made**Safe**™

# madesafe

## User Guide

www.madesafe.com

# Inhalt



## Kapitel 1 > madeSafe Companion™: erste Schritte

**madeSafe™...**

- hält Ihre persönlichen und beruflichen Informationen geheim.
- schützt Ihren PC vor Hackern.
- lässt Sie geschützte E-Mails senden.
- reagiert auf Sprachbefehle.
- lässt Sie Ihre Sicherheitsbedürfnisse mit einer einfach zu bedienenden Benutzeroberfläche verwalten und überwachen.
- schützt Ihre Kinder auf dem Internet.
- speichert und stellt alle geschützten Dateien wieder her, wo immer Sie sich gerade befinden - sogar wenn Ihr PC gestohlen wurde.
- lässt Sie von seiner Mehrbenutzer-Fähigkeit Gebrauch machen. Zusätzliche Benutzer können jederzeit hinzugefügt werden. So schützen Sie Ihr Unternehmen oder Ihre Familie.
- bietet Ihnen eine Reihe von zusätzlichen Funktionen und Erweiterungen, damit Sie madeSafe™ Ihren persönlichen Bedürfnissen anpassen können.
- verbessert Ihr Sicherheitsumfeld, wann immer Sie das möchten. Nutzen Sie unser umfangreiches Dienstleistungs- und Optionsangebot.

Wir verpflichten uns, Ihnen mit madeSafe™ das Beste in Sachen Datenschutz und Sicherheit zu bieten. madeSafe™ ist eines der führenden Verschlüsselungs-Anwenderprogramme, das Ihnen mit künstlicher Intelligenz hilft, Ihren persönlichen Platz / Ihre persönliche Zelle zu gestalten. madeSafe™ ist ganz auf Ihre persönlichen Bedürfnisse ausgerichtet und ist fähig, sich mit Ihnen und Ihren sich verändernden Bedürfnissen zu entwickeln, damit Sie für die immer raffinierter werdenden Bedrohungen gewappnet sind.

**Ihr Security Companion™**

Der madeSafe Security Companion™ wurde entwickelt, um Verschlüsselung endlich bedienerfreundlich zu machen. Alle Produkte und Dienstleistungen, die Ihnen umfassende Sicherheit für Ihren PC bieten, sind nur einen Mausklick entfernt.

Der madeSafe Security Companion™ verfügt über vier klar erkennbare Funktionsfelder. In logischen Gruppen angeordnet, schützen sie Ihre Daten und optimieren die Leistung Ihres PCs:

- Profile & Erweiterungen
- Optimierung & Speicherung
- Datei-, Laufwerk- und Verzeichnis-Fenster
- Verschlüsselung


**Verschlüsselung**
Superschnelle, führende 448-Bit Verschlüsselung – mit nur einem Mausklick. Geschwindigkeit und Verschlüsselungsstärke sind ein- und verstellbar. Schützen Sie Ihre vertraulichen Daten vor Hackern oder ungebetenen Benutzern.

**Geschützte E-Mails**
Senden Sie in der Gewissheit, ganz und gar sicher zu sein, verschlüsselte E-Mail-Anlagen um den ganzen Erdball. Und das ohne, dass der Empfänger madeSafe™ bei sich zu installiert haben braucht.

**Starke Dienstprogramme**
Ein überzeugendes Sicherheits-Paket:
**Scannen** – Durchsuchen Sie das gewünschte Laufwerk nach Material, das Sie als unangemessen erachten.
**Reinigen** – Löschen Sie nicht mehr benutzte Dateiansammlungen und machen Sie so Festplattenspeicher frei. Löschen Sie Eingabeverläufe, damit Hacker keine gespeicherten oder neuen Dateien entdecken können.
**Schredden** – Löschen Sie Dateien so, dass sie nicht wieder herstellbar sind und alle Datei- und Dokument-Spuren verwischt werden.
**Stealth™** – Für höchste Sicherheit macht madeSafes einzigartige Active Stealth Technology™ Ihre wichtigsten verschlüsselten Daten unsichtbar.

**Internet-Inhaltsfilter – madeSafe Shield™**

Zu madeSafe Shields Schlüsselfunktionen gehören:

- ✓ Sperrt geschmacklose Websites.
- ✓ Seiten werden unter Verwendung einer URL-Datenbank (URL = standardisierte Form der Adressierung von Websites) und Meta-Tags (Schlagworte und Beschreibung nach denen Suchmaschinen Ihre Auswahl treffen) herausgefiltert.
- ✓ URL-Datenbank der gesperrten Seiten wird ständig aktualisiert.
- ✓ Fähigkeit, Pop-Up-Fenster auszuschalten.
- ✓ Wird durch Eltern resp. Systemadministrator kontrolliert (normale Benutzer können das Programm nicht ausschalten).
- ✓ Fähigkeit, benutzerdefinierte URL's und Schlagworte hinzuzufügen.
- ✓ Zeigt Benutzer an, die versuchen, auf gesperrte Seiten zuzugreifen.
- ✓ Das Programm läuft diskret in der Taskleiste.
- ✓ Protokolliert den gesamten Internetverkehr (besuchte Seiten, Zeiten und Benutzer).

**Ultrasichere Speicherung & Wiederherstellung**
Werwenden Sie Vault™, um Ihre vertraulichsten Daten auf unsere extrem sichere madeSafe™ Website zu spiegeln. Sichere Datenspeicherung und –wiederherstellung, weltweit, 24 Stunden am Tag, 365 Tage im Jahr. Nur Sie haben Zugriff.

**Mehrfachbenutzer-Zellen – netzwerkfertig**
Zusätzliche Benutzerlizenzen bedeuten Datenschutz und Sicherheit - unternehmensweit. Weiten Sie Ihr bestehendes madeSafe™ Business aus, um andere Benutzer mit einzuschliessen. Jede Produkterweiterung beinhaltet drei Lizenzen.

## Dienstleistungen & Optionen

Für umfassende Sicherheit bieten wir ein umfassendes Dienstleistungs-Angebot:

**Schutz vor Passwortverlust**

Machen Sie sich Sorgen um Ihre Passwörter? Wir speichern sie für Sie in unserem sicheren, verschlüsselten Tresor (Vault™).

**Sicherheitsprüfung**
Laden Sie unsere Sicherheitsprüfungssoftware herunter und finden Sie heraus, wie sicher Ihr PC oder Netzwerk wirklich sind.

**Diebstahlaufdeckung**
Wurde Ihr PC gestohlen, sendet Ihnen dieses Dienstprogramm automatisch eine E-Mail, sobald sich jemand ins Internet einwählt.

**madeSafe™ Care**
Telefonsupport - Wir bieten Ihnen den bestmöglichen technischen Support und helfen Ihnen, das Beste aus Ihrem madeSafe™-Produkt herauszuholen.

**madeSafe™ Cover**
Versicherung - Nutzen Sie die umfassende, weltweite Versicherungsdeckung für Ihren Laptop oder PC.

## Erweiterungen & Aktualisierungen

Lebenslange Sicherheit – Produkt-Verbesserungen, Gratis-Aktualisierungen, Rabatte und Sonderangebote.

**Vault™-Erweiterung** – Sagen Sie uns, wie viel Speicherplatz Sie benötigen und erweitern Sie ihn – jederzeit.

**Internet-Filter-Erweiterung –** Erhalten Sie regelmässig Aktualisierungen zu Ihrem Inhaltsfilter, damit Sie up to date und sicher vor anstössigem Material bleiben.

# Installation von madeSafe™

## Systemanforderungen

madeSafe™ wurde für die Microsoft Windows-Umgebung entwickelt. Benutzer, die mit Windows bereits vertraut sind, werden es zu schätzen wissen, dass der madeSafe Security Companion™ so gestaltet wurde, dass er die aktuelle Arbeitsoberfläche hervorragend ergänzt.

Bevor Sie madeSafe™ installieren, stellen Sie sicher, dass die folgenden minimalen Systemanforderungen erfüllt sind:

Minimale Systemanforderungen zur Installation von madeSafe™:

- IBM™-PC oder kompatibel
- Microsoft Windows 95, 98, 2000, NT, ME oder Windows XP
- 486-Prozessor oder höher
- Mindestens 16 MB RAM
- Mindestens 100 MB Festplattenspeicher
- Webbrowser (vorzugsweise IE4, Netscape 4 oder höher)
- VGA oder höher mit 256 Farben
- CD-ROM-Laufwerk
- Internetzugang und ein **gültiges** E-Mail-Konto
- Soundkarte und Mikrofon (optional)

## Installation

Zur Installation Ihres madeSafe™-Produktes führen Sie bitte die folgenden Schritte aus.

