



"Technologie in Bewegung"



Kanguru Defender Elite Gebrauchsanleitung

HINWEISE UND INFORMATIONEN

Bitte lesen Sie die Anleitung, bevor Sie den Kanguru Defender in Gebrauch nehmen.

Copyright © 2012 Kanguru Solutions. Alle Rechte vorbehalten.

Windows 2000®, Windows ME®, Windows XP®, Windows Vista®, und Windows 7® sind registrierte Handelsmarken von Microsoft Inc. Alle anderen Marken oder Produktnamen sind Handelsmarken der jeweiligen Unternehmen oder Rechteinhaber.

Kanguru Solutions haftet nicht bei widerrechtlicher Produktanwendung oder Verlusten bei der Nutzung des Produktes. Der Nutzer ist selbst verantwortlich dafür, dass die Urheberrechte beachtet werden und das Produkt nicht widerrechtlich verwendet wird.

Kundenservice

Technische Unterstützung für Ihr System erhalten Sie beim Technischen Support von Kanguru Solutions unter (508) 376-4245, oder besuchen Sie die Website www.Kanguru.com für den Online Support.

Rechtlicher Hinweis

In keinem Fall überschreitet die Gewährleistungspflicht von Kanguru Solutions den Kaufpreis des Produktes, und zwar weder den der unmittelbaren, mittelbaren, speziellen oder nachfolgenden noch der sonstwie erforderlichen Software oder ihrer Dokumentation. Kanguru Solutions bietet keine Erstattung für Produkte. Kanguru Solutions übernimmt ausdrücklich keine implizite und keine gesetzliche Garantie und keinen Ersatz für Produkte oder Inhalte oder die Anwendung der Dokumentation und der dazugehörigen Software. Vor allem die Haftung für die Produktqualität, ihre Leistung und ihre Marktfähigkeit oder -tauglichkeit für bestimmte Zwecke wird ausdrücklich abgelehnt. Kanguru Solutions behält sich das Recht vor, Produkte, Software oder Dokumentation jederzeit zu ändern oder anzupassen, ohne verpflichtet zu sein, Personen, Unternehmen oder andere Parteien darüber in Kenntnis zu setzen.

Ausfuhrerlaubnis

Ungeachtet jeglicher Ankündigung gegenüber Kanguru Solutions bezüglich des Bestimmungsortes eines bestimmten Produktes erklären Sie sich einverstanden, dass Ihnen der unmittelbare oder mittelbare Export von Kanguru-Produkten untersagt ist, ohne dass Sie vorher eine Genehmigung von Kanguru Solutions und eine entsprechende Exportlizenz vom Handelsministerium oder einer anderen Behörde einholen. Kanguru Solutions besitzt ein breites Spektrum an Produkten und für jede Produktfamilie sind die Lizenzbedingungen für die Ausfuhr unterschiedlich.

WARNUNG: Defragmentierung des Flash-Speichersticks

Versuchen Sie nicht, den Kanguru Defender Flash Stick zu defragmentieren. Eine Defragmentierung des Flash-Speichers ist nicht notwendig und hat keinen Einfluss auf die Leistung. Wenn Sie Ihren Flash Stick defragmentieren, kann das den Speicher verkleinern, so dass Gesamtkapazität und Laufzeit des Sticks verringert werden.

1.	Einleitung	5
1.1	Inhalt	5
1.2	Modelle des Kanguru Defender Elite	5
1.3	Funktionen	6
1.4	Technische Spezifikationen	7
2.	Kanguru Defender Manager Elite	8
2.1	KDMElite einrichten.....	8
2.1.1	KDMElite mit Windows	8
2.1.2	KDMElite mit Mac OS X	10
2.1.3	KDMElite mit Linux Ubuntu.....	11
2.1.4	KDMElite mit Red Hat Enterprise Linux 5	12
2.2	Der Setup Wizard.....	13
2.2.1	Setup-Sprache auswählen	13
2.2.2	Integrierten Virenschutz aktivieren (nur unter Windows)	14
2.2.3	Passwort einrichten	15
2.2.4	KRMC Cloud.....	16
2.2.5	Kontakt Info	17
2.2.6	Ihr Gerät mit Setup Wizard zurücksetzen	18
2.3	Sichere Partition entsperren	19
2.3.1	Login-Bildschirm zurücksetzen.....	20
2.4	Passwort mit Hilfe der virtuellen Tastatur VT eingeben.....	21
2.5	Dateien und Ordner verschlüsseln	22
2.6	Integrierter Virenschutz (nur unter Windows)	23
2.6.1	Gerät scannen.....	24
2.6.2	Pfad scannen	25
2.6.3	Ordner scannen	26
2.7	Ändern des Passwortes	27
2.8	KRMC Cloud: Einstellungen.....	28
2.9	Ändern der Spracheinstellung.....	29
2.10	Online-Dokumentation	30
2.11	Über KDMElite.....	30
2.12	Schließen des Defender Elite.....	31

3.	Sicheres Entfernen des Kanguru Defender Elite.....	32
3.1	Sicheres Entfernen unter Windows.....	32
3.2	Sicheres Entfernen unter Mac OS X.....	33
3.3	Sicheres Entfernen unter Linux	33
4.	Garantiehinweise	34
5.	Technischer Support.....	34
	Anhang A - Proxy Support.....	35

1. Einleitung

Kanguru Defender Elite ist ein hardwareverschlüsselter, zugriffssicherer USB Flash Stick. Defender Elite enthält zwei Laufwerke: einen CD-ROM-Bereich und eine sichere, verschlüsselte Partition. Im CD-ROM-Bereich können Sie sich anmelden, um Zugang zur sicheren Partition zu erhalten.

Der Kanguru Defender Flash Stick sichert Ihre sensiblen Daten mit:

- Hardwareverschlüsselung 256Bit AES
- Sicherem Passwortschutz

1.1 Inhalt

Bitte überprüfen Sie den Inhalt der Packung. Wenn einer der folgenden Gegenstände fehlt, wenden Sie sich bitte telefonisch an Kanguru Solutions unter (508) 376-4245, damit Sie so schnell wie möglich Ersatz erhalten.

- Kanguru Defender Elite USB Flash Stick
- Kurzanleitung
- Registrierungsformular
- Schlüsselband
- USB-Verlängerungskabel (nur Sticks ab 32GB oder mehr)

Vorsicht! Die Öffnung am Ende des Sticks ist ausschließlich für das mitgelieferte Schlüsselband bestimmt.

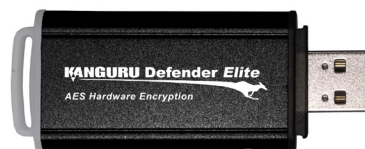
1.2 Modelle des Kanguru Defender Elite

Kanguru Defender Elite ist, abhängig von der Kapazität Ihres Laufwerks, in zwei Versionen verfügbar. Die Unterschiede zwischen den Modellen sind auf Seite 7 im Abschnitt 1.5 Technische Angaben ausführlich erläutert.

2GB - 16GB-Modell



32GB - 128GB-Modell



Systemvoraussetzungen

- USB-Port (USB 2.0 empfohlen)
- DDR RAM 256MB oder mehr
- CPU 500MHz oder schneller
- Betriebssysteme (32 und 64 Bit kompatibel)
 - Windows 2000 Service Pack 4, Windows XP Service Pack 3, Windows Server 2003, Windows Vista, Windows 7
 - Mac OS X und mehr (kompatibel nur zu intel-basierten Macs)
 - Red Hat Enterprise Linux 5, Ubuntu 9.10, Ubuntu 11.10

Anmerkung: Nutzer von Linux Red Hat müssen Superuser-Zugang haben oder andere Root-Zugriffsrechte, um KDMElite ausführen zu können.

1.3 Funktionen

- ✓ Hardwareverschlüsselung 256Bit AES
- ✓ FIPS 140-2 zertifiziert
- ✓ Passwortgeschützte Partition für Ihre verschlüsselten Daten
- ✓ Benötigt KEINE Administratorrechte (mit Ausnahme von Red Hat Enterprise Linux 5)
- ✓ Treiberlose Installation (Plug & Play)
- ✓ Hochfestes Aluminiumgehäuse
- ✓ Manipulationssicheres Design
- ✓ Schreibschutzschalter
- ✓ Antivirenschutzprogramm
- ✓ Individuelle Sicherheitsfarben wählbar (rot, grün, gelb, blau, hellbraun, grau)
- ✓ HIPAA-konform
- ✓ Konform zu Sarbanes Oxley
- ✓ GLB-konform

Remote Management

Der Kanguru Defender Elite Flash Stick kann mit der Kanguru Remote Management Console (KRMC) ferngesteuert werden. KRMC ist eine webbasierte Anwendung, die Administratoren ein umfassendes USB-Management-System an die Hand gibt.

