made**Safe**™

madesafe

User Guide

www.madesafe.com

Table des matières

Chapitre 1 Démarrer avec madeSafe Companion

De quoi madeSafe est-il capable?

- de garder vos information personnelles et d'entreprise à l'abri, en sécurité et bien cachées.
- de protéger votre PC contre les hackers.
- d'envoyer des courriels en toute sécurité.
- d'accepter vos commandes vocales.
- de gérer vos besoins en sécurité à partir d'une interface facile à utiliser.
- de protéger vos enfants sur Internet.
- de stocker et récupérer tous vos documents sécurisés où que vous soyez dans le monde …même si votre PC a été volé!
- Utilisez la fonctionnalité madeSafe multi-utilisateur … Ajoutez des utilisateurs additionnels à tout moment pour mettre votre entreprise ou votre famille en sûreté.
- Choisissez dans une gammes de fonctions additionnelles & mises à niveau pour personnaliser madeSafe selon vos besoins spécifiques.
- Elargissez votre environnement sécuritaire à tout moment… Profitez de notre gamme complète de services & options.

Nous nous engageons à faire en sorte que madeSafe vous fournisse le top de la protection et de la sécurité des données. madeSafe est un logiciel d'encodage leader sur le plan mondial qui met en œuvre l'intelligence artificielle pour vous aider à définir et à créer votre propre espace ou cellule personnels. Votre version est unique et capable d'évoluer avec vous pour faire face aux menaces de plus en plus sophistiquées.

Votre Security Companion

madeSafe Security Companion™ est une console étudiée pour la conjonction des opérations d'encodage avec un tableau de bord facile à utiliser. Vous êtes toujours à un clic des produits et des services qui mettent votre PC en sécurité et vous donnent une tranquillité absolue.

Le Security Companion™ de madeSafe a quatre secteurs de fonctionnalité distincts. Groupés en un format logique, ils sécurisent vos données et optimisent les performances de votre PC.

- Boutons de profil & progrès
- Instruments d'optimisation & de stockage
- Fenêtres document, disque & répertoires
- Encodage

Encodage

Encodage 128-bit par simple clic, ultrarapide, leader mondial. Vitesse et puissance d'encodage entièrement réglables. Protégez vos informations personnelles et professionnelles confidentielles des hackers et des utilisateurs non autorisés.

Courriels sécurisés

Envoyez des pièces jointes de courriels super-encodées partout dans le monde en toute tranquillité. Même si le destinataire n'a pas madeSafe.

Instruments puissants

Une gamme puissante d'outils de sécurité: -

Scannez – Scannez le lecteur sélectionné à la recherche de matériel que vous interdisez.
Nettoyez – Effacez les groupes de documents périmés (faites de la place sur votre disque dur) et effacer les traces de vos manipulations au clavier (pour empêcher les hackers de découvrir les documents sécurisés, les nouveau documents et leurs coordonnées).

Detruire – Déchiquetez définitivement tout document sans possibilité de récupération.

Stealth – Pour accéder au summum de la sécurité, utilisez la technologie Active Stealth unique de madeSafe pour masquer vos données encodées les plus importantes et les rendre invisibles.

Filtre Internet – madeSafe Shield

Voici les fonctions-clés de SHIELD:

- ✓ Blocage des sites web répréhensibles.
- ✓ Filtrage des sites par banque de données des URL et Meta Tags I.E: - (mot-clés & description).
- ✓ Mise à jour permanente de la banque de données des URL de sites bloqués.
- ✓ Désactivation des fenêtres pop up.
- ✓ Contrôle parental/administrateur complet (le logiciel ne peut pas être désactivé par les utilisateurs normaux).
- ✓ Personnalisation des URL et des mots-clés.
- ✓ Suivi des utilisateurs qui essaient d'accéder à des sites bloqués.
- ✓ Fonctionnement discret dans la barre de tâches.
- ✓ Compte-rendu de tout le trafic Internet (sites visités, temps et utilisateurs

Stockage & récupération haute sécurité
Utilisez Ch@mbre Forte pour placer une copie de vos informations confidentielles les plus importantes sur notre site web madeSafe haute sécurité. Back up et récupération des données sécurisées dans le monde entier, 24 heures par jour, 365 jours par an.
Vous êtes le seul à avoir accès.

Cellules multi-utilisateur – prêtes à la mise en réseau
Licences d'utilisateur additionnelles – protection et sécurité des données à l'échelle de l'entreprise.
Agrandissez votre madeSafe Business en ajoutant des utilisateurs. Chaque mise à niveau st livrée avec trois licences d'utilisateurs.

Services & Options

Pour une tranquillité totale, nous offrons une large gamme de services: -

Protection contre la perte du mot de passe
Si vous avez peur de perdre les mots de passe de vos données sécurisées, nous les stockons pour vous dans notre coffre-fort codé haute sécurité.

Audit Sécuritaire
Téléchargez notre logiciel d'audit sécuritaire pour savoir si votre PC ou votre réseau est vraiment en sûreté.

Détecteur de vol
Si votre PC est volé, cet instrument vous envoie automatiquement un e-mail dès que quelqu'un s'est connecté sur Internet pour vous annoncer qu'il a été volé.

madeSafe Care
Soutien par téléphone – nous vous offrons le meilleur soutien technique et vous aidons à tirer le meilleur parti de votre produit madeSafe.

madeSafe Cover
Assurance – profitez de notre assurance complète mondiale pour votre portable ou votre PC.

Mises à niveau & mises à jour

Une vie de sécurité – pour les mises à niveau de produits, les mises à jour gratuites, les réductions et offres spéciales.

Mise à niveau Ch@mbre Forte – Dites-nous de combien d'espace vous avez besoin et ajoutez-en à tout moment.

Mise à niveau du filtre Internet – Obtenez des mises à jour régulières de votre filtre Internet, mettez-vous à jour et à l'abri du matériel répréhensible.

