

KASPERSKY LAB

Kaspersky Mobile Security 7.0
Enterprise Edition

ADMINISTRATORHAND
BUCH

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE
EDITION

Administratorhandbuch

© Kaspersky Lab

www.kaspersky.de

Inhalt

KAPITEL 1. VERWALTUNG DES PROGRAMMS ÜBER KASPERSKY ADMINISTRATION KIT	5
KAPITEL 2. REMOTE-INSTALLATION DES PROGRAMMS.....	8
2.1. Installationspaket anlegen.....	8
2.2. Installation mit der Aufgabe zur Remote-Installation.....	9
2.3. Programm über SMS installieren.....	21
2.4. Gerät in Gruppe einfügen.....	23
KAPITEL 3. RICHTLINIENVERWALTUNG.....	26
3.1. Erstellen einer Richtlinie	26
3.2. Richtlinienparameter anzeigen und bearbeiten.....	34
3.2.1. Programm-Informationen anzeigen	35
3.2.2. Ergebnisse der Richtlinienübernahme anzeigen.....	36
3.2.3. Parameter für Ereignisregistrierung im Programmverlauf konfigurieren	37
3.2.4. Parameter für Antiviren-Untersuchung bestimmen.....	39
3.2.5. Parameter für Echtzeitschutz festlegen	40
3.2.6. Updatequelle für Programm-Datenbanken bestimmen	41
3.2.7. Parameter für Anti-Spam festlegen.....	42
3.2.8. Parameter für Anti-Theft festlegen.....	44
3.2.9. Zusätzliche Parameter eingeben	45
KAPITEL 4. VERWALTUNG DER PARAMETER FÜR PROGRAMMFUNKTIONEN	47
4.1. Programm-Informationen anzeigen.....	49
4.2. Informationen über Parameter für Antiviren-Untersuchung anzeigen.....	50
4.3. Informationen über Parameter für Echtzeitschutz anzeigen.....	51
4.4. Informationen über Updatequelle anzeigen	51
4.5. Informationen über Parameter für Anti-Spam anzeigen	52
4.6. Informationen über Parameter für Anti-Theft anzeigen.....	53
4.7. Informationen über zusätzliche Parameter anzeigen	54
4.8. Informationen über Schlüssel anzeigen	55
4.9. Ereignis-Informationen anzeigen	56

ANHANG A. KASPERSKY LAB.....	58
ANHANG B. KASPERSKY LAB ENDNUTZERVERTRAG	60

KAPITEL 1. VERWALTUNG DES PROGRAMMS ÜBER KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit ist ein Programm für die wichtigsten administrativen Aufgaben zur Verwaltung der Sicherheit von mobilen Geräten.

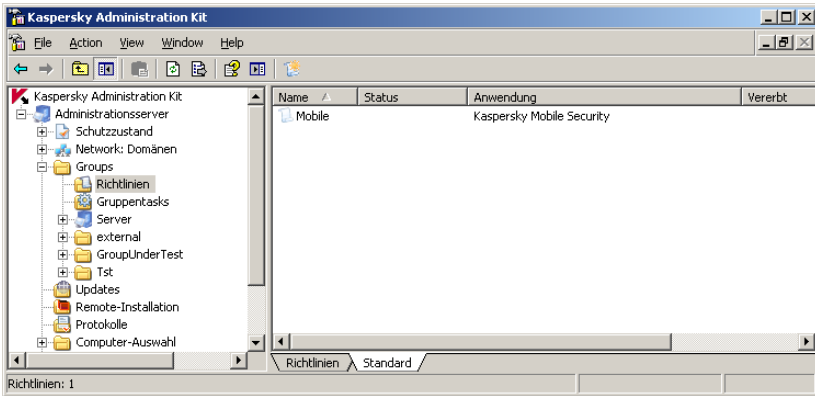


Abbildung 1. Administrationskonsole des Kaspersky Administration Kit

Bei einer zentralen Verwaltung über das Kaspersky Administration Kit bestimmt der Administrator die Richtlinien und Anwendungen. Der Schutz beruht auf diesen Einstellungen.