Installation:

1 Starten Sie Windows (falls es nicht schon läuft)
2 Legen Sie die madeSafe™-CD in das CD-ROM-Laufwerk ein
3 Klicken Sie im sich öffnenden Fenster auf „madeSafe installieren“ und folgen Sie den Anweisungen auf dem Bildschirm

## Installation & Registrierung

Nach der Installation wird das Programm die Einrichtung eines Hauptbenutzer- resp. Administrator-Kontos verlangen. Tragen Sie einfach Ihren Namen, Ihre E-Mail-Adresse sowie ein mindestens 8-stelliges, bestätigtes Passwort ein **(WICHTIG: VERGESSEN SIE IHR PASSWORT NICHT)** und tragen Sie anschliessend den CD-Schlüssel ein, um sich zu registrieren.


Diese Informationen werden auf unserem Server in einem geschützten E-Mail einen Aktivierungscode anfordern. Geben Sie diesen Code in die Aktivierungsbox ein (am besten machen Sie das mit „Kopieren“ und „Einfügen“) und klicken Sie anschliessend auf „madeSafe Companion aktivieren“. Nun werden die entscheidenden Komponenten, die Sie zur Benutzung des Produktes benötigen, heruntergeladen.

## Kapitel 2 > Einrichtung des madeSafe Security Companion™


Die Festlegung des Hauptbenutzers geschieht während des Installations- und Registrierungs-Vorganges. Die Hauptbenutzer-Passphrase kann nicht geändert werden, der Name jedoch schon. Möchten Sie den Namen ändern, markieren Sie ihn, geben Sie den neuen ein und klicken Sie auf „Änderung ausführen“. Um einen Benutzer hinzuzufügen, klicken Sie auf das Benutzer-Drop-Down-Menü, wählen einen neuen Benutzer aus und geben dessen Namen und Passphrase ein. Haben Sie diesen Vorgang abgeschlossen, klicken Sie auf „Änderung ausführen“.
Einen Benutzer zu entfernen ist genauso einfach. Wählen Sie den entsprechenden Benutzer im Drop-Down-Menü aus und klicken Sie auf „Ausgewählten Benutzer löschen“. Klicken Sie auf „Beenden“ um ins Hauptmenü zurückzukehren.
Der Hauptbenutzer hat vollständigen Zugriff auf die Files aller anderen Benutzer.

**Einrichtung der madeSafe Business-Ausgabe**
Der Hauptbenutzer muss den madeSafe Companion auf seinem Computer (d.h. auf dem Computer des Hauptbenutzers) installieren und aktivieren. Anschliessend muss der Hauptbenutzer den madeSafe Companion auf die Computer der Unter-Benutzer installieren. Während der Installation muss der Hauptbenutzer dabei anstelle des CD-Schlüssels das Wort „Netzwerk“ eingeben und danach auf „Aktivieren“ klicken. Darauf wird der Hauptbenutzer aufgefordert, das Verzeichnis anzugeben, in welches das Programm gespeichert werden soll.

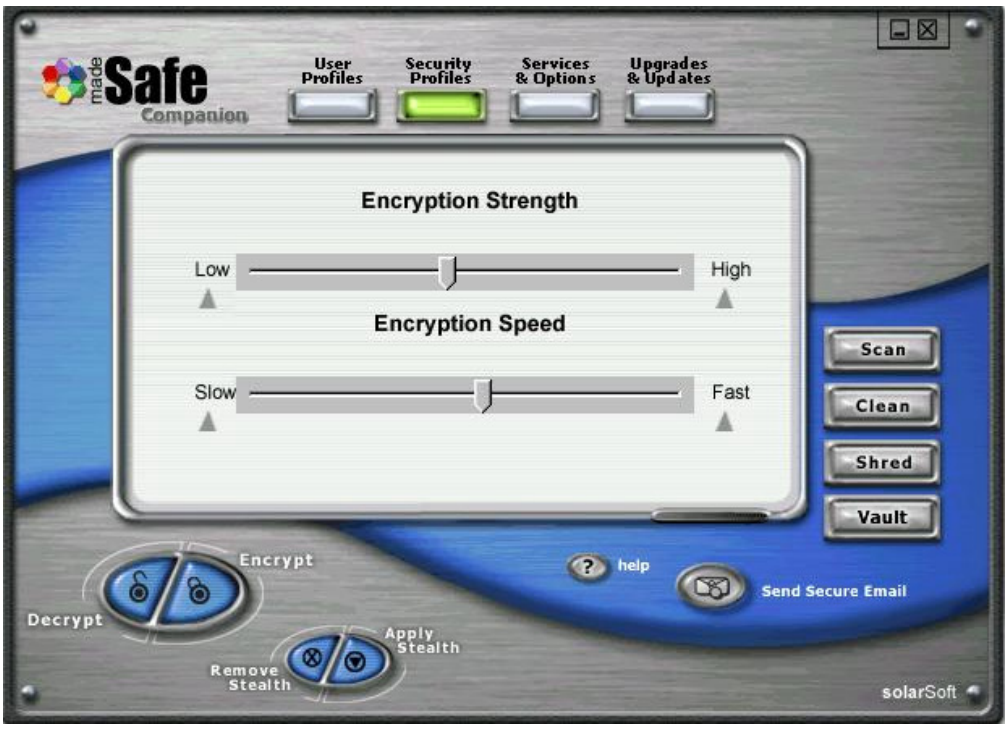
d.h. \\Admin\C:\ProgramFiles\solarsoft\madesafe.
**Vermerk – Bitte stellen Sie sicher, dass das Laufwerk des Hauptbenutzers gemeinsam (d.h. auch von den Unter-Benutzern) genutzt werden kann.**
Wurde das Verzeichnis ausgewählt, klicken Sie auf “OK”, um die Installation abzuschliessen.
Der Hauptbenutzer kann jetzt alle Konten von seinem Computer aus verwalten.
Der Hauptbenutzer kann sich nun in jeden Computer einloggen (unter Verwendung eines zweiten oder dritten Benutzernamens und Passwortes), auf den madeSafe installiert wurde und Zugriff auf jegliche verschlüsselten Daten nehmen.

WARNUNG: - VERSUCHEN SIE NICHT, DATEN ZU ENTSCHLÜSSELN, DIE NICHT **SIE** VERSCHLÜSSELT HABEN!!!
d.h. – VERSUCHT EIN ZWEITER BENUTZER EINE DATEI ZU ENTSCHLÜSSELN, DIE DURCH DEN HAUPTBENUTZER VERSCHLÜSSELT WURDE, WIRD DIE DATEI ZERSTÖRT!!!

## Sicherheitsprofile

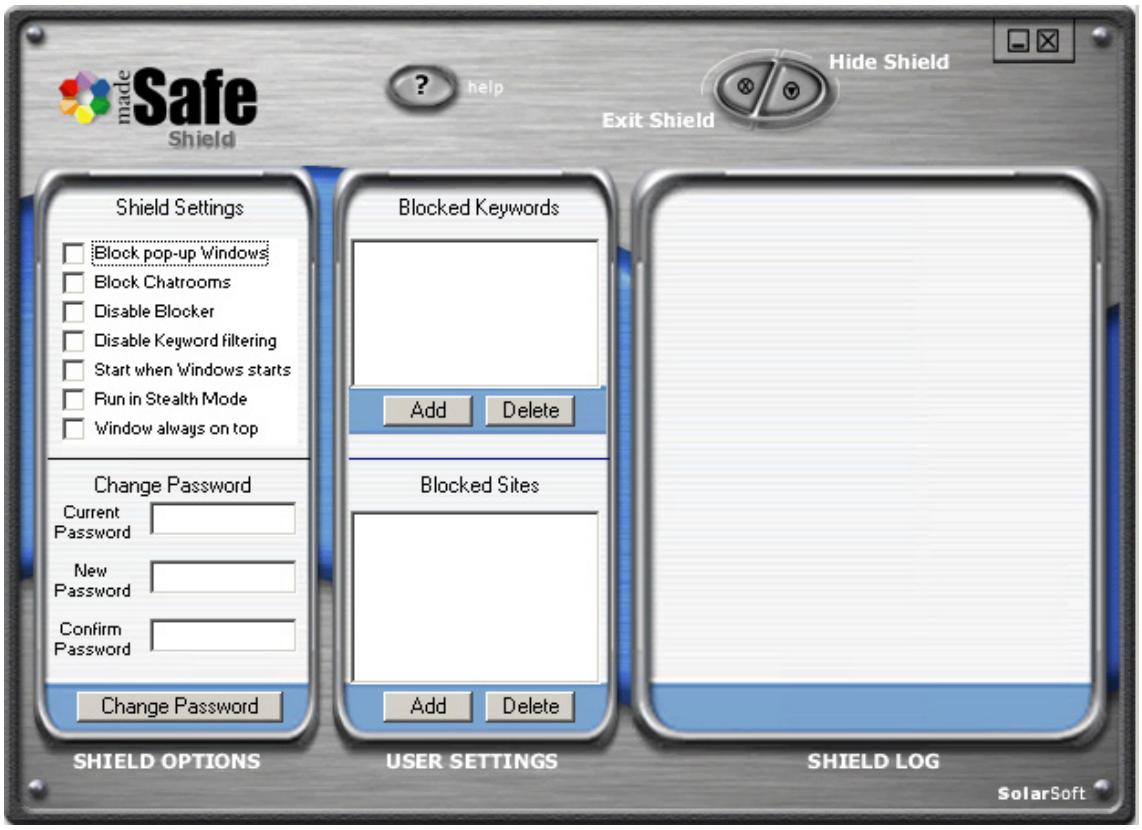

Wählen Sie aus diesen drei Optionen aus:
„Verschlüsselungs-Einstellungen“, „Filter-Einstellungen“ und „Datenbank“.

