SP2 ou SP3. Une migration de SP2 vers SP3, par example, est également possible quand SafeGuard Easy est installé.

Remarque sur SP2 de Windows XP/SP1 de Windows 2003 Server
Quand on utilise le serveur d'administration centrale en option ou l'administration à distance de SGE 4.x, des paramètres de configuration particulier doivent être définis sur SP2 de Windows XP/SP1 de Windows 2003 Server.

Vous trouverez une description des paramètres requis dans notre base de connaissance **http://www.utimaco.com/myutimaco** sous la rubrique « 106898 SafeGuard Easy and SP2 Configuration for Windows XP » (106898 SafeGuard Easy et SP2. Configuration pour Windows XP). Dans la zone de recherche (« Search ») de la base de connaissance, tapez « 106898 ».

Nous fournissons une application permettant de définir les paramètres de configuration de façon automatique. Ceci autorise l'administration centralisée et à distance avec Windows XP Service Pack 2. Vous trouverez cette application sur le CD, dans le dossier \Tools\DCOMWizard ou dans notre base de connaissance. Dans ce dernier cas, recherchez les mots clés « SP2 » ou « SGE ».

Remarque sur Windows XP Édition Familiale :
SafeGuard Easy ne prend pas en charge les éléments suivants :

- Ouverture de session automatique sécurisée avec carte à puce (Smartcard-SAL) ;
- Enregistrement central pour clients.

Remarque relative à Windows Server :
SafeGuard Easy ne prend pas en charge :

- SMP
- Serveur 64 bits

Systèmes de fichiers pris en charge

- FAT-12
- FAT-16
- FAT-32
- HPFS
- NTFS
- NTFS5

Supports mémoire pris en charge :

- Disques durs (IDE, SCSI, ATA série, Firewire, USB) ;
- Disquettes ;
- Périphériques amovibles comme ZIP/JAZ ;
- Supports mémoire USB ;
- RAID 0 (RAID 0 matériel).

  SafeGuard Easy ne prend pas en charge :
  - d'autres classes RAID ;
  - RAID 0 (logiciel).

Supports processeurs

- AMD
- Intel
- Multiprocesseurs / Hyperthreading
  SafeGuard Easy 4.x a été testé et installé avec succès à la fois sur les ordinateurs à multiprocesseurs et sur des ordinateurs hyperthreading (par exemple Pentium IV).

Spécifications matérielles

- **Emplacement mémoire sur le disque dur**
  Selon la méthode d'installation choisie, SafeGuard Easy requiert entre 5 et 15 Mo d'espace disque. SafeGuard Easy requiert les mêmes spécifications que le système d'exploitation.

  Bien que SafeGuard Easy fonctionne sans problème sur le système décrit, le chiffrement a son prix. Il est donc recommandé d'utiliser un matériel possédant une configuration supérieure au minimum requis.

- **Nombre de disques durs**
  SafeGuard Easy prend en charge au maximum 4 disques durs avec au plus 8 partitions par disque dur. Un avertissement est affiché quand un type de partition non pris en charge est décelé.

1.6 Documentation

SafeGuard Easy est livré avec le présent manuel et avec l'aide en ligne SGEasy040c.chm.

1.7 Remarques générales

Lors d'une utilisation normale, tenez compte des points suivants :

- La fonction « Changement rapide d'utilisateur » de Windows XP n'est pas prise en charge par SafeGuard Easy. Après l'installation de SafeGuard Easy, l'écran de bienvenue est automatiquement désactivé.
- Quand l'ordinateur est intégré dans un réseau LAN point à point, certaines parties des disques durs ne doivent pas être affectées à d'autres utilisateurs de ce réseau.
- Le chiffrement et le déchiffrement des disques durs sont automatiquement protégés contre les pannes de courant ou autres perturbations. Lors de la remise en service de l'alimentation électrique, l'opération en cours se poursuit au bon endroit sans intervention de l'utilisateur.

REMARQUES :
Le premier chiffrement de disques durs connectables à chaud ne doit pas être interrompu.

- Si vous faites une pause, activez l'écran de veille de Windows (bouton de [verrouillage de la station de travail]). Si vous devez vous absenter pendant une période prolongée, arrêtez le PC.
- Quand la configuration système conseillée est correcte, l'accès logique aux disques durs est impossible après l'amorçage depuis une disquette. Afin de mieux protéger votre système contre les virus de type cheval de Troie qui pourraient être utilisés pour détecter un mot de passe SafeGuard Easy, employez un verrou mécanique ou toute autre mesure interne permettant d'empêcher le démarrage de votre système avec une disquette.

1.8 Remarques relatives à la licence

Toute reproduction non autorisée du manuel et du logiciel SafeGuard Easy fera l'objet de poursuites judiciaires. SafeGuard Easy ne doit être installé que sur un seul ordinateur.

L'utilisation abusive de la copie de sauvegarde pour une installation sur plusieurs ordinateurs est contraire aux dispositions des réglementations régissant les licences et fait l'objet de sanctions pénales. Si vous souhaitez protéger plusieurs ordinateurs, une licence doit être acquise pour chacun d'entre eux.

Les termes et conditions du contrat de licence du logiciel sont applicables.

Autres remarques relatives à la licence
STEALTH Encryption Copyright (c) 1994 Intelligence Quotient International Limited. Tous droits réservés. Brevets en cours d'obtention. STEALTH encryption est une marque commerciale d'Intelligence Quotient International Limited.

Droits brevetés d'Ascom Tech Ltd. en EP, JP, US. IDEA est une marque de Ascom Tech Ltd.

Remerciements
Un merci tout particulier au Dr. Brian Gladman dont nous avons utilisé l'implémentation AES comme base de notre pilote de chiffrement AES.

2 Mise en route

Ce chapitre présente les conditions indispensables à une installation réussie de SafeGuard Easy.

2.1 Préparation de l'installation

Pour une utilisation la plus efficace possible, certaines mesures de prévention doivent être prises avant l'installation.

- Veuillez lire avec attention la liste ci-dessous et vous assurer que vous en avez compris tous les points.
- Avant l'installation de SafeGuard Easy, il est conseillé de réaliser une sauvegarde complète de vos supports de données.
- Tous les disques durs qui doivent être chiffrés doivent être connectés à l'ordinateur et activés à l'installation de SafeGuard Easy.
- Les périphériques amovibles ou les supports mémoire USB ne doivent pas être connectés à l'ordinateur quand SafeGuard Easy est installé.
- Vérifiez les défauts éventuels de votre ou de vos disques durs (CHKDSK).

  Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco **http://www.utimaco.com/myutimaco**.

  Dans la zone de recherche (« Search »), tapez « NTFS » ou « File System ».
- Les logiciels antivirus doivent être désactivés pendant la procédure d'installation/désinstallation.
- Si vous utilisez un gestionnaire d'amorçage, essayez de réinstaller le système sans ce gestionnaire d'impression.

- Si les données ont été transférées sur le disque dur via un outil de clonage (Drive Image, Ghost), nous recommandons une « nouvelle écriture » du MBR.
  Pour installer SafeGuard Easy, vous devez disposer d'un enregistrement d'amorçage principal « sans défaut ». L'utilisation de programmes de type Image/Cloner peut avoir affecté cet enregistrement.

  Nettoyez l'enregistrement d'amorçage principal (MBR) en démarrant l'ordinateur avec une disquette, un CD ou DVD (système identique à celui du disque dur recommandé) et exécutez fdisk /MBR.

- Quand la partition d'amorçage est convertie de FAT en NTFS, alors que le système n'a pas encore été réinitialisé avant l'amorçage, SafeGuard Easy ne doit pas être installé. Il est possible ce faisant que l'installation ne soit pas terminée, étant donné que le système de fichiers est encore de type FAT au moment de l'installation, alors que NTFS a été détecté au moment de l'activation. Dans ce cas, un redémarrage est nécessaire avant d'installer SafeGuard Easy.

SafeGuard Easy est constamment perfectionné. Votre version peut par conséquent comporter des nouveautés n'ayant pas pu être prises en compte avant l'édition finale de ce manuel ou de l'aide en ligne. Ces modifications sont consignées dans le fichier `lisezmoi.txt`.

2.2 Conditions pour l'installation

Pour installer SafeGuard Easy, diverses conditions doivent être remplies sur un poste de travail :

- **Microsoft Windows Software Installer (MSI) v2.0**
  - Présent par défaut dans Windows XP.
  - Avec Windows 2000, uniquement à partir du ServicePack 3.
- **High Encryption package (nécessaire uniquement pour l'administration centrale avec base de données SGE)**
  L'administration centrale via base de données SGE et serveur SGE requiert la prise en charge par Windows du chiffrement avec des clés de 128 bits.
  - Installé par défaut sous Windows XP
  - Installé sous Windows 2000 à partir du Service Pack 2

2.3 Modules pouvant être installés

SafeGuard Easy se compose de différents « modules » qui fonctionnent indépendamment l'un de l'autre.

Les différents modules se présentent sous forme de packages MSI sur le CD du produit, dans le répertoire SGEASY\INSTALL, sous les rubriques CLIENT, SERVER et RUNTIME. Les fichiers requis sont stockés, classés par langue, dans les sous répertoires.

Ces modules sont disponibles :

`SGEasy.msi`	Client Application pour SafeGuard Easy
`Runtime.msi`	Système exécutable
`Server.msi`	Composant SafeGuard Easy Server

SafeGuard Easy, le système d'exécution et SafeGuard Easy Server sont installés en tant que produits distincts. Par conséquent, ils peuvent s'afficher de façon différente dans la liste de logiciels du système.

2.4 Interface utilisateur en plusieurs langues

Si vous lancez l'installation avec « setup.exe », la langue de l'interface utilisateur pendant et après l'installation de SafeGuard Easy correspond à celle qui est définie dans la section Paramètres régionaux du Panneau de configuration. SafeGuard Easy prend en charge l'Anglais, l'Allemand et le Français. Si, par exemple, « Français » est le paramètre actif, l'interface utilisateur s'affiche en Français. Vous disposez également d'une interface en Anglais (États-Unis) et en Allemand.

L'aide en ligne est toujours disponible dans la langue sélectionnée au moment de l'installation. La modification des paramètres régionaux et linguistiques n'influe en rien sur la langue de l'aide en ligne.

Si l'installation est lancée via fichier de « msi », la langue de l'interface utilisateur est toujours l'Anglais. Pour activer d'autres langues (Français ou Allemand), des fichiers « Transforms » doivent être exécutés. Le module Windows Installer utilise les fichiers de transformation pour commuter automatiquement le logiciel d'installation sur la nouvelle langue. Les fichiers de transformation suivants sont actuellement disponibles :

`Sgeasy_g.mst` (pour l'Allemand) et `Sgeasy_f.mst` (pour le Français).

Afin d'obtenir des textes transformés pendant l'installation, exécutez la commande suivante :

`msiexec /I` <MSI package> `TRANSFORMS=`<fichier transform>

Une installation en Français requiert l'exécution de cette ligne de commande :

```
msiexec /I Sgeasy.msi TRANSFORMS=Sgeasy_f.mst
```

Veuillez noter que le paramètre TRANSFORMS doit toujours être écrit en majuscules.

Pour simplifier l'installation, vous pouvez utiliser le fichier `setup.exe`, qui sélectionne automatiquement la langue de l'Assistant d'installation et exécute `SGEasy.msi`. `SGEasy.msi` utilise le fichier `Setup.ini` dans lequel les paramètres suivants peuvent être définis, à condition qu'ils soient présents dans la syntaxe `CmdLine=`{paramètre1, paramètre2,..}.

Ceci est également valable pour l'installation du système exécutable (`Runtime.msi`) et du serveur SafeGuard Easy (`SGEasy.msi`).

3 Installation locale

Dans le cas d'une installation locale, SafeGuard Easy est installé sur un client autonome à partir du CD de produit. Les étapes suivantes expliquent comment on procède à une installation locale.

L'utilisateur qui doit installer SafeGuard Easy doit se connecter avec des **droits d'administration de Windows**, car il doit accéder au disque dur pour installer des pilotes et des services système, qui nécessitent également des droits de niveau administrateur.

3.1 Comment procéder

Comment installer SafeGuard Easy

1. Si vous utilisez un CD de programme, l'installation est automatiquement lancée lorsque vous insérez le CD dans le lecteur CD-ROM (si ce n'est pas le cas, appelez le fichier `Setup.exe` dans le répertoire \Client du CD de programme). Un assistant d'installation vous guide alors dans l'installation. Cliquez sur [Suivant].

2. La boîte de dialogue *Contrat de licence* apparaît. Si vous acceptez les termes du contrat de licence, cochez la case « J'accepte le contrat de licence ». Vous devez accepter les modalités du contrat de licence pour conclure l'installation. Cliquez sur [Suivant].

3. La boîte de dialogue *Dossier destination* s'affiche. Spécifiez le dossier cible requis. Le répertoire d'installation par défaut est \UTIMACO\SafeGuard sur le lecteur d'amorçage. Si un produit SafeGuard existe déjà sur le poste de travail, son répertoire d'installation est automatiquement sélectionné.

   Pour le nom du répertoire, n'utilisez pas de caractères spéciaux !

   Cliquez sur [Suivant].

4. La boîte de dialogue *Sélectionner mode d'installation* apparaît. Vous pouvez y sélectionner les composants que vous souhaitez installer. Cliquez sur [Suivant].

   Chiffrement
   Installe complètement SafeGuard Easy avec tous les composants disponibles.

Options facultatives :

- **SAL (Secure Auto Logon - Connexion automatique sécurisée)**
  Mémorise les données d'accès à Windows lors de la connexion initiale, de façon à ce que seules les données utilisateur de SafeGuard Easy doivent être entrées dans le module PBA (authentification avant le démarrage) pour se connecter (voir 'Ouverture de session unique (Single Sign On) dans le système d'exploitation').

- **Connexion à un serveur**
  Impératif pour la communication chiffrée entre le client et le serveur quand le poste de travail doit être administré de façon centralisée. Il n'est pas nécessaire d'installer l'agent de réseau quand le poste de travail est utilisé de façon autonome (voir 'Administration centrale').

- **Connexion automatique avec carte à puce**
  Transmet automatiquement les données d'accès à Windows à une carte à puce de telle manière que seules les données d'utilisateur SGE sont nécessaires pour l'ouverture de session à l'authentification avant amorçage 'Connexion SAL avec une carte à puce').

- **Mode FIPS**
  Il garantit que SafeGuard Easy est installé conformément aux directives par FIPS 140-2 niveau 1'Certification FIPS 140-2 (Level 1)').

Utilitaires d'administration

Il n'est pas nécessaire que tous les composants des modules soient installés sur le poste de travail d'administrateur qui sert uniquement à administrer les clients protégés par SafeGuard Easy. En règle générale, les outils d'administration suffisent (attention : SafeGuard Easy Administration n'est pas installé avec les utilitaires d'administration).

Font partie des utilitaires d'administration :

- **SafeGuard Easy Logging (l'audit de SafeGaurd Easy)**
  Permet d'auditer les événements du journal liés à la sécurité et générés par des produits SafeGuard installés. Outre la fonction de consignation classique, cette fonctionnalité intègre un mécanisme de filtrage visant à aider l'administrateur à sélectionner les événements pertinents (voir 'Audit').

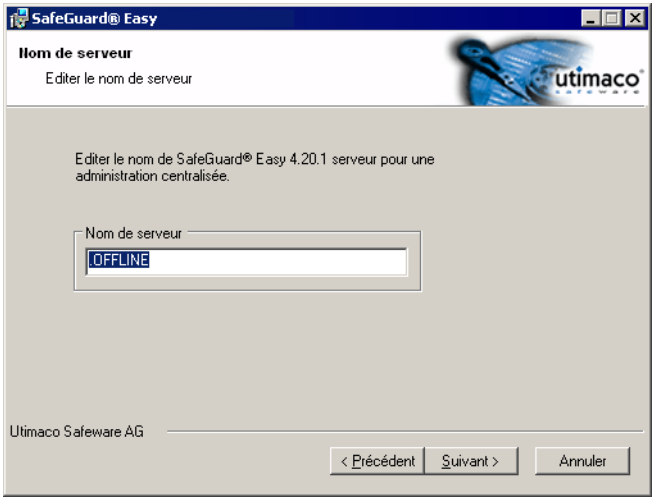
- **Assistant de configuration pour le déploiement**
  Crée des fichiers dont l'exécution modifie la configuration actuelle d'un client, par ex. ajout d'un nouvel utilisateur (voir 'Assistant Fichier de configuration').

- **Assistant de déblocage à distance**
  Sert à permettre certaines actions aux utilisateurs (par ex. définition d'un nouveau mot de passe), même quand l'administrateur n'est pas sur place (voir 'Maintenance à distance (Requête/Réponse)').

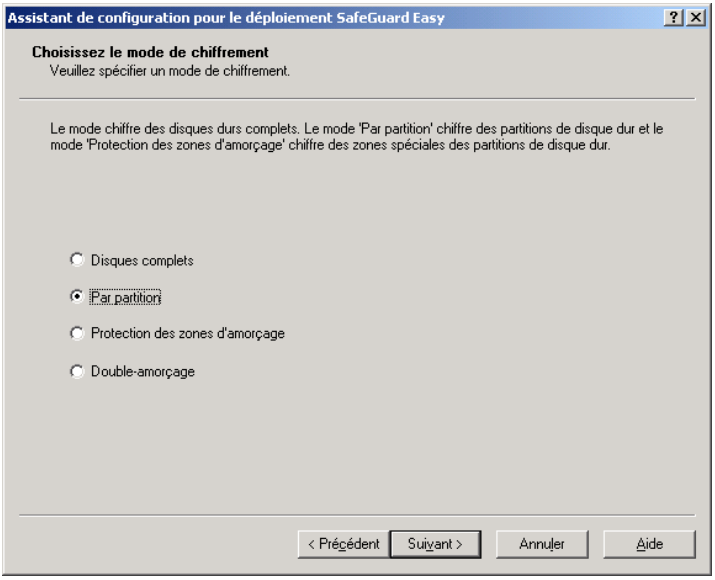
- **Administration Token Support**
  Autorise l'ouverture de session par jeton aux utilitaires d'administration de SafeGuard Easy, administration incluse (voir 'Ouverture de session unique (Single Sign On) dans le système d'exploitation').

Vous trouverez des informations détaillées sur les options d'installation dans les chapitres respectifs.

5. Après avoir cliqué sur « Nom de Serveur », entrez le nom du serveur central de SafeGuard Easy.



6. A l’étape suivante, vous allez définir le mode de chiffrement pour les disques durs de votre ordinateur. Vous trouverez des détails sous ’Mode chiffrement’.



7. A l’étape suivante, nous allons voir les paramètres de configuration spécifiques.

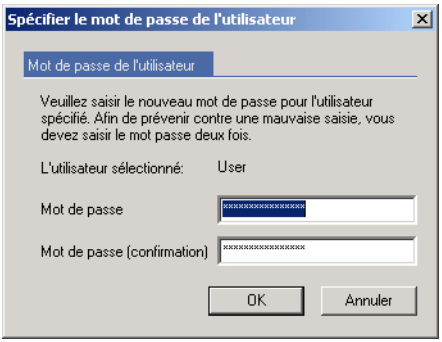
   Vous en trouverez une description détaillée aux chapitres correspondants.

REMARQUES :

L'option Token obligatoire (Général / Type d'Authentification / Mode d'Authentification) indique que SafeGuard Easy impose l'ouverture de session avec jeton pour **tous** les utilisateurs SGE d'un poste de travail.

Des utilisateurs ne peuvent ouvrir de session dans ce mode dans le PBA, que si les données SafeGuard Easy existent déjà sur le jeton. Avec un jeton « vide », vous ne pourrez plus ouvrir de session sur votre ordinateur.

8. L'étape suivante consiste à indiquer les mots de passe correspondant aux profils prédéfinis des utilisateurs de SafeGuard Easy, à savoir le système (SYSTEM) et un utilisateur (user). Ces mots de passe doivent respecter les règles de SafeGuard Easy concernant la composition des mots de passe.



REMARQUES :

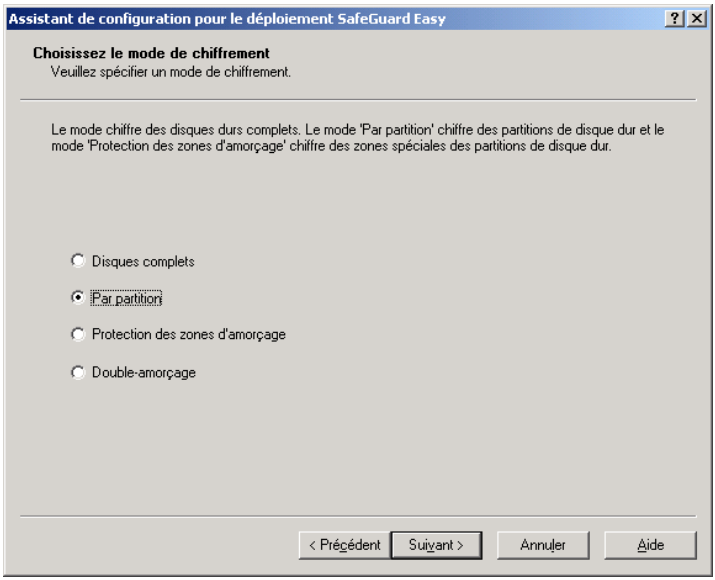
Veuillez retenir les mots de passe que vous saisissez. Lorsque l'option « Password at system start" (Mot de passe au démarrage du système = authentification avant le démarrage) du dossier Général est activée, vous pouvez également vous connecter à votre station de travail avec ce nom d'utilisateur et ce mot de passe !

9. Une boîte de dialogue (Félicitations) signale que l'installation est terminée.

10. Veuillez redémarrer votre ordinateur.

3.1.1 Mode chiffrement

Des indications sur le mode de chiffrement sont toujours requises quand SafeGuard Easy est installé (installation interactive, fichier de configuration avec la propriété « Installer »).



- **Par partition**
  Toutes les partitions sélectionnées sont complètement chiffrées. Choisissez cette option si vos disques durs comprennent plusieurs partitions que vous ne souhaitez cependant pas toutes chiffrer. Vous déciderez plus tard des partitions devant être chiffrées dans les paramètres de chiffrement.

- **Disques complets**
  Tous les disques durs connectés pendant l'installation de SafeGuard Easy sont complètement chiffrés. SafeGuard Easy reconnaît automatiquement le nombre de disques durs de votre ordinateur. Le programme peut être installé sur des systèmes comprenant jusqu'à quatre disques durs physiques et prend en charge jusqu'à huit disques/partitions logiques par disque dur. Si plus de quatre disques durs sont identifiés, SafeGuard Easy interrompt la procédure d'installation. Un disque dur peut compter jusqu'à huit partitions logiques.

- **Protection des zones d'amorçage**
  La protection des zones d'amorçage a pour avantage que quiconque ne possédant pas d'autorisation ne pourra démarrer l'ordinateur à partir d'une disquette système/CD/DVD pour obtenir l'accès au disque dur de cet ordinateur. Une protection efficace des zones d'amorçage n'est assurée que lorsque l'authentification avant amorçage est activée (voir 'Activation du mot de passe au démarrage du système').

  Les partitions non formatées ou inconnues sont complètement chiffrées.
  Avec FAT et FAT32, les zones système sont chiffrées.
  Avec NTFS, le chiffrement est effectué du début de la partition à la fin de la MFT (Master File Table).

- **Double-amorçage**
  Cette option permet de créer une partition chiffrée et une partition non chiffrée. L'une est chiffrée et l'autre est en clair. Les deux partitions doivent être des partitions primaires amorçables. Quand la partition chiffrée est amorcée, un accès à la partition non chiffrée est impossible et réciproquement. Il est ainsi possible de séparer

  Lorsque l'ordinateur est démarré à partir de la partition chiffrée, l'utilisateur doit entrer le mot de passe SafeGuard Easy pour le module PBA. SafeGuard Easy ne permet pas de protéger la partition en clair avec un mot de passe.

  Vous trouverez des informations détaillées sur le double amorçage au chapitre 'Double amorçage/Gestionnaire d'amorçage'.

3.2 Après l'installation

Redémarrer l'ordinateur
Après l'installation (ou la désinstallation) de SafeGuard Easy, l'ordinateur doit être éteint et redémarré. Toutes les applications ouvertes seront alors fermées sans sauvegarder les données. Pour éviter toute perte de données, veuillez fermer toutes les applications en cours.

L'authentification avant l'amorçage apparaît au deuxième redémarrage.
L'authentification avant l'amorçage est encore inactive au premier redémarrage. Les seuls droits disponibles jusque là sont ceux attribués à *AUTOUSER. Dès qu'un utilisateur Windows ouvre une session, l'ordinateur s'éteint et redémarre de nouveau, affiche l'écran d'authentification de SafeGuard Easy dès que la PBA est activée. Un utilisateur SafeGuard Easy peut alors ouvrir une session.

Démarrage du système à partir d'une disquette
Si l'ordinateur est éteint avant la fin du chiffrement du disque dur, il redémarre toujours DIRECTEMENT à partir du disque dur Cela s'applique également au premier redémarrage à la fin du chiffrement.

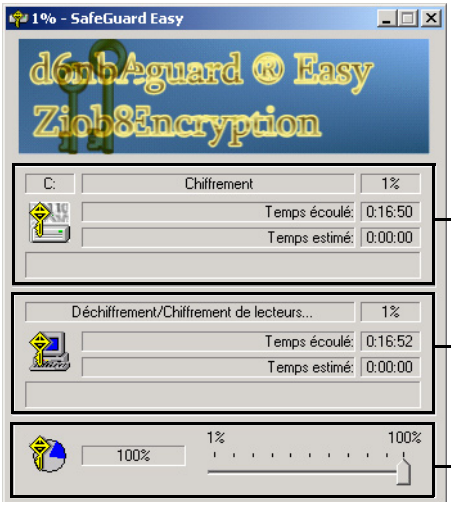
Ne plus modifier les partitions
Après le chiffrement du premier disque dur de votre ordinateur (ou d'une seule partition), vous ne pourrez plus modifier les partitions. Pour changer les partitions, vous devez commencer par désinstaller SafeGuard Easy (= supprimer le chiffrement du premier disque dur), puis créer/supprimer les partitions et réinstaller SafeGuard Easy.

Ne pas interrompre le chiffrement initial des disques durs « connectables à chaud ».
Le terme « connectable à chaud » désigne les périphériques USB qui peuvent être connectés et déconnectés sans devoir redémarrer le système. Il ne faut pas interrompre le chiffrement initial des disques durs connectables à chaud.

Durée du chiffrement initial
L'opération de chiffrement initial avec AES-256 par SafeGuard Easy nécessite environ 10 Go et dure entre 20 et 30 minutes sur un ordinateur portable de dernière génération.

3.3 Boîte de dialogue d'affichage de la progression du chiffrement

Si, pendant l'installation, le chiffrement du disque dur ou d'une partition a été activé, une fenêtre indiquant la progression du chiffrement est affichée.



Progression du chiffrement pour une partition

Progression du chiffrement pour disque dur

Vitesse de chiffrement

Le chiffrement se fait en arrière-plan, ce qui permet à l'utilisateur de poursuivre son travail. Si de très petites partitions ou uniquement des zones du système sont chiffrées, il peut arriver que la boîte de dialogue ne soit pas visible.

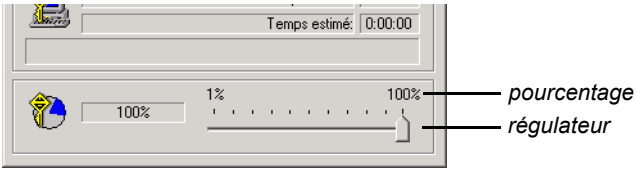
3.3.1 Masquer la boîte de dialogue

SafeGuard Easy permet de masquer l'écran de statut du chiffrement. Pour masquer la boîte de dialogue, entrez une nouvelle clé de registre [DWORD]:

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
ShowECView"=0

3.3.2 Définition de la vitesse de chiffrement

La vitesse à laquelle le chiffrement s'effectue est de 100 % par défaut, mais vous pouvez la modifier avec le régulateur. Plus le pourcentage est élevé, plus le chiffrement est rapide.



Si vous utilisez le régulateur pour réduire la vitesse de chiffrement, SafeGuard Easy n'enregistre pas la vitesse de chiffrement réduite. Une fois la station de travail redémarrée, le chiffrement reprend à sa vitesse optimale (100 %).

Définition d'une vitesse de chiffrement par défaut

Vous pouvez régler la vitesse du processus de chiffrement. Lorsque le système redémarre, la vitesse de chiffrement adopte cette valeur. Pour ce faire, entrez une nouvelle clé de registre [DWORD] :

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
"**DefaultCPUUsage**"=<pourcentage>

Quand la clé est présente, l'opération de chiffrement se poursuit avec la valeur en pourcentage spécifiée au redémarrage. La valeur en pourcentage peut toutefois être augmentée ou réduite au moyen du curseur.

Définition d'une vitesse de chiffrement maximale

La vitesse de chiffrement maximale (100 %) par défaut peut être réduite. Pour ce faire, entrez une nouvelle clé de registre [DWORD] et entrez un pourcentage (par exemple « 75 ») :

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
"MaxCPUUsage"=<pourcentage>

Désactivation du régulateur

Pour que les utilisateurs ne puissent pas modifier la vitesse de chiffrement, il est possible de **désactiver le régulateur** en générant la clé de registre [DWORD] :

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy
« ChangeCPUUsage »

et de lui donner la valeur « 0 ».

Le régulateur est alors affiché en gris.

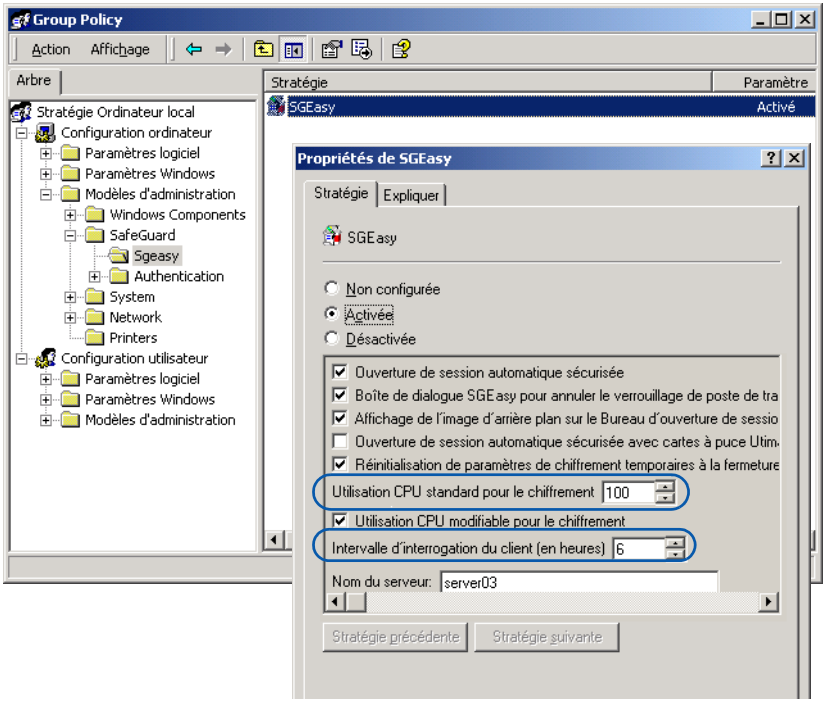
Modification de la vitesse de chiffrement dans le modèle administratif

Les paramètres de l'unité centrale (CPU) peuvent être également activés ou désactivés à l'aide d'une stratégie du modèle d'administration Utimaco (voir aussi Modification des paramètres de registre fréquemment utilisés via le modèle d'administration ('Modification des paramètres de registre fréquemment utilisés via le modèle d'administration').

La stratégie se trouve sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\SGEasy

A la page des propriétés de la stratégie « SGEasy », vous disposez à cet effet des options « Utilisation CPU standard pour chiffrement » et « Utilisation CPU modifiable pour chiffrement ».



3.4 Remplacement de l'image d'arrière plan de l'ouverture de session Windows

Vous avez la possibilité de personnaliser l'image d'arrière plan apparaissant après saisie des données d'utilisateur SafeGuard Easy. Ceci permet au client de personnaliser l'arrière plan de SafeGuard Easy selon les besoins de son entreprise.

L'image affichée par défaut a le nom **SgeLogo.bmp** et se trouve dans le **répertoire SafeGuard Easy** sélectionné.

Pour remplacer l'image de titre, il suffit de remplacer l'image par défaut par une image de même nom et de même taille personnalisée.

Si **AUCUNE image ne doit apparaître en arrière plan**, la clé de registre

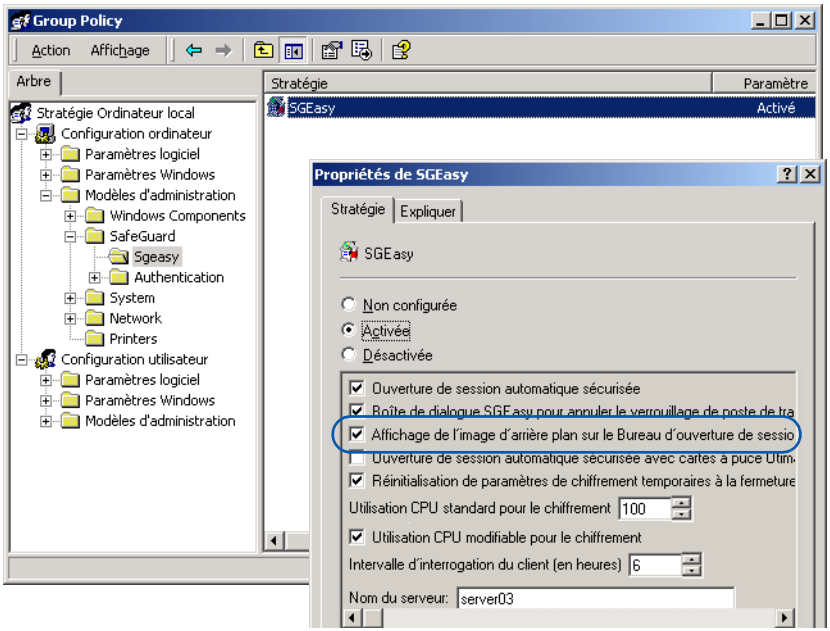
HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
SgeLogoBackGnd
doit avoir la valeur « 0 »

L'image de titre a une grandeur de 640x480 pixels et une profondeur de couleur max. de 8 bits.

L'image d'arrière-plan peut également être désactivée via une stratégie dans le modèle d'administration Utimaco. La stratégie se trouve sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\Sgeasy

A la page des propriétés de « SGEasy », il suffit d'ôter la coche devant « Affichage de l'image d'arrière-plan sur le Bureau d'ouverture de session de Windows ». L'image SafeGuard Easy n'apparaît alors plus.



3.5 Installation de SafeGuard Easy sur des PC dotés de plusieurs systèmes d'exploitation

Pour la protection des données, SafeGuard Easy peut être utilisé sur un ordinateur quand plusieurs systèmes d'exploitation sont installés dans des partitions différentes. Pour vous assurer que les systèmes d'exploitation peuvent être démarrés correctement après l'installation de SafeGuard Easy, vous devez procéder à une installation complète de SafeGuard Easy sur l'un des systèmes d'exploitation. Sur les autres systèmes d'exploitation, installez un « système d'exécution ».

Le système exécutable est démarré à partir du répertoire CD ...\RUNTIME (`Runtime.msi`). Le programme de commutation du chiffrement de disquettes et de périphériques amovibles (SGECRYPT) est également installé par un système exécutable.

Installation de SafeGuard Easy sur des PC dotés de plusieurs systèmes d'exploitation :

1. Définissez p. ex. une installation Windows pour la première installation.

2. Amorcez ensuite successivement toutes les installations Windows non primaires et installez-y respectivement le système exécutable. Pour chaque installation, choisissez un autre répertoire.

3. Pour finir, vous devez amorcer votre installation Windows primaire pour y installer SafeGuard Easy.

4. Une fois le chiffrement achevé, vous pouvez alors continuer à amorcer toutes les installations Windows non primaires.

4 Installation centrale

Les administrateurs peuvent définir la configuration globale des ordinateurs d'utilisateurs avant de distribuer le logiciel.

À cet effet, l'administrateur crée un fichier sur ordinateur qui contient tous les réglages SafeGuard Easy nécessaires aux ordinateurs des utilisateurs. Il s'agit du « fichier de configuration » pour SafeGuard Easy . Ce fichier de configuration permet d'installer SafeGuard Easy sur les ordinateurs des utilisateurs. Toute modification ultérieure de la configuration de SafeGuard Easy passera par la création d'autres fichiers de configuration.

Il est possible d'installer SafeGuard Easy dans un environnement avec ou sans Active Directory.

4.1 Création d'un fichier de configuration

Pour créer un fichier de configuration :

1. L'Assistant est appelé (quand il est installé) via **Programmes / Utimaco / SafeGuard Easy / Assistant de configuration pour le déploiement**.

2. Pour une installation de SafeGuard Easy, il convient de marquer la propriété « Installer » pour le fichier de configuration. Une fois que les paramètres souhaités ont été définis aux différentes pages de l'Assistant, un fichier de configuration est créé.

3. Lors de la création du fichier de configuration, un fichier est créé à l'installation avec par défaut le nom `Install.cfg`.

Le fichier .cfg contient toutes les indications sur la configuration souhaitée sur l'ordinateur de destination. Il est chiffré et contient la clé (disques durs/ disquettes/périphériques amovibles) et les mots de passe des utilisateurs.

Vous trouverez des détails sur l'assistant de configuration pour le déploiement sous 'Assistant Fichier de configuration'.

REMARQUES :
Les fichiers de configuration doivent être protégés contre les accès non autorisés. Les utilisateurs ordinaires ne doivent pas accéder aux fichiers de configuration.

4.2 Installation avec Active Directory

SafeGuard Easy est installé sur les clients dans un environnement Active Directory en ajoutant un programme MSI approprié (`SGEasy.msi`) à la fonction de distribution de logiciel d'un objet Stratégie de groupe).

Pour adapter le fichier MSI, vous devez disposer d'un éditeur permettant de traiter les fichiers MSI (par ex. ORCA ou NetInstall).

> ***REMARQUES :***
> ORCA fait partie du PSDK Microsoft (Platform Software Development Kit). Vous pouvez télécharger le PSDK sur le site Web de Microsoft.

4.2.1 Conditions

- Vous devez vous assurer que ni Windows 2000, ni Windows XP ne sont en service sur les ordinateurs des utilisateurs
- Avant un redémarrage, tous les appareils prévus pour l'installation doivent être déplacés également dans l'unité d'organisation pour laquelle l'OSG configuré est utilisé
- Pour la distribution centralisée du logiciel, les PC clients doivent être reliés au domaine Directory et un compte d'ordinateur doit être défini et actif pour le PC et
- Il doit y avoir suffisamment d'emplacement mémoire sur la partition système.

4.2.2 Personnalisation des packages MSI avec un éditeur

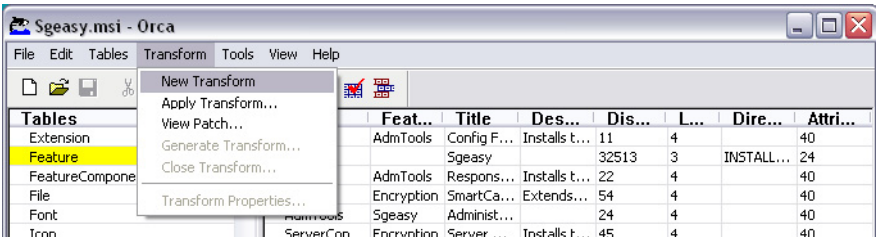
Cette section indique comment créer un « fichier de transformation » (extension .mst) afin de modifier le package MSI « SGEasy.msi ». Utilisez l'outil *Orca* pour ce faire.

Le fichier MST modifie les caractéristiques d'installation du fichier MSI. Le fichier MSI reste cependant inchangé.

> ***IMPORTANT :***
> L'installation de paquets MSI modifiés n'est pas prise en charge. Nous recommandons d'utiliser des fichiers de transformation (MST) pour les modifications.

Procédez comme suit pour créer un fichier de transformation :

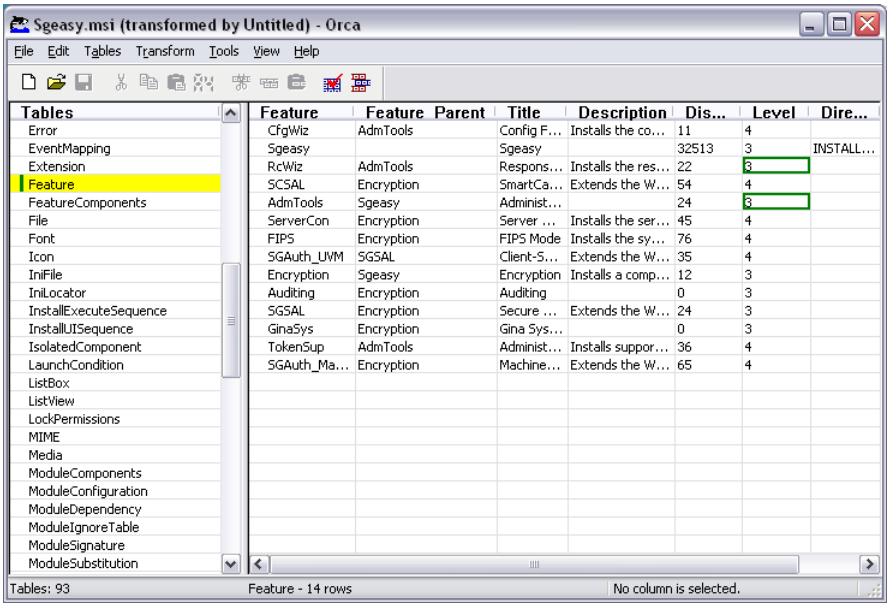
1. Démarrez Orca.msi.
2. Sélectionnez **Fichier** > **Ouvrir** et ouvrez SGEasy.msi.
3. Sélectionnez **Transform** > **New Transform**.



4. Dans **Tables**, sélectionnez l'élément **Features**. Les fonctionnalités correspondent aux composants SafeGuard Easy à installer. Vous trouverez une description des différents composants au point dans 'Composants de SafeGuard Easy'.

La valeur de la colonne « Level » (Niveau) indique si une fonctionnalité est installée ou non :

3 = fonctionnalité installée
4 = fonctionnalité non installée

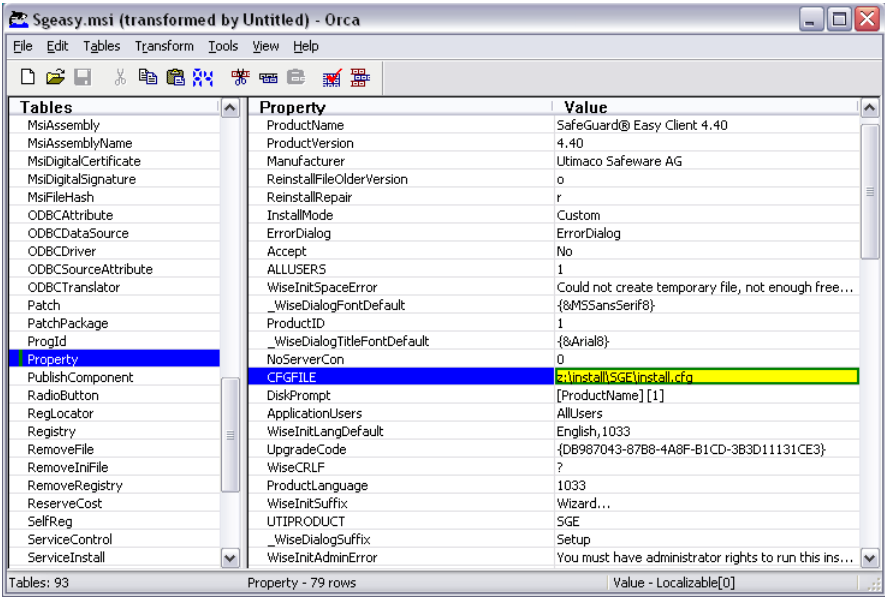


REMARQUES :

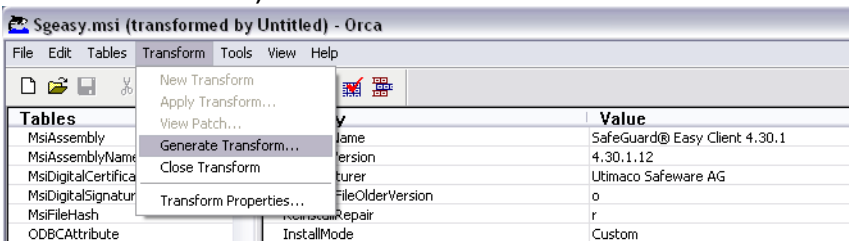
A la sélection d'un composant, tous les composants parents (Feature Parent) doivent également être ajoutés).

5. Dans **Tables**, sélectionnez l'élément **Properties** (Propriétés). Le système affiche toutes les propriétés (=paramètres de configuration de SafeGuard Easy). Vous trouverez une description des différents composants au point dans 'Paramètres SafeGuard Easy'.

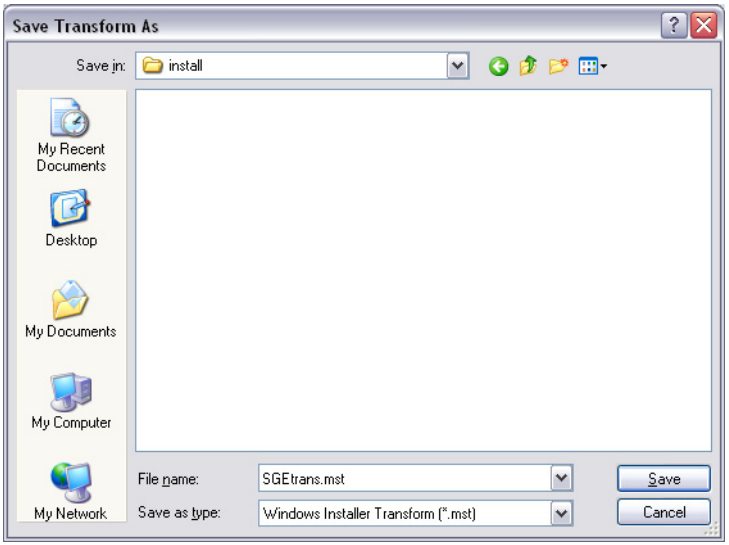
   Par exemple, entrez le nom et l'emplacement de stockage du fichier de configuration dans la section « CFGFILE ».



6. Sélectionnez **Transform** > **Generate Transform (Transformer > Générer transformation).**



7. Enregistrez le fichier de transformation dans le dossier d'installation de la version (par exemple, Z:/SGE/install).



8. Pour distribuer le fichier SGEasy.msi, vous pouvez utiliser le fichier de transformation avec msiexec.exe (voir exemple) ou via une stratégie de groupe adaptée (dans AD).

Exemple de commande d'installation (avec journalisation MSI) :

msiexec /i sgeasy.msi /L*v c:emp\easy.log TRANSFORMS=sgetrans.mst /qn

4.3 Installation sans Active Directory

Pour installer SafeGuard Easy sans environnement Active Directory, vous devez avoir des programmes de répartition de logiciel de tiers.

À cette fin, créez un programme d'installation contenant

- les fichiers programmes de SafeGuard Easy
- un script contenant la ligne de commande pour l'installation préconfigurée.

Distribuez ensuite le programme d'installation aux clients.

4.3.1 Syntaxe de ligne de commande pour Installation préconfigurée

Quand SafeGuard Easy doit être installé avec préconfiguration, utilisez le programme MSIEXEC. MSIEXEC est déjà intégré dans Windows 2000 et dans Windows XP. Ce programme d'installation permet d'exécuter le fichier de configuration créé par l'administrateur. Comme la source et la cible peuvent également être spécifiées, vous avez la possibilité de procéder à une installation unitaire sur plusieurs ordinateurs.

Syntaxe de ligne de commande

`msiexec /i` <chemin+msi nom programme> `/qn ADDLOCAL=ALL |` <fonctionnalités> <SGEasy paramètre+fichier de configuration>

La syntaxe de la ligne de commande comprend :

- **paramètres Windows Installer**, auditant par ex.les avertissements et les messages d'erreur dans un fichier pendant l'installation.
- **Les composants SafeGuard Easy** devant être installés avec un programme SGE (par ex. l'assistant de déblocage à distance).

- **propres paramètres SafeGuard Easy** via lesquels des fichiers de configuration peuvent par ex. être transmis.
- **un fichier de configuration** pour une installation avec la propriété « Installer ».

Exemple :

```
msiexec /i F :\Sgeasy.msi /qn /L* I :\Temp\SGE.log
ADDLOCAL=Sgeasy,Encryption,SGSAL Installdir=C :\SGE
CFGFILE=F :\Install.cfg
```

SafeGuard Easy est installé avec SAL dans le répertoire C :\SGE et le fichier journal SGE.log est créé dans le répertoire I :\Temp (qui doit exister). Les paramètres préconfigurés pour SafeGuard Easy se trouvent dans le fichier `Install.cfg`.

Les différents composants sous sont séparés seulement par une virgule, sans espace supplémentaire. Respectez également la casse (majuscules/minuscules) pour la saisie des différents composants et des paramètres SafeGuard Easy.

Lors de la sélection d'un composant, tous les composants parents doivent également être ajoutés à la ligne de commande !

4.3.2 Options sélectionnées utilisées par Windows Installer

REMARQUES :
Exécutez msiexec.exe à partir de l'invite de commande Windows. Le système affiche ensuite toutes les options disponibles du programme d'installation de Windows.

`/i`
Indique qu'il s'agit d'une installation.

`/qn`
Installation sans intervention de l'utilisateur et affichage d'aucune interface utilisateur.

`ADDLOCAL=`
Liste les composants qui doivent être installés. Si le paramètre n'est pas spécifié, tous les composants prévus pour une installation par défaut sont installés.

`ALL`
permet d'installer tous les composants disponibles.

`REBOOT=Forcerestart | NORESTART`
Impose ou neutralise un redémarrage après l'installation. Sans indication, un redémarrage est imposé (Forcerestart).

`/L*` <chemin + nom de fichier>
Consigne tous les avertissements et tous les messages d'erreur dans le fichier journal spécifié. Le paramètre `/Le <chemin + nom de fichier> ne consigne que les messages d'erreur.`

`Installdir= <répertoire>`
Indique le répertoire dans lequel SafeGuard Easy va être installé. Sans indication, le répertoire d'installation par défaut <SYSTEM> :\PROGRAMMES\UTIMACO est utilisé.

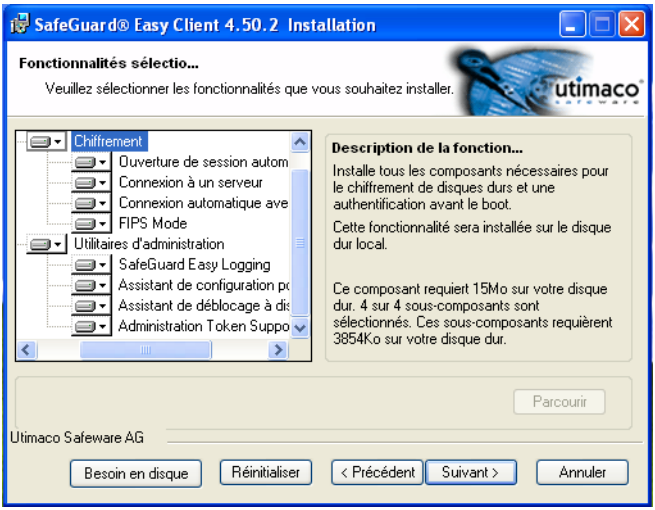
4.4 Composants et paramètres de SafeGuard Easy

Vous devez procéder à un certain nombre de préparatifs avant de procéder à une installation centralisée. Vous devez spécifier les fonctionnalités/paramètres de SafeGuard Easy à installer sur les clients. Pour installer SafeGuard Easy dans un environnement Active Directory, vous pouvez, par exemple, utiliser l'outil ORCA pour modifier le fichier MSI. En l'absence d'Active Directory, les fonctionnalités doivent figurer dans la ligne de commande.

4.4.1 Composants de SafeGuard Easy

Dans les tableaux ci-dessous se trouve une liste de tous les composants pouvant être automatiquement installés via les fichiers .msi. Elles sont identiques aux fonctionnalités qui peuvent être sélectionnées au cours d'une installation interactive.

Dans cet exemple, vous pourrez identifier toutes les fonctionnalités Sgeasy.msi pendant une procédure d'installation interactive personnalisée.



Composants installables avec Sgeasy.msi		
Paramètre	**Composant parent**	**Description**
Sgeasy	---	Installe tous les fichiers requis pour l'application de SafeGuard Easy. Aucune fonctionnalité n'est active au cours d'un redémarrage automatique. Ces fonctionnalités peuvent être activées à tout moment, sans interaction de l'utilisateur (ou manuellement par l'intermédiaire de Panneau de configuration/ Ajout/suppression de programmes).
Encryption	Sgeasy	Installe une version fonctionnelle de SafeGuard Easy (ce qui inclut SafeGuard GINA).
SGSAL	Encryption	Installe SAL (ouverture de session automatique sécurisée).
ServerCon	Encryption	Installe la connexion au serveur (agent de réseau) pour l'administration centrale.
SCSAL	Encryption	Installe SAL avec carte à puce.
FIPS	Encryption	Installe le mode FIPS.

AdmTools	Sgeasy	Installe les utilitaires d'administration (par exemple assistant de configuration pour le déploiement, assistant de déblocage à distance). Aucun composant n'est cependant actif après un redémarrage automatique, mais il est possible de les activer à tout moment sans intervention de l'utilisateur (ou manuellement via Panneau de configuration / Ajout/Suppression de programmes).
Auditing	AdmTools	Installe l'audit de SafeGuard Enterprise.
CfgWiz	AdmTools	Installe l'assistant de configuration pour le déploiement.
RcWiz	AdmTools	Installe l'assistant de déblocage à distance.
TokenSup	AdmTools	Autorise l'ouverture de session avec jeton aux utilitaires d'administration.
SGAuth_UVM	SGSAL	Élargit la procédure d'ouverture de session Windows avec la prise en charge de ThinkVantage « Client-Security-Integration ».
SGAuth_MachineBinding	Encryption	Elargit la procédure d'ouverture de session Windows avec les fonctions d'intégration de machine TPM.

Composants installables avec Runtime.msi		
Paramètre	**Composant parent**	**Description**
RuntimeSys	---	Installe un système exécutable.

Composants installables avec Server.msi		
Paramètre	**Composant parent**	**Description**
Server	---	Installe le serveur SGE, audit inclus.
SgeServer	Server	Installe le serveur SGE.
RemAdmSupport	Server	Installe le support pour l'administration à distance.
AdmConsole	Server	Installe la console d'administration.

4.4.2 Paramètres SafeGuard Easy

REMARQUES :
Tous les paramètres doivent être saisis en majuscules dans la syntaxe de ligne de commande.

`AUTOBACKUP=0|1`

Indique si l'assistant de création d'une disquette de secours pour la sauvegarde du noyau système doit être démarré une fois une installation effectuée avec succès. Dans la configuration de base, il démarre automatiquement (AUTOBACKUP=1).

`CFGFILE=`<fichier de configuration/migration>

Ce paramètre définit le nom complet d'un fichier de configuration SafeGuard Easy pour une installation/migration.

`KERNELDRV=`<nom du lecteur (C,D,…)>

Détermine le lecteur sur lequel le noyau système SafeGuard Easy va être enregistré. Dans la configuration de base, c'est le lecteur d'amorçage de Windows. Désigner un lecteur pour enregistrer le noyau système est par exemple utile quand vous souhaitez restaurer la partition système Windows avec des outils comme par ex. Ghost. La restauration supprimerait sinon le noyau système SafeGuard Easy, étant donné que celui-ci est toujours enregistré par défaut sur la partition système.

Le lecteur cible doit se trouver sur le premier disque dur !

NOACTIVATION=0|1

Avec le réglage NoActivation=1, les fichiers SafeGuard Easy sont copiés sur l'ordinateur sans activer le programme. Cette absence d'activation a les conséquences suivantes : le MBR n'est pas remplacé et le noyau système de SafeGuard Easy n'est pas installé. SafeGuard Easy pourra être activé par la suite via la commande « execcfg » du fichier de configuration (par ex. execcfg /f :C :\SGE\Install.cfg). Par défaut, SafeGuard Easy est activé (NoActivation=0).

PARTCHECK=0|1

Détermine si les types de partition existants prennent en charge les systèmes de fichiers connus (FAT, FAT 32, NTFS, etc.). Si le type de partition est inconnu, l'installation est interrompue. Dans la configuration de base, la vérification est active (PARTCHECK=1).

SERVER=<nom du serveur>

Spécifie le nom du poste de travail sur lequel le serveur SafeGuard Easy est installé. Le paramètre ne peut être utilisé que si le composant « Connexion au serveur » (qui prend en charge l'administration centrale sur un client) est sélectionné.

GROUPS=<nom de groupe1,nom de groupe2, etc.>

Définit les groupes (SafeGuard Easy) auxquels le poste de travail est assigné dans le cadre de l'administration centrale quand il s'enregistre sur le serveur SGE. Le paramètre ne peut être utilisé que si le composant « Connexion au serveur » (qui prend en charge l'administration centrale sur un client) est sélectionné.

`GINASYS=0|1`

Indique si le système SafeGuard GINA pour le contrôle de l'ouverture de session Windows doit être installé. SafeGuard GINA (GINASYS=1).est installé dans la configuration par défaut.

IMPORTANT :

Nous conseillons de toujours utiliser SafeGuard GINA. Le système Utimaco GINA est un composant fonctionnel important de SafeGuard Easy. A l'avenir, le système GINA prendra de plus en plus d'importance pour implémenter de nouvelles fonctionnalités. Quand GINA n'est pas installé, certaines fonctionnalités ne sont pas disponibles après migration vers une nouvelle version. L'absence du composant GINA peut avoir une incidence sur les migrations ultérieures.

Si vous n'installez pas Utimaco GINA, certaines fonctions de Safe Guard Easy ne seront pas disponibles après l'installation :

- la boîte de dialogue de chiffrement/déchiffrement (ECVIEW) n'est pas affichée quand l'utilisateur n'est pas connecté
- l'ouverture de session automatique sécurisée et la connexion automatique avec carte à puce ne fonctionnent pas
- L'ouverture de session Windows n'est pas bloquée quand l'activation à distance sécurisée est active.
- La synchronisation de mot de passe entre Windows et SafeGuard Easy ne fonctionne pas.

5 Mise à jour

Si vous avez déjà installé une version antérieure de SafeGuard Easy sur votre poste de travail, il vous est facile de procéder à un changement de version du système. Les paramètres déjà définis (nom d'utilisateur, mot de passe, etc. sont conservés.)

La migration est possible pour toutes les versions SafeGuard Easy 4.11.0.138.

Une migration est soit démarrée pendant l'installation de la nouvelle version, soit exécutée automatiquement à l'aide d'un fichier de migration préconfiguré. Dans les deux cas, vous utilisez l'assistant de migration.

5.1 Mise à jourlocale

Exécution d'une mise à jour locale :

1. A partir du CD de SafeGuard Easy, accédez au répertoire \CLIENT et lancez l'installation avec `Setup.exe`.

2. SafeGuard Easy détecte qu'une version ancienne est déjà installée sur un poste de travail et l'indique dans une boîte de dialogue.

3. Un programme vérifie le noyau système.

4. Si le noyau système est en ordre, la mise à jour fonctionne sans problème et l'écran de bienvenue apparaît.

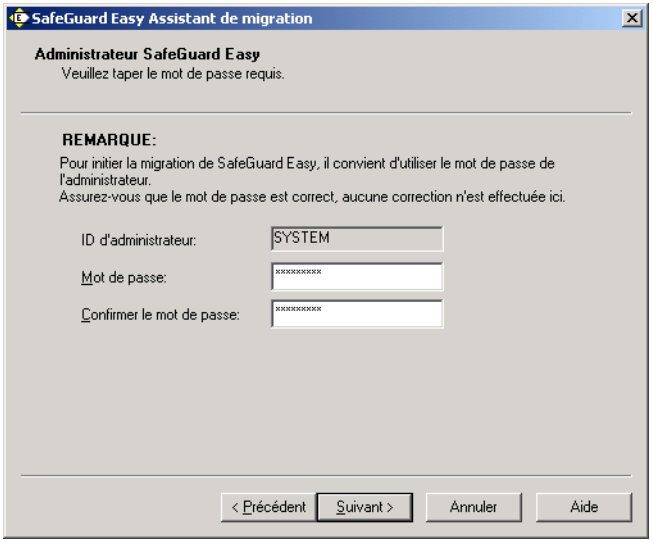
   Si le noyau système est endommagé, il doit être réparé.

5. Dans les étapes suivantes, acceptez la licence d'utilisation, spécifiez le répertoire d'installation de SafeGuard Easy et sélectionnez les composants (SAL, Server Connection, etc.)

6. La mise à jour commence.

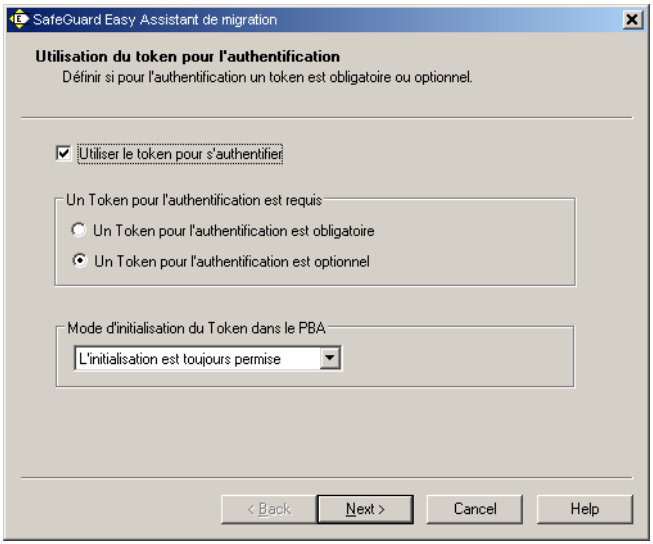
7. La boîte de dialogue « Administrateur SafeGuard Easy » apparaît.

   Seul l'utilisateur SGE « SYSTEM » est autorisé à exécuter une migration sur un poste de travail. Pour l'authentification, il convient de taper ici le mot de passe SGE approprié.



8. L’écran de dialogue « Utilisation du jeton pour l’authentification » apparaît.

Dans les versions antérieures à SafeGuard Easy 4.0, aucun support de jeton n’était proposé. Vous pouvez ici implémenter ultérieurement cette fonction dans le cadre de la mise à jour.



- **Use token for login**
  (Utiliser un jeton pour la connexion) Spécifie si la connexion avec jeton est prise en compte ou non.

  REMARQUE : Si vous voulez activer la connexion par jeton après une mise à niveau, vous devez réinstaller SafeGuard Easy.

- **Utilise le jeton pour s'authentifier**
  Indique si le support de jeton est activé ou non.

  - *Obligatoire :*
    Si le support de jeton n'est pas activé ici, il ne peut pas l'être ultérieurement après une mise à jour. Si vous voulez quand même travailler avec un jeton, SafeGuard Easy doit être réinstallé et le support de jeton activé.

  - *User-dependent :* (Selon l'utilisateur)
    Cette règle offre davantage de souplesse aux utilisateurs, dans la mesure où le droit d'utilisation d'un jeton peut toujours être accordé ou refusé après l'installation de SafeGuard Easy.

- **Mode d'initialisation du jeton dans la PBA**
  Indique qui est autorisé à écrire des données SGE dans un jeton.

  - *L'initialisation est toujours permise :*
    L'utilisateur SGE peut toujours initialiser le jeton.

  - *L'initialisation par code de requête est obligatoire :*
    Le service d'assistance est impliqué dans le processus d'initialisation (procédure Requête/Réponse).

  - *L'initialisation n'est pas permise :*
    L'utilisateur SGE ne doit pas écrire de données dans le jeton, ce dernier est émis de façon centrale par l'administration de jetons.

Veuillez noter les remarques relatives au support du jeton dans le chapitre Prise en charge des jetons.

9. L'écran de dialogue « Répertoire de destination » apparaît.

   Déterminez sur quel chemin le fichier de migration `Sgemig.cfg` doit être enregistré. Le fichier de migration contient le mot de passe SYSTEM et les paramètres de support du jeton.

Le programme reconnaît le répertoire dans lequel la version antérieure de SafeGuard Easy était enregistrée et le propose comme répertoire par défaut. En cliquant sur le bouton [Parcourir], vous pouvez choisir vous-même le répertoire dans lequel le fichier doit être enregistré. La migration est démarrée et le fichier de migration créé en cliquant sur [Suivant].

5.2 Mise à jour préconfigurée avec fichier de migration

Pour une mise à jour automatisée de SafeGuard Easy, il convient de créer tout d'abord un fichier de migration avec l'assistant de migration de la version SafeGuard Easy actuelle. La mise à jour est exécutée automatiquement après la commande.

Création d'un fichier de configuration

Pour créer un fichier de migration :

1. Sur l'ordinateur de l'administrateur, installez au moins l'assistant de configuration pour le déploiement. L'assistant de migration est alors également disponible.

2. Démarrez l'assistant de migration via `WIZLDR.EXE` dans le répertoire SafeGuard Easy.

3. Dans l'assistant de migration, entrez toutes les données requises (voir 'Mise à jourlocale').

4. Le fichier `SGEMig.cfg` est créé dans le répertoire sélectionné.

Ligne de commande (exemple)

```
msiexec /i D :\Sgeasy.msi CFGFILE=D :\SGEmig.cfg /
qn
```

Cas particulier : Administration centrale

Quand un client SGE doit être géré de façon centrale via la console d'administration SGE après la mise à jour, n'oubliez pas d'enregistrer aussi les options correspondantes (ServerCon, SERVER) dans la ligne de commande, par ex. :

```
msiexec /i D :\Sgeasy.msi
ADDLOCAL=Sgeasy,Encryption,ServerCon CFGFILE=D :\SGEmig.cfg
SERVER=Server01 /qn
```

REMARQUES :
La connexion au serveur et le support jeton ne peuvent plus être ultérieurement activés après la mise à jour.

Après la mise à jour

Après la mise à jour, le client redémarre et la migration est achevée.

5.3 Vérification du noyau système à la mise à jour

La mise à jour sera possible si le noyau système SafeGuard Easy est intact. A partir de la version 4.20.1, SafeGuard Easy vérifie le noyau avant chaque mise à jour et avertit l'utilisateur de cette opération par un message dans la fenêtre d'installation (« Votre système de fichiers est en cours d'analyse, veuillez patienter... »).

Si le noyau système est intact, la mise à jour se déroule sans problème.

Si le noyau système n'est pas intact, un message d'erreur s'affiche à l'écran pour indiquer les problèmes possibles et recommander l'exécution d'un programme de réparation (SGEInteg) avant de lancer la mise à jour.

5.3.1 Que se passe-t-il lorsque le noyau système n'est pas intact ?

1. Lancer la mise à jour du système.

2. Le programme de vérification SGEInteg démarre en arrière plan, analyse le noyau système et établit s'il est intact ou non.

3. Un message s'affiche (« SGEInteg : le système de fichiers n'est pas cohérent. La migration de SafeGuard Easy a échoué. Veuillez vous reporter au manuel d'utilisateur de SafeGuard Easy pour exécuter SGEInteg /R).

La procédure d'installation est alors interrompue. Pendant la procédure d'installation automatique, l'erreur « 2006 » s'inscrit dans le fichier journal du programme d'installation de Windows (la journalisation doit être activée).

4. Entrez « SGEInteg /R » dans la ligne de commande. Vous trouvez SGEInteg dans le répertoire \Tools du cédérom d'installation de SafeGuard Easy.

5. SGEInteg répare les fichiers et le système de fichiers en deux étapes : il corrige dans un premier temps toutes les erreurs de fichiers qui n'exigent pas un redémarrage de l'ordinateur. Si des erreurs de fichiers requièrent un redémarrage de l'ordinateur, SGEInteg lance la vérification du disque dur (Chkdsk). Si l'utilisateur accepte le redémarrage de l'ordinateur, Chkdsk sera lancé.

5.3.2 A propos du programme de réparation

Le programme de réparation SGEInteg est lancé automatiquement lors de la mise à jour de la version actuelle de SafeGuard Easy. L'utilisateur/l'administrateur peut également le lancer manuellement (par exemple, en configurant des paramètres supplémentaires dans le répertoire d'outils « Tools » du cédérom d'installation.

Si le paramètre /R a été activé au démarrage, SGEInteg répare le système de fichiers. SGEInteg indique les erreurs réparables et fatales. A la suite de la réparation, il est peut-être nécessaire de lancer ensuite le programme de vérification du disque dur (chkdsk). Généralement, l'ordinateur redémarre normalement.

5.3.3 Paramètres du programme de réparation

Vous pouvez lancer SGEInteg avec les paramètres suivants :

```
SGEINTEG [/?] [/c] [/r] [/p] [/d] [/len] [/v] [/y]
```

/?	Aide Affiche tous les paramètres.
/c	Lance l'analyse du système de fichiers.
/r	Active le mode de réparation. Le programme réparera les erreurs identifiées pour le système de fichiers. L'appel de 'SGEInteg /R' entraîne l'activation du paramètre '/P' et le lancement de l'analyse du système de fichiers. Cela se traduit par un redémarrage.
/p	Corrige le nom de chemin de SafeGuard Easy accessible par HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run Pour les versions antérieures de SafeGuard Easy, les données de chemin sont introduites dans la clé de registre sans guillemets. Avec les versions plus récentes du système Windows, cela empêche l'exécution de ces programmes dans certaines circonstances. Avec ce paramètre, SGEInteg corrige les données du chemin d'accès. Vous devez ensuite redémarrer l'ordinateur. L'appel de 'SGEInteg' sans paramètre entraîne la correction du chemin et une analyse du système de fichiers.

/d	Rétablit l'entrée d'enregistrement CRAREA La création de cette entrée d'enregistrement pendant l'installation était problématique avec les versions antérieures de SafeGuard Easy. Si cette entrée d'enregistrement est absente, cela peut être une source de problèmes au moment de la désinstallation et d'une mise à jour de version. SGEInteg /d rétablit l'entrée sous HKEY_LOCAL_MACHINE SOFTWARE Utimaco SGEasy CRAREA
/len	Rescue and Recovery (RnR) résout le problème Pendant la mise à jour avec la dernière version de SafeGuard, le problème suivant peut apparaître si RnR est installé : Le programme 'SGEDemon.exe' apparaît à chaque redémarrage puis s'interrompt. Étant donné que 'SGEDemon' sert uniquement à afficher un message d'avertissement après la mise à jour, il est possible de désactiver sans craindre d'effets négatifs. SGEInteg /len supprime 'SGEDemon.exe' dans HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run
/v	Active le mode prolixe Des messages d'état et d'erreur détaillés s'afficheront à l'écran si vous avez activé ce mode.

/y	Active le mode sans surveillance. Tous les messages sont automatiquement validés par OUI.

/V	Active le mode prolixe Des messages d'état et d'erreur détaillés s'afficheront à l'écran si vous avez activé ce mode.
/R	Active le mode de réparation. Dans ce mode, le système répare les erreurs du système de fichiers. Si 'SGEInteg /R' est exécuté, la commande de détails du chemin (paramètre /P) et une analyse du système de fichiers sont exécutés, sans intervention de l'utilisateur, en arrière-plan. Le système peut avoir à être redémarré.
/Y	Active le mode sans surveillance. Tous les messages sont automatiquement validés par OUI.

/P	Corrige le nom de chemin de SafeGuard Easy accessible par HKEY_LOCAL_MACHINE SOFTWARE Microsoft Windows CurrentVersion Run Pour les versions antérieures de SafeGuard Easy, les données de chemin sont introduites dans la clé de registre sans guillemets. Dans les nouvelles versions de Windows, sous certaines circonstances, ceci peut empêcher l'exécution de ces programmes. Lorsque ce paramètre est utilisé, SGEInteg corrige les détails du chemin. Vous devez ensuite redémarrer l'ordinateur. L'appel de 'SGEInteg' sans paramètre entraîne la correction du chemin et une analyse du système de fichiers.

6 Désinstallation

Une désinstallation de SafeGuard Easy a les conséquences suivantes :

- toutes les zones jusqu'à présent chiffrées du ou des disques durs sont déchiffrées,
- l'authentification avant amorçage (PBA) – si elle est installée – est supprimée,
- l'ouverture de session Windows initiale est restaurée si la fonction SAL/Smartcard-SAL était installée,
- tous les fichiers SafeGuard Easy sont effacés,
- toutes les entrées dans la base de registres de SafeGuard Easy sont supprimées.

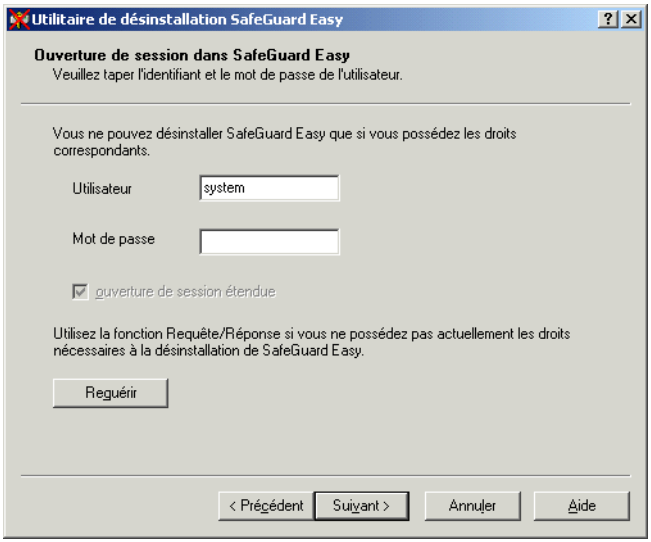
Dans la configuration de base, SafeGuard Easy ne peut être désinstallé que par l'utilisateur SYSTEM. En règle générale toutefois, chaque utilisateur SGE possédant un droit de désinstallation peut supprimer le programme d'un poste de travail.

N'essayez pas de supprimer SafeGuard Easy en effaçant les fichiers. Si SGE n'est pas correctement désinstallé, des entrées demeureront dans la base de registres. Ceci pourrait éventuellement empêcher une nouvelle installation de SafeGuard Easy. Dans ce cas, le système d'exploitation de l'ordinateur devra être réinstallé.

6.1 Désinstallation locale

Sélectionnez successivement Démarrer / Paramètres / Panneau de configuration / Ajout/Suppression de programmes, et enfin « SafeGuard Easy » (ou également des composants SGE, tels que Server ou Runtime).

Via [Supprimer] et en cliquant sur [Suivant] dans l'écran de bienvenue, vous entrez dans la boîte de dialogue Ouverture de session SafeGuard Easy.



Tout utilisateur qui souhaite désinstaller le programme, doit entrer son nom d'utilisateur et son mot de passe SafeGuard Easy. L'utilisateur doit posséder la bonne clé Nouveautés de SafeGuard Easy. Après avoir entré les données utilisateur correctes, cliquez sur [Suivant], ce qui confirmez la vérification de sécurité. Entraîne la désinstallation de SafeGuard Easy de façon automatique.

6.2 Désinstallation avec Requête/ Réponse

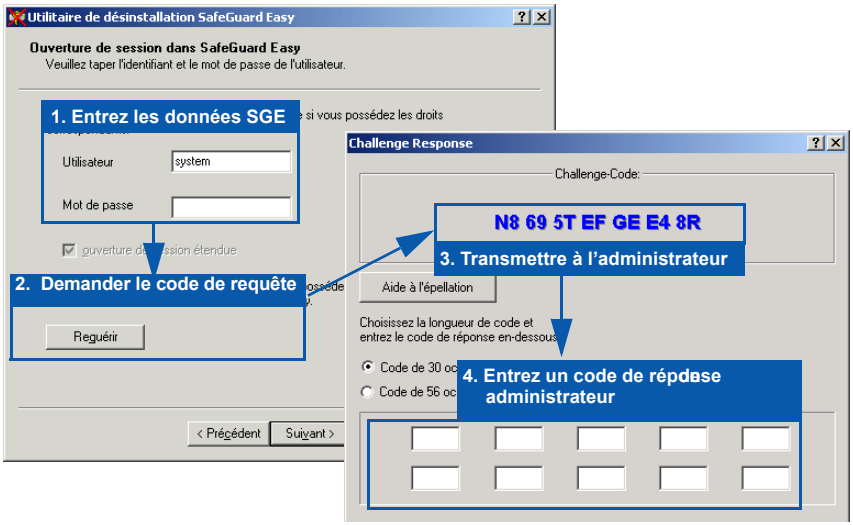
Si un utilisateur SGE n'est pas autorisé, en raison de son profil, à désinstaller SafeGuard Easy, l'administrateur peut lui octroyer ce droit à l'aide de la procédure Requête/Réponse. Dans ce but, l'utilisateur et l'administrateur échangent un code de requête et de réponse.

L'utilisateur qui génère le code de réponse (administrateur) doit connaître, sur l'ordinateur de l'utilisateur, un profil disposant d'un droit de désinstallation. Ce profil utilisateur doit en outre toujours avoir *au moins les mêmes droits* que le demandeur sur l'ordinateur de l'utilisateur.

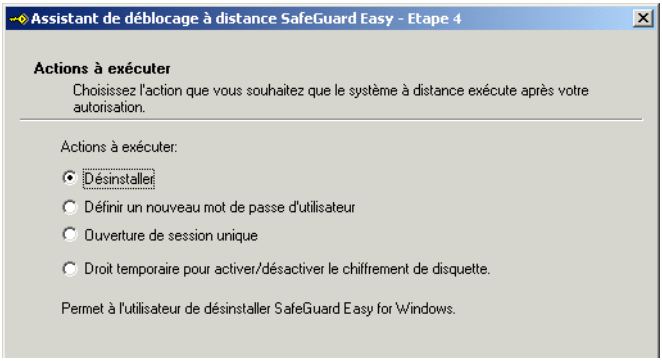
Comment procéder

1. L'utilisateur lance une désinstallation locale (voir 'Désinstallation locale') et entre dans la boîte de dialogue *Ouverture de session dans SafeGuard Easy*.

2. Il tape ses données *SGE*, demande le code de requête et le transmet par téléphone, SMS ou courrier électronique à l'administrateur.



3. L’assistant de déblocage à distance permet à l’administrateur de générer un code de réponse avec les données d’accès SGE de l’utilisateur (dans notre exemple, l’utilisateur « emiller »). Le droit de désinstallation est fourni avec le code de réponse.



4. Après échange des codes de requête et de réponse, SafeGuard Easy est désinstallé.

6.3 Désinstallation automatique avec fichier de configuration

La désinstallation de SafeGuard Easy est automatisée quand un `fichier de configuration` avec attribut « Désinstaller » est appelé avec la commande msiexec.

Syntaxe de ligne de commande

```
msiexec /x D :\SGEasy\Sgeasy.msi CFGFILE=D :\Deinstall.cfg /qn
```

7 Démarrage du système et ouverture de session

SafeGuard Easy remplace le mécanisme d'authentification propre à Windows par une ouverture de session avant le processus d'amorçage, appelée **authentification avant amorçage (PBA)**. L'ouverture de session PBA est la méthode par défaut utilisée après l'installation.

Quand l'authentification avant amorçage est activée, une ouverture de session n'est possible qu'avec les données d'accès SafeGuard Easy. A partir du mot de passe saisi, la clé de déchiffrement d'un disque dur chiffré, requise pour l'amorçage, est calculée.

Quand l'authentification avant amorçage est désactivée, le disque dur reste chiffré. L'ordinateur démarre mais sans interaction de l'utilisateur jusqu'à l'écran de bienvenue de Windows. Dans ce cas, les données de démarrage (SafeGuard Easy) sont stockées dans le disque dur sous forme de fichiers cachés. Sans authentification avant amorçage, le niveau est de sécurité d'un système est plus faible.