Eine Besonderheit für die zentrale Verwaltung ist die Organisation von mobilen Geräten in Gruppen und die Verwaltung über Gruppenrichtlinien.

Eine **Richtlinie** ist eine Sammlung von Parametern für Kaspersky Mobile Security Enterprise Edition für eine Gruppe eines logischen Netzwerkes. Die Richtlinie wird bei jeder Art der Synchronisierung mit dem Administrationsserver auf das mobile Gerät verbreitet.

Anmerkung

Damit Kaspersky Administration Kit mobile Geräte erkennt, öffnen Sie die Registerkarte **Einstellungen** im Eigenschaftfenster des Administrationsservers und setzen Sie das Häkchen bei **Port für Handheld-Geräte öffnen**.

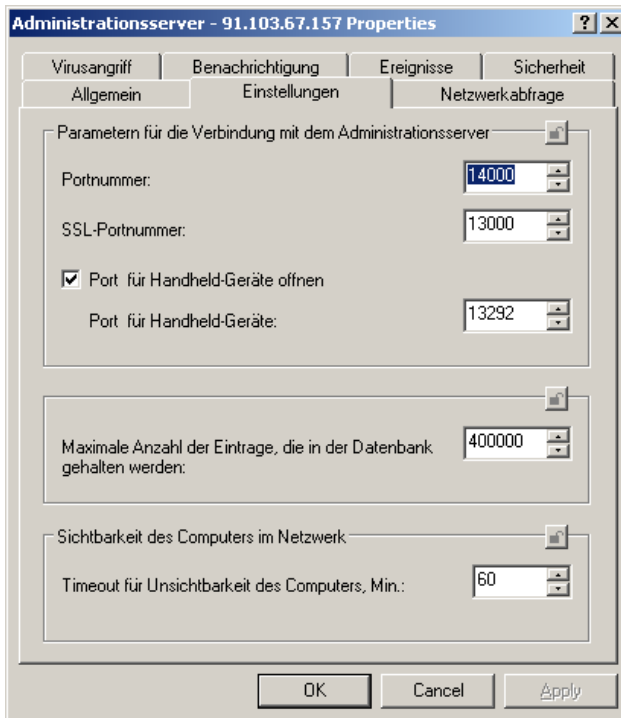


Abbildung 2. Registerkarte **Einstellungen**

Achtung!

Mobile Gerät verbinden sich über das SSL-Protokoll mit dem Administrationsserver. Um so eine Verbindung aufzubauen, muss das Zertifikat auf dem Server vorhanden sein.

Um ein Zertifikat für mobile Geräte anzulegen, machen Sie Folgendes:

1. Öffnen Sie den Installationsordner von Kaspersky Administration Kit
2. Starten Sie das Utility *klmbldct.exe*.

3. Im nächsten Fenster des Assistenten für das Anlegen eines Zertifikates geben Sie die Adresse des Administrationssservers ein (s. Abb. 3).

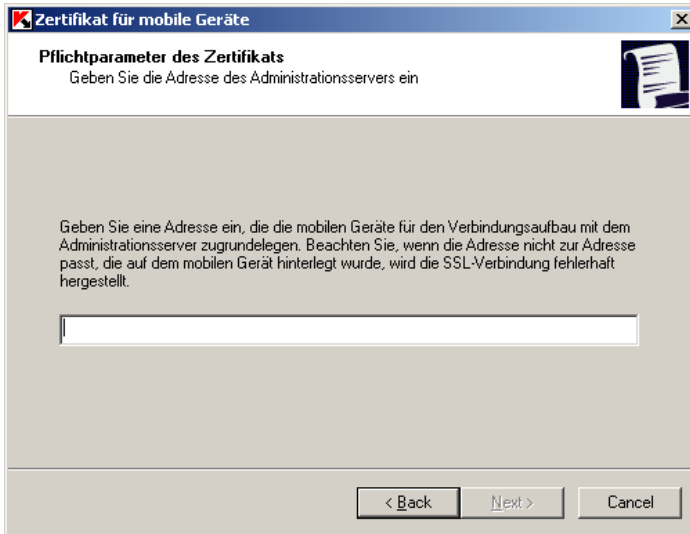


Abbildung 3. Zertifikat für mobile Geräte anlegen

4. Folgen Sie den Schritten des Assistenten bis zur Fertigstellung des Zertifikates.

KAPITEL 2. REMOTE- INSTALLATION DES PROGRAMMS

Achtung!