Installation de madeSafe

Equipement nécessaire

madeSafe se greffe sur le système Microsoft Windows. Les utilisateurs déjà habitués à utiliser Windows apprécieront que le Security Companion de madeSafe est étudié pour compléter votre tableau de bord habituel.
Avant d'installer madeSafe, assurez-vous que vous avez au moins l'équipement minimum ci-dessous:

équipement minimum pour l'installation de madeSafe:

- IBM™ PC ou compatible
- Microsoft® Windows 95, 98, 2000, NT, ME ou Windows XP
- Processeur 486 ou plus
- 16MO de RAM
- 100MO sur le disque dur
- Un logiciel de navigation (de préférence IE4 ou Netscape 4 ou ci-dessus)
- VGA ou plus avec 256 couleurs
- CD-ROM
- Accès Internet avec un compte E-mail valable
- Carte son et & microphone (en option)

Installation

Veuillez suivre les indications ci-après pour installer votre produit madeSafe

Installer:

1 Démarrer Windows (s'il ne l'est pas déjà).

2 Insérer le CD madeSafe dans le lecteur de CD-ROM.

3 Sur l'écran, cliquez Installer madeSafe et suivez les instructions à l'écran.

Installation & enregistrement

Une fois installé, le programme vous demandera d'ouvrir un compte de maître\administrateur. Inscrivez simplement votre nom, votre adresse e-mail et un mot de passe d'au moins 8 caractères confirmé. (IMPORTANT! N'OUBLIEZ PAS VOTRE MOT DE PASSE) et inscrivez le numéro-clé du CD pour vous enregistrer.

Cette information parviendra à notre serveur qui vous donnera un code d'activation (dans un e-mail sécurisé). Tapez le code dans la case d'activation box, (le mieux est de copier-coller), puis cliquer sur activation. Cette action entraîne le téléchargement de composantes vitales qui vous permettent d'utiliser votre produit.

Chapitre 2 Configuration du Security Companion

L'utilisateur maître aura été installé pendant la procédure d'installation et d'enregistrement.
Le mot de passe maître ne peut pas être changé, mais le nom peut changer. Pour ce faire, marquez simplement le nom, tapez le nouveau nom puis cliquez sur «effectuer le changement».
Pour ajouter un utilisateur, cliquez sur le menu utilisateur, sélectionnez un nouvel utilisateur, puis entrez le nom et le mot de passe. Ensuite, cliquez sur «effectuer les changements».
Pour effacer un utilisateur, c'est tout aussi simple. Sélectionnez l'utilisateur à partir du menu et cliquez «effacer l'utilisateur sélectionné». Cliquez sur terminer pour retourner au menu principal.
L'utilisateur maître a accès à tous les documents des autres utilisateurs.

Réglages business

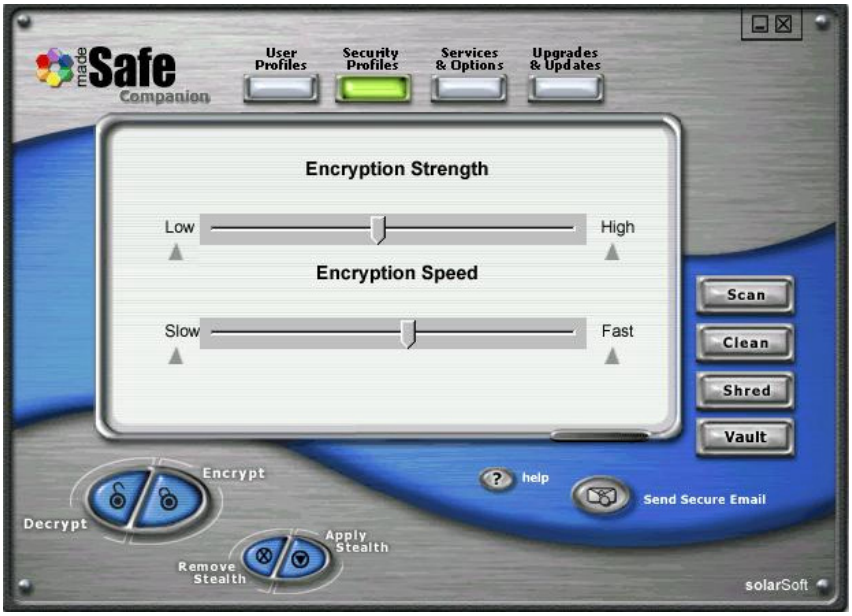
L'utilisateur maître doit installer & activer madeSafe Companion sur son ordinateur. Il doit ensuite installer madeSafe Companion sur les ordinateurs des utilisateurs subordonnés. Cette fois, pendant l'installation, au lieu d'insérer la clé du CD, l'utilisateur maître tape «Network» et clique sur activer.
Il reçoit ensuite l'injonction de naviguer sur le réseau pour localiser l'installation de l'utilisateur maître.
c.-à-d. \\Admin\C:\ProgramFiles\solarsoft\madesafe.
Note – Veuillez vous assurer que le disque sur l'ordinateur de l'utilisateur maître est partagé.
Une fois que le répertoire est localisé, cliquez "OK" pour terminer l'installation.
L'utilisateur maître peut alors administrer tous les comptes à partir de sa machine.
L'utilisateur maître peut se connecter à n'importe quelle machine où madeSafe est installé (en utilisant un deuxième ou un troisième nom et mot de passe), et accéder à toutes les données encodées.

ATTENTION: - N'ESSAYEZ PAS DE DÉCODER DES DONNÉES QUE VOUS N'AVEZ PAS ENCODÉES **VOUS-MÊME**!!!

c.-à-d. – LORSQU'UN DEUXIÈME UTILISATEUR ESSAIE DE DÉCODER UN DOCUMENT ENCODÉ PAR L'UTILISATEUR MAÎTRE, CECI ENTRAÎNE LA DESTRUCTION DU DOCUMENT!!!

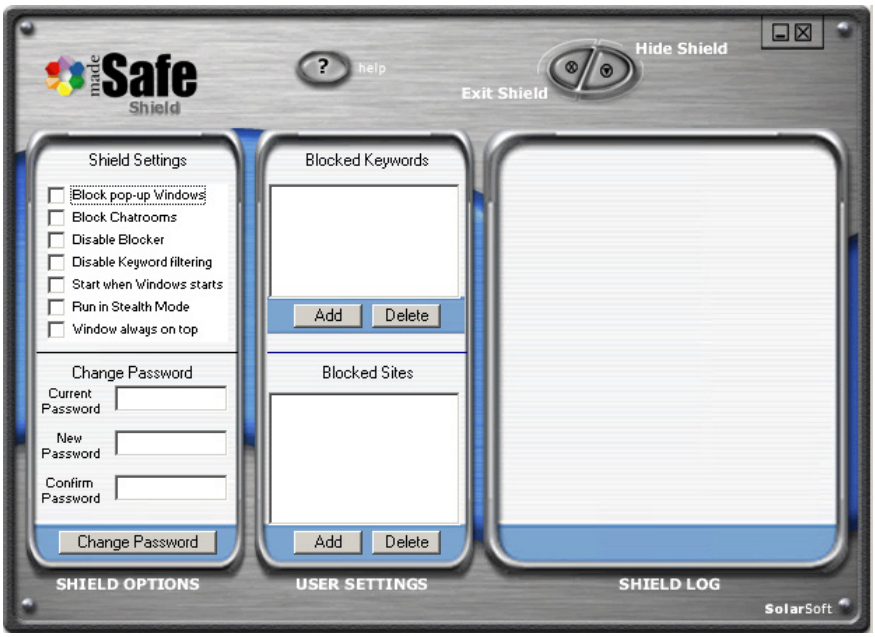
Profils de sécurité

Trois options sont présentées ici: réglage de l'encodage, filtrage et banque de données.
Le réglage de l'encodage a deux barres à glissière (voir ci-dessous), avec lesquelles vous pouvez déterminer la puissance et la vitesse de l'encodage. Si vous augmentez la puissance, la vitesse diminue, et vice-versa.