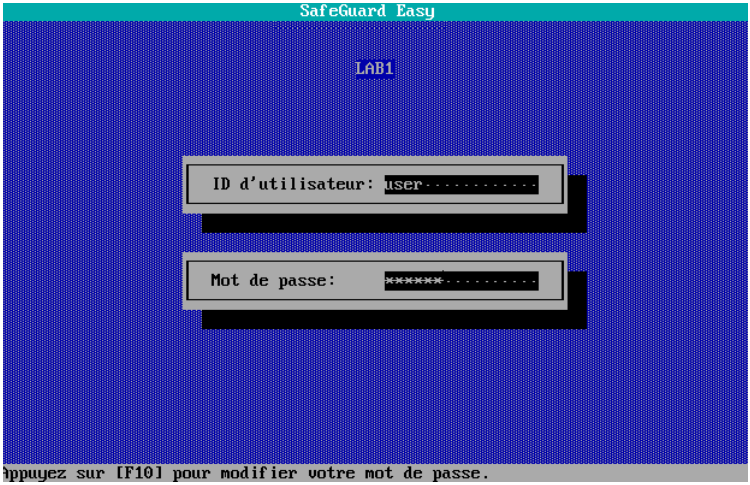
Selon la méthode d'authentification définie par défaut, l'ouverture de session dans la PBA se fait

- comme utilisateur ordinaire (avec nom d'utilisateur et mot de passe)
- comme utilisateur par défaut (avec mot de passe uniquement)
- avec une clé électronique (avec mot de passe de jeton)

Indépendamment de la méthode d'authentification, l'écran d'ouverture de session PBA a des caractéristiques et fonctions identiques

- Nom du poste de travail et mentions légales
- Fonction d'aide pour modifier le mot de passe SGE/Token
- Fonction d'aide pour réinitialiser des mots de passe oubliés

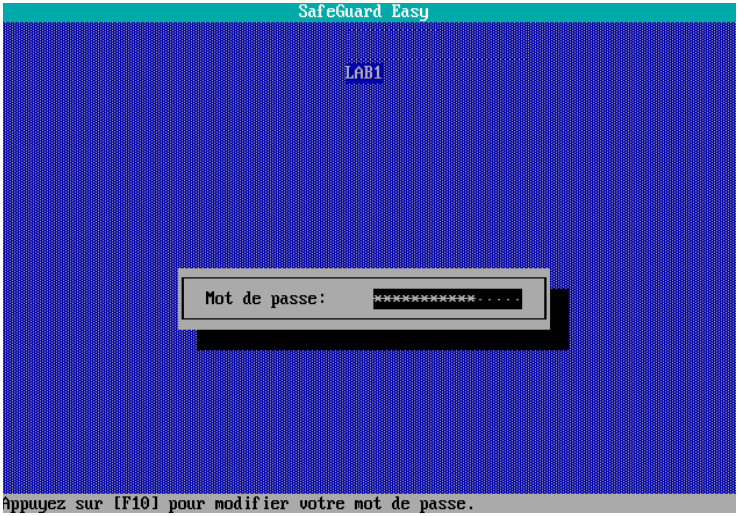
7.1 Ouverture de session comme utilisateur régulier



Normalement, l'utilisateur ouvre une session PBA avec son nom d'utilisateur et son mot de passe SafeGuard Easy.

Sous le nom du programme est affiché le nom du poste de travail (par ex « AST-VM-GER »). Ces données sont reprises des paramètres du système de votre poste de travail.

7.2 Ouverture de session comme utilisateur par défaut



Si, sur un poste de travail, un utilisateur au choix est défini comme « Utilisateur par défaut », seul le mot de passe SGE est toujours demandé. La saisie du nom d'utilisateur est inutile.

7.2.1 Ouverture de session étendue via [F2]

Si une personne autre que l'utilisateur par défaut doit se connecter, la fonctionnalité de *connexion étendue* doit être activée. Ceci a pour conséquence, qu'en supplément du mot de passe SafeGuard Easy ils doivent également entrer leur mot de passe utilisateur.

Au-dessus de la ligne de saisie du mot de passe, vous voyez apparaître le champ de saisie du nom d'utilisateur quand vous appuyez sur [F2].

IMPORTANT :
L'utilisateur SYSTEM doit **toujours** ouvrir une session avec le nom d'utilisateur et le mot de passe.

7.3 Ouverture de session avec jeton

SafeGuard Easy vous donne la possibilité d'ouvrir une session PBA avec un jeton électronique. Ceci est une méthode rapide et confortable pour ouvrir une session sur un ordinateur sécurisé.

Si un jeton USB est connecté, la boîte de dialogue PBA comporte un champ de saisie pour le mot de passe de ce jeton. Après confirmation de la saisie, le système vérifie si l'utilisateur SGE enregistré sur le jeton existe sur l'ordinateur. En cas de concordance des données, l'ouverture de session a lieu.

7.4 Modifier le mot de passe SafeGuard Easy avec la touche [F10]

Les utilisateurs peuvent modifier eux-mêmes le mot de passe SafeGuard Easy avec la touche [F10]. L'utilisateur entre d'abord dans ce cas ses données SGE actuelles et les confirme avec [F10]. Il est ensuite invité à entrer un nouveau mot de passe.

L'administrateur SGE peut toutefois prescrire également la définition d'un nouveau mot de passe après écoulement d'un certain laps de temps.

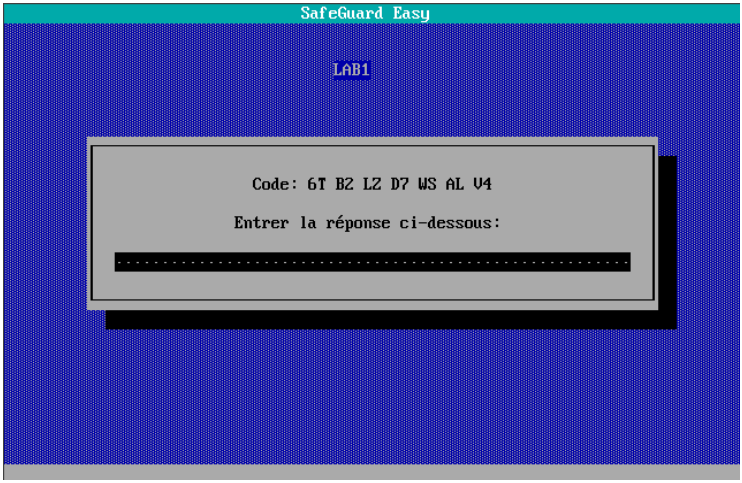
En cas d'ouverture de session avec jeton, [F10] sert à modifier le mot de passe du jeton et non pas les données SGE qu'il contient.

7.5 Fonction d'aide pour réinitialiser les mots de passe oubliés avec la touche [F9]

SafeGuard Easy offre un mécanisme Requête/Réponse pour réinitialiser les mots de passe « oubliés ». Si l'utilisateur a besoin d'aide, il doit générer un code de requête dans la PBA en appuyant sur la touche [F9].

Ce code de requête est affiché sur l'écran de l'utilisateur sous forme de chaîne de caractères ASCII (14 caractères). L'utilisateur appelle ensuite son administrateur et lui fournit ses informations personnelles et le code de requête. L'administrateur génère alors un code de réponse. Après saisie de ce code de réponse sur l'ordinateur de l'utilisateur, celui-ci peut redéfinir son mot de passe.

Pour plus de détails sur la procédure Requête/Réponse, veuillez consulter le chapitre 'Maintenance à distance (Requête/Réponse)'.



7.6 Échec d'ouverture de session

L'ouverture de session PBA peut échouer quand

- le nom d'utilisateur SafeGuard Easy a été incorrectement entré,
- le mot de passe est incorrect,
- le nom d'utilisateur n'est plus valable.

Quand un utilisateur a entré incorrectement ses données, il doit patienter quelques secondes avant de pouvoir de nouveau ouvrir une session. Pour des raisons de sécurité, le temps d'attente augmente exponentiellement à partir de la seconde tentative. Une seule ouverture de session correcte réinitialise le temps d'attente.

Réinitialiser une ouverture de session ayant échoué

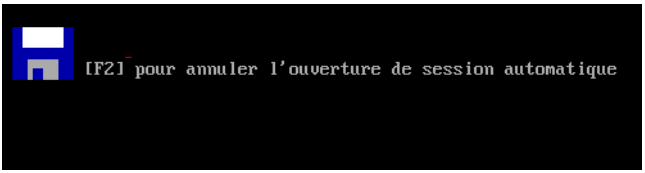
Vous pouvez réinitialiser de la manière suivante une ouverture de session ayant échoué :

1. Insérez la disquette de secours dans le lecteur et amorcez le système depuis le lecteur A :
2. Appelez le programme `Sgeasy.exe`.
3. Un menu avec les options Désinstaller, Restaurer et Réparer apparaît.
4. Quittez le menu en cliquant sur « Annuler » (Options de désinstallation, Réparer, Restaurer).
5. Redémarrez le système.

Ceci réinitialise la période d'attente.

7.7 Imposer l'ouverture de session PBA avec la touche [F2]

Lorsque PBA est désactivé, vous pouvez attendre qu'une icône de disquette s'affiche dans le coin supérieur gauche de l'écran, puis appuyer sur [F2] pour activer PBA et vous connecter de la façon habituelle.

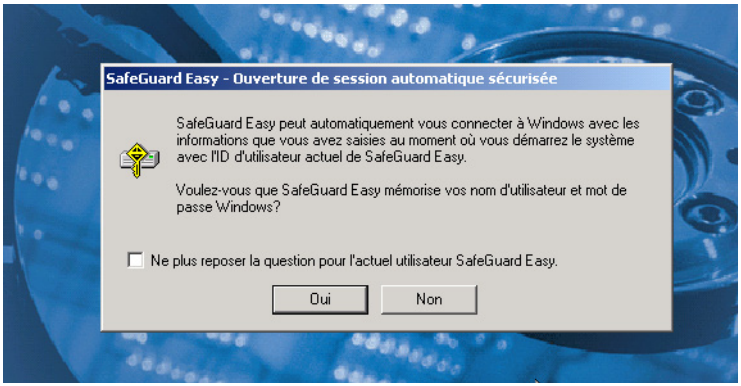


7.8 Ouverture de session automatique dans le système d'exploitation

SafeGuard Easy peut en option exécuter une ouverture de session automatique dans Windows. Dans SafeGuard Easy, cette fonction est appelée *Ouverture de session automatique sécurisée* (en abrégé SAL). Après la saisie des données Windows, la SAL les place dans une plage sécurisée et y revient après chaque ouverture de session avec succès par l'utilisateur dans la PBA.

La seule condition est que la PBA soit activée.

La SAL apparaît après l'ouverture de session dans le système d'exploitation.



Si vous répondez par oui à la question relative à l'ouverture de session automatique, vous aurez à l'avenir uniquement besoin des données SafeGuard Easy pour ouvrir la session.

La SAL peut être également utilisée en liaison avec des cartes à puce.

Pour plus de détails sur l'administration à distance, lire le chapitre 'Configuration du mot de passe Windows'.

7.9 Compatibilité avec composants d'ouverture de session d'autres concepteurs

Pour toujours garantir la sécurité, les composants de Utimaco sont toujours appelés en premier par le système d'exploitation.
Une modification de cette séquence d'appel (p.ex. à la suite de l'installation de logiciel d'ouverture de session extérieur) est automatiquement annulée. En cas de réamorçage, si ceci vous empêche d'ouvrir une nouvelle session dans Windows ou si Windows n'est pas correctement disponible après l'ouverture de session, Utimaco offre à l'administrateur deux possibilités pour annuler cette modification :

- Pour définir manuellement le composant de connexion qui doit être appelé par le composant de connexion Utimaco, maintenez enfoncée la touche [F8] lorsque le système passe de l'écran bleu au bureau (vide au départ).
- Si vous n'appuyez pas sur [F8], une boîte de dialogue s'affiche. Cette boîte de dialogue permet à l'utilisateur de décider si les composants d'ouverture de session Microsoft d'origine ou ceux d'un tiers sont adressés après appel des composants d'ouverture de session Utimaco. Cette demande est affichée jusqu'à ce que l'utilisateur décide également de désactiver la demande. Dans ce cas, la dernière sélection effectuée reste valide. L'utilisation de composants Microsoft d'origine garantit un fonctionnement correct de l'ouverture de session, mais désactive le cas échéant certaines fonctions du produit tiers supplémentaire. Le manque d'homogénéité rend parfois difficile l'exécution concomitante de plusieurs composants d'ouverture de session Windows.

Pour des restaurations importantes, il est possible de contourner cette interaction utilisateur. Pour ce faire, l'administrateur doit s'assurer que, avant le redémarrage suivant l'installation du nouveau composant de connexion, la valeur de registre « ForceKnownGina » de la clé « HKLM\Software\Utimaco\SGLogon » passe de 0 à 1 (le nouveau composant de connexion sera appelé par les extensions de connexion de SafeGuard). Par le réglage de cette valeur sur 2, les composants d'ouverture de session d'origine continueront à être appelés par Utimaco.

8 Aperçu de l'administration

SafeGuard Easy peut être configuré par le biais du programme de configuration (Assistant de configuration pour le déploiement) ou via l'utilitaire d'administration SafeGuard Easy. L'administration permet d'intervenir directement sur la configuration SGE de l'ordinateur.
Elle sert à l'administration locale sur un ordinateur unique. L'assistant de configuration pour le déploiement ne change rien aux paramètres locaux, mais il réunit les paramètres SafeGuard Easy dans un fichier, distribué ensuite aux clients.

Les programmes d'administration présentent peu de différence en matière d'options de réglage. Dans les deux programmes, il est prescrit de s'authentifier avec des données SafeGuard Easy correctes pour pouvoir procéder à des modifications.

Lequel des deux programmes doit être utilisé dépend du contexte. Vous trouverez plus de détails ci-après.

8.1 Distinction des fonctions

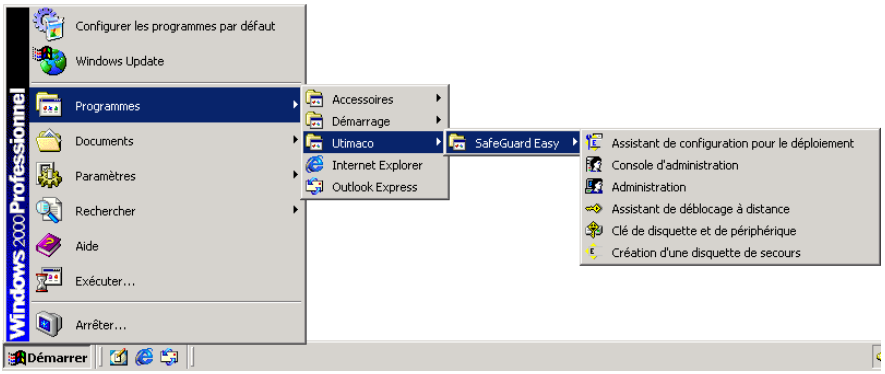
Vous devez d'abord déterminer si la fonction de l'administrateur du système doit être combinée avec celle du « simple » utilisateur, ou si elle doit s'en distinguer. Quand les fonctions sont séparées, il est possible d'intégrer un ou plusieurs assistants d'administration supplémentaires.

- **Fonction combinée :** l'utilisateur est lui-même l'administrateur du système. Il configure SafeGuard Easy sur son ordinateur, pour son usage personnel (une personne). Tous les paramètres sont définis dans l'administration. Le programme de configuration n'est pas requis. Il n'est pas non plus nécessaire de créer un fichier de configuration.

- **Fonctions distinctes sur un PC :** l'administrateur du système configure SafeGuard Easy sur le PC de l'utilisateur. Si l'administrateur système crée un compte « administrateur » en supplément du compte « utilisateur », trois personnes ont accès au système. La configuration se fait à l'aide de la fonctionnalité d'administration. Le programme de configuration n'est pas requis, étant donné qu'aucun fichier de configuration ne doit être créé.

- **Fonctions distinctes sur plusieurs PC :** l'administrateur du système configure SafeGuard Easy sur son ordinateur pour plusieurs postes de travail. Un assistant d'administration peut être intégré pour d'autres tâches d'administration. Pour ce travail, utilisez l'assistant de configuration pour le déploiement. Vous créez ainsi un fichier dans lequel les définitions sont sauvegardées. Le fichier de configuration est transmis aux utilisateurs via une installation préconfigurée. Si, sur l'ordinateur de l'administrateur du système, vous souhaitez utiliser d'autres paramètres, servez-vous également de l'utilitaire d'administration.

8.2 Démarrage de l'utilitaire d'administration et de l'assistant de configuration pour le déploiement



Après une installation complète, SafeGuard Easy crée un dossier de même nom sous Programmes / Utimaco. L'utilitaire Administration et l'assistant de configuration pour le déploiement peuvent y être démarrés.

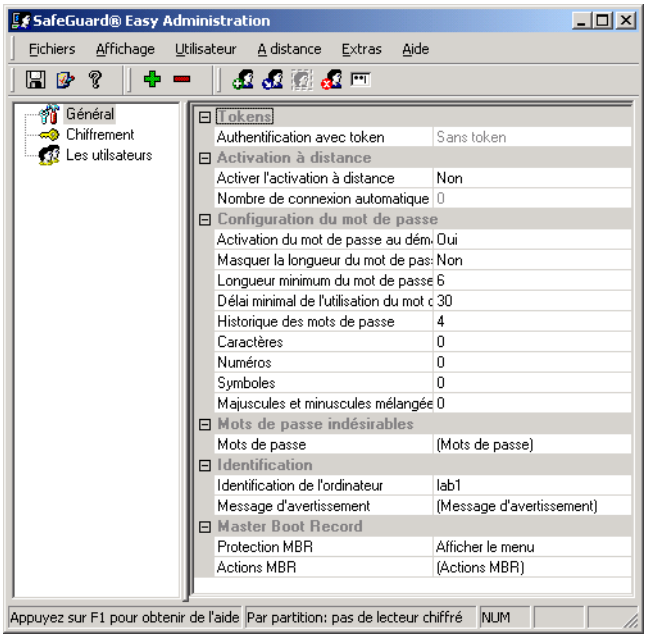
8.3 Fonction Administration

Une fois la fonction Administration exécutée, la boîte de dialogue de connexion s'affiche. Vous pouvez entrer ici les données SafeGuard Easy valides avant d'accéder à la fonction Administration.

Le nombre de tentatives d'ouverture de session est limité à cinq.
Le système doit ensuite être redémarré pour essayer à nouveau d'ouvrir une session.

8.3.1 Fenêtre d'administration

Après saisie correcte des données d'utilisateur SafeGuard Easy, la fenêtre Administration apparaît



Le volet de gauche présente une liste de toutes les pages de configuration disponibles. Si, dans la fenêtre de gauche, un fichier de configuration est sélectionné, des détails sur les possibilités de réglage sont affichés dans la partie de droite. Les différentes possibilités de paramétrage correspondent à celles qui sont disponibles lors de l'installation de SafeGuard Easy.

La fenêtre d'administration affiche d'autres informations dans la zone du bas.

- Mode de chiffrement et état de chiffrement des lecteurs (dans notre exemple : Par partition, pas de lecteur(s) chiffré(s).
- État des touches pour le pavé numérique et la touche de mise en exposant (dans notre exemple, la touche « Verr. num » est activée).

Dans la configuration de base, tout utilisateur connecté à l'administration peut y modifier son mot de passe SafeGuard Easy. L'importance de son rayon d'action dépend de son profil de droits.

8.3.2 Barre d'icônes et d'outils

L'utilitaire d'administration comporte une barre d'icônes avec des boutons pour les commandes les plus importantes (de gauche à droite) :

- **Enregistrer**
  Enregistre les nouveaux paramètres Si des modifications de paramètres requièrent un redémarrage du système, une boîte de dialogue est affichée.

- **Poste de travail**
  Permet de retrouver l'utilitaire d'administration à la prochaine ouverture de session tel qu'il a été quitté (même taille/position de fenêtre, même page de configuration, etc.).

- **Aide**
  Affiche l'aide en ligne.

- **Signe plus/moins**
  Le signe plus affiche dans la fenêtre de droite tous les paramètres subalternes, le signe moins minimise la vue, ne laissant que les titres des rubriques.

- **Créer un utilisateur**
  Ajoute un nouvel utilisateur (affichage dépendant du profil des droits de l'utilisateur ayant ouvert la session).

- **Copier un utilisateur**
  Copie un utilisateur existant (affichage dépendant du profil des droits de l'utilisateur ayant ouvert la session).

- **Supprimer un utilisateur**
  Supprime un utilisateur de la liste (affichage dépendant du profil des droits de l'utilisateur ayant ouvert la session).

- **Modifier le mot de passe**
  Permet à l'utilisateur ayant ouvert la session de modifier son mot de passe.

Toutes ces commandes peuvent être également appelées via les différents menus (Fichier, Affichage, Utilisateur, Outils, Aide).

8.4 Assistant Fichier de configuration

La seule tâche de l'assistant de configuration pour le déploiement est de créer des fichiers à l'aide desquels l'installation et la désinstallation de SafeGuard Easy peuvent être automatisées. Des tâches administratives telles que la modification d'une installation SGE existante peuvent être résolues également via les fichiers de configuration.
Dans les environnements réseau, l'administrateur envoie les fichiers de configuration aux ordinateurs des utilisateurs et les y exécute sans intervention des utilisateurs. Une fois le même fichier de configuration exécuté sur plusieurs ordinateurs, SafeGuard Easy fonctionne sur ceux-ci avec la même configuration.

Un fichier de configuration ne dépend pas d'un système particulier, c'est-à-dire qu'il peut être utilisé avec des systèmes autres que celui sur lequel il a été créé. L'essentiel est que la version de SafeGuard Easy utilisée sur les différents systèmes soit identique.

REMARQUES :
Seuls les outils d'administration sont nécessaires pour créer un fichier de configuration. A la création d'un fichier de configuration, SafeGuard Easy n'est pas installé sur votre ordinateur.

SafeGuard Easy ne prend en charge que les fichiers de configuration créés avec l'assistance de configuration pour le déploiement actuel.

Les fichiers de configuration doivent être protégés contre les accès non autorisés. Les utilisateurs ordinaires ne doivent pas accéder aux fichiers de configuration.

8.4.1 Réutilisation de fichiers de configuration de versions SafeGuard Easy antérieures

Les fichiers de configuration de versions antérieures peuvent être chargés et traités sans problème, si tant est qu'ils

- aient été créés avec un assistant de configuration pour le déploiement postérieur à SafeGuard Easy 3.20
- disposent du type de fichier « Installer ».

Au chargement d'un ancien fichier, SafeGuard Easy affiche aussi automatiquement les nouvelles possibilités de configuration (l'ouverture de session jeton par ex. est nouvelle depuis la version 3.20) et les convertit aux valeurs standard.

8.4.2 Créer un nouveau fichier de configuration

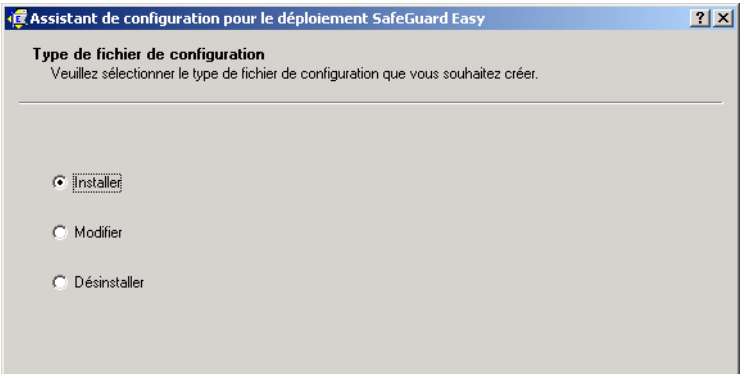
L'assistant de configuration pour le déploiement permet de créer des fichiers pour l'installation et la désinstallation sans intervention de l'utilisateur. L'assistant de configuration pour le déploiement saisit successivement les informations que doit contenir un fichier.

De nouveaux fichiers de configuration sont crées via Démarrer / Programmes / Utimaco / SafeGuard Easy / **Assistant de configuration pour le déploiement**.

Validez toutes les entrées correctes dans l'assistant avec [Suivant].

Après le démarrage, vous déterminez d'abord dans quel but le fichier de configuration est créé.

- Pour une installation
- Pour la modification d'une installation SafeGuard Easy existante (ledit fichier « Delta »)
- Pour une désinstallation

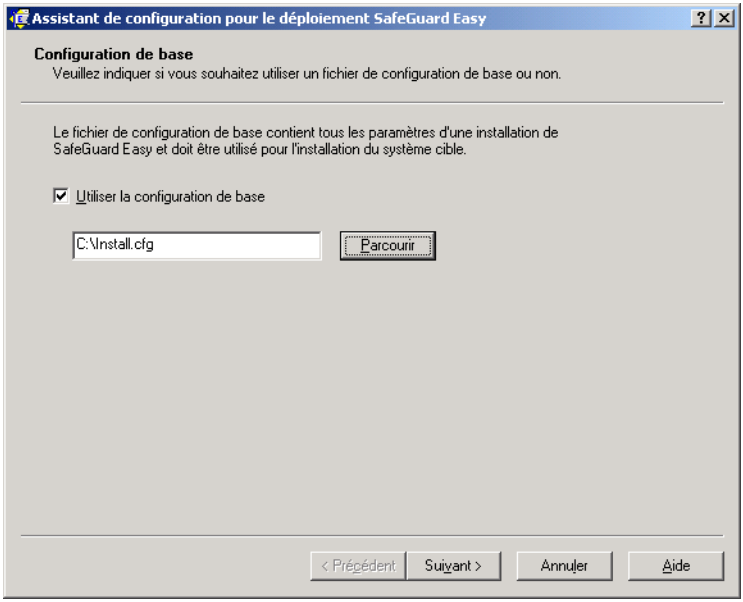


8.4.3 Création d'un fichier de configuration pour une installation

La propriété « Installer » génère un fichier de configuration avec lequel SafeGuard Easy peut être automatiquement installé sur un client (voir 'Installation centrale').

Après sélection de l'option « Installer », indiquez tout d'abord si vous souhaitez utiliser une configuration de base pour le nouveau fichier de configuration.

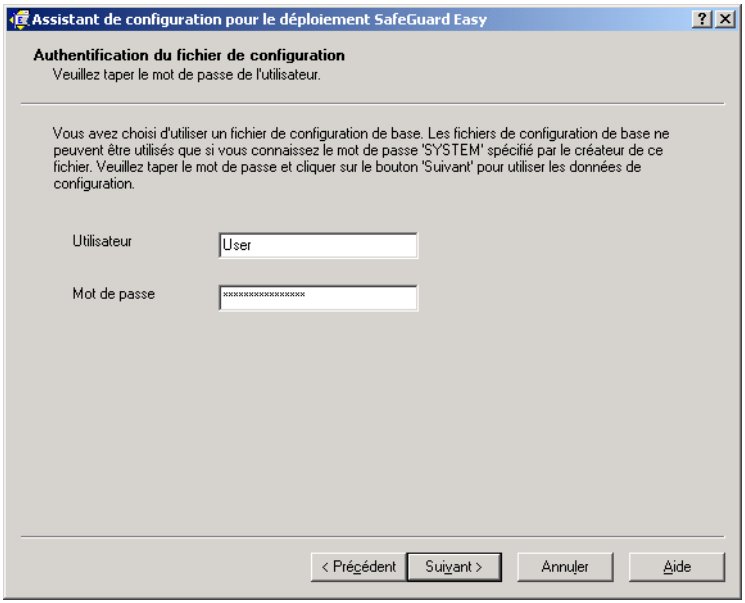
Configuration de base



Un fichier de configuration de base est un fichier de configuration existant avec propriété « Installer ». Il sert de modèle de base pour un nouveau fichier d'installation.

Avec fichier de configuration de base (option)

Les paramètres d'un fichier de configuration de base sélectionné ne deviennent pas visibles tant que l'utilisateur SafeGuard Easy SYSTEM ne s'est pas connecté.

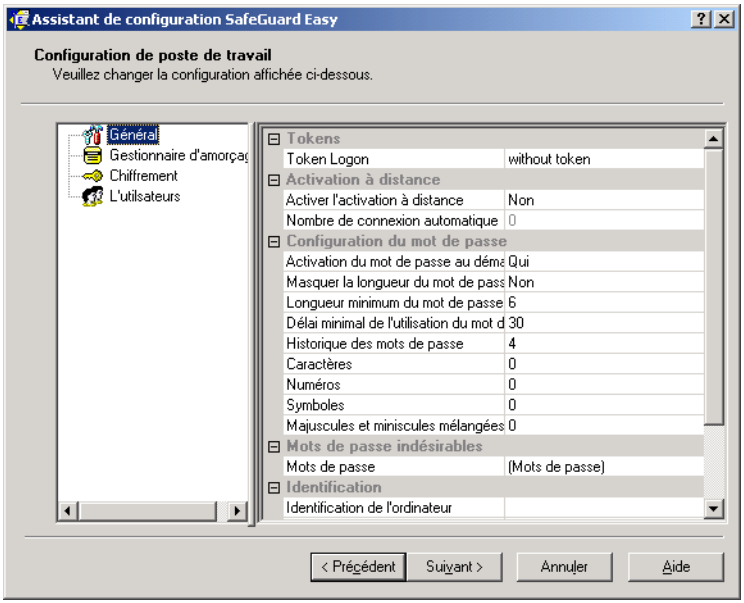


Mode de chiffrement

Sans configuration de base, le nouveau fichier de configuration doit être informé du mode de chiffrement pour que SafeGuard Easy sache quelles zones de disque dur doivent être chiffrées (voir 'Mode chiffrement').

Configuration

La fenêtre avec les différentes pages de configuration apparaît ensuite. Lorsque vous utilisez un fichier de configuration de base, ses paramètres sont chargés. Sinon, les paramètres par défaut s'affichent.



Vous trouverez des informations plus détaillées sur les différentes pages de configuration dans les chapitres correspondants.

Répertoire cible

Dans la boîte de dialogue Répertoire de destination, vous déterminez le chemin dans lequel vous souhaitez enregistrer le fichier de configuration nouvellement créé.

Pour éviter les problèmes, notez toujours les propriétés et paramètres que vous attribuez à un fichier de configuration.

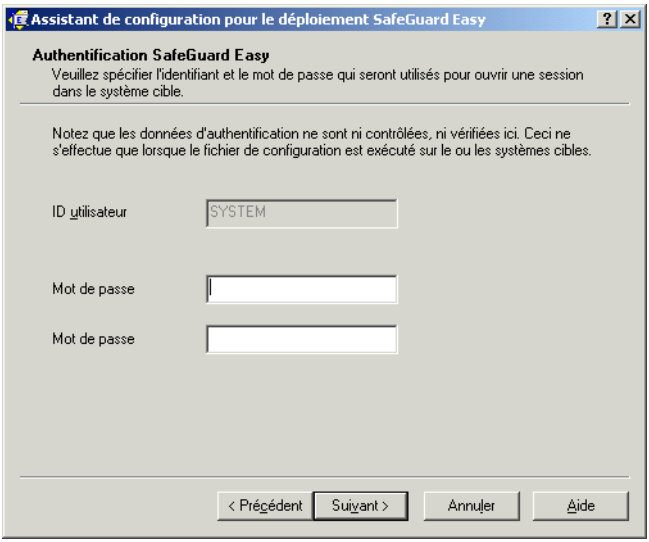
Remarque concernant le type de fichier « Change » avec le fichier de configuration de base :

Avec un fichier de configuration de base de type « Modifier avec configuration de base » et après le clic sur [Enregistrer], vous devrez ’indiquer si le fichier de configuration de base existant doit être remplacé ou non. Si vous cliquez sur [Oui], le fichier est écrasé et les modifications seront ajoutées au fichier de configuration de base existant.

Pour ce faire, il suffit de renommer le fichier de configuration de base et de l’enregistrer sous un autre nom.

8.4.4 Création d'un fichier de configuration pour une désinstallation

Le type de configuration « Désinstaller » ouvre la boîte de dialogue Authentification SafeGuard Easy.



L'utilisateur entré ici doit disposer du droit de désinstallation.

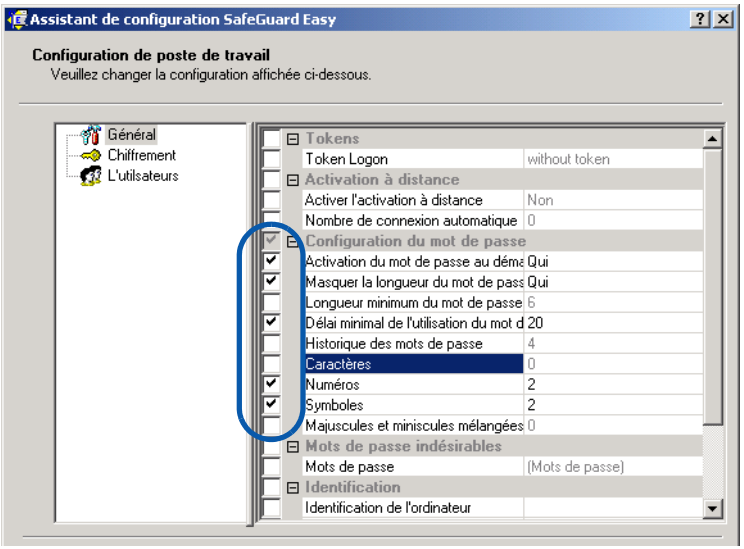
Lorsque vous avez entré toutes les données, cliquez sur [Suivant]. L'Assistant ouvre la boîte de dialogue *Répertoire cible*. Vous donnez un nom au fichier de configuration.

8.4.5 Création d'un fichier de configuration pour la modification (« fichier Delta »)

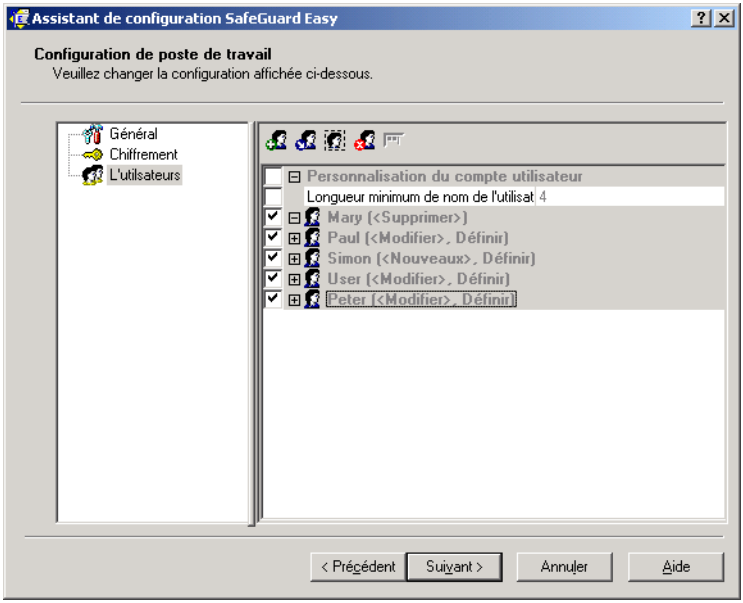
En bref, un fichier Delta modifie les paramètres d'une installation SafeGuard Easy existante. Comme un fichier d'installation, le fichier Delta peut être créé avec ou sans configuration de base.

Contrairement au fichier d'installation, il n'est cependant pas possible, dans les fichiers Delta, de modifier l'état du chiffrement de disque dur et du support de jeton.

Les options sur les différentes pages de configuration ne peuvent être traitées dans les fichiers Delta qu'une fois la case correspondante cochée.



A la page de configuration *L'utilisateur*, veuillez noter les fonctionnalités des boutons d création, copie et suppression d'utilisateur.



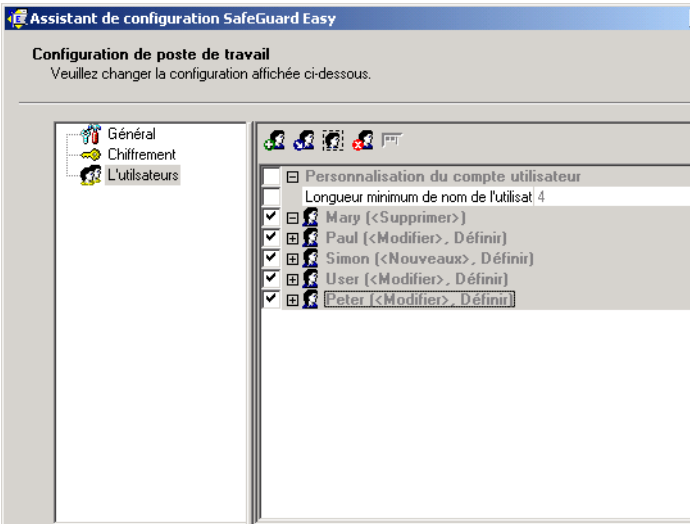
- **Créer un utilisateur** : à l'exécution du fichier de configuration, crée un nouvel utilisateur SafeGuard Easy de ce nom (dans notre exemple *Simon*).
- **Copier un utilisateur** : Tous les paramètres de l'utilisateur copié sont repris et le nouvel utilisateur de SafeGuard Easy reçoit également l'attribut « Créer ».
- **Modifier un utilisateur** : Crée un utilisateur déjà existant sur un poste de travail lui attribue de nouvelles propriétés (dans notre exemple *User, Peter* et *Paul* avec l'attribut « Modifier »).
  Tous les utilisateurs chargés d'une configuration de base reçoivent automatiquement la propriété « Modifier ».

Sans configuration de base, les utilisateurs doivent d'abord être créés avec cette propriété.

- **Supprimer un utilisateur** : indique le nom d'un utilisateur existant qui va être supprimé à l'exécution du fichier de configuration sur ce système cible (dans notre exemple, l'utilisatrice *Mary*).

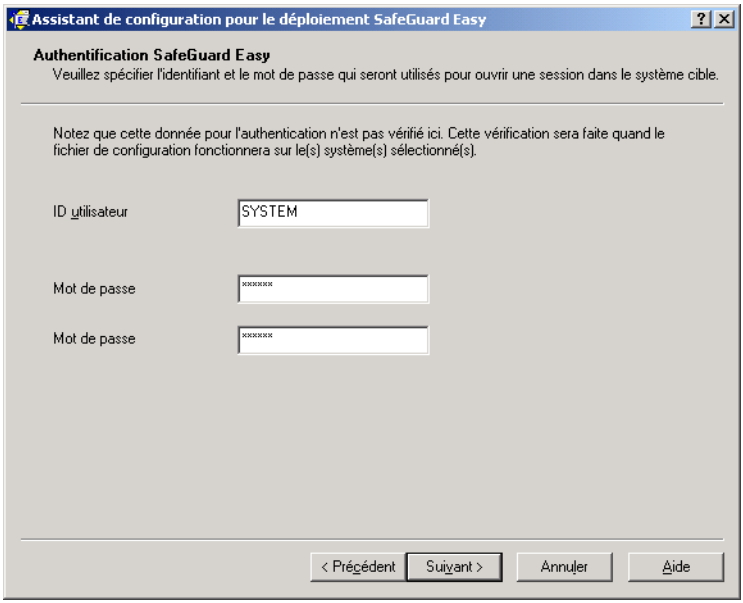
REMARQUES :

Dans les fichiers Delta sans configuration de base, la propriété « Supprimer » doit être attribuée aux utilisateurs via le champ « Commande de configuration.



Lorsque vous avez entré toutes les données, cliquez sur [Suivant]. L'Assistant ouvre la *boîte de dialogue d'authentification*, puis la boîte de dialogue *Répertoire cible*. Vous donnez un nom au fichier de configuration.

Authentification



L'utilisateur SafeGuard Easy spécifié ici doit exister sur le poste de travail sur lequel le fichier de configuration est exécuté et disposer des droits correspondants.

8.4.6 Exécuter le fichier Delta

Mode d'exécution du fichier delta :

1. Démarrez le mode MS DOS.

2. Accédez au répertoire où est installé SafeGuard Easy.

3. Tapez la commande

   `EXECCFG.EXE /f :`*<chemin et nom du fichier de configuration >*

   et cliquez ensuite sur [OK].

   Tous les paramètres sont affichés avec la commande `EXECCFG.EXE /?`

EXECCFG prend en charge le paramètre /Reboot, qui entraîne l'arrêt après l'exécution avec succès du fichier de configuration défini.

Exemple :

```
C :\SGEasy\EXECCFG /f :D :\Delta.cfg /Reboot
```

Cette commande vous permet alors d'appeler le fichier de configuration créé.

Ne laissez pas d'espaces entre « `/f` » et le nom de dossier du fichier delta !

8.4.7 Éditer un fichier de configuration

Les paramètres des fichiers de configuration avec la propriété « Installer » peuvent être ultérieurement modifiés, même une fois enregistrés.

Pour modifier un fichier de configuration, veuillez procéder comme suit :

1. Démarrez l'assistant de configuration pour le déploiement.

2. Choisissez le type de fichier « Installer » et chargez le fichier à éditer dans la boîte de dialogue *Configuration de base*.

3. Vous chargez la configuration en cliquant sur [Suivant].

4. Les paramètres qui y sont enregistrés sont affichés et peuvent être modifiés.

Si vous essayez d'appeler un fichier avec la propriété « Modifier » ou « Désinstaller », un message d'erreur est affiché.

8.5 Génération d'un fichier de configuration à partir de la ligne de commande

Si vous souhaitez générer un fichier de configuration à partir de la ligne de commande, utilisez le programme `CfgWiz`. `CfgWiz` est situé dans le dossier SafeGuard Easy.

`CfgWiz` peut être appelé avec les paramètres suivants :

`/cmd :install | change | uninstall`

Cette option remplace la boîte de dialogue du type de fichier de configuration.

`/base :<nom_fichier>`

Cette option définit le nom de la configuration de base à utiliser. Lors de l'installation, cette option remplace la boîte de dialogue de configuration de base CFGWIZ. Dans le cas d'un fichier d'installation, cette option remplace la boîte de dialogue de configuration de base.

`/instfile :<nom_fichier>`

Cette option définit le nom du fichier d'installation à générer. Lorsque ce paramètre est actif, la boîte de dialogue du dossier cible ne s'affiche pas. Si le fichier existe déjà, il sera remplacé par la nouvelle configuration.

`/changefile :<nom_fichier>`

Cette option définit le nom du fichier delta à générer. Lorsque ce paramètre est actif, la boîte de dialogue du dossier cible ne s'affiche pas. Si le fichier existe déjà, il sera remplacé par la nouvelle configuration.

`/uninstfile :<nom_fichier>`

Le nom de la configuration de désinstallation à générer en tant que sortie. Lorsque ce paramètre est actif, la boîte de dialogue du dossier cible ne s'affiche pas. Si le fichier existe déjà, il sera remplacé par la nouvelle configuration.

Exemple :

```
CfgWiz /cmd :change /base :C :\install.cfg /
changefile :C :\Change.cfg
```

REMARQUES :

Ces fonctions pourront être disponibles avec les versions ultérieures de LANDesk Management Systems.

8.5.1 Exemples d'application

Exemple 1 :

Dans l'assistant de configuration pour le déploiement, créez un fichier permettant d'installer SafeGuard Easy sans intervention de l'utilisateur sur plusieurs postes de travail d'une entreprise. Le fichier de configuration doit prendre en outre en charge un concept d'administration hiérarchisé et comporter les profils d'utilisateur suivants :

- SYSTEM : administrateur SafeGuard Easy possédant tous les droits
- SUBADMIN : sous-administrateur auquel les tâches administratives ont été déléguées. Permet de modifier les paramètres utilisateur et de changer de mode de chiffrement de la disquette.
- USER : utilisateur final ne disposant d'aucun droit.

Comment procéder :

1. Démarrez l'assistant de configuration pour le déploiement.
2. Sélectionner le type de fichier de configuration « Installer ».
3. Ne pas choisir de configuration de base.
4. Choisissez le mode de chiffrement « Disques complets.
5. Sous la rubrique « Général », choisissez l'option « Activation du mot de passe au démarrage ».

6. Dans les paramètres d'utilisateur, choisir les paramètres suivants :

   - SYSTEM (mot de passe : System)
     Droits : tous

   - SUBADMIN (Subadmin)
     Génération d'un code C/R abrége : Activee
     Droits
     - modifier les paramètres d'utilisateur
     - activer le chiffrement de disquettes

   - USER (User)
     Droits : aucun

7. Dans les paramètres de chiffrement, choisir les paramètres suivants :

   Disquettes : Activer
   Disques durs : Activer
   Périphériques amovibles : Activer

8. Sous MBR, conserver les paramètres par défaut

9. Enregistrer le fichier de configuration de base « Install.cfg » dans le répertoire de destination.

10. Distribuer le fichier Install.cfg.

Exemple 2 :

Sur la base du fichier Install.cfg de l'exemple 1, l'utilisateur « User » doit maintenant pouvoir modifier de façon temporaire la clé de disquette sur tous les postes de travail. Conformément aux structures d'administration spécifiées, ce droit est octroyé par l'utilisateur « SUBADMIN ». Pour ce faire, le SUBADMIN doit créer un fichier de configuration de type « Modifier » et le distribuer aux postes de travail concernés.

Comment procéder :

1. Démarrer l'assistant de configuration pour le déploiement.
2. Sélectionner le type de fichier de configuration « Modifier ».
3. Choisir « Install.cfg » comme fichier de configuration de base.
4. Lors de l'authentification avec fichier de configuration, ouvrir une session avec SUBADMIN (mot de passe : subadmin).
5. Dans les paramètres d'utilisateur
   - Double-cliquer sur l'option « Droits » sous « USER ».
   - Activer le chiffrement de disquettes.
6. Enregistrer le fichier « Change.cfg » dans le répertoire de destination.
7. Distribuer Change.cfg aux ordinateurs d'utilisateurs.

8.6 Modification des paramètres de registre fréquemment utilisés via le modèle d'administration

Pour améliorer le confort lors de la configuration, Utimaco a généré un modèle d'administration spécifique pour l'éditeur de stratégies de groupes (Gpedit.msc). Ce modèle (nom de fichier : Sguard.adm) permet de définir confortablement certains paramètres SafeGuard Easy sans avoir à éditer le registre.

Un administrateur peut modifier les paramètres du modèle administratif pour le PC de l'utilisateur, soit localement, par l'intermédiaire de l'éditeur de stratégie de groupe (Gpedit.msc), soit centralement par l'intermédiaire des objets de stratégie de groupe (GPOs) dans un environnement Active Directory. Les utilisateurs dans un environnement informatique n'ont normalement pas de droits d'administrateur et ne peuvent par conséquent pas modifier eux-mêmes les stratégies SafeGuard Easy.

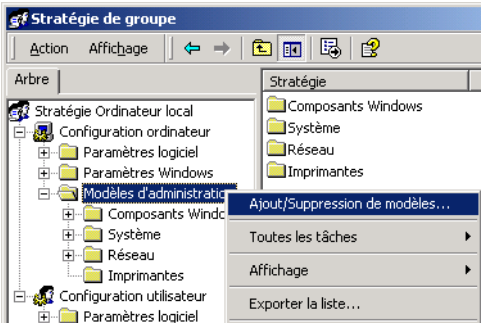
Vous trouverez ci-dessous des instructions brèves sur la manière d'intégrer le modèle Utimaco dans un système local. Pour la manipulation de modèles d'administration dans un environnement avec OSG, veuillez consulter la documentation Microsoft usuelle.

1. Ouvrir une session comme utilisateur avec droits d'administrateur Windows

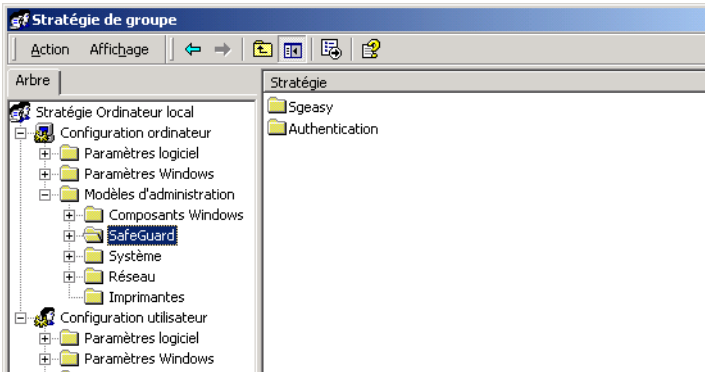
2. Cliquez sur Démarrer / Exécuter, tapez la commande « Gpedit.msc » et ouvrez l'éditeur de stratégies de groupes local.

3. Ajouter modèle SafeGuard Sguard.adm via « Modèles d'administration » > « Ajout/Suppression de modèles ».

Sguard.adm se trouve dans le répertoire d'installation SafeGuard Easy, dans le dossier \ADM.



4. Outre les dossiers précédents, le dossier« SafeGuard »apparaît dans la rubrique Configuration ordinateur de la MMC.

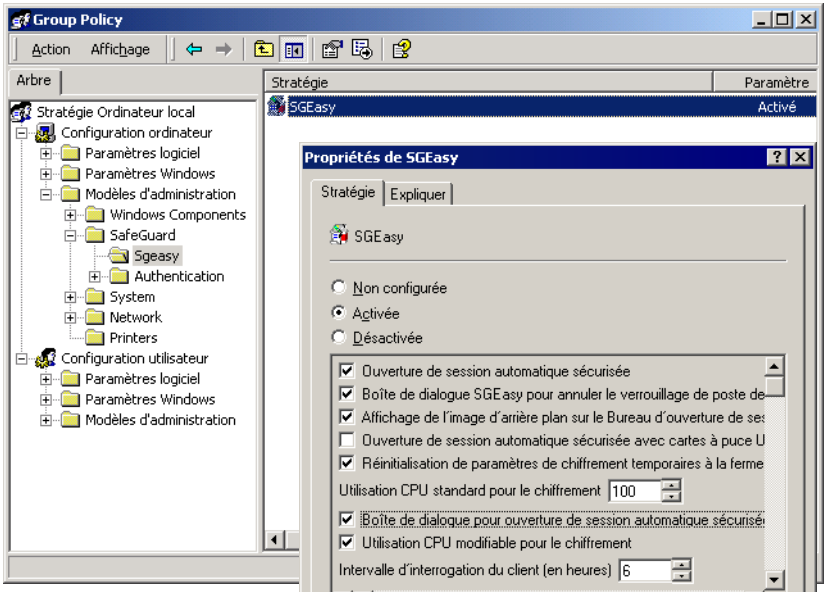


5. Avec les modèles non Windows, la vue préalablement configurée pose un problème. Par conséquent, le paramètre suivant doit être désactivé pour les stratégies individuelles :

   Windows 2000 :
   Sélectionnez « Modèles administratifs », sélectionnez le menu « Affichage » et désactivez « Afficher uniquement les stratégies » de

   Windows XP/Windows Server 2003 :
   Sélectionnez « Modèles administratifs », sélectionnez le menu « Affichage », puis « Filtrage » et désactivez « N'afficher que les paramètres de stratégie pouvant être entièrement gérés ».

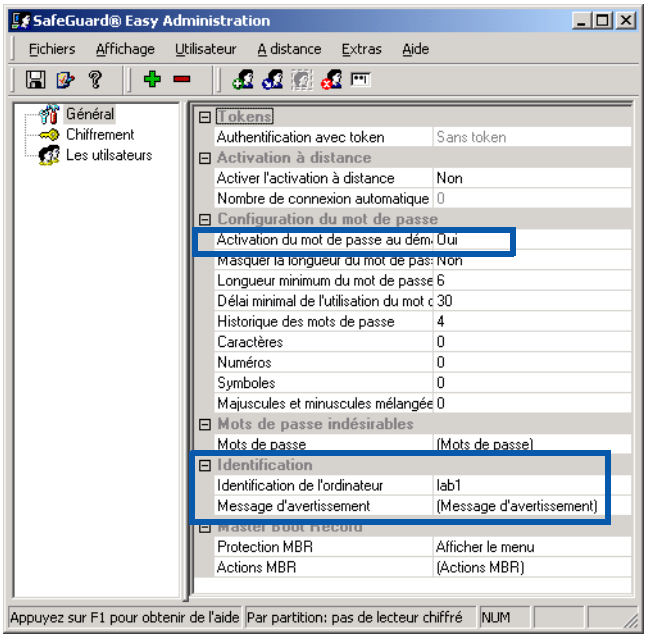
6. Double-cliquer sur la stratégie pour l'ouvrir et procéder aux réglages à la page des « Propriétés de SGEasy ».



Les stratégies peuvent avoir trois états différents :

- **Non configurée**
  Les paramètres actuels chez l'utilisateur ne sont pas modifiés, c'est-à-dire que le réglage effectué précédemment demeure.
- **Activé**
  Les paramètres sont transférés.
- **Désactivé**
  Les paramètres sont supprimés.

9 Authentification avant l'amorçage (PBA)



La fonction Pre-Boot Authentication (PBA) est une fonction qui requiert une authentification avant l'amorçage. Vous trouverez de plus amples informations sur l'authentification avant amorçage sous 'Démarrage du système et ouverture de session'.

Vous pouvez spécifier les paramètres PBA sur la page de configuration « Général ».

9.1 Vous pourrez modifier la langue choisie ultérieurement.

L'écran de connexion applique la langue sélectionnée pendant l'installation (Allemand, Anglais ou Français). Les utilisateurs n'ont plus à désinstaller SafeGuard Easy pour afficher le texte d'authentification avant le démarrage dans une autre langue.

> ***IMPORTANT :***
> Vous pouvez seulement modifier ultérieurement l'affichage des textes sur l'écran PBA, pas la composition du clavier.

Paramètres de changement de langue

Vous pouvez lancer SetPBALang avec les paramètres suivants :

```
SetPBALang [en | de | fr] | [n]
```

`[en | de | fr]`	Définit la nouvelle langue
`[n]`	Utilise un numéro (1-255) pour le réglage de la langue Les langues suivantes sont proposées : 9=Anglais 7=Allemand 12=Français

Le réglage de la langue prend effet après le redémarrage.

Vous trouverez SetPBALang dans le répertoire programme de SafeGuard Easy.

9.2 Activation du mot de passe au démarrage du système

L'option « Activation du mot de passe au démarrage » active/désactive l'authentification avant amorçage (PBA). Si la PBA est activée, un écran d'ouverture de session apparaît avant le chargement du système d'exploitation. Windows ne démarre qu'une fois l'authentification effectuée avec les données d'accès SafeGuard Easy correctes.

Si vous désactivez la fonction PBA, une ouverture de session avant le démarrage du système n'est pas nécessaire. L'authentification s'effectue alors comme d'habitude via la boîte de dialogue d'ouverture de session du système d'exploitation.

Pour des raisons de sécurité, la fonction d'authentification avant amorçage (PBA) ne doit jamais être désactivée !

9.3 Identification de l'ordinateur

Les options sous « Identification » permettent d'afficher dans la PBA des textes définissables.

9.3.1 Identification de l'ordinateur

Le texte entré dans ce champ apparaît dans la boîte de dialogue d'ouverture de session de la PBA. Vous pouvez, par exemple, spécifier un nom exact pour votre station de travail dans ce champ, ce qui vous permet d'identifier l'ordinateur avec précision. Si un nom d'ordinateur est déjà défini par les paramètres réseau de Windows, il est transféré de façon automatique.

Vous pouvez taper un maximum de 63 caractères.

L'identification de machine peut également contenir des liens avec des variables d'environnement. Ces liens sont convertis à l'installation. Ceci est utile en particulier lors de la création de fichiers de configuration, installés sur plusieurs postes de travail.

Exemple :

L'entrée dans le champ *« Identification de la machine » Ceci est %USERDOMAIN%*. L'amorçage est effectué de %WINDIR%

devient « *Le PC1234 démarre à partir de C:\WINNT »*

pendant l'installation.

Pour tous les systèmes d'exploitation, il existe la variable spéciale %COMPUTERNAME%. Le nom de l'ordinateur est intégré avec cette variable, indépendamment de la plate-forme. La variable %COMPUTERNAME% est toujours convertie dans le nom NETBIOS de l'ordinateur.

Les règles suivantes sont en outre valables :

- Les variables d'environnement non définies génèrent des liens vides.
- Quand la variable dans le champ d'identification de la machine est trop longue, elle est convertie en « [...] ».
- Pour les noms de variables, il n'est pas nécessaire de respecter la casse (majuscules/minuscules).
- Quand un signe de pourcentage est nécessaire dans le lien, utilisez « %% ».
- La conversion de variables n'est exécutée qu'une seule fois au moment de l'installation, pas à chaque démarrage de l'ordinateur.

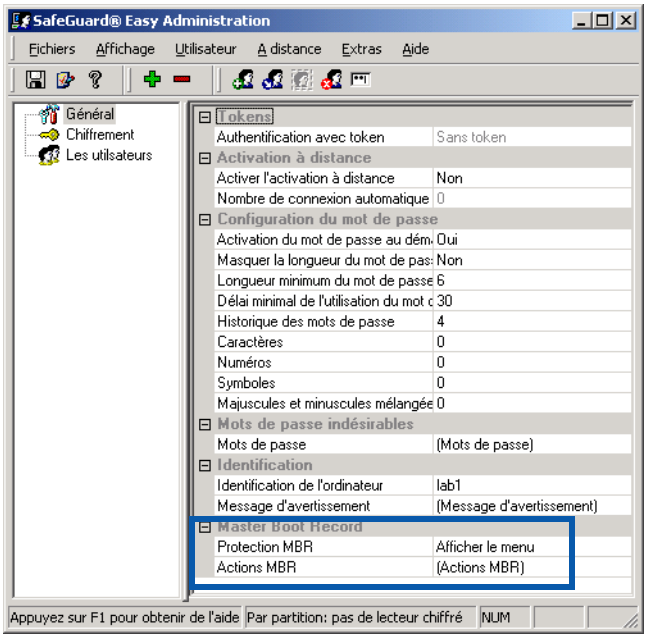
9.3.2 Message d'avertissement (Legal Notice)

Il s'agit ici d'une zone de texte de contenu librement configurable, affiché **avant l'ouverture de session avec les données SafeGuard Easy**. Dans certains pays, l'affichage d'un champ de texte d'un contenu donné est prescrit par le législateur.

Le titre peut contenir jusqu'à 68 caractères et le bloc des textes peut contenir jusqu'à 10 lignes avec 70 caractères chacune.

Les données doivent être confirmées par l'utilisateur avant que le système poursuive.

10 Enregistrement de démarrage principal



Dans le MBR d'un disque dur, diverses informations sont stockées pour chaque partition créée. Ceci indique au système le disque dur respectivement la partition utilisée pour l'amorçage. C'est donc un lieu de prédilection pour les attaques de virus, car le BIOS exécute le code machine qui s'y trouve tout au début du processus d'amorçage, avant que le système d'exploitation soit chargé. SafeGuard Easy est capable de déceler les altérations du MBR et d'y réagir de diverses façons, en affichant un menu ou en permettant à l'utilisateur de sélectionner une action une fois les modifications apportées.

Les paramètres du Master Boot Record sont définis sur la page de configuration « Général ».

10.1 Protection MBR

La protection du MBR est un mécanisme de sécurité contre les virus attaquant le secteur de partition. Si vous n'avez pas défini « Ignorer les changements », des altérations éventuelles du MBR sont vérifiées à chaque démarrage du système.

- **Ignorer les changements**
  Quand ce paramètre est défini, une modification éventuelle du MBR est acceptée. Le processus d'amorçage n'est pas interrompu.

- **Afficher le menu**
  Quand le MBR est modifié, un menu dans lequel vous pouvez choisir une des actions suivantes est affiché :

  - Action par défaut
  - Restaurer
  - Ignorer les changements
  - Conserver les modifications

  Sélectionnez *Action par défaut* pour exécuter l'action par défaut. Réglage par défaut permet à l'utilisateur de sélectionner l'action prédéfinie, *Restaurer* autorise la restauration du MBR à partir de la copie de sauvegarde. *Ignorer* permet d'ignorer les modifications et Valider d'accepter le MBR actuel. Si vous sélectionnez *Conserver les modifications* le MBR en cours reste inchangé et la sauvegarde interne est mise à jour. La vérification a lieu avant la connexion de l'utilisateur. Le menu n'est toutefois affiché qu'après une ouverture de session valide. Il est ainsi exclu qu'un utilisateur non autorisé puisse décider de la manière de procéder dans un tels cas.

10.2 Actions par défaut du MBR

Vous pouvez sélectionner une ou plusieurs actions :

- **Afficher l'avertissement**
  L'utilisateur est notifié lors de la modification du MBR créé pour SafeGuard Easy. L'utilisateur doit confirmer ce message en appuyant sur une touche.

- **Restaure MBR**
  Le MBR d'origine est restauré de façon automatique en tant que copie de sauvegarde, sans notifier l'utilisateur. Ensuite, le système redémarre et supprime tout virus éventuellement détecté.

- **Halt System**
  (Arrêter le système) Si le MBR a changé, le système affiche un message et s'arrête après la connexion, si l'utilisateur tente de se connecter. (Cependant, l'administrateur système peut se connecter.) Il n'est alors plus possible d'amorcer le poste de travail et l'utilisateur est obligé de demander l'aide de l'administrateur ou du service d'assistance technique.

10.3 Accès à la partition de configuration de Compaq

Cette option laisse le MBR pour l'essentiel inchangé. Ceci est nécessaire avec certains systèmes Compaq (et éventuellement d'autres) pour permettre l'accès à la partition de configuration. Cliquez sur « On » (Activé) pour conserver le MBR d'origine. Si vous ne souhaitez pas définir cette option, sélectionnez « Off » (Désactivé). Elle peut être activée ou désactivée dans tous les modes de chiffrement (disques complets, protection des zones d'amorçage, par partition).

Utimaco conseille de ne sélectionner cette option que lorsque cela est absolument indispensable. Si vous n'êtes pas sûr de la façon dont va réagir votre ordinateur, veuillez contacter le service d'assistance téléphonique Compaq.

11 Chiffrement

La fonction principale de SafeGuard Easy est le chiffrement des données des supports les plus divers, tels que les disques durs, les disquettes et les périphériques amovibles.

Le chiffrement de disquettes et de périphériques amovibles offre l'avantage que toutes les communications de données se déroulent en mode chiffré par rapport au monde extérieur. Sur un ordinateur avec option de chiffrement activée, les disquettes normales en texte clair sont illisibles. Les disquettes illisibles doivent être formatées à nouveau sur le lecteur de disque chiffré avant de pouvoir être utilisées. Cependant, toutes les données sont effacées pendant le formatage ! Si des disquettes passent d'un poste de travail à l'autre, les lecteurs de disquettes de ces postes de travail doivent être chiffrés avec un algorithme et une clé identiques. Dans le cas contraire, la disquette ne peut pas être lue.

Les utilisateurs possédant les droits appropriés peuvent modifier provisoirement les clés de disquettes et de périphériques amovibles, à condition que le chiffrement soit activé (voir 'Activation/désactivation du chiffrement de disquettes et de périphériques amovibles').

Le chiffrement avec des clés respectivement différentes peut être exécuté en utilisant divers algorithmes (AES-128, AES-256, Rijndael-256, IDEA, 3DES, DES, DES SB-II, Blowfish-8, Blowfish-16, STEALTH-40, XOR et XOR SB-I A=B). Selon sa définition, la clé est chiffrée et non stockée dans le système pour des raisons de sécurité. A chaque amorçage du système, elle est générée de nouveau à partir d'un code enregistré sur le disque dur et du mot de passe SafeGuard Easy de l'utilisateur.

Seules les zones du système ou des partitions isolées, ou encore un maximum de quatre disque durs, peuvent être chiffrés. Les systèmes de fichier suivants sont pris en charge : FAT-12, FAT-16, FAT-32, HPFS, NTFS et NTFS5. Le nombre de partitions d'un disque dur est limité à huit.

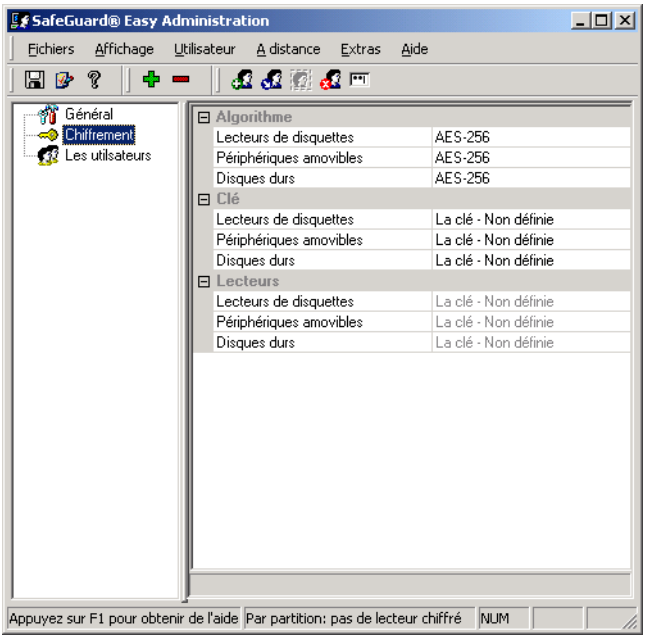
Pour définir avec précision la protection d'accès à votre système, nous vous recommandons les modules suivants de la famille de produits SafeGuard :

- **Droits d'accès spécifiques aux applications (ASAR) :**
  Élabore un concept de sécurité tridimensionnel qui permet de spécifier explicitement des droits entre les utilisateurs, les données et les applications. Ceci représente une protection contre la menace causée par certains virus (actuellement encore inconnus) et fournit un haut degré de sécurité, même dans un code non administré ou des environnements avec versions Windows mixtes.

- **Plug&Play Management (PnP):**
  Les utilisateurs peuvent connecter et utiliser immédiatement n'importe quels périphériques PnP, par ex. les sticks mémoire USB. L'administration PnP permet une importation/exportation contrôlée des données sur des supports de mémoire au niveau de catégories et d'appareils individuels.

11.1 Configuration du chiffrement

Les paramètres de chiffrement sont définis dans les programmes d'administration à la page de configuration « Chiffrement.



11.2 Lecteurs pris en charge

Disques durs

- Disques durs IDE/SCSI
- Disques durs ATA série (« connectables à chaud »)
- Disques durs Firewire (« connectables à chaud »)
- Disques durs USB (« connectables à chaud »)

Remarques relatives au chiffrement de disques durs :

- **Disques durs connectables à chaud**

  Tous les disques durs qui doivent être chiffrés doivent être déjà connectés à l'ordinateur à l'installation de SafeGuard Easy.

  Le premier chiffrement de disques durs connectables à chaud ne doit pas être interrompu !

  Les disques durs connectables à chaud doivent rester connectés même au premier redémarrage après le premier chiffrement. Après le premier chiffrement, le lecteur peut être connecté et déconnecté selon les besoins. Il est nécessaire que l'utilisateur se serve toujours du même disque dur, par ex. pour les sauvegardes régulières des données. Cela se déroule généralement sans problème.

  Si plusieurs disques durs sont utilisés (par ex. déconnexion d'un disque dur chiffré et connexion d'un disque dur non chiffré), des problèmes peuvent survenir à la suite par ex. d'incohérences dans le tableau de chiffrement SGE.

  Règle générale : La numérotation du disque (DiskManagement) utilisé doit correspondre à la numérotation pendant la procédure d'installation ou le premier chiffrement.

Les restrictions citées ne valent pour les disques durs ATA série uniquement lorsqu'ils sont utilisés comme disques durs connectables à chaud.

- **Divers types de disque dur**
  Évitez si possible de mélanger plusieurs types de disque dur (IDE/SCSI) sur un système.

- **Zones non formatées**
  Si une partition n'a pas été affectée de façon fixe à un système de fichiers, SafeGuard Easy ne le détecte pas le type d'installation « Protection des zones d'amorçage » et la partie non formatée du disque dur est également chiffrée.

- **Disques durs supplémentaires**
  SafeGuard Easy reconnaît automatiquement le nombre de disques durs de votre ordinateur. Après l'installation de SafeGuard Easy, aucun disque dur supplémentaire ne doit être intégré dans le système. Si vous souhaitez intégrer un disque dur supplémentaire dans votre système, vous devez d'abord désinstaller entièrement SafeGuard Easy. Après la désinstallation, vous intégrez le nouveau disque dur et vous réinstallez le programme.

- **Repartitionnement**
  Si un disque dur a été repartitionné, un redémarrage doit être effectué AVANT l'installation de SafeGuard Easy.
  Veuillez ne plus modifier le partitionnement du disque dur après le chiffrement. Ceci peut entraîner la perte de données.

- **Clé**
  Une seule clé de disque dur est définie, indépendamment du nombre de disques durs.

- **Sauvegarde du noyau système**
  Après le chiffrement du disque dur, effectuez impérativement une sauvegarde du noyau système !

Disquettes

- SafeGuard Easy prend en charge tout lecteur intégré dans un PC standard.

Remarques relatives au chiffrement de disquettes :

- **Disquette d'amorçage**
  Quand le chiffrement de disquettes est activé, il est impératif de créer une disquette d'amorçage chiffrée.

- **Plusieurs lecteurs de disquettes**
  Quand il existe plusieurs lecteur de disquettes, les différents lecteurs sont affichés non pas individuellement, mais ensemble (« A+B »). Les disquettes ne peuvent pas être chiffrées individuellement. L'état de chiffrement est valable pour tous les lecteurs de disquettes.

Périphériques amovibles

- Support mémoire USB
- Carte mémoire avec emplacement de lecteur intégré (carte SD, carte CF, etc.)
- Lenovo Microdrive
- Lecteur ZIP USB
- Lecteur ZIP parallèle

Remarques relatives au chiffrement de périphériques amovibles :

- **Connection possible after installation (Connexion possible après l'installation)**
  Les supports amovibles ne doivent pas être connectés pendant l'installation de SafeGuard Easy (mais des exceptions sont possibles si, par exemple, une clé USB ne fonctionne pas avec le pilote Microsoft standard, mais nécessite son propre pilote).

- **Premier chiffrement**
  Les périphériques amovibles ne sont pas sujets à un « premier chiffrement). Ils sont formatés dès que le chiffrement est activé (à la demande après l'installation de SafeGuard Easy).

- **Éjection SG**
  Les périphériques amovibles sont traités comme des disques durs, si tant est qu'un logiciel fourni par le constructeur du lecteur n'est pas utilisé. Si un périphérique amovible est chiffré, seuls les utilisateurs disposant de droits d'administrateur Windows peuvent éjecter un périphérique inséré. Les utilisateurs qui ne disposent pas de droits d'administration doivent utiliser SG Eject (Éjection SG). L'option SG Eject figure dans le menu contextuel du lecteur.

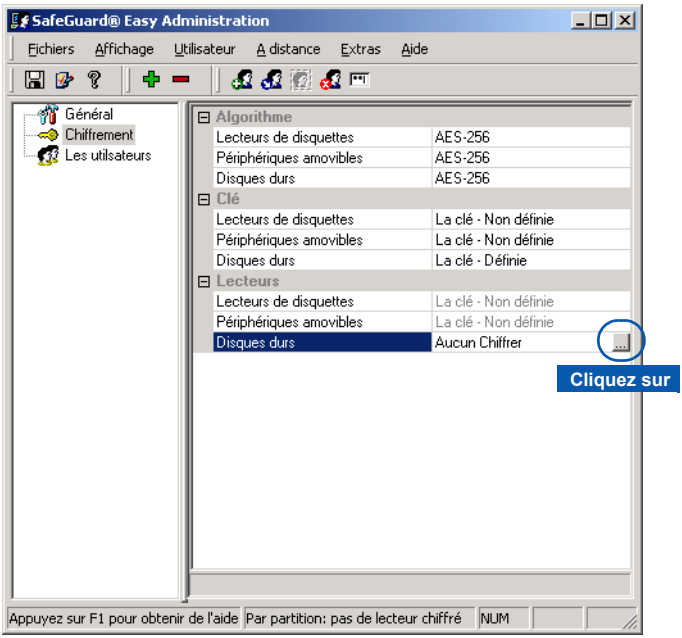
11.2.1 Chiffrement des disques durs

Dans l'exemple qui suit, nous utilisons le chiffrement de disques durs, la procédure étant identique pour les lecteurs de disquettes et les périphériques amovibles.

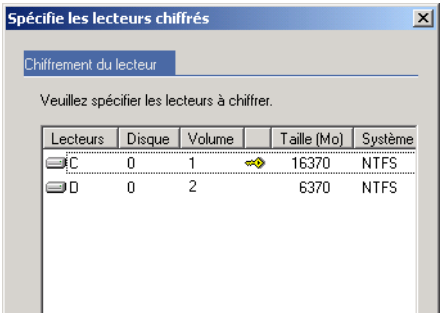
1. Sélectionnez un algorithme pour le disque dur.

2. Définissez une clé.

3. Cliquez sur Disques durs dans la rubrique Lecteurs.



4. La boîte de dialogue Spécifie les lecteurs chiffrés s'ouvre.



Une clé symbolique apparaît si vous double-cliquez sur une lettre de lecteur. Ceci indique que le lecteur / la partition est chiffré.

Les types de disques durs et le nombre de partitions pouvant être chiffrés dépendent du mode de chiffrement configuré. Le mode de chiffrement (voir 'Mode chiffrement') d'une station de travail est défini pendant l'installation, ou lorsqu'un fichier de configuration avec l'attribut « Install » est généré, et vous ne pourrez plus le changer par la suite.

5. Si vous voulez désactiver le chiffrement, double-cliquez de nouveau sur les lettres des lecteurs. La clé symbolique disparaît et le chiffrement est désactivé.

11.3 Clés

Seul un utilisateur possédant la clé correcte peut accéder aux lecteurs chiffrés. Une clé se compose d'une série de caractères (nombres, lettres, caractères spéciaux) et, tout comme un mot de passe, elle est soumise à certaines règles.

Les clés de lecteur doivent être attribuées avant le premier chiffrement. Pour tous les lecteurs, vous devez soit définir vous-même une clé, soit faire générer une clé aléatoire par le système.

11.3.1 Gestion de clés

La gestion des clés SafeGuard Easy enregistre les clés de façon sûre. Toutes les clés sont conservées dans un domaine chiffré du noyau système SafeGuard Easy, chiffrées avec une clé de chiffrement, à savoir la clé « KEK » (pour **K** ey **E** ncryption **K** ey). La KEK proprement dite n'est pas mémorisée sur le disque dur, mais créée à partir du mot de passe SafeGuard Easy.

11.3.2 Création de clé

Sans mot de passe correct, les clés ne sont pas accessibles.

Si la PBA est active, les clés ne sont créées pour le déchiffrement des lecteurs que lorsque les données SafeGuard Easy correctes ont été saisies dans la PBA.

Si la PBA est désactivée, les clés sont chiffrées et mémorisées sur le disque dur. Le chiffrement et la gestion des clés sont malgré cela absolument identiques à la sélection « PBA activée ». L'utilisation du mot de passe (ou du Scan Code) ne l'est pas. Sans attendre au niveau de la PBA que l'utilisateur tape manuellement son nom d'utilisateur et son mot de passe, SGE dispose de ces données. A cet effet, SGE crée – toujours quand la PBA est désactivée – un utilisateur ('*AUTOUSER') et lui attribue un mot de passe aléatoire. Partagé en différents éléments,, ce mot de passe est stocké dans le noyau SGE. A l'amorçage, SGE est en mesure d'en restaurer le mot de passe complet (ou à proprement parler la séquence du Scan Code complète).

11.3.3 Longueur de clé

Il n'y a pas de longueur minimale de clé prédéfinie. La longueur maximale de la clé est de 32 caractères (codes ASCII 32 à 255). Les caractères alphanumériques (A-Z; a-z; 0-9) et spéciaux (°!"„§$%&/()=?´*'-:;^+#-.,) peuvent être utilisés, mais pas les caractères spéciaux propres à une langue. Le système tient compte des majuscules et des minuscules. Ainsi MotPasse et motpasse sont considérés comme différents. sont considérés comme différents.

11.3.4 Clé banale

La banalité des clés pour disquettes, disques durs et périphériques amovibles est vérifiée. Les clés banales sont des chaînes de caractères se composant d'un ou de peu de caractères (p.ex. 22222222, aad daad daadd, 1h1h1h1h1h1h1h) ou qui correspondent à l'ordre d'une rangée du clavier (p.ex. qsdfgh, lkjhgfds). Quand vous entrez une clé banale, vous êtes avisé du risque relatif à la sécurité et vous pouvez redéfinir la clé.

11.3.5 Clé aléatoire

Une clé aléatoire a toujours une longueur de 32 octets (256 bits). Elle est ensuite raccourcie à la longueur de l'algorithme sélectionné. Les caractères * dans le champ de saisie de la clé ne servent que de caractères de remplacement.

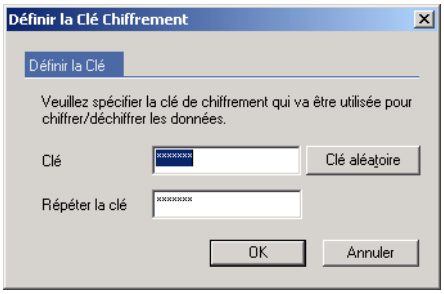
Nous recommandons de générer une clé aléatoire pour les disques durs ou les partitions lorsque SafeGuard Easy est installé sur plusieurs stations de travail avec un seul fichier de configuration. Dans ce cas, bien que les mêmes paramètres de configuration soient utilisés sur chaque ordinateur, des clés différentes et fortes sont générées.

En cas de fort trafic de disquettes/périphériques amovibles ou entre les collaborateurs, la clé ne doit **jamais** être générée de manière aléatoire. Les supports chiffrés avec cette clé aléatoire ne peuvent être lus que sur le poste de travail sur lequel ils ont été chiffrés.

11.3.6 Définition de clés

Toutes les clés ne peuvent être saisies dans la configuration de base que par l'administrateur du système (SYSTEM). Pour que les autres utilisateurs puissent disposer de cette possibilité, un droit correspondant doit leur être octroyé. Les clés pour disque dur, disquette et périphérique amovible peuvent être différentes. Une seule clé peut être attribuée pour tous les lecteurs

Lorsque vous affectez une clé pour la première fois ou modifiez une clé, sélectionnez le menu « Key » (Clé). La saisie de la clé se fait de manière identique pour tous les lecteurs. Les mêmes règles de clé sont également applicables. Une fois que vous avez défini la clé ou si vous avez choisi la définition d'une clé aléatoire, cliquez sur le bouton [OK] pour valider votre choix.



Ne transmettez jamais une clé que vous avez choisie vous-même à des tiers non autorisés.

11.3.7 Modifier les clés de chiffrement

Un disque dur ou des partitions chiffrés doivent d'abord être déchiffrés avant de pouvoir définir une nouvelle clé.

La clé pour disquettes ou périphériques amovibles peut être à tout moment redéfinie, soit par l'utilisateur SYSTEM de SafeGuard Easy, soit par un utilisateur possédant les droits appropriés. Veuillez toutefois noter que les supports de données chiffrés avec « l'ancienne » clé ne seront plus lisibles. Les utilisateurs ne peuvent accéder aux supports « anciens » que s'ils possèdent le droit d'activer la clé de disquettes / périphériques amovibles (voir 'Activation/désactivation du chiffrement de disquettes et de périphériques amovibles').

11.4 Algorithmes

C'est à leur sécurité en particulier qu'on mesure les différents algorithmes. Plus un procédé est sûr, plus le processus de chiffrement est généralement long.

11.4.1 Sélection d'algorithme

Pour sélectionner un algorithme, sélectionnez *Algorithms* (Algorithmes) et cliquez sur un lecteur de disque. Sélectionnez ensuite un algorithme pour ce lecteur de disque dans le menu déroulant.
AES-256 est automatiquement sélectionné par défaut.

11.4.2 Algorithmes SafeGuard Easy

Ci-après, vous trouverez une liste de tous les algorithmes utilisables avec leurs normes correspondantes :

Algorithme	Longueurs de clés
AES-256	32 octets (256 bits)
AES-128	16 octets (128 bits)
Rijndael-256	32 octets (256 bits)
DES	7 octets (56 bits)
3DES	21 octets (168 bits)
IDEA	16 octets (128 bits)
Blowfish-8	32 octets (256 bits)
Blowfish-16	32 octets (256 bits)
STEALTH-40	5 octets (40 bits)
XOR	8 octets (64 bits)

AES-128
L'algorithme Advanced Encryption Standard (AES) est un algorithme de chiffrement qui remplace l'algorithme DES. Pour cet algorithme, on a choisi l'algorithme Rijndael du National Institute for Standards and Technology (USA). Il s'agit d'un algorithme de chiffrement très rapide et très sûr. L'AES-128 travaille avec une clé de 128 bits.

AES-256
Cet algorithme correspond à l'algorithme AES-128, mais il travaille avec une clé de 256 bits et une longueur de bloc de 128 bits.

Rijndael-256
Cet algorithme est une implémentation spécifique de l'AES-256.
Il correspond à l'AES-256, mais il dispose d'une longueur de bloc de 256 bits.

IDEA
IDEA (International Data Encryption Algorithm) a été développé au début des années 90. C'est un algorithme de chiffrement symétrique qui travaille avec une clé de 128 bits. On le considère aujourd'hui comme sûr, tant pour ce qui est des procédés mathématiques que pour la longueur de clé, et il passe pour être extrêmement résistant à toutes les attaques de l'analyse cryptographique. CONSEIL : Si vous avez besoin d'un système très sûr, utilisez les algorithmes IDEA ou AES/Rijndael.