Die Remote-Installation von Kaspersky Mobile Security ist nicht möglich, wenn auf dem Administrator-Desktop nicht das Verwaltungs-PlugIn von Kaspersky Mobile Security installiert ist. Das Installationspaket des PlugIns gehört zum Lieferumfang von Kaspersky Mobile Security Enterprise Edition und liegt im PlugIn-Ordner.

In diesem Abschnitt ist die Installation von Kaspersky Mobile Security mit der Aufgabe zur Remote-Installation und die Installation per SMS beschrieben.

2.1. Installationspaket anlegen

Die Remote-Installation erfolgt mit einem Installationspaket.

Um ein Installationspaket anzulegen, machen Sie Folgendes:

1. Stellen Sie eine Verbindung zum Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur das Element **Remote-Installation**, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Neu** → **Installationspaket** oder auf den gleichen Punkt im Menü **Aktion**. Es wird daraufhin der Assistent aufgerufen, dessen Anweisungen Sie folgen.
3. Es wird Ihnen vorgeschlagen, den Namen des Installationspaketes und im nächsten Schritt die zu installierende Anwendung anzugeben (s. Abb. 4).
4. Mit der Dropdown-Liste entscheiden Sie sich für eine Variante: **Kaspersky-Lab-Anwendungspaket erstellen**. Mit der Schaltfläche **Durchsuchen** wählen Sie die Datei mit der Programmbeschreibung (Datei hat die Endung **.kpd** und gehört zum Lieferumfang des Programms) aus. Es werden danach automatisch die Felder mit dem Programmnamen und der Versionsnummer ausgefüllt.

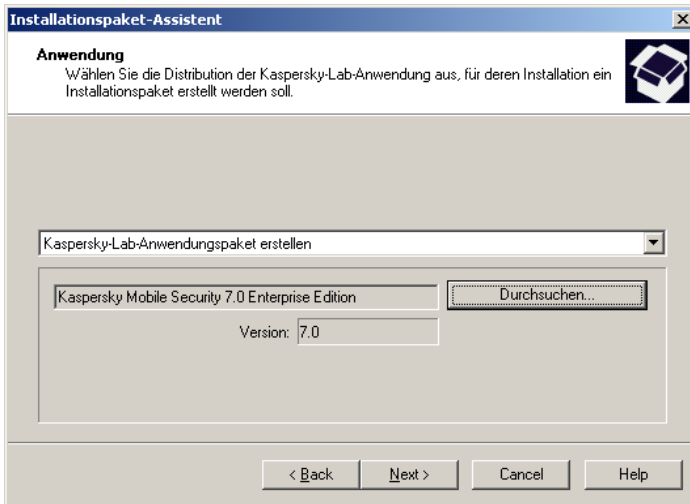


Abbildung 4. Installationspaket anlegen. Anwendung für Installation wählen

5. Jetzt werden auf den Administrationsserver in den gemeinsamen Ordner die Dateien kopiert, die für die Installation des Programms auf dem mobilen Gerät benötigt werden.

Nach Fertigstellung des Assistenten wird das neue Installationspaket dem Element **Remote-Installation** hinzugefügt und im Ergebnisfenster angezeigt.

2.2. Installation mit der Aufgabe zur Remote-Installation

Die Installation des Programms mit der Aufgabe zur Remote-Installation wird verwendet, wenn mobile Geräte mit den Computern des logischen Netzwerkes verbunden werden. Die eigentliche Installation des Programms geschieht dann, wenn das Gerät an den Computer angeschlossen wird.

Bei der Aufgabe zur Remote-Installation des Programms auf die Client-Computer kommt eine der beiden Methoden zum Einsatz: *Push-Installation* oder *Installation mit einem Start Script*.