Im Menu „Verschlüsselungs-Einstellungen“ finden Sie zwei Schieberegler, mit welchen Sie Geschwindigkeit und Stärke der Verschlüsselung einstellen können. Erhöhen Sie die Stärke, wird die Verschlüsselung langsamer. Erhöhen Sie die Geschwindigkeit, nimmt die Verschlüsselungs-Stärke ab.



## Internet-Inhaltsfilter

Filter-Einstellung – Mit dieser Option stellen Sie ein, wie Ihr Computer auf dem Internet surfen soll. Die Filter-Optionen können nur durch den Hauptbenutzer konfiguriert werden.




Wenn Sie von der Taskleiste auf Shield™ zugreifen, werden Sie aufgefordert, ein Passwort einzugeben. Das voreingestellte Passwort ist **Passwort**. Wir bitten Sie, dies über „Passwort ändern“ bei Gelegenheit zu ändern.

**Filter-Optionen**
**Pop-Up-Fenster sperren** – Aktivieren Sie diese Funktion, um ärgerliche Werbe-Fenster auszuschalten.
**Chat-Rooms sperren** – Dies verweigert den Zugriff auf alle Chat-Rooms.
**Sperrung deaktivieren** – Diese Funktion schaltet das Filter-Programm aus.
**Schlagwort-Filter deaktivieren** – Damit schalten Sie den Schlagwort-Filter aus.
**Windows Autostart** – Diese Funktion lädt den Filter gleichzeitig mit Windows.
**Stealth™-Modus** – Lässt das Programm diskret im Hintergrund laufen zu lassen.
**Fenster immer im Vordergrund** – Damit bleibt Shield™ immer im Vordergrund jedes Fensters.

**Gesperrte Schlagwörter** – madeSafe™ verfügt über eine integrierte Schlagwort-Liste; Sie können dieser Datenbank jederzeit weitere Schlagwörter hinzufügen.
**Gesperrte Seiten** – Diese Option erlaubt Ihnen, Seiten zu sperren, auf die nicht zugegriffen werden soll.
**Shield™-Protokoll** – Hier können Sie Internet-Tätigkeit auf dem Computer mitverfolgen. Gespeichert werden Name, Datum, Zeit und Seiten, auf die zugegriffen wurde.
**Sicherheits-Datenbank**
Diese Funktion erlaubt dem Hauptbenutzer, die Sicherheits-Einstellungen individuell anzupassen. Ein Beispiel: Ihr Unternehmen handelt mit Autos und Sie möchten nicht, dass jemand die Gewinnmargen erfährt. Sie ergänzen die Datenbank einfach mit „Gewinnmargen“, und madeSafe™ verweigert jeden Zugriff – mit Ausnahme des Hauptbenutzers – auf Dateien betreffend „Gewinnmargen“. Die Datenbank kann mit beliebig vielen Schlagwörtern ergänzt werden.

**Verschlüsseln**
So einfach war Verschlüsselung noch nie. Wählen Sie einfach das Laufwerk aus, dann den Ordner, in dem sich die Datei befindet und schliesslich die Datei/Dateien die Sie verschlüsseln möchten und klicken Sie auf die Schaltfläche „Verschlüsseln“.


Das wär’s. Auf diese Dateien können nun nur noch **Sie** zugreifen.

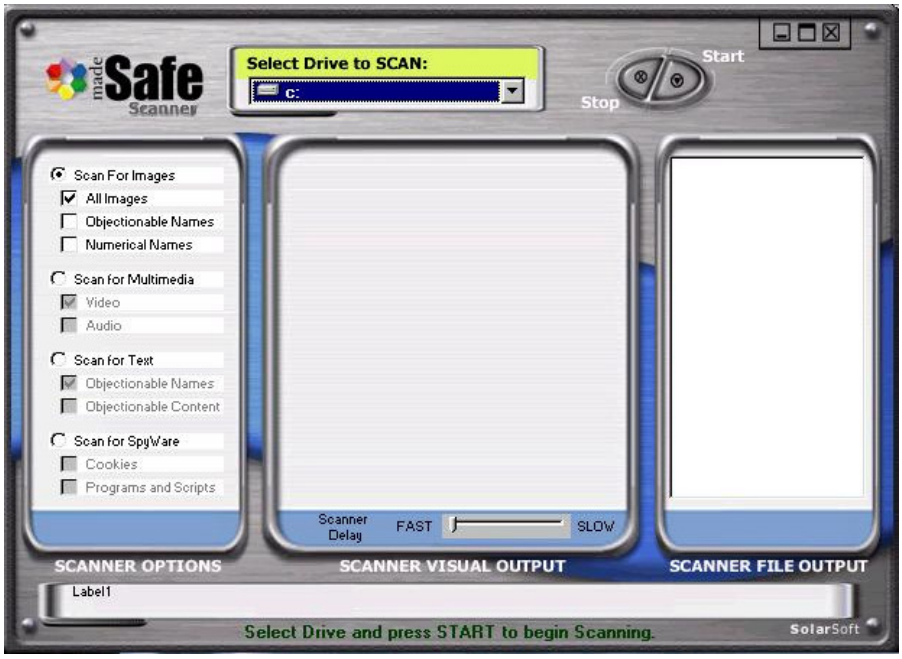
Dateien wieder zu entschlüsseln, ist genauso einfach. Markieren Sie die verschlüsselten Dateien, die Sie entschlüsseln möchten und klicken Sie auf „Entschlüsseln“.

Verschlüsselte Dateien erkennen Sie an der Dateiendung .ENC.

**Stealth™**
Für höchste Sicherheit können Sie bei den bereits verschlüsselten Dateien zusätzlich Stealth™ anwenden. Dadurch werden verschlüsselte Dateien, sollte die Festplatte durchsucht werden, unsichtbar. Markieren Sie einfach den Ordner, in dem sich die verschlüsselten Dateien befinden und klicken Sie auf „Stealth anwenden“. Die Dateien sind nun nicht mehr sichtbar.

Um so verhüllte Dateien wieder sichtbar zu machen, markieren Sie einfach den Ordner, in dem sie sich befinden und klicken auf „Stealth entfernen“.

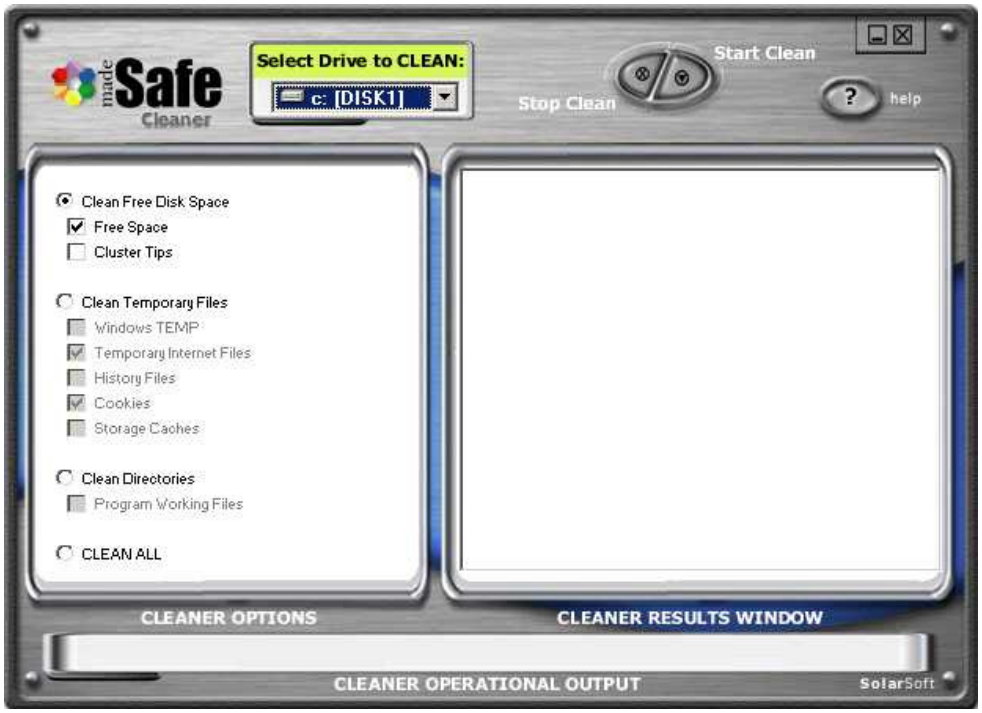
**Scannen**
Mit dieser Funktion durchsuchen Sie Ihre Festplatte nach anstössigem Material. Sie können nach Bildern, Videos, Text und allen anderen Datei-Typen suchen, die Ihrer Ansicht nach anstössiges Material enthalten könnten.