DES
Le DES (Data Encryption Standard) a été mis au point dans les années 70 et utilise une longueur de clé de 56 bits.

3DES (Triple-DES)
Triple-DES ou, en abrégé 3DES, est un perfectionnement du Data Encryption Standard (DES). 2DES utilise trois opérations de chiffrement successives de l'algorithme DES et fonctionne avec une clé de 168 bits. Le procédé 3DES est considéré comme sûr, quoiqu'un peu lent.

Blowfish-16 / Blowfish-8
Blowfish est un algorithme symétrique. Cet un algorithme de chiffrement de bloc de 64 bits qui utilise une longueur de clé de 256 bits.

L'algorithme Blowfish-8 correspond à l'algorithme Blowfish- 16, mais il est réduit à huit rounds. Il utilise une longueur de code de 256 bits.

STEALTH-40
L'algorithme STEALTH utilise une longueur de clé de 40 bits.

XOR
XOR (eXclusive Or opeRation) est un algorithme symétrique qui utilise une longueur de clé de 64 bits. Sa sécurité doit être toutefois considérée comme minime. XOR a recours à une clé de 64 bits.

Conseil : Si vous avez besoin d'un système très sûr, utilisez les algorithmes IDEA ou AES/Rijndael.

Algorithmes spéciaux pour lecteurs de disquettes :

- **DES SB-II**
  L'algorithme DES SB-II est compatible avec le chiffrement de disquettes du SafeBoard II et III ou avec le chiffrement de disquettes du SafeBoard X II et III avec ancienne gestion de clés.
- **XOR SB-I A=B**
  Pour les propriétés, cf.XOR XOR SB-I A=B est compatible avec le chiffreur de disquettes de SafeBoard I (à partir de la version 1.43) C :Crypt et Crypton DOS.

11.4.3 Changement d'algorithme

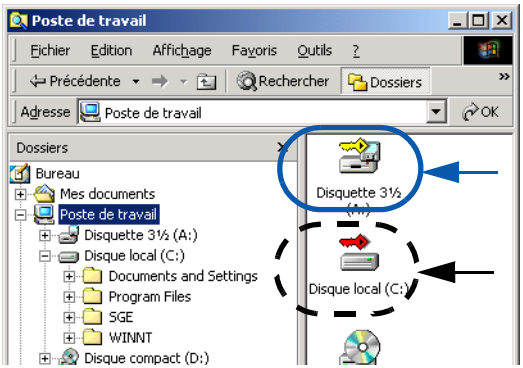
Dès que SafeGuard Easy est installé, il est impossible de changer ensuite les algorithmes. Un autre algorithme requiert une nouvelle installation de SafeGuard Easy.

11.5 Affichage de l'état de chiffrement dans l'Explorateur Windows

L'état de chiffrement des lecteurs est indiqué dans l'Explorateur Windows par une clé en couleur.

Une **clé jaune** indique qu'un lecteur est chiffré.

Une **clé rouge** signifie qu'un lecteur chiffré est en cours de déchiffrement (ou inversement).



Le lecteur est chiffré.

Le lecteur chiffré est en cours déchiffrement.

11.6 Créer une image d'un disque dur chiffré

Les outils de création d'image, tels que Symantec Ghost sont utilisés pour l'installation rapide et automatisée d'un grand nombre de PC, par exemple lorsqu'une grande société d'assurance doit installer 10 000 portables à l'identique par l'intermédiaire d'un logiciel de création d'image, tel que Symantec Ghost. Les outils de création d'image servent en outre à restaurer des partitions endommagées de différents ordinateurs au moyen d'un fichier d'image enregistré sur CD/DVD pour que le système redevienne fonctionnel.

En règle générale toutefois, des problèmes surviennent à la création d'image de disques durs chiffrés (partitions).

Les raisons en sont les suivantes :

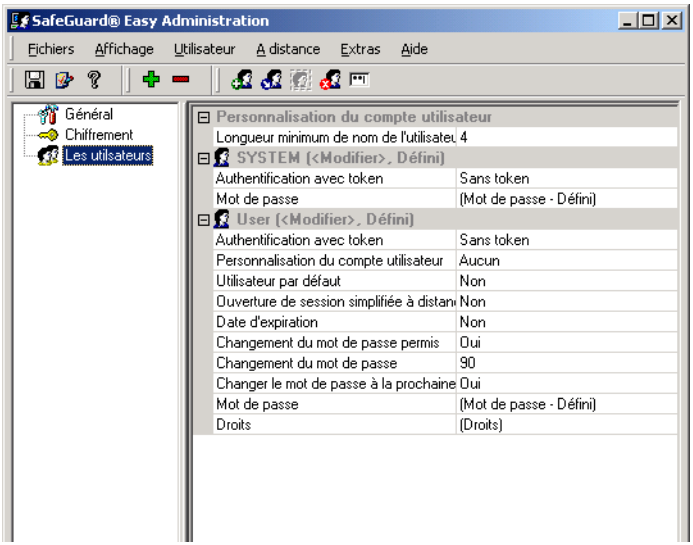
- Une image d'une partition chiffrée ne peut jamais être comprimée. Cela signifie qu'une image d'une partition chiffrée est toujours exactement de la taille de la partition réelle.
- La taille de la partition « imagée » ne doit pas changer. Sinon, il sera impossible de la restaurer.
- Si un disque dur chiffré est cloné avec SafeGuard Easy, toutes les clés de chiffrement créées de façon aléatoire sont identiques.

Dans certaines circonstances, il est quand même possible de sauvegarder des partitions de disques durs sur un disque dur chiffré avec SafeGuard Easy au moyen du logiciel de création d'image (par ex. Norton Ghost de Symantec) et de les restaurer. L'outil de création d'image doit entre autres être en mesure de déchiffrer la partition chiffrée.

Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco http://www.utimaco.com/myutimaco.

Veuillez utiliser la fonction de recherche (« Search ») de la base de données de connaissances pour rechercher des mots-clés comme « Image » ou « Imaging ».

12 Création de profils utilisateur



Vous déterminez ici les utilisateurs autorisés à travailler sur un poste de travail protégé par SafeGuard Easy. Vous pouvez créer ici de nouveaux utilisateurs SafeGuard Easy, modifier des utilisateurs existants ou supprimer des utilisateurs inutiles. Vous déterminez en outre de quels droits et pouvoirs complémentaires les utilisateurs SafeGuard Easy définis disposent.

SafeGuard Easy autorise l'accès au système pour 16 utilisateurs (*AUTOUSER inclus) au maximum. SYSTEM et USER sont définis par défaut, l'utilisateur SYSTEM ne devant jamais être supprimé.

REMARQUES :

L'assistant de configuration pour le déploiement ne montre que SYSTEM et USER si un fichier avec la propriété « Installer » est créée ou quand une configuration de base est utilisée.

12.1 Détermination de tâches d'administration

Une distinction est faite entre les utilisateurs avec tâches d'administration et les utilisateurs sans tâches d'administration.

Les utilisateurs avec tâches d'administration sont

- l'administrateur du système et
- les utilisateurs disposant de fonctions d'administrateur

La personne sans tâches d'administration est

- l'utilisateur.

La fonction d'administrateur peut être séparée de la fonction d'utilisateur, mais également y être associée. Les tâches d'administration peuvent être exécutées par une ou plusieurs personnes. SafeGuard Easy peut par conséquent configurer un ou au maximum 16 utilisateurs (*AUTOUSER inclus).

Selon l'organisation, il peut être toutefois utile de créer un système de rôles à plusieurs niveaux, l'administrateur ou le sous-administrateur du système pouvant disposer de droits différents. La structure hiérarchique ci-dessous est imaginable :

Administrateur du système

Seul l'administrateur du système est en droit d'exécuter toutes les fonctions du programme. Il peut définir un assistant et lui octroyer certains droits d'administration. L'administrateur du système ne doit jamais oublier son mot de passe. Il doit le noter et le conserver dans un endroit sûr.

Sous-administrateur du système

Les sous-administrateurs du système peuvent aider l'utilisateur, quand celui-ci a par ex. oublié son mot de passe. Dans quelle mesure un sous-administrateur peut assister l'administrateur du système dépend des droits qui lui sont octroyés au préalable.

Utilisateurs

L'utilisateur ne peut que visionner ses paramètres. Il ne peut exécuter de façon autonome que la modification du mot de passe d'utilisateur. L'administrateur du système peut en outre lui octroyer certains droits.

12.2 Utilisateurs prédéfinis

SafeGuard Easy fournit les profils d'utilisateurs prédéfinis suivants :

- SYSTEM
- USER
- *AUTOUSER

12.2.1 L'utilisateur SYSTEM

Cet utilisateur est le seul à posséder les droits du niveau hiérarchique le plus élevé. Il ne peut pas modifier ses propres paramètres. Personne ne peut le supprimer ni l'administrer. L'utilisateur SYSTEM est le seul à pouvoir modifier les paramètres de tous les autres profils d'utilisateurs. Seul le responsable au niveau supérieur de la sécurité du système doit par conséquent pouvoir ouvrir une session avec le nom d'utilisateur SYSTEM. Le mot de passe de l'utilisateur SYSTEM ne doit être connu que du responsable au niveau supérieur de la sécurité. Il doit noter ce mot de passe et le conserver p.ex. dans un coffre-fort.

12.2.2 Utilisateur USER

Comme l'utilisateur SYSTEM, l'utilisateur USER est automatiquement présent après une installation de SafeGuard Easy. Ce profil d'utilisateur ne dispose d'aucun droit et peut être supprimé à tout moment.

12.2.3 Utilisateur *AUTOUSER

L'utilisateur *AUTOUSER est particulier. SafeGuard Easy crée – toujours quand la PBA est désactivée – un utilisateur ('*AUTOUSER') et lui attribue un mot de passe aléatoire. Partagé en différents éléments, ce mot de passe est stocké dans le noyau SGE. A l'amorçage, SafeGuard Easy est en mesure de restaurer le mot de passe complet et d'exécuter l'ouverture de session.

Par défaut, *AUTOUSER n'a aucun droit. Les droits suivants peuvent être octroyés :

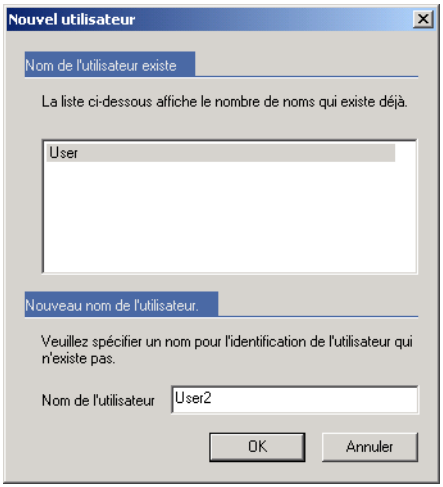
- modification temporaire d'une clé de disquette
- commutation sur le chiffrement de disquette
- modification temporaire d'une clé de périphérique amovible
- commutation sur le chiffrement de périphérique amovible

Quand la PBA est désactivée, tous les utilisateurs ouvrent la session avec les droits octroyés sur le système à l'utilisateur *AUTOUSER. Quand la PBA est de nouveau activée, *AUTOUSER disparaît de la liste des utilisateurs.

12.3 Création d'utilisateurs

Un nouveau profil d'utilisateur est créé dans les programmes d'administration via la page de configuration « Utilisateur.

Après un clic sur l'icône pour la création d'un nouvel utilisateur , la boîte de dialogue *Nouvel utilisateur* s'ouvre.

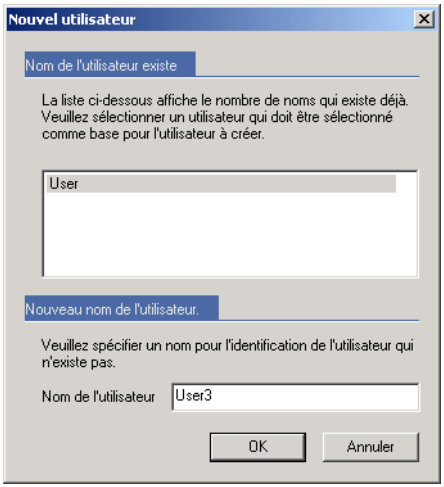


Donnez un nom au nouvel utilisateur en tapant une désignation dans le champ de saisie. Le nom du nouvel utilisateur ne doit pas dépasser **16 caractères** au maximum. Si le nom est déjà attribué, un message d'erreur s'affiche. Par défaut, le nouveau profil ne dispose d'aucun droit.
Pour l'attribution de droits, voir plus loin Attribution de droits.

12.4 Copie d'un utilisateur

Les profils d'utilisateurs similaires peuvent être copiés, puis modifiés si besoin est. Ceci permet de gagner du temps.

Après un clic sur l'icône pour la copie d'un nouvel utilisateur  , la boîte de dialogue *Copier utilisateur* s'ouvre.



Dans la liste d'utilisateurs, sélectionnez le profil que vous souhaitez copier. Tous les profils faisant partie de votre domaine d'administration s'affichent. Vous pouvez cependant ne copier que les profils possédant un niveau hiérarchique inférieur à votre propre profil.

L'utilisateur SYSTEM ne peut pas être copié.

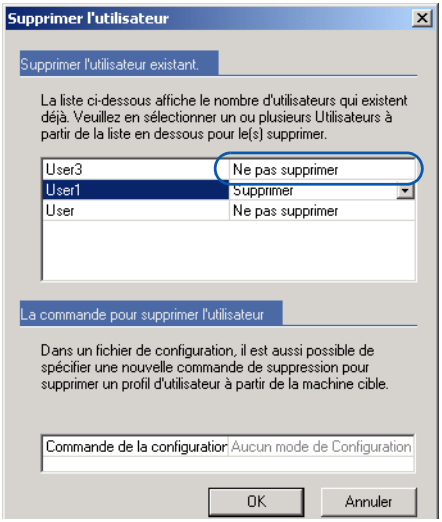
Attribuez un nouveau nom à l'utilisateur et cliquez sur [OK] pour confirmer le nom. Si le nom est déjà attribué, un message d'erreur s'affiche.

Vous pouvez ensuite modifier le nouveau profil à votre convenance.

12.5 Suppression d'un utilisateur

Les profils d'utilisateurs devenus inutiles peuvent être supprimés.

Après un clic sur l'icône pour la suppression d'un utilisateur , la boîte de dialogue *Supprimer l'utilisateur* s'ouvre.



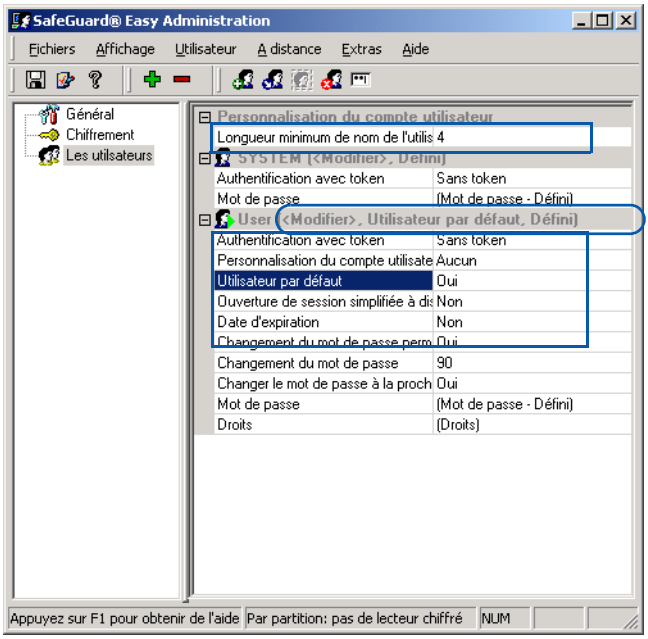
Dans la liste d'utilisateurs, sélectionnez le profil d'utilisateur que vous souhaitez supprimer. Tous les profils faisant partie de votre domaine d'administration s'affichent. Ouvrez le menu déroulant derrière le nom d'utilisateur et choisissez la propriété « Supprimer » correspondant au nom d'utilisateur à supprimer.

Vous pouvez cependant ne supprimer que les profils possédant un niveau hiérarchique inférieur à votre propre profil.

La suppression d'un utilisateur est irréversible.

12.6 Caractéristiques d'utilisateur

On reconnaît les droits attribués à un utilisateur aux extensions derrière son nom.



12.6.1 Longueur minimum du nom de l'utilisateur

Dans ce champ, vous indiquez le nombre minimum de caractères que doit comporter un nom d'utilisateur. Vous pouvez saisir le nombre souhaité des caractères soit directement, soit en augmentant ou diminuant la valeur à l'aide des touches de direction. La valeur pour la longueur du mot de passe peut se situer entre un et 16 caractères.

12.6.2 Authentification avec un jeton

Ce paramètre indique si un utilisateur doit ouvrir une session avec un jeton ou non. Cette option ne peut être sélectionnée que si la prise en charge des jetons a été installée avec l'option « En option » lors de l'installation. Vous trouverez des détails sur la prise en charge des jeton dans la section 'Support Token'.

12.6.3 Utilisateur par défaut (mot de passe uniquement)

Tout utilisateur de SafeGuard Easy peut être défini comme utilisateur par défaut, à l'exception de l'utilisateur SYSTEM. Pour se connecter, l'utilisateur par défaut doit seulement entrer le mot de passe SafeGuard Easy. Si d'autres utilisateurs que l'utilisateur par défaut souhaitent se connecter au poste de travail, ils doivent activer la fonction de « connexion étendue » (pendant la phase PBA, en appuyant sur [F2]).

12.6.4 Génération d'un code C/R abrége

Cette fonction est particulièrement adaptée aux administrateurs de sous-systèmes qui sont chargés de l'administration à distance.

Cette propriété influe sur la longueur du code de réponse échangé pendant une procédure Requête/Réponse.

Les utilisateurs disposant de la propriété « Issue abbreviated C/R Code » (Code C/R abrégé) et l'utilisateur SYSTÈME génèrent des codes de réponse courts qui ne comptent que 30 caractères, tandis que les utilisateurs « ordinaires » de SafeGuard Easy génèrent des codes de réponse qui comptent 56 caractères. Quand vous le tapez ou le transmettez à l'utilisateur, ceci peut entraîner un pourcentage d'erreur élevé.

Pour plus de détails sur la procédure Requête/Réponse, veuillez consulter le chapitre 'Administration à distance'.

12.6.5 Personnalisation du compte utilisateur

Les modèles ont une fonction bien particulière : Ils servent de profils d'utilisateur de base et sont en règle générale utilisés quand SafeGuard Easy doit être installé sur plusieurs ordinateurs avec un fichier de configuration. S'il n'existait pas de modèles, les utilisateurs posséderaient le même ID d'utilisateur sur tous les ordinateurs. Ceci va cependant à l'encontre, dans de nombreux cas, des directives en matière d'organisation dans de nombreuses entreprises, exigeant la présence de nom/mots de passe d'utilisateur individuels, p.ex. nom, code personnel, etc. Dans de tels environnements, un profil d'utilisateur SafeGuard Easy peut être alors défini comme modèle. Il en résulte que cet utilisateur de SafeGuard Easy reçoit un nouveau nom d'utilisateur, par conséquent personnalisé, à la première ouverture de session avec PBA.

La fonction de modèle est utilisée comme suit :

L'administrateur crée un utilisateur SGE et le définit comme modèle. SafeGuard Easy est installé avec ces paramètres sur l'ordinateur de destination. Le nom d'utilisateur et le mot de passe de l'utilisateur défini comme modèle sont indiqués par l'administrateur à l'utilisateur de l'ordinateur de destination à la première ouverture de session. Quand un utilisateur ouvre alors une session pour la première fois, il est tenu d'entrer ces données d'accès sur l'écran d'ouverture de session. Il est ensuite invité à entrer son nouveau nom d'utilisateur et son nouveau mot de passe avec lesquels il devra également se connecter à la prochaine ouverture de session.

Un modèle peut servir soit à renommer, soit à copier un utilisateur.

Renommer un modèle

Si vous souhaitez absolument vous assurer qu'un seul utilisateur par modèle ouvre une session sur (p.ex. ordinateurs portables pour collaborateurs des services extérieurs), attribuez au modèle la propriété « Renommer ». Le modèle est « écrasé » avec les nouvelles données d'utilisateur. Une ouverture de session avec les données d'accès connus n'est plus possible, celles-ci ayant été remplacées par celle de l'utilisateur connecté.

Copier un modèle

Si l'attribut « Copier » est sélectionné, le nouveau nom d'utilisateur est ajouté à la liste des utilisateurs de SafeGuard Easy, mais le modèle reste conservé. Les autres utilisateurs peuvent ouvrir une session avec les données d'accès du modèle. Si SYSTEM et UTILISATEUR sont définis par défaut, 13 autres utilisateurs peuvent être également créés.
Pour des raisons de sécurité, il est conseillé de n'utiliser les modèles qu'avec la fonction « Renommer ».

12.6.6 Date d'expiration

La date d'expiration indique la durée de validité maximum d'un profil d'utilisateur SGE. Vous pouvez spécifier un jour de référence (ou une période) auquel l'utilisateur pourra ouvrir une dernière session dans le système. Vous pouvez taper directement la date ou la période.

Ce paramètre est notamment utile dans les cas où l'utilisation d'un poste de travail n'est prévue que pour un certain temps, p.ex. employés temporaires ou étudiants, etc. Une fois le délai écoulé, le poste de travail est verrouillé pour l'utilisateur.

Ce paramètre n'a aucun effet sur l'utilisateur SYSTEM.

12.7 Droits utilisateur

Réfléchissez aux droits d'accès susceptibles d'être octroyés aux différents utilisateurs de SafeGuard Easy. Pour des raisons de sécurité, l'attribution des droits pour les différents utilisateurs doit être mûrement réfléchie.

Vous pouvez autoriser à des utilisateurs l'accès à des paramètres temporaires et permanents. Les paramètres temporaires ne sont valables que pour la durée d'une ouverture de session. Après un redémarrage de l'ordinateur, ils ne sont plus valides et les paramètres du système sont rétablis. Les paramètres permanents sont ceux qui restent conservés même après redémarrage du système.

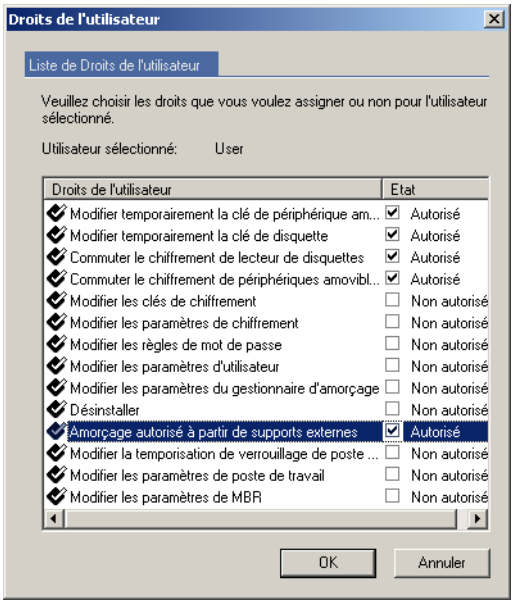
Les droits suivants peuvent être octroyés :

Modifier temporairement la clé de périphérique amovible	Permet de modifier la clé de périphériques amovibles pendant une session de travail.
Modifier temporairement la clé de disquette	Permet de modifier la clé de disquettes pendant une session de travail.
Commuter le chiffrement de disquettes	Permet d'activer ou de désactiver le chiffrement de disquettes.
Commuter le chiffrement de périphériques amovibles	Permet d'activer ou de désactiver le chiffrement de périphériques amovibles
Modifier les clés de chiffrement	Permet de modifier les clés pour tous les lecteurs. Ceci n'est pas valable pour le disque dur quand il est chiffré.
Modifier les clés de chiffrement	Permet de modifier l'état de chiffrement et les clés.
Modifier les règles de mot de passe	Permet de modifier les règles générales des mots de passe.

Modifier les paramètres de l'utilisateur	Permet de modifier les paramètres des utilisateurs. Doit être défini pour octroyer des droits à d'autres utilisateurs !
Modifier le Gestionnaire d'amorçage	Permet de modifier les paramètres des Gestionnaire d'amorçage
Pour une désinstallation	Permet de désinstaller SafeGuard Easy
Amorçage autorisé à partir de supports externes	Permet de démarrer un système protégé par SafeGuard Easy à partir de la disquette/CD/clé USB.
Modification générale	Permet de modifier les paramètres généraux suivants : - Token - Wake On LAN - Modifier mot de passe au démarrage du système - Saisie de mot de passe masquée - Identification
Modifier les paramètres MBR	Permet de modifier tous les paramètres pour le Master Boot Record.

12.7.1 Octroi de droits d'utilisateurs

Après un double-clic sur « Droits de l'utilisateur », tous les droits attribuables sont affichés. Le double-clic sur un droit commute l'état préalable « Autorisé » en état « Non autorisé » et inversement



Les nouveaux utilisateurs n'ont aucun droit lors de leur création. Seul l'utilisateur SYSTÈME dispose de tous les droits. Les droits auxquels l'utilisateur n'a pas accès ne sont pas affichés dans l'aperçu et ne peuvent pas être modifiés.

12.7.2 Transfert de droits d'utilisateurs

Un utilisateur peut également transférer des droits à d'autres utilisateurs, si tant est qu'il en dispose lui-même. Si un administrateur (par ex. un sous-administrateur système) souhaite modifier des propres droits, il ne peut pas le faire lui-même. Il doit s'adresser à un administrateur plus haut que lui dans la hiérarchie (p.ex. l'administrateur système) et lui demander de procéder aux modifications souhaitées.

Pour transférer ses propres droits à d'autres utilisateurs, un profil d'utilisateur doit avoir la propriété « Modifier les paramètres d'utilisateur ».

13 Paramètres du mot de passe

Le mot de passe joue un rôle central dans SafeGuard Easy : A partir du mot de passe SafeGuard Easy saisi à l'authentification avant amorçage, la clé de déchiffrement d'un disque dur chiffré, requise pour l'amorçage, est calculée.

Le mot de passe SafeGuard Easy doit être choisi avec circonspection. Les utilisateurs préfèrent généralement utiliser les mêmes mots de passe, ou mots de passe faibles, tels que leur prénom ou nom, leur nom de société, les séquences de lettres ou de numéros, etc. Lorsqu'un mot de passe SafeGuard Easy est trop évident, il risque d'être découvert facilement par une personne malveillante. Pour définir des restrictions à l'attribution de mots de passe, il convient donc de bien réfléchir et d'essayer.

13.1 Règles générales de mot de passe internes dans SafeGuard Easy

Pour des raisons de sécurité, certaines règles pour tous les mots de passe des utilisateurs sont prescrites après l'installation.

Un mot de passe SafeGuard Easy doit …

- comporter au maximum 16 caractères.

Un mot de passe SafeGuard Easy ne doit en aucun cas …

- comporter 50 % (ou plus) de caractères identiques (par ex. « aaabba », « 222122 »).
- comporter de caractères et/ou chiffres consécutifs (par ex. « abcdef », « 1234567 »).
- comporter de séquences de clavier (par ex. « asdfghj »).
- être identique avec les noms d'utilisateurs SafeGuard Easy (exception : mot de passe pour l'utilisateur « SYSTEM »).
- être similaire aux noms d'utilisateurs SafeGuard Easy (exception : mot de passe pour l'utilisateur « SYSTEM »).
- être similaire à l'ancien mot de passe.

Le terme « Similaire » signifie ici que la séquence de caractères du nouveau mot de passe doit se différencier d'au moins 20 % de l'ancien mot de passe / nom d'utilisateur. Par exemple, l'utilisateur « UTILISATEUR » SafeGuard Easy peut utiliser le mot de passe « U2TILISATEUR13 », « U345TILISATEUR », etc., mais SafeGuard Easy refuse les mots de passe tels que « UTILISATEUR1 », « UTILISATEUR2 », « UTILISATEURab », « 12UTILISATEUR », « 1UTILISATEURF », etc.

13.2 Les clés autorisées pour le mot de passe SafeGuard Easy

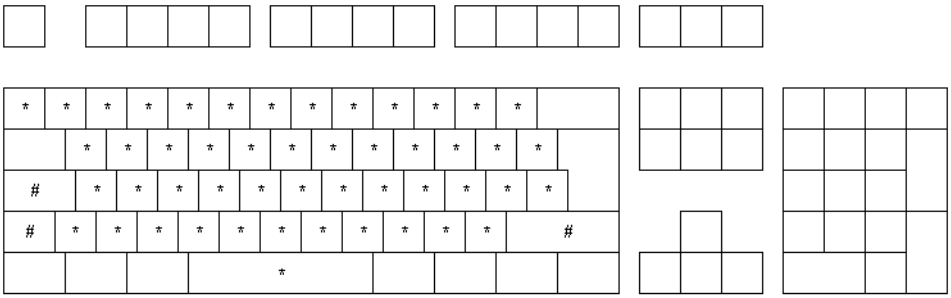
Le mot de passe SafeGuard Easy peut se composer de caractères alphanumériques et de signes de ponctuation.

SafeGuard Easy accepte

- toutes les touches signalées par « * » dans l'illustration.
- les touches [Maj] et [Verr Maj] (signalées par « # » dans l'illustration).

SafeGuard Easy n'accepte pas

- la touche [Maj] lorsque la touche [Verr Maj] est déjà enfoncée
- la touche [Alt]
- la touche [Ctrl]
- les touches du pavé numérique
- les touches de fonction (par ex. F1, F2)
- les touches de direction

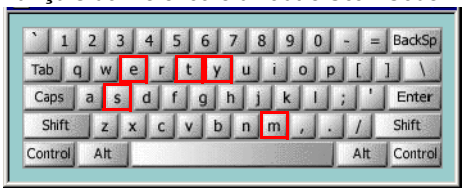


13.3 Configuration de SafeGuard Easy pour l'utilisation dans un contexte international

SafeGuard Easy enregistre toutes les séquences de caractères en format « Scan Code », étant donné qu'aucun pilote de clavier n'est normalement chargé dans la phase avant l'amorçage. Le « Scancode » est un numéro de code (Scancode hexadécimal) que le clavier transmet à l'ordinateur à l'appui sur une touche. Ce code est indépendant des lettres, chiffres ou symbole illustrés sur la touche. Il représente un caractère spécial pour la touche proprement dite et il est toujours le même pour une touche donnée.

13.3.1 Diverses configurations de clavier

SafeGuard Easy enregistre toutes les séquences de caractères en format « Scan Code ». Cela signifie que par exemple « system » sur un **clavier français** donne encore un autre Scan Code : 1f-15-1f-14-12-27



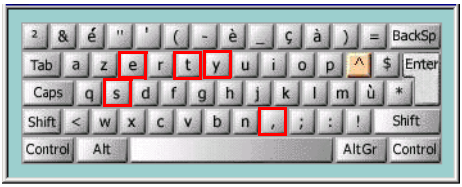
La séquence Scan Code pour « system » avec un clavier allemand est : 1 f-2d-1f-14-12-32

REMARQUES :

Y et le Z sont permutés ! L'utilisateur doit taper « szstem » pour s'authentifier avec succès.

« System » sur un clavier anglais donne le Scan Code suivant 1 f-15-1f-14-12-**27**.

Sur un clavier français, l'utilisateur doit donc taper « syste, » pour s'authentifier avec succès.



Vous trouverez d'autres configurations de clavier à l'adresse **http://www.microsoft.com/globaldev/reference/keyboards.mspx**.

13.3.2 Créations de données internationales unitaires pour SafeGuard Easy

Dès que SafeGuard Easy est utilisé dans un contacte international, il convient de s'assurer que mot de passe et code peuvent être saisis de façon correcte sur tous les claviers disponibles. Pour une utilisation internationale, il faut en particulier veiller à ce que les profils d'utilisateur SafeGuard Easy remplissent les tâches d'administration.

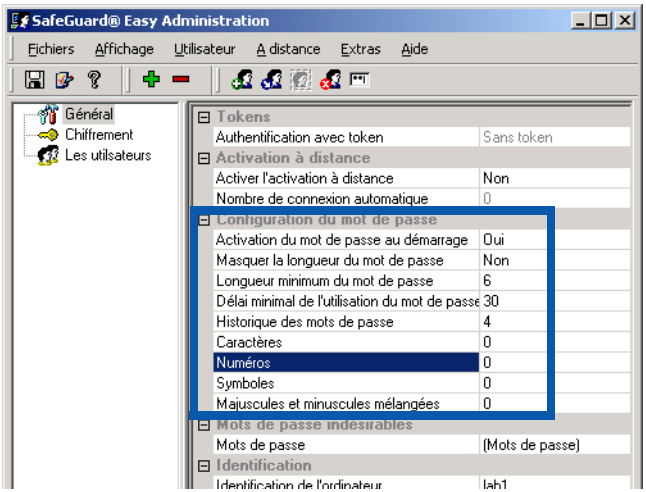
Il faudrait mentionner par exemple la procédure Requête/Réponse, si l'utilisateur appelant et l'utilisateur helpdesk qui fait office d'assistant de codes de réponse, utilisent différents claviers.

Si les données SGE (ou bien : séquences de touches) sont créées à partir d'une combinaison des 21 touches suivantes, il y a de fortes chances pour qu'elles puissent être utilisées sans problème dans un contexte international.

Valeurs inscrites sur les touches	Scan Code hexadécimal
b	30
c	2E
d	20
e	12
f	21
g	22
h	23
i	17
j	24
k	25
l	26
n	31
o	18
p	19
r	13
s	1F
t	14
u	16
x	2D
v	2F
[Espace]	39

13.4 Règles générales de mots de passe

Les règles de mot de passe générales permettent de définir des modèles pour la composition de mots de passe, comme par exemple le pourcentage de lettres et de chiffres ou leur longueur maximum.
Ces modèles sont valables pour chaque utilisateur SGE et aucun mot de passe ne correspondant pas à ces standards n'est accepté.



13.4.1 Activation du mot de passe au démarrage du système

Voir “Authentification avant l’amorçage (PBA)” .

13.4.2 Entrée de mot de passe masqué

Contrairement aux procédures d’ouverture de session conventionnelles, aucun caractère de remplacement (par ex. *) n’est affiché à la saisie du mot de passe SGE. Ceci signifie, par exemple, que d’autres personnes peuvent voir le nombre de caractères entrés. Si cette option est activée, le déplacement du curseur est également désactivé.
Veuillez aviser vos utilisateurs qu’aucun caractère n’apparaît à l’appui sur les touches. Toutefois, les « * » permettent d’éviter les erreurs de saisie.

13.4.3 Longueur minimum du mot de passe

Vous devez spécifier la longueur du mot de passe dans ce champ. Dans ce champ, vous déterminez le nombre de caractères minimum que le mot de passe doit comporter en cas de modification par l’utilisateur.

Vous pouvez saisir le nombre souhaité des caractères soit directement, soit en augmentant ou diminuant la valeur à l’aide des touches de direction. Le mot de passe peut compter entre 1 et 16 caractères.
La valeur par défaut est 6.

13.4.4 Délai minimal de l’utilisation du mot de passe

Le délai d’utilisation du mot de passe a une durée minimale en jours. Au cours de cette période, l’utilisateur ne doit pas modifier le mot de passe. Cette option vise à empêcher une réinitialisation du mot de passe par l’utilisateur.

13.4.5 Historique des mots de passe

Pour éviter que l'utilisateur passe en permanence d'un mot de passe à l'autre, vous pouvez définir un nombre de générations de mot de passe plus élevé. Chaque mot de passe est comparé au mot de passe utilisé dans le passé et refusé quand il est identique à un mot de passe existant. Le nombre de mots de passe utilisés dans le passé et enregistrés pour comparaison est régulé par ce paramètre.

Vous pouvez enregistrer jusqu'à 16 mots de passe utilisateurs. Cliquez sur le champ de saisie, puis définissez la valeur, soit en tapant le mot de passe, soit en cliquant sur les touches de direction. La définition du nombre de générations de mot de passe est particulièrement important si vous activez le paramètre « Changer le mot de passe après 'n' jours » (voir 'Changement du mot de passe après 'n' jours').

Exemple :

Vous avez défini à 4 le nombre de générations de mot de passe pour l'utilisateur Dupond, et à 30 celui des jours au bout desquels l'utilisateur doit modifier son mot de passe. Jusqu'ici, Monsieur Dupond ouvrait sa session avec le mot de passe SafeGuard Easy *« Informatique ». Ce délai étant écoulé*, il est invité, dans l'écran d'ouverture de session SafeGuard Easy (PBA), à modifier son mot de passe. Par exemple, l'utilisateur Miller tape « Ordinateur » une deuxième fois et reçoit un message d'erreur indiquant que ce mot de passe a déjà été utilisé et qu'il doit en choisir un autre. L'utilisateur Miller doit attendre la quatrième invite pour utiliser de nouveau « Ordinateur » (dans la mesure où l'option de génération de mots de passe est définie sur 4).

13.4.6 Règles de syntaxe (caractères, chiffres, symboles, inversion de casse)

Pour augmenter l'efficacité des mots de passe, vous pouvez faire appel à un mélange de lettres et de chiffres (et/ou de symboles). Le nombre indiqué définit toujours une **valeur minimum**.

Les **symboles** sont des caractères spéciaux comme par ex.
* # !"§$%&/() etc.

Majuscules/minuscules signifie qu'un nombre égal de majuscules et de minuscules doit être utilisé.

Exemple :

L'**exemple** suivant montre l'utilisation correcte des règles de syntaxe :

Spécification

lettres : 1
chiffres : 2
symboles : 1
Majuscules/minuscules : 2

Résultat :

- AAaa12# peut être utilisé
- aaAA123## peut être utilisé
- 3456## est refusé
- AAB1# est refusé

Les mots de passe déjà utilisés par des utilisateurs restent valables, même s'ils ne correspondent pas aux spécifications. Les règles n'interviennent que lorsque l'utilisateur modifie son mot de passe.

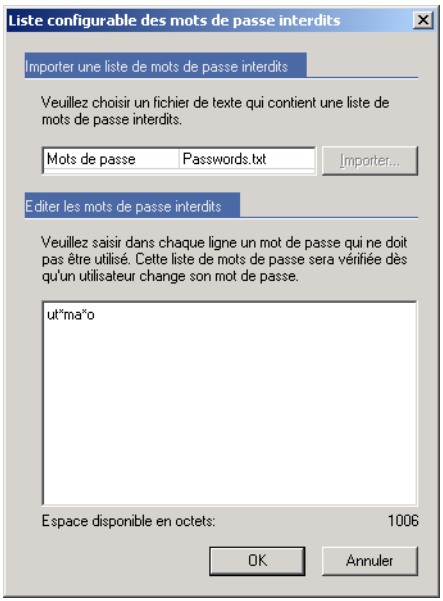
13.5 Mots de passe indésirables

Les mots de passe indésirables concernent certaines chaînes de caractères dont l'emploi dans le mot de passe SGE est exclu. Chaque nouveau mot de passe est comparé à une liste et n'est accepté que lorsqu'il n'y est pas contenu.

Vous pouvez importer une liste existante ou entrer vous-même des mots de passe interdits.

13.5.1 Définition de mots de passe interdits

Double-cliquez sur « Mots de passe », entrez des combinaisons de chiffres indésirables sous « Éditer les mots de passe interdits » et séparez-les avec Ctrl+ Entrée].



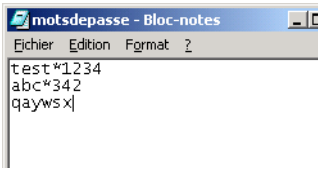
Dans la liste, entrez des mots de passe triviaux, comme par ex. Test, Système, Utilisateur, etc. Tous les mots de passe similaires à un mot de passe interdit sont refusés. Le terme « Similaire » signifie ici que la séquence de caractères du mot de passe doit se différencier d'au moins 20 % du mot de passe interdit. Si « Tester » par exemple se trouve dans la liste, l'utilisateur peut saisir le mot de passe « Tester1234 », tandis que « Tester12 » est refusé par SafeGuard Easy.

Vous pouvez également utiliser des caractères de remplacement pour la définition. Seul l'astérisque (*) est accepté comme caractère de remplacement). Remplace **un** caractère au choix dans le mot de passe. « ut*ma*o » par ex. interdit les mots de passe comme « utimaco », « ut1ma2o », etc.

AVERTISSEMENT :
Si vous ajoutez un ou plusieurs caractères de remplacement dans la liste des mots de passe interdits, des utilisateurs ne peuvent plus ouvrir de session dans le système après une modification forcée du mot de passe.

13.5.2 Importation d'une liste de mots de passe

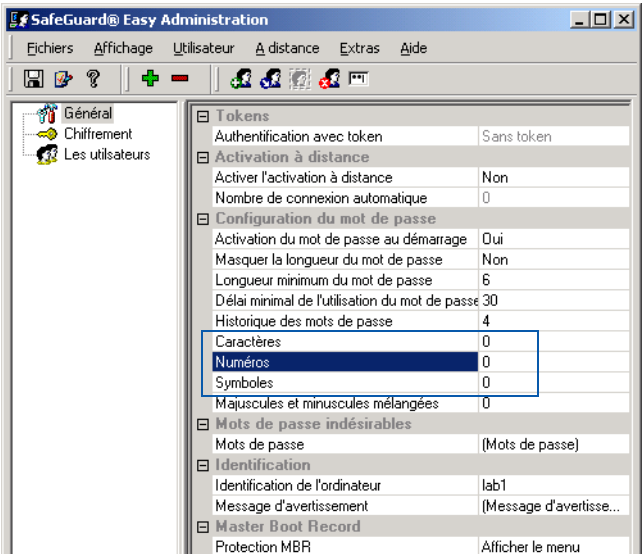
Si une liste de mots de passe indésirables existe déjà, elle peut être importée. Ceci vous permet d'utiliser la même liste sur plusieurs postes de travail. La liste peut être éditée avec n'importe quel éditeur et pourrait avoir l'aspect suivant :



Les différents mots de passe sont séparés par un espace ou par un saut de ligne.

REMARQUE :
Les utilisateurs ne doivent en aucun cas avoir accès à ce fichier !

13.6 Règles de mot de passe spécifiques à l'utilisateur



Les règles de mot de passe spécifiques à l'utilisateur s'appliquent aux options de changement de mot de passe.

13.6.1 Autorisation de la modification de mot de passe

Cette option indique si un utilisateur peut modifier ou non son mot de passe SafeGuard Easy dans la PBA ou l'administration.

13.6.2 Changement du mot de passe après ‘n’ jours

Un mot de passe SafeGuard Easy est valide sans limite de durée. Le risque d’être découvert un jour ou l’autre est toutefois très élevé. Pour minimiser ce risque, vous pouvez spécifier qu’un de ces utilisateurs doit changer son mot de passe au bout d’un certain nombre de jours.

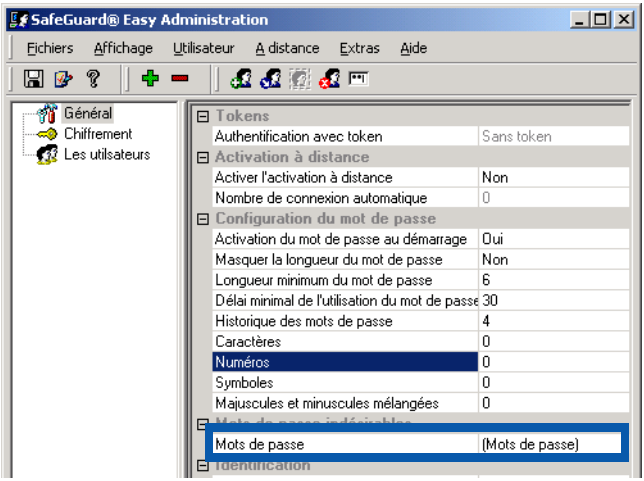
Avec les touches fléchées ou par entrée directe via le clavier, définissez une période à la fin de laquelle le mot de passe doit être changé.

La période de validité des mots de passe peut aller de 1 à 180 jours. La période par défaut est de 90 jours. Une fois le délai écoulé, l’utilisateur est tenu de modifier son mot de passe à la prochaine ouverture de session.

13.6.3 Changement du mot de passe à la prochaine ouverture de session

L’utilisateur doit modifier son mot de passe SafeGuard Easy à la prochaine ouverture de session. Pour utiliser cette fonction, l’authentification avant amorçage doit être activée.

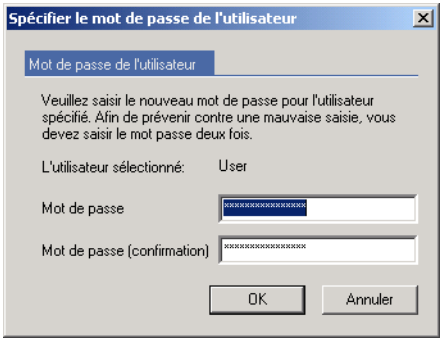
13.7 Définition de mot de passe



Les mots de passe d'utilisateur doivent être choisis avec circonspection pour ne pas être aisément devinés. Les mots de passe peuvent contenir des lettres majuscules ou minuscules non accentuées, des chiffres et des caractères spéciaux (!„§$%&/()*+;,:._-), à condition que cette combinaison n'ait pas été interdite par les règles générales de mot de passe.

Les chiffres du pavé numérique ne doivent pas être utilisés.

Un double-clic sur « Mot de passe » ouvre la boîte de dialogue dans laquelle le mot de passe est défini.



Tapez le mot de passe souhaité dans la ligne supérieure et tapez-le de nouveau dans le champ Confirmation. La répétition est nécessaire pour éviter les fautes de frappe. La correspondance des caractères tapés est vérifiée et un message d'erreur apparaît quand les mots de passe ne correspondent pas ou lorsqu'ils sont banals (par ex. « 12345 » ou « AAABBB »). Pour des raisons de sécurité, le mot de passe n'est affiché qu'avec des astérisques (*). Pour corriger les entrées, veuillez utiliser la touche Reset.

Il n'est pas possible de contourner la seconde saisie du mot de passe en utilisant la fonction « Copier-Coller ».

14 Double amorçage/ Gestionnaire d'amorçage

Double amorçage est une variante d'installation qui vous permet de réaliser une séparation claire entre les partitions professionnelle et privée d'un ordinateur.

14.1 Mode de fonctionnement

Pour la protection de données professionnelles confidentielles, la fonction de double amorçage requiert deux partitions primaires, avec chacune un système d'exploitation exécutable. Le double amorçage chiffre une partition (partition professionnelle), tandis que l'autre reste non chiffrée (partition privée). La partition professionnelle n'est accessible qu'avec le mot de passe SafeGuard Easy. La partition privée n'est en aucun cas protégée par SafeGuard Easy Les partitions professionnelles et privées sont mutuellement invisibles et aucune donnée sensible de la partition professionnelle ne peut être transférée sur la partition privée non chiffrée. Quand l'échange de données entre la partition chiffrée et la partition non chiffrée est souhaitée, une option le permet.

Via le gestionnaire d'amorçage SafeGuard Easy, vous décidez de la partition (professionnelle/privée) initialisée au démarrage de l'ordinateur). Un menu de gestion d'amorçage apparaît à l'écran et montre les différents systèmes d'exploitation. La partition chiffrée requiert une authentification avec le mot de passe SafeGuard Easy dans la PBA Pour cette raison, il convient de déterminer à partir de quel système d'exploitation le démarrage doit s'effectuer avant l'authentification avant amorçage (éventuelle).

L'installation avec double amorçage requiert l'activation du chiffrement de disquettes et de périphériques amovibles (lecteurs ZIP, MO). Les disquettes et les périphériques amovibles restent chiffrés dès qu'on démarre l'ordinateur à partir de la partition chiffrée (domaine professionnel).

Si vous sélectionnez la partition privée en texte clair, les lecteurs de disquette et amovibles ne sont pas chiffrés, mais les utilisateurs de SafeGuard Easy qui disposent des droits utilisateurs adéquats peuvent activer ou désactiver le chiffrement de façon temporaire.

REMARQUE :
D'autres partitions présentes sur l'ordinateur/Notebook peuvent être chiffrées ou rester non chiffrées.

14.2 Conditions

- Une installation avec double amorçage n'est autorisée que lorsqu'**un seul disque dur** est connecté. Si deux disques durs sont détectés, l'option Double amorçage est affichée en gris. D'autres disques durs peuvent être connectés après l'installation à double amorçage, mais aucun support SafeGuard Easy ne sera toutefois garanti en ce qui concerne le chiffrement pour ce disque dur supplémentaire.
- Avant l'installation **de SafeGuard Easy le disque dur existant doit comporter au moins deux partitions primaires avec respectivement un système d'exploitation permettant l'amorçage.**
- AVANT l'installation de SafeGuard Easy, tous les systèmes d'exploitation (**seul Windows est pris en charge !**) doivent être installés et le partitionnement du disque dur déterminé !). Les changements postérieurs ne sont pas recommandés.

14.3 Exemple

Configuration de départ

C:\	D:\	E:\	F:\	G:\
partition primaire	partition primaire	disque logique dans partition étendue	disque logique dans partition étendue	disque logique dans partition étendue
chiffré	non chiffrée	chiffré	non chiffrée	non chiffrée
disque d'amorçage 1	Disque d'amorçage 2			

Démarrage du disque d'amorçage chiffré 1

C:\	D:\	E:\	F:\	
partition primaire	disque logique dans partition étendue	disque logique dans partition étendue	disque logique dans partition étendue	
chiffré	chiffré	non chiffrée	non chiffrée	non chiffrée
disque d'amorçage 1				Disque d'amorçage 2
lisible	lisible	*non lisible*	*non lisible*	*invisible*

Démarrage du disque d'amorçage non chiffré 2

C:\	D:\	E:\	F:\	
partition primaire	disque logique dans partition étendue	disque logique dans partition étendue	disque logique dans partition étendue	
non chiffrée	chiffré	non chiffrée	non chiffrée	chiffré
Disque d'amorçage 2				disque d'amorçage 1
lisible	*non lisible*	lisible	lisible	*invisible*

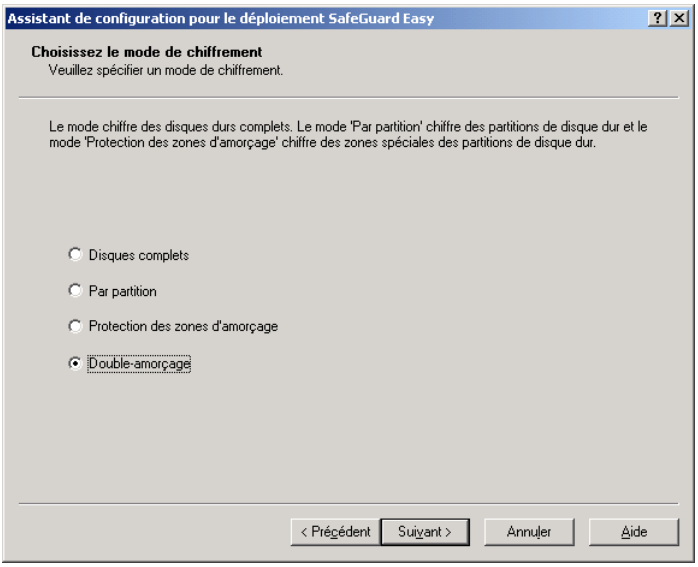
14.4 Configuration Double amorçage

1. Créez deux partitions primaires sur le disque dur de l'ordinateur et installez un système d'amorçage permettant l'amorçage sur chaque partition.

2. Amorcez ensuite la partition professionnelle.

3. Procédez à l'installation locale de SafeGuard Easy. Confirmez toutes les entrées qui s'affichent en cliquant sur Suivant.

4. Dans la boîte de dialogue « Mode de chiffrement », marquez « Double amorçage ».



5. Dans les outils d'administration de SafeGuard Easy, sélectionnez le dossier **Chiffrement**. Outre la partition d'amorçage Windows déjà marquée comme chiffrée dans la configuration de base (= partition primaire contenant les fichiers requis pour l'amorçage tels que Ntldr, Boot.ini, Ntdetect.com), les disques suivants doivent être chiffrés :

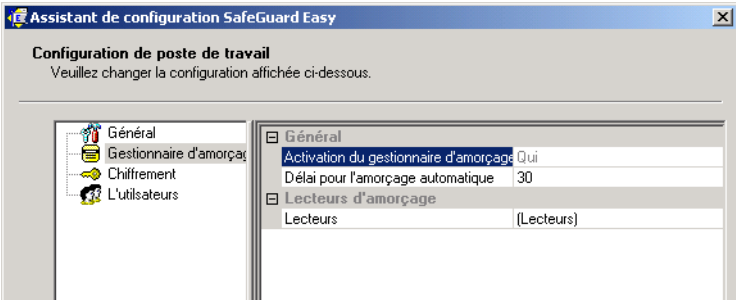
   - le disque système Windows contenant les fichiers système de Windows (peut être identique avec la partition d'amorçage),
   - le lecteur contenant le dossier d'installation de SafeGuard Easy. Ceci assure l'accès aux fichiers SafeGuard Easy.
   - Une installation Double amorçage requiert également le chiffrement de disquettes et de périphériques amovibles.

6. Le mode Double amorçage active automatiquement le gestionnaire d'amorçage SafeGuard Easy. Passez au dossier « Gestionnaire d'amorçage » et procédez aux réglages de précision.

REMARQUE :
A la sélection de partitions interdites d'accès, une boîte de dialogue affichant « Voulez-vous formater la partition » apparaît après l'installation. Si vous cliquez sur [OUI], les données sont perdues.

14.5 Configuration de Boot Manager

Le gestionnaire d'amorçage est configuré via le dossier du même nom dans les outils d'administration. La page de configuration n'est cependant affichée que lorsque le mode de chiffrement « Double amorçage » est sélectionné.



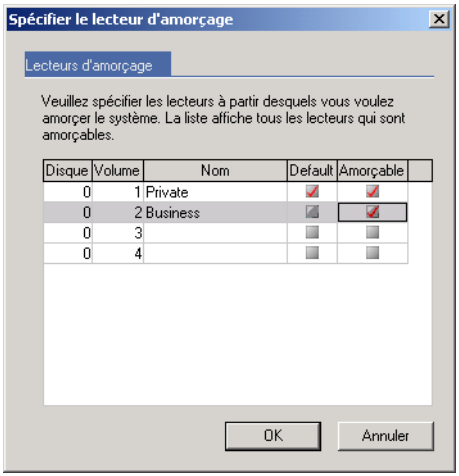
14.5.1 Paramètres généraux

- **Activation du gestionnaire d'amorçage :**
  Indique si le gestionnaire d'amorçage est activé/désactivé. Le paramètre est activé par défaut lors d'une installation Double amorçage.

- **Autoboot time-out**
  (Temporisation du démarrage automatique) Le lecteur de démarrage par défaut (défini dans la section « Boot Drives » - Lecteurs de démarrage) est démarré automatiquement lorsque le système est activé, sauf si l'utilisateur sélectionne un autre lecteur de démarrage pendant une période définie. Cette durée est définie dans le champ « Timeout. S'il n'y a pas de disque par défaut, le système d'exploitation amorce la première partition primaire.

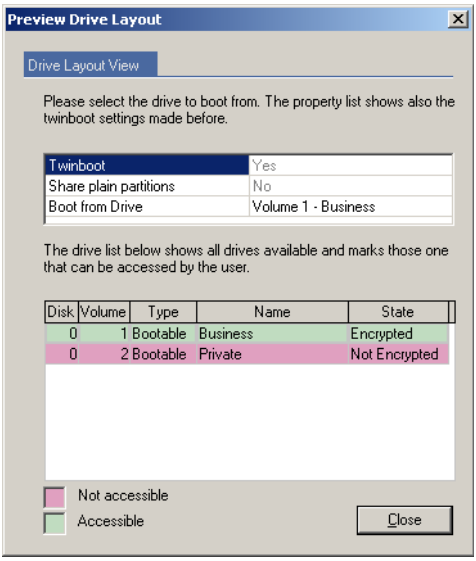
14.5.2 Lecteurs d'amorçage

Après un double-clic sur les lecteurs d'amorçage ouvre la boîte de dialogue du même nom. Les propriétés du gestionnaire d'amorçage y sont définies.



Une liste affichant toutes les **partitions primaires** de l'ordinateur apparaît. Pour différencier les différents lecteurs amorçables dans le menu gestionnaire d'amorçage, il est recommandé d'entrer tout d'abord des noms d'amorçage « **sans équivoque** » (maximum de 40 caractères, par ex. « Privé »). Les noms spécifiés sont plus tard affichés dans le menu de sélection du gestionnaire d'amorçage. Pour qu'un disque puisse être affiché dans le gestionnaire d'amorçage SafeGuard Easy, il doit être marqué comme « **amorçable** ». Un des lecteurs affichés doit en outre être spécifié comme **lecteur par défaut**, automatiquement appelé au démarrage du système quand rien n'a été sélectionné dans le gestionnaire d'amorçage.

Une prévisualisation permet d'afficher séparément le stade de chiffrement et l'accès après sélection de la partition d'amorçage.



Double amorçage :
Indique si ce mode de chiffrement est actif.

Partitions en texte clair visibles (défini sous Chiffrement / Double amorçage / Partager partitions non chiffrées) :
Indique si l'échange de données entre partitions chiffrées et non chiffrées est possible.

Lecteur d'amorçage :
Indique les droits d'accès, selon le disque de démarrage, mais SANS effet sur les paramètres définis sous « Déterminer disques de démarrage ».

REMARQUES :

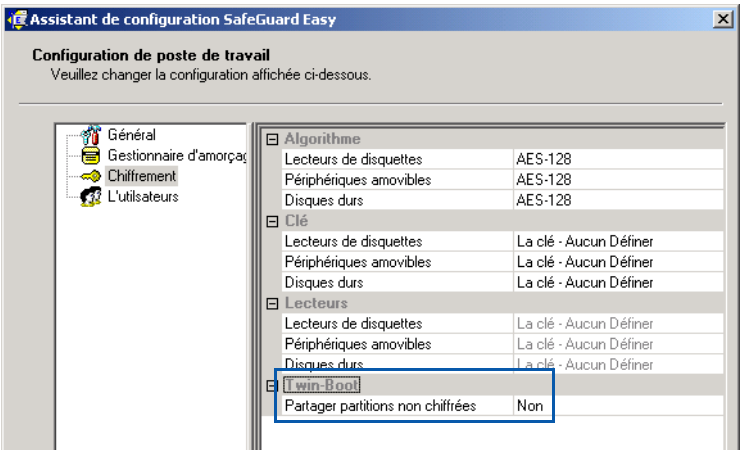
- Pour des raisons techniques, le gestionnaire d'amorçage ne fonctionne que lorsque les processus de chiffrement/déchiffrement sont terminés. Le premier redémarrage après chiffrement/déchiffrement appelle automatiquement le système d'exploitation du disque système de Windows, sans démarrer le gestionnaire d'amorçage. Ce comportement se note en particulier en cas d'installation et après création d'une sauvegarde de noyau avec l'assistant pour la disquette de secours.

- Pour chaque partition primaire amorçable non amorcée, le gestionnaire d'amorçage modifie l'entrée de type dans le tableau de partitions en « Masqué (48 h) ». Ces modifications restent conservées, même quand le code d'amorçage SafeGuard Easy MBR doit être supprimé avec la commande FDISK /MBR.FDISK /MBR doit être toujours utilisé avec la plus grande prudence.

  Attention : procédez avec précautions lorsque vous utilisez FDISK /MBR ! Pour rétablir le type de partition, vous devez désinstaller SafeGuard Easy.

14.6 Échange de données entre partitions d'amorçage

Si, pour certaines raisons, il était nécessaire d'échanger des données entre les partitions Professionnel et Privé, le paramètre « **Partager partitions non chiffrées** » l'autorise dans les paramètres de chiffrement.



Si ce paramètre est renseigné sur « OUI », l'accès aux partitions non chiffrées est possible, même quand la partition chiffrée a été amorcée.

15 Support Token

L'authentification avec nom d'utilisateur et mot de passe ne satisfait aujourd'hui bien souvent plus aux exigences de la clientèle en matière de protection optimale contre la transmission à des tiers. Pour cette raison, SafeGuard Easy offre l'ouverture de session avec une clé électronique (jeton) USB, comme alternative à la méthode d'ouverture de session « traditionnelle » et pour accroître la sécurité. L'ouverture de session via jeton est basée sur le principe de l'authentification à double facteur : un utilisateur dispose d'un jeton (possession), mais ne peut l'utiliser que lorsqu'il en connaît le mot de passe spécifique (connaissance).

Pour l'utilisation, les utilisateurs connectent simplement une clé Aladdin eToken initialisée dans un port USB de leur poste de travail, mettent l'ordinateur en marche et attendent qu'il s'arrête à l'authentification avant amorçage. Le mot de passe du jeton est alors demandé.

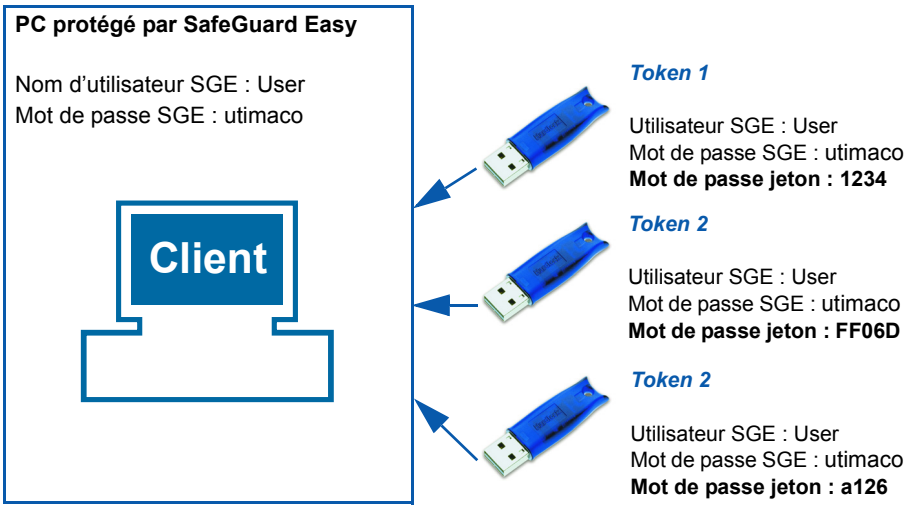
Si le mot de passe est correctement entré, SafeGuard Easy lit les données d'utilisateur du jeton, les transmet à la PBA et exécute ensuite l'ouverture de session.

L'utilisateur n'a en fin de compte plus qu'à entrer son mot de passe de jeton pour obtenir un accès aux zones chiffrées du disque dur.

15.1 Avantages d'une ouverture de session avec jeton

- Les utilisateurs doivent mémoriser le mot de passe (jeton). Lorsque la configuration requise est en place, le jeton ou le module SAL (Secure Automatic Logon) se charge de la connexion à SafeGuard Easy et au système d'exploitation.
- Dans une entreprise, un concept d'administration hiérarchisé et centralisé peut être mis en œuvre, par ex. pour la création de fichiers de configuration.
- Le concept d'utilisateur SGE reste caché à l'utilisateur « normal » quand celui-ci ne connaît pas ses données SGE.
- Si l'utilisateur ne connaît pas les données SGE, le manque de concordance entre l'utilisateur SGE et Windows est éliminé et le nombre d'utilisateurs SGE par poste de travail peut être augmenté sans restrictions.

  Si vous sélectionnez cette option, vous pouvez implémenter un **concept d'accès en fonction du rôle** et contourner le nombre maximum d'utilisateurs SafeGuard Easy autorisé par station de travail (15 utilisateurs) : dans un environnement où les rôles sont utilisés, les utilisateurs connaissent uniquement leur mot de passe (jeton) et non pas les données d'accès SafeGuard Easy (=rôle SafeGuard Easy). Quand l'administrateur délivre par exemple un nombre aléatoire de jeton contenant le même rôle SGE, un nombre illimité de possesseurs de jeton peuvent se partager un poste de travail protégé par SafeGuard Easy. Des données d'accès Windows différentes garantissent un Bureau individuel à chaque utilisateur.


PC protégé par SafeGuard Easy
Nom d'utilisateur SGE : User
Mot de passe SGE : utimaco
Client
Token 1
Utilisateur SGE : User
Mot de passe SGE : utimaco
Mot de passe jeton : 1234
Token 2
Utilisateur SGE : User
Mot de passe SGE : utimaco
Mot de passe jeton : FF06D
Token 2
Utilisateur SGE : User
Mot de passe SGE : utimaco
Mot de passe jeton : a126

15.2 Jetons pris en charge

SafeGuard Easy accepte les jetons USB suivants :

Aladdin eToken Pro

Aladdin Pro 16K, Aladdin Pro 32K
Aladdin Pro 64K / OTP*

*SafeGuard Easy prend en charge la puce de cryptage mais pas la fonction de mot de passe unique (OTP=One Time Password) du jeton.

Aladdin eToken NG-FLASH et NG-OTP

Le mot de passe pour Aladdin eToken (vide) est « 1234567890 ».

VeriSign USB Token

Version OEM Aladdin eToken.

Le numéro de série du jeton USB doit commencer par « ALPR ».

Token RSA SecurID 800

SafeGuard Easy prend en charge la puce de cryptage mais pas la fonction de mot de passe unique (OTP=One Time Password) du jeton.

AVERTISSEMENT : Vous devez posséder une version précise de RSA Authenticator Client. Pour de plus amples informations, contactez le fabricant de votre jeton. La version 4.50 de SafeGuard Easy ne prend plus en charge « RSA Authenticator Utility ».
Le mot de passe par défaut est « PIN_CODE ».

15.3 Fonctions du jeton

Action	Aladdin eToken / VeriSign USB Token	RSA SecurID 800 Token	Lecteur d'empreinte digitale de Lenovo
Authentification avant amorçage	X	X	X
Authentification pour accéder à SafeGuard Easy Administration	X[1]	X[2]	--
Authentification pour accéder aux fichiers de configuration	X[1]	X[2]	--
Authentification pour accéder à Windows	X[1]	X[2]	X[3]
Verrouiller le poste de travail Windows	X[1]	X[2]	--
Rapidité accrue du changement d'utilisateur SafeGuard Easy	X[1]	X[2]	--

[1] Uniquement avec « Aladdin Runtime Environment » (module PKCS#11)

[2] Uniquement avec « RSA Authenticator Client » (module PKCS#11)

ATTENTION : Vous devez posséder une version précise de RSA Authenticator Client. Pour de plus amples informations, contactez le fabricant de votre jeton. La version 4.50 de SafeGuard Easy ne prend plus en charge « RSA Authenticator Utility ».

[3] Uniquement avec logiciel d'empreinte digitale Lenovo ThinkVantage

15.4 Installation de la prise en charge des jetons

Procédure d'installation du support Token (jeton)

1. Démarrez le programme d'installation de SafeGuard Easy.

2. Sélectionnez les options d'installation et le mode de chiffrement.

3. Dans les paramètres de configuration, sélectionnez **Général / Authentification / Type d'authentification**. Sélectionnez, si un utilisateur se connecte avec son clavier, Token (jeton) ou Fingerprint (empreinte) dans le module PBA.

Clavier	Connexion utilisateur avec ID utilisateur et mot de passe.
Aladdin eToken	Connexion utilisateur avec Aladdin eToken.
Fingerprint	Connexion utilisateur avec une empreinte.
RSA SID 800	Connexion utilisateur avec un jeton SID RSA.
RSA SID 800 Random	Connexion utilisateur avec un jeton SID RSA. « Random » (Aléatoire) signifie qu'un mot de passe généré de façon aléatoire par SafeGuard Easy sera écrit dans le jeton. Les utilisateurs ne connaissent pas ce mot de passe.

4. Sélectionnez le mode Login (Connexion) si vous avez choisi Token (Jeton - Aladdin, RSA) ou Fingerprint (Empreinte)..

Jeton obligatoire	Cette option indique que SafeGuard Easy impose l'ouverture de session avec jeton pour tous les utilisateurs SGE d'un poste de travail. AVERTISSEMENT : Dans le mode « Uniquement avec jeton » vous devez posséder un jeton comportant les données d'accès SafeGuard Easy. Avec un jeton « vide », vous ne pourrez plus ouvrir de session sur votre ordinateur lorsque l'authentification avant amorçage aura été activée après l'installation !
Jeton facultatif	Cette option signifie que des utilisateurs ouvrent leur session soit avec jeton, soit en saisissant les données SGE. Avec cette option, un utilisateur SafeGuard Easy peut être contraint d'utiliser uniquement un jeton, tandis que tous les autres utilisateurs peuvent sélectionner un jeton ou des données utilisateur de SafeGuard Easy pour se connecter.

5. Si vous avez sélectionné « Token optional » (Jeton facultatif), sélectionnez **User / <username> / Logon**(Utilisateur / <nom d'utilisateur> / Connexion), puis spécifiez la personne devant se connecter avec un jeton.

   Vous pouvez par exemple spécifier qu'un utilisateur particulier, appelé « utilisateur_1 » doit se connecter avec un jeton (« Required » - Requis), tandis que l'utilisateur utilisateur_SYSTÈME peut choisir entre un jeton et la saisie manuelle des données d'accès SafeGuard Easy (« Not required » - Non requis).

6. Sélectionnez **Général / Authentification / mode d'émission** pour définir les personnes autorisées à écrire des donnée SafeGuard Easy sur un jeton.

SafeGuard Easy offre plusieurs possibilités :

Utilisateur	L'utilisateur peut initialiser un jeton « vide » dans la PBA. « Vide » signifie que le jeton ne comporte aucune donnée SafeGuard Easy.
Engagement externe	L'utilisateur doit appeler le service d'assistance et reçoit via la fonctionnalité Requête/Réponse la permission d'initialiser un jeton dans la PBA.
Centralisée	L'utilisateur reçoit un jeton initialisé et ne peut jamais initialiser un jeton dans la PBA.

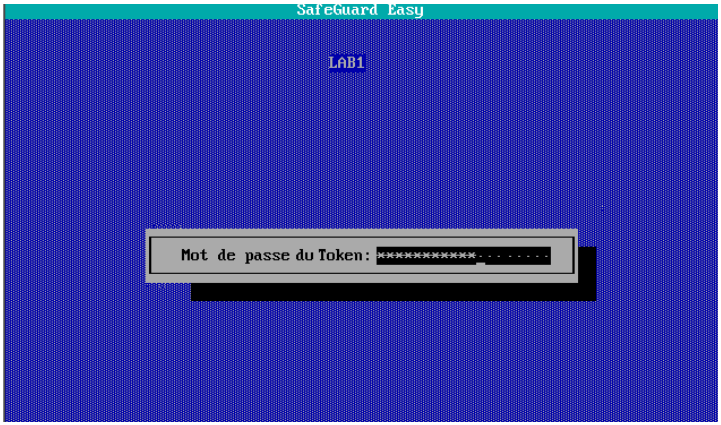
7. Première ouverture de session avec le jeton dans la PBA Vous ouvrez une session avec un jeton « vide » formaté en procédant de la manière suivante :
8. Redémarrer l'ordinateur.

15.5 Connexion initiale avec un jeton dans le module d'authentification avant le démarrage

Pour se connecter avec un jeton « vide » :

1. Insérez le jeton dans le port USB.
2. Allumez l'ordinateur et patientez jusqu'à ce que l'ordinateur s'arrête à l'authentification avant amorçage.
3. Entrez le mot de passe du jeton

   Mot de passe par défaut pour Aladdin eToken 1234567890.
   Mot de passe par défaut pour le jeton RSA SID 800 : PIN_CODE



4. Un message vous rappelle que le mot de passe par défaut du jeton constitue un risque de sécurité et doit être modifié (longueur maximale de 32 caractères).

   Entrez un nouveau mot de passe du jeton.

5. Saisissez les données d'accès SafeGuard Easy (nom d'utilisateur et mot de passe). Les données sont écrites sur le jeton.

   Le mode de délivrance paramétré établit si un utilisateur peut écrire lui-même les données d'accès SafeGuard Easy sur le jeton !

6. L'authentification SafeGuard Easy est effectuée. A l'ouverture de session suivante, il suffira d'entrer le mot de passe du jeton.

15.6 Modification du mot de passe du jeton

La procédure de modification du mot de passe lors de l'authentification avant amorçage est la suivante :

1. Insérez le jeton dans le port USB.
2. Démarrez l'ordinateur.
3. Saisissez le mot de passe du jeton dans la PBA.
4. Appuyez sur la touche [F10].
5. Entrez un nouveau mot de passe du jeton.

Les règles suivantes s'appliquent aux nouveaux mots de passe de jeton :

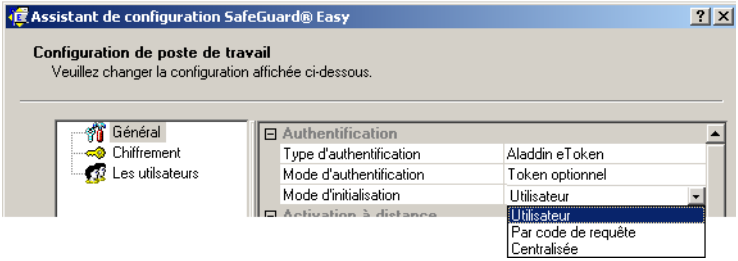
- le nouveau mot de passe doit être différent de l'ancien
- le nouveau mot de passe ne doit pas être banal (par ex. « 1234 » ou « asdf »)

15.7 Modification/suppression des données d'accès SafeGuard Easy

Les données d'accès SafeGuard Easy sont supprimées ou modifiées via l'administration du jeton (voir également 'Génération d'un jeton à partir d'un jeton existant Administration').

15.8 Définition du mode d'initialisation

« Initialisation » est la désignation du processus via lequel des données sont écrites sur le jeton, lesquelles sont ensuite utilisées pour l'authentification de l'utilisateur.



Le mode d'initialisation indique quelle instance est en droit d'écrire des informations SafeGuard Easy sur le jeton.

L'utilisateur qui initialise le jeton doit connaître le mot de passe du jeton. Sinon, il est impossible d'initialiser le jeton.

15.8.1 Mode d'initialisation

Mode d'initialisation « Utilisateur »
Quand cette méthode est sélectionnée, l'utilisateur peut entrer lui-même ses données d'accès SafeGuard Easy après sa première apparition dans la PBA. Ces données sont ensuite écrites sur le jeton. La condition en est bien entendu que l'utilisateur connaisse les données d'accès SafeGuard Easy d'un profil d'utilisateur et qu'elles soient présentes sur le poste de travail.

Mode d'initialisation « Par code de requête »
Quand cette option est sélectionnée, un utilisateur ne peut initialiser un eToken avec les données d'accès SafeGuard Easy qu'après l'échange d'un code de requête et de réponse.

Dans ce cas, l'utilisateur doit demander un code de requête dans la PBA en appuyant sur la touche [F9] et se mettre en contact avec le service d'assistance. Ce dernier démarre alors l'assistant de déblocage à distance. Il remplit les boîtes de dialogue pour l'authentification et entre le code de requête. Comme « Action à exécuter », il choisit « Accorder permission d'initialisation d'un jeton ». Le code de réponse généré est alors envoyé par email, SMS ou téléphone à l'utilisateur, celui-ci entrant alors le code de réponse dans les cases prévues à cet effet. Il peut ensuite écrire les données SGE sur le jeton.

Cette option implique un service centralisé dans une entreprise (par ex. le service assistance) et peut nécessiter dans certaines circonstances plus de travail et plus de temps. Elle évite par contre l'initialisation de plus d'un jeton pour une machine sans mise à contribution de l'assistance centralisée.

Mode d'initialisation « Centralisée »
Cette option signifie que le jeton doit être déjà initialisé par un service centralisé avant que l'utilisateur puisse en disposer. La section « Token Administration » (Administration de jeton) permet de créer des jetons de façon centrale. Vous trouverez une présentation de la création de jetons avec la fonction Token Administration (Administration de jeton) dans 'Génération d'un jeton à partir d'un jeton existant Administration'.

15.8.2 Automatisation de la création

Vous avez la possibilité d'automatiser la création de clés électroniques. Pour ce faire, vous devez recourir à un script Visual Basic (vbs). Pour ce faire, le système créant la clé électronique élabore un script Visual Basic (*.vbs) qui écrit en une opération les informations d'ouverture de session souhaitée (Windows, terminal serveur, SSO, SafeGuard Easy etc.) sur le jeton. Ce procédé est particulièrement bien approprié pour la première création d'un grand nombre de cartes d'utilisateur.

Exemple de script

La liste suivante montre un exemple de script : Ouvrez un éditeur, copiez l'exemple ligne par ligne, et enregistrez-le en tant que fichier vbs. Ensuite, fournissez les informations de connexion requise. Par exemple, remplacez *User PIN* (Code utilisateur) par le code utilisateur du jeton.

```
dim scard
dim res
dim slotID
dim pin
dim mustChangePIN
dim userID
dim password
dim domain
dim terminalServer
dim fileName
dim cerFile
dim linkFile
dim pkcsFile
dim protFile
dim cardInserted
dim authFile
dim configFile

set scard = WScript.CreateObject("SCardAdmScriptAPI.SCScriptAPI")

' *** Initialiser IMPORTANT  ! ! ! ! ***
slotID = 0
res = scard.Initialize(slotID)

' *** Carte insérée ? ***
cardInserted = scard.IsCardInserted()
if cardInserted then
```

```
WScript.Echo("Card is inserted")
else
WScript.Echo("NO Card in Slot")
end if

' *** Sortir numéro de série ***
serialNumber = scard.GetCardSerialNumber()
WScript.Echo(serialNumber)

' *** Modifier PIN utilisateur***
pin="New User PIN"
oldPIN="Old User PIN"
res = scard.SetUserPIN(oldPIN,pin)

' *** Modifier PIN RS ***
pin=« <Nouveau PIN responsable sécurité »
oldPIN=« < PIN responsable sécurité précédent »
res = scard.SetSOPIN(oldPIN,pin)

' *** Initialiser PIN utilisateur***
pin="New User PIN"
soPIN=« <PIN responsable sécurité de la clé électronique »
res = scard.InitUserPIN(soPIN,pin)

' *** Ouverture de session ***
pin = « <PIN de la clé électronique"
res = scard.LoginUser(pin)

' *** Changer PIN utilisateur : 1=changement impératif 0=changement non
nécessaire ***
mustChangePIN = 0, 1
res = scard.SetUserChangePIN(mustChangePIN)

' *** Définir les données du compte Windows ***
userID = « <Nom d'utilisateur Windows »
password = « <Mot de passe d'utilisateur Windows »
domain = « <Nom de domaine »
res = scard.SetWindowsAccount(userID,password,domain)

' *** Définir les données du compte SGEasy ***
configFile = « <Chemin absolu et nom du fichier de configuration pour l'installation SGE> »
userID = « <Utilisateur SGE écrit sur le jeton> »
authFile = « <Chemin absolu du fichier contenant les données d'authentification> pour le
        fichier de configuration>
res = scard.SetSGEasyAccount4(configFile,userID,authFile)
WScript.Echo(res)

' *** Afficher ID d'utilisateur Windows ***
userID = scard.GetWindowsAccount()
```

```
WScript.Echo(userID)

' *** Ajouter rôle(s) ***
userID = « <Nom de rôle » 
password = « <Mot de passe pour nom de rôle » 
domain = « <Nom de domaine » 
res = scard.AddMultidesktopRole(userID,password,domain)

' *** Ajouter compte(s) Terminal Server ***
userID = « <Nom d'utilisateur TS » 
userID = « <Mot de passe TS » 
domain = « <Nom de domaine » 
terminalServer = « <Nom du TS » 
res = scard.AddTerminalServerAccount(userID,password,domain,terminalServer)

' *** Créer certificat ***
'1) SSCertImport
fileName = "Fichier PKCS#12"
password = "Mot de passe pour PKCS#12 file"
res=scard.ImportCertificate(fileName,password)

'2) SSCert by SC
userID = "Nom d'utilisateur Windows"
cerFile = "Nom du fichier CER"
linkFile = "Nom du fichier CSV"
res=scard.CreateSSCertSC(userID,cerFile,linkFile)

'3) SSCertBySW

userID = "Nom utilisateur"
cerFile = "Chemin et nom du fichier de certificat (fichier CER)"
linkFile = "Chemin et nom du fichier Link (*.csv)"
pkcsFile = "Chemin et nom du fichier PKCS#12"
protFile = "Chemin et nom du fichier journal"
res=scard.CreateSSCertSW(userID, cerFile, linkFile, pkcsFile, protFile)

' *** Fermer session IMPORTANT  ! ! ! ! ***
res = scard.Uninitialize()
```

Remarques :

- Ne supprimez pas les guillemets indiqués ! Une entrée de ligne peut avoir par ex. l'aspect suivant : password="distribution". Si par ex. aucun mot de passe ne doit être entré dans un champ, laissez les guillemets en place dans la ligne, comme caractères génériques (par ex. password = "").
- Indiquez toujours les codes PIN actuellement valides pour la clé électronique connectée. Dans le cas contraire, le script est interrompu et un message d'erreur apparaît.
- Après exécution d'un script, un compte Windows déjà existant sur la clé électronique est écrasé.
- Après exécution du script, un nouveau rôle supplémentaire est créé sur la clé électronique. Si des rôles MultiDesktop existent déjà, ils ne sont ni supprimés, ni écrasés.
- Si un compte Terminal Server existe déjà, il n'est ni supprimé, ni écrasé après l'exécution du script.