Filtre Internet

Réglage du filtre – Vous pouvez personnaliser complètement la manière dont votre machine surfe sur Internet grâce à ces options. Seul l'utilisateur maître peut configurer les options de filtrage.



Lorsque vous accédez au Shield à partir de la barre de tâches, un mot de passe vous sera demandé. Le mot de passe par défaut est Password. Il peut être modifié au moment voulu.

Options de filtrage

Bloquer les fenêtres pop-up – utilisez cette fonction pour stopper les publicités dérangeantes.
Bloquer les chat-rooms – cette fonction annule l'accès à tous les chat-rooms.
Désactiver le blocage – le programme de filtrage est désactivé.
Désactiver le filtrage par mots-clés - cette fonction vous donne la liberté de désactiver le filtrage des mots-clés.
Start up – cette fonction charge le filtre automatiquement en même temps que Windows.
Stealth – le programme fonctionne discrètement en arrière-plan.
Windows toujours en surface – option de maintien de Shield en surface de l'écran.
Mots-clés bloqués – madeSafe a une liste de mots-clés standard; vous pouvez ajouter des mots-clés à cette banque de données selon vos préférences.
Sites bloqués – cette option vous permet d'ajouter des sites web que vous interdisez.

Shield Log – Ce journal vous permet de visualiser l'activité Internet de l'ordinateur. L'information enregistrée concerne le nom, la date, l'heure et les sites consultés.

Banque de données de sécurité

Cette fonction permet à l'utilisateur maître de personnaliser les réglages de sécurité. Si, par exemple, votre entreprise s'occupe de ventes de voitures et que vous ne souhaitez pas que le public connaisse vos marges, ajoutez simplement «marges» à votre banque de données et madeSafe refusera l'accès à tout document concernant les «marges», sauf à l'utilisateur maître. Vous pouvez ajouter un nombre illimité de mots-clés à la banque de données pour une totale tranquillité.

Encodage

L'encodage n'a jamais été aussi facile. Sélectionnez simplement votre disque, ensuite le répertoire où se trouve le document, puis sélectionnez le/s document/s que vous souhaitez coder et cliquez sur le bouton d'encodage.

C'est tout! Maintenant, ces documents ne sont accessibles **qu'à vous**.

Pour déverrouiller (décoder) un document, c'est tout aussi simple. Sélectionnez les documents encodés, et cliquez sur décoder.

Les documents décodés sont identifiables par leur extension .ENC

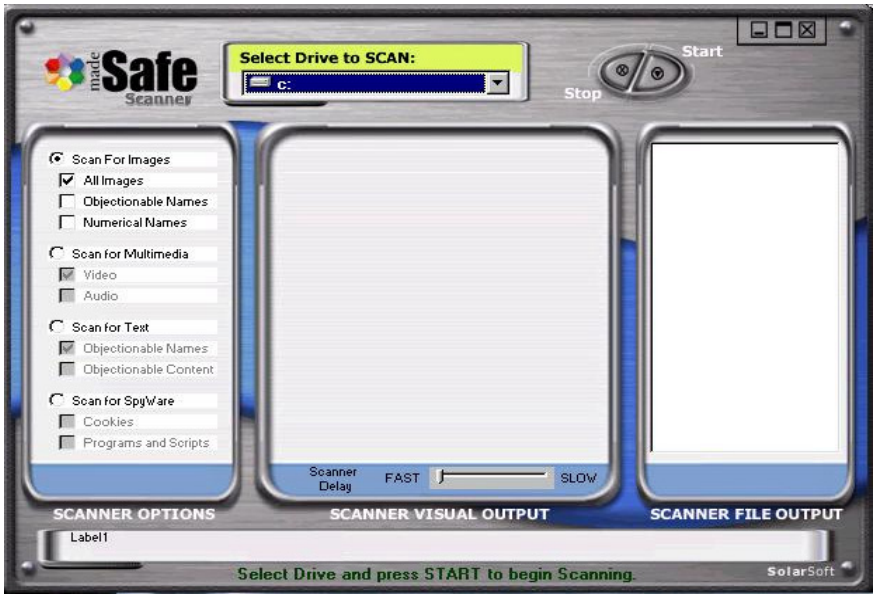
Stealth

Pour le summum de la sécurité, vous pouvez appliquer Stealth à vos documents encodés. Cette fonction rend invisible les documents encodés pour le navigateur occasionnel sur disques durs. Il suffit de sélectionner le répertoire ou se trouvent les documents encodés, et de cliquer sur «appliquer Stealth». Les documents deviennent invisibles.

Pour voir des documents masqués, il suffit de sélectionner le répertoire où ils se trouvent, et de cliquer le bouton «enlever Stealth».

Scannez

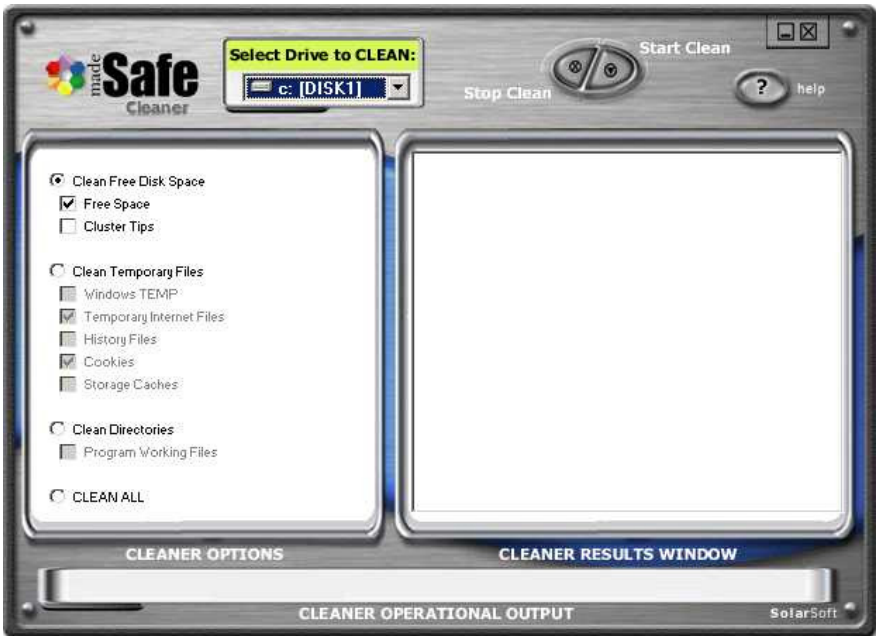
Cette fonction scanne votre disque dur à la recherche de divers types de matériel répréhensible. Vous pouvez chercher des images, des vidéos ou du texte, en fait toute sorte de document que vous considérez comme répréhensible ou dangereux.