Wählen Sie den Durchsuchungs-Typ aus und klicken Sie auf “Start”. Im mittleren Fenster wird das gefundene visuelle Material angezeigt. Um die Dateien einzeln anzuschauen, muss der Scan-Vorgang mit dem Schieberegler verlangsamt werden. Im rechten Fenster werden die entsprechenden Dateibezeichnungen/Dateinamen aufgelistet.

## Reinigen

Diese Funktion reinigt die Festplatte und macht so auf sichere Weise Speicherplatz frei. Damit Hacker weder Passwörter noch Dateien entdecken können, löscht sie nicht mehr benutzte Datei-Ansammlungen und Eingabeverläufe. Diese Funktion wird idealerweise benutzt, nachdem „Schredden“ angewandt wurde. Da sie ausserordentlich gründlich ist, kann es - abhängig von der gewählten Reinigungs-Option - eine Weile dauern, bis der Vorgang abgeschlossen ist.




**Schredden**

Damit kann jede Datei auf Ihrem Computer vollständig zerstört werden. Bevor Sie „Schredden“ anwenden, müssen Sie sich bewusst sein, dass zerstörte Dateien unter keinen Umständen wiederhergestellt werden können.


Bevor der Prozess zu laufen beginnt, werden Sie noch einmal gefragt, ob Sie die Datei wirklich “Schredden” möchten.

## Geschützte E-Mails


Dieser Vorgang erlaubt Ihnen, verschlüsselte Dateien um den ganzen Erdball zu senden, ohne dass der Empfänger ebenfalls madeSafe™ auf seinem Computer installiert haben muss. Wählen Sie zuerst das Sicherheits-Niveau aus (geringe oder hohe Sicherheit). Sie werden nun aufgefordert, die E-Mail-Anlage, die sie schützen/verschlüsseln möchten, auszuwählen. Der Assistent wird Sie durch den ganzen Vorgang begleiten. Als Teil des E-Mails werden Anweisungen mitgesandt, wie das Mail gelesen werden kann. Dazu muss der Empfänger WinZip auf seinem Computer installiert haben. Nun brauchen Sie dem Empfänger zur Entschlüsselung nur noch das Passwort zu übermitteln.

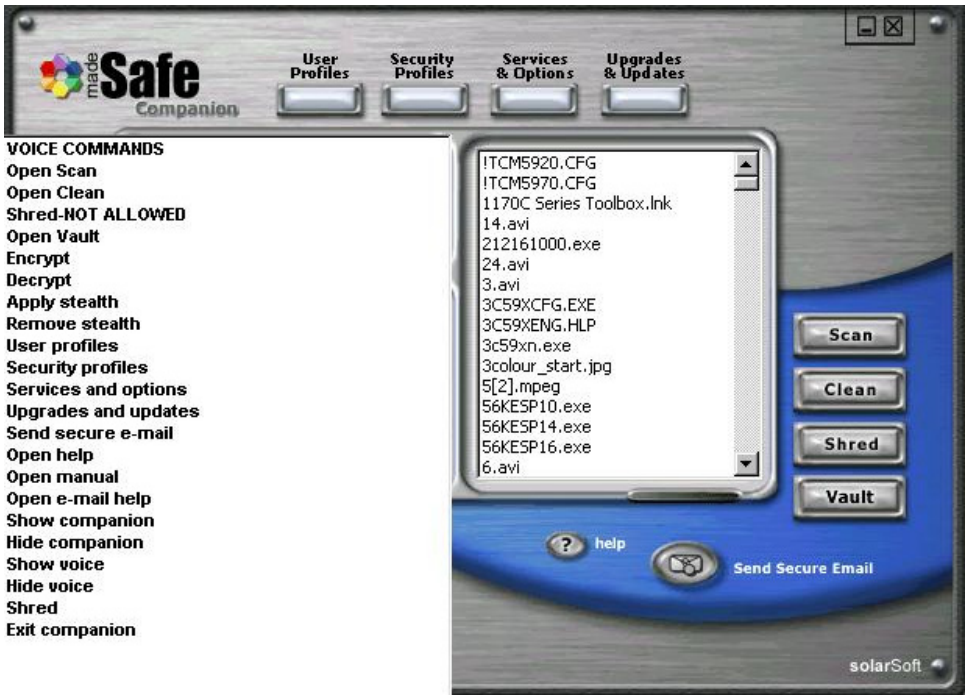
## Tresor™-Bedienung

Tresor ist ausgesprochen bedienerfreundlich. Sobald Sie Benutzernamen und Passwort eingegeben haben, sehen Sie den hier gezeigten Bildschirm. Sie verfügen über 10 Schubladen, die nach Ihren Wünschen beschriftet werden können.
Um eine Schublade zu öffnen, klicken Sie einfach auf die entsprechende grüne Lampe. Nun wird der Inhalt der Schublade angezeigt.


Um Dateien an Ihren Tresor (Tresor™) zu übermitteln, ziehen Sie diese mit der Maus einfach in die offene Schublade („Drag and Drop“). Sie werden gefragt, ob Sie die Dateien gleich oder erst später senden möchten. Möchten Sie die Dateien erst später senden, werden sie in eine Warteschlange gestellt. Sobald Sie die Auswahl abgeschlossen haben, klicken Sie auf „Dateien senden“. Möchten Sie Dateien zurückzuholen, gehen Sie umgekehrt vor. Wählen Sie in Ihrem Tresor™ die entsprechenden Dateien aus und klicken Sie auf die Schaltfläche „Zurückholen“.

Mit dem Verschieben von Dateien in den Tresor verändert sich auch die Kapazitätsanzeige. So wissen Sie immer, wie viel Speicherplatz Ihnen noch zur Verfügung steht. Sobald Ihr Tresor zu 85% gefüllt ist, werden Sie gebeten, mehr Tresor™-Platz zu kaufen. Das Hinweisfenster führt Sie auf unsere Website, wo Ihnen alles Weitere erklärt wird.

## Sprachbefehle




In madeSafe™ können Sie sich auch unter Verwendung von Sprachbefehlen bewegen. Möchten Sie die Liste der Befehle anschauen, sagen Sie einfach „Sprachbefehle anschauen“ und die Liste mit den Befehlen erscheint. Geben Sie „V“ ein, erscheint die Liste ebenfalls. Um die Liste wieder auszublenden, geben Sie „Strg+V“ ein.