Explications sur les entrées éditables pour SafeGuard Easy

- **configFile**
  Désigne le chemin absolu et le nom du fichier de configuration SafeGuard Easy.

  Ex. : configFile = "D :\Install.cfg"

  Le fichier de configuration doit avoir été créé avant le déploiement automatique via l'assistant de configuration pour le déploiement SafeGuard Easy. Il doit s'agit ici d'un fichier de configuration disposant de la propriété « Installer ».

Le fichier de configuration doit impérativement contenir les profils d'utilisateurs SGE suivants :

1) l'utilisateur qui doit être inscrit sous *userID* sur le jeton (par ex.
2) l'utilisateur qui ouvre une session sous *authFile* dans le fichier de configuration (par ex. « Helpdesk »)

- **userID**
  Utilisateur SafeGuard Easy écrit sur le jeton. Cet utilisateur doit être créé dans le fichier de configuration.

  Ex. : userID = "User"

- **authFile**
  Chemin absolu du fichier qui contient les données de profil SGE pour l'ouverture de session avec le fichier de configuration.

  Ex. : authFile = "D :\Token.PWD"

  Le fichier chiffré Token.PWD contient les données de profil SGE. Token.PWD est créé avec l'outil SGECPWF.exe. (qui se trouve sur le CD SafeGuard Easy dans le répertoire \Tools).

Exécution de script

Voici comment exécuter un script :

1. Installez les utilitaires Token Support et Token Administration.

2. Écrivez/copiez le texte complet du script exécuté dans un éditeur et enregistrez le fichier avec l'extension .VBS (p.ex. Smartcard.vbs).

3. Adaptez les champs modifiables.

4. Insérez une carte à puce dans le lecteur de cartes ou connectez une clé électronique à l'ordinateur.

5. Exécutez le script (par ex. en double-cliquant dessus dans l'Explorateur Windows).

6. La carte à puce /la clé électronique sont créés avec les données entrées.

15.9 Prise en charge des jetons par les utilitaires d'administration de SafeGuard Easy

SafeGuard Easy offre différents outils pour réaliser les tâches administratives (administration, assistants pour le fichier de configuration et pour les codes de réponse). Certaines actions de ces outils d'administration nécessitent des données SafeGuard Easy, par exemple lors de la connexion au module Administration ou lors de l'authentification à un fichier de configuration de base dans l'Assistant Configuration File (Fichier de configuration).

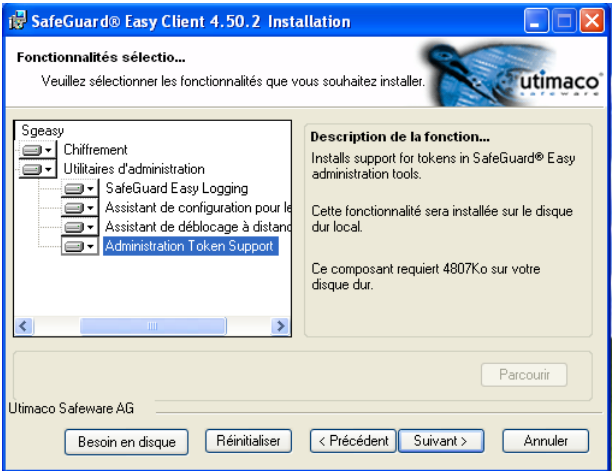
La prise en charge des jetons par SafeGuard Easy est semblable à la connexion de préparation au démarrage : une fois le jeton inséré, l'utilisateur doit entrer son code. Dans ce cas, le système lit le mot de passe SafeGuard Easy et le nom d'utilisateur du jeton pour procéder à la connexion (authentification).

L'enregistrement du jeton dans les outils d'administration est disponible en option et sert également en cas de désinstallation de SafeGuard Easy.

15.9.1 Activation de Support Token pour les utilitaires d'administration

La procédure d'activation du support eToken pour les utilitaires d'administration est la suivante :

1. Pendant l'installation, activez « Support Token pour l'administration » sur un poste de travail.



2. Redémarrez l'ordinateur.
3. Installez les modules logiciels suivants :

Token inséré	Logiciels nécessaires
Aladdin eToken Verisign USB Token	Aladdin eToken Runtime Environment (voir également http://www.utimaco.com/etoken)
RSA SecurID 800	RSA Authenticator Client

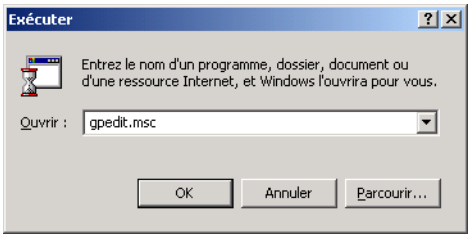
4. Enregistrez le module PKCS#11 du jeton.

15.9.2 Enregistrement du module PKCS#11

Pour que SafeGuard puisse « faire connaissance » avec le eToken, vous devez enregistrer le module PKCS#11 du jeton.

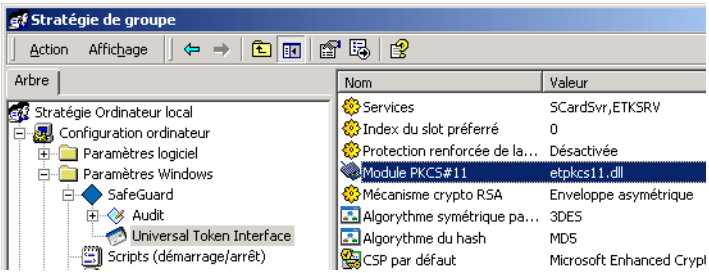
1. Cliquez sur le bouton [Démarrer] de Windows, puis sur *Exécuter*.

2. Dans la boîte de dialogue Ouvrir, tapez `gpedit.msc`.



Microsoft Management Console s'affiche.

3. Configuration
   Ordinateur
   \Paramètres Windows
   \SafeGuard
   \Universal Token Interface
   les réglages suivants sont possibles



Token inséré	**Paramétrage nécessaire**
Aladdin e Token Verisign USB Token	Services : SCardSvr, ETOKSRV Module PKCS#11 : « etpkcs11.dll » (à partir du répertoire SYSTEM32)
RSA SecurID 800	Services : SCardSvr Module PKCS#11 : « pkcs11.dll » Pour ajouter le module PKCS#11 pour RSA, vous devez indiquer le chemin complet. AVERTISSEMENT : Vous devez posséder une version précise de RSA Authenticator Client. Pour de plus amples informations, contactez le fabricant de votre jeton. La version 4.50 de SafeGuard Easy ne prend en charge plus « RSA Authenticator Utility »

4. Enregistrer les paramètres.
   Vous pouvez désormais utiliser un jeton pour vous connecter aux outils d'administration de SafeGuard Easy.

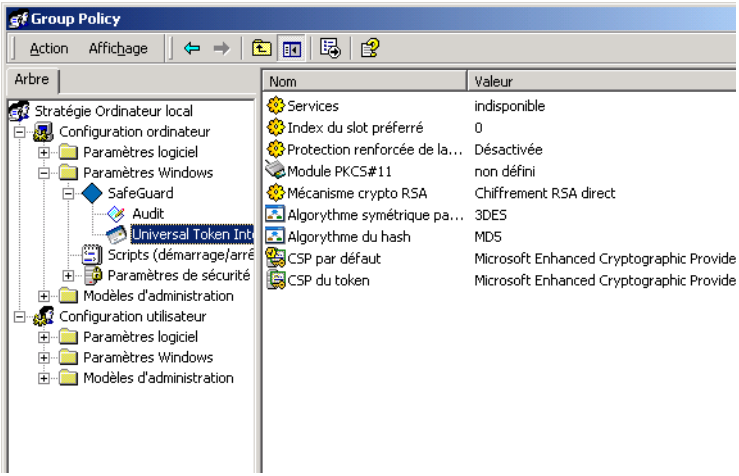
15.9.3 Interface universelle de jeton

L'interface universelle de jeton est une API qui est utilisée par les applications Utimaco pour communiquer avec différents jetons. Elle offre des fonctions pour accéder (lecture/écriture) aux données privées enregistrées sur le jeton. De plus, elle permet de chiffrer/déchiffrer, signer et vérifier les données en utilisant la paire de clés RSA stockée dans le jeton.

L'Interface Universal Token est présentée si « Administration Token support » est installé.

Les paramètres de l'interface universelle pour le Token se trouvent dans la MMC sous :

Configuration Ordinateur\Paramètres
Windows
\SafeGuard
\Universal Token Interface



Les paramètres suivants peuvent être configurés :

Services
Ici les services, qui sont nécessaires à l'utilisation du jeton doivent être spécifiés. Il doivent être initialisés avant l'interface universelle pour le Token.

`SCardSvrService`
pour les cartes à puce du système d'exploitation. Cette entrée est obligatoire.

De plus des jetons requièrent des services additionnels spécifiques, qui doivent aussi être spécifiés. Les services doivent être séparés par des virgules.

Slot index préféré
Un Token requiert un index de slot spécifique. Saisissez le slot pour votre jeton. Si le module PKCS#11 pour SafeGuard Smartcard Provider est sélectionné, le slot 0 est saisi automatiquement.

> ***REMARQUE :***
> Vérifiez que votre jeton est connecté au slot spécifié.

Module PKCS#11
Le module PKCS#11 assure la commutation (lecture/écriture) avec le jeton.

Saisissez le module PKCS#11 correspondant pour votre jeton.

Module PKCS#11, Services, Slots

Fournisseur de jetons	Logiciel	Module PKCS#11	Services
Aladdin (USB Token)	le plus récent Aladdin Runtime Environment (RTE)	eTpkcs11.dll	SCardSvr ETOKSRV
Verisign (jeton USB)	voir Aladdin	voir Aladdin	voir Aladdin
RSA SecurID Token	le plus récent RSA Authenticator Client	pkcs11.dll	SCardSvr

Protection renforcée de la clé privée
Si elle est activée, on demandera à l'utilisateur de s'authentifier chaque fois que la clé privée est utilisée par une application.

CSP par défaut
Tous les CSP disponibles sur votre système s'affichent ici. Vous pouvez choisir celui qui est utilisé pour les opérations qui utilisent la clé publique.

Il est recommandé d'utiliser le Enhanced Cryptographic Service Provider de Microsoft.

CSP pour le Token
Spécifie le CSP pour le jeton que vous utilisez. Si vous utilisez les cartes à puce Utimaco, vous devez sélectionner le CSP Universal Smartcard d'Utimaco.

Mécanisme Crypto RSA
Pour les CSP qui n'offre pas un chiffrement direct par le mécanisme RSA, l'option **enveloppe asymétrique** est fournie. Dans ce cas, les données en masse sont chiffrées en utilisant un algorithme symétrique qui peut être sélectionné. Le chiffrement RSA s'applique sur la clé utilisée.

Algorithme Symétrique par défaut
Choisir l'algorithme pour le chiffrement symétrique des données en masse, si vous avez sélectionné l'**enveloppe asymétrique** comme mécanisme crypto.

Algorithme Hash
Sélectionnez l'algorithme pour le hash qui va être utilisé.

15.10 Ouverture de session avec jeton sur le système d'exploitation

Lorsque l'authentification SafeGuard Easy a été acceptée, le système d'exploitation invite l'utilisateur à saisir les données d'accès valides. Cela signifie que les données d'utilisateur sont demandées deux fois dans le cadre d'une authentification avec jeton : une fois dans la phase PBA (mot de passe du jeton) et une fois lors de l'ouverture de session normale dans le système d'exploitation.

REMARQUES :

- Les composants SafeGuard acceptent des mots de passe d'une longueur maximale de 63 caractères pour l'ouverture de session dans le système d'exploitation.

  Utimaco recommande de ne pas dépasser cette longueur maximale pour le mot de passe du jeton.

- On suppose que les fabricants du jeton proposent des pilotes précis (PKCS#11, Cryptographic Service Provider (CSP)) permettant le support du jeton au niveau du système d'exploitation.

15.10.1 Initialisation du jeton

Si l'utilisateur est en droit d'initialiser le jeton, le processus d'initialisation se déroule comme suit :

1. Insérez le jeton (formaté) dans le port USB et démarrez le PC.

2. Entrez le mot de passe du jeton pour la PBA. Le système d'exploitation démarre.

3. Entrez le mot de passe du jeton et cliquez sur [OK].

4. Comme le jeton ne contient pas encore de données d'ouverture de session dans Windows, le système demande, après confirmation avec « OK », si le jeton doit être initialisé.

5. Après un clic sur [OK], la boîte de dialogue *Initialiser jeton avec données d'accès Windows* est ouverte. L'utilisateur est invité à saisir son nom d'utilisateur et son mot de passe Windows.

Une boîte de dialogue confirme l'initialisation avec succès du jeton. Suite au redémarrage, vous êtes connecté de façon automatique au système d'exploitation.

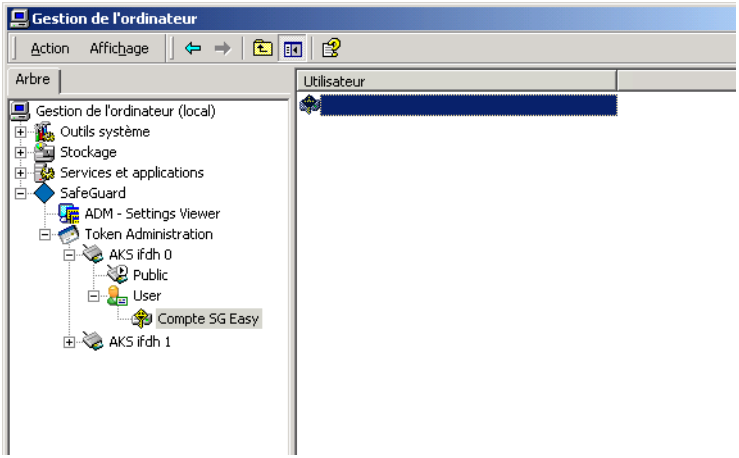
15.10.2 Données Windows enregistrées dans le fichier SAL

Les données du système d'exploitation sont synchronisées avec le fichier SAL chiffré, `SGSAL.dat`, après toute connexion réussie avec un jeton, si la **procédure facultative de connexion par jeton de SafeGuard Easy** est sélectionnée. En particulier dans les cas d'urgence (l'utilisateur a perdu son jeton avec données Windows, entre autres), ceci garantit que l'utilisateur peut de nouveau accéder aux données. Quand l'utilisateur modifie ses données Windows, le fichier `SGSAL` .dat est également mis a jour.

15.11 Génération d'un jeton à partir d'un jeton existant Administration

Quand Token Administration est installé, les données suivantes peuvent être enregistrées dans la clé électronique :

- Numéro d'identification personnel (PIN)
- Données SafeGuard
- Données Windows



15.11.1 Installation du module d'administration de jeton

1. Installe les fichiers du répertoire \TOOLS du CD SafeGuard Easy

   - TokenAdmin.msi
   - SCAdmin_SGEasy.msi

2. Pour sécuriser la liaison eToken/SafeGuard GINA, le module PKCS#11du eToken doit être indiqué (voir détails sous). La stratégie se trouve sous 'Enregistrement du module PKCS#11'.

3. Connectez la clé eToken au PC.

4. Appelez la Gestion de l'ordinateur via Démarrer / Paramètres / Panneau de configuration / **Outils d'administration**.

   Le dossier « SafeGuard » de Gestion de l'ordinateur affiche « Token Administration » (Administration de jetons).

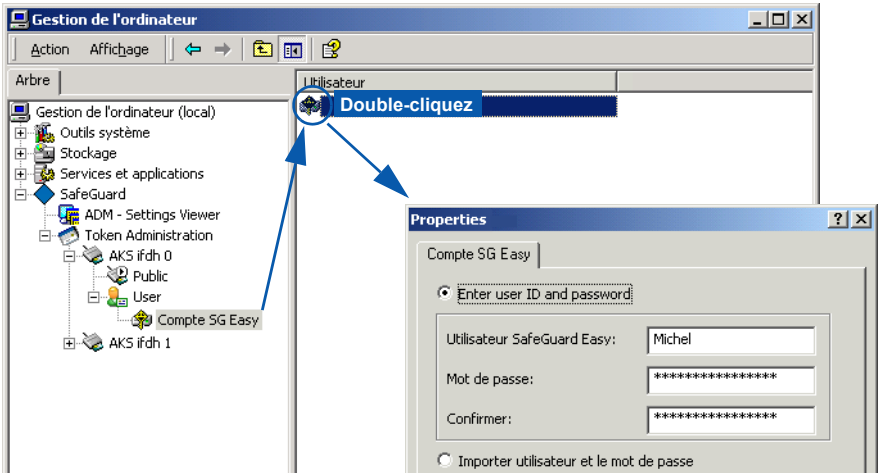
5. Connectez-vous au module Token Administration en entrant le mot de passe correspondant au jeton.

6. Ouvrez le dossier **User**.

7. Sélectionnez le dossier **SGEasy Account**.

8. Ouvrez la boîte de dialogue **Propriétés** en double cliquant sur l'icône SafeGuard Easy dans la colonne « Utilisateur ».

9. Sélectionnez « Enter user ID and password » (Entrer ID utilisateur et mot de passe), puis entrez le nom d'utilisateur et le mot de passe.



10. Ensuite confirmez en cliquant sur [OK].

Le jeton comporte désormais vos données.

Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco http://www.utimaco.com/myutimaco d'Utimaco.

Dans la zone de recherche (« Search »), tapez « Token & Admin".

15.11.2 Suppression de données sur le jeton

Pour supprimer les données du jeton, sélectionnez la commande « Delete » (Supprimer) dans le menu contextuel « Sgeasy Access Data » (Données d'accès Sgeasy). La même procédure s'applique à la suppression des données d'accès de Windows.

15.11.3 Importation de données SafeGuard Easy du fichier de configuration

Si vous importez des données, les données utilisateur de SafeGuard Easy (nom et mot de passe) sont écrites sur le jeton à partir d'un fichier de configuration existant. Cette procédure s'applique lorsque l'émetteur ne connaît pas le mot de passe utilisateur de SafeGuard Easy ou ne doit pas le connaître.

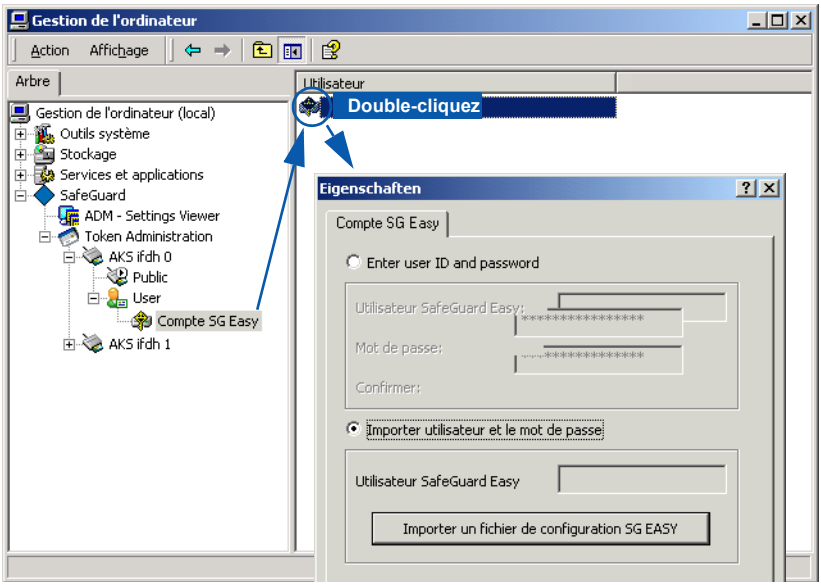
Comment procéder :

1. Activez l'option « Entrer ID utilisateur et mot de passe ».

2. Ouvrez le dossier **Utlisateur**.

3. Sélectionnez le dossier **Compte SGEasy**.

4. Ouvrez la boîte de dialogue **Propriétés** en double cliquant sur l'icône SafeGuard Easy dans la colonne « Utilisateur ».

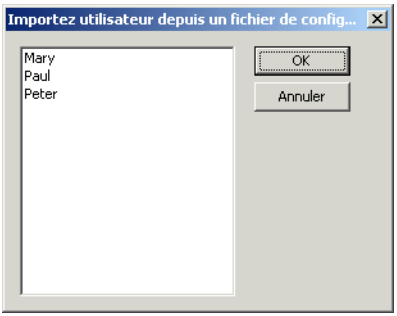


5. Sélectionnez « Importer ID utilisateur et mot de passe ».

6. Cliquez sur le bouton [Importer le fichier de configuration SG Easy] et sélectionnez le fichier de configuration.

7. Connectez-vous au fichier de configuration avec les informations d'identification de SafeGuard Easy qui sont disponibles dans le fichier.

8. Une nouvelle boîte de dialogue s'affiche, qui donne la liste de tous les utilisateurs entrés dans le fichier de configuration sélectionné. Sélectionnez l'utilisateur SafeGuard Easy voulu.



9. Cliquez sur [OK] pour confirmer votre sélection. Ces données sont ensuite écrites sur le jeton.

15.12 Changement rapide d'utilisateur SafeGuard Easy

En règle générale, les utilisateurs SafeGuard Easy partageant un ordinateur ont les mêmes droits. Il peut toutefois arriver que des utilisateurs possédant des droits SafeGuard Easy différents se partagent un ordinateur. Normalement (sans authentification avec jeton), un changement d'utilisateur SafeGuard Easy n'est possible que si l'ordinateur est complètement arrêté, le nouvel utilisateur ouvrant alors une session dans la PBA avec ses données de profil. Ceci peut dans certaines circonstances prendre beaucoup de temps. Les utilisateurs préfèrent cependant qu'il s'écoule le moins de temps possible entre la fermeture de session de l'ancien utilisateur et l'apparition du Bureau du nouvel utilisateur.

Un long redémarrage de l'ordinateur pour un changement d'utilisateur SafeGuard Easy n'est pas nécessaire quand des jetons sont utilisés. Dans ce cas, une simple fermeture de session Windows suffit. Dans la boîte de dialogue d'ouverture de session Windows, le l'utilisateur concerné insère son jeton dans le port USB, s'authentifie avec le code PIN et ouvre sa session avec le profil de droits SafeGuard Easy (et Windows) enregistré sur le jeton. La condition pour un changement d'utilisateur est toutefois que la PBA soit activée et que des données SafeGuard Easy valides y aient été préalablement entrées. Cependant, avant de changer d'utilisateur, le module PBA doit être actif et des données SafeGuard Easy valides doivent être saisies dans ce dernier.

15.12.1 Conditions

1. Enregistrez les données SafeGuard Easy et Windows sur le jeton

2. Activez la PBA (ouverture de session avec ou sans jeton).

3. Pour changer rapidement d'utilisateur SafeGuard Easy, fermez la session Windows via Démarrer / Quitter / Fermer la session « <Utilisateur> » ou [Ctrl]+[Alt]+[Suppr]+[fermer la session].

15.12.2 Exemple

Procédure de remplacement rapide :

1. L'utilisateur 1 insère son jeton, allume l'ordinateur.

2. La PBA apparaît. L'utilisateur 1 entre le code PIBN du jeton dans la PBA.

   Ses données de profil SafeGuard Easy se trouvent sur le jeton :
   Nom d'utilisateur : User01
   Mot de passe : password01
   Droits SGE : Aucun

   Si des données Windows sont également enregistrées sur jeton, l'utilisateur est automatiquement authentifié dans SafeGuard Easy et Windows, sans autres indications.

   Le profil SafeGuard Easy de l'utilisateur 1 est actif. L'utilisateur ne possède pas de droits SafeGuard Easy.

3. L'utilisateur 1 termine son travail, ferme sa session Windows via DEMARRER / QUITTER / Fermer la session « <Utilisateur> » (alternative : [Ctrl]+[Alt]+[Supp]+[Fermer la session]) et retire son jeton une fois la session fermée.

4. La boîte de dialogue d'ouverture de session de Windows apparaît.

5. L'utilisateur insère son jeton (avec données SafeGuard Easy et Windows) dans le port USB, entre son code PIN de jeton et ouvre sa session avec ces données de profil SafeGuard Easy.

   Nom d'utilisateur : User2
   Mot de passe : password2
   Droits SGE : Activer le chiffrement de disquettes

Le profil SafeGuard Easy de l’utilisateur 2 est actif. L’utilisateur est en droit d’activer ou de désactiver le chiffrement de disquettes.

15.13 Télé-assistance

L'administration distante est requise lorsque l'utilisateur et l'administrateur sont éloignés physiquement (par exemple, si l'utilisateur est un commercial) et si l'administrateur ne peut pas résoudre une erreur personnellement, sur site.

La télé-assistance peut être nécessaire pour les scénarios suivants

- L'utilisateur a perdu son jeton
- l'utilisateur a oublié son jeton (par ex. chez lui)
- l'utilisateur a oublié le mot de passe de son jeton

Dans tous les cas, le mécanisme Requête/Réponse de SafeGuard Easy fournit un remède. La procédure Requête/Réponse assiste l'administrateur du système en lui permettant un certain nombre d'ouvertures de session sans le jeton de l'utilisateur. L'emploi de la procédure Requête/Réponse permet donc à l'utilisateur d'accéder au système quand le jeton n'est pas disponible ou quand le mot de passe du jeton a été oublié. Cette méthode garantit en outre que seul un utilisateur légitime peut ouvrir une session.

15.13.1 Conditions pour la télé-assistance

Une télé-assistance jeton effective nécessite l'installation des paramètres suivants sur le client SGE :

- Mode d'authentification : jeton optionnel
  (voir General/Authentication/Login Mode - Général/ authentification/Mode de connexion)
- Type d'authentification (pour l'utilisateur) : requis
  (voir Users/<nom_utilisateur>/Logon - Utilisateur/ <nom_utilisateur>/Connexion)

REMARQUES :

- L'utilisateur doit connaître les données de l'utilisateur SafeGuard Easy sur l'ordinateur de l'utilisateur ! Dans le cas contraire, il n'est pas possible de lancer la procédure Requête/ Réponse (à moins que l'administrateur ne fournisse les données d'un autre utilisateur SGE à l'utilisateur).
- Une désactivation permanente du support de jeton n'est pas possible via la procédure Requête/Réponse.

15.13.2 Exemple d'utilisation

Dans les exemples ci-dessous, nous allons expliquer quelles sont les tâches de l'utilisateur et de l'administrateur quand un utilisateur oublie/perd son jeton ou ne se rappelle plus son mot de passe de jeton.

Pour tous les exemples, les conditions suivantes doivent être remplies sur le client SGE

- Mode d'authentification : jeton facultatif
  (voir General/Authentication/Login Mode - Général/authentification/Mode de connexion)
- Mode de génération : utilisateur
  (voir General/Authentication/Issuing Mode - Général/authentification/Mode de génération)
- Type d'authentification (pour l'utilisateur) : requis
  (voir Users/<nom_utilisateur>/Logon - Utilisateur/<nom_utilisateur>/Connexion)
- PBA activée
- SAL activée

L'utilisateur a oublié son jeton

Utilisateur	Administrateur/Assistance/ Aide
Entre ses données d'utilisateur SGE dans la PBA et requiert le code de requête avec [F9]. Appelle l'administrateur/assistance/ helpdesk.	
	S'assure que le demandeur est bien l'utilisateur. Appelle l'assistant de déblocage à distance. Demande le code de requête de l'utilisateur. Dans la boîte de dialogue « Remote command » (Commande distante), sélectionnez l'option « **Logon without required token for X logons** » (Connexion sans le jeton requis pour X connexions). Transmet le code de réponse à l'utilisateur.
Entre le code de réponse dans les cases prévues à cet effet et ouvre une session. Ils peuvent désormais se connecter au module PBA x fois sans jeton. Pour l'ouverture de session dans le système d'exploitation (l'utilisateur ne connaît pas les données), le fichier SAL est ouvert, les données de système d'exploitation de l'utilisateur sont sorties et l'ouverture de session est automatiquement effectuée.	

L'utilisateur a perdu son jeton

Utilisateur	Administrateur/Assistance/ Helpdesk
	Envoie à l'utilisateur un nouveau jeton (vide) avec mot de passe standard.
Entre ses données d'utilisateur SGE dans la PBA et requiert le code de requête avec [F9]. Appelle l'administrateur/assistance/aide.	
	Appelle l'assistant de déblocage à distance. Demande le code de requête de l'utilisateur. Choisit, dans la boîte de dialogue « Actions à exécuter », l'option **« Accorder permission d'initialisation d'un jeton »**. Transmet le code de réponse à l'utilisateur.
Entre le code de réponse dans les cases prévues à cet effet et ouvre une session. Connecte le nouveau jeton au redémarrage de l'ordinateur, entre le mot de passe standard et écrit les données d'accès SGE sur le jeton (quand celui-ci n'est pas encore initialisé). L'utilisateur n'écrit pas personnellement les données du système d'exploitation sur le jeton : ces dernières proviennent du fichier SAL et sont enregistrées sur le jeton pendant la connexion.	

REMARQUE :
Quand le jeton a déjà été initialisé via Token Administration, une procédure Requête/Réponse est inutile. L'administrateur doit uniquement communiquer le mot de passe du jeton à l'utilisateur.

L'utilisateur a oublié son mot de passe de jeton

Utilisateur	Administrateur/Assistance/ Helpdesk
Autoriser une ouverture de session unique sans jeton à l'utilisateur via la procédure Requête/Réponse (voir « L'utilisateur a oublié son jeton »)	
L'utilisateur a ouvert une session sans jeton dans SafeGuard Easy et Windows via Requête/Réponse. Connecte le jeton au port USB.	

	Se connecte à l'ordinateur de l'utilisateur via la fonction d'administration à distance de la Token Administration et modifie le mot de passe de jeton. Indique à l'utilisateur le nouveau mot de passe de jeton. Conditions : - l'administrateur connaît le mot de passe d'administrateur du jeton - l'utilisateur PC doit être dans le réseau. doit être installé sur l'ordinateur de l'administrateur et de l'utilisateur - doit être installé sur l'ordinateur de l'administrateur et de l'utilisateur le jeton dispose d'un mot de passe d'administrateur qui correspond au code PIN du responsable de la sécurité dans la Token Administration.
Redémarre l'ordinateur et ouvre la session avec le jeton.	

15.13.3 Administration de jeton à distance avec Token Administration

L'administration à distance sert à aider les utilisateurs dans les situations d'urgence, par ex. quand ils ont oublié leur code PIN et ne peuvent donc plus ouvrir de session.

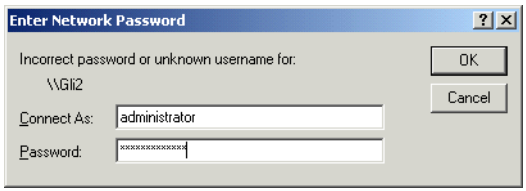
Pour administrer à distance une clé électronique,

- une connexion réseau doit exister entre l'ordinateur de l'utilisateur et l'administrateur,
- Token Administration doit exister sur le PC de l'administrateur,
- Token Support et Token Administration doivent être installés sur le PC de l'utilisateur et la clé électronique connectée au poste de travail,
- l'administrateur doit connaître le code PIN responsable sécurité de la clé d'utilisateur.

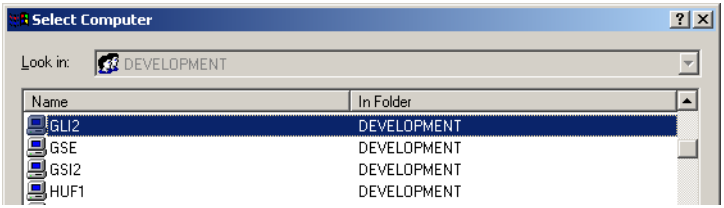
Voici comment administrer la clé électronique à distance :

1. Authentifiez-vous en tant qu'administrateur sur le PC d'utilisateur auquel la clé électronique est connectée.

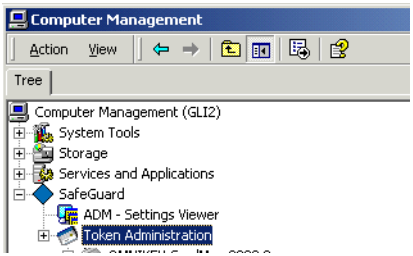
2. Établissez une nouvelle communication avec le PC de l'utilisateur via la gestion de l'ordinateur.



3. Sélectionnez le PC de l'utilisateur.



4. Ouvrez Token Administration via la gestion de l'ordinateur du PC d'administrateur.



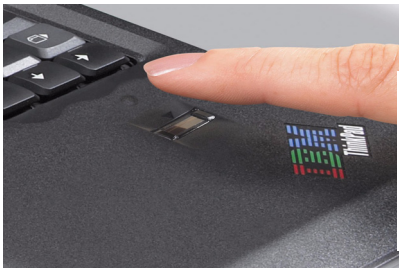
5. Ouvrez une session sur Token Administration avec le code PIN responsable sécurité.

Vous pouvez à présent attribuer un nouveau code PIN utilisateur, débloquer des clés électroniques, etc.

16 Authentification par le lecteur d'empreinte digitale de Lenovo

Les utilisateurs doivent désormais se souvenir de diverses combinaisons de chiffres pour accéder à leur ordinateur de bureau ou portable. A la différence d'un jeton ou d'un mot de passe, une empreinte digitale est unique et ne peut être devinée (à la différence du mot de passe) ou oubliée (jeton).

Certains ordinateurs portables Lenovo intègrent directement un lecteur d'empreinte digitale. Mais l'authentification par empreinte digitale est également possible par un clavier ou un lecteur USB externe.



SafeGuard Easy établit un lien entre un doigt de l'utilisateur et les données d'accès de SafeGuard Easy. Il suffit donc de procéder à l'authentification en insérant un doigt dans le lecteur pour accéder automatiquement à SafeGuard Easy.

Avantages d'une authentification par empreinte digitale

- Sécurité : un mot de passe ou un jeton ne sont plus nécessaires.
- Confort : connexion automatique à SafeGuard Easy et Windows (et à toutes les applications exigeant une authentification).

REMARQUE :
Le système ne permet de connecter qu'un seul lecteur d'empreintes.

Action	Lecteur d'empreinte digitale Lenovo
Authentification avant amorçage	X[3]
Authentification pour accéder à SafeGuard Easy Administration	--
Authentification pour accéder aux fichiers de configuration	--
Authentification pour accéder à Windows	X[3]
Verrouiller le poste de travail Windows	--
Rapidité accrue du changement d'utilisateur SafeGuard Easy	--

[3] Uniquement avec logiciel d'empreinte digitale Lenovo ThinkVantage

16.1 Préparation

- Ordinateur de bureau ou portable Lenovo des séries 5x ou 6x
- Un BIOS récent est recommandé
- Lecteur d'empreinte digitale intégré à l'ordinateur portable ou clavier USB avec lecteur d'empreinte digitale, lecteur d'empreinte digitale USB
- SafeGuard Easy à partir de la version 4.30
- Logiciel d'empreinte digitale ThinkVantage supporté :
  - Logiciel ThinkVantage Fingerprint 5.5.0
- ThinkVantage Fingerprint Software 5.60/5.6.1 (minimum) :
  À partir de la version 5.60/5.61, vous devez modifier l'entrée
  HKLM
  SOFTWARE
  Protector Suite QL
  1.0

  du registre : définissez la valeur « **BiosFeatures** » DWORD sur « 2 ». Software

16.2 Équipements compatibles

SafeGuard Easy accepte l'authentification via le lecteur d'empreinte digitale intégré aux ordinateurs de bureau ou portables Lenovo qui sont commercialisés depuis l'automne 2005.

Ordinateurs portables Lenovo compatibles	Z60/Z61
	T60/T61
	X60/X61
	R60

Ordinateurs de bureau Lenovo compatibles	A51
	A52
	M51
	M52
	M52e

Ordinateurs portables Lenovo non compatibles	3000
	T4x

Portables Tablet PC Lenovo non compatibles	X41
	R61

REMARQUES :

Les portables Lenovo de la gamme 3000 ne sont pas compatibles puisqu'ils intègrent un lecteur d'empreinte digitale d'un autre fournisseur.

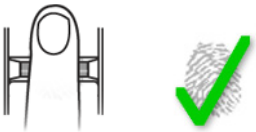
Les modèles Tablet PC requièrent un clavier connecté pour l'authentification par empreinte digitale. Une saisie via un clavier sera demandée lors de l'authentification au démarrage afin d'établir la liaison entre les données d'accès SafeGuard Easy et l'empreinte digitale ! Une détection manuscrite est impossible lors de l'authentification au démarrage.

16.3 Installer le lecteur d'empreinte digitale Lenovo

AVERTISSEMENT :
En cas d'authentification par empreinte digitale, la fonction « Utilisateur standard » de SafeGuard n'est pas prise en charge. Un utilisateur SafeGuard Easy, connecté via une empreinte digitale, doit toujours connaître le nom d'utilisateur et le mot de passe de SafeGuard Easy.

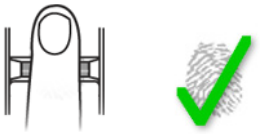
Installation de la fonction de lecture d'empreinte digitale :

1. Installez le logiciel ThinkVantage Fingerprint (s'il n'est pas déjà installé).
2. Relevez l'empreinte d'un ou plusieurs doigts dans le logiciel de lecture d'empreinte digitale. La procédure d'inscription lie ces empreintes avec les données de connexion Windows (pour plus de détails sur l'enregistrement d'une empreinte, consultez l'aide du logiciel ThinkVantage ou consultez la page http://www-307.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-58403).
3. Pour tester l'empreinte, redémarrez le PC/ordinateur portable.Après le redémarrage, insérez le doigt enregistré dans le lecteur. La connexion à Windows s'établit automatiquement.



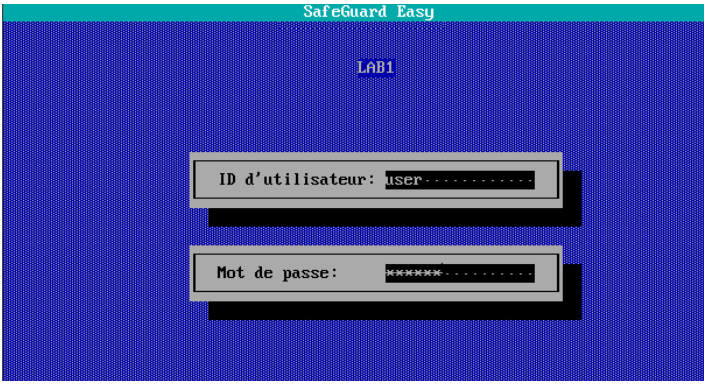
4. Lancez la fonction Control Center du logiciel ThinkVantage Fingerprint.

5. Lorsque vous inscrivez une empreinte pour la première fois, vous devez également indiquer si cette empreinte doit être utilisée lors du démarrage. Cliquez sur [Oui].
6. Cochez la case « Replace the power-on and hard drive passwords with the fingerprint reader ».
7. Installez SafeGuard Easy.
8. Dans les paramètres de configuration, sélectionnez **Général / Authentification / Type d'authentification**, puis l'option « Empreinte ».
9. Redémarrez l'ordinateur.
10. Après le redémarrage, insérez un des doigts enregistrés dans le lecteur.



11. L'écran d'authentification au démarrage s'affiche. Aucune donnée n'est demandée, mais la ligne « Démarrer l'authentification avec le lecteur d'empreinte digitale » s'affiche (continuer en appuyant sur n'importe quelle touche)".
12. L'écran d'authentification Fingerprint apparaît. Insérez le doigt dans le lecteur qui doit être associé aux données SafeGuard Easy. L'empreinte du doigt doit avoir été préalablement relevée avec le logiciel ThinkVantage Fingerprint.

13. L’écran d’authentification au démarrage s’affiche. Saisissez maintenant les données d’accès de SafeGuard Easy qui seront utilisées pour l’authentification via l’empreinte digitale.



14. A l’aide de la touche [F6], associez un autre doigt aux données d’accès à SafeGuard Easy au cas où le premier ne serait pas reconnu (par ex. en cas de blessure).

15. L’association avec les doigts est maintenant établie. A chaque redémarrage de l’ordinateur, il suffit d’insérer un des doigts enregistrés pour établir son identité dans SafeGuard Easy et Windows.

REMARQUES :

L'utilisateur abandonne l'authentification par empreinte digitale avec la touche [Échap] et s'identifie en entrant le nom d'utilisateur et le mot de passe SafeGuard Easy.

L'abandon via [Échap] est nécessaire dans les cas suivants :

- l'authentification par empreinte digitale a été installée, mais aucun lecteur d'empreinte digitale n'est connecté à l'ordinateur,
- l'utilisateur n'est pas en mesure de s'authentifier par empreinte digitale ou le lecteur d'empreinte est défectueux. La touche [Échap] permet de revenir à l'authentification au démarrage. L'utilisateur peut alors s'authentifier par la procédure habituelle de saisie du nom d'utilisateur et de mot de passe SafeGuard Easy.

16.4 Modifier le mot de passe SafeGuard Easy

L'utilisateur peut modifier son mot de passe dans l'écran

- d'authentification au démarrage de l'application
- SafeGuard Easy Administration.

La procédure de modification du mot de passe lors de l'authentification avant amorçage est la suivante :

1. Démarrez l'ordinateur. L'écran d'authentification Fingerprint apparaît.
2. Appuyez sur [Échap]. L'écran d'authentification au démarrage s'affiche.
3. Saisissez vos données d'accès à SafeGuard Easy.
4. Appuyez sur [F10] et modifiez le mot de passe.
   L'ordinateur démarre sans exiger l'empreinte digitale.
5. Redémarrez l'ordinateur. L'écran d'authentification Fingerprint apparaît.
6. Insérez le doigt dans le lecteur. L'écran d'authentification au démarrage s'affiche.
7. Saisissez votre nom d'utilisateur et le nouveau mot de passe.
8. Confirmez avec la touche Entrée. L'écran d'authentification Fingerprint apparaît.
9. Insérez le doigt dans le lecteur. Les données de SafeGuard Easy sont associées au doigt et l'authentification est opérée.

Le mot de passe a été redéfini.

Modifiez le mot de passe dans SafeGuard Easy Administration selon la procédure suivante :

1. Lancez l'application Administration via Programmes/Utimaco/SafeGuard Easy/Administration.
2. Sélectionnez le dossier « Utilisateurs » et modifiez votre mot de passe dans « Configuration du mot de passe".
3. Redémarrez l'ordinateur. L'écran d'authentification Fingerprint apparaît.
4. Insérez le doigt dans le lecteur. L'écran d'authentification au démarrage apparaît et indique que les données ne concordent pas.
5. Saisissez vos données d'accès à SafeGuard Easy (nouveau mot de passe !). L'authentification est effectuée.

Les nouvelles données d'accès à SafeGuard Easy sont associées à l'empreinte digitale.

16.5 Foire aux questions

Faut-il avoir d'autres logiciels comme Client Security Solution (CSS) de Lenovo ?

La solution d'empreinte digitale SafeGuard Easy fonctionne indépendamment de CSS. Vous avez seulement besoin du logiciel ThinkVantage Fingerprint pour relever les empreintes.

Est-ce que plusieurs utilisateurs sont acceptés ?

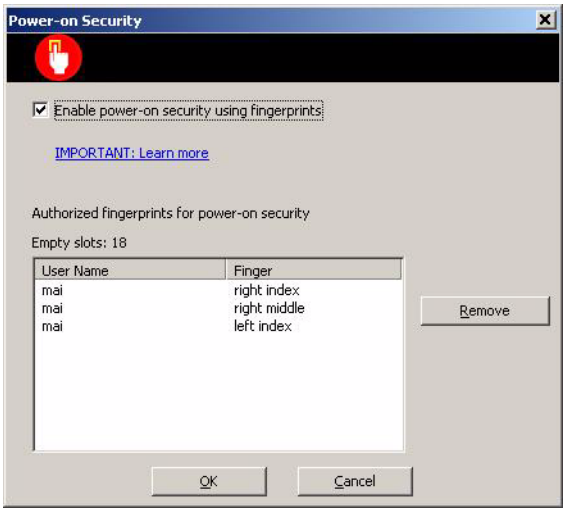
Le lecteur peut mémoriser 21 empreintes digitales. Chacune de ces empreintes peut être associée à n'importe quel utilisateur Windows via le logiciel ThinkVantage Fingerprint. SafeGuard Easy fonctionne de la même façon. La seule différence est que les empreintes et les données utilisateur de SafeGuard Easy sont liées pendant l'authentification avant le démarrage (par exemple, vous pouvez utiliser l'index de la main gauche pour vous connecter en tant qu'utilisateur SYSTÈME et celui de la main droite pour vous connecter en tant qu'UTILISATEUR).

Que se passe-t-il lorsque l'authentification par empreinte digitale ne fonctionne pas (par ex. lecteur défectueux) ?

L'appui sur la touche [Échap] permet à l'utilisateur d'accéder à l'authentification au démarrage et de s'identifier en saisissant son nom d'utilisateur et son mot de passe SafeGuard Easy. Si l'utilisateur ne connaît pas le mot de passe, un nouveau mot de passe pourra être attribué par le procédé Requête/Réponse.

Comment supprimer un utilisateur ?

1. Sélectionnez Programmes > ThinkVantage > ThinkVantage Software (TFS).
2. Dans l'écran de démarrage, sélectionnez successivement Settings > Power On Security. L'écran « Power-on Security » (Sécurité au démarrage) s'affiche.
3. Sélectionnez un utilisateur, puis cliquez sur [OK].



17 Configuration du mot de passe Windows

Avec l'authentification avant amorçage (PBA) comme premier composant du système, SafeGuard Easy requiert une authentification. Ce n'est qu'après que le système a été déverrouillé avec des données SafeGuard Easy valides que la boîte de dialogue d'ouverture de session de Windows apparaît.

Les utilisateurs trouvent cependant souvent fastidieux de se rappeler des mots de passe différents pour avoir accès à leur ordinateur.
Par conséquent, il est parfois nécessaire d'écrire ces différents mots de passe de façon à les mémoriser. Ceci représente toutefois un risque considérable pour la sécurité de la société. Les mots de passe oubliés représentent en outre un surplus de tâches pour le centre d'assistance dans les réseaux importants.

C'est pourquoi SafeGuard Easy offre une fonctionnalité de synchronisation SAL (Secure Automatic Logon) et de mot de passe pour éviter aux utilisateurs d'avoir à s'identifier de plusieurs façons. Désormais, il leur suffit d'entrer leurs données utilisateur une fois, pendant la préparation du démarrage. Pour que l'ouverture de session Windows soit encore plus conviviale, le modèle d'administration comprend des options supplémentaires.

17.1 Ouverture de session unique (Single Sign On) dans le système d'exploitation

L'ouverture de session automatique est une fonction confortable pour la procédure d'ouverture de session. Un utilisateur entre une fois ses données Windows. Pour les autres ouvertures de session, la connexion à Windows s'effectue automatiquement et l'utilisateur n'a plus à s'authentifier qu'avec les données d'utilisateur SafeGuard-Easy dans la PBA. SafeGuard Easy appelle cette procédure d'ouverture de session une **ouverture de session automatique** sécurisée, en bref **SAL**.

La SAL peut s'effectuer avec ou sans carte à puce. Ceci peut être sélectionné pendant l'installation de SafeGuard Easy.

L'ouverture de session automatique dans le système d'exploitation est optionnelle et peut être désactivée ultérieurement avec la commande SafeGuard Easy `Chgsal.exe`.

IMPORTANT :
Installez soit la SAL, **soit** l'ouverture de session automatique avec carte à puce.

Toutes les autres ouvertures de session dans d'autres applications doivent se faire manuellement.

L'ouverture de session dans Novell n'est prise en charge qu'avec une carte à puce.

Si l'option Windows « Connecter toujours cet utilisateur » est activée, aucune SAL ne peut être effectuée.

17.1.1 Installation de SAL (Secure Automatic Logon)

Techniquement, la SAL fonctionne comme suit : un utilisateur ouvre une session dans la PBA avec des données d'accès SafeGuard Easy et entre ensuite ses données Windows dans la boîte de dialogue d'ouverture de session de Windows. La SAL établit une relation entre l'utilisateur SafeGuard Easy ayant ouvert la session et l'utilisateur Windows et l'enregistre dans le fichier chiffré `Sgsal.dat`. Sgsal.dat se trouve dans *<disque système>*\`SYSTEM`. A une nouvelle ouverture de session dans la PBA, la SAL transmet les données Windows dans la boîte de dialogue d'ouverture de session Windows, sans intervention de l'utilisateur.

Comment configurer SAL :

1. installez SafeGuard Easy avec

   - "Ouverture de session automatique sécurisée".
     ATTENTION : n'installez pas l'option « Connexion automatique avec carte à puce" !
   - Authentification avant amorçage ("PBA") - option "Activation du mot de passe au démarrage du système"

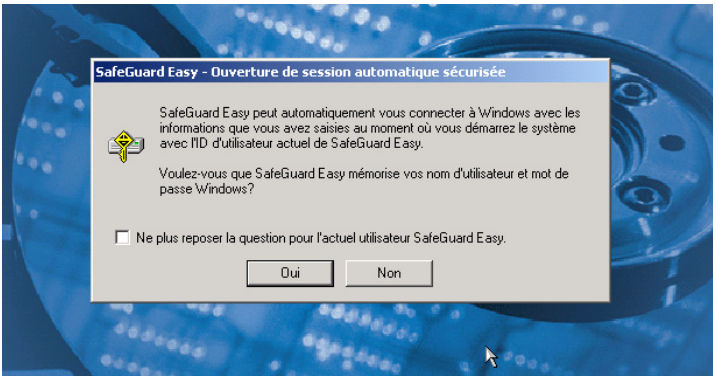
2. Redémarrez l'ordinateur.

3. Authentifiez-vous dans la PBA avec les données d'utilisateur SafeGuard Easy.

4. Après l'ouverture de session, la boîte de dialogue d'ouverture de session Windows usuelle apparaît à la première ouverture de session.

5. Remplissez les champs de saisie avec les informations d'ouverture de session correctes et cliquez sur [OK].

6. La boîte de dialogue SAL est alors affichée.



[Oui] : Active la relation entre l'utilisateur SafeGuard Easy et l'utilisateur Windows

[Non] : N'utilise pas la fonctionnalité SAL

L'état de la case à cocher « Don't ask this question again for the current SafeGuard Easy user » (Ne plus poser cette question pour l'utilisateur SafeGuard Easy actuel) indique si la boîte de dialogue doit être affichée après chaque connexion ou non.

7. Cliquez sur [OK] et cochez la case.

8. L'utilisateur SafeGuard Easy est associé à l'utilisateur Windows. Au prochain redémarrage de l'ordinateur, l'ouverture de session dans Windows sera automatiquement effectuée après saisie des données d'utilisateur SafeGuard Easy dans la PBA.

Modification du mot de passe Windows quand la fonction SAL est activée

Pour des raisons de sécurité, les mots de passe Windows doivent toujours être changés de temps à autre. La manière d'intégrer un mot de passe nouvellement défini dans l'ouverture de session automatique sécurisée dépend cependant de la méthode utilisée pour le modifier.

- **Modification forcée du mot de passe**
  Une modification de mot de passe est imposée dans le profil d'utilisateur via l'option « L'utilisateur doit modifier le mot de passe à la prochaine ouverture de session. Quand cette option est activée, l'utilisateur reçoit un message d'invite du système. A ce moment, la SAL est désactivée.

  Vous devez confirmer le message système en cliquant sur [OK]. La boîte de dialogue suivante demande à l'utilisateur d'entrer un nouveau mot de passe. Dès que l'utilisateur a confirmé le nouveau mot de passe, le fichier SAL est synchronisé avec les nouvelles données. A l'ouverture de session suivante, les données d'utilisateur Windows sont à nouveau transmises automatiquement.

- **L'utilisateur modifie lui-même son mot de passe**

  - Quand l'utilisateur appuie sur son Bureau sur les boutons [CTRL]+[ALT]+[SUPPR], il peut modifier son mot de passe dans la **boîte de dialogue de connexion Windows** via « Modifier le mot de passe". Quand la modification est effectuée de cette manière**, une synchronisation de mot de passe automatique** a lieu et les nouvelles données sont enregistrées dans le fichier `Sgsal.dat`. En cas d'ouverture de session après modification du mot de passe, l'utilisateur n'a pas à entrer de nouveau les données d'accès à Windows.
  - Lorsque le mot de passe est modifié par le service d'**administration des utilisateurs de Windows**, le système **n'accepte pas de façon automatique le nouveau mot de passe Windows** et ce dernier n'est pas enregistré dans le fichier `Sgsal.dat`.

Par contre, un message d'avertissement s'affiche pour indiquer que le mot de passe Windows n'est pas valide et que l'utilisateur doit entrer le nouveau mot de passe dans l'écran de connexion. Une fois le mot de passe modifié, l'utilisateur peut se connecter sans avoir à spécifier de nouveau ses données d'accès à Windows et SAL s'exécute sans notification.

17.1.2 Connexion SAL avec une carte à puce

La fonction Smartcard-SAL enregistre le code PIN sur la carte de manière que celle-ci soit automatiquement débloquée dans la PBA à l'entrée des données SafeGuard Easy. Les données d'ouverture de session de Windows sont alors chargées par la carte à puce (à condition qu'elles soient enregistrées sur la carte) et permettent une ouverture de session dans le système d'exploitation.

Pour utiliser la fonction Smartcard-SAL,

1. Installez SafeGuard Easy.

   - « Connexion automatique avec carte à puce »
     Avertissement : n'installez pas l'option « Ouverture de session automatique sécurisée ».
   - Authentification avant amorçage (« Activation du mot de passe au démarrage »)

2. Redémarrez l'ordinateur et ouvrez la session.

3. Authentifiez-vous dans la PBA avec les données d'utilisateur SafeGuard Easy.

4. Insérez votre carte dans son lecteur. La boîte de dialogue PIN s'affiche. Tapez le code PIN utilisateur.

5. Si la carte à puce ne comporte pas encore de données Windows, une boîte de dialogue s'affiche et demande si les données doivent à présent être entrées. Si vous cliquez sur « Oui », la boîte de dialogue « Windows Access Data » (Données d'accès Windows) s'affiche. Entrez le nom d'utilisateur, le mot de passe et le domaine à écrire sur la carte.

REMARQUE :
Veuillez noter que l'utilisateur Windows entré doit être également créé sur le poste de travail ! Dans le cas contraire, l'ouverture de session échoue.

6. La boîte de dialogue permettant d'activer/désactiver la fonction Smartcard-SAL est ensuite affichée.
   Avec Smartcard-SAL : [OUI]
   Sans Smartcard-SAL : [NON] :

7. Au prochain redémarrage de l'ordinateur, l'ouverture de session dans Windows sera automatiquement effectuée après saisie des données d'utilisateur SafeGuard Easy dans la PBA, la carte à puce étant insérée.

Modification de code PIN de carte à puce

Les codes PIN peuvent être modifiés avec des outils SafeGuard externes, par ex. avec Token Administration.

Lorsqu'un utilisateur modifie le code de la carte avec cet outil, ceci affecte la fonction SAL de la carte, dans la mesure où le code stocké sur la carte ne correspond plus au code stocké dans le fichier `Sgsal.dat`.
Au redémarrage, le système s'arrête dans la boîte de dialogue de saisie du code PIN. L'ancien code PIN spécifié déclenche un message d'erreur et l'utilisateur est invité à saisir le code PIN correct. Quand l'utilisateur tape alors le nouveau code PIN, l'ouverture de session a lieu et le code PIN est `enregistré` pour les ouvertures de session à venir.

17.1.3 Désactivation temporaire du module SAL

Avec `CHGSAL.EXE` dans le répertoire SafeGuard Easy, les fonctions SAL Smartcard-SAL peuvent être désactivées ultérieurement par un utilisateur possédant des droits d'administrateur Windows et de nouveau activées.

Procédez de la façon suivante :

1. Démarrez l'ordinateur en mode MS DOS ou sélectionnez la commande Exécuter dans le menu Démarrer de Windows, puis exécutez « cmd » pour afficher l'invite DOS.

2. Accédez au répertoire où est installé SafeGuard Easy. Tapez la commande suivante, avec les paramètres correspondants :

```
CHGSAL.EXE /SAL :ON | /SAL :OFF | /SCSAL :ON |
/SCSAL :OFF | [ /? ]
```

/SAL:ON	Activer SAL
/SAL:OFF	Désactiver SAL
/SCSAL:ON	Activer SAL avec carte à puce
/SCSAL:OFF	Désactiver SAL avec carte à puce
/?	Sommaire de l'Aide

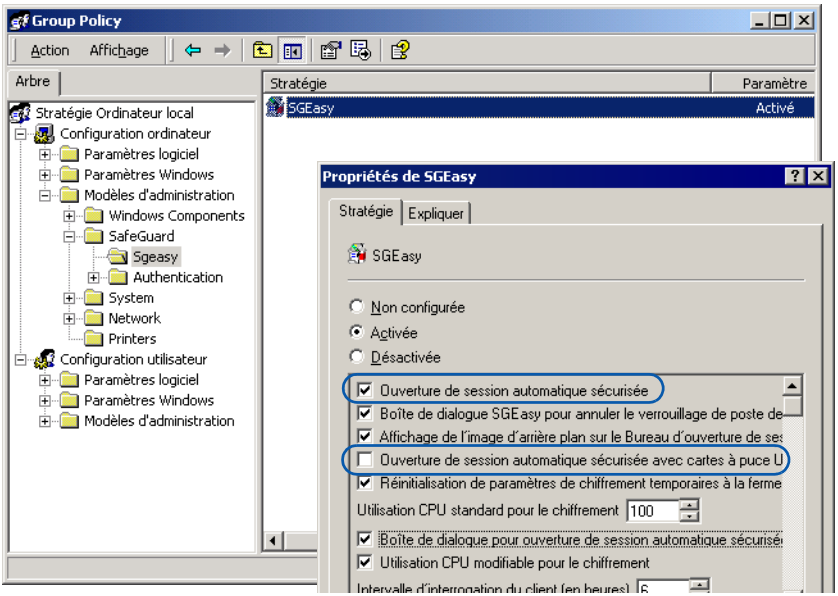
Cet outil ne fonctionne que lorsque SafeGuard Easy a été installé avec SAL ou Smartcard-SAL.

SAL et Smartcard-SAL peuvent également être activées via une stratégie dans le modèle d'administration Utimaco. La stratégie se trouve sous

Configuration ordinateur\Modèles d'administration

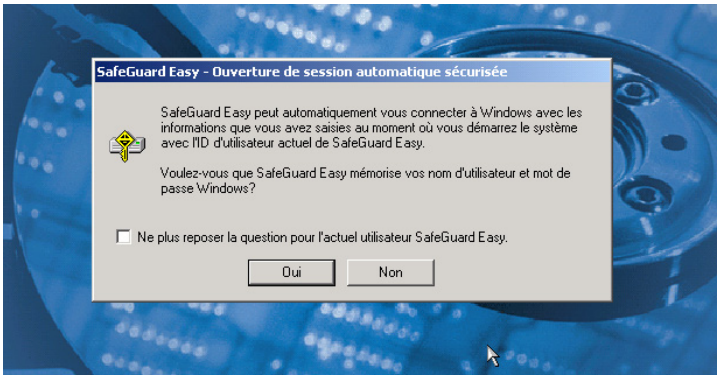
\SafeGuard
\SGEasy

Sur la page des propriétés, il suffit de cocher ou de décocher la case devant « Ouverture de session automatique sécurisée » ou « Ouverture de session automatique sécurisée » avec carte à puce".



17.1.4 Masquage de la boîte de dialogue SAL

La fonction SAL de SafeGuard Easy signale automatiquement les utilisateurs au système d'exploitation. La fonction SAL est activée par l'utilisateur lui-même via la boîte de dialogue SAL.

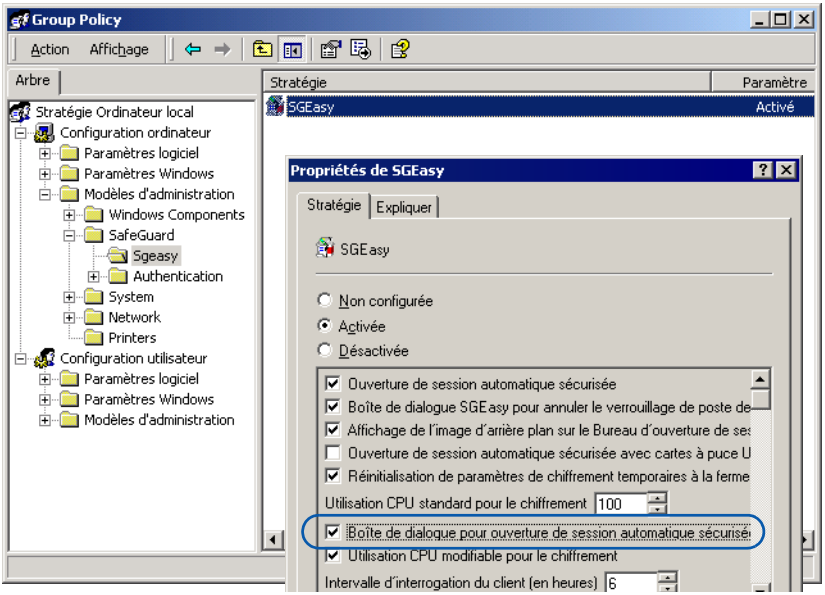


Pour éviter que des utilisateurs refusent l'ouverture de session automatique de Windows, SafeGuard Easy supprime à la demande la boîte de dialogue et exécute la fonction SAL sans confirmation.

La boîte de dialogue est supprimée au moyen d'une stratégie dans le modèle d'administration Utimaco sous.

Configuration ordinateur
\Modèles d'administration
 \SafeGuard
  \SGEasy

A la page des propriétés de « SGEasy », il suffit de supprimer la coche devant « Boîte de dialogue pour ouverture de session sécurisée".



17.1.5 Suppression de données pour la connexion SAL/SCSAL

Si vous supprimez le fichier `Sgsal.dat` (<disque système>\SYSTEM32), toutes les données d'utilisateur enregistrées sont supprimées. Après un redémarrage de l'ordinateur, vous pouvez attribuer de nouvelles données à un utilisateur SafeGuard Easy.

Quand un utilisateur SafeGuard Easy ayant déjà établi une connexion est supprimé d'un système, cette relation reste conservée à la création du même utilisateur.

17.1.6 Restriction

La SAL est provisoirement désactivée quand un utilisateur ouvre une session par Requête/Réponse via l'option « Ouverture de session unique. Cette « ouverture de session unique » permet à un utilisateur d'ouvrir une session dans l'authentification avant amorçage (PBA) de SafeGuard Easy sans connaître le mot de passe SafeGuard Easy (voir 'Maintenance à distance (Requête/Réponse)').

Si l'ouverture de session unique dans la PBA a été alors permise à un utilisateur, il n'ouvrira pas automatiquement de session dans Windows, même quand la SAL est activée. Dans ce cas, le système d'exploitation stoppe à la boîte de dialogue d'ouverture de session spécifique de Windows et requiert des données Windows valides. Toutes les actions sont dès lors enregistrées sous le nom de l'utilisateur ayant ouvert la session Windows.

Après chaque nouvelle ouverture de session régulière avec données SafeGuard Easy dans la PBA, la SAL et l'ouverture de session Windows automatique sont exécutées comme c'est normalement le cas.

17.2 Ouverture de session Windows et SafeGuard Easy avec un mot de passe identique (synchronisation de mot de passe)

La fonction SafeGuard Easy « Synchronisation de mot de passe » aide à minimiser les oublis éventuels de mot de passe en faisant du mot de passe Windows le mot de passe pour SafeGuard Easy.

Il s'ensuit que l'utilisateur n'a plus à se rappeler que d'un seul mot de passe (celui de Windows) pour ouvrir une session à la fois dans SafeGuard Easy et dans le système d'exploitation.

Si l'ouverture de session automatique sécurisée (SAL) est en outre active, il suffit d'entrer le mot de passe (Windows) dans l'authentification avant amorçage (PBA)

La synchronisation du mot de passe comporte également des mécanismes permettant de conserver synchrones le mot de passe SafeGuard Easy et le mot de passe Windows après changement de ces mots de passe.

Par défaut, la synchronisation du mot de passe est désactivée. Elle est activée au moyen d'une clé de registre.

17.2.1 Avantages de la synchronisation du mot de passe

- Les utilisateurs ne doivent se souvenir que d'un seul mot de passe (le mot de passe Windows).
- Le service d'assistance n'a plus qu'un mot de passe à administrer par utilisateur.
- L'administration en parallèle de SafeGuard Easy et de Windows n'a plus lieu d'être. Avec la configuration appropriée, les règles de mot de passe peuvent n'être gérées que via les stratégies de Windows.

17.2.2 Activation de la synchronisation de mot de passe

Comment préparer l'activation de la synchronisation de mot de passe

1. Activez « Secure Automatic Logon » (SAL).

   Nécessaire lorsque les noms d'utilisateur de SafeGuard Easy et de Windows sont différents.
   Non nécessaire lorsque les noms d'utilisateur de SafeGuard Easy et de Windows sont identiques.

2. Activation de l'authentification avant le démarrage.

3. Modification des règles de mot de passe de SafeGuard Easy.

   Si vous avez recours à la synchronisation de mots de passe, nous recommandons de désactiver toutes les règles de mot de passe de SafeGuard Easy !

En effet, lorsque les règles de mot de passe de SafeGuard Easy sont actives, elles risquent d'interférer avec les règles de compte Windows et d'entraîner des incohérences

> ***REMARQUE :***
> Vous devez procéder à la configuration suivante dans SafeGuard Easy :
> Minimum age of passwords = 0 (Âge minimum des mots de passe)

4. Activez la synchronisation des mots de passe.

   Définissez la clé de registre « PasswordSync » comme indiqué et redémarrez le PC.

5. Activez la fonctionnalité de connexion SafeGuard Easy Logon (Utimaco Master GINA).

   Dans une installation standard de SafeGuard Easy, Utimaco Master GINA est systématiquement installé et ne doit pas être activé à nouveau.
   Cependant, la synchronisation des mots de passe ne peut pas avoir lieu si Utimaco Master GINA a été désactivé de façon spécifique dans le cadre d'une distribution centralisée de SafeGuard Easy.

17.2.3 Activation de la synchronisation de mot de passe

Pour activer la synchronisation de mot de passe, des modifications doivent être effectuées dans la base de registres Windows. La base de registres peut être modifiée avec l'éditeur de registres (« regedit ») ou des mécanismes centralisés.

Une fois l'éditeur de registre ouvert, on trouve sous la rubrique de registre

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy

créez la valeur DWORD « **PasswordSync** ».

Pour activer la synchronisation de mot de passe, changez la valeur « PasswordSync » de 0 (désactivée) en 1 (activée).

Quittez ensuite le registre et redémarrez l'ordinateur.

17.2.4 Exécution de la synchronisation de mot de passe

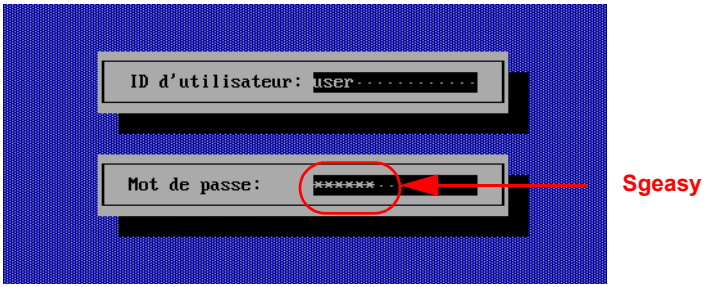
1. Exécutez toutes les mesures de préparation pour la synchronisation du mot de passe.

   Veuillez ne pas oublier de définir le paramètre SafeGuard Easy : Définir l'« Age minimum des mots de passe » sur la valeur "0".

2. Redémarrez l'ordinateur.

3. L'écran d'ouverture de session SafeGuard Easy (PBA) apparaît. Entrez les données utilisateur de SafeGuard Easy, par exemple

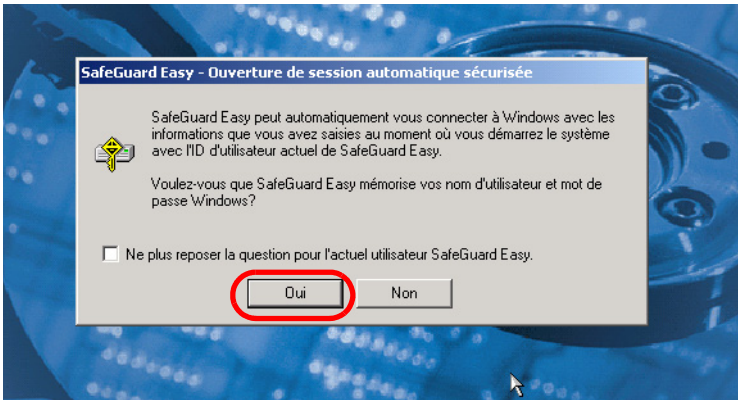
   Nom d'utilisateur SGE : **Utilisateur**
   Mot de passe SGE :**Sgeasy**



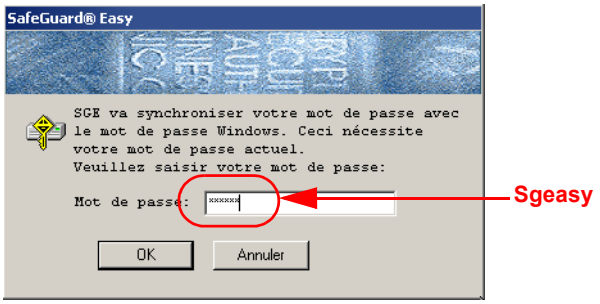
4. La boîte de dialogue d'ouverture de session de Windows apparaît. Entrez les données Windows, par exemple

   Nom utilisateur Windows :**AMiller**
   Mot de passe Windows :**WinSecurite**

5. La boîte de dialogue SAL apparaît. Confirmez avec [OUI].



6. La boîte de dialogue pour synchronisation de mot de passe apparaît. Le mot de passe SafeGuard Easy vous est demandé (dans notre exemple « **Sgeasy** »). Quand le mot de passe est correct, SafeGuard Easy « autorise » la synchronisation des mots de passe. Confirmez avec [OK].

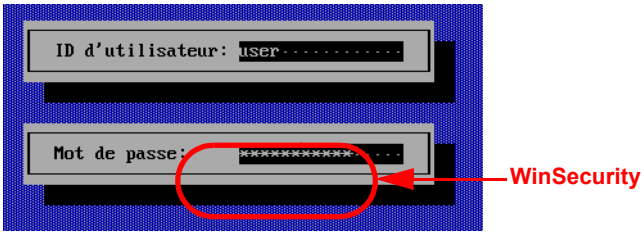


7. Le Bureau de Windows apparaît.

8. Redémarrez l'ordinateur.

9. La PBA apparaît. Tapez les données de l'utilisateur de SafeGuard Easy.

   Nom d'utilisateur SGE : **User**
   Mot de passe SGE : **WinSecurity (= mot de passe Windows)**



10. L’ordinateur démarre (une ouverture de session dans Windows n’est plus nécessaire !)

11. Le Bureau de Windows apparaît.

17.2.5 Modification du mot de passe Windows quand la synchronisation de mot de passe est activée

IMPORTANT :
Les stratégies de mot de passe de Windows – et non pas les règles SafeGuard Easy – sont appliquées au nouveau mot de passe !

1) L'utilisateur modifie localement le mot de passe Windows via la boîte de dialogue Sécurité Windows ([Ctrl]+[Alt}+[Suppr])

Résultat : Le nouveau mot de passe Windows est immédiatement valable pour Windows et pour SafeGuard Easy.

2) L'administrateur modifie centralement ou via télé-assistance le mot de passe Windows

Résultat : le nouveau mot de passe n'est valable que pour Windows, et non pas pour SafeGuard Easy.

Le « vieux » mot de passe SafeGuard Easy et le « nouveau » mot de passe Windows sont ainsi à nouveau synchronisés :

1. Après un redémarrage, l'utilisateur entre l'ancien mot de passe dans la PBA.

2. L'ouverture de session automatique de Windows échoue, car le mot de passe SafeGuard Easy et le mot de passe Windows ne sont pas encore synchronisés. L'utilisateur est pour cette raison invité, sur l'écran d'ouverture de session de Windows , à saisir le nouveau mot de passe Windows.

3. La boîte de dialogue SAL apparaît et doit être à nouveau confirmée en cliquant sur [Oui].

4. La boîte de dialogue pour synchronisation de mot de passe apparaît. La synchronisation a lieu suite à la saisie de « l'ancien » mot de passe.

5. Après redémarrage de l'ordinateur, l'utilisateur ouvre une session dans la PBA avec le nouveau mot de passe (Windows).

17.2.6 Modifier le mot de passe SafeGuard Easy

Par la synchronisation du mot de passe, le mot de passe Windows actuel devient à chaque fois le mot de passe pour SafeGuard Easy.

Utimaco recommande par conséquent de ne pas modifier le mot de passe SafeGuard Easy. Pour le changement de mot de passe, nous recommandons l'utilisation des mécanismes Windows bien connus.

Si, à telle ou telle occasion, il est cependant nécessaire de modifier le mot de passe SafeGuard Easy, le nouveau mot de passe est assujetti aux règles de mot de passe définies dans l'administration SafeGuard Easy.

17.2.7 Annulation de la boîte de dialogue de synchronisation du mot de passe

La permission de fermer la boîte de dialogue de synchronisation du mot de passe sans qu'elle soit remplie peut être réglée par clé de registre. Avec ce réglage, des administrateurs peuvent par ex. obliger des utilisateurs à procéder à une synchronisation du mot de passe.

Une fois l'éditeur de registre ouvert, on trouve sous la rubrique de registre

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
Sgeasy

créez la valeur DWORD « **ForcePasswordSync** ».

Avec la valeur « 1 », le bouton « Annuler » est affiché en gris et l'utilisateur ne peut poursuivre que lorsque la boîte de dialogue de synchronisation est remplie. La valeur « 1 » permet aux utilisateurs de contourner cette boîte de dialogue.

Quittez ensuite le registre et redémarrez l'ordinateur.

17.2.8 Restrictions

SafeGuard Easy limite les mots de passe à 16 caractères
A l'ouverture de session dans la PBA, SafeGuard Easy n'accepte que les mots de passe comportant au maximum 16 caractères. Cette règle est prescrite par SafeGuard Easy et elle ne peut pas être contournée. Si un mot de passe Windows synchronisé est trop long, les caractères en excès sont « coupés » pour l'authentification dans SafeGuard Easy (PBA, administration, etc.).

Exemple :
Mot de passe Windows (avec 20 caractères) : « UtimacoSecurity12345 »
Ouverture de session dans la PBA (avec 16 caractères) :
« UtimacoSecurity1 »

Il n'y a pas de synchronisation quand le mot de passe Windows

- n'obéit pas aux règles de mot de passe internes de SafeGuard Easy
  (voir 'Règles générales de mot de passe internes dans SafeGuard Easy')
- se trouve dans l'historique des mots de passe SafeGuard Easy
- contient certains caractères spéciaux

  Sont autorisés : tous les caractères pouvant être
  générés par appui sur une touche ou en combinaison avec la touche MAJ, par ex. ! " § $ % &/( ) = ? * ' ; : -
  Ne sont pas autorisés :
  tous les caractères générés via la touche ALT Gr, par ex. ² ³ { [ ] } \~ @ € | µ é è ê (et toutes les autres lettres avec accent)

REMARQUE :
Certains claviers permettent de créer un caractère spécial en appuyant sur une touche ou avec une combinaison incluant la touche de majuscules, notamment pour certains caractères accentués sur le clavier français. Dans ce cas, le caractère spécial est pris en charge par la synchronisation de mots de passe de SafeGuard Easy.

Autres restrictions quand la synchronisation du mot de passe est activée :

- Pas plus de 16 utilisateurs Windows autorisés par machine (16 = nombre maximum d'utilisateurs SafeGuard Easy).
- La synchronisation du mot de passe avec le jeton n'est possible que si le jeton reste inséré pendant l'échange du mot de passe.

17.2.9 Que faire, si ...

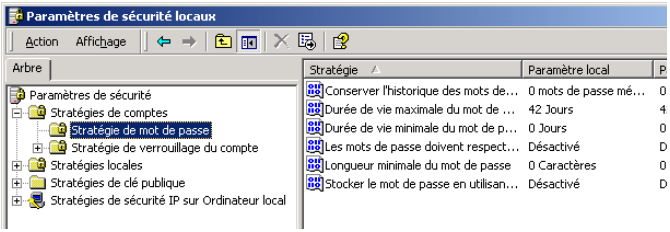
... la synchronisation de mot de passe échoue et un message d'erreur est affiché ?
Les raisons suivantes sont possibles :

- le mot de passe synchronisé n'obéit pas aux règles de mots de passe de SafeGuard Easy (mot par ex. trop court, etc.)
- le mot de passe synchronisé contient des caractères spéciaux invalides ou non pris en charge par SafeGuard Easy
- le mot de passe synchronisé a déjà été utilisé selon l'historique de mots de passe SafeGuard Easy.

Résolution du problème :

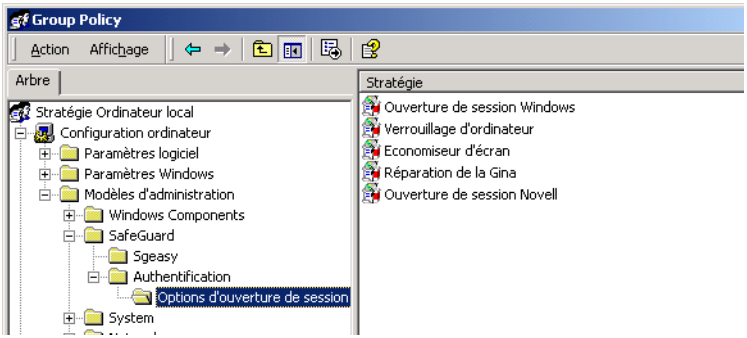
Définissez un nouveau mot de passe synchronisé n'entrant pas en conflit avec les règles Windows/SafeGuard Easy.

... vous ne savez pas comment sont définies les stratégies pour le mot de passe synchronisé (= mot de passe Windows) ?
Dans le menu de démarrage de Windows, appelez **Paramètres / Panneau de configuration / Outils d'administration / Paramètres de sécurité locaux**. Sous Stratégies de comptes > Stratégie de mot de passe, tous les réglages possibles sont disponibles.



17.3 Options supplémentaires de connexion sous Windows

Vous pouvez utiliser le modèle d'administration Sguard.adm pour définir des paramètres connexion Windows par l'intermédiaire de stratégies de groupe. On peut ici en outre définir par ex. des paramètres d'économiseur d'écran normalement intouchables dans Windows.



17.3.1 Personnalisation de l'écran de connexion de Windows

Ces paramètres conditionnent l'affichage du bureau pendant les procédures de connexion et déconnexion, et lorsque la station de travail est verrouillée.

Cette stratégie se trouve dans le modèle d'administration de SafeGuard Easy sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\Authentification
\Options d'ouverture de session
\Ouverture/fermeture de session Windows

- **Utiliser l'écran d'ouverture de session Utimaco**
  Quand la case est cochée, la boîte de dialogue d'ouverture de session est affichée à l'ouverture de session. Quand la case n'est plus cochée, vous pouvez ouvrir une session dans le système avec la boîte de dialogue d'ouverture de session de Windows.

- **Utiliser l'écran de démarrage Utimaco**
  Quand la case est cochée, la boîte de dialogue SafeGuard Commencer ouverture de session est affichée. Vous êtes invité à taper [Ctrl] + [Alt] + [Suppr] pour ouvrir la boîte de dialogue d'ouverture de session. Quand la case n'est plus cochée, la boîte de dialogue Windows correspondante est affichée.

- **Utiliser l'écran de verrouillage Utimaco**
  Quand la case est cochée, la boîte de dialogue SafeGuard Lock est affichée au lieu de la boîte de dialogue Windows au verrouillage du poste de travail avec [Ctrl] + [Alt] + [Suppr.] Si une connexion utilisateur non valide a été enregistrée, cette dernière s'affiche dans la boîte de dialogue de verrouillage d'Utimaco.