Die *Push-Installation* erlaubt die Remote-Installation des Programms auf ausgewählten Client-Computern des logischen Netzwerkes. Beim Start der Aufgabe kopiert der Administrationsserver aus dem gemeinsamen Ordner die Installationsdateien des Programms auf die Client-Computer in ein temporäres Verzeichnis und startet überall das Setup-Programm. Zur erfolgreichen

Aufgabenausführung mit der Push-Installation muss der Administrationsserver über die Berechtigungen des lokalen Administrators auf den Client-Computern des logischen Netzwerks verfügen. Diese Methode eignet sich für die Installation von Anwendungen auf Computern, die unter den Betriebssystemen Microsoft Windows NT / 2000 / 2003 / XP laufen, bei denen diese Option unterstützt wird, oder auf Computern mit den Betriebssystemen Microsoft Windows 98 / Me, auf denen der Administrationsagent installiert ist.

Achtung!

Besteht zwischen dem Administrationsserver und dem Client-Computer eine Verbindung über das Internet oder ist die Verbindung durch eine netzwerkinterne Firewall gesichert, können die gemeinsamen Ordner für die Datenübertragung nicht verwendet werden. In so einem Fall werden die für die Installation des Programms benötigten Dateien vom Administrationsagenten übertragen. Die Installation des Administrationsagenten erfolgt auf solche Computer lokal.

Die zweite Methode, die *Installation mit einem StartszENARIO*, erlaubt es, den Start der Aufgabe zur Remote-Installation an ein konkretes Konto eines Benutzers (mehrerer Benutzer) zu binden. Nach Fertigstellung der Aufgabe wird in das StartszENARIO für die angegebenen Benutzer der Start des Setup-Programms eingetragen, das sich im gemeinsamen Ordner des Administrationsservers befindet. Zur erfolgreichen Aufgabenausführung müssen das Benutzerkonto, mit dem die Aufgabe gestartet wird, oder der Administrationsserver über das Recht zum Ändern von Startskripten in der Datenbank des Domänen-Controllers verfügen. Diese Berechtigung hat der Administrator der Domäne, so dass die Aufgabe oder der gesamte Administrationsserver mit den Rechten dieses Benutzers gestartet werden. Als Ergebnis wird bei der Anmeldung des Benutzers an der Domäne versucht, die Installation des Programms auf dem Client-Computer durchzuführen, von dem aus sich der Benutzer anmeldet. Diese Methode eignet sich für die Installation von Kaspersky-Lab-Anwendungen auf Computern, die unter den Betriebssystemen Microsoft Windows 98/Me laufen.

Achtung!

Damit die Aufgabe zur Remote-Installation mit StartszENARIO des Benutzers erfolgreich ausgeführt wird, müssen die Benutzer, bei denen im Szenario Änderungen eingetragen werden, auf ihren Computern über die Berechtigungen des lokalen Administrators verfügen.

Die Gruppenaufgaben Remote-Installation des Programms auf Client-Computern werden nur mit der Push-Installation durchgeführt. Wenn Sie eine globale Aufgabe erstellen, können Sie die gewünschte Methode angeben: Push-Installation oder Installation mit einem StartszENARIO.

Um eine globale Aufgabe zur Remote-Installation mit Push-Installation zu erstellen, machen Sie Folgendes:

1. Stellen Sie eine Verbindung zum Administrationsserver her.
2. Markieren Sie in der Konsolenstruktur das Element **Globale Tasks**, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Neu / Task** oder auf den gleichen Punkt im Menü **Aktion**. Es wird daraufhin der Assistent für eine neue Aufgabe aufgerufen, dessen Anweisungen Sie folgen.
3. Legen Sie den Namen der Aufgabe fest.
4. Beim Festlegen des Programms und Bestimmen der Aufgabenart (s. Abb. 5) setzen Sie die Werte jeweils auf **Kaspersky Administration Kit** und **Remote-Installation**.
5. Geben Sie danach das Installationspaket an, dessen Installation mit dieser Aufgabe verbunden ist (s. Abb. 6). Markieren Sie das Paket, das für diesen Administrationsserver angelegt wurde, oder erstellen Sie ein neues Paket mit der Schaltfläche **Neu**.