Il suffit de sélectionner le type de scannez que vous voulez et de cliquer sur «Démarrer». La fenêtre centrale affichera les documents trouvés, et cette procédure peur être ralentie pour les visualiser. Dans la fenêtre de droite, une liste de documents trouvés est affichée que vous pouvez analyser à loisir.

Nettoyer

Cette fonction nettoie le disque et fait de la place sur votre machine. Elle efface les groupes de documents périmés et supprime les traces de manipulation au clavier pour empêcher les hackers de découvrir les mots de passe et les documents. L'idéal est d'utiliser cette fonction après avoir déchiqueté un/des document/s. Comme cette fonction est très systématique, elle peut prendre du temps à s'exécuter, selon l'option que vous avez sélectionnée.



Detruire

Le déchiquetage: un outil très puissant qui détruit complètement tout document sur votre machine. Avant de l'utiliser pour un document, sachez qu'un document déchiqueté ne peut plus jamais être récupéré.

Vous recevrez un message qui vous demande de confirmer que vous voulez vraiment effacer le document.

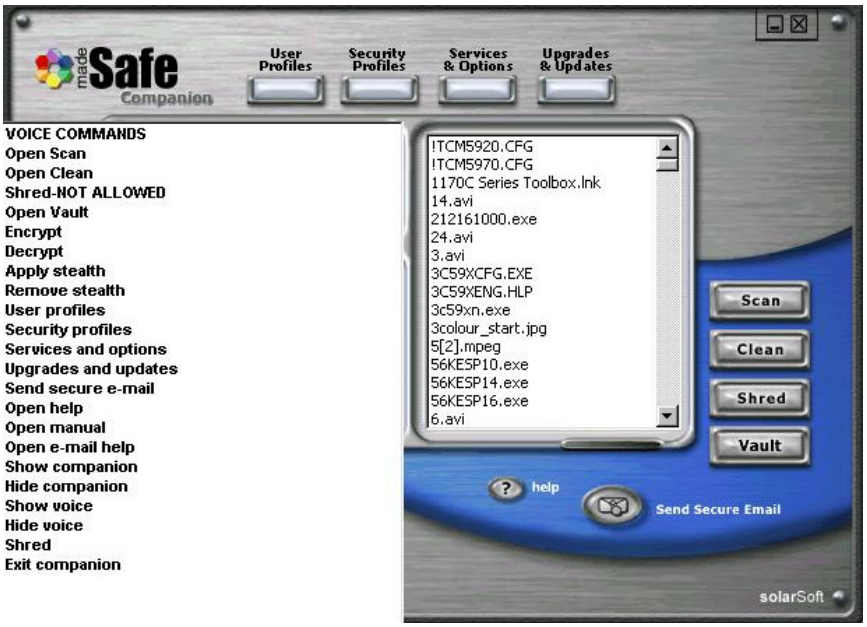
Courriel sécurisé

Cette procédure vous permettra d'envoyer des documents super-encodés à n'importe qui dans le monde, sans que le destinataire ait besoin d'avoir madeSafe installé sur son ordinateur. Pour utiliser cette fonction, choisissez vos exigences de sécurité (haute sécurité ou standard). Le système vous demande alors de sélectionner la pièce jointe de courriel que vous voulez sécuriser. Le génie madeSafe vous guidera tout au long de la procédure. Dans le courriel envoyé, le destinataire trouvera des instructions pour récupérer le message. (Il faut qu'il ait WinZip installé sur son ordinateur). Il vous demandera un mot de passe pour décoder la pièce jointe.

Instructions Ch@mbre Forte

Ch@mbre Forte est très facile à utiliser. Lorsque vous avez tapé votre nom d'utilisateur et votre mot de passe, le système affichera l'écran ci-dessus. Il y a 10 tiroirs, que vous pouvez étiqueter comme vous le souhaitez.
Pour ouvrir un tiroir, cliquez simplement sur le feu vert correspondant pour afficher le contenu de ce tiroir.
Pour envoyer des documents dans votre vault, tirez simplement les documents et lâchez-lez dans le tiroir ouvert. Le système vous demandera si vous si vous voulez envoyer les documents maintenant ou plus tard. Si vous choisissez plus tard, ils seront placés en file d'attente, et lorsque vous avez terminé votre sélection, cliquez simplement sur le bouton «envoyer». La procédure est inverse pour récupérer des documents. Sélectionnez les documents dans le vault et cliquez sur le bouton «réceptionner».
Lorsque vous remplissez votre vault de documents, l'indicateur de capacité se déplace en montrant combien de place il vous reste. A 85%, il vous sera demandé d'acheter un supplément de mémoire vault. Le message vous guide vers notre site web et vous donne les instructions suivantes.

Commandes vocales



Vous pouvez naviguer sur votre madeSafe avec des commandes vocales. Pour faire apparaître la liste de commandes, dites simplement “View Voice”. Une liste de commandes apparaîtra. Pour visualiser manuellement les commandes vocales, tapez V, pour désactiver la fonction voix, tapez Ctrl+V.
Voici la liste de toutes les commandes vocales disponibles sur madeSafe.