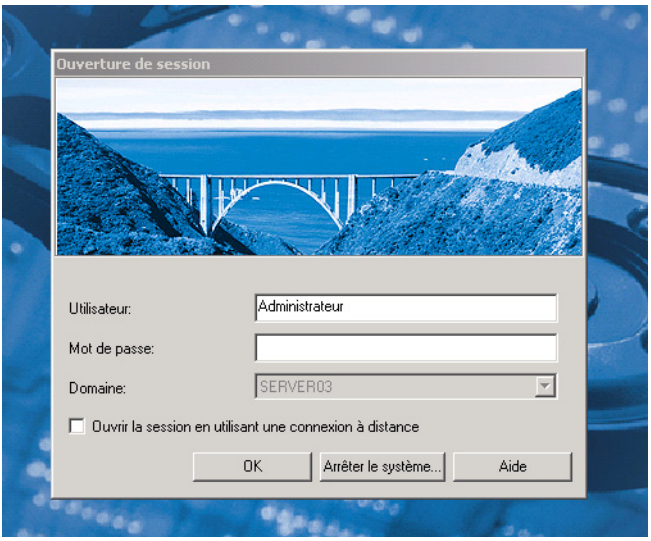
- **Désactiver la vérification des données utilisateur avec le RAS**
  Quand la case est cochée, aucune vérification préliminaire n'est effectuée à l'établissement de la connexion RAS.

- **Activer le verrouillage de fermeture de session**
  Si un utilisateur a verrouillé un poste de travail, vous pouvez permettre à d'autres utilisateurs le déverrouillage en cochant la case. Pour annuler le verrouillage, l'ouverture de session par l'autre utilisateur suffit.

- **Désactiver l'option RAS de l'écran d'ouverture de session Utimaco**
  Quand la case est cochée, l'option « Ouverture de session via réseau RAS » est désactivée dans la boîte de dialogue d'ouverture de session Utimaco.

- **Afficher le plugin SafeGuard dans les écrans d'ouverture de session tiers**
  Quand cette option est active, la boîte de dialogue d'ouverture de session tiers indique également que SafeGuard Authentication est installé.

- **Replace bitmap with**
  (Remplacer le bitmap par) Ce champ d'édition, qui s'affiche dans la boîte de dialogue de connexion, permet de spécifier un fichier bitmap, tel qu'un logo de société avec un arrière-plan standard. Le bitmap doit être au format .bmp et doit résider dans le dossier System32 du dossier d'installation de Windows. La taille de l'image est fixée à 413x140 pixels.



17.3.2 Verrouillage du poste

Au verrouillage de poste, on détermine après combien de tentatives infructueuses d'ouverture de session l'ordinateur va être verrouillé et comment le temps d'attente entre des tentatives d'ouverture de session augmente. Le mécanisme ne fonctionne qu'avec les utilisateurs qui ne sont pas membres du groupe local des administrateurs.

Cette stratégie se trouve dans le modèle d'administration de SafeGuard Easy sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\Authentification
\Options d'ouverture de session
\Verrouillage du poste

Le mécanisme ne fonctionne qu'avec les utilisateurs qui ne sont pas membres du groupe local des administrateurs. Vous trouverez les restrictions dans l'environnement du terminal serveur au chapitre *Support Terminal Server*.

- **Essais d'ouverture de session**
  Dans ce champ, vous déterminez le nombre des essais infructueux d'ouverture de session par un utilisateur se connectant avec un nom et/ou un mot de passe incorrect. Si vous spécifiez par ex. « 3 », l'ordinateur sera verrouillé si l'utilisateur entre trois fois de suite un nom ou un mot de passe incorrect à l'ouverture de session.
  Valeur minimum/maximum : 0-999

- **Délai en secondes**
  Entrez ici la valeur de base qui, multipliée avec le « Multiplicateur », donnée le temps d'attente après la première tentative infructueuse d'ouverture de session. Quand une nouvelle tentative infructueuse est effectuée, le temps d'attente de la tentative précédente est pris comme valeur de base. La valeur par défaut est 10.
  Valeur minimum/maximum : 0-999

- **Multiplicateur**
  Le multiplicateur est multiplié avec le délai de base en secondes.
  La valeur par défaut est 3.
  Valeur minimum/maximum : 0-99

- **Désactiver le Ctrl+Alt+Suppr lorsque la station est verrouillée**
  Le verrouillage du poste ne peut pas être annulé avec Ctrl+Alt+Suppr en cas d'ouverture de session par jeton.

Exemple :

Délai de 10 secondes et multiplicateur de :
1ère tentative infructueuse : 50 secondes d'attente 5)
2ème tentative infructueuse : 250 secondes d'attente 5)
3ème tentative infructueuse : 1250 secondes d'attente (250 * 5)

REMARQUE :

Le verrouillage du poste peut être annulé

- en redémarrant l'ordinateur
- via l'ouverture de session par l'administrateur.
- en répliquant des données à partir du contrôleur de domaine. A ce sujet, veuillez noter également le verrouillage d'utilisateur de Windows.

17.3.3 Économiseur d'écran

Si, sur un poste de travail, on a spécifié la mise en route de l'économiseur d'écran au bout d'une durée donnée, vous pouvez décider comment le système doit réagir à son activation après une période déterminée. Les paramètres ne sont effectifs que lorsque l'économiseur d'écran de Windows est lui aussi activé !

Cette stratégie se trouve dans le modèle d'administration de SafeGuard Easy sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\Authentification
\Options d'ouverture de session
\Économiseur d'écran

- **Action**
  La section *Action* permet de définir les réactions suivantes lors de l'exécution d'un économiseur d'écran. Ces actions peuvent avoir différents effets selon l'endroit où elles sont définies (sessions de la station de travail locale ou du serveur de terminal). Pour définir ces actions pour les sessions de serveur de terminal, vous devez les définir sur le serveur de terminal :

  A) Logoff user :
  (Déconnecter l'utilisateur) L'utilisateur actif sera déconnecté de l'ordinateur. D'autres utilisateurs enregistrés sur le poste de travail ou dans le réseau peuvent (aussi) ouvrir une session.

  B) Arrêt du système
  Le PC est automatiquement arrêté et doit être redémarré pour une autre session de travail.
  Lors des sessions Terminal Server, l'utilisateur sera déconnecté.

  C) Restart the workstation:
  (Redémarrer la station de travail) La station de travail sera redémarrée de façon automatique.

Lors des sessions Terminal Server, l'utilisateur sera déconnecté.

D) Hibernate the workstation
(Mise en veille prolongée de la station de travail) Place l'ordinateur en mode Veille prolongée.
Lors des sessions Terminal Server, l'utilisateur sera verrouillé.

REMARQUE :
Si SafeGuard Advanced Security et SafeGuard Easy sont installés sur le même ordinateur, cette option fonctionne uniquement à partir de SafeGuard Easy Version 4.0.

E) Disconnect the session
(Déconnecter la session) N'a aucun effet sur la station de travail locale.
Lors des sessions Terminal Server, la session sera déconnectée.

F) Standby
(Veille) L'ordinateur est mis en veille.
Lors des sessions Terminal Server, la session sera verrouillé.

Aperçu des actions possibles et leurs effets sur l'ordinateur local ou sur la session terminal serveur :

Paramètre	**Action local ou sur serveur**	**Action dans session terminal serveur**
<Aucun>	aucune	aucune
Fermeture de la session	fermer	fermer
Arrêter la station de travail	arrêter	fermer
Redémarrage du système	redémarrer	fermer
Mettre en veille la station de travail	mettre en veille prolongée	Verrouiller la session
Déconnexion de la session	aucune	Déconnexion de la session
En veille	En veille	Verrouiller la session

REMARQUE :
Lors d'une **session Bureau à distance**, les mêmes actions s'appliquent comment indiqué dans la section **local ou serveur**.

- **Délai**
  Sous "Délai", vous réglez la durée (en minutes) après laquelle le système doit exécuter une action décrite. La valeur par défaut est 15. Vous pouvez taper le nombre directement au clavier ou le modifier avec les touches fléchées.
  Valeurs minimales et maximales : 0-900

- **Disable Screensaver**
  (Désactiver l'écran de veille) De manière générale l'écran de veille est désactivé lorsqu'un utilisateur déplace la souris ou utilise le clavier. Il peut ensuite poursuivre normalement son travail. Si la case « Désactiver l'économiseur d'écran » est cochée, le poste de travail est verrouillé. L'accès au poste de travail n'est plus possible qu'après saisie des données d'accès correctes.

Exemple :

Sur les postes de travail, on a spécifié que l'économiseur d'écran devait démarrer dix minutes après la dernière action de l'utilisateur. Si vous avez choisi l'action 'Arrêt du système' et entré un délai de 13, le PC sera automatiquement arrêté 23 minutes après la dernière action effectuée sur le poste de travail.

17.3.4 Réparation de la GINA

Utimaco utilise son propre composant de connexion (SafeGuard GINA (`SGGINA.dll`). Suite à l'installation, il s'agit toujours du premier composant de connexion Windows appelé par le système d'exploitation.

L'installation d'autres produits peut modifier l'ordre des composants d'ouverture de session appelés.

Cette stratégie se trouve dans le modèle d'administration de SafeGuard Easy sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\Authentification
\Options d'ouverture de session
\Réparation de la Gina

- **Réparer le registre GINADLL si modifié**
  Assure le que le composant SafeGuard GINA apparaît en première position lors du démarrage du système d'exploitation.

- **En cas de GINA inconnue**

  Demander à l'utilisateur
  A la première initialisation, le système demande dans une boîte de dialogue si la GINA inconnue ou la GINA Microsoft d'origine doit être utilisée. Si, dans cette boîte de dialogue, la case « Ne plus afficher ce message » est cochée, l'action de l'utilisateur est enregistrée dans le registre et cette valeur est utilisée au prochain redémarrage.

  Utiliser la GINA Microsoft d'origine
  La GINA Microsoft d'origine est placée en première position de la chaîne GINA.

  Utiliser la GINA inconnue
  La GINA inconnue est placée en première position de la chaîne GINA.

17.3.5 Ouverture de session Novell

Peut uniquement être utilisé en combinaison avec la fonction de signature unique de SafeGuard Advanced Security.

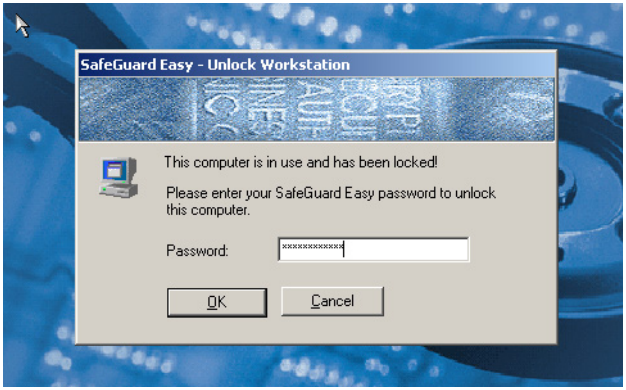
Cette règle permet à SafeGuard Single Sign On de détecter les boîtes de dialogue de connexion de Novell lorsqu'une version multilingue est utilisée. SafeGuard Single Sign On détecte le titre de la boîte de dialogue Novell par défaut et de la boîte de dialogue de connexion entré ici et les complète avec les informations de connexion Novell qui figurent sur le jeton.

Cette stratégie se trouve dans le modèle d'administration de SafeGuard Easy sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\Authentification
\Options d'ouverture de session
\Ouverture de session Novell

18 Mode de chiffrement SafeGuard Easy Verrouillage du poste

SafeGuard Easy peut remplacer le verrouillage de poste de travail Windows normal par sa propre boîte de dialogue.



Quand l'ordinateur est en mode veille, seul l'utilisateur l'ayant verrouillé peut réactiver l'interface utilisateur en entrant son mot de passe SafeGuard Easy.

Écran et interface utilisateur sont verrouillés

- après appui sur [CTRL]+[ALT]+[SUPPR] et [Verrouiller ordinateur]
- après écoulement d'une durée réglée sans intervention de l'utilisateur (temps d'attente)
- en retirant le jeton

Pour le verrouillage du poste de travail, le même écran d'arrière-plan que pendant l'ouverture de session apparaît (voir 'Remplacement de l'image d'arrière plan de l'ouverture de session Windows').

18.1 Conditions

Le verrouillage du poste de travail ne fonctionne que si

- l'authentification avant amorçage est active
- l'utilisateur a été automatiquement connecté via SAL au système d'exploitation
- l'économiseur d'écran de Windows est activé avec protection par mot de passe

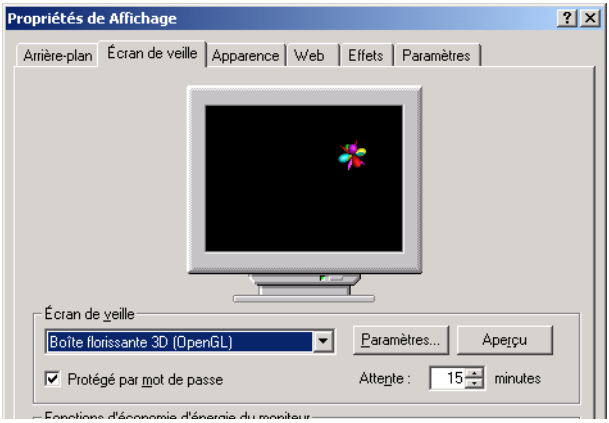
Après configuration de l'économiseur d'écran de Windows, l'ordinateur doit être redémarré.

Le verrouillage de poste de travail de SafeGuard Easy est ultérieurement désactivé quand un utilisateur ferme et rouvre une session après une ouverture de session avec succès dans Windows.

18.2 Activation de l'économiseur d'écran de Windows avec protection par mot de passe

Le verrouillage du poste de travail SafeGuard Easy est commandé dans les paramètres Windows via Programmes / Panneau de configuration/ Affichage / Écran de veille.

Redémarrez la station de travail après avoir activé l'économiseur d'écran.



Il convient de choisir également un économiseur d'écran et d'adapter ensuite les options « Protégé par mot de passe » et « Attente.

- **Protégé par mot de passe**
  Impose la demande du mode de passe SafeGuard Easy, la case doit être cochée.

- **Attente**
  Indique la durée (en minutes) devant s'écouler sans intervention de l'utilisateur sur le poste de travail avant que le verrouillage du poste de travail ne s'active.

Si vous entrez ici 15, l'écran sera éteint au bout de 15 minutes si aucune intervention de l'utilisateur n'a lieu pendant ce temps. Pour continuer son travail, l'utilisateur doit ouvrir à nouveau une session avec le mot de passe SafeGuard Easy.

Pour protéger le poste de travail contre l'intervention non autorisée de tierces personnes, veuillez activer le verrouillage de poste de travail.

18.3 Désactivation du verrouillage de poste de travail SafeGuard Easy

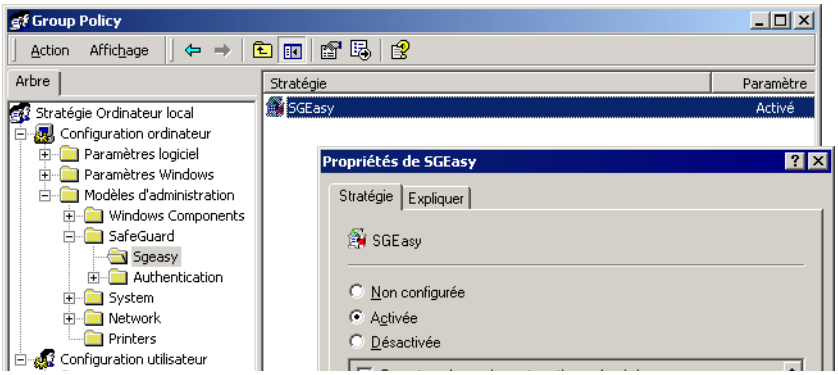
Vous avez la possibilité de désactiver le verrouillage de poste de travail SafeGuard Easy et d'afficher à la place la boîte de dialogue Windows normale.

AVERTISSEMENT :
La boîte de dialogue Windows normale n'est pas déverrouillée avec le mot de passe SafeGuard Easy, mais avec le mot de passe de Windows. La protection par mot de passe de SafeGuard Easy pour le verrouillage de poste de travail n'est alors plus disponible.

Si **AUCUN** verrouillage de poste de travail SafeGuard Easy ne doit être indiqué, ceci peut être configuré via la stratégie « Utiliser boîte de dialogue SGEasy pour annuler le verrouillage de poste de travail » (retirez la coche devant la stratégie).

Cette stratégie se trouve dans le modèle d'administration de SafeGuard Easy sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\SGEasy



19 Activation à distance (Wake-On-LAN) sécurisée

Le mode d'activation à distance sécurisée de SafeGuard Easy constitue le moyen le plus sûr d'allier les avantages de l'activation à distance et le chiffrement des disques durs pour protéger le PC. Pour ce faire, l'activation à distance de SafeGuard Easy autorise la désactivation de l'authentification avant amorçage pendant un nombre prédéfini de redémarrages. Ensuite, cette fonction peut être réactivée pour permettre, par exemple, la distribution de nouveaux logiciels. Cependant, avec l'activation à distance, il est impossible de désactiver l'authentification avant amorçage et de s'introduire dans le système avec un identifiant Windows.

WOL représente un compromis optimal entre la protection avant amorçage et l'exécution de tâches exécutées de manière centralisée.

19.1 Aperçu

En général, l'activation à distance sécurisée permet à tout ordinateur d'un réseau local d'être démarré par un autre ordinateur du réseau. Ceci peut se produire de façon à charger les nouvelles mises à jour ou procéder à des tâches de maintenance de routine.

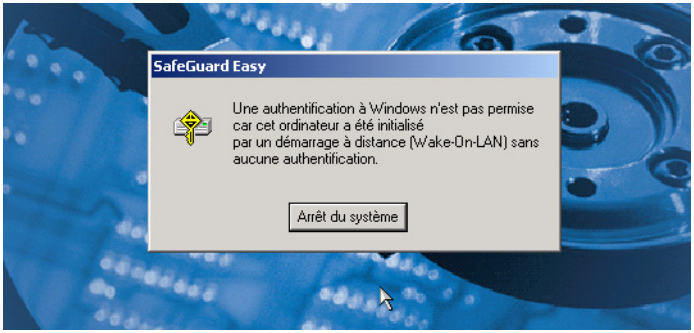
Il n'était pas possible d'utiliser cette méthode simple d'exécution de tâches centralisées sur les ordinateurs sécurisés avec les versions de SafeGuard Easy antérieures à la version 4.0, du fait de l'authentification avant amorçage (PBA). Ceci était dû au fait que l'ordinateur s'arrêtait à la phase d'authentification avant amorçage (PBA) et que l'utilisateur devait entrer ses données SafeGuard Easy. Dans ce cas, le système d'exploitation ne redémarre pas et ne crée pas de lien réseau. Par conséquent, les tâches contrôlées de façon centrale devenaient impossibles à exécuter.

La nouvelle technique WOL dans SafeGuard Easy permet à l'administrateur d'autoriser aux clients SafeGuard Easy un certain nombre de redémarrages avant d'activer à nouveau l'authentification avant amorçage. Par exemple, lorsque le nombre de connexions automatiques est défini sur « 3 », le PC peut être redémarré trois fois de suite avec l'authentification avant amorçage (PBA) désactivée. Lors du quatrième démarrage, l'écran d'authentification avant amorçage (PBA) s'affiche de nouveau de façon automatique (si cette fonction est active).

Lors de ces phases de connexion automatique, la boîte de dialogue de connexion de Windows ne s'affiche pas. L'ordinateur démarre de façon autonome et la mise à jour automatique du logiciel peut être exécutée via le réseau.

19.2 Verrouillage de l'ouverture de session Windows

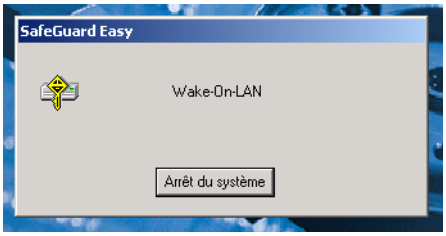
En mode Wake On LAN, l'ordinateur est protégé contre les ouvertures de session Windows locales par l'utilisateur. Par contre, le système affiche une boîte de dialogue d'activation à distance (« Windows logon is not allowed because this workstation was started by Wake On LAN without authentication. » - La connexion Windows n'est pas autorisée car cette station de travail a été activée à distance sans authentification).



Cependant, le verrouillage de connexion Windows en mode d'activation à distance fonctionne uniquement lorsque SafeGuard GINA (Utimaco Master GINA) est installé !

19.3 Adapter le message WOL

Vous pouvez adapter le message WOL (« Une authentification à Windows n'est pas autorisée ... ») de manière centralisée à l'aide des mécanismes standard du système Windows (entrées de la base de registre).



Insérer le bouton Redémarrer

Les utilisateurs doivent redémarrer l'ordinateur lorsque la clé de registre [DWORD] a été définie sur « 0 » :

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy
WOLDisableShutdown

Modifier le message

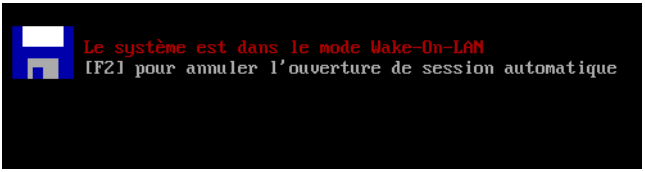
Une adaptation du texte du message s'affichera à l'écran si vous avez saisi un nouveau en dessous de la clé de registre suivante [STRING] :

HKEY_LOCAL_MACHINE
Software
Utimaco
SGEasy
WOLNotice

19.4 Annulation temporaire du verrouillage d'activation à distance

Si un utilisateur doit utiliser son ordinateur malgré le verrouillage WOL, il est possible d'annuler provisoirement ce verrouillage.

Pendant la phase de pré-amorçage, une icône de disquette s'affiche pendant environ 5 secondes dans la partie supérieure gauche de l'écran.



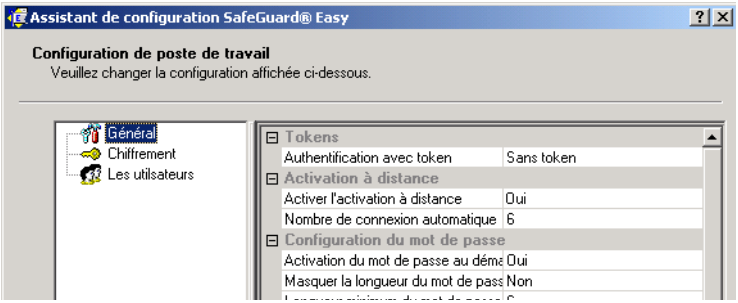
Si, pendant cette durée, [F2] est actionnée, la PBA apparaît et l'utilisateur peut ouvrir normalement sa session avec les données SafeGuard Easy valides et plus tard dans Windows. L'utilisateur remarque que l'ordinateur se trouve en mode Wake On LAN à un petit avertissement clignotant au-dessus de [F2].

Si l'ordinateur est démarré en mode sécurisé (appuyer sur [F8] pendant le processus d'amorçage), le verrouillage incorporé permet seulement aux utilisateurs possédant des droits d'administrateur d'ouvrir leur session en mode sécurisé.

19.5 Configuration de l'activation à distance

WOL est utilisé en règle générale dans les environnements informatiques plus étendus et non pas pour les ordinateurs autonomes. L'administrateur crée un fichier de configuration avec les paramètres WOL correspondants et le distribue aux clients dans l'entreprise.

Le mode d'activation à distance SafeGuard Easy Wake-On LAN sécurisée est configuré dans les outils d'administration par le biais de la page « Général ».



Les réglages suivants sont possibles :

- **Activer l'activation à distance** :
  Active/désactive le mode Wake On LAN.

- **Nombre de connexions automatiques** (par défaut : 1) :
  Définit le nombre des redémarrages avec PBA désactivée quand l'activation à distance est en service.

  Utimaco recommande de toujours autoriser un redémarrage de plus que nécessaire pour contourner les problèmes inattendus.

Dès que le fichier de configuration a été distribué aux ordinateurs des utilisateurs, le PC redémarre n fois sans PBA. Une fois que le nombre de redémarrages sans PBA défini est atteint, l'authentification avant l'amorçage est réactivée et demande les données d'utilisateur SafeGuard Easy correctes.

20 Mise en veille prolongée

La fonctionnalité de Windows « Mise en veille prolongée » est très appréciée des utilisateurs d'appareils mobiles pour interrompre provisoirement leur travail. Lorsqu'un ordinateur portable disposant d'une fonction de mise en veille prolongée active est arrêté pendant une opération, il s'arrête automatiquement. Lors du redémarrage suivant, il rétablit l'écran tel qu'il était lors de la demande d'arrêt.

Pour la sauvegarde des données en veille prolongée, SafeGuard Easy propose ici une solution particulière qui n'est pas propre à tout produit de chiffrement.

20.1 Aperçu

En mode Veille prolongée, le contenu de la mémoire vive est écrit dans un fichier système, Hiberfile.sys, situé dans le répertoire racine de la partition du système d'exploitation (généralement C:) et est stocké sur le disque dur. La taille du fichier Hiberfile.sys correspond à peu près à la taille de la mémoire de travail disponible. L'ordinateur est ensuite éteint. Si vous rallumez l'ordinateur, le Bureau réapparaît exactement tel que vous l'avez quitté à l'extinction de l'ordinateur, c'est-à-dire que le contenu du fichier Hiberfile.sys est réécrit dans la mémoire de travail. Après désactivation du mode de veille prolongée, le fichier Hiberfile.sys est invalidé.

20.2 Mise en veille prolongée et SafeGuard Easy

Lorsque la partition système du système d'exploitation n'est pas chiffrée, l'activation du mode Veille prolongée représente un risque de sécurité dans la mesure où cette procédure transfère tout le contenu de la mémoire vive, qui est alors accessible librement par des personnes non autorisées.

Dans une partition de système d'exploitation chiffrée, SafeGuard Easy permet d'utiliser le mode de veille prolongée et de chiffrer le fichier Hiberfile.sys créé, puis de le stocker de façon sûre sur le disque dur. Toutes les données sont ainsi chiffrées à tout moment sur le disque dur. L'accès au système est réservé exclusivement aux utilisateurs ayant pu s'authentifier avec des données SafeGuard Easy correctes après un redémarrage de l'ordinateur en mode PBA (pour autant qu'elle soit activée).

REMARQUE :
Quand plusieurs utilisateurs SafeGuard Easy se partagent un poste de travail, chacun d'entre eux parvient, après authentification via diverses données SafeGuard Easy dans la PBA, dans le profil de l'utilisateur qui a initié la mise en veille prolongée.

Il est possible dans ce cas d'exiger l'entrée du mot de passe Windows au redémarrage (Options d'alimentation / Avancé / Demander un mot de passe lorsque l'ordinateur sort de mise en veille). Ce paramètre oblige l'utilisateur à ouvrir une session supplémentaire avec ses données Windows (inconvénient : double authentification).

20.3 Conditions et restrictions

La combinaison de SafeGuard Easy et de la mise en veille prolongée fonctionne dans les conditions suivantes :

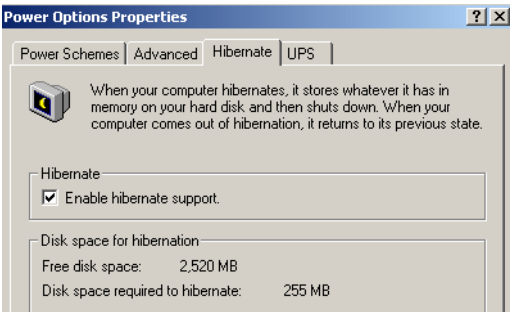
La mise en veille prolongée avec SafeGuard Easy prend en charge...	La mise en veille prolongée avec SafeGuard Easy ne prend pas en charge...
Windows 2000 et Windows XP	
les disques durs (Microsoft IDE, Serial-ATA, SCSI) qui utilisent les interfaces par défaut de Microsoft. Si aucune interface par défaut n'est utilisée, Serial-ATA risque de provoquer des problèmes pour certains périphériques.	Pilotes de disque dur d'autres fabricants
Modes de chiffrement SGE « Standard » et « Partitionnement ».	Mode de chiffrement SGE « Protection des zones d'amorçage »

REMARQUE :
Lorsque vous utilisez des périphériques externes ou des cartes d'extension (cartes son, etc.) assurez-vous qu'elles prennent en charge les fonctionnalités de gestion d'énergie Microsoft et que l'ordinateur peut être placé en mode Veille prolongée et réactivé, même si SafeGuard Easy n'est pas installé.

20.4 Configuration de la mise en veille prolongée

Pour garantir la plus haute sécurité possible à l'activation de la mise en veille prolongée, nous recommandons la configuration ci-dessous :

1. Dans le menu de démarrage de Windows, appelez successivement Paramètres / Panneau de configuration / Options d'alimentation. Sous l'onglet *Mise en veille prolongée*, cochez la case « Activer la prise en charge de la mise en veille prolongée »..



2. Si deux utilisateurs partagent un ordinateur géré par SafeGuard Easy, ouvrez l'onglet *Avancé*. Dans cet onglet, sélectionnez le champ « Mot de passe pour sortir d'une mise en veille (prolongée) ».

3. Démarrez l'utilitaire d'administration de SafeGuard Easy.

4. Activez l'authentification avant amorçage (PBA), si ce n'est pas déjà fait, dans General/Password settings/Password (Général/Choix des mots de passe/Mot de passe) lors du démarrage du système.

5. Chiffrez la partition du système d'exploitation avec Encryption/Drives/Hard disk drive (Chiffrement/Lecteurs/Disque dur).
   Pour protéger votre système, nous recommandons de chiffrer en outre les partitions de données complètes, en plus de la partition de système d'exploitation.

21 Activation/désactivation du chiffrement de disquettes et de périphériques amovibles

Pour protéger de manière optimale un poste de travail, il est recommandé d'activer le chiffrement de disquettes et de périphériques amovibles de SafeGuard Easy. Certaines situations requièrent toutefois une manipulation plus souple du mécanisme de chiffrement.

SafeGuard Easy vous permet d'activer ou de désactiver le chiffrement de lecteurs de disquettes et de périphériques amovibles pendant la durée d'une ouverture de session et de définir provisoirement vos propres clés. Les paramètres temporaires sont réinitialisés une fois que l'utilisateur de Windows a fermé sa session de travail et les paramètres système sont de nouveau valables.

La condition pour le changement provisoire des paramètres de chiffrement est qu'une authentification avec des données d'utilisateur ait eu lieu dans la PBA et que le chiffrement de disquettes/périphériques amovibles soit activé.

Afin d'éviter tout problème, lisez attentivement les conseils relatifs au chiffrement des lecteurs amovibles dans la section 'Remarques'.

21.1 Droits SafeGuard Easy requis

La condition pour l'activation du chiffrement est que l'utilisateur dispose des droits SafeGuard Easy correspondants. Le droit octroyé à un utilisateur pour l'activation du chiffrement de disquettes ou de périphériques amovibles est défini dans les paramètres d'utilisateur SafeGuard Easy à la rubrique « Droits » (voir 'Droits utilisateur').

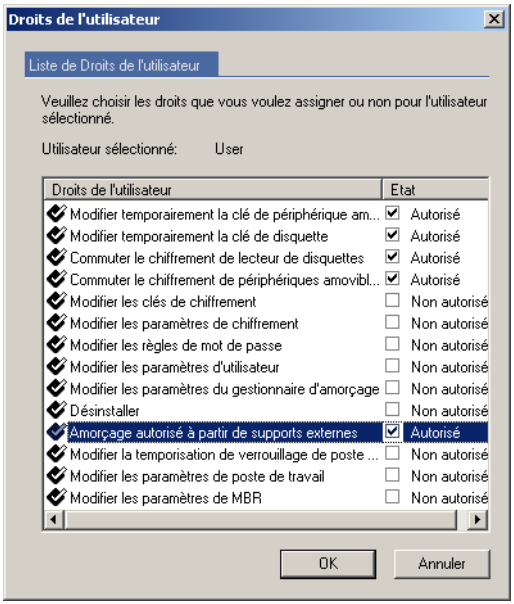
Les droits d'utilisateur suivants sont nécessaires :

- Pour la commutation du chiffrement :

  - modification temporaire d'une clé de périphérique amovible
  - commutation sur le chiffrement de périphérique amovible

- Pour la définition d'une clé temporaire :

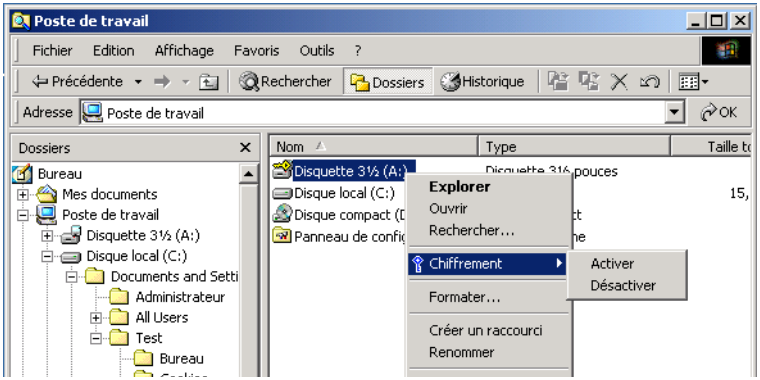
  - Modifier temporairement la clé de périphérique amovible
  - Modifier temporairement la clé de disquette



21.2 Commutation du chiffrement

L'état de chiffrement est commuté via l'Explorateur Windows. Par conséquent, SafeGuard Easy ajoute un élément de menu appelé « Encryption » (Chiffrement) dans le menu contextuel de l'Explorateur Windows.

Si vous cliquez avec le bouton de droite de la souris sur un lecteur chiffré, une commande d'activation/désactivation du chiffrement de disquette ou de périphériques amovibles est affichée.



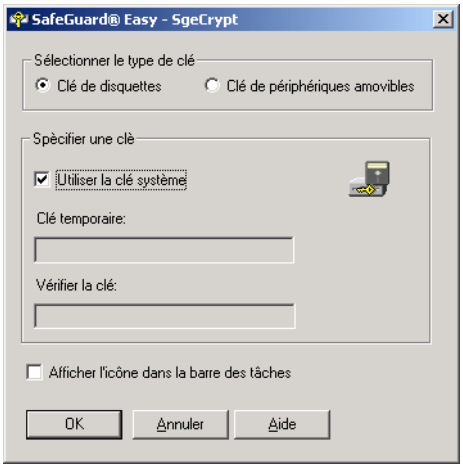
REMARQUES :

L'état de chiffrement peut être défini individuellement pour chaque périphérique amovible !

21.3 Définition de clé avec SgeCrypt

De nouvelles clés sont attribuées pour la durée d'une ouverture de session avec l'outil SGECRYPT.

Pour ouvrir SGECRYPT, sélectionnez successivement Programmes / Utimaco / SafeGuard Easy / **Clé de disquette et de périphérique**.



Vous pouvez choisir parmi les options suivantes :

- **Sélectionner le type de clé**
  Indique si la clé doit s'appliquer à une disquette ou à un périphérique amovible.

- **Utiliser la clé système**
  Activée (case cochée) :
  La clé prédéfinie sur le poste de travail (par exemple pendant l'installation) pour les disquettes ou les périphériques amovibles est utilisée.

  Désactivée (case non cochée) :
  Une nouvelle clé est utilisée.

Pour pouvoir sélectionner une clé système, celle-ci doit être définie également sur le poste de travail. Si ce n'est pas le cas, un utilisateur avec les droits correspondants dans l'utilitaire d'administration peut définir ultérieurement cette clé système.

- **Clé temporaire**
  La clé temporaire n'est valable que pour la durée d'une session de travail. Après un redémarrage, elle est de nouveau supprimée et la clé système est réactivée.

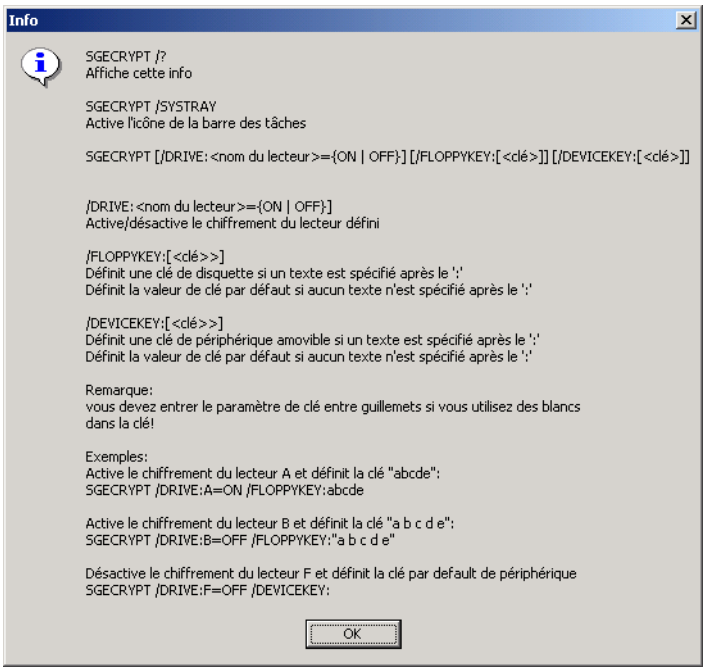
- **Show icon in taskbar**
  (Afficher une icône dans la barre des tâches) Affiche une icône dans la barre des tâches sur laquelle l'utilisateur peut cliquer pour afficher cette boîte de dialogue. Le réglage n'est valable que pour l'utilisateur actuellement connecté. Aucun droit d'administrateur Windows n'est requis pour afficher / masquer l'icône.

21.4 Commutation de paramètres de chiffrement via ligne de commande

Le chiffrement de disquettes / périphériques amovibles peut également être lancée de la ligne de commande.

Tapez la commande suivante, pour afficher les paramètres disponibles :

```
SGECRYPT /?
```



21.5 Remarques

- **Clé et algorithme**
  Un support de données est chiffré à la fois avec une clé et un algorithme. Veuillez vous enquérir des algorithmes qui sont utilisés pour les disquettes et/ou périphériques amovibles de votre poste de travail.

  Exemple : les disquettes d'un poste de travail sont chiffrées avec l'algorithme DES. Vous enregistrez les données importantes sur une disquette pour pouvoir les charger ensuite dans un autre ordinateur. Si les données y sont chiffrées avec IDEA, l'accès aux données est refusé.

- **Lecture de supports chiffrés**
  Il convient de procéder également avec précaution lorsque vous essayez de charger des supports de données chiffrés dans un lecteur non chiffré et inversement. Quand un support amovible chiffré est inséré dans un lecteur non chiffré, le système affiche un message vous informant que le système de fichiers de votre support (chiffré) est invalide. Si, suite à ce message, vous essayez de formater ce support dans le lecteur non chiffré, les données qui y sont enregistrées sont irréversiblement perdues. Si le système tente d'accéder sans succès à un support amovible ou une disquette, du fait que le chiffrement est actif, un nouveau message s'affiche pour indiquer que tous les fichiers stockés sur la disquette seront effacés si vous la formatez.

- **Activer/désactiver le chiffrement**
  L'activation/désactivation du chiffrement de disquettes ou de périphériques amovibles dans l'utilitaire d'administration de SafeGuard Easy est immédiatement effective tandis que le nouvel octroi de droits pour SGECRYPT ne fonctionne qu'après le redémarrage de l'ordinateur.

- **Avertissement**
  Quand vous tentez d'accéder à des disquettes/périphériques amovibles non formatés ou non chiffrés, un message vous informant de la perte de données en cas de formatage apparaît.

22 Certification FIPS 140-2 (Level 1)

La certification FIPS décrit les exigences en matière de sécurité pour les modules de chiffrement. Les administrations gouvernementales des États-unis et du Canada requièrent par exemple un logiciel certifié FIPS 140-2 pour les informations particulièrement critiques en matière de sécurité.

La caractéristique d'une installation SafeGuard Easy conforme à la certification FIPS est que seuls certains algorithmes doivent être utilisés pour le chiffrement. Ce sont les suivants :

- AES-128
- AES-256
- 3DES

Quand SafeGuard Easy est installé en mode FIPS, une icône apparaît dans la barre des tâches.

22.1 Nouvelles fonctions

Pour satisfaire aux exigences de la certification FIPS 140-2, SafeGuard Easy prend en charge ces deux nouvelles fonctionnalités.

Test à réponse connue (« Known Answer Test » – KAT)
Le test KAT est exécuté pour vérifier si les algorithmes de chiffrement utilisés fonctionnent correctement et s'ils fournissent des résultats appropriés. Le KAT est exécuté pour tous les algorithmes de chiffrement autorisés par le FIPS, et également pour la fonctionnalité hash HMAC-256 utilisée pour le contrôle d'intégrité.

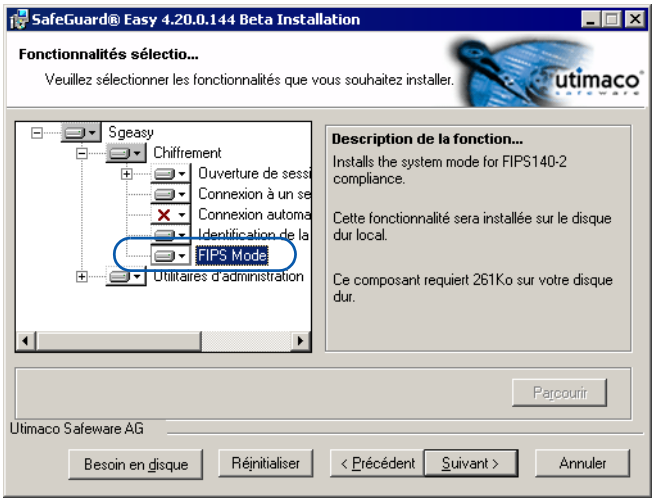
Pour le test KAT, un module de chiffrement chiffre un bloc de données défini et vérifie, au vu du résultat, si les données générées chiffrées sont celles que l'on attend. Si le résultat est erroné, le module de chiffrement doit verrouiller tout autre processus de chiffrement. Les pilotes de chiffrement de SafeGuard Easy exécutent automatiquement le test KAT après initialisation du pilote. Le texte KAT est exécuté pour le chiffrement et le déchiffrement. Les modules de chiffrement installés dans le noyau système SafeGuard Easy exécutent les mêmes tests.

Contrôle d'intégrité
Un contrôle d'intégrité est exécuté pour les modules de chiffrement afin de s'assurer qu'ils n'ont pas été modifiés. En cas d'échec d'un contrôle d'intégrité, le système stoppe tous les autres processus. Ce test est exécuté pour les fichiers pilotes de chiffrement de SafeGuard Easy et les modules de chiffrement dans le noyau système SafeGuard Easy. Un contrôle d'intégrité est également exécuté au sein du noyau système pour les données du système afin de déceler les manipulations illégales.

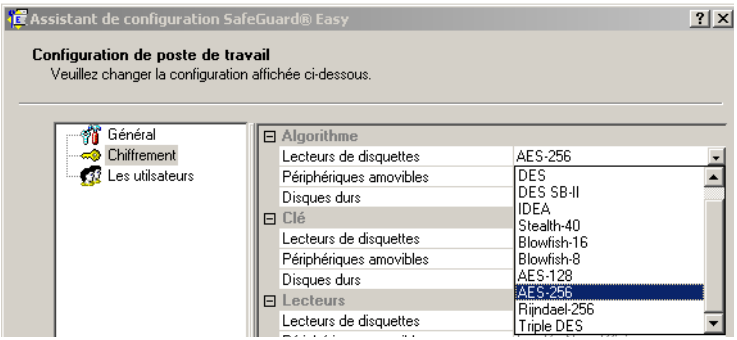
Dès que SafeGuard Easy est installé de façon conforme à la certification FIPS, les deux procédures de test pour le noyau système et le mode Win32 sont exécutées. Le test KAT est exécuté même si le mode FIPS est désactivé.

22.2 Installation de SafeGuard Easy de façon conforme à la certification FIPS

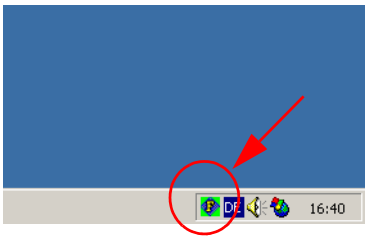
Un paramètre pendant l'installation (« mode FIPS ») détermine si un système SafeGuard Easy doit être installé de façon conforme à la certification FIPS.



Plus loin dans l'installation, un des algorithmes requis (AES-128, AES-256, 3 DES) doit être sélectionné pour les différents disques).



Une fois l'installation terminée, une icône dans la barre des tâches indique que SafeGuard Easy fonctionne en mode FIPS.



Si, plus loin dans l'installation, d'autres algorithmes que ceux qui sont autorisés sont sélectionnés, SafeGuard Easy affiche un message d'erreur.

Après confirmation du message d'erreur, SafeGuard Easy interrompt l'installation et l'utilisateur doit la relancer.

22.3 Utilisation sécurisée de SafeGuard Easy dans la configuration certifiée

Pour utiliser SafeGuard Easy dans une configuration certifiée et donc pour garantir la plus grande sécurité de produit possible, le système doit être configuré de la manière suivante :

- Installation avec PBA
- Longueur de mot de passe minimum : 6 caractères
- Utiliser les algorithmes de chiffrement AES-128, AES-256 ou 3DES
- Activer le chiffrement intégral du disque dur
- Activer le chiffrement des disquettes/périphériques amovibles
- Les utilisateurs ne sont pas autorisés à activer le chiffrement des disquettes/périphériques amovibles
- Activer le verrouillage d'écran SafeGuard Easy
- Lors de la définition manuelle de clés, un nombre si possible élevé de caractères aléatoires (max. 32 caractères) doit être saisi. Ne pas définir des clés banales susceptibles d'être aisément devinées par un agresseur.

23 SafeGuard Easy et Lenovo ThinkVantage Technologies - Embedded Security Subsystem (Lenovo ESS Chip)

Dans le cadre de l'association de constructeurs internationaux, la société Trusted Computing Group (TCG) s'est fixé comme objectif l'amélioration de la sécurité et de la fiabilité des plates-formes informatiques et des systèmes d'exploitation modernes

La technologie principale est le Trusted Platform Module (TPM), une puce matérielle cryptographique incorporée à la carte mère qui, en tant que périphérique de cryptographie, sert de mémoire clé et de générateur de nombres aléatoires sûrs.

Comme les cartes à puce, le TPM requiert un logiciel approprié pour pouvoir déployer toutes ses ressources. Sous sa forme de base, TPM peut gérer les clés de façon sécurisée et mettre ces clés à la disposition des utilisateurs et des applications par l'intermédiaire de mécanismes standard, tels qu'un fournisseur de services cryptographiques (CSP). Le TPM ne chiffre pas directement les données du système d'exploitation ou de l'utilisateur.

L'emploi du TPM permet en outre d'élaborer des concepts de sécurité, comme par ex. l'intégration de machines.

Lenovo équipe dès aujourd'hui un grand nombre de ses ordinateurs portables et de bureau avec une puce de sécurité conforme à TPM. Lenovo appelle ce système ESS (Embedded Security Subsystem) et le logiciel client correspondant « Client Security Software » (CSS). Lenovo est depuis longtemps le fournisseur de pointe en matière de Notebooks avec TPM et était récemment le seul à proposer une solution adéquate.

Utimaco Safeware est le premier concepteur professionnel à compléter à présent la solution de base Lenovo avec un chiffrement de disques durs compatible ESS et d'autres produits de sécurité. Ceux-ci montrent comment les utilisateurs peuvent tirer le meilleur profit de la « sécurité dans le matériel » avec contrôle intégral simultané de leur infrastructure.

Pour plus amples informations sur TPM, ESS et CSS, veuillez vous référer à votre documentation Lenovo.

23.1 SafeGuard Easy et TPM

Le support SafeGuard Easy TPM offre une fonctionnalité étendue pour PC avec puce ESS/TPM. Les fonctions les plus importantes sont :

- **Intégration CSS**
  Quand des utilisateurs de postes de travail avec puce TPM veulent continuer à utiliser CSS, SafeGuard Easy intègre sans problèmes cette fonction.
  Si SafeGuard Easy est combiné avec CSS, l'utilisateur a la possibilité de faire ouvrir automatiquement une session dans le TPM après authentification avant amorçage. Dans ce cas, les données sont enregistrées par SafeGuard Easy et transférées automatiquement au processus de connexion de SafeGuard. Ceci évite à l'utilisateur d'avoir à mémoriser un autre mot de passe.

- **Générer une clé aléatoire via TPM**
  La puce Lenovo ESS/TPM Chip comporte un générateur de nombres aléatoires. SafeGuard Easy exploite ce mécanisme pour générer des clés de session et des clés aléatoires.

- **Sécuriser la connexion client-serveur SGE via TPM**
  SafeGuard Easy peut également utiliser le générateur TPM pour sécuriser la connexion client-serveur dans le cadre de l'administration centrale.
  Dans le cadre de l'administration centrale, client et serveur SGE génèrent respectivement une paire de clés RSA pour s'authentifier mutuellement et pour sécuriser la connexion à la base de données. Cette paire de clés peut également être générée par la puce ESS/TPM.

- **Intégration machine**
  Permet l'intégration d'un disque dur dans un ESS/TPM donné. Il n'est alors plus possible d'utiliser un disque dur éventuellement volé dans un autre ordinateur, même quand le mot de passe est connu.

23.2 Préparation de l'utilisation de la puce

Avant de pouvoir utiliser la puce (et **avant l'installation de SafeGuard Easy**), les préparatifs suivants sont nécessaires :

1. Assurez-vous que la puce ESS est activée dans le BIOS.

2. Installez le pilote Atmel pour la puce ESS/TPM.

   No est requis à partir de la version CSS 6.0.

3. Installez le pilote SMBus (chaque Thinkpad Lenovo possède son propre pilote).

4. Pour SafeGuard Easy, il vous faut les versions suivantes du « Client Security Software » (CSS).

   - **Pour la génération de clés aléatoires et l'intégration UVM :«** Client Security Software » (CSS) à partir de la version 5.21
   - **Pour l'authentification client/serveur :«** Client Security Software » (CSS) à partir de la version 5.30

23.3 Paramètres requis pour l'intégration CSS

L'intégration dans CSS de SafeGuard Easy requiert un CSS configuré en conséquence. Vous trouverez des détails à ce sujet dans le manuel CSS.

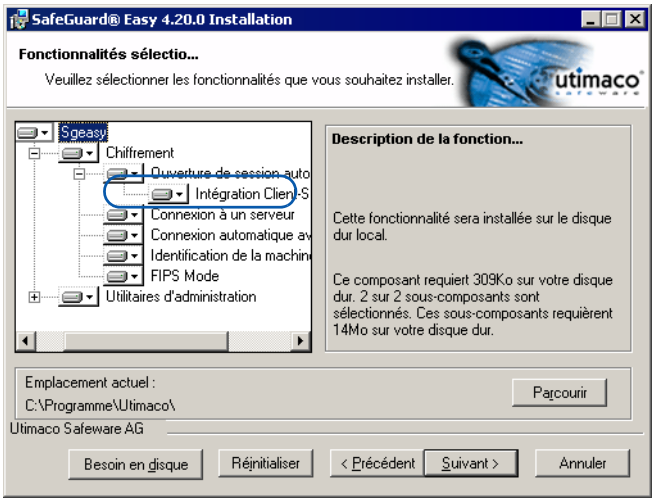
Voici comment combiner CSS et SafeGuard Easy :

1. Préparez l'utilisation de la puce.

2. Lors de la configuration de CSS, veillez à ce que la case « Remplacer l'ouverture de session Windows normale par l'ouverture de session du client Lenovo Security sécurisé » soit cochée !

   Non requis à partir de la version CSS 6.0.

3. Installez SafeGuard Easy.
   Lors de l'installation de SafeGuard Easy, veillez à ce que l'option « Intégration Client Security » soit active.



Pour le reste, aucun autre paramètre de configuration spécial n'est nécessaire dans SafeGuard Easy.

4. Après le redémarrage, vous obtenez un écran d'ouverture de session modifié qui requiert la « phrase mot de passe » au lieu du mot de passe Windows normal.

Intégration CSS et fonction d'ouverture de session automatique sécurisée (SAL) de SafeGuard Easy

Après une saisie des données Windows, la SAL les place dans une zone sécurisée et y revient après chaque ouverture de session avec succès par l'utilisateur dans la PBA pour connecter automatiquement l'utilisateur au système d'exploitation ('Configuration du mot de passe Windows').

La procédure est similaire quand l'intégration CSS et la SAL fonctionnement ensemble sur un ordinateur. La phrase mot de passe CSS est enregistrée chiffrée et n'a plus à être entrée. Les données d'ouverture de sessions ne sont plus demandées que dans la PBA.

REMARQUE :

Quand la SAL était activée pour l'ouverture de session Windows normale, le fichier `SGSAL.dat` (qui se trouve dans <disque système>`/System32`) doit être effacé avant l'intégration CSS.

`SGSAL` .dat doit être recréé étant donné que le format des données TPM se différencie de celui d'une ouverture de session Windows normale. Aucun fichier `SGSAL` .dat ne doit par conséquent exister quand CSS/SAL doit fonctionner.

23.4 Paramètres requis pour la génération de clés aléatoires via puce TPM

La génération de clés aléatoires via la puce ESS/TPM est imposée par des entrées dans le registre qui doivent être créées **avant l'installation de SafeGuard Easy**.

Voici comment générer des clés aléatoires avec puce TPM :

1. Préparez l'utilisation de la puce (cf. 'Préparation de l'utilisation de la puce').

2. Dans le registre Windows
   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy

   Entrez de nouvelles sous-clés :

   Fournisseur de services cryptographiques [STRING]

   a) avec CSS<= 5,40 entrez :
   "IBM Embedded Security Subsystem Enhanced CSP"
   a) avec CSS<= 6,0 entrez
   "ThinkVantage Client Security Solution CSP"

   UseCSPRandomGenerator [DWORD]
   Définissez la valeur sur « 1 ».

3. Installez SafeGuard Easy.

Les clés aléatoires sont alors générées sans autres paramètres de configuration de la puce ESS/TPM.

23.5 Paramètres requis pour la sécurisation de l'authentification client/serveur via puce TPM

Paramètres pour Client Security Software <= 5.40

La génération de paires de clés via une puce ESS/TPM est sécurisée via le mot de passe d'administrateur de la puce. Le mot de passe d'administrateur est fixé pendant l'installation du logiciel CSS. Si SafeGuard Easy est distribué dans le cadre d'une installation centrale sur des clients avec puce TPM, le mot de passe d'administrateur sur les clients doit être connu.

Dans les réseaux comportant plusieurs clients TPM, les utilisateurs ne connaissent pas généralement le mot de passe de l'administrateur de la puce. Les administrateurs préfèrent généralement appliquer le même mot de passe TPM à l'ensemble des utilisateurs du réseau.

Avec un utilitaire propre à SafeGuard Easy, il est possible de générer un fichier chiffré avec le mot de passe d'administrateur de la puce. Ce fichier est distribué aux clients TPM dans le cadre d'une installation centrale. SafeGuard Easy complète de façon automatique la boîte de dialogue de saisie du mot de passe utilisateur côté client. Par conséquent, la clé RSA est générée sans interaction utilisateur.

Voici comment générer des paires de clés RSA avec puce TPM :

1. Préparez l'utilisation de la puce sur le client/serveur (cf. 'Préparation de l'utilisation de la puce').

2. Dans le registre Windows du client/serveur, créez les entrées suivantes sous
   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy
   Cryptographic Service Provider [STRING]
   La valeur à entrer est : « IBM Embedded Security Subsystem Enhanced CSP » ForceCSPUsage [DWORD]

   La valeur doit être "1".
   (ForceCSPUsage prend également en charge la génération de clés aléatoires).

3. Sur un ordinateur avec SafeGuard Easy installé, appelez l'utilitaire `SGTpmApn.exe` et créez le fichier chiffré avec le mot de passe d'administrateur pour la puce ESS/TPM. Le nom du fichier par défaut est `SGTPMGNA.DAT`

   Quand le nom par défaut de ce fichier est modifié, l'entrée suivante doit être effectuée dans le registre de Windows du client sous
   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy

   ESSAdminPassword [STRING]
   La valeur à entrer est le fichier avec le mot de passe d'administrateur, par ex. :« `D :\Programmes\Utimaco\SafeGuard Easy\AdminPW.dat.`

4. Distribuez le fichier chiffré avec les paquets SafeGuard Easy aux clients. Le fichier avec le mot de passe d'administrateur doit se trouver dans le répertoire d'installation de SafeGuard Easy .

Juste avant la génération de clés RSA, SafeGuard Easy démarre un moniteur qui charge le mot de passe d'administrateur du fichier, remplit automatiquement la boîte de dialogue de mot de passe du ESS CSP et efface ensuite le fichier.

Après l'installation de SafeGuard Easy, la paire de clés RSA est automatiquement générée et l'utilisateur n'a plus à définir d'autres paramètres de configuration.

Paramètres pour Client Security Software >= 6.0

À compter de la version 6.0 de CSS, le mot de passe d'administration de la puce n'est pas requis, et la paire de clés RSA est générée de façon interactive. Par conséquent, il n'est pas nécessaire de créer et déployer un fichier chiffré avec l'outil SafeGuard Easy fourni, comme ce fut le cas lorsque CSS <= 5,40.

Voici comment générer des paires de clés RSA avec puce TPM :

1. Préparez l'utilisation de la puce sur le client/serveur (voir 'Préparation de l'utilisation de la puce').

2. Dans le registre Windows du client/serveur, créez les entrées suivantes sous
   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGEasy
   Cryptographic Service Provider [STRING]La valeur à entrer est :
   « ThinkVantage Client Security Solution CSP »

   ForceCSPUsage [DWORD]
   La valeur doit être « 1 ». (ForceCSPUsage prend également en charge la génération de clés aléatoires).

REMARQUE :
La génération de paires de clés à l'aide d'une puce TPM est beaucoup plus lente que lorsque cette opération se fait à l'aide d'une solution logicielle. Ceci peut avoir un impact sur les temps de réponse. Celles-ci sont causées par la procédure d'authentification du client et du serveur, pas par les opérations de chiffrement.

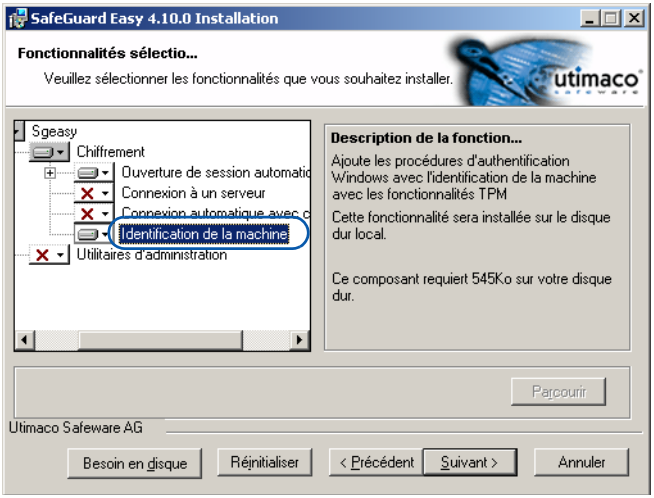
23.6 Paramètres requis pour l'intégration de machine

L'intégration de machine génère une liaison claire entre l'ordinateur et le disque dur raccordé. Ceci se fait via une signature, dont la concordance avec la signature générée à l'exécution de l'intégration initiale est vérifiée. Cette signature de référence est ensuite stockée dans le Registre. Le processus de démarrage ne peut alors aboutir que si les deux signatures sont identiques. Dans le cas contraire, le processus d'initialisation est interrompu.

Voici comment combiner Intégration de la machine et SafeGuard Easy :

1. Préparez l'utilisation de la puce.

2. Installez SafeGuard Easy.
   Lors de l'installation de SafeGuard Easy, veillez à ce que l'option « Indentification de la machine » soit active.



Pour le reste, aucun autre paramètre de configuration spécial n'est nécessaire dans SafeGuard Easy.

23.6.1 Intégration de machine initiale

Lorsque le système est démarré pour la première fois suite à l'installation de la fonctionnalité de liaison, l'*Assistant de liaison et d'identification des ordinateurs de SafeGuard* est activé et informe l'utilisateur que la liaison n'a pas encore été activée.

REMARQUE :

CSS<6.0 Le mot de passe Security Chip est requis.

CSS=>6.0 Le mot de passe Security Chip no est requis.

Cliquez sur **Continuer** pour démarrer le processus d'intégration de machine initiale.

Comme chaque opération sur la puce sécurité concernant la clé privée requiert un mot de passe, le mot de passe Security Chip doit être tapé.

CSS 6.0 le mot de passe Lenovo Security Chip no est requis.

Une boîte de dialogue confirme le succès de l'intégration de machine. Le disque dur local ne peut dès lors n'être utilisé qu'avec cet ordinateur.

Lors de chaque démarrage de l'ordinateur, le logiciel vérifie l'état de l'intégration des ordinateurs. Le processus d'initialisation n'est poursuivi que lorsque les signatures concordent.

23.6.2 Échec de l'intégration des ordinateurs

Les situations suivantes ont pour conséquence un échec de la vérification des signatures.

- Le matériel Module de sécurité est désactivé.
- Le matériel Module de sécurité est endommagé.
- La clé principale du module de sécurité a été modifié.
- La signature de référence a été modifiée.
- La signature de référence manque.
- La paire de clés nécessaire pour l'opération de signature a été modifiée.
- Le CSP à utiliser ne fonctionne pas ou a été modifié.
- La configuration CSS a été modifiée.

Pour accéder au système en cas d'échec de l'intégration, vous disposez d'une fonctionnalité de restauration dans cette boîte de dialogue.

Pour restaurer le système à l'aide d'une sauvegarde d'ESS (Embedded Security System), veuillez vous reporter à votre documentation Lenovo.

23.6.3 Restauration après intégration

Pour pouvoir accéder à nouveau au système en cas d'échec d'intégration, cliquez sur le bouton **Restaurer**.

Dans cette boîte de dialogue, chaque mot de passe de puce de sécurité Lenovo entré à l'identification initiale de la machine doit être saisi. Même quand le mot de passe a été modifié après l'identification initiale de la machine.
Si la fonction de restauration est utilisée parce qu'une nouvelle puce de sécurité a été installée, le mot de passe de l'ancienne puce doit être entré pour la restauration.

A partir de CSS >= 6.0, la boîte de dialogue est remplacée par la boîte de dialogue « SafeGuard Authentication - Restauration » et l'utilisateur Windows, le mot de passe et le domaine sont demandés.

Dès que avez de nouveau accès au système, l'identification initiale de la machine doit être à nouveau exécutée quand une des situations suivantes à entraîné un échec de la vérification :

- Le matériel Module de sécurité est endommagé.
- Le Master Key du module de sécurité a été modifié.
- La signature de référence a été modifiée.
- La signature de référence manque.
- La paire de clés nécessaire pour l'opération de signature a été modifiée.

Avant de pouvoir exécuter à nouveau l'identification de la machine, vous devez

1. impérativement effacer les valeurs suivantes dans le registre,

   - **Machine Binding**
   - **Recovery**

   sous la clé

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   SGLogon
   Embedded Security System

Attention :

Ces valeurs doivent impérativement être supprimées avant de pouvoir relancer l'intégration. Si ces valeurs existent encore quand l'identification de la machine est relancée, des situations dans lesquelles vous n'avez plus aucun accès au système peuvent se produire.

2. Les données présentes sur la puce de sécurité Security Chip doivent être réinitialisées à l'aide des outils Lenovo.

La nouvelle identification initiale de la machine débute automatiquement au prochain démarrage du système.

23.6.4 Configuration du mode de restauration

A côté de la boîte de dialogue standard pour la restauration du système, SafeGuard Authentication Support TPM fournit une seconde boîte de dialogue pour autorisation de la restauration. Dans cette boîte de dialogue, le nom et le mot de passe, et le nom de domaine (facultatif) sont utilisés pour récupérer l'accès au système. Sur cet ordinateur, l'utilisateur doit posséder des droits d'administrateur.

La boîte de dialogue à utiliser peut être spécifiée via un modèle ADM installé à l'utilisation du support TPM. Le paramètre se trouve dans la console de gestion sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\Authentification
\Identification machine
\Restauration

Sous Type de restauration, vous pouvez sélectionner :

- **Données d'accès administratives**
  pour l'utilisation du nom d'utilisateur Windows et du mot de passe ou
- **Mot de passe TPM**
  pour l'utilisation du mot de passe de la puce de sécurité Lenovo,

en fonction du contexte.

Dans la boîte de dialogue qui apparaît, entrez le nom et le mot de passe d'un utilisateur existant sur l'ordinateur. Le nom de domaine est facultatif.

REMARQUE :
Sur cet ordinateur, l'utilisateur doit posséder des droits d'administration.

24 SafeGuard Easy et technologies Thinkvantage de Lenovo - Rescue and Recovery

Ceci permet aux utilisateurs de faire appel à la méthode efficace de sauvegarde et de restauration de Lenovo, même quand la partition du système d'exploitation est chiffrée avec SafeGuard Easy. SafeGuard Easy offre ici une fonctionnalité unique en son genre !

24.1 Aperçu

Rescue and Recovery™ offre une fonction centrale pour la restauration de données par appui sur une touche. Même quand le système d'exploitation primaire est endommagé et n'amorce plus, Rescue and Recovery™ sauvegarde les données via un environnement de secours. Les outils de sauvetage peuvent être appelé depuis le Bureau de Microsoft Windows ou la touche bleue « Thinkvantage » (Access IBM) intégrée dans les systèmes Lenovo. Rescue and Recovery™ prend cependant également en charge les système non-Lenovo.

Rescue and Recovery sert surtout de « planche de salut » aux utilisateurs d'ordinateurs quand le système d'exploitation est défaillant et quand des données importantes ne sont plus accessibles.

Utimaco Safeware est à présent le premier fournisseur professionnel de systèmes de chiffrement de disques durs à proposer la solution Lenovo pour restaurer des systèmes endommagés sans perdre le chiffrement. Cette solution protège l'ensemble des données du système et assure la sécurité des données.

Pour de plus amples informations sur Rescue and Recovery™, veuillez consulter votre documentation Lenovo.

24.2 Rescue and Recovery et SafeGuard Easy

SafeGuard Easy s'intègre sans problèmes dans les schémas Rescue and Recovery et prend également en charge les fonctions spécifiques à Lenovo telles que la touche bleue « Thinkvantage » (Access IBM) sur le clavier des ordinateurs portables ou la touche « Entrée » bleue des ordinateurs.

Une fois le chiffrement terminé, l'utilisateur a la possibilité de créer une copie de sauvegarde des modifications. Pour ce faire, le système contient, par exemple, le pilote SafeGuard Easy, qui permet de restaurer ce type de sauvegarde. (La sauvegarde sécurisée avec SafeGuard Easy et ses pilotes est appelée « sauvegarde SGE »).

SafeGuard Easy n'est pas affecté par une restauration système, tous ses paramètres restent valides et il n'est nécessaire de procéder à sa réinstallation. L'utilisateur peut continuer à travailler sans interruption après la restauration et n'est pas importuné par un relancement du chiffrement.

24.2.1 Avantages de la combinaison de Rescue and Recovery™ et de SafeGuard Easy

- SafeGuard Easy chiffre tout le disque dur, fichiers temporaires, fichier d'échange, mise en veille prolongée et fichier de vidage de mémoire inclus, et le protège en interrogeant les données d'utilisateur SafeGuard Easy contre un accès non autorisé.
- Toutes les copies de sauvegarde sont stockées de façon chiffrées dès qu'elles sont enregistrées sur un disque dur local chiffré.
- Le module Rescue and Recovery permet de restaurer un système endommagé sans avoir à réinstaller SafeGuard Easy et chiffrer de nouveau le disque dur.
- La restauration d'une sauvegarde SGE de l'environnement Rescue and Recovery n'est possible que si les données d'utilisateur SafeGuard Easy ont été entrées au préalable dans l'authentification avant amorçage.

24.2.2 Préparation

- Ordinateurs de bureau ou portables de Lenovo
- BIOS actuel pour votre système
- Version de Rescue and Recovery™ :
  - Rescue and Recovery™ 1.0 (Build 033)
  - Rescue and Recovery™ 2.0 (Build 2.00.0170)
  - Rescue and Recovery™ 3.0 (Build 3.00.0029.00)
  - Rescue and Recovery™ 4.0 (Build 4.0.0114)
  - Rescue and Recovery™ 4.2 (Build 4.20.0510)

24.3 Pour une installation

Pour les exemples d'installation ci-dessous, nous supposons que l'environnement Rescue and Recovery n'est pas installé sur la partition IBM_SERVICE. Toutes les particularités dont il convient de tenir compte quand on utilise la partition IBM_SERVICE sont listées au chapitre Particularités.

Si vous installez Rescue and Recovery sur un disque dur sans partition IBM_SERVICE, Rescue and Recovery™ sera installé avec les paramètres par défaut suivants :

- L'environnement Rescue and Recovery se trouve par défaut sur une partition virtuelle, installée sur le disque C (partition primaire du disque dur principal) de l'ordinateur.
- Une partition virtuelle comporte deux répertoires : \minint et \preboot. Ces deux répertoires sont protégés par Rescue and Recovery lui-même.
- Les sauvegardes ou copies de sauvegarde sont enregistrées par défaut dans le répertoire C :\RRUbackups. Quand il se trouve sur la partition locale du disque dur primaire, ce répertoire est protégé par Rescue and Recovery pour qu'il ne soit ni effacé, ni déplacé. Dans ce cas, la suppression est impossible.

A l'installation de Rescue and Recovery et de SafeGuard Easy, l'ordre d'installation est important. Lisez impérativement les instructions des chapitres suivants.

24.3.1 Ni SafeGuard Easy, ni Rescue and Recovery ne sont installés

1. Désinstallez toutes les versions Rescue and Recovery avec Rapid Restore qui sont antérieures à la version 4.0 !

2. Installez Rescue and Recovery™.

3. Installez SafeGuard Easy à partir de la version.

   SafeGuard Easy vérifie si la version Rescue and Recovery correcte est installée et ajoute ses fichiers et ses paramètres dans l'environnement de secours Lenovo.

   Veuillez vous assurer que l'authentification avant amorçage est bien activée de façon à ce qu'aucune personne non autorisée ne puisse restaurer des sauvegardes.

   L'authentification avant amorçage est activée pendant l'installation ou plus tard dans l'administration via le dossier Général / Configuration de mot de passe / Activation du mot de passe au démarrage du système.

24.3.2 Seul SafeGuard Easy est déjà installé.

SafeGuard Easy à partir de la version 4.10 est installé.

1. Installez Rescue and Recovery.

2. Avant le redémarrage, appelez successivement les outils suivants du répertoire SafeGuard Easy- MBRsync.exe
   - MBRsync.exe
   - WinPERepair.exe

SafeGuard Easy < 4.10 est installé.

1. Installez SafeGuard Easy >= Version 4.10 (mise à jour).

2. Installez Rescue and Recovery™.

3. Avant le redémarrage, appelez successivement les outils suivants du répertoire SafeGuard Easy- MBRsync.exe
   - MBRsync.exe
   - WinPERepair.exe

- ou -

1. Installez Rescue and Recovery.

2. Avant le redémarrage, appelez successivement les outils suivants du répertoire SafeGuard Easy- MBRsync.exe
   - MBRsync.exe

3. Installez SafeGuard Easy >= Version 4.10 (mise à jour).

IMPORTANT :
A chaque fois que Rescue and Recovery est installé après SafeGuard Easy, les outils « MBRsync.exe » et « WinPErepair.exe » doivent être exécutés avant le redémarrage qui active Rescue and Recovery. Sinon, le message suivant s'affiche « Error! Fichier noyau introuvable". Les deux outils se trouvent dans le répertoire SafeGuard Easy et sont exécutés simplement en double-cliquant dessus.

24.4 Mise à niveau

Mise à niveau signifie qu'à la fois SafeGuard Easy à partir de la version 4.10 et Rescue and Recovery™ sont installés, l'un des deux programmes étant mis à jour.

24.4.1 Mise à niveau de SafeGuard Easy

La mise à niveau de SafeGuard Easy met à jour le système complet, Rescue and Recovery inclus. Aucune autre action n'est nécessaire.

24.4.2 Mise à niveau de Rescue and Recovery

A chaque fois que Rescue and Recovery est mis à jour, les outils MBRsync.exe et WinPErepair.exe doivent être exécutés avant le redémarrage. Les deux outils se trouvent dans le répertoire SafeGuard Easy et sont exécutés simplement en double-cliquant dessus.

24.5 Désinstallation

A la désinstallation des deux produits, veuillez observer ce qui suit :

- Désinstallez d'abord SafeGuard Easy, puis Rescue and Recovery.
- La désinstallation de SafeGuard Easy ne doit pas s'effectuer aussitôt après une restauration du système. Redémarrez l'ordinateur et désinstallez ensuite SafeGuard Easy !

24.6 Création d'une copie de sauvegarde

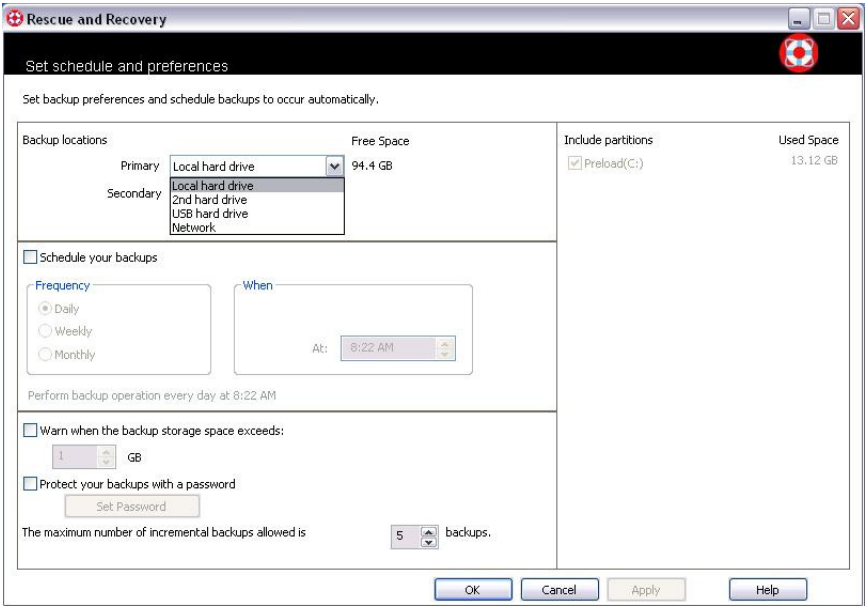
Remarque générale :
Les captures d'écran des chapitres suivants présentent des extraits de la version Rescue and Recovery™ avec Rapid Restore™ 4.0 (version 033). L'interface utilisateur des versions suivantes pourra partiellement différer, les fonctionnalités restant toutefois identiques.

Les copies de sauvegarde sont créées via le logiciel Rescue and Recovery™ dans l'environnement Windows actif. Sur les ordinateurs avec Rescue and Recovery, SafeGuard Easy conseille à l'utilisateur de créer impérativement une nouvelle copie de sauvegarde du système une fois l'installation effectuée avec succès.

La manière de créer une sauvegarde du système à partir de l'environnement Windows est décrite dans les documents Lenovo correspondants.

Pour les sauvegardes SGE, SafeGuard Easy prend en charge les supports suivants :

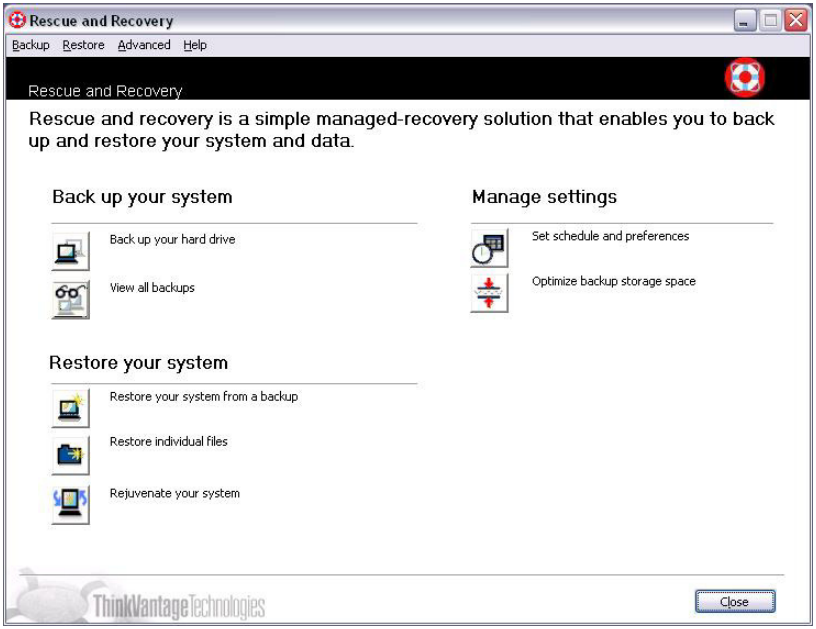
- disque dur local
- 2ème disque dur
- disque dur USB
- réseau
- Support mémoire USB
- CD/DVD



Les sauvegardes sont enregistrées par défaut dans le répertoire C :\RRUbackups. Quand il se trouve sur la partition locale du disque dur primaire, ce répertoire est protégé par Rescue and Recovery pour qu'il ne soit ni effacé, ni déplacé. Dans ce cas, la suppression est impossible.

24.7 Restauration de fichiers

Rescue and Recovery™ restaure sans problème des fichiers individuels ou des répertoires d'une sauvegarde SGE en un environnement Windows fonctionnel. Il suffit aux utilisateurs de démarrer Windows, puis le logiciel Rapid Restore et de restaurer les fichiers recherchés. Un redémarrage n'est pas nécessaire, c'est-à-dire que les données restaurées sont immédiatement disponibles pour la poursuite du traitement par l'utilisateur.



24.8 Restauration du système

Pour restaurer une sauvegarde SGE, l'utilisateur démarre l'environnement Rescue and Recovery. Ceci s'affiche lorsque vous appuyez sur cette touche pendant le démarrage du PC ou de l'ordinateur portable :

- "Thinkvantage"/"Access IBM" (ordinateurs portables Lenovo).
- Touche « Entrée bleue » (ordinateurs de bureau Lenovo).
- [F11] sur tout autre clavier.

Remarque relative à Rescue and Recovery™ 2.0 :
Utimaco recommande en général de restaurer le disque dur complet.

Si vous avez cependant sélectionné par inadvertance l'option « Ne restaurer que le système d'exploitation Windows et les applications depuis la sauvegarde », Utimaco ne garantit pas que les fichiers SafeGuard Easy seront complètement restaurés. Si, dans ce cas, des problèmes surviennent à l'amorçage, vous ne devez pas craindre de conséquences négatives pour votre système. Après un redémarrage, appelez simplement l'environnement Rescue and Recovery™ avec la touche Lenovo de votre PC ou Notebook et restaurez l'ensemble du disque dur.

24.8.1 Environnement de démarrage

Pour amorcer l'environnement Rescue and Recovery, les conditions suivantes doivent être remplies :

SafeGuard Easy **autorise** l'amorçage de l'environnement Rescue and Recovery à partir du...

- *disque dur local*
  Partition virtuelle sur le disque dur local ou partition IBM_SERVICE locale

SafeGuard Easy **N'autorise PAS** l'amorçage de l'environnement Rescue and Recovery à partir d'un...

- *CD exécutable*
- *Disque dur USB exécutable*

Si l'environnement Rescue and Recovery est amorcé quand même à partir d'un support externe, SafeGuard Easy est supprimé pendant le processus de restauration.

Pour sauvegarder à nouveau le système, SafeGuard Easy doit être réinstallé.

24.8.2 Restauration d'un système SafeGuard Easy

1. Ouvrir l'environnement Rescue and Recovery en appuyant sur la touche « Thinkvantage » (ordinateur portable) ou la touche « Entrée » bleue.

2. L'invite d'authentification avant amorçage apparaît. L'Utlisateur doit entrer les données SafeGuard Easy.

3. L'interface utilisateur de l'environnement Rescue and Recovery apparaît.

4. L'écran de bienvenue s'affiche. Cliquez sur le bouton Suivant pour continuer.

5. Dans le menu de gauche, sélectionnez Restaurer via sauvegarde.

6. La boîte de dialogue Restaurer d'une sauvegarde apparaît.

7. Sélectionnez la sauvegarde SGE et restaurez.

24.9 Partitions de récupération de service et d'usine

Lenovo fournit de nouveaux PC dotés de partitions préinstallées, appelées "partition de service (service partition)" et "partition de récupération usine (factory recovery partition)" :

- Partition de service : contient l'environnement d'initialisation Rescue and Recovery.
- Partition de récupération usine : contient toutes les informations pour la récupération des paramètres d'usine de l'ordinateur.