Hier ist die Liste mit allen in madeSafe™ verfügbaren Sprachbefehlen:

| **Companion™ Befehle** | **Scan-Befehle** |
|---|---|
| <Sagen Sie>=Scannen öffnen | <Sagen Sie>=Scannen starten |
| <Sagen Sie>=Reinigen öffnen | <Sagen Sie>=Scannen anhalten |
| <Sagen Sie>=Vault öffnen | <Sagen Sie>=Hilfe öffnen |
| <Sagen Sie>=Verschlüsseln | <Sagen Sie>=Hilfe schliessen |
| <Sagen Sie>=Entschlüsseln | <Sagen Sie>=Scanner anzeigen |
| <Sagen Sie>=Stealth anwenden | <Sagen Sie>=Scanner ausblenden |
| <Sagen Sie>=Stealth entfernen | <Sagen Sie>=Sprachbefehle anzeigen |
| <Sagen Sie>=Benutzerprofile | <Sagen Sie>=Sprachbefehle ausblenden |
| <Sagen Sie>=Sicherheitsprofile | <Sagen Sie>=Alle Bilder |
| <Sagen Sie>=Dienstleistungen und Optionen | <Sagen Sie>=Anstössige Bilder |
| <Sagen Sie>=Erweiterungen und Aktualisierungen | <Sagen Sie>=Bilder numerisch |
| <Sagen Sie>=Geschütztes E-Mail senden | <Sagen Sie>=Multimedia Video |
| <Sagen Sie>=Hilfe öffnen | <Sagen Sie>=Multimedia Audio |
| <Sagen Sie>=Bedienungsanleitung öffnen | <Sagen Sie>=Text Namen |
| <Sagen Sie>=E-Mail-Hilfe öffnen | <Sagen Sie>=Text Inhalt |
| <Sagen Sie>=Companion anzeigen | <Sagen Sie>=Spion Programme |
| <Sagen Sie>=Companion ausblenden | <Sagen Sie>=Spion Cookies |
| <Sagen Sie>=Sprachbefehle anzeigen | <Sagen Sie>=Media abspielen |
| <Sagen Sie>=Sprachbefehle ausblenden | <Sagen Sie>=Media anhalten |
| <Sagen Sie>=Schredden | <Sagen Sie>=Media Pause |
| <Sagen Sie>=Companion schliessen | <Sagen Sie>=Schneller scannen |
| | <Sagen Sie>=Langsamer scannen |
| | <Sagen Sie>=Scanner schliessen |

# Kapitel 3 > Was bedeutet Ihnen Sicherheit?

**Sicherheit dominiert das 21. Jahrhundert**

Im heutigen elektronischen Zeitalter ist das Speichern vertraulicher Daten zunehmend der Gefahr von Diebstahl, Betrug und Zerstörung durch technisch immer raffinierter werdende Angriffe ausgesetzt.

Die Notwendigkeit, heikle Daten elektronisch zu zentralisieren, stellt für Möchtegern-Hacker und Cyberterroristen offensichtliche und erkennbare Angriffspunkte dar.

Der dadurch entstehende emotionale und finanzielle Schaden kann katastrophale Auswirkungen haben. Was die Sache noch schlimmer macht, ist die Tatsache, dass gemäss aktuellen Untersuchungen des FBI die grössten Gefahren innerhalb einer Organisation lauern.

**Es kann jeden treffen.**

Nicht nur Unternehmen drohen Gefahren aus dem Cyberspace. Jedes mal, wenn Sie sich von zu Hause aus ins Internet einwählen, werden Ihre persönlichen und privaten Informationen dem immer grösser werdenden Risiko ausgesetzt, von Eindringlingen missbraucht zu werden.

**Moderne Sicherheitslösungen**

Der zur Zeit erhältliche Schutz gegen diese Art von Bedrohung lässt sich in drei Kategorien einteilen: vorgeschaltete Sicherheitssysteme (Firewall), Antivirus- und einfache Verschlüsselungsprodukte.

Die Vermehrung und zunehmende technische Raffinesse der Viren, die Anwendungen unterbrechen, ganze PCs ausser Betrieb setzen und per E-Mail replizieren können, machen solche Antivirus-Programme für Privatpersonen wie Unternehmen zu einem absoluten Muss. Leider trägt Antivirus-Software bis heute wenig dazu bei, die Datenintegrität zu schützen.

Firewalls (Hardware und Software) haben sich zum Schutz vor engagierten Hackern in der Vergangenheit als relativ unsicher erwiesen. Um unerlaubten Zugriffen innerhalb einer Organisation vorzubeugen, sind sie teilweise sogar nutzlos.

Datenverschlüsselung scheint die naheliegendste Lösung zum Schutz vor solchen Angriffen zu sein. Die erhältlichen Produkte sind teilweise jedoch sehr kompliziert oder nicht wirklich sicher.

**Um diesen Gefahren die Stirn bieten zu können, sind eine neue Denkhaltung und neue Technologien notwendig...**

# Die Antwort heisst madeSafe™

## Kapitel 3 > Was bedeutet Ihnen Sicherheit?

Stellen Sie sich folgendes Szenario vor:

Sie nehmen Ihren Job als Systemadministrator ernst und haben in Ihr Netzwerk nur das Beste in Sachen Sicherheitsvorkehrungen implementiert. Der Firewall ist eingerichtet und mit den neuesten Patches versehen. Die Router sind richtig konfiguriert. Alle Benutzer- und Gruppenberechtigungen wurden geprüft und bestätigt.

Eines Tages ruft Sie der Generaldirektor zu sich ins Büro, um Ihnen zu berichten, dass Kunden angerufen und sich beschwert hätten, ihre Kreditkarten seien unberechtigterweise mit Gebühren belastet worden. Aber damit noch nicht genug. Die Kreditkarte des Unternehmens sei ebenfalls aus unbekannten Gründen mit £15,000 belastet worden.

Eine detaillierte Inspektion der Logbuch-Datei bringt einige erfolglose Zugriffs-Versuche zu Tage. Nach einer zweiten und dritten Durchsicht kommen Sie zum Schluss, dass es nur jemand von innerhalb des Unternehmens gewesen sein kann. Sie kontrollieren die Benutzerkennungen auf dem Kundendaten-Server und die einzigen, die Sie finden, sind Ihre eigenen. Sie kontrollieren auch den Server, auf dem sich die Finanzdaten befinden und die einzigen Benutzerkennungen die Sie finden können, sind die des Generaldirektors. Bei einem genaueren Blick auf die Anmelde-Zeiten stellen Sie fest, dass die Benutzerkennung des Generaldirektors benutzt wurde, als er an einer Konferenz war und mindestens eine Ihrer Benutzerkennungen wurde an einem Tag verwendet, an dem Sie den ganzen Tag in einer Sitzung waren. Jemand hatte also physischen Zugriff auf Ihre Server und hat Informationen, inklusive Benutzernamen und Passwörter, gestohlen.

Dies ist ein frei erfundener Vorfall, aber einer, der in Wirklichkeit wieder und immer wieder geschieht. Hat jemand physischen Zugriff auf Ihren Server, kann auf alle Informationen zugegriffen werden. Der Eindringling kann sich ungenehmigten Zugriff auf das Netzwerk verschaffen und dort jegliche Information stehlen oder kopieren. Die einzige Möglichkeit, dies zu verhindern, ist, den Zugriff auf Ihre Server einzuschränken. Selbstverständlich ist physische Sicherheit nicht nur auf Server begrenzt. Auch Laptops und Arbeitsstationen müssen mit einbezogen werden. Das betrifft Sie, den Kunden und den IT-Profi.

## Die Antwort heisst madeSafe™

# Kapitel 4 > Problembehandlung

## HÄUFIG GESTELLTE FRAGEN

**1) Wie verschlüssle ich eine Datei?**
Öffnen Sie einfach Ihren Companion™ und klicken Sie das Laufwerk an, in der sich die Datei befindet. Nun klicken Sie auf die Datei, die Sie verschlüsseln möchten. Jetzt brauchen Sie nur noch auf die Schaltfläche „Verschlüsseln“ zu klicken. Die Datei ist nun nur noch für Sie sichtbar.

**2) Wie erkenne / entschlüssle ich eine verschlüsselte Datei?**
Die verschlüsselten Dateien tragen die Dateinamenserweiterung .ENC. Um die Dateien zu entschlüsseln, markieren Sie sie und klicken einfach auf die Schaltfläche „Entschlüsseln“.

**3) Ich habe einige Dateien verschlüsselt. Jetzt sind sie verschwunden. Wie finde ich sie wieder?**
Möglicherweise haben Sie bei der Verschlüsselung der Dateien Stealth™ angewendet. Wählen Sie das Laufwerk aus und klicken Sie auf „Stealth™ entfernen“. Nun ist Stealth™ von ALLEN verschlüsselten Files entfernt.

**4) Ich habe mein Passwort vergessen. Wie stelle ich meine Daten wieder her?**
Solarsoft rät dringend, den Passwortschutz-Plan abzuschliessen, um diese Situation zu vermeiden. Verfügen Sie über diesen Schutz, können Sie unseren Support kontaktieren, der Ihnen umgehend Ihr Passwort mitteilen wird. Ohne sind die Dateien nicht wieder herstellbar.

**5) Auf meinem Computer befinden sich vertrauliche Daten, die ich dauerhaft entfernen** möchte. Wie mache ich das?
Auf dem Companion™ finden Sie die Schaltfläche „Schredden”. Markieren Sie die Datei, die sie DAUERHAFT entfernen möchten und klicken Sie auf „Schredden“. Nun ist die Datei zerstört und kann nicht wiederhergestellt werden.

**6) Ich besitze madeSafe™ Home und möchte es um die Vault™-Funktion erweitern. Wie mache ich das?**
Um Vault™ zu kaufen, klicken Sie einfach auf die Schaltfläche “Erweiterung” auf Ihrem Companion™ und folgen Sie den Anweisungen auf dem Bildschirm.