Companion Commands

<Say>=ouvrir Scan
<Say>=ouvrir Clean
<Say>=ouvrir Vault
<Say>=encoder
<Say>=décoder
<Say>=apliquer stealth
<Say>=supprimer stealth
<Say>=profils d'utilisateur
<Say>=profils de sécurité
<Say>=services and options
<Say>=mises à niveau et mises à jour
<Say>=envoyer un courriel sécurisé
<Say>=ouvrir l'assistance
<Say>=ouvrir le manuel
<Say>=ouvrir e-l'assistance courriel
<Say>=afficher le companion
<Say>=masquer le companion
<Say>=afficher les commandes vocales
<Say>=masquer les commandes vocales
<Say>=déchiqueter
<Say>=quitter le companion

Commandes Scan

<Say>=démarrer scan
<Say>=Stopper scan
<Say>=ouvrir l'assistance
<Say>=fermer l'assistance
<Say>=afficher le scanner
<Say>=masquer le scanner
<Say>=afficher les commandes vocales
<Say>=masquer les commandes vocales
<Say>=toutes les images
<Say>=images répréhensibles
<Say>=images numériques
<Say>=multimédia vidéo
<Say>=multimédia audio
<Say>=noms de textes
<Say>=contenu de textes
<Say>=programmes espions
<Say>=cookies espions
<Say>=lecture de média
<Say>=stopper le média
<Say>=pause média
<Say>=scan plus rapide
<Say>=scan plus lent
<Say>=quitter le scanner

Chapitre 3 Etre en sécurité, qu'est-ce que cela signifie pour vous?

La question majeure du XXI^{e} siècle

A notre époque électronique, le stockage de données sensibles, personnelles et d'entreprise devient de plus en plus vulnérable aux menaces criminelles d'intrusions de plus en plus sophistiquées (vol, fraude, destruction).

La nécessité commerciale de centraliser électroniquement les données sensibles crée des points d'attaque facilement identifiables pour les apprentis-hackers et terroristes virtuels.
Les dégâts émotionnels et financiers causés par de telles infractions peuvent être catastrophiques, et qui pis est, selon de récentes découvertes largement diffusées du FBI, la plupart des fraudes ou des menaces viennent de l'intérieur d'une organisation.

Tout le monde est concerné!

Il n'y a pas que les entreprises qui sont vulnérables à la menace virtuelle. Chaque fois que vous vous connectez à Internet depuis chez vous, vous ouvrez la porte à de potentiels intrus qui peuvent pénétrer dans votre PC, et vous exposez vos données personnelles et privées à d'éventuels abus.
Les risques s'accroissent rapidement pour les entreprises comme pour les particuliers.

Solutions de sécurité courantes

Les défenses courantes contre les menaces se divisent en trois catégories: firewall, anti-virus et simple codage.

Les logiciels anti-virus sont une nécessité évidente tant pour les particuliers que pour les entreprises. La fréquence et la sophistication croissante des virus qui peuvent paralyser un PC, détruire des applications, et se dupliquer par e-mail font de ces logiciels un must. Mais ces logiciels font peu pour protéger effectivement l'intégrité des données.

L'histoire a déjà prouvé que les firewalls (hardware et logiciels) sont relativement peu sûrs contre un hacker déterminé, et que parfois ils ne servent à rien contre l'accès non autorisé de l'intérieur de l'organisation.

Alors que le codage des données semblerait être la solution évidente pour se protéger contre de telles attaques, les produits courants peuvent être compliqués à utiliser, ou ne pas être très sûrs. Les solutions courantes offrent une protection insuffisante contre des menaces de plus en plus sophistiquées et très réelles.

Contre ces menaces, il faut un nouveau concept et des technologies nouvelles.....

La réponse est: -

Chapitre 3 Etre en sécurité, qu'est-ce que cela signifie pour vous?

Imaginez le scénario suivant:

Vous avez été un bon administrateur de la sécurité et vous avez installé les mesures de sécurité les plus sophistiquées sur votre réseau. Le firewall est en place et bardé de tous les derniers gadgets. Les routeur sont configurés correctement. Et toutes les permissions d'utilisateurs et de groupes ont été dûment auditées et vérifiées. Un jour, le PDG vous appelle dans son bureau pour vous dire que de nombreux clients ont appelé pour se plaindre que leurs cartes de crédit ont été débitées de sommes non autorisées. Il y a pire: la carte de crédit de l'entreprise aussi a un débit inexplicable de £15,000. Une inspection approfondie des documents de journalisation fait apparaître quelques tentatives d'intrusion, mais aucune n'a réussi. Après les avoir passées en revue une deuxième et ne troisième fois, la seule conclusion qui vous reste est qu'il s'agit de quelqu'un de l'intérieur. Vous vérifiez les connexions sur le serveur qui conserve les données client et les seules connexions qui y figurent sont les vôtres. Vous passez au serveur des données financières de l'entreprise et les seules entrées sont celles du PDG lui-même. En analysant les heures de connexion, vous constatez qu'il y a une connexion du PDG à une heure où vous savez qu'il était à une conférence et au moins une des vôtres a eu lieu un jour où vous étiez toute la journée en réunion avec le chef de l'unité informatique. Quelqu'un a eu un accès physique à vos serveurs et a volé des informations d'utilisateur y compris leurs noms et leurs mots de passe.

Ceci est un événement fictif, mais ce genre de choses se produit tout le temps dans la réalité. Si quelqu'un peut accéder physiquement à votre serveur, il peut obtenir toutes les informations qu'il veut. Il peut craquer l'accès à tout votre réseau et voler ou copier n'importe quelle information. La seule manière d'empêcher ces actes de se produire est de restreindre l'accès à vos serveurs. Bien sûr, la sécurité physique n'est pas limitée aux serveurs. Elle s'applique aussi aux portables et aux postes de travail. C'est un problème qui vous touche, en tant que client, et qui touche le professionnel de la TI. La réponse est: -

Chapitre 4 Dépannage

FOIRE AUX QUESTIONS

1) **Comment encoder/décoder des documents ?**

Ouvrez tout simplement votre Companion, sélectionnez l'emplacement du document dans la liste du lecteur, sélectionnez le disque dans lequel se trouve le document et ensuite marquez le document que vous voulez encoder. Quand le document est marqué, cliquez tout simplement le bouton d'encodage. Le document est à présent visible seulement pour vous.

2) **Comment puis-je identifier/décrypter un document crypté ?**

Vos documents encodés auront une extension .ENC. Marquez-les tout simplement et cliquez «décoder» pour ouvrir ces documents.

3) **J'ai crypté des documents et je ne les trouve plus. Comment les trouver?**

Vous pouvez avoir utilisé «stealth» quand vous avez encodé les documents. Sélectionnez votre répertoire et cliquez «supprimer stealth». Ceci enlèvera stealth de TOUS les documents encodés.

4) **J'ai oublié mon mot de passe, comment récupérer mes données?**

SolarSoft vous recommande vivement le plan de protection par mot de passe pour éviter cette situation. Si vous avez la protection, contactez l'assistance et ils vous fourniront votre mot de passe. Si vous n'avez pas de protection, les documents ne sont pas récupérables.

5) **J'ai des information confidentielles que je veux effacer définitivement de mon ordinateur, comment faire?**

Dans votre Companion, vous verrez un bouton appelé «Detruire». Marquez le fichier que vous voulez effacer DÉFINITIVEMENT et cliquez «Detruire». Ceci détruira le fichier sans possibilité de récupération.