Si votre ordinateur ne comporte pas encore de partition de service, et si vous voulez quand même travaillez avec, créez-la avant d'installer SafeGuard Easy.

Pour créer la partition de service, consultez la documentation Lenovo correspondante.

24.9.1 Particularités

Les particularités suivantes doivent être notées quand vous utilisez la partition de service et de récupération usine :

Système d'exploitation	Mode de chiffrement SafeGuard Easy Mode de chiffrement	État des deux partitions speciales
Windows 2000	Par partition	Les partitions ne sont pas chiffrées. Avantage : les paramètres d'usine Lenovo peuvent être restaurés du disque dur local. Inconvénient : les pirates informatiques peuvent manipuler un environnement d'amorçage Rescue and Recovery non chiffré.
Windows XP	Par partition Disques complets, Protection des zones d'amorçage	
Windows 2000	Disques complets Protection des zones d'amorçage	Les partitions sont chiffrées. Avantage : l'environnement d'amorçage est chiffré. Il ne peut être modifié que lorsque le mot de passe SafeGuard Easy est connu. Inconvénient : les paramètres d'usine Lenovo ne peuvent pas être restaurés du disque dur local. Pour la réinitialisation des paramètres d'usine, un CD ou DVD spécial est nécessaire. En alternative, le disque dur peut être déchiffré via la disquette de secours et l'utilitaire DOS Sgeasy.exe (=désinstallation de SafeGuard Easy).

Utimaco recommande, soit de chiffrer la partition de service, soit d'installer l'environnement Rescue and Recovery sur la partition virtuelle. La partition virtuelle est toujours protégée dès que le disque système de Windows est chiffré.

24.10 Que faire, si …

… un avertissement de virus est affiché à l'écran par SafeGuard Easy après redémarrage de l'ordinateur ?

Causes possibles :

1. *Le système contient un virus.*

   Contactez sans retard votre administrateur système.

2. *Vous avez oublié, après l'installation, la modification ou la désinstallation de Rescue and Recovery, de synchroniser le MBR avec la commande MBRsync.exe.*

   SafeGuard Easy détecte des modifications du MBR et affiche un avertissement de virus, si nécessaire. Si vous êtes sûr que le message a été affiché par Rescue and Recovery, cliquez sur « Reprendre » dans le menu. Seul le « SYSTÈME » peut afficher le menu.

… le système de fichiers est endommagé ?
Il suffit ici, en règle générale, de charger simplement une copie de sauvegarde (avec SafeGuard Easy) avec Rescue and Recovery.

En alternative, le disque dur peut être déchiffré via la disquette de secours et l'utilitaire DOS Sgeasy.exe (désinstallation de SafeGuard Easy). Le disque dur est alors de nouveau disponible en texte clair et peut être traité avec les outils de sauvegarde de fichiers normaux. Si l'utilisateur n'est pas autorisé à désinstaller SafeGuard Easy en raison de droits insuffisants, la procédure Requête/Réponse de SafeGuard Easy peut être activée pour accorder un droit provisoire à cet effet à l'utilisateur.

... le disque dur est physiquement endommagé ?
Si le disque dur est physiquement endommagé et ne peut pas être déchiffré, même avec Sgeasy.exe, Utimaco contacte à la demande des partenaires spécialisés dans le sauvetage de disques durs physiquement endommagés.

… le noyau système SafeGuard Easy est endommagé ?
Avec les défauts minimes, comme un MBR écrasé, Sgeasy.exe répare le MBR ou charge une sauvegarde du noyau système préalablement enregistrée

25 Compatibilité avec le logiciel Absolute Computrace

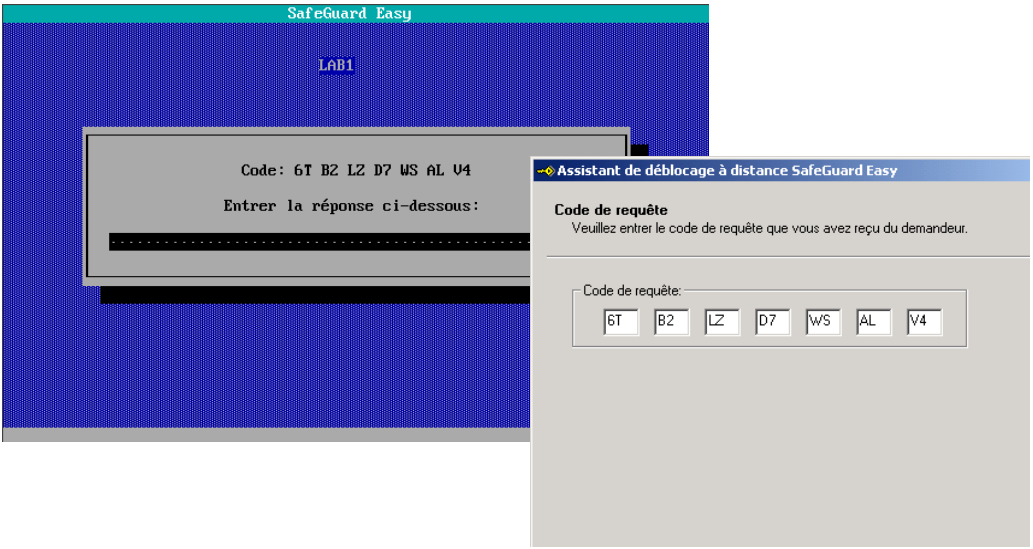
Lenovo protège ses nouveaux ordinateurs portables Thinkpad avec de nombreuses fonctions de sécurité (entre autres SafeGuard Easy et SafeGuard PrivateDisk) et garantit ainsi à leurs utilisateurs une sécurité « mobile » élevée. En complément de ces produits de la famille SafeGuard, Computrace, d'Absolute Software Corp. est également installé en usine sur les ordinateurs portables Lenovo.

Computrace aide à retrouver un ordinateur portable en cas de vol, dès que l'appareil volé est connecté à Internet. À la demande du propriétaire légal, il permet également d'effacer des données confidentielles de l'ordinateur volé. Lenovo est le seul constructeur à intégrer Computrace dans le matériel de l'ordinateur (BIOS persistent agent).

Grâce à sa compatibilité avec SafeGuard Easy, le logiciel Computrace fonctionne avec des disques durs chiffrés.

SafeGuard Easy est compatible avec Computrace Complete avec « BIOS Persistence », mais pas avec « Software Persistence ».

26 Maintenance à distance (Requête/Réponse)

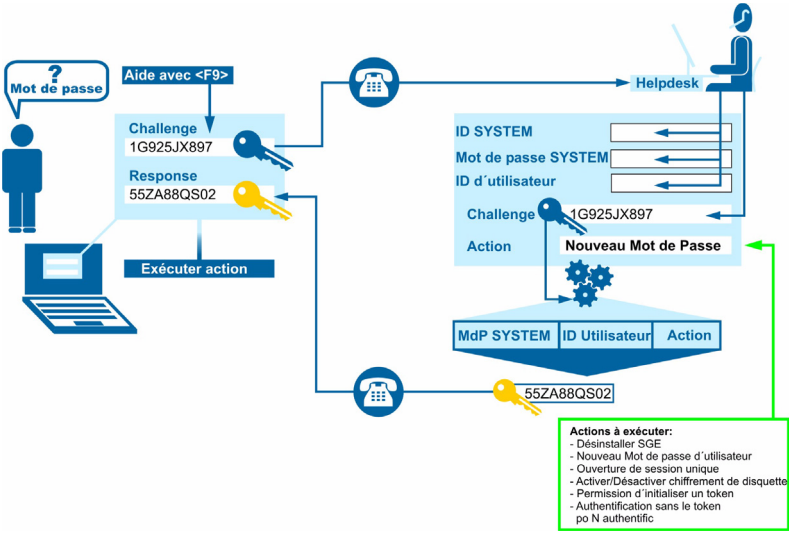


SafeGuard Easy propose la procédure de Requête/Réponse pour réinitialiser des mots de passe SafeGuard Easy ou de jeton « oubliés ».

La procédure Requête/Réponse est très sûre et très efficace :

- pas d'échange de données confidentielles ;
- écoute ou interception de données est sans effets ;
- utilisation également avec des appareils sans connexion réseau ;
- utilisateur peut reprendre son travail en très peu de temps.

26.1 Mode de fonctionnement



Si un utilisateur (utilisateur supprimé) a besoin d'aide, il doit générer un code de requête. Ce code de requête est affiché sur l'ordinateur de l'utilisateur sous forme de chaîne de caractères ASCII. L'utilisateur appelle ensuite son administrateur (helpdesk) et lui fournit ses informations personnelles et le code de requête. Le personnel d'assistance ouvre l'assistant de déblocage à distance SafeGuard Easy et génère le code de réponse. Ce personnel fournit le code de réponse à l'utilisateur via téléphone ou SMS. Après saisie de ce code de réponse, l'utilisateur peut redéfinir son mot de passe.

En règle générale, les droits spéciaux suivants peuvent être octroyés via Requête/Réponse :

- définition d'un nouveau mot de passe d'utilisateur SafeGuard Easy (quand l'ancien a été oublié)
- désinstallation de SafeGuard Easy
- ouverture de session unique (par ex. pour travaux de maintenance)
- attribution temporaire du droit de commutation du chiffrement de disquettes (pendant la durée d'une ouverture de session)
- Ouverture de session sans jeton pour X sessions
- autorisation d'initialisation d'un jeton

L'assistant de déblocage à distance peut être installé sur un ordinateur ou sur le PDA du collaborateur du service assistance.

26.1.1 Version PDA de l'assistant de déblocage à distance

La version PDA de l'assistant de déblocage à distance se trouve sur le CD SafeGuard Easy.

1. Copiez le fichier `SGE_CRW.PPC30_ARM.cab` du répertoire \TOOLS du CD SafeGuard Easy sur le PDA.

2. Accédez au fichier `SGE_CRW.PPC30_ARM.cab` à l'aide de l'explorateur de fichiers du PDA. L'installation est immédiatement effectuée.

3. Après l'installation, un démarrage à chaud est nécessaire.

Si le code de réponse est généré sur un PDA, SafeGuard PDA doit y être installé.

26.2 Création d'un code de requête

Le code de requête est généré par l'utilisateur qui a par ex. oublié son mot de passe SafeGuard Easy. Indépendamment du type de démarrage du système, il en résulte des méthodes différentes à la création du code de requête.

Démarrage du système avec PBA

Lors du **démarrage du système avec PBA**, l'utilisateur doit entrer son nom SGE dans la PBA, puis modifier son mot de passe. Le code de requête est affiché après appui sur [F9].

Démarrage du système sans PBA

Au **démarrage du système sans PBA**, un symbole de disquette apparaît pendant quelques secondes dans le coin de gauche dans le haut de l'écran lors de l'amorçage de l'ordinateur. L'utilisateur doit appuyer sur la touche [F2] pendant ce laps de temps. La boîte de dialogue d'ouverture de session de la PBA s'ouvre et l'utilisateur y entre son nom SGE dans la PBA. Le champ de mot de passe est ensuite activé. Le code de requête est affiché après appui sur [F9].

Cas particulier : désinstallation

Pour désinstaller SafeGuard Easy via Requête/Réponse, le code de requête doit être généré dans la boîte de dialogue de désinstallation (Programmes / Panneau de configuration / Ajout/Suppression de programmes, puis « SafeGuard Easy »). Une désinstallation de SafeGuard Easy avec la fonctionnalité Requête/Réponse ne peut pas être lancée **dans la PBA**.

26.3 Code de réponse

Le code de réponse est généré par l'administrateur ou le collaborateur du service d'assistance avec l'assistant de déblocage à distance.

Quiconque génère le code de réponse doit d'abord connaître les données d'un profil d'utilisateur SafeGuard Easy sur un ordinateur éloigné, par ex. les données du profil utilisateur « Helpdesk ». Sur l'ordinateur de l'utilisateur, « Helpdesk » doit avoir au moins les mêmes droits que le demandeur SafeGuard Easy.

Pour que le profil d'utilisateur « Helpdesk » puisse octroyer des droits spéciaux, il doit disposer pour l'action concernée des droits d'utilisateur suivants :

Action SafeGuard Easy	Droit d'utilisateur requis de SafeGuard Easy
Pour une désinstallation	désinstallation de SafeGuard Easy
Définir un nouveau mot de passe	Modifier les paramètres de l'utilisateur
Ouverture de session unique	Modifier les paramètres de l'utilisateur
Activer/désactiver temporairement le chiffrement de disquette	Commuter le chiffrement de disquettes
Ouverture se session sans jeton pour X sessions	Modifier les paramètres de l'utilisateur
Octroyer autorisation d'initialisation de jeton	---

26.3.1 Créer un code de réponse

REMARQUE :
Critères de génération d'un code de réponse sur un ordinateur :
1) Assistant de code de réponse.

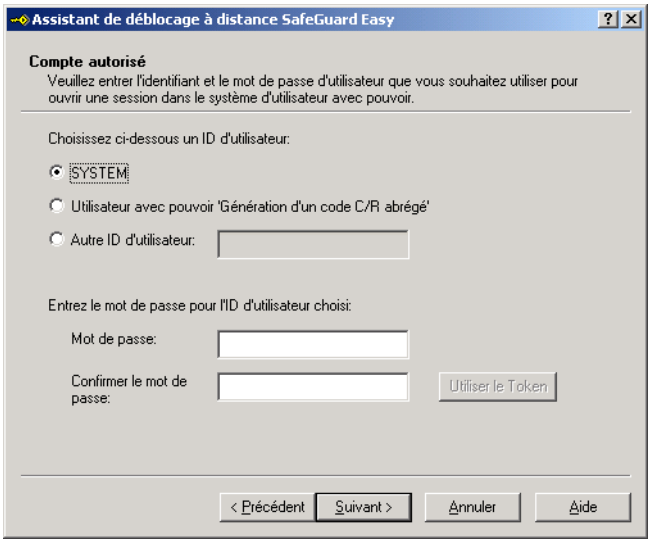
Critères de génération d'un code de réponse sur un PDA :
1) SafeGuard PDA.
2) Version PDA de l'assistant de déblocage à distance.

Démarrez l'assistant via **Programmes / Utimaco / SafeGuard Easy / Assistant de déblocage à distance**.

La première boîte de dialogue affiche des informations sur l'assistant. Confirmez successivement la saisie en cliquant sur [Suivant].

Compte d'autorisation

Dans la boîte de dialogue suivante, sélectionnez l'utilisateur SafeGuard Easy avec lequel vous souhaitez ouvrir une session dans le système de l'utilisateur à distance.



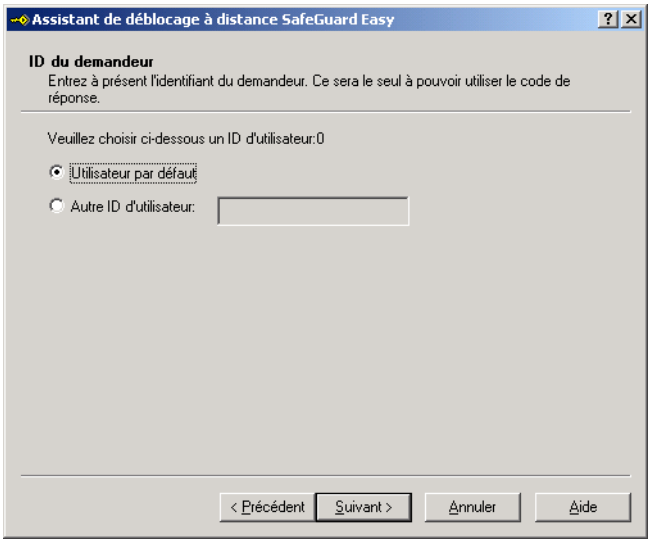
- **SYSTEM :**
  Nom de l'administrateur du système pour SafeGuard Easy.
- **Utilisateur avec droit « Génération d'un code C/R abrége » :**
  L'utilisateur auquel ce pouvoir a été affecté sur le système cible. Il doit posséder au moins les droits de l'utilisateur à distance.
- **Autre ID d'utilisateur :**
  Nom d'un utilisateur SafeGuard Easy pouvant octroyer le droit spécial.
- **Bouton «Utiliser jeton »**
  Charge le mot de passe utilisateur SafeGuard Easy du jeton lorsque ce dernier est utilisé pour la connexion.

Les noms de l'utilisateur choisis ici influent sur la longueur du code réponse généré ultérieurement. Plus il est long, plus grand est le risque d'erreurs au moment de sa saisie et/ou de sa transmission à l'utilisateur.

ID d'utilisateur	Longueur de la réponse (caractères)
SYSTEM	30
Génération d'un code C/R abrége	30
Autre ID d'utilisateur	56

ID du demandeur distant

Dans la boîte de dialogue suivante, sélectionnez le nom de l'utilisateur distant. Demandez à cet utilisateur de fournir les données d'ouverture de session.

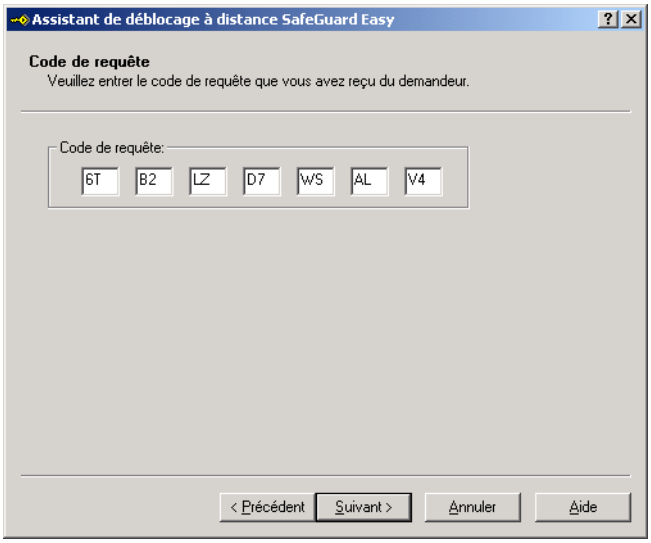


- **Utilisateur par défaut :**
  l'utilisateur ouvre sa session avec son mot de passe SafeGuard Easy. Ceci signifie qu'il est enregistré comme utilisateur par défaut sur le système cible et qu'il ne connaît pas son nom d'utilisateur par défaut.

- **Autre ID d'utilisateur :**
  l'utilisateur ouvre sa session avec le nom d'utilisateur SafeGuard Easy et le mot de passe. Le nom de l'utilisateur SafeGuard Easy est par conséquent connu. Entrez-le dans le champ.

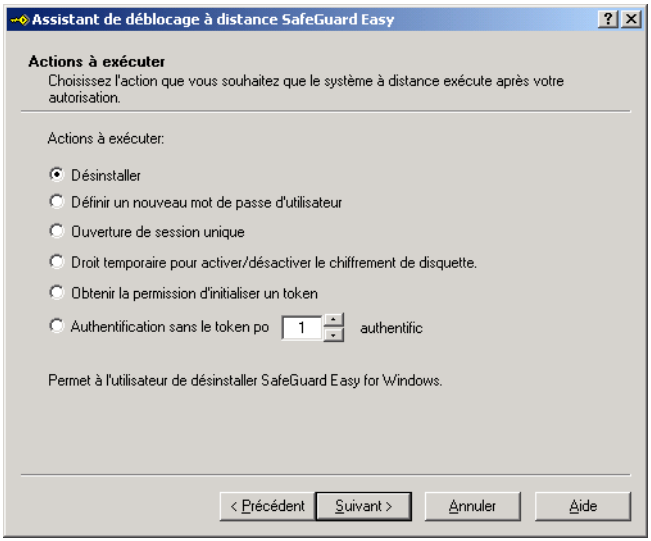
Code de requête

Dans les champs répartis par paires de la boîte de dialogue suivante, tapez le code que l'utilisateur distant vous a transmis (p.ex. Par téléphone). Le **code de requête** s'affiche sur l'ordinateur de l'utilisateur comme chaîne de caractères ASCII (14 caractères).



Commande distante

Dans la boîte de dialogue suivante, sélectionnez l'**action** qui doit être exécutée par l'utilisateur.



Une des actions suivantes peut être exécutée :

- **Désinstaller**
  L'utilisateur est autorisé à désinstaller SafeGuard Easy. Ce mode de désinstallation n'est utile que lorsque l'administrateur du système est absent.

- **Définir un nouveau mot de passe d'utilisateur**
  L'utilisateur peut modifier son mot de passe, par ex. quand il a oublié l'ancien ou quand le temps d'attente à la PBA est dépassé à la suite d'une saisie incorrecte répétée du mot de passe.

  Le mot de passe de l'utilisateur SYSTEM ne peut pas être de nouveau attribué via Requête/Réponse.

- **Ouverture de session unique**
  L'utilisateur obtient l'accès à l'ordinateur concerné pour la durée d'une session de travail).

  Ceci peut être utile, par ex. quand un technicien exécute des travaux de maintenance.

- **Droit temporaire pour activer/désactiver le chiffrement de disquettes**
  Pendant une session de travail, l'utilisateur est autorisé à activer/désactiver le chiffrement de disquette. La clé de chiffrement de disquette doit être définie à l'avance.

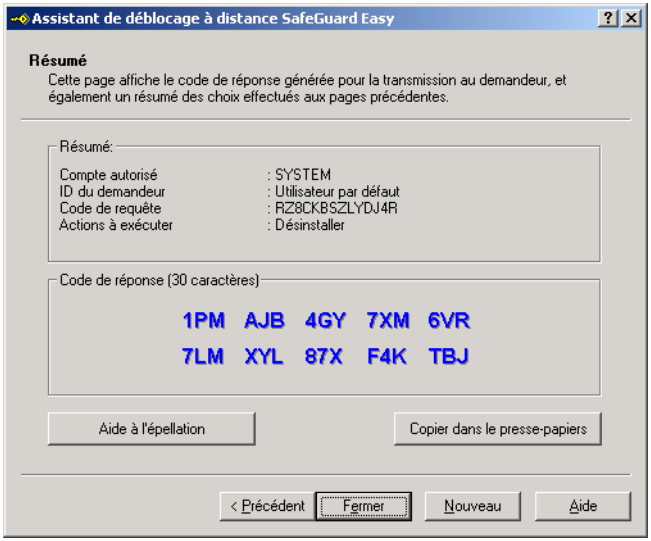
- **Obtenir la permission d'initialiser un jeton**
  L'utilisateur peut initialiser un jeton pour une fois. Cette option est important lorsqu'un jeton peut seulement être initialiser via la fonctionnalité Requête/Réponse (mode d'initialisation « Engagement externe ».

- **Authentification sans le jeton pour « X » sessions**
  L'utilisateur peut ouvrir X fois (maximum : 12) une session sans jeton (maximum 12). Cette action est utilisée quand le jeton a été oublié au domicile, alors que l'utilisateur en a absolument besoin.

Le code de réponse est généré quand la saisie est confirmée.

Résumé

Dans la dernière boîte de dialogue, vous obtenez un aperçu complet des paramètres que vous avez définis dans les boîtes de dialogue précédentes de l'assistant de déblocage à distance. Ce qui suit est en outre affiché :



Code de réponse

Affiche le code de réponse en lettres bleues. Ce code doit être transmis au demandeur. Le demandeur entre le code de réponse dans les champs prévus à cet effet. Le code de réponse n'est valable qu'une seule fois ! Un nouveau code doit être généré pour chaque requête.

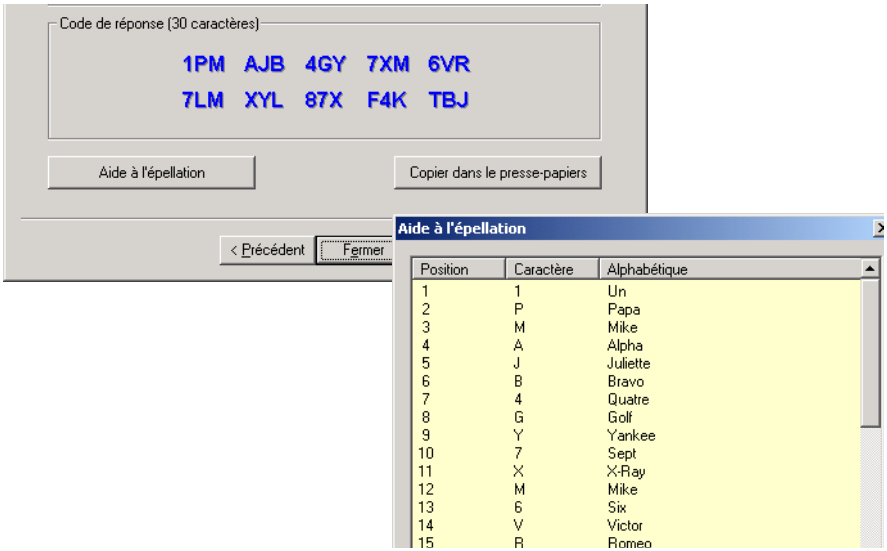
Copie dans le Presse-papiers

Le code de réponse est copié dans le Presse-papiers et peut être entré dans n'importe quel éditeur de texte. Cette fonctionnalité permet, par exemple, d'envoyer le code de réponse de façon simple par SMS ou courrier électronique à l'utilisateur.

Si toutes les valeurs sont correctes et si le demandeur a pu exécuter les actions requises, l'assistant de déblocage à distance est fermé en cliquant sur **Quitter**. Un clic sur **Nouveau** efface toutes les valeurs et permet de générer un nouveau code de réponse ou un code supplémentaire.

Aide à la rédaction
Pour faciliter la transmission du code et pour éviter les erreurs, l'assistant de déblocage à distance inclut un correcteur orthographique.

Quand vous cliquez sur le bouton [Aide à l'épellation], une fenêtre divisée en trois colonnes apparaît avec les titres de colonne correspondants. « Position » indique l'emplacement du caractère dans le code. Il est ainsi possible de répondre sans perte de temps (par exemple, décompte des positions) aux questions. Vous pouvez voir le caractère qui doit être entré. « Alphabétique » indique avec quel mot le caractère peut être « lié » pour éviter les confusions, comme les mots de code radio (dans cet exemple). En règle générale, on utilise des prénoms dont la première lettre est alors entrée dans les champs de code. La fenêtre affiche le code de réponse réel. Il vous suffit de le lire de haut en bas.



26.4 Élargissement du concept Requête/Réponse

Outre le procédé standard, il existe encore diverses solutions Requête/Réponse logicielles et matérielles :

26.4.1 Console service assistance

Pour les environnements de plus grande étendue, dans lesquels le personnel du service d'assistance ne doit pas connaître les mots de passe principaux des clients SGE, le système peut être étendu par un module matériel de chiffrement (CryptoServer) et une solution logicielle.

Console service assistance matérielle

Quand on utilise le CryptoServer 2000, les mots de passe de l'administrateur SafeGuard Easy sont saisis une fois dans le CryptoServer 2000 et y restent mémorisés de façon sûre. Ces mots de passe ne sont pas connus du personnel du service d'assistance.

Le code de réponse est généré dans CryptoServer 2000. Le personnel du service d'assistance peut ainsi générer un code de réponse pour les données d'utilisateur correspondantes (nom, code de requête) sans connaître personnellement le mot de passe de l'administrateur SafeGuard Easy. Chaque collaborateur du service d'assistance se voit attribuer à cet effet par l'administrateur du CryptoServer 2000 un compte (nom d'utilisateur, mot de passe) sur le Cryptoserver qui l'autorise à générer un code de réponse. Ce compte peut à tout moment être supprimé (par exemple quand le collaborateur quitte le service), ce qui fait que le collaborateur concerné n'est alors plus en mesure d'accéder au CryptoServer 2000.

La console service assistance matérielle est disponible comme compagnon séparé.

Console service assistance centrale

La console service assistance centrale fonctionne de façon similaire à la solution CryptoServer. Dans ce scénario, le personnel du service d'assistance ne connaît pas non plus les mots de passe de l'administrateur SGE.

Avec cette variante logicielle (interface Web), l'information nécessaire pour générer une réponse est enregistrée dans une base de données protégée (chiffrée avec AES-256) sur un PC sur lequel fonctionne Microsoft Internet Information Services. Le code de réponse correspondant aux requêtes est calculé et est présenté à l'employé du centre d'assistance. Les membres du service d'assistance s'identifient de façon individuelle et à distance sur la page Web du serveur d'informations Internet.

La console service d'assistance centrale est disponible sous forme de complément autonome.

26.4.2 Auto-assistance Web

L'avantage essentiel de l'assistance Web est que les utilisateurs peuvent réinitialiser les mots de passe SGE oubliés sans faire appel au service d'assistance. Pour qu'un utilisateur soit autorisé à redéfinir lui-même son mot de passe, il doit d'abord s'enregistrer dans une base de données centrale. L'enregistrement se fait via un mécanisme spécial : l'utilisateur tape ses réponses pour un nombre de données de questions au choix. Ces réponses sont enregistrées dans la base de données. L'utilisateur enregistré est validé par l'administrateur et reçoit un courrier électronique contenant un code PIN. Si l'utilisateur souhaite ensuite générer un code de réponse d'auto-assistance Web pour son profil SGE, il doit saisir le code PIN et les réponses correctes.

La procédure s'effectue sur le Web et est donc accessible de pratiquement n'importe où sans logiciels supplémentaires.

La fonctionnalité d'auto-assistance est disponible sous forme de complément autonome.

26.4.3 VOICE.TRUST

Une autre extension possible du système Requête/Réponse est la configuration d'un serveur biométrique de VOICE.TRUST avec modules à connecter pour SafeGuard Easy ou SafeGuard PDA.
Le serveur VOICE.TRUST est en mesure d'authentifier la voix des utilisateurs (Voiceprint) et exécute automatiquement la procédure Requête/Réponse complète avec l'utilisateur sous forme de reconnaissance et synthèse vocale, 24 heures sur 24.
Le personnel du service d'assistance n'est mis à contribution que dans des cas exceptionnels, ce qui permet de le libérer des tâches de routine telles que la réinitialisation de mots de passe oubliés.

Veuillez contacter votre fournisseur SafeGuard Easy local pour plus de détails sur les extensions en option.

27 Création de supports de restauration d'urgence et sauvegarde du noyau système

Quand votre ordinateur affiche des messages d'erreur SafeGuard Easy une fois le disque dur chiffré, le noyau système SafeGuard Easy ne peut pas être trouvé dans la plupart des cas. Le noyau système contient les pilotes pour SafeGuard Easy et le MBR.

Les erreurs qui se sont produites peuvent être fréquemment corrigées en chargeant le noyau système actuel sécurisé. Pour charger le noyau système, l'utilisateur doit cependant disposer à la fois d'un noyau système intact et d'une **disquette/CD/clé de USB de secours**. Cette disquette/CD/clé USB contient le noyau système sécurisé et les fichiers de résolution des erreurs SafeGuard Easy.

Comme vous ne pourrez probablement pas, en cas de défaillance du système, accéder au disque dur, le noyau système et tous les fichiers de secours doivent être toujours sauvegardés sur une disquette ou sur un périphérique amovible.

REMARQUE :
Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco http://www.utimaco.com/myutimaco.

Dans la zone de recherche (« Search »), tapez « Emergency » ou « Emergency Disk ».

27.1 Création d'une disquette de secours/sauvegarde du noyau système

La disquette de secours est créée par « l'Assistant de création d'une disquette de démarrage », disponible en standard sur tous les clients. Si des lecteurs de disquettes/périphériques amovibles sont chiffrés, le chiffrement est désactivé pendant la création de la disquette de démarrage.

Ceci implique que la disquette de restauration d'urgence dispose de la version la plus récente du noyau système. Toute modification importante, telle qu'une modification du statut du chiffrement, doit faire l'objet d'une sauvegarde sur une disquette. Une option de l'Assistant de création de disquette de démarrage permet de demander à intervalles réguliers la sauvegarde du noyau système. Ceci doit être copié sur la disquette de démarrage.

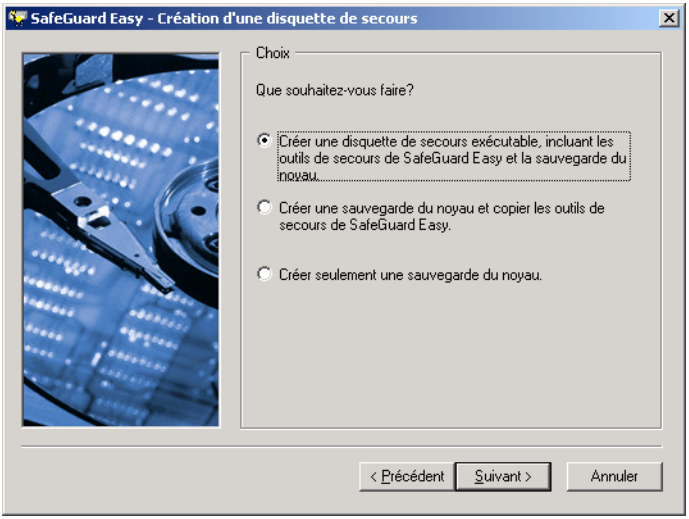
L'Assistant dispose d'une option supplémentaire pour la création d'une disquette de démarrage d'urgence contenant le noyau système, des outils d'urgence et les fichiers du pilote de clavier.

27.1.1 Exécution de l'Assistant de création d'une disquette de démarrage d'urgence

L'Assistant de création de disquette de démarrage d'urgence s'exécute de façon automatique à l'issue de l'installation de SafeGuard Easy. Cependant, vous pouvez également l'exécuter en sélectionnant **Programmes/Utimaco/SafeGuard Easy/Emergency Disk Wizard**.

Pour valider les données entrées dans l'assistant, cliquez sur [Suivant].

1. Une fois l'Assistant démarré, une seconde boîte de dialogue s'affiche. Cette boîte de dialogue permet de spécifier les fichiers à enregistrer sur la disquette de démarrage d'urgence.



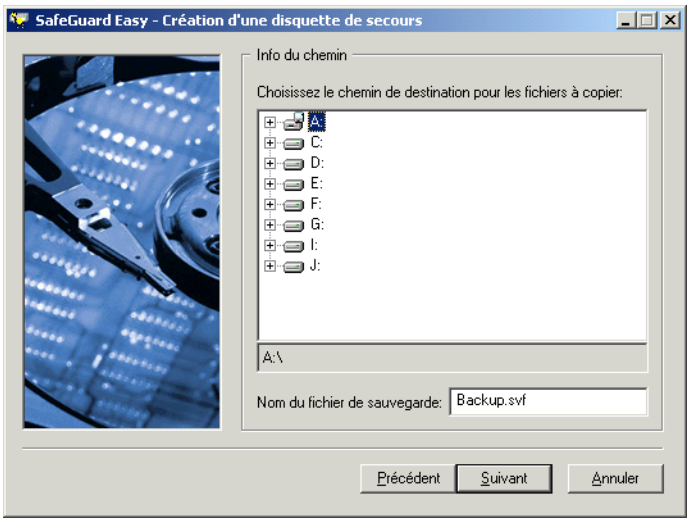
Les options ci-dessous sont disponibles :

- **Créer seulement une sauvegarde du noyau**
  Cette fonction sauvegarde le noyau système complet (pilotes pour SafeGuard Easy et le MBR) dans un fichier.

- **Créer une sauvegarde du noyau et copier les outils de secours de SafeGuard Easy**
  Copie le noyau système et les fichiers de démarrage suivants :

- **Créer une disquette de secours exécutable, incluant les outils de secours de SafeGuard Easy et la sauvegarde du noyau**
  Crée une disquette exécutable avec une version FreeDOS, le noyau système et les fichiers de démarrage.

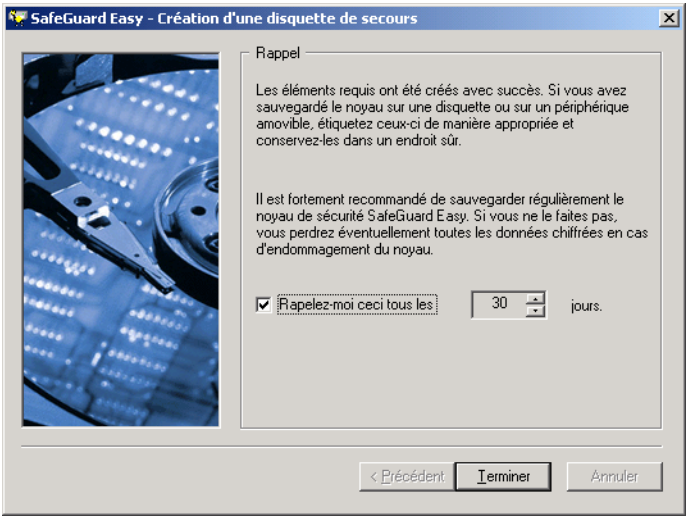
2. Vous choisissez ensuite l'endroit où les données (noyau système et fichiers de secours) doivent être enregistrées.



Le champ *Info du chemin* permet de définir l'emplacement d'enregistrement du noyau système et des fichiers d'urgence (si sélectionnés). Entrez le nom du noyau système dans le champ *Nom du fichier de sauvegarde*. La valeur par défaut est `BACKUP.svf`, mais vous pouvez modifier le nom et l'extension .svf si nécessaire. Vous pouvez également enregistrer le noyau système sur un disque dur ou un réseau.

En cas d'erreur système, cependant, il est probable que vous ne pourrez pas accéder au disque dur. Vous devez pas conséquent toujours stocker le noyau système et les fichiers de démarrage d'urgence sur une disquette, un autre type de support amovible ou le lecteur réseau.

3. Dans la boîte de dialogue *Rappel*, vous pouvez indiquer ici les intervalles de rappels de sauvegarder du noyau système.



Dans la mesure où il est essentiel que vous disposiez de la version la plus récente du noyau système en cas d'erreur système, nous recommandons fortement de procéder toujours à des sauvegardes régulières.

27.1.2 Sauvegarde du noyau système via la ligne de commande

Le noyau système peut être également sauvegardé à partir de la ligne de commande de la manière suivante :

```
SGEBACK.EXE /f :<chemin/nom de fichier> | /S | /?
```

/f: Affiche le chemin et le nom de fichier utilisé pour enregistrer le noyau

Vous pouvez donner le nom et l'extension de votre choix au fichier cible.

/S Envoie la sauvegarde de noyau définie dans le paramètre /f sur

le serveur SGE

/? Affiche cette aide

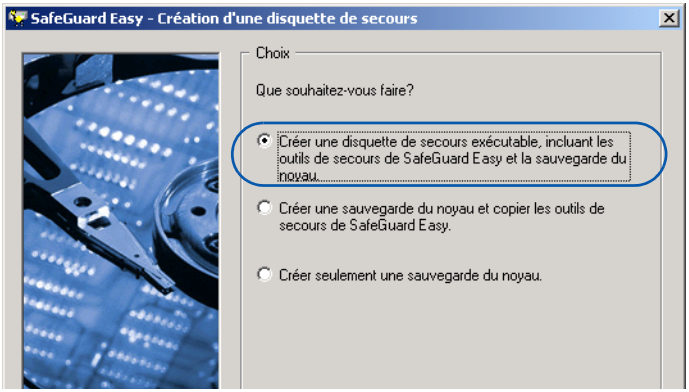
27.1.3 Sauvegarde des fichiers de secours SafeGuard Easy sur disquette

Vous pouvez également enregistrer les fichiers d'urgence sur une disquette de façon manuelle. Copiez les fichiers suivants du répertoire d'installation de SafeGuard Easy :

- SGEASY.exe
- Sgeasy.hmf
- Sgecrypt.mod
- Sgenls.mod
- Sgekrnl.mod

27.2 Création d'une disquette de démarrage

L'Assistant propose en outre l'option de création d'une disquette de démarrage avec noyau système, outils de secours et fichiers de pilotes pour la configuration du clavier. Cette option simple permet de combiner disquette de démarrage et disquette de secours SafeGuard Easy.



Démarrez l'assistant de création d'une disquette de démarrage.

1. Insérez une disquette et lancez l'Assistant de création de disquette de démarrage.

2. Sélectionnez l'option « Créer une disquette de démarrage, incluant les outils de secours de SafeGuard Easy et la sauvegarde du noyau ».

Lors de la première sauvegarde du noyau système, Utimaco recommande de créer une disquette de démarrage et de mettre à jour celle-ci dès que le noyau système est modifié.

27.3 Création d'un CD de démarrage

Les appareils mobiles ne possèdent normalement plus, aujourd'hui, de lecteurs de disquettes. SafeGuard Easy permet par conséquent également le démarrage à partir d'un CD.

Voici comment créer un CD de démarrage :

1. Enregistrez le fichier d'image d'amorçage `Floppy.iso` (se trouve sur le CD SafeGuard Easy dans le répertoire \TOOLS) sur le disque dur et gravez-le sur le CD au moyen d'un logiciel de gravure usuel.

   Le fichier Iso contient la disquette de démarrage complète, telle qu'elle est créée par l'Assistant, à l'exception de la sauvegarde du noyau système.

2. Exécutez une sauvegarde du noyau système via l'Assistant de création de disquette de démarrage. Enregistrez la sauvegarde du noyau système sur le CD proprement dit ou sur un support externe en texte clair, auquel vous pourrez accéder en cas d'urgence.

Dans le BIOS, assurez-vous que le système démarre bien du CD.

La version du BIOS de l'ordinateur conditionne le démarrage du système !

27.4 Création d'une clé USB de démarrage

La clé USB doit pouvoir être amorcée sur votre système !

Voici comment créer une clé UB de démarrage :

1. Préparez la clé USB pour permettre l'amorçage.
2. Copiez les fichiers de secours SafeGuard Easy sur la clé.
3. Exécutez SGEasy.exe.

La version du BIOS de l'ordinateur conditionne le démarrage du système !

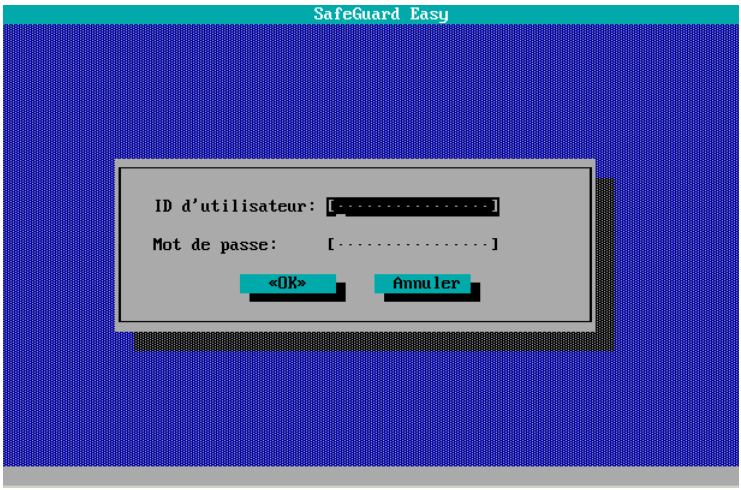
27.5 Exécution d'un démarrage d'urgence

En cas de problème sur un disque dur chiffré, procéder comme suit :

1. insérez une disquette ou un CD de démarrage et démarrez l'ordinateur.

2. Le programme des secours `Sgeasy.exe` est lancé automatiquement.

3. Entrez le mot de passe SafeGuard Easy. Confirmez la saisie en cliquant sur [OK].



4. Un menu avec les rubriques *Désinstaller, Sauvegarder*, *Restaurer* et Réparer *apparaît.*

27.5.1 Restauration du noyau système

La restauration du noyau système requiert la présence d'un noyau système valide sur le poste de travail. Lorsqu'il existe une sauvegarde, le MBR et le noyau système SafeGuard Easy peuvent être aisément restaurés sur le poste de travail à partir de cette sauvegarde.

Cette fonction ***ne doit pas*** être exécutée si

- SafeGuard Easy a été précédemment désinstallé
- la sauvegarde du noyau système ne correspond plus à sa version actuelle. C'est le cas quand, par exemple, l'état de chiffrement du ou des disques durs a été modifié entre la sauvegarde et la restauration du noyau système.

Tous les utilisateurs de SafeGuard Easy (et pas seulement l'utilisateur « SYSTEM ») peuvent restaurer le noyau système.

27.5.2 Réparation du noyau système

Contrairement à la fonction « Restaurer », une réparation s'effectue également sans copie de sauvegarde du noyau système. La fonction de réparation parcourt la totalité du disque dur à la recherche du noyau système SafeGuard Easy et essaie de le restaurer (succès non garanti !).

Cette fonction est requise uniquement

- quand il n'existe pas de sauvegarde du noyau système
- quand la sauvegarde du noyau système ne correspond plus à sa version actuelle. C'est le cas quand l'état de chiffrement du ou des disques durs a été modifié entre la sauvegarde et l'apparition de la panne système.

Après sélection de la fonction « Réparer », une routine de diagnostic essaie de localiser le noyau système et de le réactiver. Ceci peut durer plusieurs minutes. Le déroulement est indiqué par une barre de progression. Le système vous indique ensuite si la réparation s'est effectuée avec succès.

> ***REMARQUE :***
> Les tentatives de résolution de panne système avec la fonction Réparer n'ont pas toujours le succès escompté. Il est donc recommandé de toujours disposer d'une sauvegarde récente du noyau système.

27.5.3 Désinstallation d'urgence de SafeGuard Easy

Quand l'erreur système ne peut être éliminée ni avec « Restaurer », ni avec « Réparer », il ne reste plus que la variante trois, le déchiffrement du disque dur et la désactivation de la PBA. Après la désinstallation, le poste de travail est redémarré automatiquement deux fois.

Cependant, avant de procéder, le profil utilisateur de SafeGuard Easy doit disposer de droits suffisants. Si un utilisateur ne dispose pas de droits de désinstallation, ces derniers ne peuvent être affectés par l'intermédiaire de la procédure Requête/Réponse (voir 'Maintenance à distance (Requête/Réponse)').

Il est judicieux de procéder également à une vérification des supports de données dans Windows. Vous trouverez des informations à ce sujet dans votre documentation Windows.

Échec du déchiffrement

Veuillez contacter notre équipe de support en cas d'échec de la procédure de chiffrement ou déchiffrement.

Support étendu des expertises (paramètre /NoReboot)

La fonction de déchiffrement d'urgence de SafeGuard Easy inclut le paramètre de commande `/NoReboot` pour le programme d'urgence `SGEASY.exe`. Ce paramètre de ligne de commande permet d'éviter le redémarrage automatique après le déchiffrement d'urgence. Ceci est particulièrement utile en cas d'expertise du disque dur.

Comment procéder :

1. Démarrez le support d'urgence.
2. Démarrer `Sgeasy.exe /NoReboot`.
3. Le déchiffrement ou la désinstallation d'urgence est terminée
4. L'ordinateur est arrêté et le système affiche un texte d'information. Il est possible d'exécuter d'autres programmes ou d'effectuer toute autre opération avec l'ordinateur.

Le disque dur est endommagé

Veuillez noter ce qui suit : Si vous suspectez que le disque dur chiffré présente des dommages physiques, il est recommandé de ne pas le déchiffrer avec un support de secours.

Un défaut physique peut se remarquer par exemple de la manière suivante : le disque dur émet de bruits de frottement ou des cliquets, ou n'est plus reconnu par le BIOS. Dans ce cas, n'intervenez pas vous-même, mais adressez-vous à un spécialiste. Ils tenteront de transférer le contenu du disque dur corrompu sur un disque intact , de façon à pouvoir procéder à un déchiffrage d'urgence des données. Cette intervention externe entraîne naturellement des frais, qui seront à opposer à la valeur des données présentes sur le disque dur.

REMARQUE :
Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco http://www.utimaco.com/myutimaco.

Dans la zone de recherche (« Search »), tapez « Data & Recovery ».

27.5.4 Remarques

- **Emplacement du noyau système**
  Si la partition d'amorçage de Windows ne se trouve pas sur le premier disque dur, le noyau système SafeGuard Easy est automatiquement stocké pendant l'installation sur la partition C:. Cette partition ne doit par conséquent plus être formatée après l'installation, car elle contient les informations Windows les plus importantes (noyau système, pilotes, etc.). Si toutefois un formatage est effectué après l'installation de SafeGuard Easy, le système doit être réinstallé.

  Cette sauvegarde est toutefois spécifique au système, c'est-à-dire qu'elle ne peut être restaurée que sur l'ordinateur où elle a été effectuée.

  Cependant, si une erreur système se produit, le disque dur risque de ne plus être accessible. Comme vous ne pourrez probablement pas, en cas de défaillance du système, accéder au disque dur, le noyau système et tous les fichiers de secours doivent être toujours sauvegardés sur une disquette ou sur un périphérique amovible.

- **Langue de Sgeasy.exe**
  La langue de l'interface utilisateur du programme de secours est déterminée par le fichier Sgeasy.hmf (qui se trouve sur la disquette de secours).Les différentes éditions du fichier de langue pour l'Allemand (Sgeasy07.hmf), l'Anglais (Sgeasy09.hmf) et le Français (Sgeasy0C.hmf) se trouvent dans le répertoire d'installation de SafeGuard Easy. L'utilisateur doit renommer le fichier SGEASY, <09,07,0C>.hmf pour la disquette de secours, en SGEASY.HMF pour obtenir la langue souhaitée dans SGEASY.EXE.

27.6 Accès aux données chiffrées lors du redémarrage à partir d'un support externe

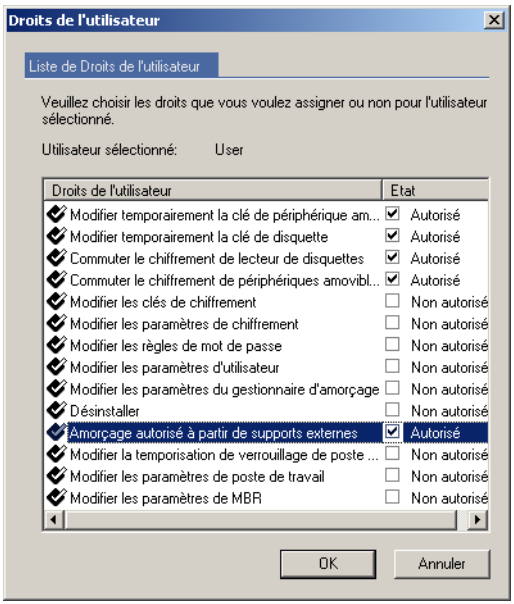
Dans certaines situations (d'urgence), les utilisateurs doivent démarrer un système chiffré avec SafeGuard Easy à partir d'un support de données externe, par exemple pour sauvegarder des données quand le système d'exploitation ne démarre plus. Les utilisateurs ne peuvent toutefois démarrer le système à partir d'un support externe (et accéder aux données sur l'ordinateur) qu'une fois que des données SafeGuard Easy valides ont été entrées dans l'authentification avant amorçage.

Cette méthode d'amorçage est recommandée pour sauvegarder des données en cas d'urgence avant la réparation du système d'exploitation ou la désinstallation d'urgence de SafeGuard Easy.

Les supports d'amorçage pris en charge par SafeGuard Easy sont les disquettes MS DOS/Windows 9x et les CD/clés USB (pour DOS et Windows EP). Il est essentiel que les supports d'amorçage contiennent le pilote SafeGuard Easy.

27.6.1 Conditions

L'amorçage à partir d'un support externe est un droit d'administrateur SafeGuard Easy qui n'est accordé, dans la configuration de base, qu'à l'utilisateur « SYSTEM ». Si le système doit être démarré à partir d'un support externe, le profil SafeGuard Easy s'étant identifié dans la PBA doit disposer du droit « Amorçage autorisé à partir de supports externes ».



27.6.2 Comment procéder

1. Démarrez le système à partir du disque dur.

2. L'authentification avant amorçage de SafeGuard Easy apparaît.

3. Entrez les données dans la PBA.

4. a) Insérez la **disquette d'amorçage**. Confirmez les données PBA en appuyant sur **[Entrée]**.
   b) Insérez le **CD de démarrage**. Confirmez les données PBA en appuyant sur **[F7]**.

5. L'ordinateur redémarre à partir du support de démarrage externe.

6. Une fois le redémarrage effectué avec succès, il est possible d'accéder aux données ou de les sauvegarder.

27.6.3 Remarques

- La version du BIOS conditionne le bon démarrage via CD/clé USB !
- Vous trouverez dans notre base de connaissances une description du mode de création de CD Windows PE de démarrage.

  Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco **http://www.utimaco.com/myutimaco**.

  Dans la zone de recherche (« Search »), tapez « BartPE » ou « SGE ».
- La fonction Rescue and Recovery de Lenovo, « Create Rescue Media », crée automatiquement un CD, avec pilotes SafeGuard Easy lorsque SafeGuard Easy est installé. Cette option est disponible via Programmes / Thinkvantage (Access IBM).

27.6.4 Que faire, si ...

... le démarrage à partir d'un support externe échoue ?

Les raisons suivantes sont possibles :

- L'utilisateur SafeGuard Easy ayant ouvert la session ne dispose pas du droit « Amorçage autorisé à partir de supports externes ».
- Le chiffrement du disque dur a été lancé, mais n'est pas encore terminé.

Les raisons suivantes sont également possibles en cas d'échec de démarrage à l'aide d'une disquette :

- Le lecteur de disquettes n'est pas appelé par le contrôleur de disquettes standard, mais via l'interface USB.
- Le lecteur de disquettes est chiffré, mais la disquette de démarrage ne l'est pas encore.

28 Affichage de l'état système de SafeGuard Easy

SafeGuard Easy dispose d'un outil de ligne de commande, SGEState, qui indique l'état de l'installation SafeGuard Easy sur l'ordinateur de l'utilisateur (version, mode de chiffrement, chiffré/non chiffré, etc.). Cet outil convient particulièrement aux installations dans un environnement étendu en permettant à un administrateur d'interroger simplement l'état d'une installation SafeGuard Easy.

On peut également utiliser SGEState pour exécuter certaines opérations ou procédures lorsque l'installation (ou le chiffrement) de SafeGuard Easy est terminée.

Après l'installation de SafeGuard Easy Client, vous trouverez SGEState dans le répertoire Programmes.

28.1 Génération de rapports

SGEState peut également servir à la génération de rapports :

- Le code de retour de SGEState peut être évalué, côté serveur, par les outils de gestion de fournisseurs tiers.
- SGEState /LD renvoie une sortie formatée pour LANDesk (et autres produits). Cette sortie est dirigée vers un fichier et peut être envoyée au serveur pour évaluation.

28.2 Paramètres

SGEState peut être appelé avec les paramètres suivants :

```
SGESTATE [/?] [/Q | /L | /LD] [/E [/Mvalue]] [/Dvalue] [/R]
```

SGEState /? donne une vue d'ensemble de tous les paramètres de ligne de commande disponibles :

```
/Q...Quiet mode: No output, program ends with return code:

  0...SafeGuard Easy not installed.
  2...SafeGuard Easy installed.
  3...SafeGuard Easy installed. Encryption or decryption process active.
255...An error occurred during the check. In this case, a message
      to the console will state the nature of the problem.

/L...Loud mode. Will display details to the console including:

Operating System: [WINDOWS 2000 ¦ WINDOWS XP ¦ WINDOWS SERVER 2003]

Installation Status         : [INSTALLED ¦ NOT INSTALLED ¦ UNKNOWN ¦
                               INSTALLED (NOT READY FOR BACKUP)]
Version number              : [N/A ¦ number]
Installation Mode           : [N/A ¦ STANDARD ¦ PARTITIONED ¦ BOOT PROTECTION ¦
                               UNKNOWN]
Disk Encryption             : [N/A ¦ OFF ¦ ON]
Floppy Encryption           : [N/A ¦ OFF ¦ ON]
Removable Media Encryption  : [N/A ¦ OFF ¦ ON]
Initial Encryption          : [N/A ¦ ACTIVE ¦ INACTIVE]

Pre Boot Authentication     : [N/A ¦ OFF ¦ ON]
Current Authentication      : [N/A ¦ USER ¦ WAKE ON LAN]
Secure Auto Logon           : [N/A ¦ OFF ¦ ON]
Secure Smartcard Auto Logon: [N/A ¦ OFF ¦ ON]
SGE Management Server       : [N/A ¦ <UNMANAGED> ¦ OFFLINE ¦ server]

Return code                 : [ReturnCode]

/LD...The details are displayed in LANDesk mode:

/E...Extended return code:

En-/Decryption in process          :  1
SafeGuard Easy installed           :  2
Floppy Encryption "ON"             :  4
Disk Encryption "ON"               :  8
Installation Mode "Boot Protection": 16 (hex 10)
Installation Mode "Partitioned"    : 32 (hex 20)
Installation Mode "Standard"       : 64 (hex 40)
                                     only one mode is possible, (16, 32 or 64)

/Mvalue...value mask for extended return code 1..127

For example: SGESTATE /E produces return code 43 (hex 2b). This indicates:
Partitioned mode, Disk Encryption "ON", SGEasy installed, Encryption in process

For example: SGESTATE /E /M15 produces return code 11 (hex 0b)

/Dvalue...value for desired return code 0..127
          The return code is computed until the desired one is reached
          Calculation can be stopped by pressing any key

/R...the return code is stored in the registry

The input charaters are not case sensitive.
```

29 Audit

L'enregistrement d'événements intéressant la sécurité est la condition pour une analyse approfondie du système. Sur la base des événements audités, des opérations effectuées sur une station de travail ou dans un réseau peuvent être suivies de manière plus exacte. L'audit permet de prouver par exemple des violations de droits par des tiers non autorisés. L'audit offre également à l'administrateur une aide pour retrouver ou corriger des droits d'utilisateur refusés par erreur.

L'audit enregistre les événements déclenchés par des produits SafeGuard installés, tels qu'une connexion par carte à puce, modification d'un code confidentiel, certificat expiré, etc.

L'utilisateur possédant les droits appropriés peut soit visualiser les événements audités directement via l'observateur d'événements de Windows, soit les exporter dans un fichier personnalisé à des fins d'archivage. Les données sont soit enregistrées localement, soit transmises à distance à une station de travail centrale.

Outre l'audit pour des données, il existe un mécanisme de filtrage qui, grâce à une sélection ciblée des événements concernés, aide à contenir le flux de données causé par l'enregistrement de tous les événements possibles.

L'audit enregistre les événements SafeGuard Easy suivants :

- déroulement du processus d'ouverture de session à la PBA (succès/échec)
- actions d'administration (création d'un utilisateur, etc.)
- déroulements avec administration centrale (client assigné au serveur, etc.)
- succès/échec de l'exécution de fichiers de configuration
- processus d'installation/désinstallation
- processus de chiffrement/déchiffrement

29.1 Domaines d'application

SafeGuard Auditing est une solution conviviale pour enregistrer des événements. Des exemples montrent quelques scénarios typiques de la manière d'utiliser SafeGuard Auditing.

Surveillance centrale de stations de travail sur le réseau

L'administrateur souhaite être par exemple informé des événements SafeGuard intéressant la sécurité (par exemple exécution de fichiers, pour lesquels l'utilisateur ne possède pas d'autorisation, etc.). Il peut configurer SafeGuard Auditing de manière à ce que les événements SafeGuard soient automatiquement transférés et enregistrés par certains ordinateurs à l'observateur d'événements ou à un fichier journal choisi lui-même sur une station de travail d Les événements sur diverses stations de travail sont donc contrôlés en continu sans que le collaborateur puisse influer d'une manière ou d'une autre sur les enregistrements. Pour utiliser ce mécanisme, l'emploi du composant Microsoft Message Queuing est nécessaire.

Surveillance d'utilisateurs mobiles

Les utilisateurs mobiles ne sont normalement pas reliés en permanence au réseau de l'entreprise.

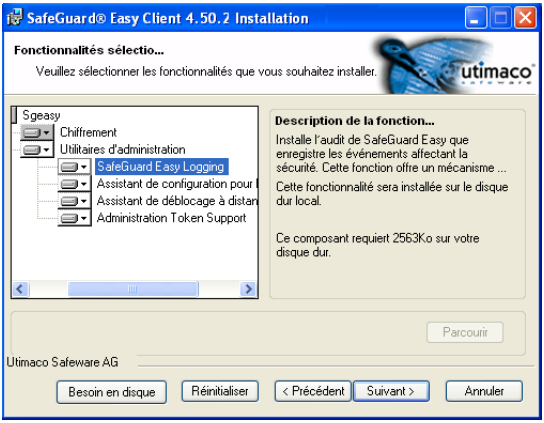
Quand il a un rendez-vous, un collaborateur du service extérieur déconnecte par exemple son ordinateur portable du réseau. Dès qu'il se reconnecte au réseau, les événements SafeGuard audités par SafeGuard Auditing pendant la déconnexion sont transmis. SafeGuard Auditing fournit ainsi à l'administrateur un aperçu exact des activités de l'utilisateur pendant que l'ordinateur n'était pas connecté au réseau.

29.2 Installation d'Auditing

Pour installer SafeGuard Easy Auditing, activez la fonctionnalité SafeGuard Easy Logging pendant l'installation de SafeGuard Easy Client.

1. Exécutez le fichier Sgeasy.msi, situé dans le dossier Client sur le CD du produit.

2. Lorsque la boîte de dialogue Fonctionnalités selectionées s'affiche, sélectionnez SafeGuard Easy Logging (l'audit de SafeGuard Easy) en plus des composants déjà sélectionnés puis poursuivez l'installation.



3. Une fois l'installation terminée, redémarrez votre ordinateur.

29.3 Configuration

Tous les paramètres pour Auditing sont gérés via des stratégies de groupe/objets Stratégie de groupe à l'aide du **composant logiciel enfichable de stratégie** de groupe dans la console MMC (**Microsoft Management Console).** Par défaut, MMC est intégré avec Windows 2000 et Windows XP.

Procédez comme suit pour ajouter le composant logiciel enfichable Stratégie de groupe :

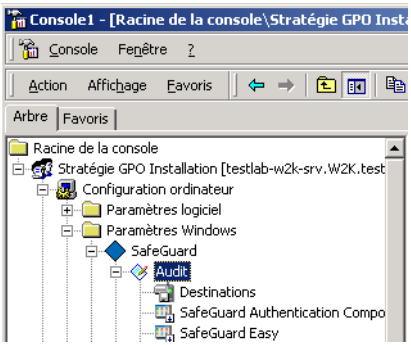
1. Activez Microsoft Management Console (sélectionnez Démarrer, Exécuter... et tapez « mmc ».)

2. Le module MMC s'affiche. Dans le menu *Console*, cliquez sur *Ajouter/ supprimer un composant logiciel enfichable* et cliquez sur Ajouter.

3. Double-cliquez sur le composant de stratégie de groupe à ajouter.

4. Choisissez un « ordinateur local » (c'est-à-dire l'ordinateur sur lequel la console est active) ou un objet Stratégie de groupe via le bouton [Parcourir] dans un environnement Active Directory.

Le dossier Auditing s'affiche ensuite dans la configuration Utilisateur et Ordinateur des paramètres Windows.



29.4 Configuration de la journalisation des événements

Pour consigner les événements dans un journal, les étapes suivantes doivent être exécutées en série :

- définir la destination des événements
- déterminer les événements à enregistrer
- afficher les données enregistrées

29.4.1 Définition des destinations

L'exécution manquée ou réussie d'événements est consignée dans ce qu'il est convenu d'appeler des modules de sortie. SafeGuard Auditing appelle ces modules *Destinations*. La destination peut être soit l'observateur d'événements de Windows, soit un fichier journal. L'enregistrement des événements est également possible d'une station de travail à l'autre. Dans une destination, SafeGuard Auditing ne consigne que les événements associés à un produit Utimaco.

Observateur d'événements
L'observateur d'événements de Windows est un outil permettant de recueillir des informations de surveillance. L'observateur d'événements peut afficher et administrer des journaux pour les événements intéressant le système, la sécurité ou l'application, et également sauvegarder ces journaux d'événements. Il permet également d'enregistrer ces journaux d'événements.

Fichier journal
Pour l'archivage, les événements SafeGuard peuvent également être sauvegardés dans des fichiers. Ces derniers peuvent être analysés et traités avec les outils les plus divers (par ex. MS-Excel).

Journal distant
La tâche du journal distant est d'échanger des données entre une station de travail de destination et une station de travail distante dans un réseau. Pour ce faire, l'ordinateur de destination rassemble des informations (événements) dans son observateur d'événements ou dans un fichier journal. Ces informations sont ensuite transférées à partir de la station de travail distante suite à une connexion distante. **Le journal distant ne fonctionne qu'en liaison avec le module de base de SafeGuard Advanced Security.**

REMARQUE :
Pour l'échange de données d'audit entre plusieurs stations de travail, il est recommandé d'employer le mécanisme de journal distant et d'éviter l'écriture dans un fichier journal sur un lecteur réseau partagé.

Lors de l'audit sur un serveur , l'enregistrement à distance doit être utilisé, étant donné que le compte système travaille avec SafeGuard Auditing, qu'il n'a pas de d'autorisation réseau et ne peut par conséquent pas écrire dans un fichier journal situé sur un lecteur réseau.

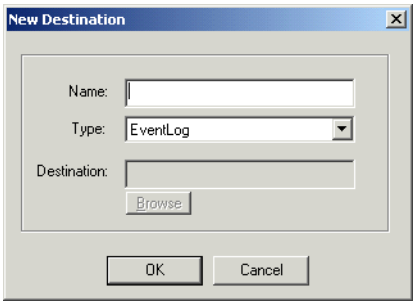
29.4.2 Création d'une destination

Voici comment créer une nouvelle destination :

1. Cliquez sur **Destination**.

2. Cliquez sur l'icône ou, avec le bouton droit de la souris, sur **Destinations**, puis sur **Ajouter une nouvelle destination**.

3. La boîte de dialogue Nouvelle destination apparaît.



Nom :
Entrez ici un nom de votre choix pour la destination. Le nom peut contenir des espaces et des caractères spéciaux.

Type :
Détermine le type de journal à utiliser :

- Sélectionnez **Observateur d'événements** quand les événements doivent être stockés dans l'observateur d'événements de Wndows.
- Sélectionnez **Fichier journal** quand les événements doivent être enregistrés dans un fichier.

  Conseil : Le fichier sélectionné ne doit pas être protégé en écriture.

- Sélectionnez **Enregistrement à distance** quand les événements doivent être stockés sur une autre station de travail.
  Disponible uniquement en combinaison avec le module de base de SafeGuard Advanced Security.

Destination :
Cliquez sur le bouton [Parcourir]. Sélectionnez le fichier journal ou, dans le cas de RemoteLog, la station de travail devant servir à consigner les événements.

Le nombre de destinations possibles est illimité.

29.4.3 Suppression des destinations

Si une destination n'est plus requise, vous pouvez la supprimer de la liste. Choisissez la commande Supprimer et confirmez votre choix à la demande du système.

> ***REMARQUE :***
> Vous pouvez supprimer les destinations qui restent utilisées ! Pour éviter tout problème, un avertissement s'affiche.
>
> Dès qu'une destination est supprimée, tous les événements qui y sont liés sont « désactivés ».

29.4.4 Copie de destinations

Les destinations sont copiées entre différents OSG

- via les commandes copier/coller dans le menu contextuel Auditing
- avec la fonctionnalité glisser-déposer.

Toutes les destinations existantes sont écrasées.

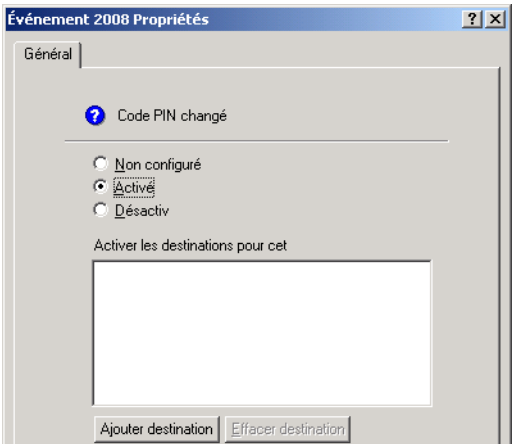
29.5 Sélection d'événements

Chaque produit de la famille SafeGuard comprend, sous SafeGuard Auditing, divers répertoires contenant les événements prédéfinis pour chacun des produits installés.

Voici comment configurer les événements et les affecter à des destinations définies :

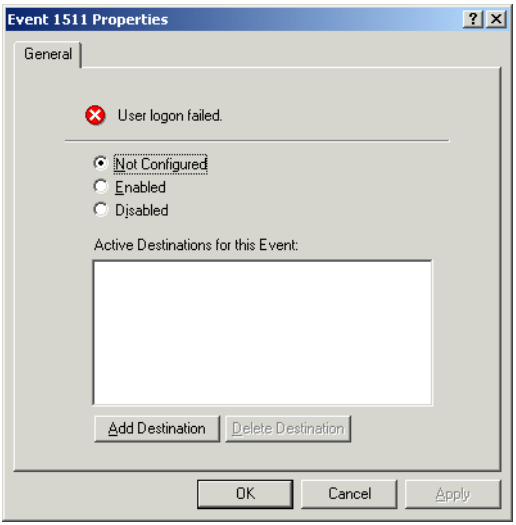
1. Cliquez sur un des répertoires de l'arborescence sous Auditing.

2. Différentes colonnes apparaissent dans la partie droite de l'écran. Cliquez sur un en-tête de colonne pour trier les événements en fonction de ce dernier.
   Vous pouvez trier les données en fonction de la catégorie, du type, de l'événement, du statut ou de la destination.



3. Double-cliquez dans le champ de droite sur un événement ou sélectionnez-le sous Propriétés dans son menu contextuel.

4. Dans cette boîte de dialogue, vous déterminez le statut et la destination.



Statut

- Non configuré (par défaut) : L'événement est désactivé et non consigné.

  AVERTISSEMENT :
  Les destinations définies ont priorité sur ces paramètres. S'il existe une destination, ce paramètre est invalide.

- Activé : L'événement est enregistré dans une ou plusieurs destinations.

- Désactivé : L'événement est invalidé et n'est pas enregistré.

Activer les destinations pour cet événement

- [Ajouter] ouvre une boîte de dialogue dans laquelle sont affichés toutes les destinations enregistrées. Sélectionnez au moins l'une de ces destinations. Lorsque vous cliquez sur OK, les destinations s'affichent dans le champ *Destinations actives pour l'événement*.

- [Supprimer] supprime toutes les destinations actives.

5. Cliquez sur [Appliquer], puis sur [OK].

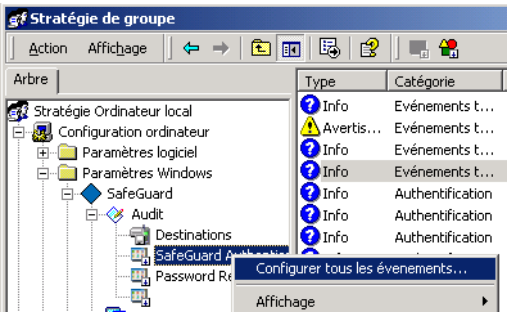
Sélection multiple

La sélection de plusieurs événements/destinations est aussi possible. Appuyez sur les touches [Ctrl] et [Maj] en même temps. Vous pouvez ensuite sélectionner plusieurs événements en un simple clic. Cliquez avec le bouton droit de la souris sur les événements sélectionnés pour l'ouvrir. Vous pouvez ensuite procéder à la configuration. Un clic sur [OK] applique les paramètres définis à tous les événements sélectionnés.

29.5.1 Configuration de tous les événements

La commande **Configurer tous les événements** permet de configurer en une étape les événements possédant des paramètres identiques.

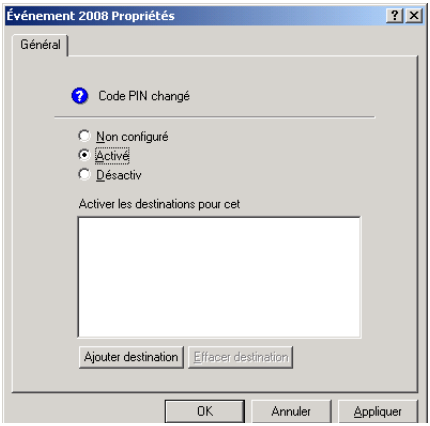
Cliquez sur le répertoire Auditing ou sur un sous-répertoire. Dans le menu contextuel, sélectionnez la commande « Configurer tous les événements ».



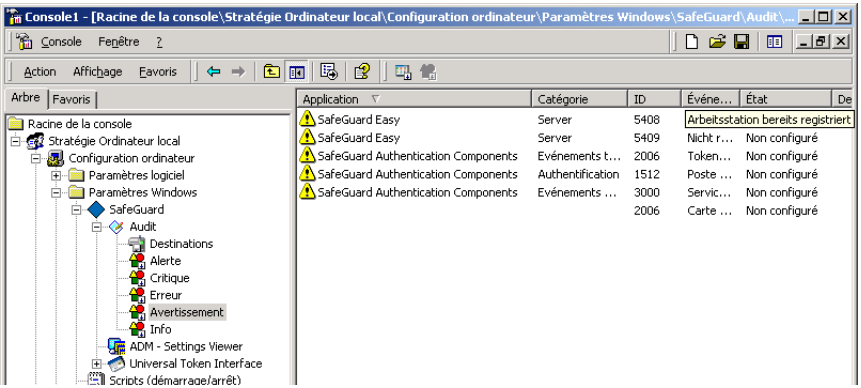
Dans la boîte de dialogue, déterminez le statut et les destinations actives. Cliquez sur [Appliquer].

29.5.2 Changement d'affichage

Dans la configuration de base, les événements sont affichés et classés par applications SafeGuard.



Via le mécanisme de filtrage, il est possible d'afficher tous les événements triés par niveau d'avertissement, indépendamment de l'application les ayant activés (par exemple, tous les événements critiques).



Vous changez d'affichage en cliquant sur les icônes et .

29.6 Visualisation des événements audités

les événements audités peuvent être visualisés dans l'observateur d'événements ou dans le fichier journal.

Les événements audités affichent les paramètres suivants :

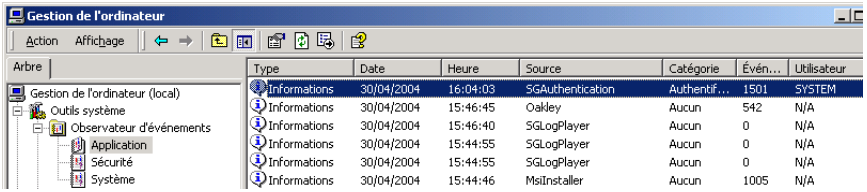
- Ordinateur : nom de l'ordinateur sur lequel l'événement audité s'est produit.
- Date : date système à laquelle l'événement a été créé.
- Heure : heure système à laquelle l'événement a été créé.
- Utilisateur : utilisateur connecté au moment de l'événement.
- Type : classification de l'événement par Windows, par ex. avertissement, erreur.
- ID événement : numéro d'identification de l'événement. Il peut s'agir de tout numéro compris entre 0 et 0xffffffff (par ex. 4 294 967 295.)
- Source : Application enregistrant l'événement, par ex. SGPWC = restrictions du mot de passe.
- Catégorie : classification de l'événement par la source.

Les événements sont toujours affichés dans la langue système définie.

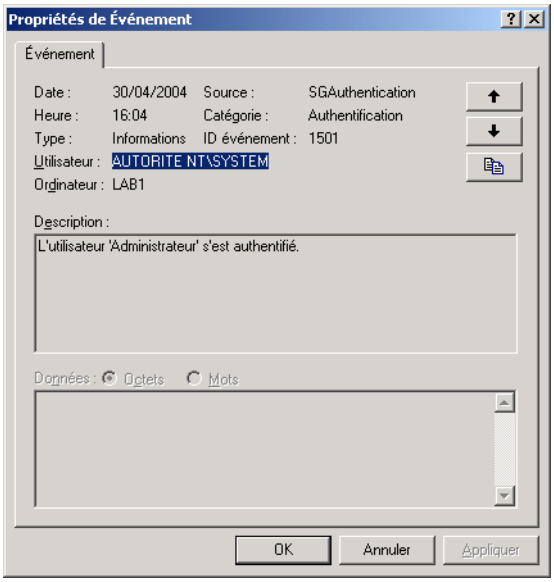
29.6.1 Observateur d'événements

SafeGuard Auditing affiche les événements audités dans le journal applications de l'Observateur d'événements de Windows.

Pour ouvrir l'observateur d'événements, cliquez sous Windows sur Démarrer, pointez sur Programmes, pointez sur Outils d'administration, puis cliquez sur Observateur d'événements. Dans l'arborescence de la console, cliquez sur le journal Application. Les événements s'affichent dans la fenêtre des détails. Un clic sur le journal des applications affiche ensuite les événements audités dans la liste détaillée.



Double-cliquez sur un événement de la liste pour en afficher le détail.



REMARQUE :
Avec le journal distant, les données de la station de travail auditant les événements sont toujours entrées dans l'observateur d'événements, dans les champs Nom d'ordinateur, Heure et Date. Les données de l'ordinateur qui active un événement apparaissent dans le champ Description.

L'observateur d'événements de Windows n'affiche pas tous les niveaux d'avertissement de SafeGuard Auditing. Pour cette raison, les différents niveaux d'avertissements sont affichés comme suit dans l'observateur d'événements :

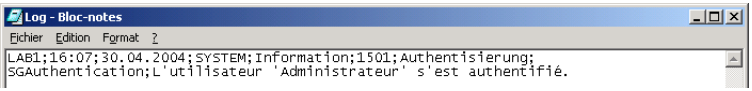
SafeGuard Auditing	**Observateur d'événements**
Urgence Alarme Erreur Critique	Erreur
Avertissement	Avertissement
Notification	Notification
Information	Information

29.6.2 Fichier journal [LogFile]

Le fichier journal de SafeGuard Auditing est le pendant du fichier journal de Windows. Il ne contient toutefois que les événements déclenchés par un produit Utimaco . Vous pouvez exporter les données d'audit et également les convertir et les analyser dans un programme de base de données.

> ***REMARQUE :***
> Pour l'enregistrement des événements, veuillez ne pas utiliser de fichiers codés EFS ou se trouvant dans un répertoire codé EFS.

L'entrée dans un fichier journal peut avoir par exemple l'aspect suivant :



Les différentes entrées ont la signification suivante :

Lab1	Nom de l'ordinateur
20:00	Time
03.05.2004	Date
Système	Spécifie un utilisateur ou un groupe ayant créé cet événement.
Information	Warning level
1511	ID de l'événement.
Authentification	Catégorie.
SGAuthentication	Source
L'utilisateur 'Administrateur' s'est authentifié.	description de l'événement

29.7 Remarques

- Si un fichier journal doit être enregistré sur un support externe, comme par ex. un disque amovible, un message d'erreur est affiché dans l'observateur d'événements en cas de dépassement de la mémoire du disque.

  Nous déconseillons de consigner les événements sur un support externe.

- Les événements ne pouvant pas être écrits dans un fichier journal sont entrés comme erreurs dans l'observateur d'événements.

- Si plusieurs stations de travail écrivent dans un fichier journal défini (par ex. un fichier sur lecteur réseau partagé), des recoupements peuvent se produire, le cas échéant, en cas d'accès simultané des différents ordinateurs. Pour éviter dans ce cas la perte de données, SafeGuard Auditing offre la solution suivante : dès que le fichier journal défini est inaccessible, parce qu'utilisé momentanément par une autre station de travail, SafeGuard Auditing crée de nouveaux fichiers.

  Les nouveaux fichiers journaux sont créés comme suit :
  L'accès est refusé au fichier journal Sglog.txt défini par défaut .
  SafeGuard Auditing crée le fichier de remplacement Sglog.txt
  L'accès est refusé aux fichiers journaux Sglog.txt et Sglog.txt.1.
  SafeGuard Auditing crée le fichier de remplacement Sglog.txt
  etc.

  999 fichiers au maximum peuvent être créés. Quand ce nombre est dépassé, les événements sont automatiquement écrits dans l'observateur d'événements. Cette méthode est également utilisée quand le fichier journal est en lecture seule ou si sa taille excède 2 Go.

  Nous recommandons de procéder à la consignation à distance lorsque cette dernière porte sur plusieurs stations de travail.

- **SNMP Traps**
  Au cas où, sur une machine client, un événement devant être signalé à l'administrateur se produit, vous avez la possibilité de créer des SNMP Traps à partir de SafeGuard Auditing.

  Une description de solution Utimaco indique comment utiliser SNMP et Auditing.

  Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco **http://www.utimaco.com/myutimaco**.

  Dans la zone de recherche (« Search »), tapez « SNMP".

30 Administration centrale

Pour compléter les mécanismes d'administration connus, il existe à présent une application spécifique qui remplit des tâches centrales. Elle administre tous les clients installés dans un réseau d'entreprise et se charge également de la distribution sécurisée et centrale d'éventuelles mises à jour de configuration à des groupes de clients, de l'affichage de leur état actuel et sert d'archive centrale pour les sauvegardes du noyau système. Les clients qui ne sont qu'occasionnellement connectés au réseau (clients hors connexion) peuvent également être intégrés dans l'administration centrale.