**7) Meine Kinder beschweren sich, das Internet funktioniere nicht mehr richtig. Woran kann das liegen?**
Einige Internetseiten werden in einem neuen Fenster geöffnet. Diese Funktion ist standardmässig eingeschaltet. Um sie auszuschalten, klicken Sie auf das entsprechende Symbol in der Symbolleiste und setzen ein Häkchen bei „Pop-Up-Fenster ausschalten“.

**8) Ein Freund hat mir mitgeteilt, er habe mir ein geschütztes E-Mail gesandt, welches ich jedoch nicht erhalten habe.**
Das verschlüsselte E-Mail wird als .zip-File gesandt. Die meisten Firewalls und Antivirus-Programme fangen diesen Dateityp auf. Schalten Sie das Antivirus-Programm / den Firewall aus, um dieses Mail empfangen zu können.

# Kapitel 5 > Glossar

**Active Stealth Technology™**
madeSafes Active Stealth Technology™ erlaubt dem Nutzer, bereits verschlüsselte Daten so zu verstecken, dass Hacker oder unerwünschte Eindringlinge keine vollständige Quelle oder einen Eintrittspunkt finden können

**Algorithmus (Hash)**
Eine (logische) Rechenvorschrift oder ein Verfahren, das bei der Erstellung einer Mitteilung und bei der Erzeugung von Schlüsseln und (digitalen) Unterschriften verwendet wird

**Algorithmus (Verschlüsselung)**
Eine (logische) Rechenvorschrift oder ein Verfahren, das bei Ver- und Entschlüsselungsprozessen verwendet wird

**Antivirus**
Ein Programm, das den PC vor internetbasierten Viren schützt. Typischerweise führen solche Viren zu kostspieligen und zeitraubenden Störungen/Unterbrechungen

**Asymmetrische Schlüssel**
Ein getrenntes aber in Beziehung zueinander stehendes Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Jeder Schlüssel ist nur einseitig benutzbar, das heisst, der Schlüssel, der zu Verschlüsselung der Information benutzt wird, kann nicht auch zur Entschlüsselung derselben Daten verwendet werden

**Authentifizierung**
Echtheitsbestätigung/-nachweis. Der Vorgang, der zur Feststellung der Identität eines Benutzers, der auf das System zuzugreifen versucht, verwendet wird

**Blinde Unterschrift**
Die Fähigkeit, etwas zu unterschreiben, ohne den Inhalt zu kennen (vergleichbar mit einem Notar)

**Blockweise Verschlüsselung**
Eine symmetrische Verschlüsselung die in Blöcken (normalerweise 64 Bits) von Plain-Text und chiffriertem Text arbeitet. *Siehe auch Plain-Text*

**Blowfish**
Verbesserte blockweise Verschlüsselung, symmetrischer Algorithmus

**Chiffrierter Text**
Plain-Text wird durch die Verwendung eines Verschlüsselungs-Algorithmus in ein „geheimes Format“ umgewandelt. Der chiffrierte Text kann durch einen Schlüssel wieder in den originalen Plain-Text umgewandelt werden. *Siehe auch Plain-Text*

**Client**
Der Computer, der die Anfragen an einen Server stellt und Inhalte vom Server erhalten kann. Verbinden Sie sich zum Beispiel mit einem ISP oder Firmennetzwerk, ist Ihr Computer der Client und der ISP oder Netzwerkcomputer ist der Server. Als Client wird inzwischen auch die Programmumgebung des Nutzer-PCs bezeichnet. *Siehe auch ISP*

**Codierung**
Schütz heikle E-Mail-Nachrichten und dessen Anlagen. *Siehe auch Verschlüsselung*

**Companion™**
Der madeSafe Security Companion™ ist eine einfach zu bedienende Benutzeroberfläche (auch Player genannt), die den Benutzer von einer einzigen Plattform auf alle madeSafe™-Produkte, Erweiterungen und Dienstleistungen zugreifen lässt

**Cookie**
Ein kleines Informations-Element, das die Nutzer im WWW eindeutig identifiziert, sobald sie mit einem Cookie-tauglichen Web-Browser eine Website erneut besuchen (das Cookie wird beim ersten Besuch vom Web-Server durch den Web-Browser auf die Festplatte Ihres Computers gespeichert). Grundsätzlich sind Cookies ideal, um gerade bei passwortgeschützten Bereichen dem Nutzer das Leben zu erleichtern, in dem z.B. Nutzerdaten automatisch in Bestellformulare eingetragen werden oder der Passworteintrag automatisiert werden kann. Wegen datenschutzrechtlicher Bedenken ist dem Nutzer jedoch die Entscheidung über die Nutzung des Cookies zu überlassen. Über spezielle Einstellungen im Browser kann man sich vor Cookies warnen lassen oder sie ausschalten

**Cracker**
Jemand, der den Kopierschutz eines Programms entfernt oder umgeht, normalerweise indem er das Programm verändert.

**Datenintegrität**
Ein Verfahren, das sicherstellt, dass keine Informationen auf unerlaubten oder unbekannten Wegen verändert wurden

**Decodierung**
Den Schutz auf einer E-Mail-Nachricht und dessen Anlagen entfernen. *Siehe auch Entschlüsselung*

**DES (Data Encryption Standard)**
Ein konventionelles Verschlüsselungssystem, das häufig auf Regierungsebene eingesetzt wird. Arbeitet 64-Bit blockweise (block cipher) und verwendet einen symmetrischen Algorithmus. DES ist auch bekannt unter „Data Encryption Algorithm (DEA)“ von ANSI und DEA-1 von ISO

**Digitale Unterschrift**
Mit den digitalen Unterschriften und dem dazugehörigen Dokument der Zertifizierungsbehörde werden Dokumente unterschrieben. So kann die Quelle des Dokumentes oder der Anwendung genau festgestellt werden

**Digitales Zertifikat**
Ein Dokument, das von einer Zertifizierungsbehörde ausgestellt wird, um die Echtheit eines Webdokumentes oder einer URL zu beweisen. Ein digitales Zertifikat ist eine passwortgeschützte, verschlüsselte Datei, die zusätzlich zur „normalen“ gesendeten Nachricht, die verschlüsselte Nachricht und die Benutzer-Identifikation enthält. Obwohl immer noch jeder Computer auf dem Internet auf die sich im Verkehr befindende Datei zugreifen könnte, kann nur der beabsichtigte Empfänger die Nachricht entschlüsseln und lesen.

**EES (Escrowed Encryption Standard)**
Ein von der US-Regierung vorgeschlagener Verschlüsselungsstandard

**Entschlüsselung**
Ein Verfahren, das verschlüsselte Informationen wieder so zusammenfügt, dass sie gelesen werden können. Zur Entschlüsselung wird der private Schlüssel des Empfängers verwendet. *Siehe auch Decodierung*

**Extranet**

Ein Netzwerk, das ein Unternehmensnetzwerk mit dem weltweiten Internet verbindet. Extranets sind dazu gedacht, von unternehmensinternen Verkäufern und anderen vertrauenswürdigen Handelspartnern genutzt zu werden, um den Austausch von Produkten, Dienstleistungen und anderen Informationen zu beschleunigen

**File Transfer Protocol (FTP)**
FTP ist ein standardisiertes Protokoll/Programm, das systemunabhängige Datenübertragung zwischen zwei Rechnern ermöglicht, sei es über das Internet oder zwischen PCs auf einem Netzwerk

**Firewall**
Der Firewall ist ein Rechner, der auf der einen Seite mit dem Internet und auf der anderen Seite mit dem Firmennetz verbunden ist. Jedes Datenpaket, das ins Firmennetz rein oder raus will, wird von der Software auf dem Rechner kontrolliert, was gegen Eingriffe von aussen als Barriere wirkt. *Siehe auch Proxy-Server*

**Hacker**
Führen Angriffe auf Computersysteme aus. *Siehe auch Cracker*

**HTML (Hyper Text Markup Language)**
Seitenbeschreibungs-/Programmiersprache für WWW-Dokumente mit der Möglichkeit zur Einbindung von Bildern und anderen multimedialen Elementen

**HTTP (Hyper Text Transfer Protocol)**
Dieses Protokoll wir zum Transport von HTML-Dokumenten im Internet verwendet

**HTTPS (HTTP over SSL)**
HTTP over SSL. Ist das sichere Protokoll zum Transport von HTML-Dokumenten im Internet. *Siehe auch HTTP*

**Hyperlink**
Ein Wort, Satz (normalerweise durch Unterstreichung gekennzeichnet) oder Bild, das durch Anklicken mit der Maus mit einem anderen Dokument verlinkt wird