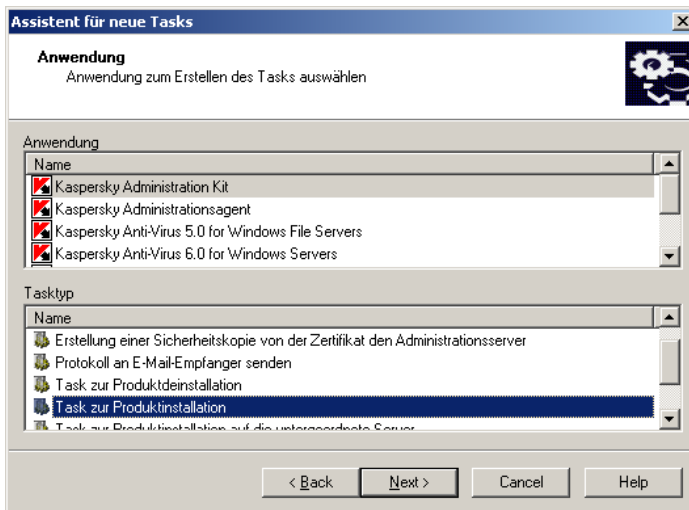


Abbildung 5. Aufgabenart festlegen

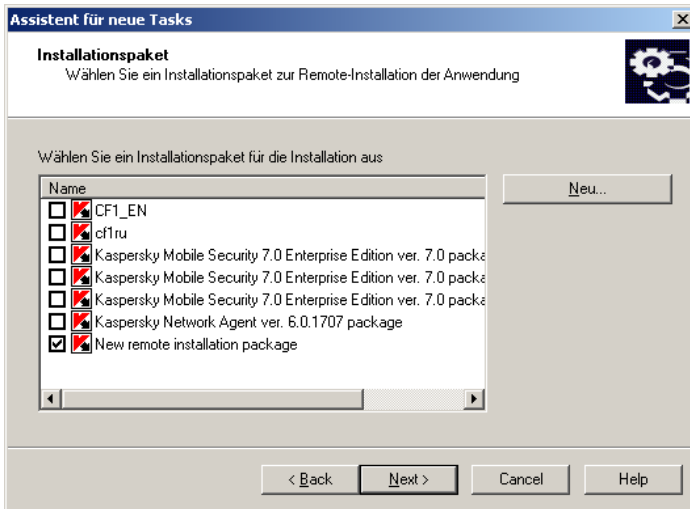


Abbildung 6. Installationspaket auswählen

- In dieser Etappe gehen Sie auf die Variante **Installieren Erzwingen** (s. Abb. 7).

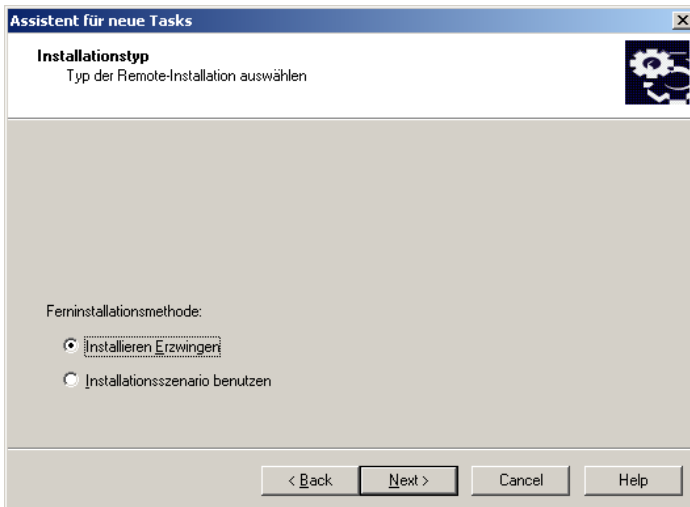


Abbildung 7. Installationsmethode auswählen

- In diesem Fenster des Assistenten (s. Abb. 8) legen Sie Zusatzparameter für die Installation fest:

- Ob das Programm erneut installiert werden soll, wenn es noch nicht auf dem Client-Computer installiert ist.
- Setzen Sie das Häkchen im Kontrollkästchen **Anwendung nicht installieren, wenn sie schon installiert ist**, damit keine neue Installation erfolgt (Standardeinstellung). In so einem Fall wird für die Computer, auf denen die Anwendung bereits lokal installiert ist bzw. nach einem vorangegangenen zeitplangesteuerten Start der Aufgabe zur Remote-Installation die Aufgabe nicht gestartet.