6) **Je possède madeSafe Home et je veux avoir un Ch@mbre Forte à moi. Comment faire?**

Pour acheter Ch@mbre Forte, cliquez sur le bouton «mise à niveau» dans le Companion et suivez les instructions à l'écran.

7) **Les enfants se plaignent qu'Internet ne marche pas. Qu'est-ce qui ne fonctionne pas?**

Quelques pages Internet surgissent dans une nouvelle fenêtre. Cette fonction est activée par défaut; pour la désactiver, cliquez l'idéogramme dans la barre des tâches et contrôlez «Désactiver les fenêtres popup».

8) **Un collègue m'a informé qu'ils m'ont envoyé un mail sécurisé, mais je ne l'ai pas reçu.**

L'e-mail encodé contient probablement un document .zip. La majorité des firewalls et des programmes anti-virus bloquent cela. Désactivez l'anti-virus \ firewall pour recevoir le mail.

Chapitre 5 Glossaire

Active Stealth Technology™
La technologie Active Stealth de madeSafe permet à l'utilisateur de cacher des données déjà encodées de manière qu'un hacker ou un intrus ne trouvera aucune source complète ou point d'entrée.

Algorithme (encodage)
Un ensemble de règles mathématiques (logiques) utilisé dans les processus d'encodage et de décodage.

Algorithme (Hash)
Un ensemble de règles mathématiques (logiques) utilisé dans les processus de création de message et de génération de clé/signature.

Antivirus
Logiciel qui protège un PC des virus basés sur Internet. Typiquement, ces virus endommagent le PC d'une manière qui peut être à la fois disruptive et chère.

Intelligence Artificielle
Une branche de l'informatique qui vise à produire une technologie qui puisse imiter le comportement humain intelligent.

Clefs asymétriques
Une paire de clés d'utilisateur séparée mais intégrée, composée d'une clé publique et d'une clef privée. Chaque clef est à sens unique, c-à-d. qu'une clef qui a servi à encoder une information ne peut pas être utilisée pour décoder les mêmes données.

Certification
Le processus de détermination de l'identité d'un utilisateur qui essaie d'accéder à un système

Autorisation
Accorder une sanction officielle, un accès ou un pouvoir légal à une entité.

Signature aveugle
Capacité de signer des documents sans connaître le contenu, semblable à un notaire public.

Chiffre bloc
Chiffrage de fonctionnement symétrique sur blocs de texte en clair et texte chiffré, habituellement 64 bits.

Blowfish
Un chiffre bloc perfectionné, algorithme symétrique.

Certificats
Une CARTE D'IDENTITÉ numérique publiée par une autorité certifiante (AC) servant à certifier et à valider le transfert de données sur Internet.

Autorité certifiante

Une organisation qui publie des certificats numériques prouvant l'identité de l'expéditeur d'un message e-mail ou d'un document.

Texte chiffré
Texte en clair converti en un format dissimulé au moyen d'un algorithme d'encodage. Le texte en clair original peut être décodé à partir du texte chiffré avec une clef d'encodage

Outil de nettoyage
L'instrument Clean de madeSafe, nettoie à fond et range votre disque dur, en libérant de l'espace précieux.

Client
Un ordinateur qui demande un service à un autre ordinateur a appelé le serveur. Par exemple, si vous vous connectez à un ISP ou ordinateur du réseau de l'entreprise, votre ordinateur est le client et l'ISP ou l'ordinateur du réseau de l'entreprise est le serveur.

Companion™
Le Companion de sécurité de madeSafe est une interface d'usage facile qui offre à l'utilisateur un environnement à fenêtre unique à partir duquel il peut accéder aux produits madeSafe, aux mises à niveau et aux services.

Outil de filtrage du contenu
Le filtre Internet est un dispositif standard de madeSafe Home et une mise à niveau pour madeSafe Mobile et Business.

Cookie
Une petite unité d'information qu'un serveur web peut déposer sur votre disque dur à travers votre navigateur web, et relire plus tard depuis votre navigateur.
Les sites Web rassemblent cette information vous concernant sur la base d'un outil connu sous le nom de cookie. Les programmes cookie peuvent rassembler de l'information sur vos pérégrinations sur le réseau. Ils sont insérés automatiquement, à la fois par Netscape Navigator et par Microsoft Internet Explorer, mais ils peuvent être mis hors fonction. L'information qu'ils rassemblent est entreposée sur votre disque dur. Toutes les fois que vous visitez un site plus d'une fois, ce site accède à votre fichier témoin pour voir ce que vous avez consulté auparavant pour en savoir plus sur ce qui vous intéresse.

Cracker
Quelqu'un qui enlève ou met hors circuit la protection contre la copie sur logiciel, généralement en modifiant le logiciel.

Cryptographie
L'art et la science de créer des messages qui ont pour caractéristique d'être privés, signés, non modifié avec non - répudiation.

Intégrité des données
Une méthode pour s'assurer que l'information n'a pas été changée par des moyens non autorisés ou inconnus.

Décodage
Déprotégez un message e-mail et ses documents à l'appui.

Decryptage
Une méthode de déchiffrage de l'information codée afin qu'elle redevienne lisible. La clef privée du destinataire est utilisée pour décryptage.

Certificats numériques
Documents publiés par les Autorités certifiantes qui prouvent l'authenticité d'un document web ou d'une URL. Un certificat numérique est un dossier de données encodé, protégé par un mot de passe qui contient l'identification de l'utilisateur de l'encodage du message en plus du message qui est envoyé. Bien que tout ordinateur sur Internet puisse accéder au dossier encore en transit, seul le destinataire prévu peut décrypter et lire le message.

Signature numérique
Une technique de sécurité pour identifier de manière unique la source d'un document ou d'une application.

DES (Data encodage Standard)
Un chiffre bloc algorithmique symétrique 64-bit également connu sous le nom de Data encodage Algorithm (DEA) pour ANSI et DEA-1 pour ISO. Un standard largement répandu.

Encoder
Protégez un message e-mail et chacun de ses documents sensibles.

Encodage
Une technique de sécurité visant à prévenir l'accès à l'information en la convertissant en texte chiffré (texte brouillé, illisible). Le texte chiffré doit ensuite être décodé par l'utilisateur Internet avant de pouvoir être lu.
L'encodage peut être utilisé pour tout sécuriser: du document informatique sensible à la transmission de données financières sur en passant par les appels passés sur des téléphones cellulaires numériques.

EES (Escrowed encodage Standard)
Un standard proposé par le gouvernement américain pour le dépôt des clefs privées.