Mit KRMC sind Sie in der Lage:

- ✓ Ein Master-Passwort für Ihre Defender zu erstellen und zu verwalten
- ✓ Alle Daten eines Ziellaufwerks aus der Ferne zu löschen
- ✓ Maßnahmen für gegenwärtige oder zukünftige Aktionen festzulegen
- ✓ Kontrollen in der Rolle des Administrators oder Super-Administrators vorzunehmen
- ✓ Geräte über IP-Adressen zu lokalisieren (IP-Adresse / Netzwerkstandort)
- ✓ Geräte über den Hostnamen zu lokalisieren
- ✓ Befehle über die Fernsteuerung zu ändern wie:
 - Passwortstärke und -länge (bspw. 10 Zeichen: 2 Großbuchstaben, 2 Zahlen etc.)
 - Ungültige Login-Versuche (bspw. 3 Versuche, bevor der Stick gelöscht wird)
 - Häufigkeit von Passwortänderungen (bspw. alle 30, 60 oder 90 Tage)
 - Nutzer-Passwort
 - Master-Passwort
- ✓ Benutzergruppen zu erstellen

Ihr Kanguru Defender Elite ist bei standardmäßiger Aktivierung nicht mit der Kanguru Remote Management Console ausgestattet. Weitere Informationen zu KRMC finden Sie hier: <https://www.kanguru.com/index.php/flash-management>

1.4 Technische Spezifikationen

Allgemeine Angaben

Schnittstelle	USB 2.0 (USB 1.1 kompatibel)
Verschlüsselungsfunktionen	Hardwarebasierte Verschlüsselung 256 Bit AES
Kompatibilität mit Betriebssystemen	Windows XP Service Pack 3, Server 2003, Vista 7 Mac OS X und höher (kompatibel mit intel-basierten Macs) Red Hat Enterprise Linux 5, Ubuntu 9.10, Ubuntu 11.10 (32 und 64 Bit kompatibel)
Schreibzyklen	10.000 Schreibzyklen / sperren
Datenspeicherung	10 Jahre und mehr
Betriebstemperatur	0°C – 70°C
Luftfeuchtigkeit	20% - 90%
Druckfestigkeit	1000G Max
Vibration	15G Belastung bis Maximalbelastung

Spezifikationen für Defender Elite 2GB - 16GB

Datentransferrate	Lesen: 20 - 33 MB/s Schreiben: 10 - 13 MB/s
Gewicht	10g
Maße	64mm x 18.5mm x 9mm
Leseleistung	Max Lesen: 5 VDC @ 122mA
Schreibleistung	Max Schreiben: 5 VDC @ 182mA

Spezifikationen für Defender Elite 32GB - 64GB

Datentransferrate	Lesen: 31 MB/s Schreiben: 10 MB/s
Gewicht	15g
Maße	71mm x 27mm x 9mm
Leseleistung	Max Lesen: 5 VDC @ 150mA
Schreibleistung	Max Schreiben: 5 VDC @ 266mA

2. Kanguru Defender Manager Elite

Kanguru Defender Manager Elite (KDMelite) ist das Client-Programm, das bereits im CD-ROM-Bereich des Defender Elite installiert ist. Der Nutzer muss sich zuerst bei KDMelite anmelden, um Zugang zur sicheren, verschlüsselten Partition zu erhalten. KDMelite ist bereits auf Ihrem Defender Elite installiert und muss auf dem PC nicht installiert werden.

2.1 KDMelite einrichten

Der Kanguru Defender Elite ist zu vielen Betriebssystemen kompatibel. Wie KDMelite eingerichtet wird, hängt vom Betriebssystem Ihres Computers ab.

2.1.1 KDMelite mit Windows

Um KDMelite auf einem Windows-Betriebssystem einzurichten, verbinden Sie den Defender Elite einfach über den USB-Anschluss mit Ihrem Computer. KDMelite startet selbständig, wenn die Autorun-Funktion aktiviert ist.

Falls KDMelite nicht automatisch startet:

1. Öffnen Sie **Mein Computer** und das CD-ROM Laufwerk **KDMelite** des Defender Elite. Welches Laufwerk angezeigt wird (etwa D:, E: oder F:), hängt von den Einstellungen Ihres Computers ab.

Geräte mit Wechselmedien

 3 1/2-Diskette (A:)	3 1/2-Diskette
 NRMEVOL_DE (D:)	CD-Laufwerk
 Defender Elite (E:)	CD-Laufwerk
 Wechseldatenträger (F:)	Wechseldatenträ

2. Starten Sie KDMelite durch einen Doppelklick auf **KDMelite.exe**.

Bei der ersten Anwendung müssen Sie KDMelite mit dem Setup Wizard vollständig installieren, um Ihr Sicherheitspasswort einzurichten (siehe Abschnitt 2.2 *Der Setup Wizard* auf Seite 13). Wenn Sie bereits ein Sicherheitspasswort festgelegt haben, werden Sie aufgefordert, sich anzumelden (siehe Abschnitt 2.3 *Sichere Partition entsperren* auf Seite 19).

Achtung! Die Datei **KDM.exe** bleibt immer auf der CD-ROM-Partition des Kanguru Defender, damit Sie das Programm auf unterschiedlichen Computern ausführen können. Bitte starten Sie das Programm immer von der CD-ROM-Partition aus, nicht von der Festplatte ihres Laptops oder Desktops. Versuchen Sie nicht, KDMelite an einen anderen Ort zu kopieren.

Anmerkung: Nutzern von Windows 7 wird das Wechsellaufwerk erst angezeigt, wenn sie sich vorher bei KDMelite angemeldet haben. Wenn Sie Windows 7 nutzen und das Wechsellaufwerk sehen möchten, bevor Sie sich bei KDMelite anmelden, folgen Sie bitte den Anweisungen auf Seite 9.

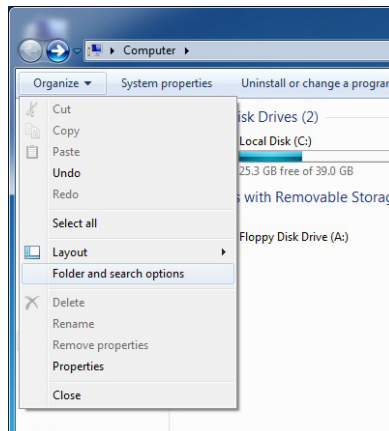
Vorsicht: Nutzer von Windows 7

Nutzern von Windows 7 wird das Wechsellaufwerk erst angezeigt, wenn sie sich vorher bei KDMElite angemeldet haben (für weitere Informationen siehe Abschnitt 2.3 *Sichere Partition entsperren* auf Seite 19).

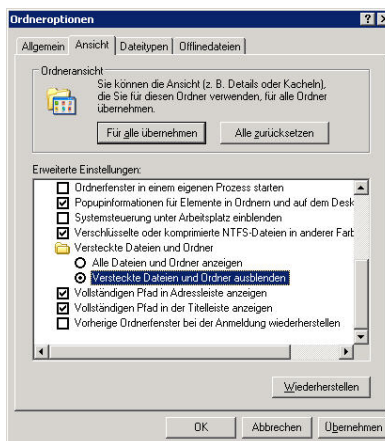
Wenn Sie Windows 7 nutzen und das Wechsellaufwerk sehen möchten, bevor Sie sich bei KDMElite anmelden, konfigurieren Sie Windows auf folgende Weise:

Anmerkung: Dies betrifft nur Ihre Benutzereinstellungen. Um Ihren Defender normal zu verwenden, müssen Sie Windows nicht konfigurieren.

1. Gehen Sie auf **Mein Computer**, klicken Sie auf **Organisieren** und wählen Sie dann **Ordner- und Suchfunktionen** aus.



2. Auf dem Bildschirm erscheint das Fenster **Optionen**. Scrollen Sie nach unten, bis Sie zur Option „Versteckte Dateien und Ordner“ gelangen, und wählen **Alle Dateien und Ordner anzeigen** aus.



3. Klicken Sie auf **OK**, um die Konfiguration für Windows fertigzustellen. Das Wechsellaufwerk ist nun schon sichtbar, bevor Sie sich bei KDMElite anmelden.

2.1.2 KDMElite mit Mac OS X

Um KDMElite auf einem Mac-OS-X-Betriebssystem einzurichten, verbinden Sie Ihren Defender Elite über den USB-Anschluss mit Ihrem Computer. Das Symbol KDMElite erscheint auf Ihrem Desktop. Öffnen Sie **KDMElite** mit einem Doppelklick.



Starten Sie die Anwendung KDMElite mit einem Doppelklick auf **KDMElite.app**.

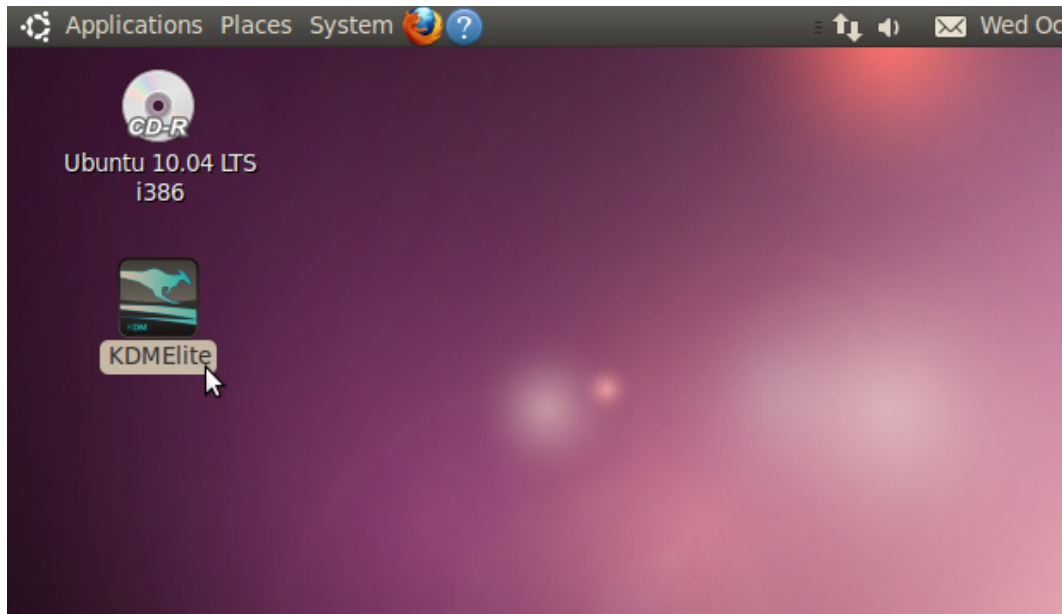
Bei der ersten Anwendung müssen Sie KDMElite mit dem Setup Wizard vollständig installieren, um Ihr Sicherheitspasswort einzurichten (siehe Abschnitt 2.2 *Der Setup Wizard* auf Seite 13). Wenn Sie bereits ein Sicherheitspasswort festgelegt haben, werden Sie aufgefordert, sich anzumelden (siehe Abschnitt 2.3 *Sichere Partition entsperren* auf Seite 19).