**Inhaltsfilter**
Vermeidet, dass Kinder oder Angestellte beim Surfen auf dem Internet anstössiges oder schädliches Material zu Gesicht bekommen. *Siehe auch Internet-Inhaltsfilter*

**Integrität**
Gewissheit, dass Daten während der Übertragung oder solange sie gespeichert waren, nicht (durch unberechtigte Personen) verändert wurden

**Internet**
Das weltgrösste Computernetzwerk, das unzählige Unter-Netzwerke miteinander verbindet

**Internet-Inhaltsfilter**
Der Internet-Inhaltsfilter ist eine Standardfunktion von madeSafe™ Home und als Erweiterung zu madeSafe™ Mobile und Business erhältlich. *Siehe auch Inhaltsfilter*

**Intranet**
Einheitliche, meist mit der Internet-Technologie realisierte Datenübertragung innerhalb einer Organisation

**ISO (International Organization for Standardization)**

Eine Organisation, die für eine Fülle von Technologie-Standards verantwortlich ist

**ISP (Internet Service Provider)**
Eine Firma, die für Benutzer, die sich über ein Modem einwählen und/oder Firmennetzwerke Zugriff aufs Internet gewährt. Der Zugriff wird Kunden auf einer Art Service-Basis „vermietet“

**Kryptographie**
Kryptographie ist die Wissenschaft von der Ver- und Entschlüsselung von Daten mit Hilfe mathematischer Verfahren

**Künstliche Intelligenz**
Ein Zweig der Computerwissenschaft, der Technologien entwickelt, die das intelligente menschliche Verhalten nachahmen können

**MIME (Multipart Internet Mail Encoding)**
Verfahren, um auf einem Browser, die empfangenen Daten als Grafik, Musikdatei oder Text zu identifizieren und entsprechend darzustellen

**Nachrichten-Authentifizierung**
Der Vorgang, den Sender und den Empfänger einer E-Mail-Nachricht sicherzustellen

**Öffentlicher Schlüssel**
Der Teil eines Schlüsselpaares, mit dem die Nachricht verschlüsselt wird. Der öffentliche Schlüssel kann nicht zur Entschlüsselung verwendet werden; dazu benötigt man den zugehörigen privaten oder geheimen Schlüssel. Der öffentliche Schlüssel ist allen bekannt, der private dagegen bleibt geheim. *Siehe auch privater Schlüssel*

**Passphrase**
Eine Passphrase besteht aus mehreren Wörtern und ist daher theoretisch sicherer als ein Passwort. Die sichersten Passphrasen sind relativ lang und komplex und enthalten eine Kombination aus Klein- und Grossbuchstaben, Zahl- und Interpunktionszeichen.

**Passwort**
Eine Zeichenfolge oder ein Wort, die ein Nutzer an ein System zur Authentifizierung, als Beweis oder zur Überprüfung übermittelt

**PGP (Pretty Good Privacy)**
PGP ist ein hybrides Verschlüsselungssystem, in welchem einige der besten Funktionen der konventionellen Verschlüsselung und der Verschlüsselung mit öffentlichen Schlüsseln vereint sind

**PKI (Public Key Infrastructure)**
Ein System, das über Sicherheit, Speicherkapazität und den Austauschmechanismus verfügt, um öffentliche Schlüssel resp. die Zertifikate dazu aufzubewahren und zu verteilen. Zudem besitzt es Zertifikatsverwaltungsfunktionen (die Fähigkeit, Zertifikate auszustellen, zurückzunehmen, zu speichern, abzurufen und Zertifikaten zu vertrauen)

**Plain-Text**
Klartext, unchiffrierter Text. Daten, die von jedermann gelesen und verstanden werden können

**Privater Schlüssel**
Privates oder geheimes Schlüsselpaar, dass zur Unterschrift und Entschlüsselung von Information verwendet wird. Der private Schlüssel sollte geheim gehalten werden und nur dem Nutzer bekannt sein. *Siehe auch öffentlicher Schlüssel*

**Proxy / Proxy-Server**
Ein Proxy oder Proxy-Server dient im WWW als Zwischenstation auf dem Weg vom Client zum eigentlichen WWW-Server. Der Client fordert ein Dokument in dieser Konfiguration nicht unmittelbar vom Ursprungsserver an, sondern wendet sich an den Proxy. Dieser besorgt das Dokument und leitet es an den Client weiter. Proxy-Server agieren oft als Firewalls. *Siehe auch Firewall*

**Reinigen**
madeSafes Reinigungs-Funktion reinigt und räumt auf sichere Weise Ihre Festplatte auf und macht so wertvollen Speicherplatz frei

**Scannen**
madeSafes Scan-Funktion durchsucht das ausgewählte Laufwerk nach Material, das der Hauptbenutzer als unangemessen betrachtet

**Schlüssel**
Ein Schlüssel ist ein Wert, der zur Erstellung eines verschlüsselten Textes, einer digitalen Unterschrift, zur Entschlüsselung sowie zur Verifikation von Nachrichten und Dateien verwendet wird. Es wird immer ein Schlüsselpaar benötigt. Schlüssel werden an Schlüsselbunden gespeichert

**Schlüsselbund**
Jeder Benutzer hat zwei Schlüsselbunde: einen privaten und einen öffentlichen

**Schlüsselgrösse**
Die Schlüsselgrösse wird in Bit angegeben. Je länger der Schlüssel, desto sicherer ist er

**Schlüsselverwaltung**
Das Verfahren und das Vorgehen zur sicheren Aufbewahrung und Verteilung kryptographischer Schlüssel

**Schredden**
madeSafes Schredder-Funktion löscht auf sichere Weise jede Datei / jedes Dokument, und zwar so, dass alle Spuren verwischt sind und es nicht wiederhergestellt werden kann

**Secure Cellular Architecture™**
madeSafe™ Home und Mobile verfügen über eine geschützte, verschlüsselte 448-Bit-Zelle, die die von Ihnen ausgewählten Dateien umgibt. Dies gewährleistet einen sicheren, durch den Hauptbenutzer genehmigten und kontrollierten Mehrfachbenutzer-Zugriff.
madeSafe™ Business ist mit einer Hauptbenutzerzelle und weiteren Zellen für ausgewählte Benutzer ausgestattet. Verschlüsselungsgrad und Funktionalität sind in allen Zellen gleich. Der Hauptbenutzer hat jedoch umfassende Kontrolle und überall Zugriff

**Secure Channel**
Wörtlich: Geschützter/sicherer Übertragungskanal. Eine Website, die die sichere Übertragung von an sie übermittelter Information garantiert

**Server**
Ein Rechner, der Daten für den Abruf eines Clients aus einem Rechnernetz bereit hält. *Siehe auch Client*

**SET (Secure Electronic Transactions)**
Ein Standard zur sicheren Übermittlung von E-Commerce-Transaktionsdaten im Internet

**Sicherheit**
Verfahren, die Computer-Ressourcen inklusive Daten, Hardware, Telekommunikations-Leitungen und Programme vor unberechtigtem Zugriff schützen

**SLIP (Single Line Internet Protocol)**
Einfaches, älteres Protokoll, das eine Verbindung von einem PC zu einem Provider herstellt

**Smart Encryption™**
madeSafes Verschlüsselungstechnologie, kombiniert mit künstlicher Intelligenz heisst Smart Encryption™. Die madeSafe™-Produkte sind standardmässig auf 448-Bit Superverschlüsselung eingestellt. Der Verschlüsselungsgrad kann, wenn Sie z.B. den Vorgang beschleunigen möchten, über das Sicherheitsprofil auf Ihrem madeSafe Companion™ verringert werden

**S/MIME (Secure Multipart Internet Mail Encoding)**
Eine Verschlüsselungsmethode für E-Mails. *Siehe auch MIME*

**SMTP (Simple Mail Transport Protocol)**
Das Standardprotokoll für die Übertragung von E-Mails

**SSL (Secure Socket Layer)**
Sehr sicheres Übertragungsprotokoll im Internet, das von Netscape entwickelt wurde und auf einem Verschlüsselungsverfahren basiert. Sender und Empfänger der übermittelten Information können eindeutig identifiziert werden

**Steganographie**
Das Verfahren, Daten in anderen Daten zu verstecken. Eine Text-Datei könnte zum Beispiel „in" einer Bild- oder Sound-Datei versteckt werden. Würden Sie sich dann das Bild anschauen oder die Sound-Datei anhören, würden Sie aber nichts davon bemerken

**Suchmaschine**
Programm, welches das Internet automatisch nach durch den Benutzer spezifizierte Informationen durchsucht