Extranet
Les extranets sont des réseaux qui connectent des intranets d'entreprise à Internet.
Ils sont conçus pour être utilisé par des vendeurs de l'entreprise et autres partenaires de commerce de confiance pour activer l'échange de produits, de services et autres informations déterminantes pour les opérations de l'entreprise.

File Transfer Protocol (FTP)
Le FTP est un programme de transfert des documents entre ordinateurs soit par Internet soit entre PC.

Firewall (mur anti-feu)
Un processus de sécurité qui programme un système informatique pour contrôler la circulation de l'information entre Internet et d'autres ordinateurs de l'Intranet. La barrière du système informatique empêche les extérieurs d'accéder au réseau interne d'une entreprise: le réseau interne, en revanche, accède à Internet indirectement à travers le système du réseau interne. *Voir Proxy Server.* .

Hacker
Un utilisateur qui pénètre dans les ordinateurs sans y être autorisé. *Voyez Cracker*

Lien hypertexte
Un mot ou une expression soulignés ou signalés autrement pour indiquer sa capacité d'établir le lien avec un autre document quand on clique avec la souris.

Hyper Text Mark-up Language (HTML)
Le langage d'auteur utilisé pour développer des pages web et des messages électroniques.

Hyper Text Transfer Protocol (HTTP)
Le protocole utilisé pour transporter des documents HTML sur Internet.

HTTPS
Indique un serveur Internet sécurisé. C'est le protocole sécurisé utilisé pour transporter des documents HTML sur Internet.

Integrité
Assurance que les données ne sont pas modifiées (par des personnes non autorisées) pendant le stockage ou la transmission.

Internet
Le plus grand réseau informatique du monde, qui connecte de nombreux réseaux informatiques de campus, d'Etat, d'entreprise, régionaux et nationaux.

Filtre Internet
Pour empêcher des enfants ou des employés de voir des sites web répréhensibles ou nuisibles pendant qu'ils sont en ligne, il existe plusieurs logiciels qui filtrent le matériel. *Voyez Filtrage des contenus*

Intranet
Un Internet interne placé derrière un mur anti-feu (firewall) d'entreprise.

Fournisseur de Service Internet (ISP)
Une entreprise qui fournit l'accès à Internet pour les utilisateurs sur appel téléphonique et/ou réseaux d'entreprises. Il loue l'accès aux clients sur la base d'une sorte de service.

ISO (International Organization for Standardization)
Une instance responsable d'une large gamme de normes de la technologie.

Clé
Un code numérique utilisé pour encoder, signer, décrypter et vérifier des messages aussi bien que des documents

Longueur de clé
Le nombre de bits qui représente la dimension de la clé. Plus la clé est longue, plus elle est puissante

Porte-clés
Un jeu de clés. Chaque utilisateur a deux types de porte-clés: un privé et un public.

Gestion des clés
Procédure et processus de stockage et de distribution des clés cryptographiques exactes; processus général de génération et de distribution des clés cryptographique aux destinataires autorisés d'une manière sûre.

Certification du message
Le processus de validation du destinataire et de l'expéditeur d'un message e-mail.

Laissez-passer
Une expression facile à mémoriser utilisée pour plus de sécurité qu'un simple mot de passe; le coup de clé la convertit en une clef aléatoire.

Mot de passe
Une séquence de caractères ou un mot qu'un sujet soumet à un système pour buts de certification, de validation, ou de vérification.

Texte en clair
Caractères sous une forme lisible par une personne ou bits sous une forme lisible sur machine.

PGP
Mis pour 'Pretty Good Privacy' (haute confidentialité). Un système de cryptographie des clés publiques-privées composé de deux clefs; l'une est une clef publique que vous livrez à quelqu'un à qui vous voulez envoyer un message. L'autre est une clef privée que vous utilisez pour décrypter des messages que vous recevez.

PKI (Public Key Infrastructure)
Un système de certificat largement disponible pour obtenir la clé publique d'une entité avec un haut niveau de certitude que vous avez la "bonne" clé qu'elle n'a pas été révoquée.

Clef privée
Une partie secrète d'une paire de clés pour signer et décrypter de l'information. La clef privée d'un utilisateur devrait être gardée secrète, connue uniquement de lui-même.

Proxy (serveur)
Un serveur qui agit comme un firewall (barrière), servant de médiateur de la circulation entre un réseau protégé et Internet.

Clef publique
Données utilisées pour encoder des messages en code Clé publique. Elle ne peut pas être utilisée pour décrypter un message; il n'est pas dangereux de la distribuer au public, comme son nom l'indique.

Nombre aléatoire
Un moyen de produire une clé unique imprévisible pour un intrus.

Outil Scan
L'outil Scanner de madeSafe parcourt le disque que vous avez sélectionné pour chercher du matériel que l'utilisateur maître juge défendu.

Moteur de recherche
Programme qui parcourt automatiquement Internet pour chercher des informations spécifiées par l'utilisateur.

Architecture Cellulaire de sécurité™
Les produits personnels madeSafe (Home & Mobile) fournissent une cellule encodée à 128-bit qui enveloppe les données ou documents que vous choisissez. Ceci fournit un accès multi - utilisateur sécurisé, autorisé et contrôlé par l'utilisateur-maître.
madeSafe Business fournit une cellule d'utilisateur-maître avec des cellules supplémentaires qu'ils nomment. Chaque cellule fournit les mêmes niveaux d'encodage et de fonctionnalités Cependant, l'utilisateur-maître a accès à tout et contrôle tout.

Canal Sécurisé
Un site web qui garantit la transmission sécurisée de toute information qui lui est envoyée.

Secure Electronic Transactions (SET)
Protocoles Internet sécurisés pour traiter les transactions en argent électronique.

Secure Multipart Internet Mail Encoding (S/MIME)
Le protocole utilisé pour envoyer des messages e-mail sécurisés.

Secure Socket Layer (SSL)
Technologie de sécurité du programme interne de Netscape, conçue pour identifier clairement le destinataire et l'envoyeur d'informations transmises sur Internet.

Séurité
Méthodes de protection des ressources informatiques, y compris les données, le hardware, les lignes de télécommunication et les applications de logiciels contre l'accès non autorisé.

Serveur
Un ordinateur qui fournit de l'information ou des connexions avec d'autres ordinateurs sur un réseau. *Voyez Client.*

Outil de déchiquetage
L'outil de déchiquetage de madeSafe, efface définitivement tout dossier ou document sans possibilité de récupération.

Single Line Internet Protocol (SLIP)
Un protocole de communication plus ancien pour les connexions Internet sérielles par appel téléphonique.