Achtung! Die Datei **KDMElite.app** bleibt immer auf der CD-ROM-Partition des Kanguru Defender, damit Sie das Programm auf unterschiedlichen Computern ausführen können. Bitte starten Sie das Programm immer von der CD-ROM-Partition aus, nicht von der Festplatte ihres Laptops oder Desktops. Versuchen Sie nicht, KDMElite an einen anderen Ort zu kopieren.

Anmerkung: Das Symbol für **KDMElite** wird nicht immer auf dem Desktop angezeigt. Wenn das Symbol nicht auf Ihrem Desktop erscheint, können Sie die Datei **KDMElite.app** mit der Suchfunktion auf der CD-Rom-Partition finden.

2.1.3 KDMelite mit Linux Ubuntu

Um KDMelite mit dem Linux-Ubuntu-Betriebssystem einzurichten, verbinden Sie Ihren Defender Elite über den USB-Anschluss mit Ihrem Computer. Das Symbol KDMelite erscheint auf Ihrem Desktop. Öffnen Sie **KDMelite** mit einem Doppelklick.



Starten Sie die Anwendung KDMelite mit einem Doppelklick auf das Fenster **KDMelite**.

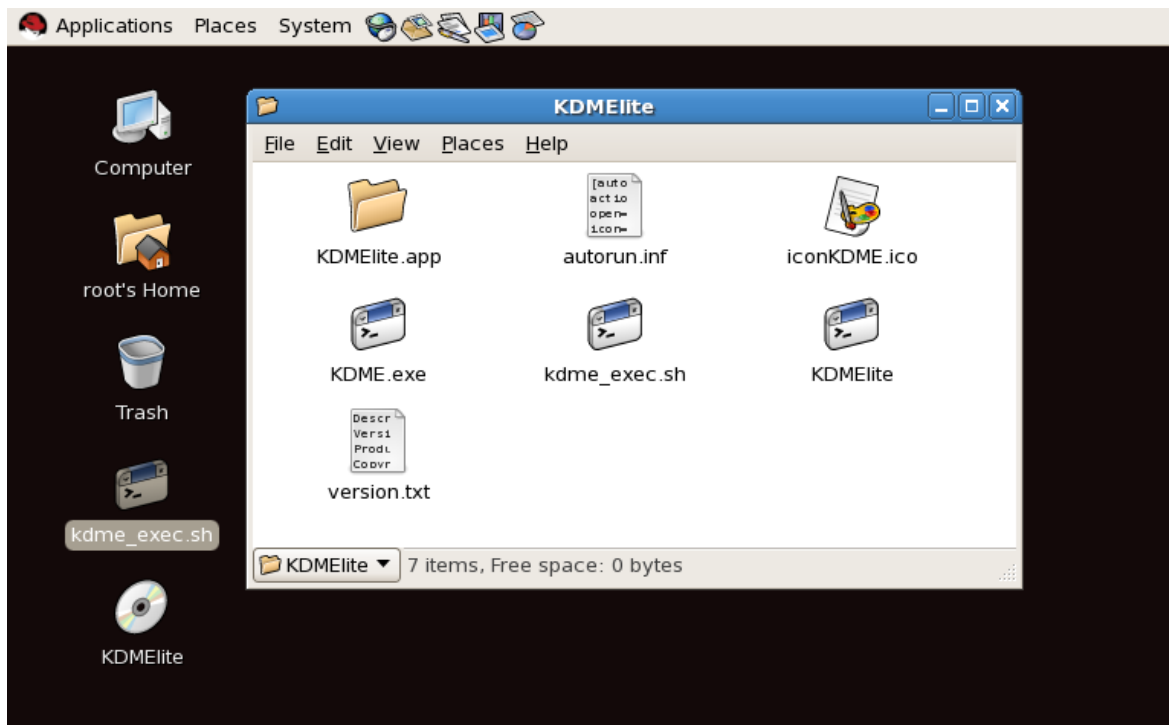
Bei der ersten Anwendung müssen Sie KDMelite mit dem Setup Wizard vollständig installieren, um Ihr Sicherheitspasswort einzurichten (siehe Abschnitt 2.2 *Der Setup Wizard* auf Seite 13). Wenn Sie bereits ein Sicherheitspasswort festgelegt haben, werden Sie aufgefordert, sich anzumelden (siehe Abschnitt 2.3 *Sichere Partition entsperren* auf Seite 19).

Achtung! Die Datei **KDM.exe** bleibt immer auf der CD-ROM-Partition des Kanguru Defender, damit Sie das Programm auf unterschiedlichen Computern ausführen können. Bitte starten Sie das Programm immer von der CD-ROM-Partition aus, nicht von der Festplatte ihres Laptops oder Desktops. Versuchen Sie nicht, KDMelite an einen anderen Ort zu kopieren.

2.1.4 KDMElite mit Red Hat Enterprise Linux 5

Anmerkung: Um KDMElite mit Red Hat Enterprise Linux 5 zu nutzen, benötigen Sie eine Super-User- oder Root-Berechtigung.

Um KDMElite mit Red-Hat-Enterprise-Betriebssystemen zu starten, verbinden Sie Ihren Defender Elite mit dem USB-Anschluss Ihres Computers. Das CD-Symbol KDMElite erscheint nun auf Ihrem Desktop. Falls das Fenster KDMElite nicht automatisch öffnet, öffnen Sie es mit einem Doppelklick auf das Symbol **KDMElite**.



Ein Bildschirmfenster öffnet sich. Kopieren Sie die Shell-Script-Datei **kdme_exec.sh** an einen Ort auf der lokalen Festplatte Ihres Computers.

Nachdem Sie die Shell-Script-Datei **kdme_exec.sh** auf die lokale Festplatte kopiert haben, können Sie KDMElite folgendermaßen ausführen:

1. Öffnen Sie das Eingabefenster mit einem Klick auf **Anwendungen** → **Zubehör** → **Terminal**. Der Speicherort des Terminal kann anderswo sein, das hängt von Ihrer Red-Hat-Version ab.
2. Navigieren Sie vom Terminal in das Verzeichnis, in das Sie die **kdme_exec.sh** Shell-Script-Datei kopiert haben.
3. Geben Sie „`chmod 007 kdme_exec.sh`“ ein, um volle Ausführungsrechte zu erhalten.
4. Geben Sie „`./kdme_exec.sh`“ ein, um das Shell-Script auszuführen.

Bei der ersten Anwendung müssen Sie KDMElite mit dem Setup Wizard vollständig installieren, um Ihr Sicherheitspasswort einzurichten (siehe Abschnitt 2.2 *Der Setup Wizard* auf Seite 13). Wenn Sie bereits ein Sicherheitspasswort festgelegt haben, werden Sie aufgefordert, sich anzumelden (siehe Abschnitt 2.3 *Sichere Partition entsperren* auf Seite 19).

2.2 Der Setup Wizard

Beim ersten Starten von KDMElite werden Sie vom **Setup Wizard** begrüßt. Folgen Sie den Instruktionen des Setup Wizard, um ein Sicherheitspasswort für die sichere, verschlüsselte Partition Ihres Defender Elite zu erstellen.

Anmerkung: Bevor Sie den Defender Elite einrichten, müssen Sie den manuellen Schreibschutzschalter entsperren.



Vorsicht! Wenn der Setup Wizard einmal gestartet ist, trennen Sie die Verbindung zum Defender Elite bitte nicht, ohne vorher den Setup Wizard fertigzustellen oder den Setup Wizard mit einem Klick auf den **X-Button** zu schließen.

2.2.1 Setup-Sprache auswählen

Die Standard-Sprache des Setup Wizard ist Englisch. Sie können die Sprache des Setup Wizard ändern:

1. Klicken Sie im Eingangsfenster auf das Symbol neben dem Sprachen-Menü  .



2. Eine Liste mit den verfügbaren Sprachen wird geöffnet. Wählen Sie die gewünschte Sprache aus dem Drop-down-Menü aus. Der Setup Wizard wechselt nun in die gewählte Sprache.
3. Gehen Sie auf **Weiter**, um mit dem nächsten Schritt fortzufahren.

2.2.2 Integrierten Virenschutz aktivieren (nur unter Windows)

Anmerkung: Dieser Abschnitt gilt nicht, wenn Sie den Setup Wizard für Linux oder Mac OS X nutzen. Für Nutzer der Enterprise Edition gilt dieser Abschnitt ebenfalls nicht. Der Virenschutz für Nutzer der Enterprise Edition wird durch die Kanguru Remote Management Console (KRMC) aktiviert. Wenn Sie die Enterprise Edition nutzen, kontaktieren Sie bitte Ihren Administrator.

KDMElite überprüft automatisch, ob Ihr Gerät eine gültige Lizenz für ein Virenschutzprogramm hat.

Anmerkung: Ihr Defender Elite muss an einen Computer mit Internetzugang angeschlossen sein, um den integrierten Virenschutz zu aktivieren.



Falls Ihr Defender Elite keine gültige Lizenz für ein Virenschutzprogramm besitzt, füllen Sie bitte das folgende Anmeldeformular aus und klicken auf **Übernehmen**, um Ihren Gratis-Virenschutz für ein ganzes Jahr (!) zu aktivieren.

Falls Sie Ihren Virenschutz nicht aktivieren möchten, **Überspringen** Sie diese Option. Wenn Sie die Aktivierung überspringen, können Sie den Virenschutz nachträglich nur aktivieren, wenn Sie vorher Ihr Laufwerk auf Standardeinstellungen zurücksetzen.