**Symmetrischer Schlüssel**
Bei der konventionellen Verschlüsselung, auch Verschlüsselung mit Geheimschlüsseln oder symmetrischen Schlüsseln genannt, wird ein Schlüssel für die Ver- als auch die Entschlüsselung verwendet. madeSafe™ arbeitet mit symmetrischen Schlüsseln

**TCP/IP (Transmission Control Protocol/Internet Protocol)**
Protokoll, das festlegt, in welcher Form und nach welchen Regeln Daten von einem Server aus im Internet verschickt werden

**Time-Stamping**
Zeitmarke. Zeichnet auf, wann die Information erstellt wurde

**Two Fish**
Blockweise Verschlüsselung, die einen symmetrischen Algorithmus verwendet

**URL (Uniform Resource Locator)**
Die Seitenadresse, die verwendet wird, um eine Website (HTML-Dokument) im Internet zu lokalisieren. Die URL besteht aus vier Komponenten: Übertragungsprotokoll, Rechneradresse, Unterverzeichnis, Dateiname

**Validierung**
Verleiht Gewissheit, dass der Schlüssel tatsächlich dem angegebenen Besitzer gehört

**Tresor™**
Tresor™ erlaubt Ihnen, Ihre verschlüsselten Daten auf unsere extrem sichere madeSafe™ Website zu spiegeln, damit Sie über eine Sicherheitskopie verfügen, weltweit, 24 Stunden am Tag, 365 Tage im Jahr. madeSafe Tresor™ kann in 5 MB-Einheiten erweitert werden

**Verifikation**
Vergleicht eine (digitale), mit einem privaten Schlüssel erstellte Unterschrift mit dem dazugehörigen öffentlichen Schlüssel

**Verschlüsselung**
Eine Sicherheits-Methode, die Zugriff auf Information verhindert, indem sie sie in chiffrierten Text umwandelt. Der chiffrierte Text muss vom Internet-Nutzer entschlüsselt werden, bevor er ihn lesen kann. Verschlüsselung kann zum Schutz von sensitiven Computer-Dateien über die Übermittlung von Finanzdaten bis hin zu Telefonanrufen, die von digitalen Mobiltelefonen aus gemacht werden, verwendet werden

**VPN (Virtual Private Network)**
Normalerweise ein Intranet-basiertes, privates Netzwerk, das ein öffentliches Netzwerk (Internet) mit einem anderen Netzwerk Ihrer Wahl verbindet.

**WWW (World Wide Web)**
Als WWW versteht man alle Dateien , die im HTML-Datenformat im Internet liegen und über Hyperlinks miteinander verknüpft sind

**Zertifikat**
Ist eine digitale ID, ausgestellt durch eine Zertifizierungsbehörde, die verwendet wird, um dem Datenverkehr auf dem Internet Rechtskraft zu verleihen und übermittelte Dokumente als echt zu erweisen

**Zertifizierungsbehörde**
Eine Organisation, die digitale Zertifikate ausstellt, um die Identität eines E-Mail- oder Datei-Absenders zu beweisen

**Zufallszahl**
Ein zufällig generierter, einmaliger Schlüssel, der von einem unerwünschten Eindringling nicht berechnet oder vorhergesehen werden kann

**Zugriffsberechtigung**
Offizielle Berechtigung und/oder rechtsmässige Erlaubnis auf ein Element/Objekt zuzugreifen

# Kapitel 6 > Technischer Support

Solarsoft verpflichtet sich dazu, einen ausgezeichneten Service und Support zu bieten. Unser Ziel ist es, Ihnen die nötige professionelle Unterstützung zu bieten, damit Sie das Beste aus Ihrem madeSafe™-Produkt herausholen können.

**Registrierung**
Sobald Sie Ihr madeSafe™-Produkt registriert haben, sind Sie berechtigt, den Web-Support zu benutzen wie auch dazu, von den Aktualisierungen und Spezialangeboten Gebrauch zu machen.

**Kundendienst**
Auf unserer Website www.madesafe.com finden Sie umfassende und ausführliche Informationen zu madeSafe™. Oder schicken Sie uns eine E-Mail auf sales@madesafe.com.

**Gratis Web-Support**
Durch Anklicken der Schaltfläche "Hilfe" auf Ihrem madeSafe Companion™ können Sie direkt mit unserem Web-Support Kontakt aufnehmen. Oder Sie tun das direkt über www.madesafe.com/support. Der Web-Support steht Ihnen von Montag bis Freitag, 9.00-17.00 Uhr zur Verfügung.

**Telefon-Support**
Solarsoft bietet einen gebührenpflichtigen technischen Telefon-Support für alle madeSafe™-Produkte an. Kunden können über die Schaltfläche „Dienstleistungen & Optionen" auf Ihrem madeSafe Companion™ darauf zugreifen.

# Kapitel 7 > Copyrightvermerk & Markennamen

# Kapitel 8 > Kontakt

Wir freuen uns immer, von unseren Kunden hören. Möchten Sie mit uns Kontakt aufnehmen, rufen Sie uns an. Benötigen Sie aktuelle Informationen oder Support, besuchen Sie unsere Website.

Solarsoft Limited, Phillips House, Station Road, Hook, Hampshire, RG27 9HD, Grossbritannien

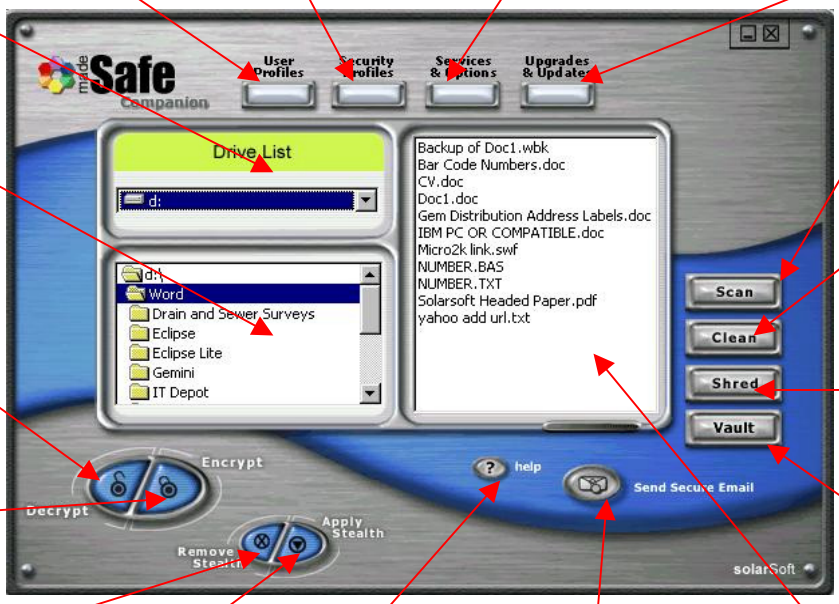
Telefon: +44 (0) 870 872 8210, Fax: +44 (0) 1256 769770
Web: http://www.madeSafe.com

# Kapitel 9 > Hilfe-Assistent


Sobald der Hilfe-Assistent sichtbar ist, wird die Funktion der Schaltflächen ausgeschaltet. Um Informationen zu den einzelnen Funktionen zu erhalten, klicken Sie einfach auf die Schaltfläche, zu der Sie mehr Informationen oder Hilfe benötigen. Der Hilfe-Assistent wird Ihnen diese Funktion erklären.

Hat er Ihnen die benötigte Erklärung geliefert, klicken Sie mit der rechten Maustaste auf den Hilfe-Assistenten und markieren Sie „Ausblenden“ oder benutzen Sie die „Escape“-Taste auf Ihrer Tastatur, um den Assistenten zu schliessen.

# Kapitel 10 > Kurzübersicht




**Einrichtung/Bearbeitung der Benutzer-Profile**

**Einrichtung/Bearbeitung der Sicherheits-Typen**

**Sehen Sie sich die erhältlichen Optionen und Dienstleistungen an**

**Schauen Sie nach, welche Aktualisierungen und Erweiterungen erhältlich sind**

**Ziel-Laufwerk**

**Zeigt die Dateien im laufenden Verzeichnis an**

**Ziel-Verzeichnis**

**Durchsucht Ihr Laufwerk nach Material, das der Hauptbenutzer als unangemessen betrachtet**

**Entschlüsseln Sie die ausgewählten Dateien**

**Reinigen Sie auf sichere Weise Ihre Festplatte**

**Verschlüsseln Sie die ausgewählten Dateien**

**Direktzugriff auf den persönlichen Tresor ™**

**Machen Sie unsichtbare Dateien wieder sichtbar**

**Machen Sie ausgewählte Dateien unsichtbar**

**Rufen Sie den Hilfe-Assistenten**

**Senden Sie geschützte E-Mails**

**Löschen Sie Dateien sicher und dauerhaft**