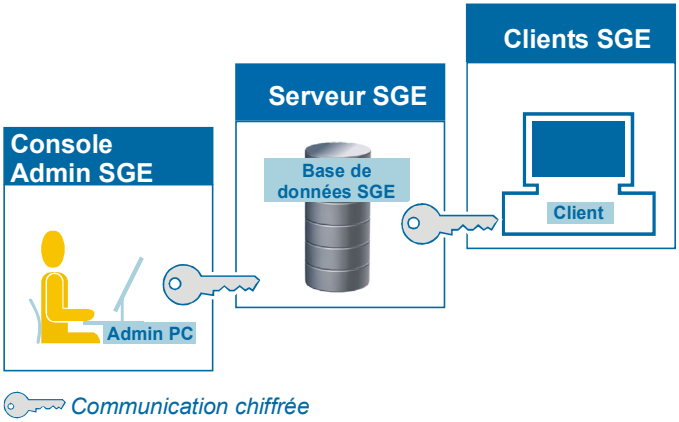
Le mécanisme d'administration des versions précédentes, qui utilisait les fichiers de configuration et des outils de distribution de logiciel d'un tiers, reste utilisable.

30.1 Mode de fonctionnement

Dans le cadre de l'administration centrale, des ordinateurs clients SafeGuard Easy sont administrés depuis un poste central via la console d'administration. La console d'administration gère une base de données centrale qui contient les paramètres de configuration des clients SafeGuard Easy. Des données supplémentaires comme par ex. des modifications souhaitées de paramètres de configuration sont en outre enregistrées également dans la base de données.

L'administration centrale de SafeGuard Easy requiert les composants suivants :

- le serveur SafeGuard Easy (appelé ci-après serveur SGE) avec la base de données SafeGuard Easy.
- la console d'administration SafeGuard Easy qui contrôle la base de données sur le serveur (console d'administration SGE)
- les ordinateurs clients SafeGuard Easy (clients SGE)



La base de données SGE centrale rassemble diverses informations sur les clients SGE. L'administrateur SGE utilise la console d'administration pour gérer les contenus de la base de données et pour générer des souhaits de modification sous forme de « requêtes ».
Les clients SafeGuard Easy ont recours à un agent réseau pour charger les modifications de la configuration de la base de données, par l'intermédiaire du serveur, et reporter les modifications réussies sur le serveur. Si la modification est réussie, le serveur stocke les nouveaux paramètres de configuration dans la base de données. La communication avec le serveur SGE est réalisée par le processus serveur SGE qui utilise une interface ODBC garantissant la plus grande flexibilité possible dans le choix du type de base de données.

30.1.1 Serveur SGE/ Base de données SGE

Le serveur SGE est le point de stockage central de tous les clients, car c'est ici que sont enregistrés les paramètres de tous les clients SGE dans une base de données. SafeGuard Easy peut prendre en charge n'importe quel type de base de données employant l'interface ODBC. Dans la configuration de base, SafeGuard Easy utilise Microsoft Access.

La base de données SGE sur le serveur SGE contient les informations suivantes sur les clients SGE :

- paramètres SGE actuels (sans mots de passe, ni clés)
- nom du réseau

Ces informations peuvent être consultées sur la console d'administration SGE.

Sur le serveur est également créé le répertoire Backups dans lequel chaque poste de travail enregistré sur le serveur crée automatiquement une sauvegarde de noyau système, mise à jour à chaque changement de configuration. Cette sauvegarde est mise à jour après toutes les modifications de configuration.

REMARQUE :
Si vous prévoyez d'utiliser SafeGuard Easy conjointement à une administration basée sur serveur dans une nouvelle installation, vous préférerez peut-être déployer le produit Utimaco de dernière génération, SafeGuard Enterprise. SafeGuard Enterprise fournit des options de gestion améliorées, notamment l'intégration d'Active Directory, la distribution de stratégies via le Web ainsi que la prise en charge de Windows Vista. Pour de plus amples informations, contactez votre partenaire commercial SafeGuard Easy.

REMARQUE :
Dans le réseau, et pour des raisons techniques et d'organisation, il peut y avoir naturellement plusieurs serveurs SGE auquel peuvent être affectés les clients SafeGuard Easy. Dans la version 4.0, SafeGuard Easy **ne prend en charge aucun mécanisme de synchronisation entre les serveurs**. Cette fonctionnalité est fournie dans certaines circonstances par une base de données avec mécanismes de réplication.

30.1.2 Console d'administration SGE

La console d'administration est un programme qui accède à la base de données du serveur et qui lance par ex. la distribution centrale des fichiers de configuration. L'accès à la console d'administration est réservé à des utilisateurs privilégiés.

Tâches types de la console d'administration :

- interrogation des paramètres des clients SGE et détermination de leur état (Hors connexion, Standard, Push).
- regroupements de clients SGE pour simplifier l'administration
- génération de nouvelles configurations distribuées aux clients SGE
- surveillance du traitement correct des fichiers de configuration distribués

La console d'administration ne doit pas nécessairement fonctionner sur la même machine que le serveur SGE Il suffit de connaître le nom de l'ordinateur serveur SGE et une connexion réseau doit être présente.

Pour garantir la cohérence des données, **une seule connexion administrative simultanée** est possible. La tentative d'établir plusieurs connexions est vouée à l'échec.

30.1.3 Clients SafeGuard Easy

Les clients sont en mesure d'établir une liaison avec le serveur SGE quand un agent de réseau est installé (option « Liaison serveur). La liaison entre le serveur SGE et le client SGE est établie à l'aide d'un agent de réseau et par le nom UNC NETBIOS du serveur SGE qui sont fournis aux clients au moment de l'installation.

Au premier enregistrement, le client SGE transmet au serveur SGE

- ses paramètres de configuration SGE
- le GUID
- sa clé publique
- son nom de réseau

En outre, lors du premier enregistrement, la clé publique est également échangée avec le serveur.

Quand un autre contact est ensuite établi avec le serveur, le client SGE demande une mise à jour des paramètres qui le concernent. En règle générale, les clients SGE essaient d'établir une liaison avec le serveur SGE à chaque démarrage de l'ordinateur. Pendant cette phase, toutes les modifications stockées de manière centralisée sur le serveur SGE sont collectées et exécutées sur le client.

Les modifications exécutées localement sur le client SGE (quand l'administrateur procède par ex. à une configuration locale) sont immédiatement signalées par le client au serveur afin que la base de données reste à jour. En cas de désinstallation, le client en informe le serveur qui supprime alors l'entrée du client concerné de la base de données.

30.1.4 Combinaisons SGE client/SGE serveurs prises en charge

Les versions SGE Client et SGE Server peuvent être systématiquement combinées. Par exemple, SafeGuard Easy Server v4.50 fonctionne avec SafeGuard Easy Clients, v4.40, sans aucun problème, et inversement.

Pour les clients SGE < v4.11, toutefois, il existe les restrictions suivantes en matière de fonctionnalité :

- pas de changement de l'état client après mise OFFLINE
- pas de nouvel enregistrement d'un client
- L'enregistrement d'autres versions de SafeGuard Easy Clients sur un autre serveur SafeGuard Easy Server est impossible.

30.2 Échange de données entre client et serveur

Dans la version actuelle de SafeGuard Easy, les informations SafeGuard Easy sensibles ne sont plus simplement transférées à l'aide des fichiers de configuration, mais également échangées en ligne entre SafeGuard Easy Server et SafeGuard Easy Client. Cette connexion doit être protégée et configurée.

30.2.1 Communication sécurisée

Pour protéger de façon appropriée les informations Safeguard Easy , le transfert des données est chiffré. Le chiffrement de la connexion n'est toutefois utile qu'une fois que chaque client s'est authentifié sur le serveur SGE pour l'échange d'informations, et inversement.

> ***REMARQUE :***
> Client et serveur communiquent par le biais du service RPC/DCOM de Microsoft. Vous pouvez déterminer librement via quel port ou quel protocole la communication doit être établie.
> Si vous utilisez un programme de pare-feu, les ports via lesquels le client et le serveur communiquent doivent être débloqués. Pour plus de détails sur RPC/DCOM, consultez la documentation Microsoft correspondante.

Authentification client / serveur

Pour l'authentification mutuelle, SafeGuard Easy utilise un chiffrement sûr de type clé publique/clé privée. Pour générer une paire de clés, la procédure RSA est utilisée, avec une longueur de clé de 1 024 bits.
La communication entre la version Client et Server est protégée par le protocole Interlock.

Quand il n'existe pas encore de paire de clés RSA, elle est générée sur le client et sur le serveur au moment de l'installation du logiciel SafeGuard Easy. Une fois les touches de la paire générées, ces dernières sont stockées, sans modification, sur l'ordinateur.

Lorsque le serveur et le client entrent en contact, ils échangent des clés publiques et s'authentifient mutuellement pour la première fois. Le client et le serveur enregistrent la clé publique et se « reconnaissent » ensuite de façon automatique. Ainsi lorsque le client et le client communiquent à nouveau, ils ont recours à la clé publique échangée pour vérifier la clé privée de leur correspondant et vérifier son identité.

En option, la création de la paire de clés peut également être prise en charge par un module TPM (Trusted Platform Module), comme la puce Lenovo ESS. Ceci garantit une sécurité matérielle supplémentaire pour la mémoire de clés, mais fonctionne moins rapidement que la solution logicielle.

Chiffrement des données pendant le transfert

Toutes les informations SafeGuard Easy transmises depuis ou vers le serveur SGE sont chiffrées. Une fois l'authentification mutuelle effectuée, une clé de session symétrique aléatoire est créée, échangée et utilisée pour le transfert de données chiffré au moment de la communication.

Une nouvelle clé de session est créée pour chaque nouvelle connexion entre le client SGE et le serveur SGE. La procédure est identique pour la communication entre la console d'administration SGE et le serveur SGE.

Pour le chiffrement on utilise RC4 avec une clé de session 128 bits. La clé de session peut être créée par le client ou par le serveur et est chiffrée avec la clé publique du destinataire avant d'être envoyée.

30.2.2 Charge de réseau à attendre

Le montant de données généré lorsque le client SafeGuard Easy vérifie les mises à jour de configuration lors de son démarrage est seulement légèrement différent par rapport au montant de données généré lorsque ce client recherche les mises à jour de configuration à l'issue d'une période définie, et s'appuie sur les modifications éventuelles et leur nature. Dans les deux cas, des données d'une taille approximative de 2 k-octets sont échangées. La taille exacte dépend un peu du nombre de modifications.

Si vous utilisez déjà des fichiers de configuration pour l'installation/la configuration de SafeGuard Easy, leur taille vous donne une idée approximative de la quantité de données.

En raison de la configurabilité de l'intervalle d'échange de données décrite au point 'Capacité maximale de la base de données SafeGuard Easy', l'administration centrale SafeGuard Easy ne contribue, du point de vue d'Utimaco, que de façon insignifiante à une charge de réseau plus élevée.

30.2.3 Définition de l'intervalle d'échange des données

En règle générale, un ordinateur client demande régulièrement au serveur si des modifications doivent être exécutées lors du démarrage. D'autres demandes ont lieu à des intervalles déterminés. **La valeur par défaut** pour d'autres demandes de mise à jour est de **6 heures**.

Cet intervalle peut être adapté de façon centrale avec des mécanismes Windows standard, car il s'agit d'une entrée dans le registre. Pour modifier l'intervalle, modifiez également la clé de registre [DWORD] :

HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy

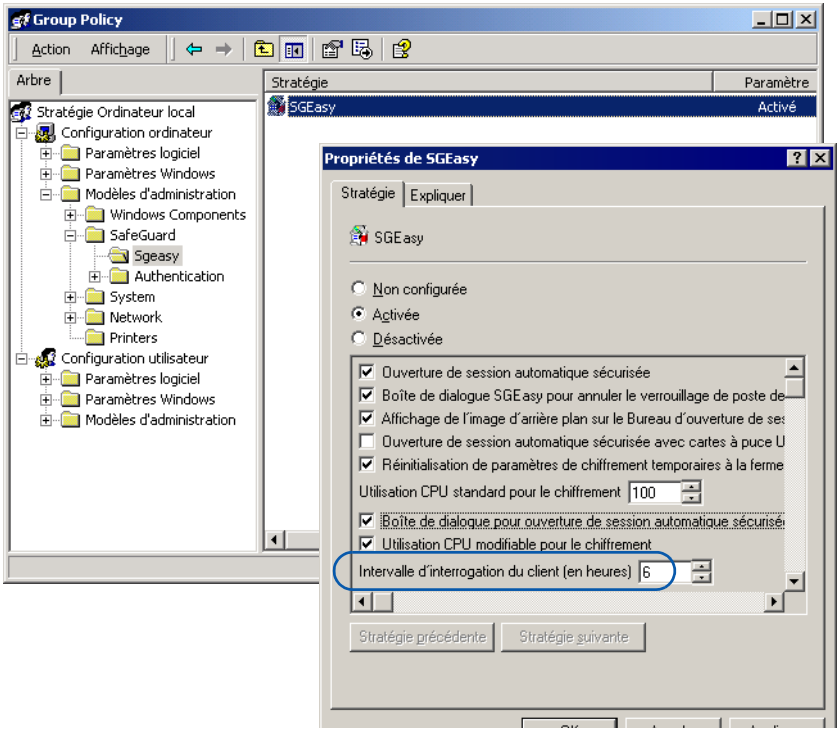
"**NotifyPeriod**"=<Intervalle>

Quand la clé est présente, les clients envoient des requêtes aux intervalles spécifiés. Vous pouvez spécifier des valeurs entre 1 et X heures.

L'intervalle peut également être désactivé via une stratégie dans le modèle d'administration Utimaco. La stratégie se trouve sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\SGEasy

A la page des propriétés de « SGEasy », il suffit d'entrer la valeur souhaitée sous « Intervalle d'interrogation du serveur (en heures) ».



30.3 Pour une installation

Remarque sur SP2 de Windows XP/SP1 de Windows 2003 Server 1
Quand on utilise le serveur d'administration centrale en option ou l'administration à distance de SGE 4.x, des paramètres de configuration particulier doivent être définis sur SP2 de Windows XP/SP1 de Windows 2003 Server.

Vous trouverez une description des paramètres requis dans notre base de connaissance **http://www.utimaco.com/myutimaco** sous la rubrique **« 106898 SafeGuard Easy and SP2 Configuration for Windows XP »** (106898 SafeGuard Easy et SP2. Configuration pour Windows XP). Dans la zone de recherche (« Search »), recherchez « 106898 ».

Le répertoire \Tools du CD contient également un outil permettant de définir de façon automatique les propriétés nécessaires pour procéder à l'administration centrale ou distante.

Conditions

- **Microsoft High Encryption Package**
  La condition pour l'administration centrale est la prise en charge le chiffrement avec des clés de 128 bits par les systèmes d'exploitation du client, du serveur et de l'ordinateur faisant fonction de console d'administration. A cet effet, le « **High Encryption Package** » de Microsoft doit être partout installé. Vous pourrez définir si ceci doit être installé avec Internet Explorer (Aide/À propos d'Internet Explorer/Degré de cryptage).

  Le High Encryption Package est installé en standard dans Windows XP et à partir du Service Pack 2 dans Windows 2000 (ou toute version plus récente).

- **Ports**
  Client et serveur communiquent par le biais du service RPC/DCOM de Microsoft. Vous pouvez déterminer librement via quel port ou quel protocole la communication doit être établie.
  Si vous utilisez un programme de pare feu, les ports via lesquels le client et le serveur communiquent doivent être débloqués.

Pour plus de détails sur RPC/DCOM, consultez la documentation Microsoft correspondante.

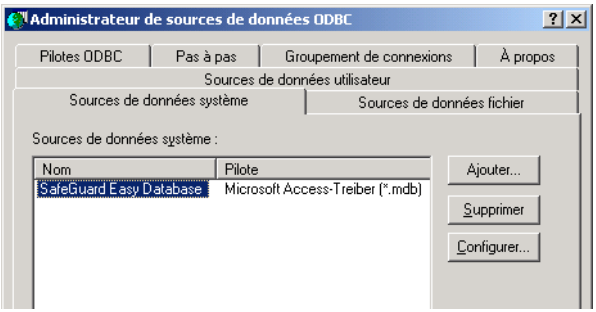
30.3.1 Installation du serveur/base de données SafeGuard Easy

L'ordinateur qui contient la base de données SGE est le « coeur » de l'administration centrale et doit être configuré en premier ou le nom de l'ordinateur doit au moins être connu pour être transmis aux clients SGE.

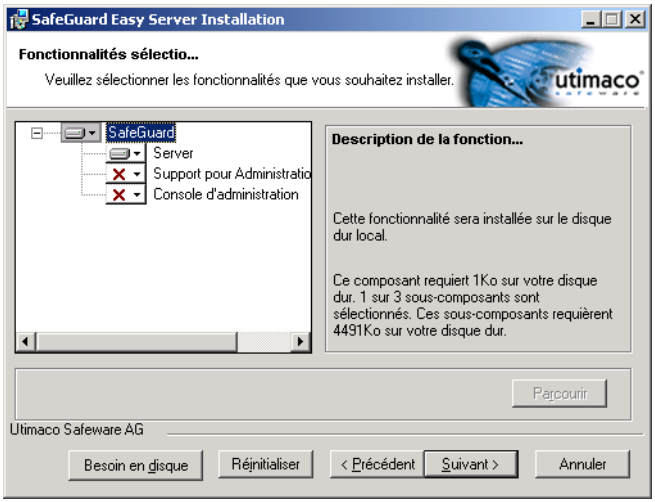
Il est déconseillé de modifier le nom du poste de travail du serveur SGE après enregistrement du client. Cela signifie que la communication entre les clients et le serveur est interrompue et qu'un échange de données n'a plus lieu !

Le serveur SGE peut se trouver sur un serveur réseau physique ou sur n'importe quel poste de travail connecté au réseau. La connexion d'un client à la base de données centrale de SafeGuard Easy Database ne peut s'établir que si un protocole réseau adapté est installé sur toutes les stations de travail et est actif.

Lorsque vous installez le composant serveur, aucune autre application n'est installée. Par contre, une base de données Microsoft Access (Sgeasy.mdb) est simplement générée dans le dossier d'installation de SafeGuard Easy du serveur (voir Paramètres/Panneau de configuration/ Outils d'administration/Sources de données (ODBC)). Cette base de données est protégée par un mot de passe.



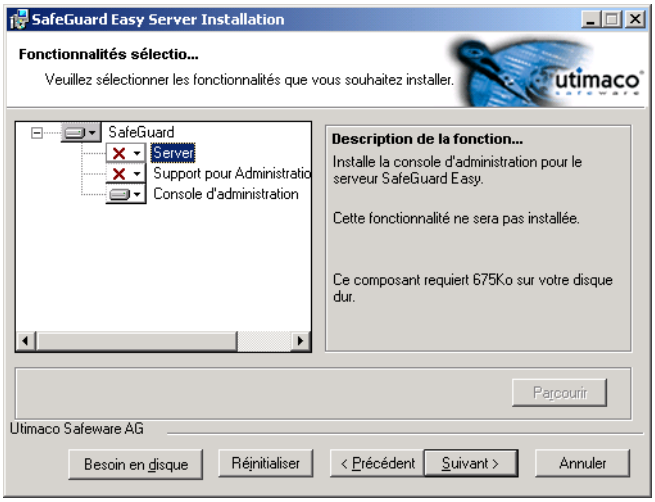
Installez le serveur SGE en appelant `Server.msi` à partir du répertoire du CD **...\Server**. Dans le cadre d'une installation « 'personnalisée », sélectionnez l'option « Serveur ». Dès que vous en avez terminé, le système doit être redémarré.



30.3.2 Installation de la console d'administration SafeGuard Easy

De manière générale, il est déconseillé de procéder à l'installation et à la configuration directement sur le serveur. Par conséquent, la base de données doit être administrée à partir d'une station de travail d'administration. Vous pouvez faire de n'importe quel poste de travail un poste de travail d'administration

Installez la console d'administration en appelant `Server.msi` du répertoire du CD ...\Server. Dans le cadre d'une installation « personnalisée », sélectionnez l'option « Console d'administration » et poursuivez l'installation.



Dès que vous en avez terminé, le système doit être redémarré.

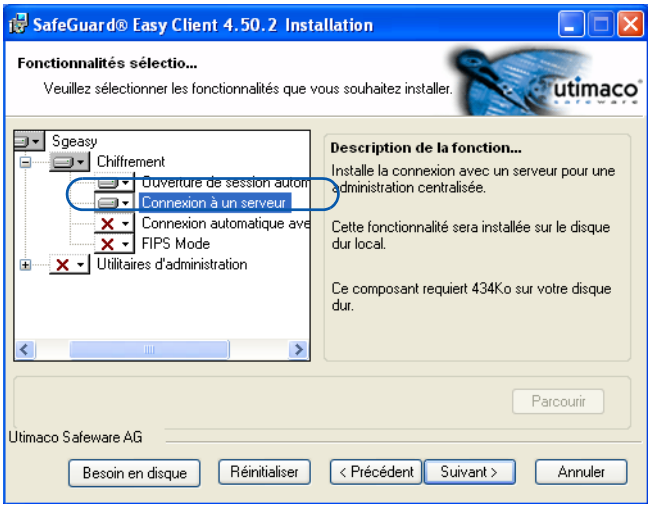
Après un redémarrage, vous trouvez les entrées Console d'administration et Assistant de configuration pour le déploiement sous Programmes / Utimaco / SafeGuard Easy.

30.3.3 Installation des clients SafeGuard Easy

La procédure d'installation fonctionne de façon habituelle (cf. installation locale ou centrale). Pour la communication avec le serveur, le nom UNC NETBIOS du serveur SGE et l' « agent de réseau » permettant la communication avec le serveur doivent cependant être fournis aux clients.

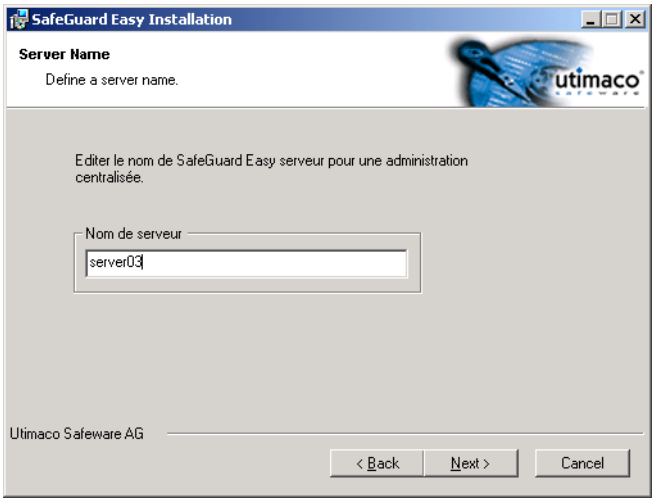
L'agent de réseau ne peut plus être fourni après l'installation de SafeGuard Easy ! Si un client doit être administré de façon centralisée, SafeGuard Easy doit être réinstallé avec agent de réseau activé.

Démarrez l'installation en appelant `Sgeasy.msi` du répertoire de CD ...\Client (installation interactive). Dans le cadre d'une installation « personnalisée », sélectionnez l'option « Liaison serveur » en plus des composants déjà sélectionnés.



Plus loin dans la procédure d'installation, entrez le UNC Netbios nom du serveur SGE (par ex. « server03 ») dans la boîte de dialogue *Serveur*.

Pour l'administration des clients hors ligne, ces clients reçoivent un nom de serveur spécial : « OFFLINE », qui active un autre mécanisme de communication. Pour plus de détails concernant les clients hors connexion, voir 'État « Hors connexion »'.



Poursuivez l'installation comme décrit au point « Installation locale ». Dès que vous en avez terminé, le système doit être redémarré.

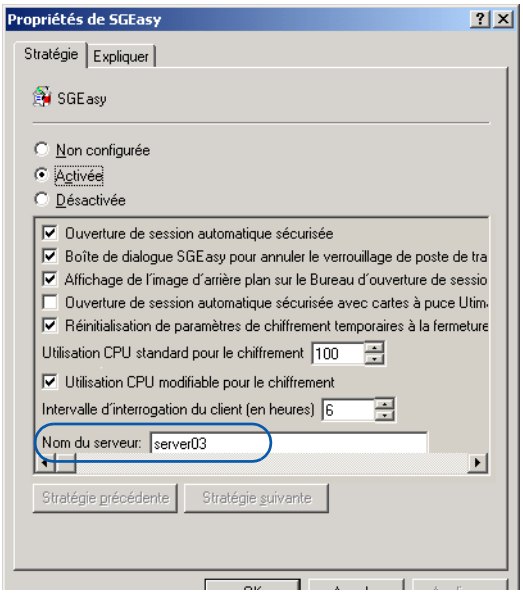
AVERTISSEMENT :
Si le nom du client SGE est modifié après l'installation SGE, le serveur ne « reconnaît » plus le client. L'entrée du client SGE doit dans ce cas être supprimée de la base de données et SGE doit être réinstallé sur le client. Après la nouvelle installation, le client s'enregistre avec un nouveau nom.

Mise en place d'un client SafeGuard Easy avec le nom de serveur SafeGuard Easy après l'installation

Si vous ne connaissez pas le nom de serveur, vous ne pouvez laisser le champ Server Name (Nom serveur) vide pour l'instant. Le nom de serveur peut être ajouté de façon centrale sur le client, à l'aide des mécanismes Windows standard, dans la mesure où il s'agit simplement d'une entrée « nom de serveur » dans le modèle administratif d'Utimaco.

Cette stratégie se trouve dans le modèle d'administration de SafeGuard Easy sous

Configuration ordinateur
\Modèles d'administration
\SafeGuard
\SGEasy



30.3.4 Capacité maximale de la base de données SafeGuard Easy

La base de données SafeGuard Easy est, dans ses paramètres de base, une base de données Microsoft Access. La taille d'une base de données Microsoft Access est limitée à 2 Go, mais peut être agrandie en renvoyant d'autres bases de données.

Un client SafeGuard Easy requiert après l'enregistrement environ 5 à 7 Ko de l'emplacement mémoire de la base de données. Pour 50 000 clients, ceci représente donc env. 340 à 350 Mo.

Cependant, nous recommandons de ne pas utiliser une base de données (serveur) pour administrer un nombre important de stations de travail. Vous devez alors mettre en place une structure organisationnelle et administrative dans laquelle les stations de travail sont administrées par différents serveurs.

30.3.5 Restauration de serveur/base de données SafeGuard Easy

Pour restaurer avec succès le serveur SGE, ce qui suit est essentiel :

- Sauvegardez certains fichiers se trouvant par défaut dans le répertoire de produit (C :\Programme\Utimaco\SafeGuard Easy) :
  - Sgeasy.mdb
  - WksInfo.stg
  - Pubkey.sto
- Noter le nom NetBIOS et l'adresse IP de (l'ancien) serveur SGE à fins de restauration.

Avec les fichiers sauvegardés, le NetBIOS et l'adresse IP, vous pouvez restaurer l'état du dernier niveau des fichiers à la remise en service d'un serveur SGE.

Ce faisant, veuillez noter ce qui suit :

1. Affectez au nouvel ordinateur (serveur) la même adresse IP et le même nom de NetBIOS.

2. Réinstallez ensuite le serveur SGE (server.msi).

3. Une fois l'installation terminée, *ne redémarrez pas* immédiatement l'ordinateur.

4. Copiez les trois fichiers SGE sauvegardés dans le répertoire de produit de SafeGuard Easy.

5. Redémarrez l'ordinateur.

6. Après redémarrage, ouvrez la console d'administration de SGE. Les entrées des clients SGE sont à nouveau disponibles.

30.4 Prise en charge Microsoft SQL Server

Pour l'enregistrement d'informations sur les clients SGE, SafeGuard Easy utilise comme type standard une base de données Microsoft Access. Certains utilisateurs peuvent préférer un autre type de base de données. SafeGuard Easy répond à ce souhait de certains clients et agrandit la palette des bases de données prises en charge avec Microsoft SQL Server.

Deux phases sont nécessaires pour l'installation de la prise en charge de Microsoft SQL Server :

- Il convient tout d'abord de créer une base de données SafeGuard Easy vide sur le serveur SQL.
- Cette base de données vide doit ensuite être enregistrée sur le serveur SGE.

30.4.1 Remarques importantes

- La solution Microsoft SQL Server n'est prise en charge qu'à partir de la version SafeGuard Easy 4.11.
- Microsoft SQL Server peut être installé sur la machine sur laquelle le serveur SafeGuard Easy sera ultérieurement installé. Ceci n'est toutefois pas une obligation.
- S'il est prévu d'utiliser une base de données SQL, aucun client SGE ne doit être installé ou enregistré avant que la solution der Microsoft SQL Server ait été installée comme base de données par défaut.

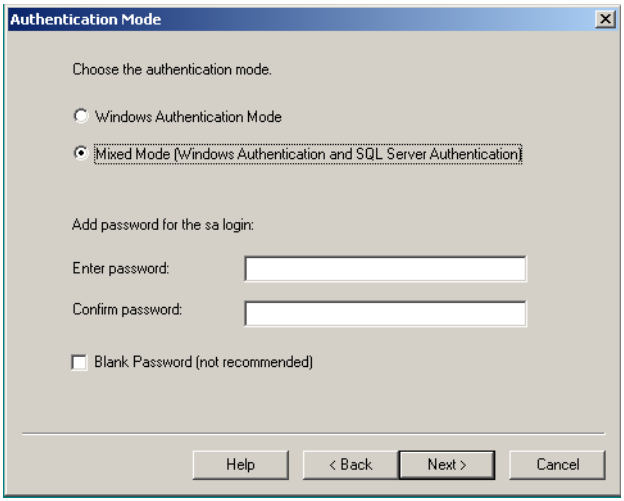
- La prise en charge par SafeGuard Easy du serveur SQL a été conçue et testée avec les versions suivantes :
  - SQL Server 2005
  - SQL Server Enterprise Edition8.00.760 (ServicePack3)
  - SQL Server Developer Edition 8.00.194 (RTM)

30.4.2 Création d'une base de données SafeGuard Easy vide sur le serveur SQL

REMARQUE :
Il est impératif d'installer le serveur AVANT SafeGuard Easy !

1. Installez le serveur SQL (si ce n'est pas déjà fait).

   A l'installation, notez ceci :
   Dans le « Mode d'authentification », choisissez l'option « Mode mixte ».



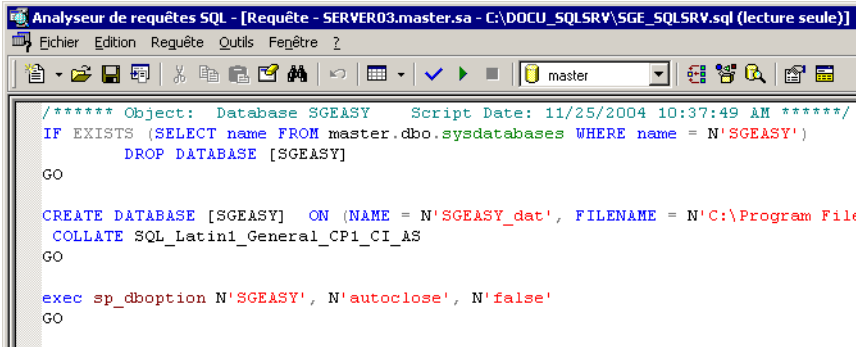
   Le mode d'authentification peut être également défini après l'installation de SQL Server.

2. Appelez Analyseur de requêtes SQL via **Programmes / Microsoft SQL Server / Analyseur de requêtes**.

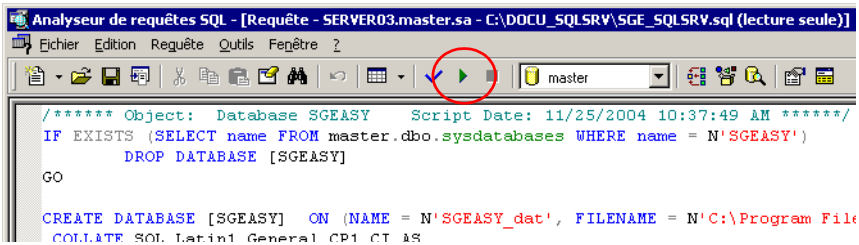
3. Ouvrez le fichier `SGE_SQLSRV.sql` de l'Analyseur de requête. (Le fichier est compressé dans l'archive `SQL-info.zip` enregistrée dans le dossier \TOOLS du CD de SafeGuard Easy).

   `SGE_SQLSRV.sql` contient le script nécessaire pour créer une base de données SGE vide sur le serveur SGE. Cette base de données est utilisée plus tard comme base de données SGE par le serveur SGE.

   Écrasez les entrées « C :\Program Files\Microsoft SQL Server » avec le répertoire d'installation du serveur SQL sur votre ordinateur (par ex. « D :\Microsoft SQL Server »).

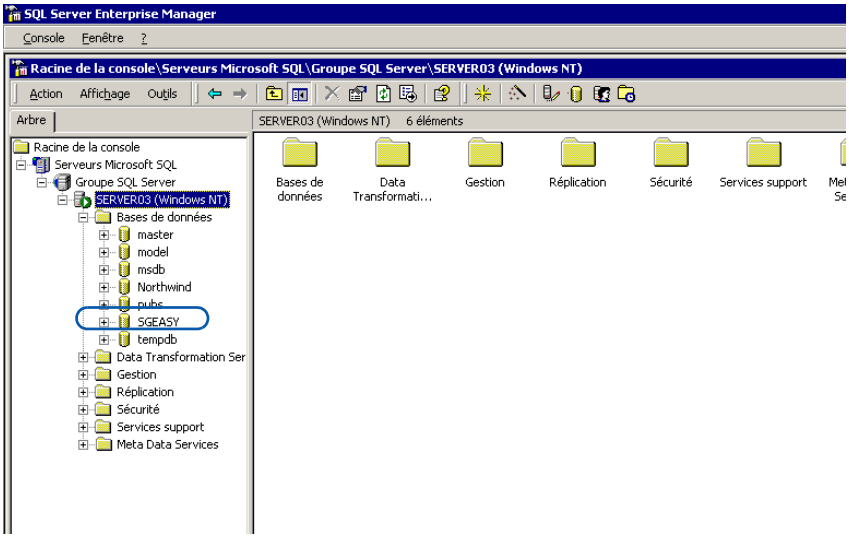


4. Exécutez le script SGE_SQLSRV.sql.

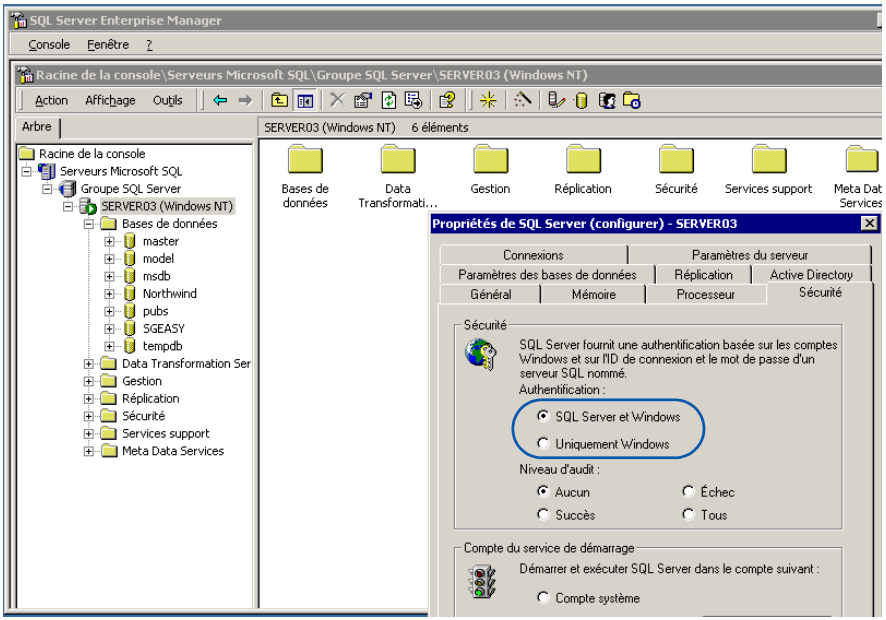


5. Après exécution du script, appelez SQL Enterprise Manager via **Programmes / Microsoft SQL Server / Enterprise Manager**.

6. Une base de données SafeGuard Easy vide appelée « SGEASY » a été créée sur votre serveur SQL.



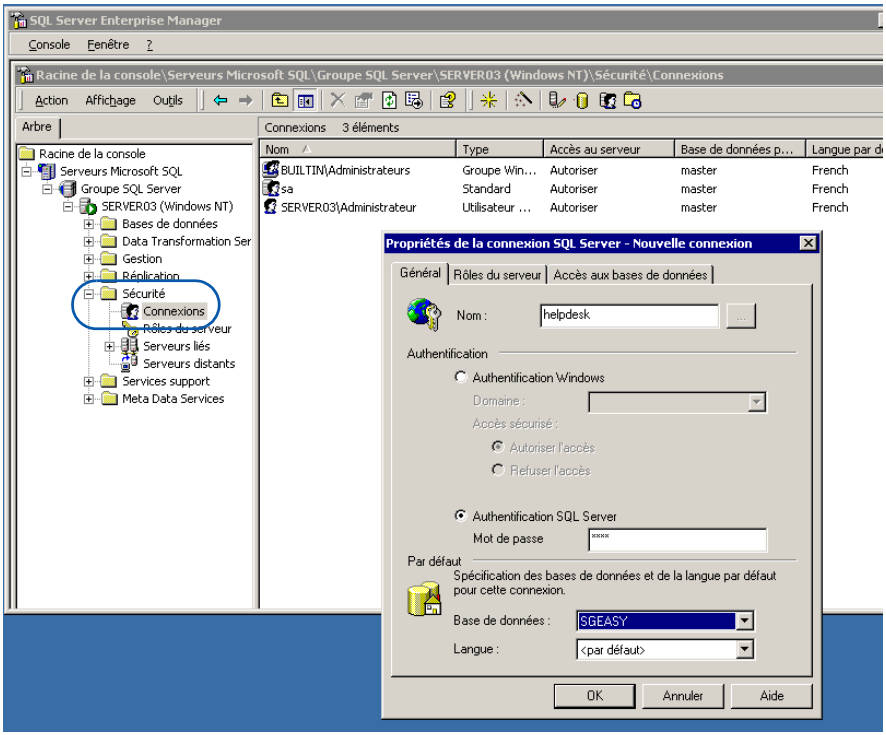
7. Si cela n'a pas été fait pendant l'installation du serveur SQL : dans la structure arborescente, sélectionnez le propre serveur SQL (dans notre exemple « Server03 (Windows NT) » et affichez la page des propriétés via le menu contextuel.



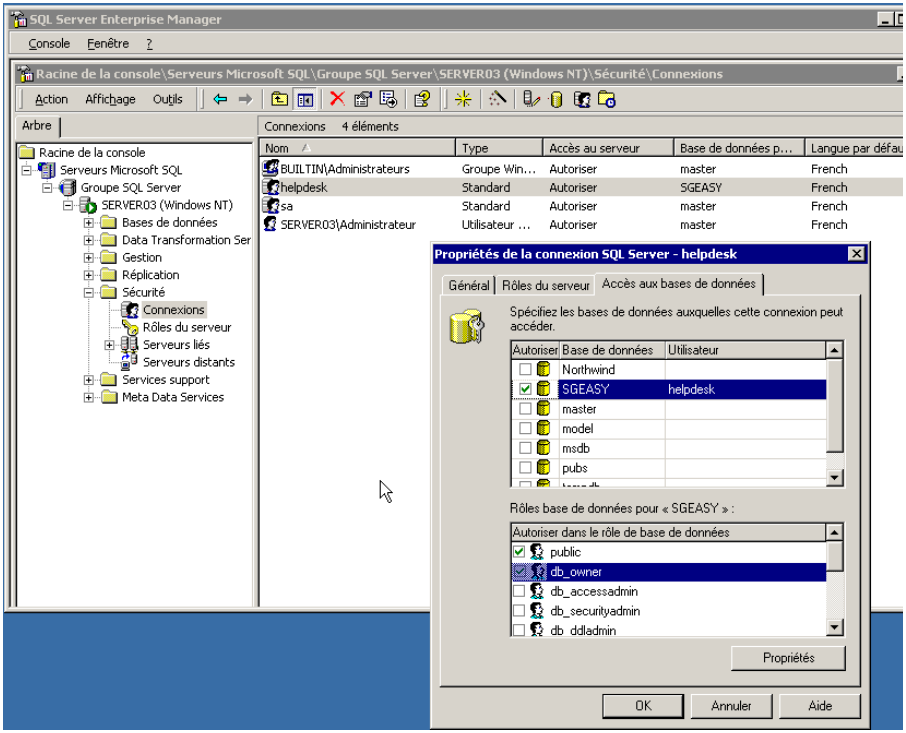
Dans l'onglet « Sécurité », définissez l'authentification sur « SQL Server et Windows".

8. Option : un autre compte système que le compte système standard (l'utilisateur « sa ») pour la base de données SGEASY est créé via Sécurité > Nom de l'utilisateur > « Nouvel utilisateur » dans le menu contextuel.

   Sous l'onglet « Général » dans la rubrique « Authentification », choisissez l'option « Authentification SQL Server »et tapez le mot de passe. Spécifiez la « base de données » SGEASY.



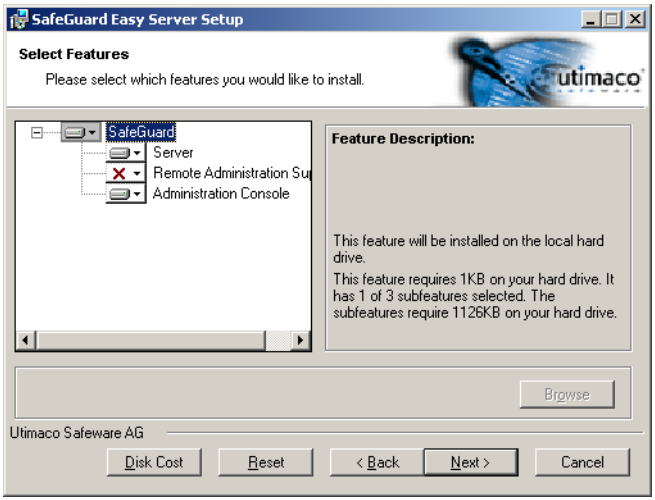
Dans la section « Accès à la base de données » sélectionnez « public » et « propriétaire » comme rôles autorisés.



30.4.3 Enregistrement de la nouvelle base de données (vide) de SafeGuard Easy sur SafeGuard Easy serveur

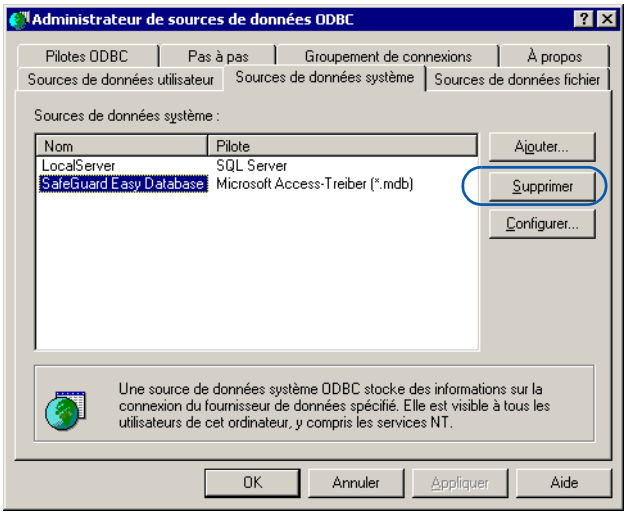
1. Installez le serveur SafeGuard Easy en appelant le fichier `Server.msi` du répertoire \SERVER sur le CD produit. En plus du serveur, vous pouvez également installer la console d'administration.

> ***AVERTISSEMENT :***
> NE PAS redémarrer l'ordinateur après l'installation !

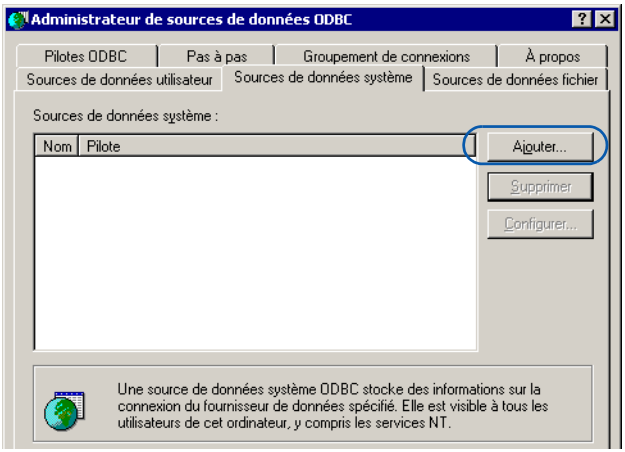


2. Appelez successivement **Paramètres / Panneau de configuration / Outils d'administration / Sources de données (ODBC)**.

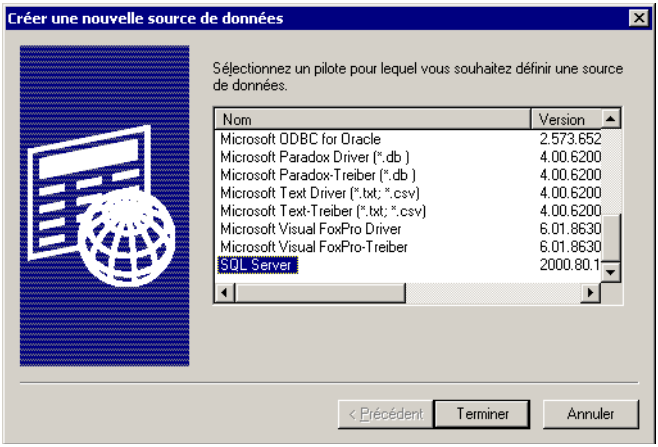
3. Ouvrez l'onglet « Sources de données système » et retirez de la liste la « base de données SafeGuard Easy » par défaut avec le pilote Microsoft Access..



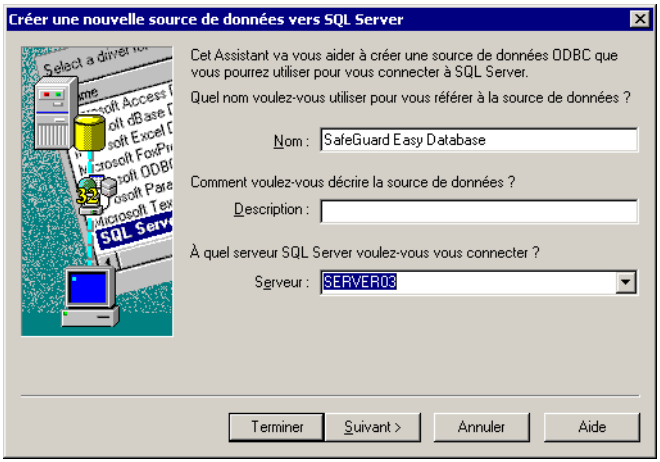
4. Créez une nouvelle source de données avec [Ajouter] sous l'onglet Sources de données système.



5. Choisissez le pilote « SQL Server ».

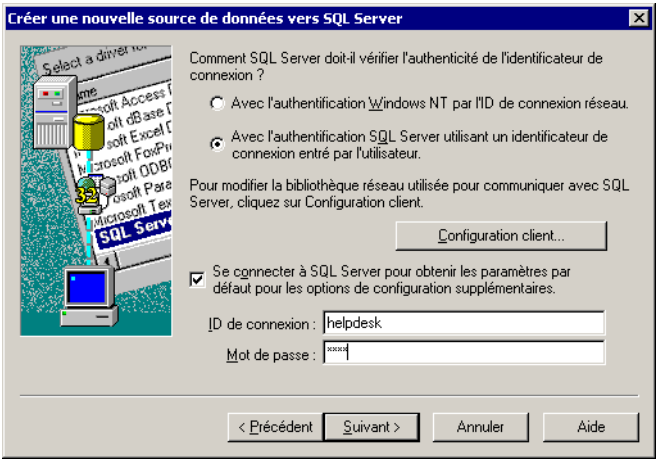


6. Établissez la liaison avec SQL Server.

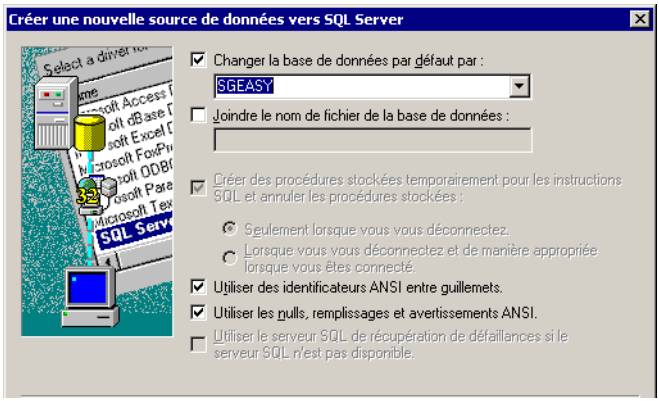


REMARQUE :
Le nom de la base de données doit impérativement être « SafeGuard Easy Database » !

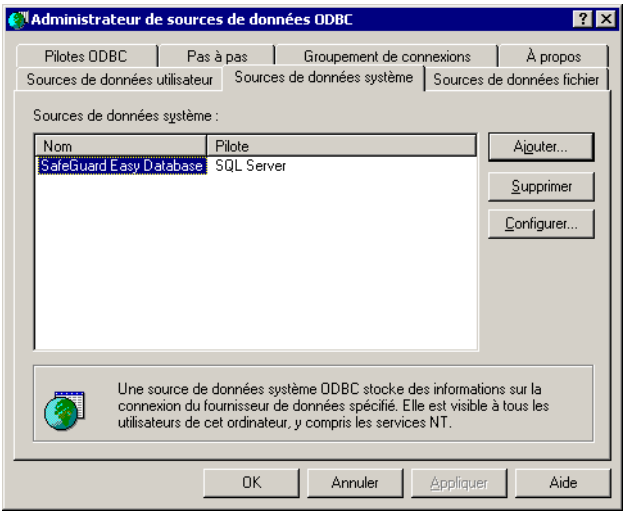
7. Sélectionnez l'option « Avec authentification de serveur SQL... » Sélectionnez l'option « Avec l'authentification SQL Server... » et choisissez un utilisateur par défaut pour la base de données SQL (normalement l'utilisateur « sa » ou, dans l'exemple, l'utilisateur « helpdesk »).



8. Choisissez la base de données « SGEASY » par défaut et conservez les autres paramètres par défaut.



9. Le « nouveau » type de base de données SafeGuard Easy est à présent la base de données SQL.

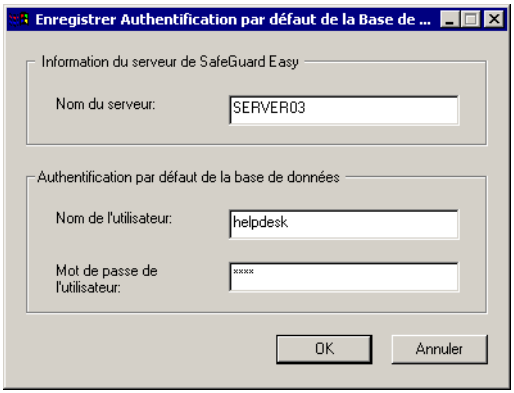


10. Redémarrez le système et terminez les services SGEasy, SgeSrv.exe et CfgDBSrv.exe (SgeSrv.exe=SafeGuard Easy serveur et CfgDBSrv.exe=SafeGuard Easy DB).

11. Les données d'accès à la base de données SGE ne sont pas transférées en texte clair. `SetDBPwd.exe` met à jour l'utilisateur par défaut et enregistre le mot de passe dans le fichier `DBPwd.stg` chiffré, afin qu'il puisse être utilisé par le serveur SGE.

REMARQUE :
Quand un utilisateur de base par défaut ouvre une session SANS mot de passe, les étapes 10 et 11 ne sont pas nécessaires !

Exécutez depuis le répertoire d'installation SGE Server, le fichier `SetDBPwd.exe` et entrez les données demandées.



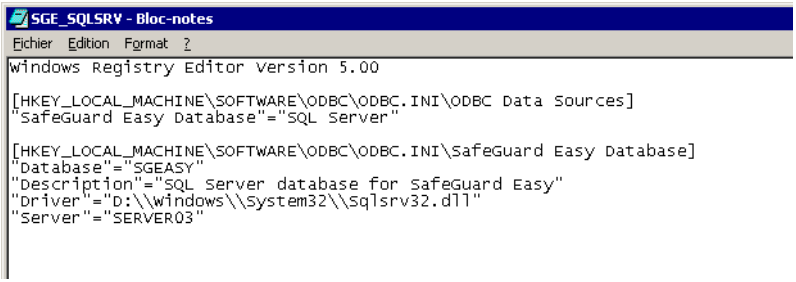
REMARQUE :

- Dans le champ « Nom du serveur », vous devez avoir le nom (ou l'adresse IP) de l'ordinateur sur lequel est installé le serveur SGE (dans notre exemple, SGE Server et SQL Server sont installés sur le même ordinateur).
- Sous « Authentification de la base de données », les données d'utilisateur de la base de données SGEASY doivent être entrées sur le SQL Server" !
  Si, au lieu de l'utilisateur par défaut (dans notre exemple « helpdesk »), un autre compte utilisateur veut s'authentifier, il doit être présent pour la base de données SGEASY et disposer des droits correspondants.

12. Redémarrez l'ordinateur.

Les utilisateurs peuvent également remplacer les étapes 4 à 7 :

1. Ouvrez le fichier du Registre `SGE_SQLSRV.reg`. (Ouvrez le fichier d'enregistrement SGE_SQLSRV.reg (sur le CD SafeGuard Easy dans le répertoire \TOOLS\SQL-info.zip).



2. Modifiez les clés suivantes :

   - **« Driver »**
     Entrez le chemin correct pour le fichier `SQLSRV3.dll` sur votre serveur SGE (par ex.
     « D :\\Windows\\System32\\SQLSRV32.dll »)

   - **« Server »**
     Indiquez le nom du serveur SQL (par ex. « EMOINTL24 »).

3. Exécutez `SGE_SQLSRV.reg`.

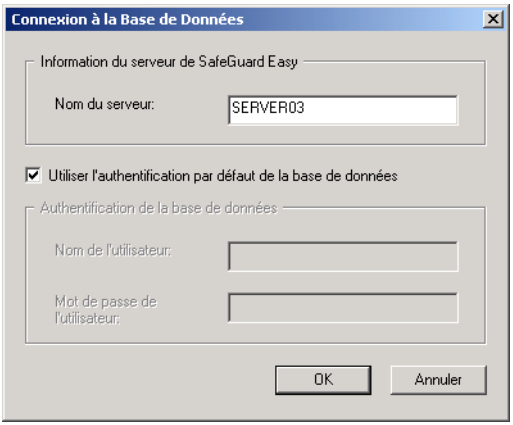
31 Console d'administration

Avant de pouvoir travailler avec la base de données, une communication doit être établie avec le serveur SGE via la console d'administration. Le serveur SafeGuard Easy contient la base de données SafeGuard Easy, son enregistrement OBDC et le processus serveur.

31.1 Ouverture de session

Appelez la console d'administration via **Démarrer / Programmes / Utimaco/ SafeGuard Easy / Console d'administration**.

Un masque d'ouverture de session apparaît.



Vous devez y entrer les informations suivantes :

- **Nom du serveur**
  Nom du serveur SGE sur lequel se trouve la base de données SGE. Le nom de serveur peut également être entré sous forme d'adresse IP.

- **Données d'accès par défaut à la base de données**
  Si la case « Utiliser l'authentification par défaut de la base de données » est cochée, SafeGuard Easy utilise par défaut les données d'ouverture de session actuelles pour la base de données SGE.

  Dans la configuration de base, c'est le nom d'
  utilisateur « Admin »
  Mot de passe :*Pas de mot de passe*
  D'autres données d'accès peuvent être saisies quand la case n'est plus cochée.

Une fois la liaison établie avec succès, le nom de serveur et le nom d'utilisateur (mais pas la base de données ou le mot de passe) sont enregistrés dans le registre et automatiquement réutilisés à la prochaine ouverture de session. La console d'administration ne se connecte cependant automatiquement au serveur que lorsque la dernière ouverture de session a été effectuée avec les « données d'accès par défaut ».

Sans données d'utilisateur par défaut, vous vous connectez en coupant tout d'abord la communication via le menu Fichier dans la console d'administration, puis en la rétablissant. Sélectionnez ensuite l'option « Connecter » dans le menu Fichier pour revenir au masque de connexion de la base de données.

En général, le serveur SGE et la console d'administration se trouvent sur la même machine (mais ce n'est pas une obligation !).
Si la base de données SafeGuard Easy et la console Administration figurent sur des ordinateurs différents (serveur SafeGuard Easy et ordinateur d'administration), le lien s'établit par l'intermédiaire de la procédure d'authentification à l'aide des données utilisateur de Windows. Ainsi, l'utilisateur actuellement connecté à l'ordinateur d'administration doit également utiliser un compte utilisateur adapté pour se connecter au serveur SafeGuard Easy.

31.1.1 Modification des données d'accès à la base de données

Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco http://www.utimaco.com/myutimaco. Dans la zone de recherche (« Search »), tapez « Login & database ».

La base de données fournie avec SafeGuard Easy est une base de données de type Microsoft Access. Pendant l'installation du serveur SGE, elle est enregistrée comme source de données ODBC avec le nom de source de données (DSN) « SafeGuard Easy Database ». La base de données SGE utilise le pilote ODBC standard pour Microsoft Access, intégré dans votre version de Windows. Comme le pilote ODBC pour Microsoft Access est déjà installé dans la configuration de base de Windows 2000 et Windows XP, il n'est pas nécessaire d'installer MS Access pour pouvoir accéder à la base de données SafeGuard Easy. Si, pour une raison ou une autre, vous souhaitez toutefois les données d'ouverture de session par défaut pour votre base de données, Microsoft Access doit être installé pour créer un fichier de données d'utilisateurs.

Un fichier de données d'utilisateurs de type Microsoft Access contient des informations sur l'utilisateur, les mots de passe et l'appartenance à un groupe. Dans la configuration de base, un fichier de données d'utilisateurs possède l'extension .mdw et est également désigné par Microsoft comme « Workgroup Information File ». Une installation de Microsoft Access génère le Workgroup Information File standard `System.mdw` et le stocke sous

- MS Access 97 \WinNT\System32
- MS Access 2000 \Programmes\Fichiers communs\Système

L'outil MS Access `Wrkgadm.exe`, un nouveau fichier MDW peut être créé et utilisé comme fichier d'utilisateur SafeGuard Easy. Vous pouvez cependant utiliser le fichier .mdw standard.

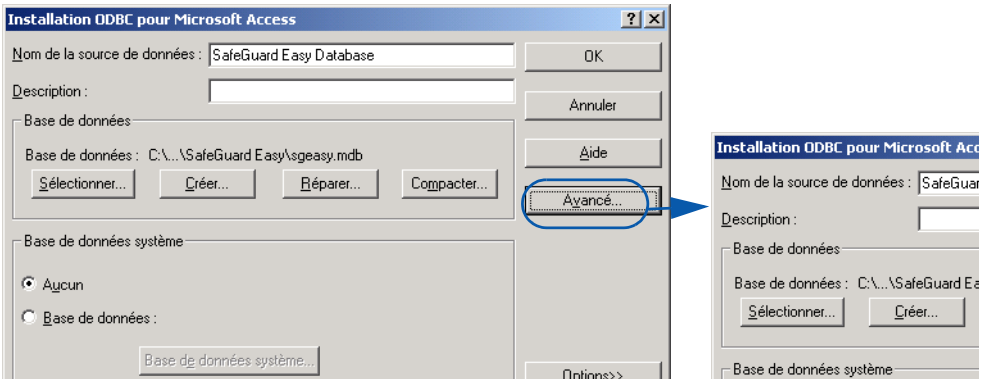
`Wrkgadm.exe` se trouve dans :

- MS Access 97 \WinNT\System32
- MS Access 2000 \Programmes\Microsoft Office\Office\1033\

Si vous utilisez le fichier .mdw standard, ouvrez MS Access. Sous Outils / Sécurité, sélectionnez l'option « Gestion des utilisateurs et des groupes ». Vous pouvez définir ici les utilisateurs, les mots de passe et l'appartenance à des groupes. Ouvrez ensuite la base de données SGE Sgeasy.mdb avec Microsoft Access. Dans le menu Outils / Sécurité, sélectionnez « Autorisations d'accès ». Vous pouvez y attribuer des droits d'accès à des utilisateurs déterminés.

Dans la configuration de base, SafeGuard Easy ne relie pas la base de données SGE à un fichier .mdw. Dans ce cas, le nom d'utilisateur « Admin » est utilisé sans mot de passe comme données d'ouverture de session par défaut.

Pour autoriser les autres données d'ouverture de session, appelez Paramètres / Panneau de configuration / Outils d'administration / Sources de données (ODBC) / DSN système / Configurer. Entrez le fichier MDW standard `System.mdw` dans le champ Base de données système. En cliquant sur le bouton « Avancé », vous pouvez également entrer des données d'ouverture de session par défaut modifiées. Veuillez noter que le profil d'utilisateur entré par défaut existe également comme utilisateur en droit d'utiliser la base de données.


Installation ODBC pour Microsoft Access
Nom de la source de données : SafeGuard Easy Database
Description :
Base de données
Base de données : C:\...\SafeGuard Easy\sgeasy.mdb
Sélectionner...
Créer...
Réparer...
Compacter...
Base de données système
Aucun
Base de données :
Base de données système...
OK
Annuler
Aide
Avancé...
Options>>
Installation ODBC pour Microsoft Acc
Nom de la source de données : SafeGuar
Description :
Base de données
Base de données : C:\...\SafeGuard Ea
Sélectionner...
Créer...
Base de données système

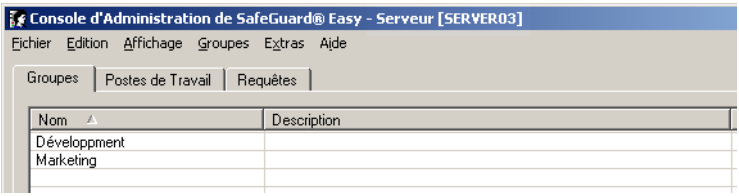
31.2 Interface utilisateur de la console Administration

Après l'établissement de la connexion à la base de données SGE, la fenêtre d'administration de la console d'administration apparaît. Elle comprend les onglets Postes de travail, Groupes et Requêtes. Un passage aux différents onglets est possible par un simple clic sur l'onglet correspondant ou via le menu **Affichage**.

Postes de travail

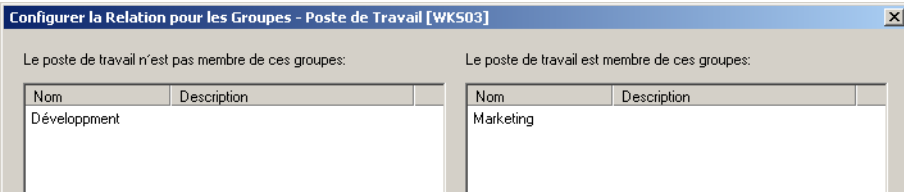
Affiche une liste de tous les clients SGE authentifiés sur le serveur.

- **Nom :** nom UNC Netbios du poste de travail enregistré.
- **État :** poste de travail en ligne (par défaut) ou hors ligne
- **Description :** informations détaillées sur le poste de travail enregistré
- **Date de configuration :** indique quand (date, heure) un client SGE a envoyé la dernière fois ses données de configuration actuelles au serveur SGE.



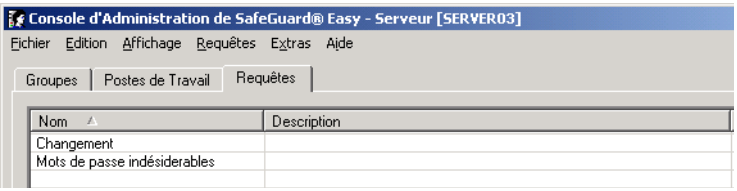
Groupes

Affiche tous les groupes SGE créés où sont rassemblés des clients SGE individuels.

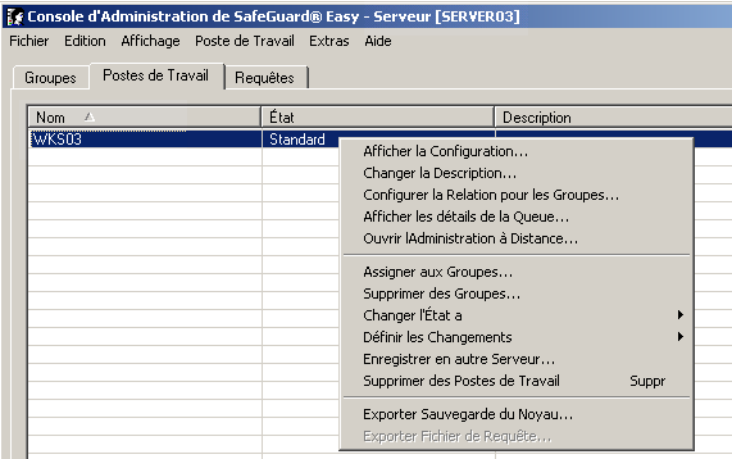


Requêtes

Affiche une liste de toutes les modifications de configuration effectuées et exécutées sur les clients SGE



Les commandes les plus importantes pour un poste de travail, un groupe ou une requête sont disponibles dans le menu contextuel respectif. En outre, vous pouvez appeler toutes ces commandes par l'intermédiaire de différentes menus (Stations de travail, Groupes, Requêtes). Le système affiche les menus correspondant à l'onglet actif (par exemple, lorsque l'onglet Stations de travail est actif, le menu Stations de travail s'affiche, etc.).



Si plusieurs postes de travail, groupes, requêtes sont présents, une sélection multiple via les mécanismes Windows usuels (CTRL/MAJ) ou via le menu **Edition** est possible.

L'administration à distance peut également être appelée de la console d'administration (Poste de travail/Ouvrir l'**Administration à distance**. Pour plus de détails sur l'administration à distance, lire le chapitre 'Administration à distance'.

31.2.1 Enregistrement du contenu des onglets comme fichier de texte

La console d'administration fournit une fonctionnalité permettant d'enregistrer le contenu de l'onglet momentanément actif (groupes, postes de travail ou requêtes) dans un fichier de texte ou de le « copier » dans le Presse-papiers. Le fichier de texte et son contenu dans le Presse-papiers peuvent être par exemple importés et traités dans n'importe quel programme. La fonctionnalité est active dès qu'un groupe, un poste de travail ou une requête sont sélectionnés. L'enregistrement du contenu des fichiers est en particulier approprié à des fins d'archivage ou d'évaluation.

La fonction de copie et d'enregistrement est appelée via le menu **Edition** de la console d'administration.

- La sous-rubrique **Enregistrer** données comme crée un fichier ASCII qui peut être enregistré dans un répertoire sous un nom au choix. Ce fichier contient les titres de colonnes, plus les entrées d'onglets sélectionnées.
- Le sous-menu **Copier données** place temporairement les entrées d'onglets cochées (sans titres de colonnes) dans le Presse-papiers. Le contenu du Presse-papiers peut être inséré dans n'importe quel programme.

31.3 Affichage de la configuration actuelle d'un client SGE

Dès que le client SGE et le serveur SGE sont authentifiés avec succès, l'utilisateur en session sur la console d'administration peut consulter les paramètres SafeGuard Easy du client.

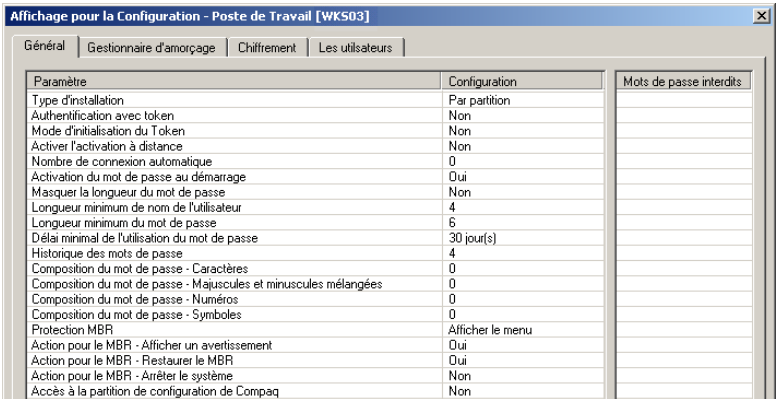
Pour vérifier les paramètres actuels ou pour préparer des modifications, il est presque toujours conseillé de se faire une idée générale des configurations actuelles. Cette fonction permet également de contrôler aisément si des requêtes ont bien été exécutées avec succès sur des clients ou non.

Pour la distribution du logiciel dans un environnement Active Directory, procédez comme suit,

1. Cliquez sur l'onglet **Poste de travail** et sélectionnez un client SafeGuard Easy.

2. Via le menu **Postes de travail / Afficher la configuration**, il est possible d'interroger les détails des paramètres SGE.

3. Vous voyez apparaître une fenêtre avec quatre onglets identiques à ceux de SafeGuard Easy Administration, c'est-à-dire : Général, Chiffrement, Gestionnaire d'amorçage et Utilisateurs. Chaque onglet montre la configuration SGE du client sélectionné.



31.3.1 Modification de la description du client

Pour donner un autre nom et une autre description à un poste de travail affiché sous l'onglet « Poste de travail », ouvrez la commande **Changer la description** dans le menu **Poste de travail**. Les entrées modifiées sont immédiatement validées.

31.3.2 Suppression de client

Pour supprimer un client, cliquez sur Supprimer le poste de travail dans le menu **Postes de travail**. Le client est alors supprimé de la liste des postes de travail enregistrés.

31.4 Nouvel enregistrement du client SafeGuard Easy

Le mode utilisé pour le nouvel enregistrement d'un client SGE est nécessaire quand le client SGE n'est pas connu du serveur SGE.

Dans la pratique, la fonction peut être appliquée par exemple dans le cas suivant : dans une entreprise, la base de données SGE est sauvegardée chaque jour à 5 h. A 8 h, un nouveau client SGE s'enregistre avec succès sur le serveur SGE et une panne de serveur se produit à 10 h. Le serveur SGE est restauré, avec toutefois la 'l'ancienne' sauvegarde de base de données exécutée à 5 h. Cette sauvegarde ne comporte pas le nouveau client SGE qui s'est enregistré à 8 h. Via le nouvel enregistrement, le client SGE est à nouveau ajouté dans la base de données SGE.

Pour que ce nouvel enregistrement soit validé, l'utilisateur de la console d'administration doit connaître les données d'utilisateur SafeGuard Easy valides du nouveau client SGE et s'authentifier avec ces données sur le client.

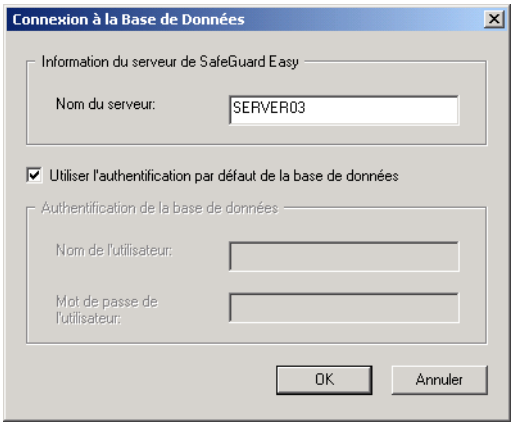
REMARQUE :
Vous ne pouvez enregistrer qu'un et un seul client à la fois.

Conditions

- Une connexion réseau doit exister entre le nouveau client SGE et le serveur SGE.
- SafeGuard Easy doit être installé sur le client SGE concerné avec l'option « Liaison serveur ».
- Le nouveau client SGE ne doit pas être enregistré sur le serveur. Si le nouveau client SGE est déjà enregistré sur le serveur SGE et doit impérativement être réenregistré, l'entrée client doit être d'abord supprimée de la base de données, puis enregistrée à nouveau. Les clients sont supprimés de la base de données SGE via le menu Postes de travail / Supprimer le poste de travail.
- L'utilisateur de la console d'administration doit connaître les données d'accès SafeGuard Easy au nouveau client SGE.

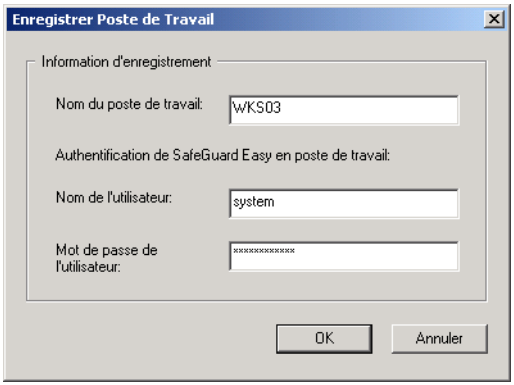
Comment procéder

1. Contrôler la connexion réseau entre le client et le serveur.
2. Démarrer la console d'administration et ouvrir une session dans la base de données.

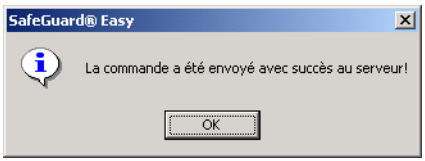


3. **Appeler le menu Extras/ Enregistrer poste de travail.**

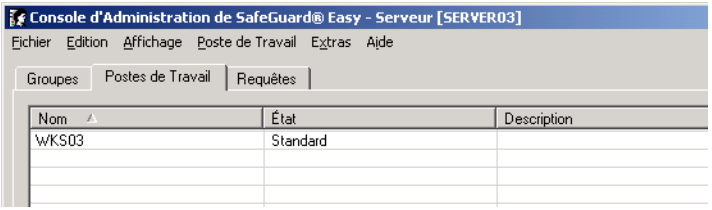
4. Une boîte de dialogue apparaît, demandant le nom du client SGE et les données d'authentification pour ce client.
   Le profil de l'utilisateur SafeGuard Easy entré doit exister sur le client SGE. Le profil ne requiert aucun droit SafeGuard Easy particulier.



5. Confirmer la saisie avec [OK]. Le succès ou l'échec de l'opération sont indiqués dans une boîte de dialogue.



6. Le client dépose alors des informations sur le serveur SGE. Selon le taux d'utilisation du réseau, ceci peut prendre un certain temps. Une fois la période d'attente terminée, le nouveau client SafeGuard Easy s'affiche dans la console Administration. (Vous pouvez également mettre à jour l'affichage de façon manuelle dans la console Administration en appuyant sur [F5].



31.4.1 Nouvel enregistrement de plusieurs clients SafeGuard Easy

Ce nouvel enregistrement concerne tous les clients SGE à partir de la version 4.11.

La procédure de nouvel enregistrement de plusieurs clients SGE est la suivante :

1. Utilisez l'assistant de configuration pour générer un nouveau fichier de configuration avec la propriété « Installer ».
2. Saisissez dans ce fichier de configuration le mot de passe de l'utilisateur SYSTEM défini pour les clients SGE.
3. Enregistrez le fichier de configuration sous « SGEREG.cfg ».
4. Dans le client SGE, copiez le fichier SGEREG.cfg dans le répertoire <lecteur système>/System 32.
5. Dans le client SGE, créez deux nouvelles entrées de registre (valeurs DWORD) dans la section

   HKEY_LOCAL_MACHINE
   SOFTWARE
   Utimaco
   Sgeasy

   NotRegistered=1
   RegReport=1
6. Redémarrez le client SGE (ou le service SGE).

31.5 Enregistrement de clients SGE sur un autre serveur SGE

Si des clients SGE doivent être administrés par un serveur autre que le serveur sur lequel ils sont enregistrés, ceci peut se faire avec la fonction « Enregistrement sur un autre serveur ». Pour ce faire, une requête d'enregistrement est générée. Cette requête est similaire à une requête « normale », mais elle contient – au lieu de la mise à jour de configuration – le nouveau nom de serveur SGE et les données SafeGuard Easy pour l'authentification sur le client SGE devant être « déplacé ».

Le traitement d'une requête pour enregistrement correspond à peu près à celui d'une requête « normale ». Une fois l'opération terminée, la console d'administration entre la requête pour enregistrement dans la file d'attente. Dès qu'un client SGE interroge « l'ancien » serveur SGE, il y trouve la requête pour enregistrement qu'il envoie au « nouveau » serveur SGE. L'ancien serveur SGE reçoit pour finir du client SGE un rapport sur le nouvel enregistrement, le client SGE étant alors supprimé de « l'ancienne » base de données SGE.

REMARQUE :

Le nouveau serveur SGE ne doit pas être enregistré comme client SGE sur l'ancien serveur SGE.

Vous pouvez déplacer les clients SGE de façon individuelle ou par groupes.

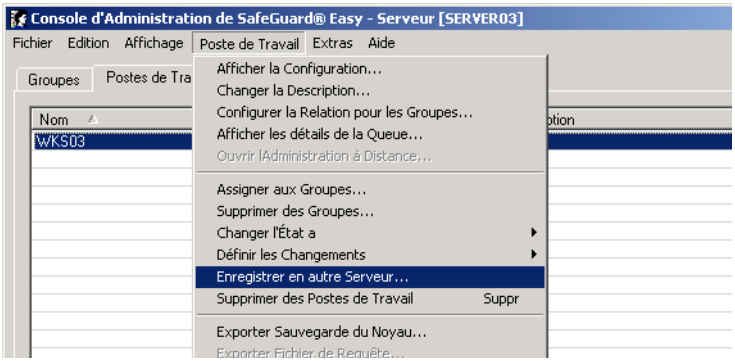
Une fois le client SGE déplacé avec succès, la requête d'enregistrement est supprimée, car le client SGE a changé d'emplacement. La requête d'enregistrement ne demeure dans la file d'attente que tant que son état demeure « En attente », « Planifié » ou « Échoué ».

Conditions

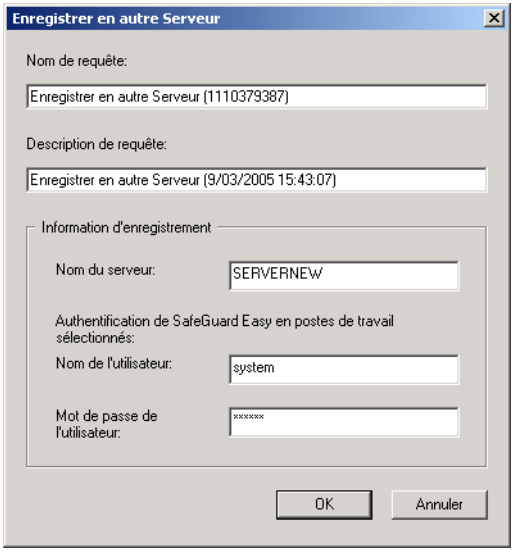
- Une connexion réseau doit exister entre le client SGE et le serveur SGE.
- L'utilisateur de la console d'administration doit connaître les données d'accès SafeGuard Easy pour le client SGE.
- Le client SGE doit déjà être enregistré sur l'ancien serveur SGE (= il doit déjà exister dans la base de données SGE).

Comment procéder

1. Démarrez la console d'administration et ouvrez une session dans la base de données.
2. Cochez les clients/groupes sélectionnés.
3. Sélectionnez l'option **Postes de travail / Enregistrer en autre serveur.**

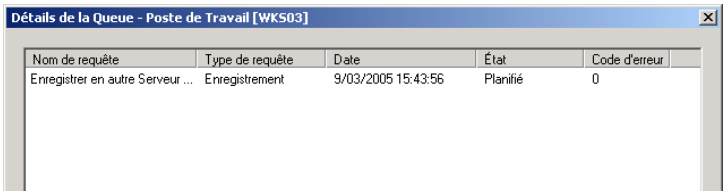


4. Une boîte de dialogue apparaît, demandant le nom du nouveau serveur SGE et les données d'authentification pour ce client. Le nom et la description de la requête doivent être sans équivoque.
   Le profil de l'utilisateur SafeGuard Easy entré doit exister sur le client SGE, mais peut ne pas posséder de droits SafeGuard Easy particuliers. .