Klicken Sie auf **Weiter**, um mit der Einrichtung des Login-Passwortes für den Defender Elite fortzufahren

2.2.3 Passwort einrichten

Von der Bildschirmmaske **Passwort einrichten** aus:

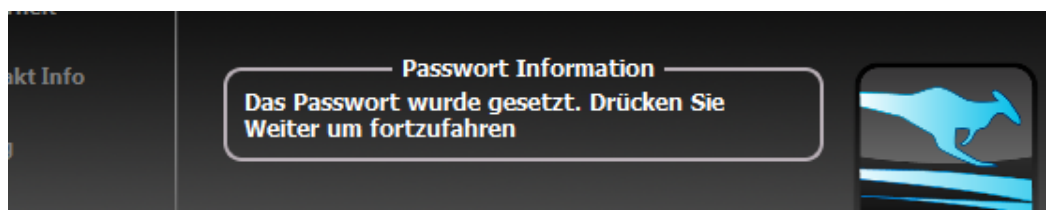
1. Geben Sie Ihr Passwort in das Passwort-Feld ein. Klicken Sie auf das Symbol **VK**, wenn Sie das Passwort mit der virtuellen Tastatur von KDMElite eingeben möchten. Weitere Informationen zur virtuellen Tastatur siehe Abschnitt 2.4 *Passwort mit Hilfe der virtuellen Tastatur eingeben* auf Seite 21.

Anmerkung: Um maximale Sicherheit zu erreichen, wird empfohlen, ein starkes Passwort zu wählen, das aus Buchstaben, Zahlen und Symbolen besteht.

2. Geben Sie das gleiche Passwort in das Feld **Passwort bestätigen** ein. Falls Ihre beiden Eingaben nicht übereinstimmen oder beim Eintragen des Passwortes ein anderes Problem entsteht, erscheint eine Erklärung in der Passwort-Information.

Anmerkung: Das Fenster Passwort-Information wird Sie über jegliche Passwort-Anforderungen informieren. Die Passwort-Information überprüft Ihr Passwort in Echtzeit. Bitte lassen Sie die Meldungen der Passwort-Information so lange außer Acht, bis Sie das Passwort und die Passwortbestätigung vollständig eingetragen haben.

3. Klicken Sie auf **Übernehmen**, um Ihr Passwort festzulegen. Sobald Sie Ihr Passwort eingerichtet haben, wird folgende Benachrichtigung in der Info-Box angezeigt:



4. Gehen Sie auf **Weiter**. KDMElite konfiguriert nun die Sicherheitsparameter automatisch.

Anmerkung: Wenn Sie Ihren Defender Elite mit einem administrativen Programm wie KLA oder KRMC verwalten, können Sie ein Master-Passwort einrichten. Falls Sie dann Ihr Passwort einmal verloren oder vergessen haben, können Sie es mit dem Master-Passwort jederzeit zurücksetzen und neu einrichten.

2.2.4 KRMCloud

Anmerkung: Dieser Abschnitt gilt nicht für Nutzer der Enterprise Edition.

Kanguru Defender Sticks können durch die Kanguru Remote Management Console (KRMCloud) ferngesteuert verwaltet werden. Die KRMCloud wird auf den Servern von Kanguru gehostet und kann auf jedem Defender Elite aktiviert werden, außer bei der Enterprise-Version.



So aktivieren Sie die Funktion KRMCloud:

1. Wählen Sie **KRMCloud aktivieren** und klicken Sie auf **Übernehmen**.
2. Ein Dialogfenster öffnet sich mit der Frage, ob Sie Ihr Gerät mit KRMCloud registrieren möchten. Bestätigen Sie mit **Ja**.
3. Der Webbrowser öffnet sich und leitet Sie automatisch auf die Anmeldeseite von KRMCloud weiter. Wenn Sie noch kein Benutzerkonto haben, müssen Sie sich registrieren, bevor Sie sich einloggen.
4. Erwerben Sie eine Lizenz für Ihr Laufwerk, um es mit KRMCloud zu verwalten.

Wenn Sie Ihren Defender nicht remote mit Hilfe von KRMCloud verwalten möchten, **deaktivieren** Sie die Option **KRMCloud** und fahren mit **Weiter** fort. Sie können die Funktion KRMCloud nachträglich nur wieder aktivieren, wenn Sie vorher Ihr Laufwerk auf Standardeinstellungen zurückgesetzt haben.

Gehen Sie auf **Weiter**, um mit der Einrichtung Ihres Sticks fortzufahren.

2.2.5 Kontakt Info

Anmerkung: Dieser Abschnitt gilt nicht für Nutzer der Enterprise Edition.



Ihre Kontaktinformationen werden auf dem Laufwerk gespeichert. Wenn Sie Ihr Laufwerk mit KRMC Cloud verwalten, werden Informationen, die Sie hier eingeben, automatisch zur KRMC Cloud weitergeleitet, sobald Sie Ihr Laufwerk angemeldet haben.

Geben Sie Ihre Daten in die entsprechenden Felder ein und klicken dann auf **Übernehmen**. Ein Fenster öffnet sich mit der Information, dass Ihre Daten gespeichert wurden. Gehen Sie auf **OK** und dann auf **Weiter**, um die Einrichtung Ihres Sticks fertigzustellen.

Herzlichen Glückwunsch! Ihr Defender Elite ist nun fertig eingerichtet und Sie können ihn benutzen.

2.2.6 Ihr Gerät mit Setup Wizard zurücksetzen

Wenn während des Setup-Wizard-Prozesses Probleme auftreten, müssen Sie möglicherweise das Gerät zurücksetzen, bevor Sie die Einrichtung fertigstellen können.

So setzen Sie Ihr Gerät während des Setup-Wizard-Prozesses zurück:

1. Klicken Sie so lange auf **Zurück**, bis Sie wieder zum Eingangsfenster gelangen.
2. Auf der Eingangsseite finden Sie links unten im Fenster die Schaltfläche **Zurücksetzen**. Klicken Sie darauf.

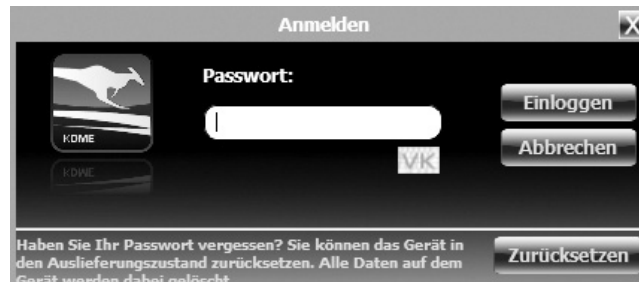


3. Eine Dialogbox erscheint mit der Aufforderung, das Zurücksetzen zu bestätigen. Klicken Sie auf **Ja**, um Ihr Gerät auf Standardeinstellungen zurückzusetzen.

Nachdem das Gerät auf die Standardeinstellungen zurückgesetzt ist, werden Sie aufgefordert, den Setup Wizard erneut zu starten.

2.3 Sichere Partition entsperren

Jedes Mal, wenn Sie KDMElite nutzen, werden Sie nach Ihrem Sicherheitspasswort gefragt. Sie müssen das korrekte Sicherheitspasswort eingeben, um Zugang zur sicheren Partition des Defender Elite zu erhalten.



Wenn der Bildschirm "Anmelden" erscheint:

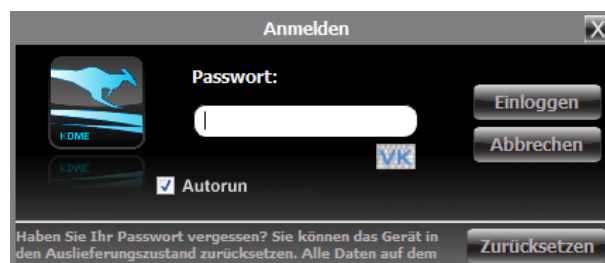
1. Geben Sie Ihr Passwort in das Passwort-Feld ein.
2. Klicken Sie auf **Einloggen**.

Vorsicht! Wenn Sie Ihr Passwort 7-mal hintereinander falsch eingeben, werden aus Sicherheitsgründen alle Daten in der sicheren Partition automatisch gelöscht. (Die Standardeinstellung erlaubt sieben Versuche, die Anzahl kann je nach individueller Einstellung abweichen.) Vor dem letzten Versuch erscheint eine Meldung auf dem Bildschirm mit der Warnung, dass Sie nur noch einen Versuch haben. Gehen Sie auf **Beenden**, um den Login-Versuch zu beenden. Wenn Sie Ihren Defender Elite herausziehen und wieder anschließen oder **KDMElite.exe** manuell ausführen, gelangen Sie erneut zum Login-Fenster.

Sobald Sie sich erfolgreich bei KDMElite angemeldet haben, erhalten Sie mit **Mein Computer** oder **Windows Explorer** Zugang zur sicheren Partition des Defender Elite. Für weitere Informationen siehe Abschnitt 2.5 *Dateien und Ordner verschlüsseln* auf Seite 22.

Vorsicht! Trennen Sie nie die Verbindung, während KDMElite aktiv ist, ohne die Anwendung vorher ordnungsgemäß zu schließen: Klicken Sie auf die KDMElite Symbolleiste und wählen Sie **Kanguru Defender schließen** aus. Siehe Erläuterungen im Abschnitt 2.12 *Defender Elite schließen* auf Seite 31.

Anmerkung: Wenn Ihr Defender Elite Stick mit KRMC verwaltet wird, sehen Sie möglicherweise eine **Autorun**-Kontrollbox. In diesem Fall hat der Administrator Ihr Gerät so konfiguriert, dass eine gespeicherte Datei in der sicheren Partition automatisch ausgeführt wird, sobald Sie sich einloggen. Sie können die Autorun-Funktion beenden, indem Sie die Autorun-Kontrollbox deaktivieren.



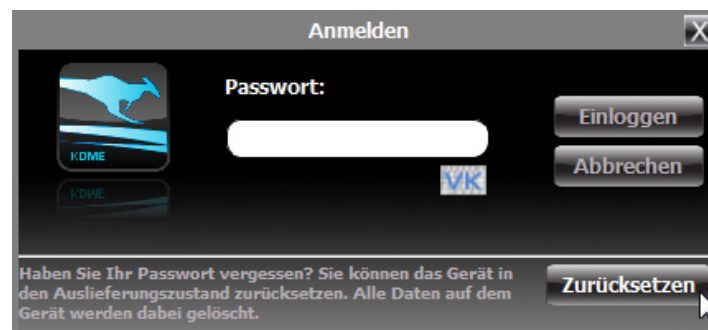
2.3.1 Login-Bildschirm zurücksetzen

Für den Fall, dass Sie Ihr Passwort vergessen haben, können Sie das Gerät auf die Standardeinstellungen zurücksetzen, um Ihr Passwort erneut einzurichten. Diese Funktion löscht alle Passwörter und Daten, die in der sicheren Partition Ihres Gerätes gespeichert sind, und setzt Ihr Gerät auf Standardeinstellungen zurück.