Simple Mail Transport Protocol (SMTP)
Un protocole Internet pour envoyer des e-mails.

S/MIME
Voir Multipurpose Internet Mail Extensions (MIME).

Smart encodage™ (Encodage intelligent)
La technologie d'encodage de madeSafe, combinée avec l'intelligence artificielle, est appelée Smart encodage™. Les produits madeSafe sont configurés pour assumer le super-encodage 448-bit dual end.
Le niveau de cryptage peut être réduit (p. ex. pour accélérer la performance) en réglant le profil de sécurité de madeSafe Companion.™

Stéganographie
Par exemple, un document -texte pourrait être caché “à l'intérieur d'”une image ou d'un document audio. En regardant l'image, ou en écoutant le son, on ne se rend compte de rien.

Clef symétrique
Une clé conventionnelle, secrète et un algorithme clé unique où les clés du décodage et de l'encodage sont soit identiques soit reliées par calcul. madeSafe utilise une clef symétrique.

Marquage temporel
Enregistrement de l'heure de création ou d'existence d'une information

Transmission Control Protocol/Internet Protocol (TCP/IP)
L'ensemble de standards (protocole) pour la transmission de données et la correction d'erreurs qui autorise le transfert de données d'un ordinateur relié à Internet à un autre.

Two Fish
Un chiffre bloc, algorithme symétrique.

The World Wide Web
(a.k.a., WWW, W3, Le Web) Un système d'information hypertexte Internet distribué sur Internet, basé sur le protocole HTTP et le langage HTML.

Uniform Resource Locator (URL)
L'adresse de site utilisée pour spécifier l'emplacement d'une page web (document HTML). C'est le nom formel et technique d'une chaîne de texte qui fournit une adresse Internet, et la méthode par laquelle on y accède.

Validité
Indique à quel niveau de certitude la clé appartient réellement au propriétaire présumé.

Ch@mbre Forte
Cha@mbre Forte vous permet de placer une copie de vos données codée sur notre site madeSafe ultra-sécurisé, et vous restitue votre back-up, dans le monde entier, 24 heures par jour, 365 jours par an. Les extensions de madeSafe Ch@mbre Forte se font par incréments de 5 MO.

Vérification
Comparer une signature créé avec une clé privée à sa clé publique.

VPN (Virtual Private Network)
En règle générale, un réseau privé basé sur un Intranet qui relie un réseau public (Internet) à un autre réseau au choix.

Chapitre 6 Soutien technique

Solarsoft s'engage à fournir un soutien et des services excellents. Notre but est vous fournir toute l'assistance professionnelle nécessaire à l'usage de nos logiciels et services madeSafe.

Inscription

Enregistrer votre produit madeSafe vous donne droit au soutien web aussi bien qu'aux mises à jour et offres spéciales.

Service client

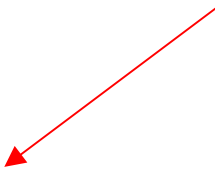
Une gamme étendue d'informations au sujet de madeSafe se trouve sur notre site web à l'adresse www.madesafe.com. Ou bien, envoyez-nous un e-mail à sales@madesafe.com.

Soutien Web gratuit

Vous avez accès au soutien Web gratuit par le bouton help (aide) sur le Companion madeSafe. Ou vous pouvez y accéder directement par www.madesafe.com/support. Le service fonctionne du lundi au vendredi de 9.00 à 17.00.

Soutien par Téléphone

Solarsoft fournit une assistance technique par téléphone payante pour tous ses produits madeSafe. Les clients peuvent y accéder via leur bouton Services & Options sur leur Companion madeSafe.



Chapitre 7 Droit d'auteur & marques déposées

SOLARSOFT LIMITED. TOUS DROITS RÉSERVÉS.

Ce logiciel est prévu pour l'usage de l'acheteur original uniquement et pour constituer une cellule sécurisée unique. Dans le cas du produit madeSafe Business, deux cellules supplémentaires 'employés' sont fournies comme partie de la licence. Les utilisateurs légaux de ce logiciel sont autorisés par la présente licence à lire le logiciel sur le CD ci-joint et à le stocker dans la dans la mémoire d'un ordinateur dans le seul but de l'exécuter. Vendre ou distribuer autrement ce logiciel constitue une violation de la loi.

Solarsoft Limited garantit que le CD sur lequel le logiciel est fourni est exempt de défauts de matériel et d'exécution, et que le logiciel fonctionne conformément aux spécifications décrites dans les textes d'accompagnement. Solarsoft Limited ne donne pas d'autre garantie, implicite ou explicite, en ce qui concerne le logiciel et la documentation, la qualité, la performance, la valeur marchande, ou l'aptitude pour un but particulier. De plus, Solarsoft Limited ne garantit pas que le logiciel fonctionne correctement dans tous les environnements et applications. Solarsoft Limited se réserve le droit de faire des changements au contenu du logiciel et du Guide de l'Utilisateur sans obligation d'annoncer la révision ou le changement à toute personne ou organisation.

Chapitre 8 Détails de communication

Nous toujours sommes heureux d'avoir des nouvelles de nos clients. Si vous avez besoin de nous contacter, téléphonez-nous. Si vous avez besoin de rester à jour ou de soutien, jetez un coup d'oeil sur notre site web.

Solarsoft Limited
Phillips House, Station Road, Hook, Hampshire, United Kingdom. RG27 9HD

Tél: +44 (0) 870 872 8210 Fax: +44 (0) 870 872 8209
Web: http: www.madeSafe.com

Chapitre 9 **Information sur le génie**

Quand le génie Help est visible, les fonctionnalités des boutons sont mises hors fonction. Pour obtenir de l'information sur une des fonctions, cliquez simplement le bouton avec lequel vous demandez de l'aide. Le génie madeSafe vous l'expliquera.

Une fois vous avez eu l'explication, cliquez avec la touche de droite de la souris sur le génie et sélectionnez hide, ou tapez Esc pour fermer le génie.

Chapitre 10 Petit guide de référence

Réglage des profils d'utilisateur

Réglage types de sécurité

Voir les options et services disponibles

Voyez les mises à niveau/ mises à jour disponibles

emplace-ment du disque but

Afficher les documents dans le répertoire en cours

Emplace-ment du répertoire but

Scannez votre disque pour trouver tout matériel sur lequel l'utilisateur maître applique des restrictions

Décodez les documents choisis

Efface définitivement les documents et en sécurité

Encodez les documents choisis

Nettoie les documents temp de votre disque dur en toute sécurité

Démasquez les documents choisis

Masquez les documents choisis

Assistance du génie madeSafe

Envoyer des e-mails sécurisés

Accès direct à votre chambre forte personnelle