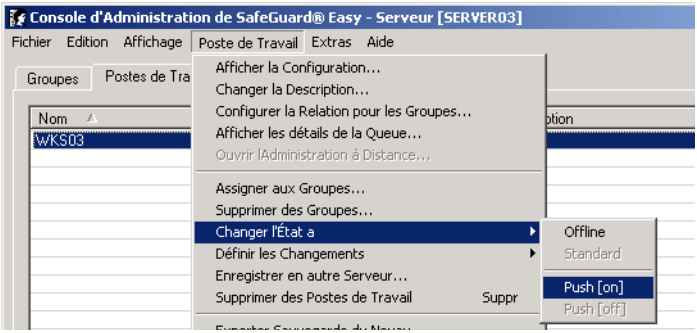


5. Confirmer la saisie avec [OK].

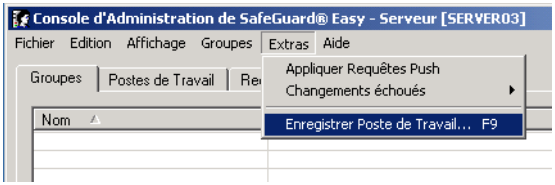
6. La demande pour enregistrement apparaît dans la file d'attente.



7. Définir l'état du client SGE sur « Push » via le menu **Postes de travail / Changer l'état à / Push [on]**.

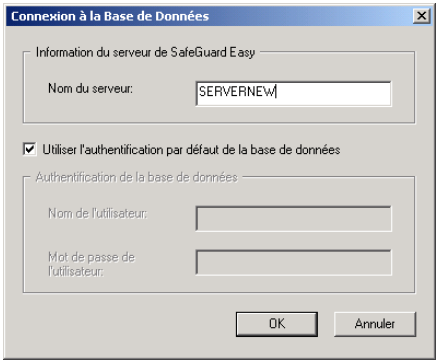


8. Lancer la requête pour enregistrement via le menu **Extras / Appliquer requêtes Push**.

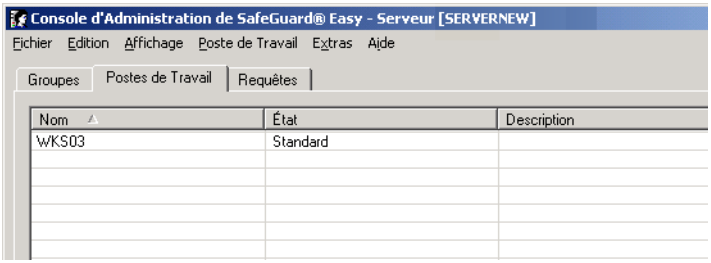


9. Le client SGE, sa file d'attente et autres dépendances de base de données sont supprimées de l'ancienne base de données.

10. Démarrer la console d'administration et la connecter au nouveau serveur.



11. Le client SGE réenregistré apparaît dans la console d'administration.



31.6 Définition de groupes

La console Administration administre les différents clients SafeGuard Easy qui sont inscrits sur le serveur SafeGuard Easy. Dans les grandes organisations, cependant, il est souvent préférable de créer des groupes de clients SafeGuard Easy. Ceci permet de distribuer les paramètres de configuration à un grand nombre d'ordinateurs à la fois. Les groupes se subdivisent par ex. en services ou également en configurations SGE identiques. Malgré l'affectation à des groupes, les clients peuvent également effectuer leurs propres configurations.

Les groupes SafeGuard Easy ne comportent pas de hiérarchies. Par exemple, vous ne pouvez pas exclure le groupe B du groupe A, accorder plus de droits au groupe C qu'au groupe D, etc. Chaque client SGE peut toutefois être membre de plusieurs groupes.

Le regroupement de clients prend beaucoup de temps dans les grandes organisations. Dans le cadre d'une installation préconfigurée, un paramètre SafeGuard Easy peut affecter automatiquement des clients à un ou plusieurs groupes pendant l'installation (cf. Paramètre `Groupes` sur 'Paramètres SafeGuard Easy').

Les groupes SGE travaillent indépendamment des groupes d'utilisateurs Windows existants !

31.6.1 Création/Suppression de groupes

Pour créer un groupe, cliquez sur l'onglet **Groupes et sélectionnez Créer un groupe**. Une boîte de dialogue s'affiche pour vous permettre d'entrer le nom de groupe. Toute entrée confirmée s'affiche dans la liste de l'onglet Groupes.

Les groupes qui ne sont plus nécessaires sont supprimés via le menu **Groupes / Supprimer des groupes**.

Malgré la suppression, les requêtes envoyées pour les groupes demeurent en liste d'attente et sont envoyées.

31.6.2 Ajout ou suppression d'un client SafeGuard Easy à un/d'un groupe

Pour administrer des clients SGE sur la base de groupes, un nom de groupe existant doit leur être attribué. Cliquez pour ce faire sur l'onglet Poste de travail. Marquez un client SGE et appelez dans le menu **Postes de travail** la commande **Assigner aux groupes...** Cochez un groupe et confirmez votre choix.

Un client est supprimé via le menu **Postes de travail / Supprimer des groupes**.

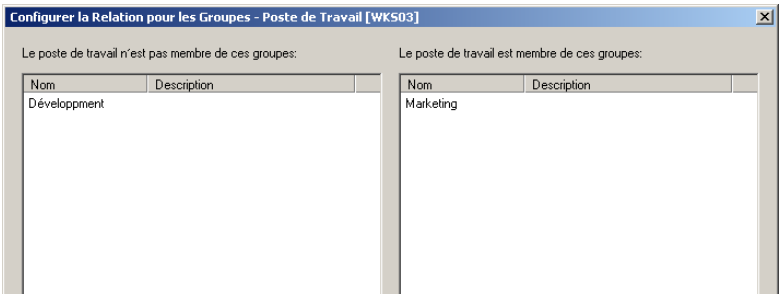
La composition d'un groupe ne doit pas être modifiée tant qu'il existe encore des requêtes à exécuter !

31.6.3 Identification de membres de groupe

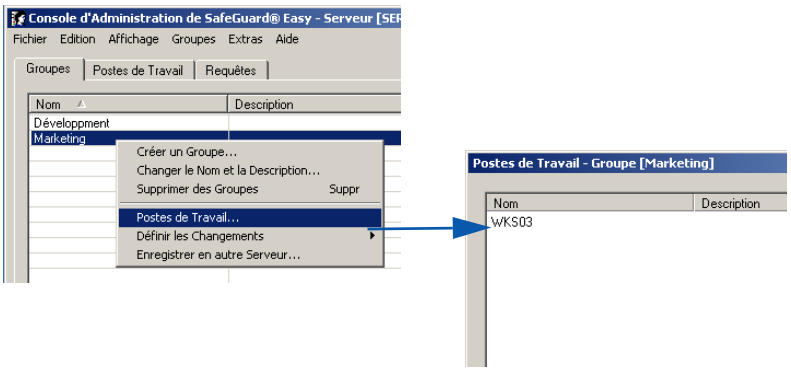
Les administrateurs doivent se faire rapidement une idée générale des compositions de groupes pour garantir que les clients recevront toujours les données correctes.

La console d'administration fournit ces données via le menu Postes de travail / Configurer la relation pour les groupes :

- **Station de travail/Configuration de l'appartenance de groupe...**
  Cette option de menu permet d'identifier les membres d'un groupe sur un client SafeGuard Easy. Vous pouvez utiliser les touches de direction pour modifier l'appartenance au groupe.



- **Groupes / Postes de travail :**
  Ce menu donne la liste des membres d'un groupe.



31.6.4 Modification d'un nom de groupe

Pour modifier un nom de groupe, cliquez sur **Changer les groupes** dans le menu **Groupes**. Entrez le nom du groupe et confirmez-le avec OK.

31.6.5 Suppression de groupes

Pour modifier un nom de groupe, cliquez sur **Supprimer des groupes** dans le menu **Groupes**.

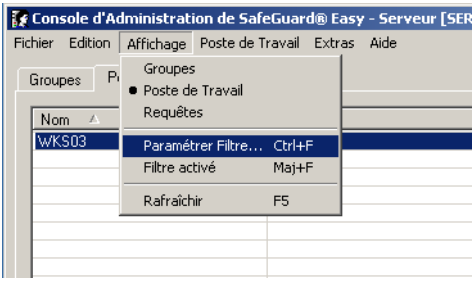
31.7 Définition de filtre

La console d'administration possède un mécanisme de filtrage au moyen duquel l'administrateur peut déterminer avec précision quels clients SGE, groupes ou requêtes il voit à l'écran. Cette méthode est pratique – quand de nombreux objets doivent être administrés – pour faciliter l'administration et conserver une clarté suffisante.

Le menu **Affichage** de chaque onglet permet d'accéder à la définition du filtre.

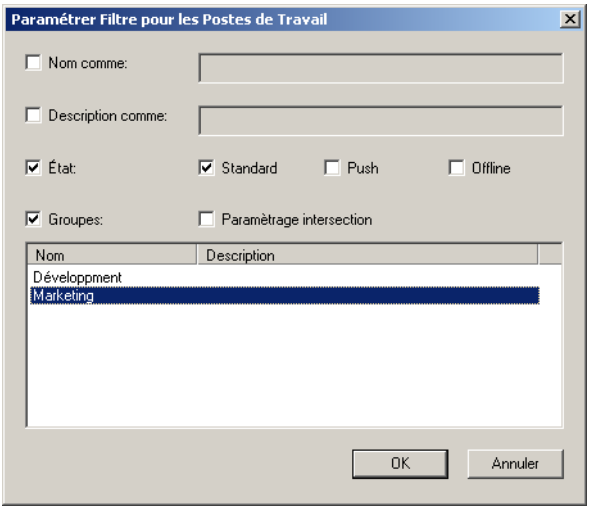
Le filtre est défini en deux étapes :

- Paramétrage du filtre ;
- Activation du filtre.



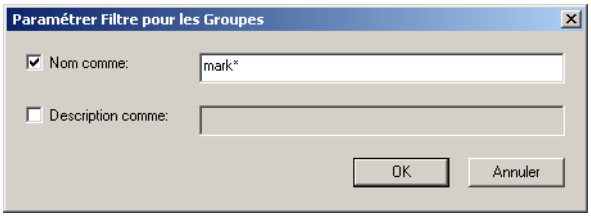
31.7.1 Configuration d'un filtre

Les *postes de travail* peuvent être affichés/masqués de diverses manières. Une option avancée permet même de définir comme règle l'intersection de groupes marqués (c'est-à-dire que les postes de travail ne sont affichés que lorsqu'ils sont membres du groupe A et du groupe B).

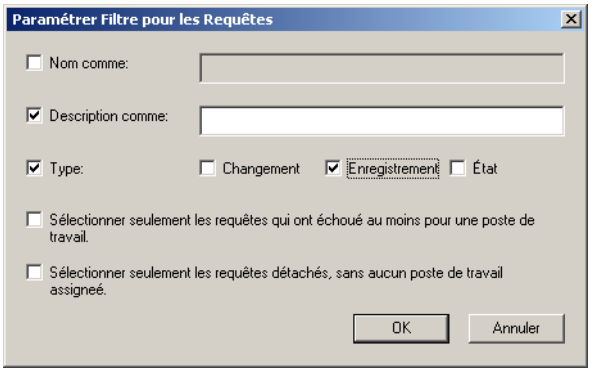


Vue des stations de travail

Pour les *groupes et requêtes*, le filtrage est possible par nom et description. Avec les requêtes, il est en outre possible de n'afficher que les requêtes ayant échoué.



Vue des groupes



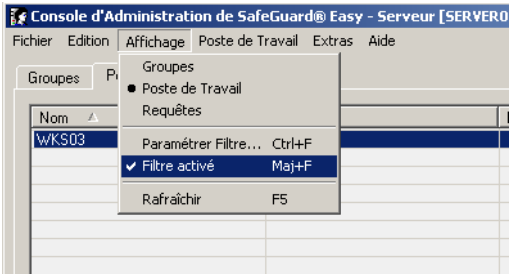
Vue des requêtes

Des caractères génériques peuvent également être utilisés dans les champs « Nom comme » et « Description comme ». Seul l'astérisque (*) est accepté comme caractère générique. Cela signifie que la position dotée d'un « * » peut comporter plusieurs caractères au choix dans le nom / dans la description.

La règle suivante s'applique normalement : seuls les postes de travail / groupes / requêtes pour lesquels chacune des propriétés sélectionnées est valable sont affichés.

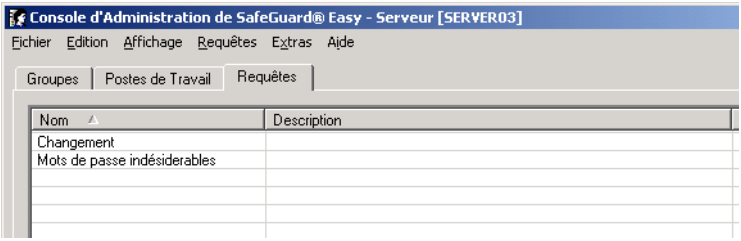
31.7.2 Activation d'un filtre

Le filtre n'agit que lorsqu'il a été activé. L'utilisateur reconnaît qu'il se trouve en mode de filtrage à la couleur modifiée de la surface de travail de la console d'administration. Le fond blanc standard devient par exemple bleu.



31.8 Requêtes et listes d'attente

Les requêtes comportent des mises à jour de configurations pour les clients SGE. Le client SGE va chercher ces mises à jours sur le serveur SGE dès qu'ils sont en communication. Quand un client SGE détecte des modifications, il les exécute dans l'ordre où elles ont été attribuées au client via la console d'administration. Les requêtes générées une fois sont utilisables aussi longtemps que vous le désirez pour différents groupes / postes de travail. Toutes les requêtes envoyées sont regroupées dans la file d'attente sous l'onglet « Requêtes », indépendamment de leur état.



Une requête est par principe similaire à la fonction d'un fichier de configuration (cf. 'Créer un nouveau fichier de configuration') et exécute des modifications de paramètres existants d'un client SafeGuard Easy. Une modification peut être une petite intervention dans la configuration du client SafeGuard Easy, mais une désinstallation de SafeGuard Easy est aussi possible. Seules des installations via requête ne sont pas prévues. Si besoin est, les requêtes intègrent également des fichiers de configuration existants.

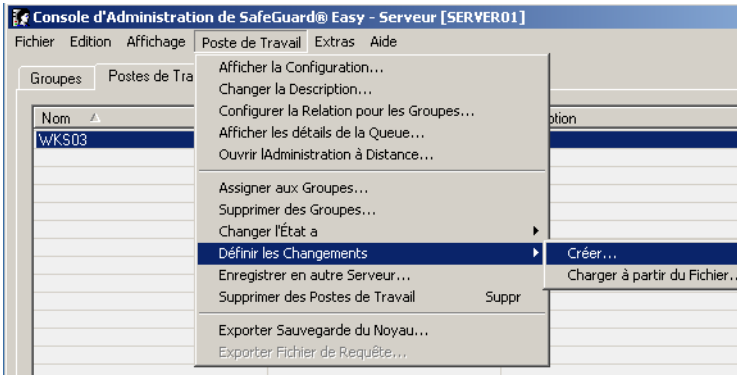
Le succès/l'échec d'une requête sont immédiatement transmis au serveur, ce qui fait que l'administrateur est toujours informé avec précision de l'état actuel. Une requête n'est exécutée avec succès que lorsque les informations de création (Identifiant d'un utilisateur et mot de passe SafeGuard Easy) correspondent à celles d'un utilisateur SGE sur le client SGE. Le profil des droits de l'auteur doit en outre permettre l'exécution des modifications indiquées sur le client.

Les requêtes sont ordonnées suivant la date de leur création dans une **file d'attente serveur** où elles attendent que le client vienne les chercher. Les clients commencent toujours par la requête la plus ancienne.

31.8.1 Création de requêtes

De nouvelles requêtes peuvent être élaborées pour des clients SGE individuels ou pour des groupes. La requête n'est exécutée qu'une fois, même si un client SGE est présent dans plusieurs groupes.

Les nouvelles requêtes sont créées via **Définir les changements**, que l'on trouve à la fois dans le menu **Postes de travail** et dans le menu **Groupes**.

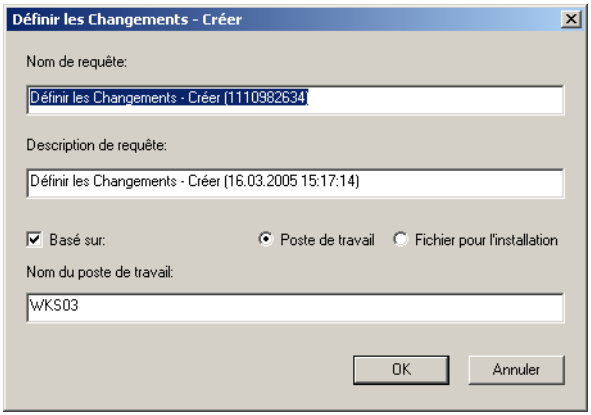


Après appel de **Définir les changements**, l'utilisateur a le choix entre :

- **Créer**
  Crée une nouvelle requête
- **Charger à partir du fichier**
  Utilise un fichier de configuration actuel comme requête.

31.8.2 Création d'une nouvelle requête

Via **Postes de travail (Groupes) / Définir les changements / Créer**, vous appelez une boîte de dialogue dans laquelle vous décidez si une requête doit être créée avec modèle (une configuration de base, par exemple) ou non.



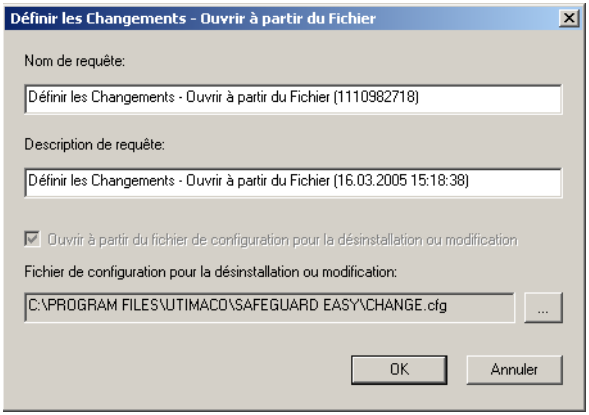
Il est conseillé de charger un modèle quand il contient des paramètres qui ne se différencient que peu de ceux de la requête planifiée. Il facilite le travail de l'administrateur, étant donné que celui-ci n'a pas à taper/ sélectionner des options de façon répétée. Le modèle pour la requête est basé soit sur les paramètres d'un client enregistré sur le serveur SGE (taper par ex. « WKS- »), soit sur un fichier de configuration avec l'attribut « Installer ». Cette méthode permet par ex. de copier des paramètres d'une machine à l'autre.

Sans modèle, une nouvelle requête est créée en ne basant ses paramètres ni sur un fichier de configuration, ni sur un poste de travail.

La confirmation des entrées de la boîte de dialogue démarre l'assistant de configuration pour le déploiement (voir 'Assistant Fichier de configuration'). Si l'assistant de configuration pour le déploiement reconnaît comme base un fichier d'installation, il demande une authentification avant l'affichage de toutes les données.

31.8.3 Utilisation de fichier de configuration existant comme requête

Via **Postes de travail (Groupes) / Définir les changements / Charger à partir du fichier**, un fichier de configuration existant peut être directement affecté à une requête. Ce fichier est désinstallé par un client SGE ou seules des modifications sont effectuées. La condition est que ce fichier ait été préalablement créé avec l'assistant de configuration pour le déploiement.



Leur « durée de vie » est un atout du travail avec des fichiers de configuration existants. Les requêtes complétées qui ne sont pas associées à un fichier de configuration ne sont pas accessibles en tant que fichiers distincts. Par contre, ils sont stockés en tant que liens dans la base de données de SafeGuard Easy. Quand ils ont été exécutés avec succès, leurs paramètres ne peuvent plus être édités ultérieurement ou assignés à d'autres postes de travail !

31.8.4 Échec d'une requête

Des requêtes peuvent échouer

- lorsque les profils de droits du créateur requis n'autorisent pas la modification entrée dans la requête à appliquer sur le client SafeGuard Easy. Si au moins l'un des paramètres de la requête de modification ne peut pas être appliqué, l'ensemble de la requête de modification sera rejeté !
- quand l'authentification du demandeur a échoué sur le client SGE,
- quand, pour des raisons déterminées, aucune connexion réseau n'est établie entre le client SGE et le serveur SGE (dans les cas d'urgence, il est recommandé de travailler avec des clients hors connexion),
- quand des entrées dans la requête ne correspondent pas aux paramètres SGE sur le client (par ex. saisie d'un mot de passe SGE invalide dans la requête pour un utilisateur SGE).

Tout échec de tâche arrête le traitement des autres tâches de la file d'attente. D'autre part, par exemple, il est impossible d'enregistrer des fichiers de requête pour les clients hors connexion en cas d'échec d'une tâche.

Dès que la requête ayant échoué est retirée de la file d'attente ou y est réintroduite (menu Extras / Modifications ayant échoué) toutes les requêtes en attente sont à nouveau exécutées. Pour supprimer les tâches qui ont échoué ou les ajouter à nouveau, sélectionnez l'option **Extras/ Failed changes (Extras/Échec des modifications).**

31.8.5 Modification du nom de requête

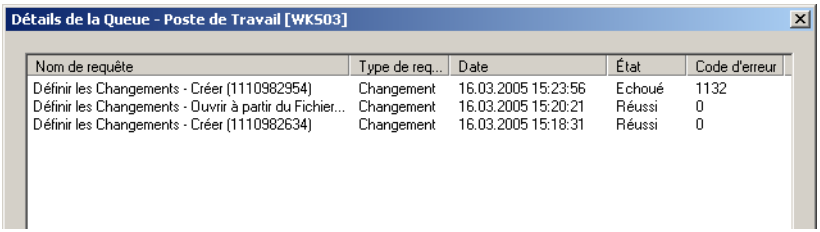
Pour donner un autre nom et une autre description à une requête affichée sous l'onglet « **Requêtes »,** ouvrez la commande **Changer le nom & la description dans le menu Requêtes**. Les entrées modifiées sont immédiatement validées.

31.8.6 Suppression d'une requête

Tant qu'une requête n'a pas encore été exécutée avec succès, les modifications « indésirables » peuvent être annulées. Dans ce but, la requête doit être retirée de la file d'attente. Dans le menu **Requêtes / Supprimer des requêtes**, une requête marquée est supprimée et retirée de la file d'attente.

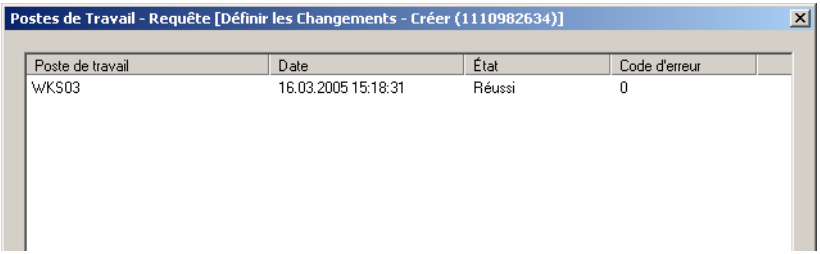
31.8.7 File d'attente

La file d'attente générale (menu **Postes de travail / Détails** de la queue) comporte toutes les requêtes définies pour les clients SGE, leur état actuel (réussi, échoué, etc.), ainsi que des indications sur le moment où la requête a été créée.



REMARQUE :
Le bouton [Supprimer] est actif quand aucune des entrées de file d'attente sélectionnées n'est sur « En attente ».

La file d'attente spécifique aux requêtes (menu **Requêtes / Postes de travail**) indique à quel poste de travail une requête marquée est liée



Les requêtes d'une file d'attente peuvent avoir les propriétés suivantes :

- **Réussi :** la requête a été exécutée sur un client SGE et le serveur a reçu une information sur le succès de l'opération.
- **Échoué :** la requête a été exécutée, mais une erreur s'est produite pendant l'exécution et le serveur en a été informé. La signification du numéro d'erreur qui s'affiche peut être consultée au chapitre "Erreurs".
- **En attente :** la requête a été envoyée au client SGE, mais aucune information sur la réussite/l'échec de l'opération n'est encore parvenue au serveur.
- **Planifié :** la requête attend d'être envoyée au client SGE. Cet état est noté dès que le client SGE contacte le serveur ou quand la file d'attente est mise en mode Push.

31.9 État d'un client SafeGuard Easy

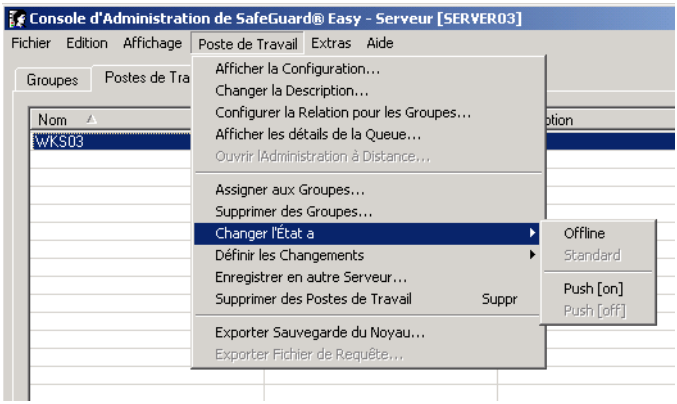
L'état d'un poste de travail indique le type de communication entre le serveur SGE et le client SGE. L'état spécifie également la façon dont le serveur SafeGuard Easy traite la file d'attente de la station de travail.

Les postes de travail peuvent avoir différents états, qui sont :

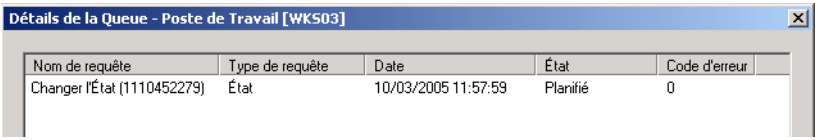
- Standard (= en ligne)
- Hors connexion
- Activer Push
- Désactiver Push

Les états (standard/en ligne et hors connexion) montrent le type de connexion entre le serveur SGE et le client SGE et déterminent ainsi les conditions de communication entre le serveur SGE et le client SGE. « Push on » et « Push off » peuvent être combinés avec les deux autres états (standard/en ligne et hors connexion). Les postes de travail avec l'attribut « Push (on) » sont des postes de travail dont la file d'attente doit être immédiatement traitée après exécution d'une commande dans la console d'administration du serveur SGE.

Le changement d'état se fait via le menu **Postes de travail / Changer l'état à**.



Dès que l'état (standard ou hors connexion) d'un client SGE est modifié, SafeGuard Easy entre une « requête d'état » dans la file d'attente.



31.9.1 État « Standard (= en ligne) »

Après échange des informations de communication (paire de clés, création GUID, assignation d'un nom de serveur SGE) et le premier enregistrement qui suit sur le serveur, chaque client possède l'état « Standard ». Les clients avec l'attribut « Standard » sont les PC qui entrent régulièrement en contact avec le réseau (par ex. ordinateurs stationnaires dans les bureaux). Ces clients SGE recherchent toujours d'eux-mêmes le contact avec le serveur et reprennent les requêtes qui les concernent à chaque prise de contact, la première fois au démarrage du client SGE, puis toutes les 6 heures.

31.9.2 État « Hors connexion »

Les clients hors connexion sont des ordinateurs dont on sait d'avance qu'ils ne sont jamais connectés au réseau ou au serveur SGE (par ex. ordinateurs portables des collaborateurs des services extérieurs), mais qui doivent être toutefois administrés de façon centrale. L'installation pour de tels ordinateurs est exécutée comme d'habitude avec premier enregistrement au serveur SGE. Dans la console d'administration, l'administrateur commute également « Hors connexion » l'état du client concerné". Il ne le fait que quand il sait que celui-ci n'essaiera pas d'entrer de lui-même en contact avec le réseau. Les requêtes ayant échoué du client au serveur n'affectent *pas* l'état « Hors connexion » à un client.

L'état « Hors connexion » peut être assigné dès l'installation à un client en attribuant le nom de serveur « OFFLINE ».

L'état « Hors connexion » influe également sur la manipulation de requêtes créées pour l'ordinateur commuté en mode Hors connexion et devant être exécutées sur celui-ci. Si l'administrateur crée une (ou plusieurs) requêtes pour le client, celles-ci sont mises en file d'attente, mais attendent en vain leur reprise par le client SGE, étant donné qu'aucune liaison avec le serveur SGE n'est établie.

Pour que les modifications soient transférées malgré l'absence de liaison client-serveur, une fonction de la console d'administration exporte toutes les requêtes valables pour un client hors connexion dans un fichier. L'administrateur envoie ce fichier par courrier électronique à l'utilisateur du client Hors connexion. Celui-ci importe le fichier à l'aide des utilitaires fournis par SafeGuard Easy. Dès que des requêtes sont enregistrées dans un fichier de requêtes, elles reçoivent l'état « En attente » dans la file d'attente du serveur. Ceci empêche l'ajout postérieur de fichier de requêtes. Dès que le fichier de requêtes a été importé, les requêtes sont traitées dans l'ordre prescrit sur l'ordinateur hors connexion.

Sans contact avec le client hors connexion, l'administrateur ne sait pas si les modifications ont été exécutées avec succès ou si elles ont échoué. Les informations manquantes lui sont fournies par un fichier de rapport créé après exécution du fichier de requêtes. Ce fichier de résultat doit être transmis à l'administrateur et importé dans la console d'administration (celle-ci comprend la fonction d'importation nécessaire). Après l'importation, l'administrateur voit si les modifications de configuration ont été exécutées avec succès en appelant les propriétés du client hors connexion.

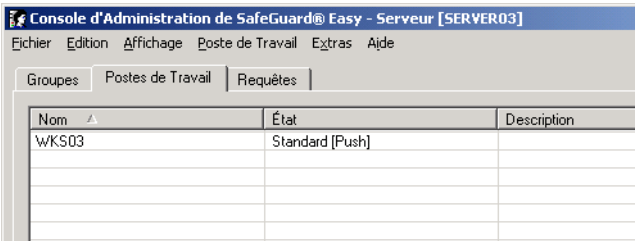
Un client ne peut passer du mode hors connexion au mode Standard quand il est installé avec l'option « Liaison serveur » et quand le nom du serveur SGE lui est fourni.

L'échange de fichier de requêtes/rapport n'est pas restreint aux clients hors connexion. En cas de défaillance par ex. de la connexion réseau entre les clients SGE et le serveur SGE, les modifications de configuration peuvent être transmises aux clients non accessibles avec ce procédé jusqu'à ce que les clients puissent à nouveau être administrés.

31.9.3 État « Push [on] »

Un client SGE peut être forcé de synchroniser ses paramètres avec le serveur avant tous les autres clients. Ceci peut être le cas quand un utilisateur a un souhait de configuration ou quand l'administrateur doit exécuter des modifications immédiates sur le client (le collaborateur quitte l'entreprise ou l'accès au client doit être bloqué).

Pour que le serveur SGE sache quel client SGE est concerné, ce dernier reçoit l'attribut « Push » via le menu Postes de travail / Changer l'état à / Push [on], par ex. « Standard [Push] ». Pour ce faire, sélectionnez l'option **Workstations/Change State to/Push [on]** (Stations de travail/Modifier l'état/Push - activé).

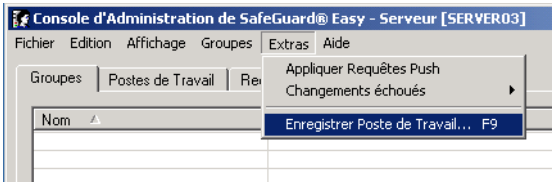


Après exécution de la commande « Appliquer Requêtes Push » dans le menu Extras, l'attribut « Push » d'un client active le serveur qui se comporte normalement de façon passive, attendant les requêtes des clients. Le serveur SGE essaie de lui-même de contacter un client avec l'attribut « Push » et de traiter pour ce client toutes les requêtes avec la propriété « Planifié »se trouvant en file d'attente jusqu'à ce que celle-ci soit vide ou qu'une requête échoue. Dans les deux cas, le serveur revient en état passif (normal) et y demeure jusqu'à ce que l'administrateur le remette en mode « Push ».

L'attribut « Push » est ce faisant automatiquement supprimé.

Le mécanisme Push est un compromis entre charge de réseau et sécurité.

La prise de contact du serveur SGE avec les clients est initiée en mode Push via le menu **Extras / Appliquer requêtes Push**.



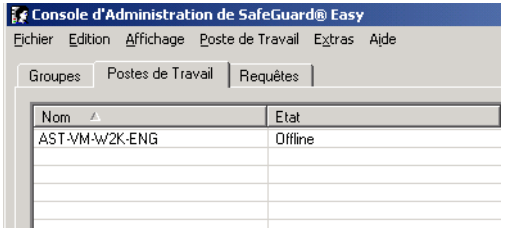
31.9.4 L'état « Push [off] »

Via le menu **Postes de travail / Changer l'état à / Push [off]**, SafeGuard Easy supprime l'attribut Push du client SGE.

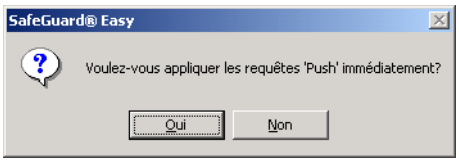
31.9.5 Commutation du client SGE en mode hors connexion

1. Appeler le menu **Postes de travail / Changer l'état à**.

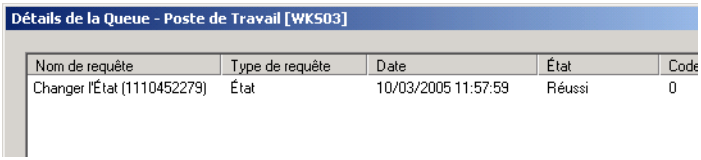
   Définir l'état sur
   a) Hors connexion
   b) Push [on]



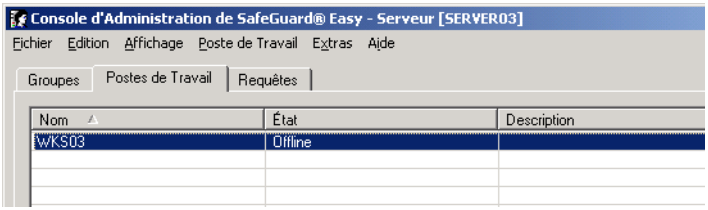
2. Si le client SGE doit être immédiatement commuté en mode OFFLINE, répondre par [OUI] dans la boîte de dialogue suivante.



3. Dans la file d'attente du client SGE, une requête de changement d'état et possédant l'attribut « Avec succès » est générée.

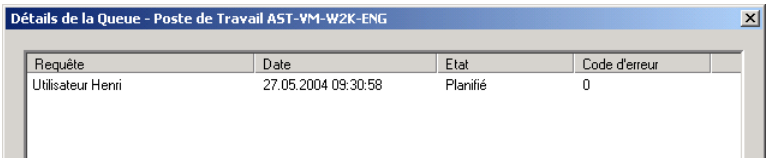


4. Le client SGE est alors dans l'état « Hors connexion ».

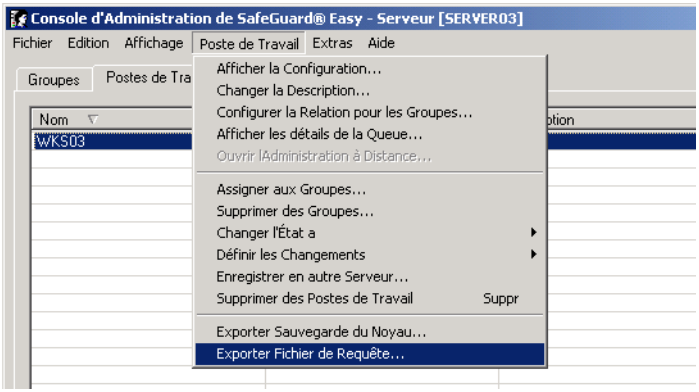


31.9.6 Création de mises à jour pour clients hors connexion dans la console d'administration

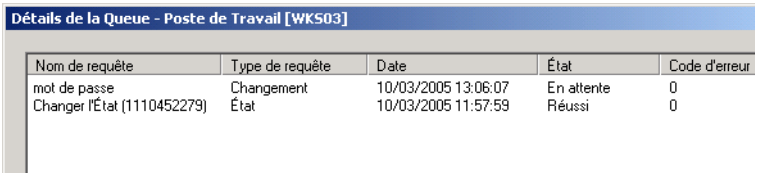
1. L'administrateur SGE, via le menu **Postes de travail / Définir les changements**, une mise à jour de configuration (« requête de changement »). Dans la file d'attente, la requête reçoit l'état « Planifié ».



2. L'administrateur SafeGuard Easy sélectionne l'option **Workstation/ Export Request File...** (Station de travail/Exporter le fichier de requête) pour exporter la requête dans un fichier (extension .req).

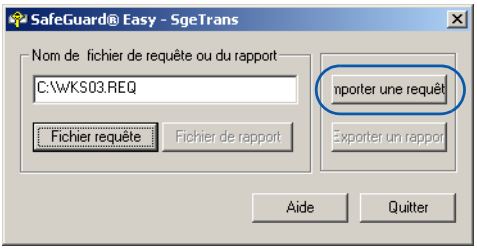


3. Dès que le fichier de requête est créé, l'état de la requête dans la file d'attente passe en mode « En attente ».



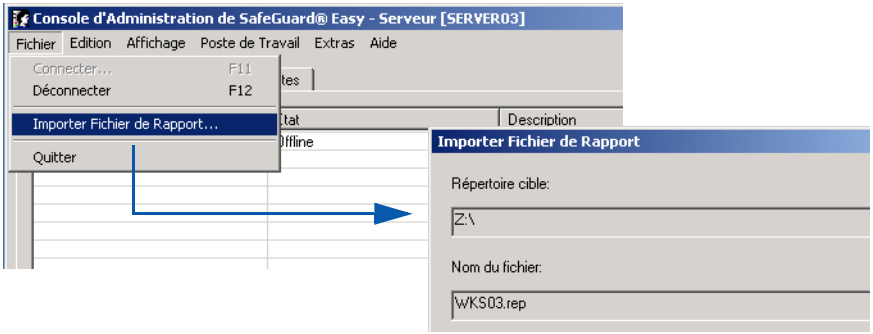
4. L'administrateur envoie le fichier de requête, par ex. par courrier électronique, à l'utilisateur du client Hors connexion.

5. L'utilisateur du client Hors connexion importe le fichier de requête avec SGETrans (voir également Charger mise à jour de configuration sur client Hors connexion avec SGETRANS (voir 'Chargement de mise à jour de configuration sur client Hors connexion avec SGETRANS').

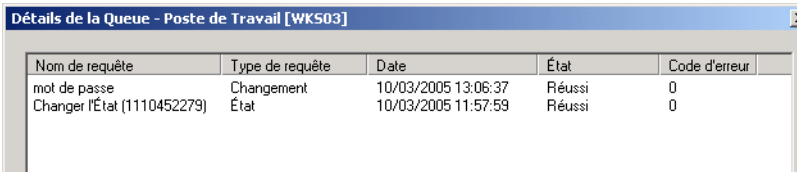


6. Indique à l'utilisateur du client Hors connexion si le fichier de modifications a été exécuté avec succès.
   En même temps, un « fichier de rapport » (extension .REP) est créé sur le client Hors connexion, envoyé par l'utilisateur à l'administrateur SafeGuard Easy.

7. L'administrateur SGE importe le fichier de rapport dans la console d'administration via le menu **Fichier / Importer fichier de rapport**.



8. Via la file d'attente (ou la page de propriétés du poste de travail), l'administrateur SGE voit si les modifications ont été exécutées avec succès.



31.9.7 Chargement de mise à jour de configuration sur client Hors connexion avec SGETRANS

Le programme sert d'interface pour l'échange de requêtes et de fichiers de rapport pour le travail avec clients hors connexion. SGETrans n'est présent dans le répertoire SGE que si l'option « Liaison serveur » a été sélectionnée à l'installation du client.

- **Fichier requête**
  Importe le fichier de requête que l'utilisateur reçoit par ex. par email de l'administrateur.
- **Importer une requête**
  Enregistre les paramètres du fichier de requête sur l'ordinateur de l'utilisateur.
- **Fichier de rapport**
  Définit un nom de fichier pour le fichier de rapport.
- **Exporter un rapport**
  Enregistre le fichier de rapport que l'utilisateur envoie à l'administrateur.

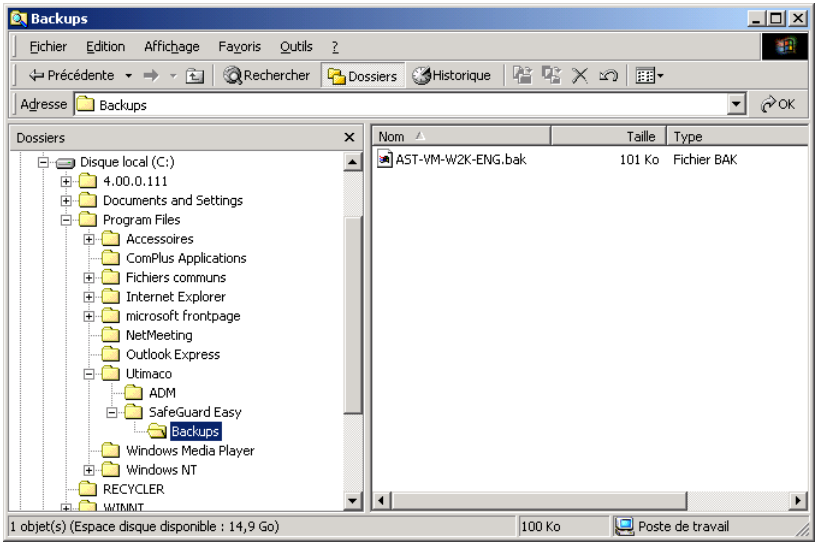
31.10 Sauvegarde automatique du noyau système

Le noyau système contient les fonctions nécessaires à l'authentification sur l'ordinateur, les pilotes requis pour le démarrage du système d'exploitation, ainsi que tous les paramètres système d'un client SGE. Une sauvegarde actuelle est nécessaire surtout dans les situations d'urgence, quand le noyau système d'un client SGE est endommagé et quand les utilisateurs ne peuvent plus ouvrir de sessions sur le système. Dans de tels cas, un noyau système intact du poste de travail concerné est nécessaire pour restaurer l'état initial et pour rétablir les capacités de fonctionnement du système ('Création de supports de restauration d'urgence et sauvegarde du noyau système').

Cette sauvegarde automatique du noyau système évite à l'administrateur la tâche de rappeler les sauvegardes nécessaires aux utilisateurs ou de les effectuer lui-même. C'est un mécanisme de sauvegarde automatique qui se charge de cette tâche dans le cadre de l'administration centrale. Il requiert du client SGE l'envoi d'une sauvegarde du noyau système au serveur SGE après un enregistrement avec succès.
Après des interventions dans la configuration SGE (par ex. via fichiers de configuration exécutés), le client effectue également la sauvegarde, l'envoie au serveur et écrase les anciennes données. La sauvegarde automatique garantit que l'administrateur ne dépend pas de la présence/absence des sauvegardes des utilisateurs en cas d'urgence.

31.10.1 Stockage du ou des noyaux système dans le répertoire BACKUPS

Dans la configuration de base, SafeGuard Easy enregistre le noyau système d'un client SGE sauvegardé dans le répertoire SGE de l'ordinateur qui contient la base de données SGE (en règle générale, le serveur SGE). Un dossier de sauvegarde est créé pour copier les noyaux système. L'affectation des sauvegardes aux postes de travail est très simple. Le nom du fichier se compose du nom du poste de travail enregistré et de l'extension .bak.



31.10.2 Indication d'un nouveau répertoire

Avec l'entrée de registre **BackupDirectory** dans

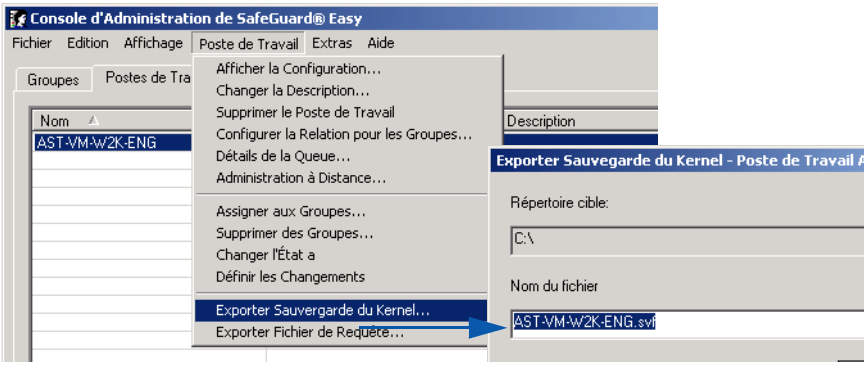
HKEY_LOCAL_MACHINE
SOFTWARE
Utimaco
SGEasy

un autre répertoire peut être défini. Le paramètre ne devient actif qu'après un redémarrage. De manière générale, il est possible d'entrer un chemin local ou UNC. Si vous entrez un chemin UNC, assurez-vous que vous disposez de droits suffisants (« Modification »).

L'entrée de registre doit être définie dans l'ordinateur contenant la base de données SGE.

31.10.3 Exportation de sauvegarde du noyau système

Les sauvegardes du noyau système de tous les clients SGE peuvent également être directement exportées par le biais de la console d'administration. Enregistrez le noyau système sauvegardé via le menu **Postes de travail/Exporter sauvegarde du noyau dans un fichier**. Le répertoire de destination, le nom de fichier et son extension peuvent être choisis à votre convenance.



Transmettez le fichier à l’utilisateur sur l’ordinateur duquel une erreur système s’est produite. Voir le chapitre pour apprendre comment des erreurs du système peuvent être réparées sur les postes de travail avec un noyau système intact ’Création de supports de restauration d’urgence et sauvegarde du noyau système’.

32 Administration à distance

Avec l'administration à distance, l'administrateur se connecte de son poste de travail avec un seul client SGE et adapte la configuration SGE en fonction des besoins. L'administrateur a ainsi directement accès au client SGE et peut procéder aux modifications comme s'il était connecté en local.

Les modifications via l'administration à distance agissent en partie directement sur le client SGE, comme par ex. au lancement du chiffrement/déchiffrement, d'autres requérant un redémarrage du client SGE.

L'administration à distance fonctionne indépendamment de l'administration centrale et est pratique pour des tâches d'administration dans des réseaux de moindre étendue. Elle peut être utilisée de façon autonome ou qu'élément intégral de la console Administration. L'administrateur peut l'utiliser pour effectuer les tâches suivantes :

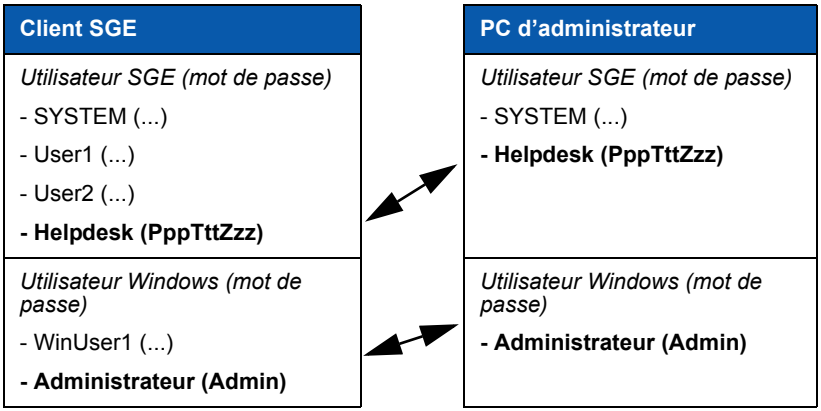
- Connexion à un client SGE ;
- Authentification sur le client SGE ;
- Modification des paramètres du client SGE ;
- Affichage des processus de chiffrement/déchiffrement sur le client SGE ;
- Enregistrement des paramètres ;
- Lancement de la sauvegarde de noyau système du client SGE.

La fonctionnalité d'administration à distance s'intègre dans l'administration SafeGuard Easy connue et appelle les mécanismes d'administration existants.

32.1 Conditions

La visualisation et l'édition des paramètres d'un client SGE sur l'ordinateur de l'administrateur sont uniquement possibles

- si une connexion réseau est établie entre l'ordinateur de l'administrateur et le client SGE.
- Le compte Windows avec lequel l'administrateur a ouvert une session sur l'ordinateur de l'administrateur existe sur le client SGE à l'établissement de la connexion, une ouverture de session automatique a lieu sur le client SGE. Lorsque le lien est mis en place, l'administrateur est connecté de façon automatique au client SafeGuard Easy.
- si au moins un utilisateur SGE identique (mot de passe inclus) a été créé sur le client SGE et sur l'ordinateur de l'administrateur
- si l'utilisateur de l'ordinateur d'administrateur ouvre sa session avec ces informations d'utilisateur SGE identique sur l'administration SafeGuard Easy via l'administration à distance.

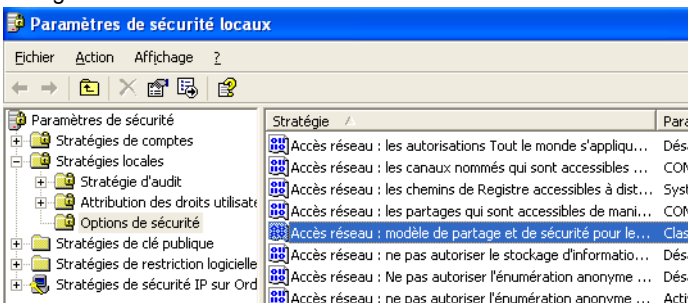


L'utilisateur SGE sur l'ordinateur de l'administrateur ne peut exécuter les tâches auxquelles son profil d'utilisateur l'autorise !

REMARQUE :

Le système d'exploitation Windows XP requiert les paramètres de sécurité locaux suivants sur les ordinateurs client et/ou administrateur :

« Accès réseau : modèle de partage de sécurité pour les comptes locaux = Classique - les utilisateurs locaux s'authentifient eux-mêmes ». Les paramètres de sécurité locaux sont ouverts par l'intermédiaire du Panneau de configuration/Outils d'administration/ Stratégie de sécurité locale.



32.2 Installation de l'administration à distance

Pour la configuration à distance des clients SGE, il est nécessaire d'installer l'administration à distance sur l'ordinateur (PC d'administrateur) à partir duquel vous souhaitez configurer les clients SGE.

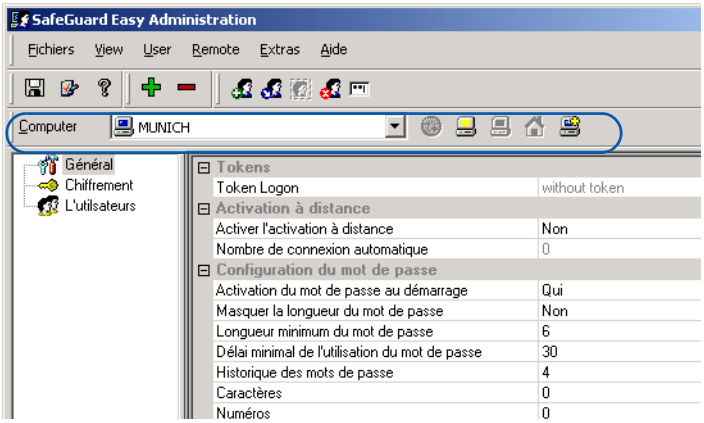
L'installation requiert ce qui suit :

1. Appelez `Sgeasy.msi` dans le répertoire du CD ...\CLIENT. Sélectionnez le type d'installation « Standard ».

2. Appelez `Server.msi` dans le répertoire du CD ...\SERVER. Sélectionnez l'option« Administration à distance ».

3. Assurez-vous qu'une connexion réseau est établie entre l'ordinateur de l'administrateur et l'ordinateur de l'utilisateur.

4. Lancez l'administration à distance via Démarrer / Programmes / Utimaco/ SafeGuard Easy / Administration.



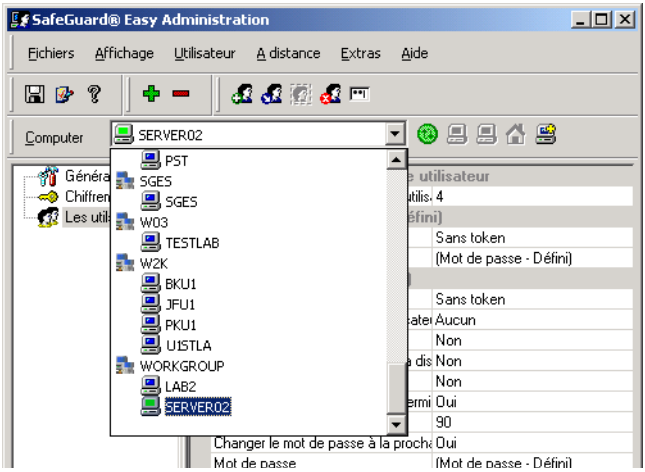
Après l'installation de l'administration à distance, SafeGuard Easy Administration possède les fonctions supplémentaires suivantes :

- sélection de clients via une liste d'ordinateurs ;
- mise à jour de la liste d'ordinateurs ;
- établissement / interruption de liaison avec le client ;
- saisie manuelle du nom de client n'apparaissent pas dans la liste d'ordinateurs ;

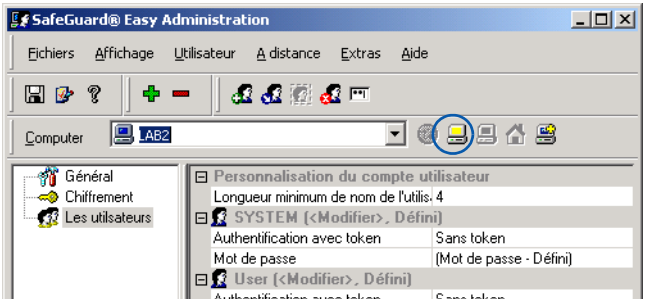
32.3 Connexion

1. L'utilisateur du PC administrateur ouvre une session dans l'administration SafeGuard Easy.

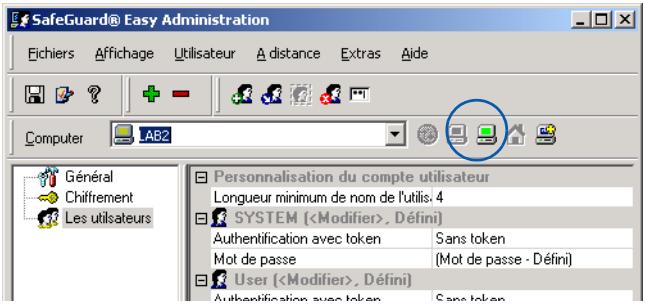
2. Dès que la liste d'ordinateurs est ouverte, elle est visible sur les ordinateurs connectés en réseau (domaines également).



3. L'ordinateur marqué en vert est l'ordinateur de l'administrateur. Quand un client est sélectionné dans la liste et quand vous cliquez ensuite sur l'ordinateur marqué en jaune, une connexion est établie entre l'ordinateur de l'administrateur et le client SGE.



4. Une fois la connexion établie avec succès, une ouverture de session automatique a lieu avec le client SGE, utilisant l'ID de l'utilisateur SafeGuard Easy qui s'est authentifié localement au démarrage de l'Administration SafeGuard Easy (dans notre exemple, « Helpdesk »).



5. Si une ouverture de session avec cet utilisateur SGE a échoué, l'utilisateur est invité à saisir des données valides.

33 Erreurs

Dans ce chapitre, vous trouverez une liste de tous les messages d'erreur. Comme à chaque message d'erreur de SafeGuard Easy le numéro d'erreur est affiché, il vous est facile de trouver le commentaire recherché.

Le format est le suivant : SGEnnnn : <texte>

« SGE » correspond à l'ID de produit SafeGuard Easy et « nnnn » est un code d'erreur à quatre chiffres.

Vous trouverez plus d'informations à ce sujet dans la base de connaissances Utimaco http://www.utimaco.com/myutimaco. Vous y trouverez des informations détaillées sur les messages d'erreur SafeGuard Easy suivants :
0104, 0113, 0400, 0401, 0404, 1048, 1062, 1074, 1089, 1104, 1109, 1121, 1123, 1244, 1254, 1264, 1274, 1306, 1315, 1509, 1602.
Veuillez utiliser la fonction de recherche (« Search ») de la base de données de connaissances pour rechercher des mots-clés comme « Messages d'erreur » ou des numéros d'erreur.

Erreur du produit

0001	Erreur fatale.
0002	Répéter
0100	Version différente de [PN] ou Crypton déjà installée.
0101	Lecture impossible du fichier de configuration.
0102	Fichier de configuration invalide.
0103	Écriture impossible du fichier de configuration.
0104	Le pilote installé n'est pas compatible.
0105	Pilote déjà installé.

0106	Ce programme ne peut pas être exécuté sous &0.
0107	Écriture impossible du fichier de sauvegarde.
0108	Lecture impossible du fichier de sauvegarde.
0109	Fichier de sauvegarde invalide.
0110	Installation impossible d'une seconde partition d'amorçage sur le disque.
0111	Installation impossible sur le Gestionnaire d'amorçage OS/2.
0112	Version antérieure de [PN] ou C :CRYPT déjà installée.
0113	Dernière opération d'installation, désinstallation ou mise à jour incomplète.
0114	Espace mémoire contigu insuffisant sur la partition d'amorçage.
0115	Accès impossible à la partition d'amorçage du pilote.
0116	Fichier de ressources introuvable.
0117	Ouverture impossible du fichier de ressources.
0118	Fichier de ressources erroné ou illisible.
0119	Le module algorithme manque.
0120	Le module noyau manque.
0121	Le module PBA manque.
0122	Création impossible de *AUTOUSER.
0200	Analyse impossible de la structure du disque dur.
0201	Erreur de lecture du disque dur.
0202	Erreur d'écriture sur le disque dur.
0203	Table de partition invalide sur le disque 0.
0204	Incompatibilité ROM BIOS.
0205	Secteur d'amorçage invalide.
0206	Verrouillage impossible du volume.
0300	Disque protégé en écriture.
0301	Unité inconnue.

0302	Le lecteur &0 n'est pas prêt.
0303	Commande inconnue.
0304	Erreur contrôle CRC.
0305	Longueur de structure de requête erronée.
0306	Erreur de recherche.
0307	Type de périphérique inconnu.
0308	Secteur introuvable.
0309	Plus de papier dans l'imprimante.
0310	Erreur d'écriture.
0311	Erreur de lecture.
0312	Erreur générale.
0320	Mémoire insuffisante.
0321	Erreur de division à l'adresse du programme &0.
0322	Dépassement de pile à l'exécution.
0500	Pilote de chiffrement non installé.
0501	Version incorrecte du pilote de chiffrement.
0502	Argument(s) de ligne de commande invalide(s).
0503	Aucune clé définie pour le déchiffrement.
0999	Erreur inconnue.

Erreurs du System API

1001	Aucun sous-système n'est actif.
1002	Changement invalide d'un paramètre système.
1003	Algorithme de chiffrement invalide ou manquant.
1004	Erreur interne décelée dans le sous-système.
1005	Le sous-système a signalé une erreur E/S.
1006	La tentative d'accès au noyau a échoué.
1007	Un utilisateur a déjà ouvert une session dans [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102].

1008	Un utilisateur incorrect a été défini.
1009	L'assignation de droits définis à l'utilisateur n'est pas autorisée.
1010	L'utilisateur défini existe déjà.
1011	Le mot de passe attribué a déjà été utilisé par cet utilisateur.
1012	Le mot de passe attribué fait partie de la liste des mots de passe interdits.

Erreurs de fichier

1031	Ouverture impossible du fichier %1.
1032	Fermeture impossible du fichier %1.
1033	Création impossible du fichier %1.
1034	Erreur d'écriture dans le fichier %1.
1035	Erreur de lecture du fichier %1.
1036	La tentative d'accès au fichier %1 a échoué.
1037	Fichier %1 introuvable.
1038	Chemin ou nom de fichier invalide.
1039	Espace mémoire insuffisant sur le disque.
1040	La partition du disque dur est trop fortement fragmentée.
1041	Détection d'un système de fichiers invalide.
1042	Détection d'un système de fichiers inconnu.
1043	Le fichier %1 existe déjà.
1044	Détection d'une structure erronée du système de fichiers.
1045	Détection d'une entrée invalide dans le système de fichiers.
1046	La demande d'informations de partition a échoué.

1047	Détection d'un système de fichiers inconnu ou invalide.
1048	Impossible de copier le fichier %1.
1049	Impossible de supprimer le fichier %1.
1052	Le contrôle CRC pour le fichier %1 a échoué.
1053	Impossible de renommer le fichier %1.

Erreurs d'installation

1061	Lecteur d'installation invalide.
1063	SafeGuard Easy est déjà installé.
1064	CardMan API n'est pas installé.
1065	Le fichier Config.sys est protégé en écriture.
1066	Entrée introuvable dans le fichier INI ou dans le fichier de configuration.
1067	Un système [PN] complet ou exécutable ne peut pas être installé avec des disques dynamiques.\n\nSeuls les utilitaires d'administration peuvent être sélectionnés pour l'installation.
1068	Impossible de créer le fichier de noyau.
1069	Impossible de modifier le fichier Config.sys.
1070	Impossible de copier le fichier %1.
1071	Aucun répertoire de destination n'a été défini.
1072	Un mot de passe d'administrateur système incorrect a été spécifié.\n\nVoulez-vous essayer à nouveau ?
1073	Aucun mot de passe d'administrateur système n'a été défini.
1074	En mode « double amorçage », le lecteur d'amorçage de Windows doit être défini sur « amorçable ».
1075	Le lecteur d'installation doit être chiffré pour le mode « double amorçage ».

1076	L’opération de désinstallation a échoué.\nVous trouverez des informations additionnelles dans le fichier Sgeasy.log.
1077	La désinstallation du système GINA a échoué.
1078	De nouveaux pilotes et services ont été installés. Nous vous recommandons fermement de créer maintenant une nouvelle sauvegarde parce que vous ne pouvez pas utiliser les anciennes sauvegardes pour la restauration lorsque SafeGuard Easy est installé !
1079	La désinstallation du client GINA SGEGINA a échoué.
1080	La suppression d’une entrée de menu système a échoué.
1081	La suppression d’une entrée de menu système a échoué.
1082	Entrée introuvable dans le fichier INI.
1083	L’installation de Cardman API a échoué.
1084	Pour le mode à double amorçage (Twin-Boot), le lecteur contenant le noyau doit être chiffré.
1085	Pour le mode « double amorçage », au moins un lecteur d’amorçage non chiffré doit être défini.
1086	Un système [PN] complet est déjà installé\nsur votre ordinateur, dans un autre système d’exploitation. Vous devez désinstaller ce système\navant de pouvoir désinstaller la composante exécutable du système d’exploitation actuel.
1087	L’installation d’un système [PN] n’est pas autorisée.
1088	Un fichier de ressources PBA requis (.MOD) n’a pas pu être trouvé !

1089	L'[i] de [PN] n'a pas été effectuée avec succès.\n\nL'échec de l'[i] est dû à l'erreur suivante :\n\n%1\n\nVeuillez cliquer sur le bouton OK pour supprimer tous les composants installés de [PN].\nEnsuite, un redémarrage automatique du système
1090	Détection d'une version incorrecte du système d'exploitation.\n\nLe système d'exploitation Windows NT v4.00 est requis.
1091	Détection d'une version incorrecte du système d'exploitation. \n\nLe système d'exploitation Windows 95/98/ME est requis.
1092	La procédure de désinstallation ne peut pas être démarrée car un ou plusieurs composants[[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102] sont actuellement inactifs.
1093	Ce processus ne peut pas être exécuté car une opération de chiffrement est actuellement en cours. Veuillez attendre que toutes les opérations de chiffrement soient terminées et redémarrer ce programme.
1094	Le processus de désinstallation est en cours. L'administration n'est plus possible.
1095	Nombre maximum de disques durs dépassé. \nInstallation de [PN] non prise en charge sur ce système.
1096	Quelques partitions non-DOS susceptibles d'être chiffrées avec le type d'installation sélectionné ont été trouvées.\nIl est donc recommandé de choisir le type d'installation 'Par partition'.
1097	Détection d'une version incorrecte du système d'exploitation. \n\nLe système d'exploitation Windows 2000 est requis.
1098	L'installation de SafeGuard Easy a échoué.
1099	La désinstallation de SafeGuard Easy a échoué.

Erreurs générales.

1101	Échec du test automatique.
1102	Initialisation impossible du système d'aide.
1103	Une classe n'a pas pu être enregistrée.
1104	Les informations sur la configuration de partition sont incohérentes.
1105	Paramètre invalide ou incorrect.
1106	Pas ou trop peu de paramètres ont été définis.
1107	Définition d'un paramètre inconnu.
1108	Capacité mémoire insuffisante.
1109	Impossible de charger le module '%1'.
1110	Impossible de créer une boîte de dialogue.
1111	Impossible d'initialiser une boîte de dialogue.
1112	Impossible de créer un thread.
1113	Impossible de créer une fenêtre.
1114	Vous devez posséder des droits d'administrateur pour l'installation ou la désinstallation.
1115	Une violation d'accès à la mémoire s'est produite !
1117	Impossible d'ouvrir le fichier journal '%1'.
1118	Vous ne pouvez pas exécuter simultanément les programmes Désinstallation et Administration de [PN].\n\nVeuillez quitter le programme en cours avant d'en démarrer un autre.
1119	Fichier noyau introuvable.
1120	L'installation du gestionnaire de contrôle a échoué.
1121	Définition d'une variable d'environnement inconnue.
1122	Impossible de définir une variable d'environnement.
1123	Taille de mémoire tampon insuffisante.

1124	Impossible de charger la bibliothèque de liaisons dynamiques ’%5’.
1125	La fonction ’%5’ spécifiée est introuvable.
1126	Impossible d’ouvrir le sémaphore ’%5’.
1127	Impossible de libérer le module ’%5’.
1128	Une exception s’est produite pendant l’exécution d’une\nfonction sous-système de [PN].\nCode dernière erreur :%1\nCode de retour fonction :%2\nModule :%3\nNuméro de ligne :%4\nAdresse :%5\nVeuillez contacter Utimaco Safeware AG !
1129	Une erreur critique s’est produite pendant l’exécution\nd’une ou de plusieurs fonctions sous-système de [PN].\n\nCode d’erreur fatale : %1\nCode d’erreur OS : %2\nModule : %3\nFonction : %4\nDescription : [[MSGLINK]=%1
1130	Impossible de libérer une mémoire allouée.
1131	Une fonction n’est actuellement pas prise en charge.
1132	Accès refusé.
1133	Le démarrage du programme ’%1’ a échoué.
1134	Fonction ou ressource non disponible.
1135	Processus interrompu par l’utilisateur.
1136	Entrée invalide ou incorrecte.
1137	Le système est actuellement en train de procéder à des changements de paramètres systèmes. Les nouveaux changements ne sont pas permis actuellement.
1139	Type de données non valide pour le champ de boîte de dialogue
1141	La sauvegarde du noyau a échoué.
1143	La station de travail définie n’existe pas

1144	Client d'ouverture de session « SgeGina.dll » introuvable. Ce composant est vital pour le fonctionnement de[PN]. Sa suppression ou sa désactivation peuvent causer de sérieux problèmes requérant une nouvelle installation de [PN] ou du système d'exploitation.
1145	Service « SgeCtl.exe » introuvable. Ce composant est vital pour le fonctionnement de base de[PN]. Sa suppression ou sa désactivation peuvent causer de sérieux problèmes requérant une nouvelle installation de [PN] ou du système d'exploitation.
1146	Le noyau système est altéré !
1147	Une opération de chiffrement ou de déchiffrement du disque dur est en cours d'exécution ou une opération de ce type a été initialisée.\nVous ne pourrez effectuer une sauvegarde du noyau que lorsque toutes ces opérations auront été achevées.
1148	Impossible de trouver l'interface sur le système.\n\nIdentifiant de classe :%1 (%3)\nInterface :%2\nRésultat :%4 ([[OSERRLINK]=%5])\n\nIl est possible que [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102] ne soit pas installé sur '%6' !

Erreurs de fichier de configuration.

1151	Fichier de configuration %1 introuvable.
1152	Aucun fichier de configuration défini.
1153	Fichier de configuration invalide.
1154	Entrée invalide détectée dans le fichier de configuration.
1155	Impossible de créer le fichier de configuration %1.
1156	Erreur décelée à la ligne %1 du fichier de configuration.

1158	Le fichier de configuration spécifié est introuvable !
1159	Une commande inconnue a été trouvée dans le fichier de configuration.
1160	Un type de fichier de configuration inconnu a été détecté.
1161	Le type de fichier de configuration est invalide.
1162	Impossible de créer l'identificateur pour le fichier de configuration.
1163	Impossible de créer le fichier de configuration pour la désinstallation.
1164	Impossible de créer le fichier de configuration pour l'installation.
1165	Fichier de configuration %1 introuvable.
1166	Le type de fichier de configuration est invalide.
1167	L'exécution du fichier de configuration '%1' a échoué.

Erreurs de contrôle MESSAGE.

1171	ID message %1 introuvable.
1172	Texte de contrôle pour introuvable pour l'ID de contrôle.
1173	Impossible d'écrire le journal des événements de Windows NT.
1174	Un lien fichier ou message invalide a été détecté :\n\nIndentificateur de message : %1\nCommande de lien : %2.
1175	Le format du fichier de message '%1' est invalide.
1176	Erreur de mot de passe.

Erreurs liées au mot de passe

1181	Aucun mot de passe d'administrateur système n'est défini.
1182	Mot de passe inconnu. Veuillez retaper votre mot de passe.
1183	Aucun mot de passe n'est défini.
1184	Le mot de passe défini est trop court.
1185	Le mot de passe défini est trop long.
1186	Les mots de passe définis ne correspondent pas.
1187	Le mot de passe est faible.\nVoulez-vous entrer un autre mot de passe ?
1188	Un autre utilisateur possède déjà ce mot de passe. \nVoulez-vous l'utiliser quand même ?
1189	Le mot de passe ne contient pas le nombre requis de caractères, des caractères de casse différente, des caractères avec des chiffres et des symboles.
1190	Le mot de passe n'a pas encore atteint sa durée minimale définie.

Erreurs de clé

1201	Une clé de disque dur n'est pas encore définie.\n\nL'activation du déchiffrement pour des partitions de disque dur n'est pas autorisée\ntant qu'aucune clé n'est définie pour ces disques durs.
1202	Une clé de lecteur de disquette n'est pas encore définie.\n\nL'activation du déchiffrement pour des lecteurs de disquettes n'est pas autorisée\ntant qu'aucune clé n'est définie pour ces lecteurs.
1203	Une clé de périphérique amovible n'est pas encore définie.\n\nL'activation du déchiffrement pour des périphériques amovibles n'est pas autorisée\ntant qu'aucune clé n'est définie pour ces périphériques.
1204	La clé définie est trop longue.

1205	La clé définie est trop courte.
1206	Les clés définies ne correspondent pas.
1207	Aucune clé n'a été définie.
1208	Le mode de protection de zones d'amorçage requiert\nune clé de chiffrement pour le disque dur.
1209	Le mode Disques complets requiert une\nclé de chiffrement pour le disque dur.
1210	La clé est banale.\nVoulez-vous en définir une autre ?

Erreurs IPC

1221	Impossible de démarrer le serveur IPC.
1222	Impossible de démarrer le client IPC.
1223	Impossible d'établir la communication IPC.
1224	Impossible d'appeler le message IPC.
1225	Impossible d'attribuer le message IPC.
1226	La fonction IPC IPC_SGE_PROCESS_DEF_MSG\nn'a pas pu être traitée.
1227	Impossible de fermer le serveur IPC.
1228	Impossible de fermer le client IPC.
1229	Impossible de démarrer le thread IPC.
1230	L'attente d'un message IPC a échoué.
1231	Objet de communication IPC introuvable.

Erreurs de lecteur.

1241	Lecteur inconnu ou invalide.
1242	Autres lecteurs introuvables.
1243	L'opération E/S lecteur a échoué.

1244	La tentative de lecture d'un lecteur a échoué.
1245	La tentative d'écriture sur un lecteur a échoué.
1246	La tentative d'accès à un lecteur a échoué.
1247	Lecteur non prêt.
1248	La tentative de verrouillage d'un lecteur a échoué.
1249	La tentative de déverrouillage d'un lecteur a échoué.
1250	La partition système doit être une partition primaire.\n\nCeci est par exemple nécessaire si l'option « Accès à la partition de configuration Compaq » est active.
1251	Le démontage d'un volume a échoué.\n\nDes fichiers ou fenêtres du volume sont peut-être encore ouverts.
1252	Le premier disque physique n'est pas un disque dur.
1253	Toutes les entrées de la table de partition du secteur MBR sur le premier disque dur sont déjà utilisées.\n\nL'option « Accès à la partition de configuration Compaq » requiert une entrée de table de partition libre !
1254	Le système a démarré en mode compatible.
1255	Pour installer SafeGuard Easy, veuillez retirer le disque dur connectable.
1256	Aucun lecteur de ce type n'est disponible.
1257	Erreur interne lors de l'accès à la partition système

Erreurs SERVICE

1261	Des informations sur un objet de mémoire pour un service système\nn'ont pas pu être débloquées.
1262	Erreur décelée dans le répartiteur du service système.
1263	Impossible de démarrer le service système.
1264	Impossible de modifier l'état du service système.

1265	Impossible d'enregistrer la routine pour le service système.
1266	La fonction d'initialisation du service a signalé une erreur.
1267	Bloc d'information de service introuvable.\nLa mémoire est vraisemblablement insuffisante.\n\nCode d'erreur : %1.

Erreurs BASE DE REGISTRES

1271	Impossible d'ouvrir l'entrée dans la base de registres.
1272	Impossible de lire l'entrée dans la base de registres.
1273	Impossible d'écrire l'entrée dans la base de registres.
1274	Impossible de créer l'entrée dans la base de registres.
1275	Impossible de supprimer l'entrée de la base de registres.
1276	L'entrée pour le service système dans la base de registres\nn'a pas pu être ouverte.
1277	L'entrée pour le service système dans la base de registres\nn'a pas pu être créée.
1278	L'entrée pour le service système dans la base de registres\nn'a pas pu être supprimée.
1279	L'entrée pour le service système dans la base de registres\nexiste déjà.
1280	Impossible d'ouvrir le 'Session Control Manager'.
1281	L'entrée pour une session dans la base de registres\nn'a pas pu être trouvée.
1282	Entrée invalide détectée dans la base de registres.

Erreur de base de données de pilotes.

1291	Autres pilotes de chiffrement introuvables.

1292	Base de données de pilotes introuvable.
1293	Erreur survenue à la lecture de la base de données de pilotes.
1294	La base de données de pilotes est vide.
1295	Entrée illégale ou invalide dans la base de données de pilotes.

Erreurs CRAREA

1301	Accès impossible au lecteur d'installation.
1302	La demande d'informations de partition a échoué.
1303	La tentative d'accès à la partition d'amorçage a échoué.
1304	Option de processus invalide.
1305	Définition d'un système de fichiers inconnu ou invalide.
1306	Différence notée entre le type de système de fichiers actuel\net le type de système de fichiers défini.
1307	Différence notée entre la taille de cluster actuelle et\nla taille de cluster définie.
1308	Cluster de démarrage invalide pour la zone de noyau.
1309	Secteur de démarrage invalide pour la zone de noyau.
1310	Type de partition invalide.
1311	Clusters libres introuvables pour le noyau.
1312	Impossible de marquer les clusters comme « utilisés ».
1313	Impossible de marquer les clusters comme « corrects ».
1314	Impossible de marquer les clusters comme « non utilisés ».
1315	Impossible de marquer les clusters comme « incorrects ».

1316	Les informations sur les clusters sont altérées.
1317	Zones marquées comme « incorrectes » introuvables.
1318	Taille de zone de noyau invalide.
1319	Impossible de remplacer le secteur MBR sur le 1er disque dur.

Erreurs SGOCA

1401	Les informations requises pour la zone de communication d'objet existent déjà.
1402	La zone de communication d'objet existe déjà.
1403	Les informations requises pour la zone de communication d'objet existent déjà.
1404	Zone de communication d'objet introuvable.
1405	Les informations requises pour la zone de communication d'objet n'existent pas.
1406	Informations d'objet supplémentaires trouvées.

Erreurs SGUICL

1511	La configuration des composants n'a pas pu être chargée !

Erreurs ADMLOGON

1601	La tentative d'ouverture de session a échoué. Essayez à nouveau.
1602	Le sous-système [PN] n'autorise pas plus de 5 tentatives d'ouverture de session. Vous devez redémarrer votre ordinateur pour relancer cette application.

1603	La tentative de démarrage de la composante d'ouverture de session de [PN] a échoué.
1604	
1605	L'ouverture de la session [PN] s'est effectuée avec succès, mais vous\nne possédez pas les droits suffisants pour désinstaller le produit.

Erreurs Administration - USER

1801	L'utilisateur '%1' ne peut pas être créé car\nle nombre d'utilisateurs maximum est atteint.
1802	Il n'est pas possible de créer ou de supprimer le '*AUTOUSER'.
1803	L'utilisateur '%1' existe déjà. Veuillez spécifier un autre nom d'utilisateur.
1804	Le nombre d'utilisateurs maximum a été dépassé.
1805	Il n'est pas possible de créer ou de supprimer le profil d'utilisateur\n'SYSTEM'. Il est seulement permis de le modifier.
1806	Le profil d'utilisateur requiert un Token pour l'ouverture de session dans [[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102].
1807	L'application a été bloquée pendant plus de 30 secondes, car elle attend un appel pour se terminer. Dans la plupart des cas, ceci se produit lorsque l'ordinateur est occupé. Voulez-vous attendre jusqu'à ce que l'application soit prête, ou terminer l'appel ?

Erreurs de l'Assistant de migration

2001	L'Assistant Migration n'a pas pu être initialisé

Erreurs SGEGINA

2100	La tentative d'ouverture automatique de session a échoué.\n\nVoulez-vous modifier la relation actuelle entre l'utilisateur de [PN]\net l'utilisateur du système d'exploitation ?
2101	Vous devez modifier votre mot de passe. \nLa connexion automatique (SAL) sera désactivée au cours de cette session de connexion !

Erreurs de désinstallation

2201	La procédure de désinstallation ne peut pas être démarrée car une\nopération de chiffrement ou de déchiffrement est actuellement en cours !
2202	Le désenregistrement d'un composant a échoué !
2203	La procédure de désinstallation ne peut pas continuer, car au moins une partition étrangère de disque dur a été détectée. La désinstallation de [[MSGFILE]=SGE_INFO.dll][[MSGLINK=102] ne peut pas se poursuivre.

Erreurs d'installation étendue

2301	Le programme d'installation possède le mauvais numéro de version et n'a pas pu être utilisé !
2302	Pour l'installation en mode « Disques complets » ou « Protection des zones d'amorçage », le nombre maximum de partitions par disque dur est de 8 !
2303	L'enregistrement du composant a échoué !

2304	L’installation de [PN] requiert Microsoft’s Windows Installer !\nVeuillez lire le fichier LISEZMOI pour la manière d’installer Windows Installer.
2305	Détection d’une version incorrecte du système d’exploitation.\n\nLe système d’exploitation Windows NT/2000 est requis.

Erreurs de l’Assistant de création de disquette de démarrage

2401	La création du fichier de sauvegarde de noyau a été annulée !
2402	Tous les outils de secours n’ont pas pu être copiés avec succès !

Erreurs SAL

2501	Impossible d’ouvrir le fichier SAL.
2502	Le fichier SAL est dans un état indéfini.
2503	Une erreur indéfinie s’est produite lors d’opérations sur le fichier.
2504	Impossible de positionner correctement le fichier SAL.
2505	Erreur à la lecture du fichier SAL.
2506	Erreur à l’écriture du fichier SAL
2507	L’utilisateur spécifié est introuvable.
2508	Aucune utilisateur actuellement connecté n’a été trouvé.
2509	L’écriture dans le fichier SAL a échoué. L’enregistrement existant doit avoir la même taille.
2510	Le tampon de destination est trop petit pour toute l’entrée.
2511	Pas de mémoire disponible.

Erreurs de la base de données

2601	L'écriture de données dans la base de données a échoué !
2602	La lecture de données de la base de données a échoué !
2603	La création d'une entrée dans la base de données a échoué !
2604	La suppression d'une entrée de la base de données a échoué !
2605	La base de données est inaccessible !

Erreurs Interface

3001	Impossible de chiffrer l'interface COM spécifiée.\nNom de l'interface :%1\nNuméro d'erreur : %2\n\nDétails :\n%3
3002	L'exécution d'une méthode d'interface a échoué. Les détails suivants sont disponibles :\nNuméro d'erreur : %1\nhRésultat : %2\nDescription : %3\nInterface :%4\Veuillez contacter votre administrateur système !

Erreurs Client/Server

3201	Le serveur ou client est actuellement occupé et n'est pas capable d'exécuter la requête.

Erreurs Administration Console

3301	La liaison avec la base de données a échoué !
3302	Interface de console serveur introuvable !

3303	Interface d’administrateur à distance introuvable !
3304	Impossible de trouver l’interface de l’assistant de configuration des fichiers !