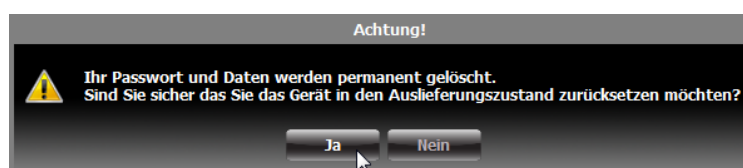
Vorsicht! Die Funktion **auf Standardeinstellungen zurücksetzen** löscht alle Daten auf Ihrem Gerät! Alle Daten auf dem Gerät gehen somit verloren.

So setzen Sie Ihren Defender Elite zurück:

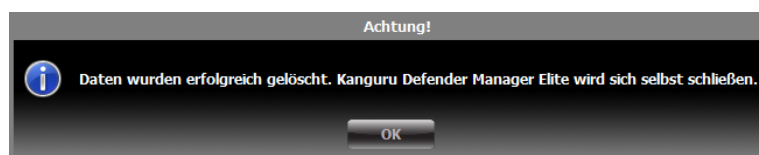
1. Starten Sie KDMElite.
2. Klicken Sie im Login-Bildschirm auf **Zurücksetzen**.



3. Bestätigen Sie das Zurücksetzen mit **Ja**.



4. Wenn Ihr Passwort und Ihre Daten in der sicheren Partition gelöscht sind, erscheint folgende Nachricht. Klicken Sie auf **OK**, um den Vorgang fertigzustellen.



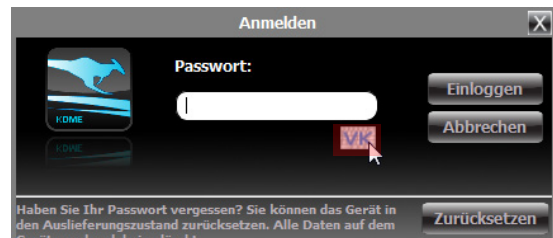
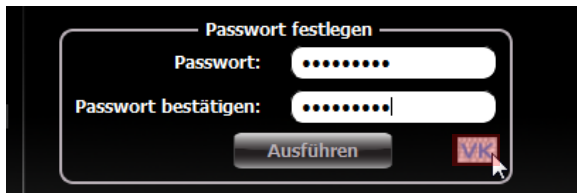
Beim nächsten Start von KDMElite muss der Setup Wizard erneut ausgeführt werden, bevor Sie Zugang zur sicheren Partition erhalten. Die Anleitung zur Ausführung des Setup Wizard finden Sie in Abschnitt 2.2 *Der Setup Wizard* auf Seite 13.

2.4 Passwort mit Hilfe der virtuellen Tastatur VT eingeben

Wenn Sie aufgefordert werden, Ihr Passwort einzugeben, können Sie die Funktion **virtuelle Tastatur** aktivieren, um sich vor Keylogging-Software zu schützen, die Passwörter ausspioniert.

So nutzen Sie die virtuelle Tastatur für Ihre Passwort-Eingabe:

1. Klicken Sie auf die Schaltfläche **VK** (Virtual Keyboard) neben dem Eingabefeld des Passwortes.



2. Die virtuelle Tastatur erscheint unterhalb des Setup-Wizard-Fensters. Geben Sie Ihr Passwort über die Tasten der virtuellen Tastatur ein.



3. Klicken Sie erneut auf die Schaltfläche **VK**, um die virtuelle Tastatur zu schließen.

Anmerkung: Um die Tasten der virtuellen Tastatur in eine zufällige Anordnung zu bringen, drücken Sie die Schaltfläche **Shuffle**. Die zufällige Anordnung der Tasten schützt Sie vor Mouse-Tracking-Programmen, die virtuelle Tastaturen umgehen können.

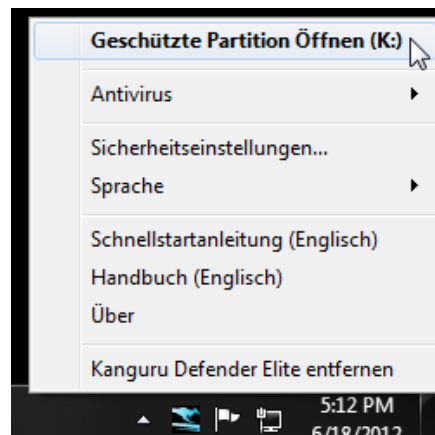
2.5 Dateien und Ordner verschlüsseln

Ein Hauptmerkmal des Defender Elite ist die Funktion **Drag & Drop** (Ziehen und Ablegen). Sie ermöglicht Ihnen, Dateien und Ordner zu verschlüsseln, indem sie diese einfach in die sichere Partition verschieben. Der Kanguru Defender verschlüsselt sie automatisch, so dass Ihre Daten vertraulich und sicher bleiben.

Öffnen Sie die sichere Partition:

1. Starten Sie KDMElite.
2. Melden Sie sich bei KDMElite an, um Zugang zur sicheren Partition zu erhalten.
3. Klicken Sie auf das KDMElite Symbol  in der Taskleiste und wählen Sie im Pop-Up-Menü **Sicherheitslaufwerk überprüfen** aus.

Anmerkung: Linux-Nutzer gehen über einen Rechtsklick auf das KDMElite-Symbol in der Taskleiste vor.



Wir empfehlen, die Funktion Drag & Drop (Ziehen und Ablegen) oder die Tastaturkürzel zum Kopieren (Ctrl+C) und Einfügen (Ctrl+V) von Dateien und Ordnern zu nutzen.

Anmerkung: Auf Dateien, die in der sicheren Partition Ihres Defender Elite abgelegt sind, können Sie erst zugreifen, nachdem Sie sich beim KDMElite angemeldet haben.

2.6 Integrierter Virenschutz (nur unter Windows)

Sie müssen Ihr Gerät bei Kanguru Solutions registrieren, um die Vorteile des integrierten Virenschutzes von Defender Elite nutzen zu können (siehe Abschnitt 2.2.2 *Integrierten Virenschutz aktivieren (nur unter Windows)* auf Seite 14).

Ist der integrierte Virenschutz einmal aktiviert, läuft die Virenprüfung jedes Mal automatisch, sobald Sie angemeldet sind. Alle Ordner im Defender werden auf Viren und Malware überprüft.

Anmerkung: Updates für die aktuellste Version des Virenschutzes werden automatisch heruntergeladen, sobald das Gerät über einen Computer mit dem Internet verbunden ist. Wenn Sie Ihren Defender trennen, bevor das Update vollständig heruntergeladen werden konnte, fährt der Defender bei der nächsten Verbindung mit dem Internet an dieser Stelle fort.

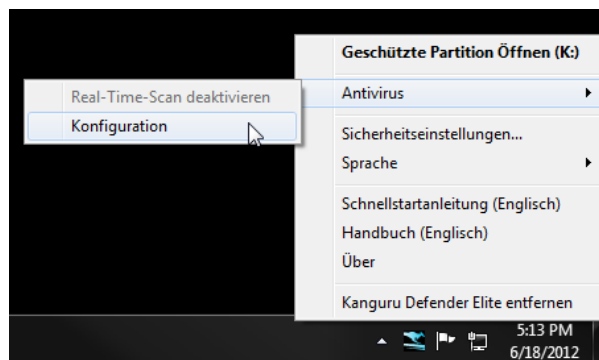
Viren-Definitionen sind in der sicheren Partition im Ordner **System** gespeichert. Falls diese Dateien gelöscht wurden, werden sie automatisch wieder heruntergeladen. Wenn das Gerät auf Standardeinstellungen zurückgesetzt ist, werden diese Dateien gelöscht und müssen erneut heruntergeladen werden.

Vorsicht! Speichern Sie keinerlei Daten im Ordner **System**. Alle Daten, die hier gespeichert sind und nicht den Viren-Definitionen entsprechen, werden automatisch gelöscht.

Integrierte Antivirus-Konsole

Sie können die integrierte **Antivirus-Konsole** aufrufen, um Ihr Gerät, einen Pfad oder einen Ordner zu überprüfen. Öffnen Sie die **Antivirus-Konsole** folgendermaßen:

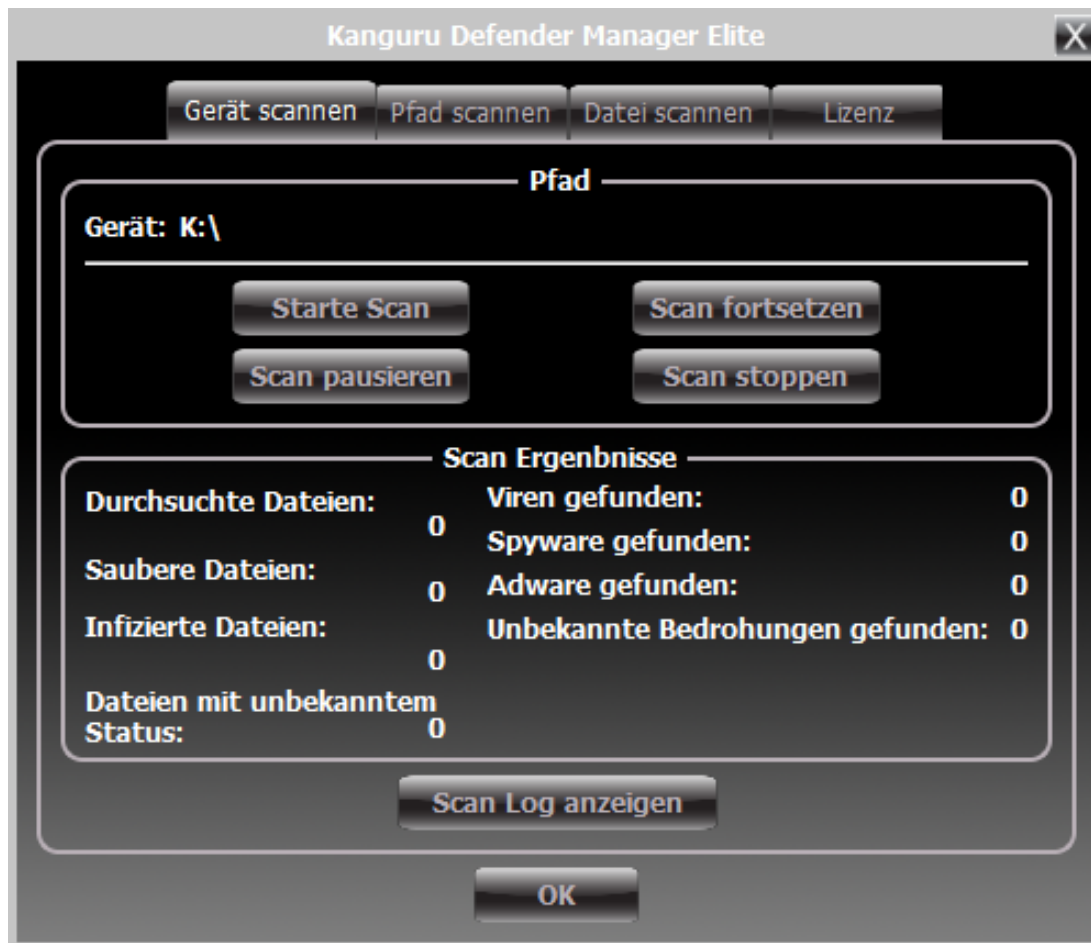
1. Klicken Sie mit einem Rechtsklick auf das KDM Elite-Symbol  in der Taskleiste.
2. Wählen Sie **Antivirus** im Pop-Up-Menü aus und gehen Sie dann auf **Konfigurieren** im Untermenü.



Die Antivirus-Konsole erscheint.

2.6.1 Gerät scannen

Mithilfe der Antivirus-Konsole können Sie den Defender Elite auf bekannte Viren und Malware überprüfen.



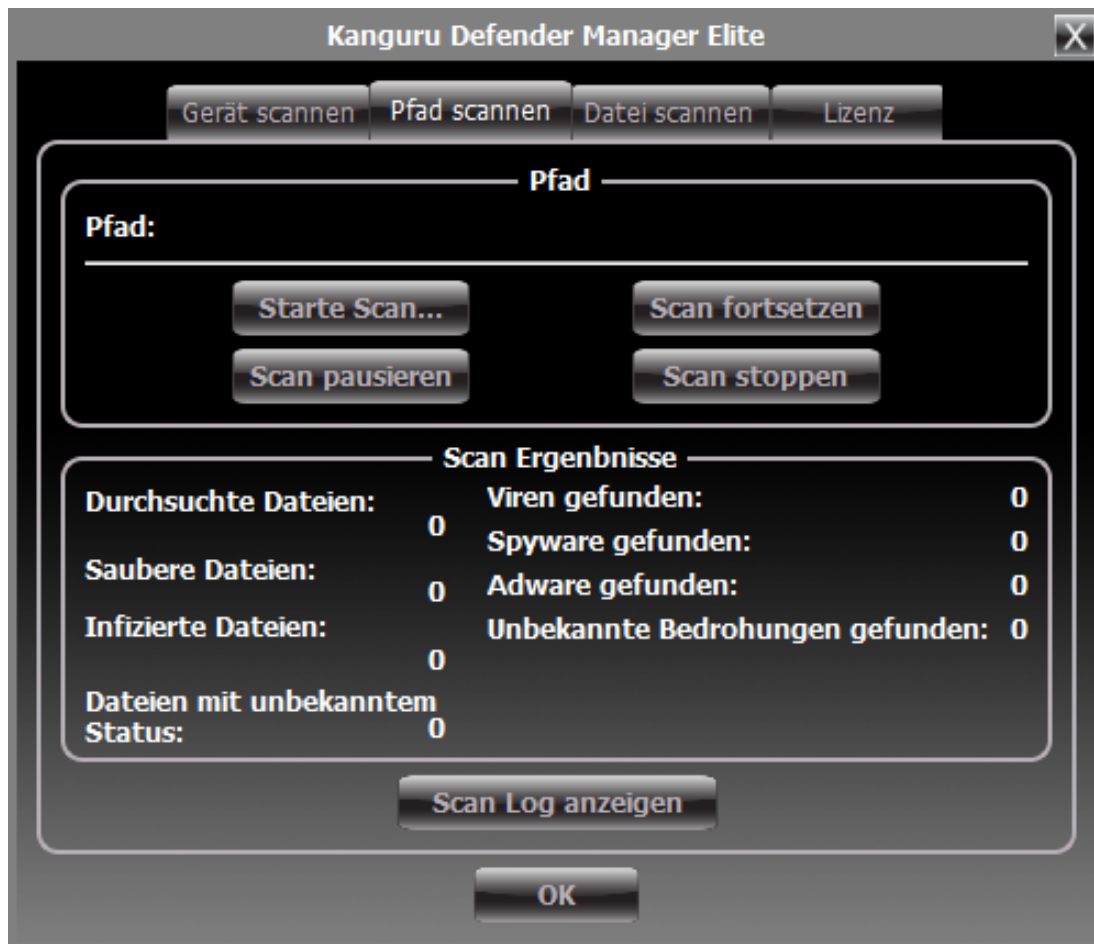
Überprüfen des Defender Elite:

1. Klicken Sie auf die Schaltfläche **Gerät scannen** ganz oben auf der Antivirus-Konsole.
2. Klicken Sie auf **Starte Scan**, um Ihren Defender Elite zu überprüfen.
3. Der Scan startet:
 - Um den Scan anzuhalten, klicken Sie auf **Scan pausieren**.
 - Um den Scan fortzusetzen, klicken Sie auf **Scan fortsetzen**.
 - Um den Scan zu beenden, klicken Sie auf **Scan stoppen**.
4. Die Ergebnisse der Überprüfung erscheinen im Fenster **Scan-Ergebnisse**.
5. Wenn Sie das Protokoll der letzten Überprüfung sehen möchten, klicken Sie auf **Scan Log anzeigen**.
6. Um die Antivirus-Konsole zu schließen, klicken Sie auf **OK**.

2.6.2 Pfad scannen

Mithilfe der Antivirus-Konsole können Sie jeden einzelnen Pfad auf bekannte Viren und Malware überprüfen.

Anmerkung: Die Funktion **Pfad scannen** kann auf Geräten der Enterprise Edition deaktiviert sein. Bitte kontaktieren Sie Ihren Administrator für weitere Informationen.



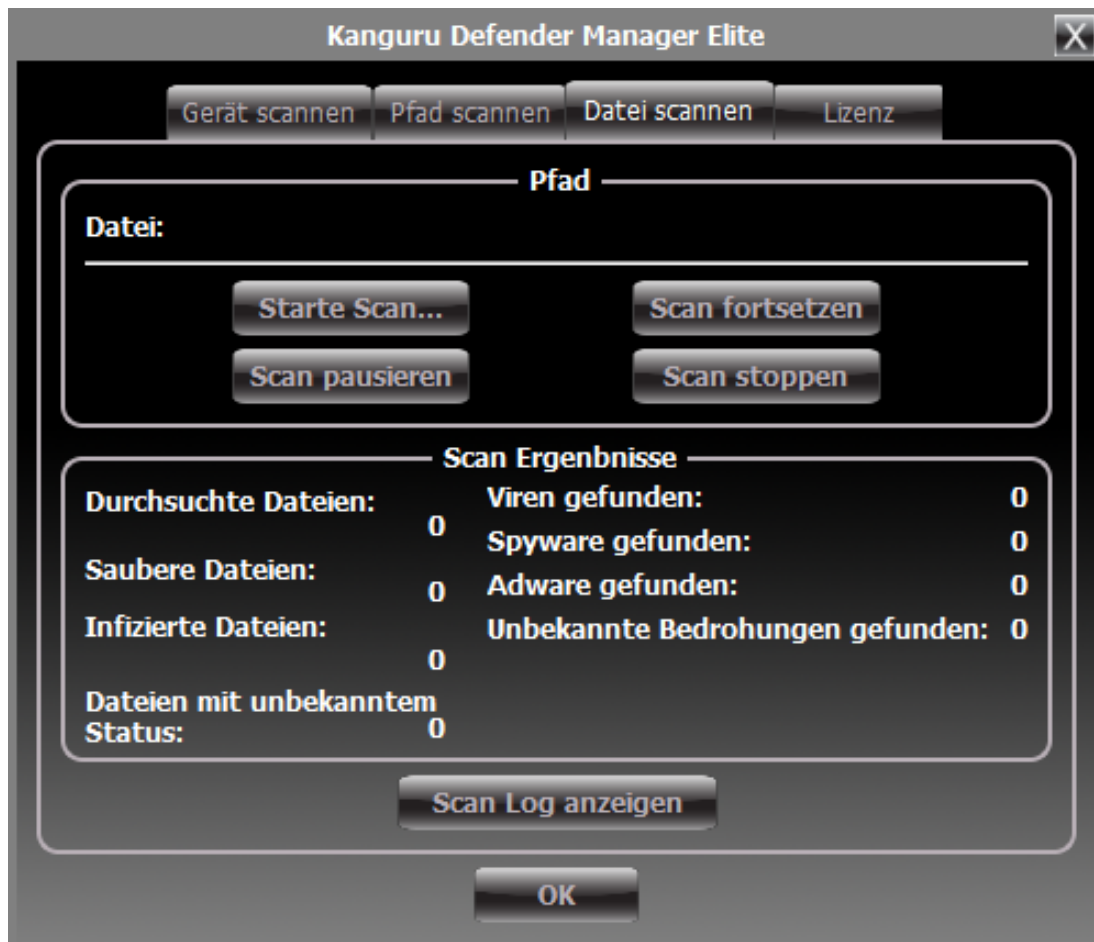
Überprüfen eines Pfades auf Ihrem Computer:

1. Klicken Sie auf **Pfad scannen** ganz oben auf der Antivirus-Konsole.
2. Klicken Sie auf **Starte scan** und wählen Sie dann einen Pfad auf Ihrem Computer aus, um die Überprüfung zu starten.
3. Der Scan startet:
 - Um den Scan anzuhalten, klicken Sie auf **Scan pausieren**.
 - Um den Scan fortzusetzen, klicken Sie auf **Scan fortsetzen**.
 - Um den Scan zu stoppen, klicken Sie auf **Scan stoppen**.
4. Die Ergebnisse der Überprüfung erscheinen im Fenster **Scan-Ergebnisse**.
5. Wenn Sie das Protokoll der letzten Überprüfung sehen möchten, klicken Sie auf **Scan Log anzeigen**.
6. Um die Antivirus-Konsole zu schließen, klicken Sie auf **OK**.

2.6.3 Datei scannen

Mithilfe der Antivirus-Konsole können Sie jede einzelne Datei auf bekannte Viren und Malware überprüfen.

Anmerkung: Die Funktion **Datei scannen** kann auf Geräten der Enterprise Edition deaktiviert sein. Bitte kontaktieren Sie Ihren Administrator für weitere Informationen.



Überprüfen einer Datei auf Ihrem Computer:

1. Klicken Sie auf **Datei scannen** ganz oben auf der Antivirus-Konsole.
2. Klicken Sie auf **Starte Scan** und wählen Sie dann eine Datei auf Ihrem Computer aus, um die Überprüfung zu starten.
3. Der Scan startet:
 - Um den Scan anzuhalten, klicken Sie auf **Scan pausieren**.
 - Um den Scan fortzusetzen, klicken Sie auf **Scan fortsetzen**.
 - Um den Scan zu stoppen, klicken Sie auf **Scan stoppen**.
4. Die Ergebnisse der Überprüfung erscheinen im Fenster **Scan-Ergebnisse**.
5. Wenn Sie das Protokoll der letzten Überprüfung sehen möchten, klicken Sie auf **Scan Log anzeigen**.
6. Um die Antivirus-Konsole zu schließen, klicken Sie auf **OK**.

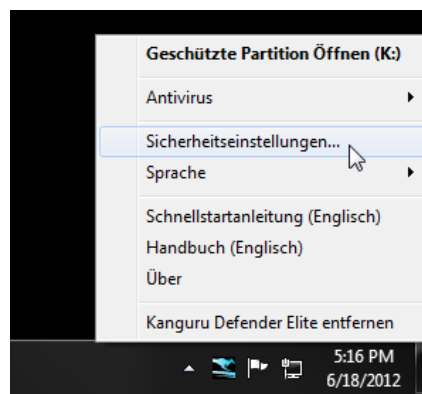
2.7 Ändern des Passwortes

Sie können Ihr Passwort in den **Sicherheitseinstellungen** ändern.

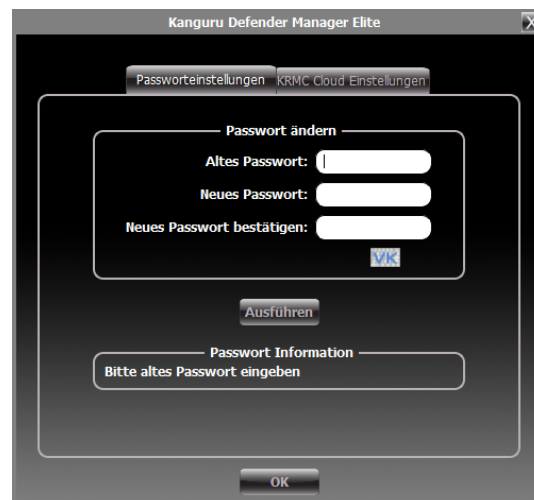
So ändern Sie das Passwort:

1. Klicken Sie auf das KDMElite-Symbol  in der Taskleiste und wählen Sie im Popup-Menü **Sicherheitseinstellungen**.

Anmerkung: Linux-User gehen über einen Rechtsklick auf das KDMElite-Symbol in der Taskleiste vor.



2. Das Fenster für die Passwordeinstellungen öffnet sich. Tragen Sie Ihr aktuelles Passwort in das Feld **Altes Passwort** ein. Schreiben Sie Ihr neues Passwort in das Feld **Neues Passwort** und wiederholen die Eingabe im Feld **Neues Passwort bestätigen**.



3. Wenn Sie fertig sind, klicken Sie auf **Ausführen**, um Ihr neues Passwort zu speichern.
4. Sobald Ihr neues Passwort gespeichert ist, öffnet sich ein Fenster mit der Bestätigung, dass das Passwort erfolgreich geändert wurde. Klicken Sie auf **OK**, um das Ändern des Passwortes abzuschließen.

2.8 KPMC Cloud: Einstellungen

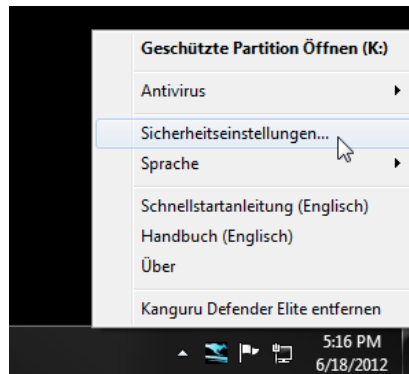
Anmerkung: Dieser Abschnitt gilt nicht für Nutzer der Enterprise Edition.

Sie können die Funktionsweise von KPMC Cloud in den Sicherheitseinstellungen aktivieren und deaktivieren.

Ändern der KPMC-Gerätefunktionen:

1. Klicken Sie auf das KDMElite-Symbol  in der Taskleiste und wählen **Sicherheitseinstellungen** im Popup-Menü aus.

Anmerkung: Linux-User gehen über einen Rechtsklick auf das KDMElite-Symbol in der Taskleiste vor.



2. Das Fenster für die Passwort-Einstellungen öffnet sich. Klicken Sie auf die Registerkarte **KPMC-Cloud-Einstellungen**.
3. Aktivieren oder deaktivieren Sie die KPMC Cloud durch Auswahl der entsprechenden Schaltknöpfe und klicken Sie auf **Ausführen**.

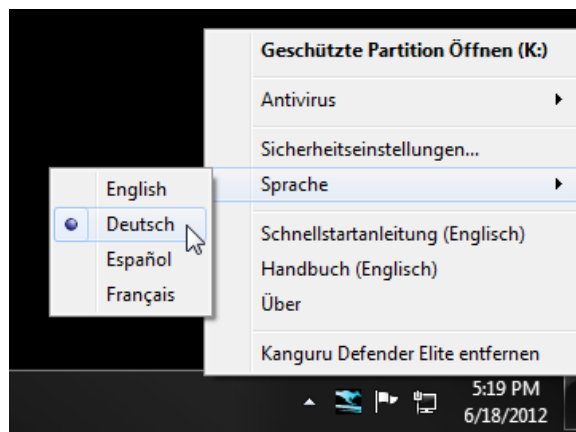


2.9 Ändern der Spracheinstellung

KDMElite unterstützt verschiedene Sprachen. Standardmäßig ist die englische Sprache eingestellt.

Ändern der Spracheinstellung:

1. Klicken Sie mit der rechten Maustaste auf das KDMElite-Symbol in der Taskleiste  und bewegen Sie den Cursor über die Option **Sprache** im Popup-Menü. Eine Liste der verfügbaren Sprachen erscheint.



2. Wählen Sie die Sprache aus, in der Sie den KDMElite ausführen möchten.

2.10 Online-Dokumentation

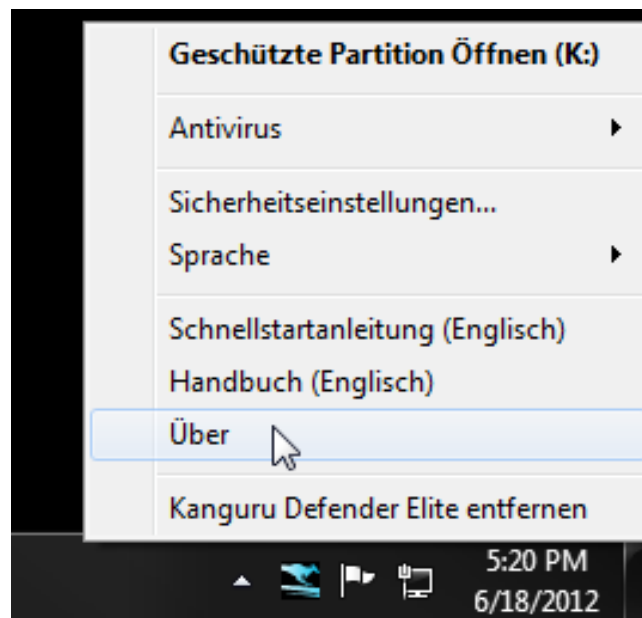
Die Dokumentation des Kanguru Defender Elite können Sie sich aus dem Internet herunterladen.

Zum Download der Dokumentation klicken Sie mit der rechten Maustaste auf das KDMElite-Symbol  in der Taskleiste.

- Klicken Sie auf **Kurzanleitung**, um die Kurzanleitung des Defender Elite herunterzuladen.
- Klicken Sie auf **Gebrauchsanleitung**, um die Gebrauchsanleitung des Defender Elite herunterzuladen.

2.11 Über KDMElite

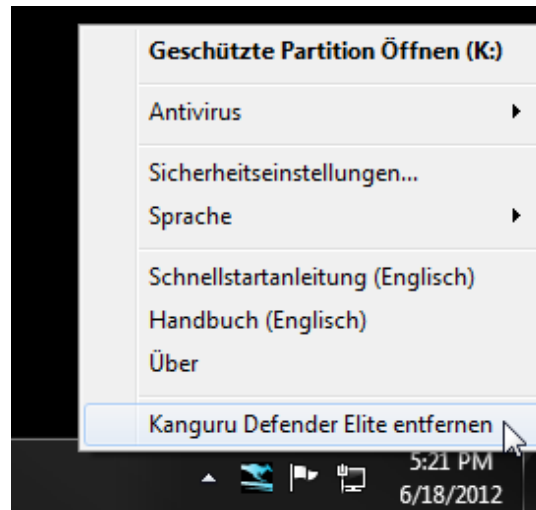
Informationen zur Version des aktuell auf Ihrem Gerät installierten KDMElite erhalten Sie über einen Rechtsklick auf das KDMElite-Symbol  in der Taskleiste unter dem Punkt **Über KDMElite**.



2.12 Schließen des Defender Elite

Wenn Sie den Defender Elite beenden, schließt sich die KDMElite-Applikation und die sichere Partition mit Ihren verschlüsselten Daten wird bis zum nächsten Login nicht erreichbar sein.

Um den Defender Elite zu beenden, klicken Sie mit der rechten Maustaste auf das KDMElite-Symbol  in der Taskleiste und wählen **Kanguru Defender Elite entfernen**.



Das KDMElite-Symbol verschwindet aus der Taskleiste und die sichere Partition des Defender Elite ist nicht mehr erreichbar.

Achtung! Trennen Sie die Verbindung zum Kanguru Defender Elite nicht, ohne das Gerät zuvor korrekt - so wie in diesem Kapitel beschrieben - geschlossen zu haben. Entfernen Sie das Gerät bitte wie in Kapitel 3. *Sicheres Entfernen des Kanguru Defender Elite* auf Seite 32 beschrieben. Sonst riskieren Sie Datenverlust oder -beschädigung.

3. Sicheres Entfernen des Kanguru Defender Elite

Bevor Sie den Defender Elite aus dem USB-Anschluss herausziehen, sollten Sie sich immer versichern, dass Sie die sichere Partition geschlossen haben (siehe Kapitel 2.12 *Beenden des Defender Elite* auf Seite 31). Nachdem Sie den Defender geschlossen haben, können Sie die Funktion Ihres Betriebssystems nutzen, um das USB-Gerät sicher zu entfernen.

3.1 Sicheres Entfernen unter Windows

Achtung! Stellen Sie sicher, dass die sichere Partition geschlossen wurde, bevor Sie versuchen, den Defender zu entfernen. Siehe Kapitel 2.12. *Beenden des Defender Elite* auf Seite 31.

Bitte nutzen Sie die Windows-Funktion **Hardware sicher entfernen**, bevor Sie den Defender herausziehen.

Sicheres Entfernen des Defender Elite:

1. Klicken Sie auf das Symbol **Hardware sicher entfernen** in der Taskleiste.

Anmerkung: Das Symbol kann unterschiedlich aussehen, je nachdem, welche Windows-Version Sie nutzen.

Windows XP / 2000



Windows Vista / 7



2. Ein Popup-Menü erscheint mit einer Liste aller USB-Geräte, die mit dem Computer verbunden sind. Wählen Sie den Defender Elite aus (Er erscheint mit zwei Laufwerksbuchstaben).
3. Eine Nachricht zeigt an, dass das mobile Speichergerät sicher entfernt werden kann. Sie können den Defender Elite nun herausziehen.

Wenn die Nachricht „Das Laufwerk kann derzeit nicht entfernt werden“ erscheint, stellen Sie bitte sicher, dass alle Fenster und Applikationen, die mit dem Defender Elite zusammenhängen, geschlossen sind, und versuchen es erneut.

3.2 Sicheres Entfernen unter Mac OS X

Achtung! Stellen Sie sicher, dass Sie die sichere Partition geschlossen haben, bevor Sie versuchen, den Defender zu entfernen. Siehe Kapitel 2.12. *Beenden des Defender Elite* auf Seite 31.

Um das Defender-Laufwerk zu entfernen, klicken Sie auf das **KDMelite-Symbol** und ziehen es vom Desktop in den Papierkorb. Wenn Sie das KDMelite-Symbol bewegen, verwandelt sich das Papierkorb-Symbol in ein Auswerfen/Beenden-Symbol.

Alternativ können Sie durch einen Rechtsklick auf das **KDMelite-Symbol** ein Popup-Menü öffnen und dort „Auswerfen/Beenden“ wählen.

Sobald das KDMelite-Symbol nicht mehr auf Ihrem Desktop angezeigt wird, können Sie den Defender Elite sicher herausziehen.

3.3 Sicheres Entfernen unter Linux

Achtung! Stellen Sie sicher, dass Sie die sichere Partition geschlossen haben, bevor Sie versuchen, das Defender-Laufwerk zu entfernen. Siehe Kapitel 2.12 *Beenden des Defender Elite* auf Seite 31.

Um das Defender-Laufwerk zu entfernen, klicken Sie mit der rechten Maustaste auf das **KDMelite-Symbol** auf dem Desktop und klicken im Popup-Menü auf **Beenden**. Sobald das KDMelite-Symbol nicht mehr auf Ihrem Desktop angezeigt wird, können Sie den Defender Elite sicher herausziehen.

4. Garantiehinweise

Dieses Produkt besitzt eine dreijährige Garantie ab Kaufdatum. Kanguru Solutions ist nicht für Schäden verantwortlich, die im Auslieferungsprozess auftreten. Jegliche Ansprüche wegen Verlustes oder Beschädigung müssen dem Lieferanten direkt angezeigt werden. Ansprüche aufgrund von Lieferfehlern sollten Kanguru Solutions innerhalb von drei (3) Werktagen nach Erhalt der Ware mitgeteilt werden.

5. Technischer Support

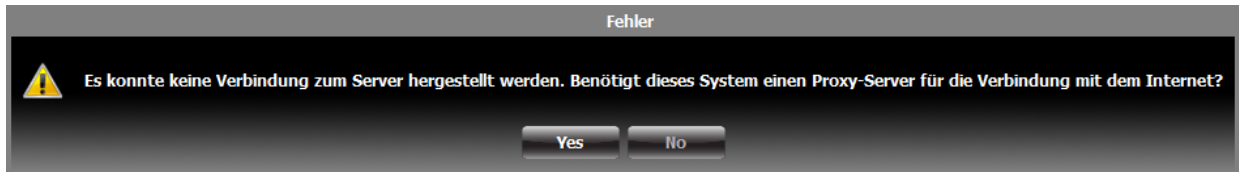
Falls bei der Verwendung Ihres Kanguru Defender Elite irgendwelche Probleme auftreten oder Sie irgendwelche technischen Fragen zu einem unserer Produkte haben, rufen Sie bitte unsere Abteilung Technischer Support an. Unser technischer Support ist kostenlos montags bis freitags zwischen 9 und 17 Uhr erreichbar.

Telefon 1-508-376-4245
oder besuchen Sie unsere Webseite unter www.kanguru.com

Anhang A - Proxy Support

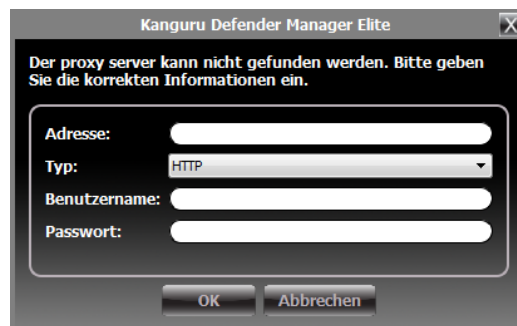
Wenn Ihr Computer einen Proxy Server für den Internetzugang nutzt, benötigen Sie für die Konfiguration des KDMelite die genauen Proxy-Informationen.

Falls sich die KDMelite-Applikation nicht mit dem Internet verbinden kann, sehen Sie folgende Fehlermeldung:



Wenn der Computer, mit dem der Defender Elite verbunden ist, einen Proxy Server nutzt, um einen Internetzugang zu erhalten, klicken Sie bitte den **JA**-Button. KDMelite versucht nun, die Informationen zum Proxy Server in der Konfiguration des Computers zu lesen.

- **Proxy Server ohne Authentisierung:** Wenn es KDMelite möglich ist, die Adresse des Proxy Servers zu ermitteln und keine **Authentisierung** benötigt wird, liest der KDMelite die Information ein und stellt eine Verbindung mit dem Internet her.
- **Proxy Server mit Authentisierung:** Wenn es KDMelite möglich ist, die Adresse des Proxy Servers zu ermitteln, aber eine **Authentisierung** benötigt wird, werden Sie aufgefordert, die Berechtigungsdaten in das sich öffnende Fenster einzutragen.
- Wenn es KDMelite möglich ist, sich mit den ermittelten Berechtigungsdaten mit dem Proxy Server zu verbinden, wird die Authentisierung in einer verschlüsselten Proxy-Einstellungsdatei gespeichert. Wenn es KDMelite nicht möglich ist, die Adresse des Proxy Servers zu ermitteln, werden Sie aufgefordert, die Adresse des Proxy Servers, den Proxy-Typ und die Berechtigungsdaten einzutragen:



Tragen Sie die Proxy-Adresse und den Port der Verbindung in das Adressfeld ein (zum Beispiel 192.168.0.193:8080 oder proxycom:8080). Wählen Sie Ihren Proxy-Typ aus und tragen Sie Ihre Berechtigungsdaten ein. Wenn es KDMelite möglich ist, sich mit diesen Informationen mit dem Proxy Server zu verbinden, werden die Proxy-Information und die Authentisierungsinformation in einer verschlüsselten Datei in den Proxy-Einstellungen gespeichert.



"Technologie in Bewegung"



Kanguru Solutions
1360 Main Street
Millis, MA 02054
www.kanguru.com

07.20.12 V 2.0 © 2012 Kanguru Solutions

Die rechtlichen Bestimmungen und Nutzungsbedingungen finden Sie auf www.kanguru.com