Wenn das Häkchen nicht gesetzt ist, wird die Aufgabe zur Remote-Installation solange nach Zeitplan gestartet, bis die Installationsversuche erschöpft sind.

- Geben Sie die Methode für die Übergabe der Installationsdateien an die Client-Computer an.

Setzen Sie unter **Laden des Installationspakets** folgende Häkchen in den Kontrollkästchen:

- Setzen Sie das Häkchen im Kontrollkästchen **Mittels Microsoft Windows aus gemeinsamen Ordner**, damit die Übertragung der Dateien für die Installation auf die Client-Computer mit Windows-Mitteln aus dem gemeinsamen Ordner erfolgt (Standardeinstellung). Diese Übertragungsvariante wird empfohlen, wenn auf dem Computer, auf dem die Installation erfolgt, der Administrationsagent nicht installiert ist, der mit diesem Administrationsserver verbunden ist.
- Setzen Sie das Häkchen im Kontrollkästchen **Mit Hilfe des Administrationsagenten**, damit die Übertragung der Dateien auf die Client-Computer durch den auf jedem Computer installierten Administrationsagenten erfolgt (Standardeinstellung). Der Administrationsagent muss mit diesem Administrationsserver verbunden sein.
- Geben Sie im Feld **Maximale Anzahl der gleichzeitigen Downloads** die maximale Anzahl der Client-Computer an, die gleichzeitig Daten vom Administrationsserver herunterladen können.
- Die Anzahl der Installationsversuche beim zeitgesteuerten Task-Start kann festgelegt werden, indem Sie den gewünschten Wert im Feld **Anzahl der Versuche** eingeben. Ein erneuter Versuch wird unternommen, wenn während der Ausführung der vorhergehenden Installation Fehler auftraten.

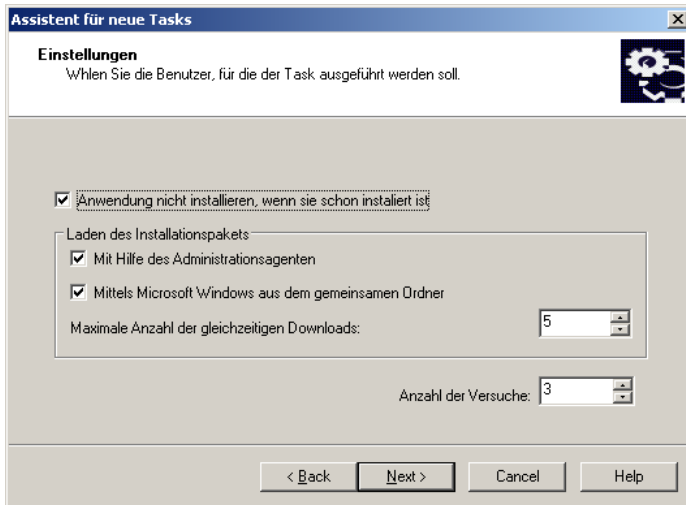


Abbildung 8. Zusatzparameter der Installation

8. In diesem Schritt (s. Abb. 9) können Sie entscheiden, ob mit dem Programm der Administrationsagent installiert werden soll.

Wenn auf dem Netzwerkcomputer, mit dem das mobile Gerät eine Verbindung aufbaut, der Administrationsagent nicht installiert ist, dessen Installation Sie aber für notwendig erachten, können Sie die Installationsdateien des Administrationsagenten in das Installationspaket des Programms aufnehmen.

Setzen Sie dazu das Häkchen im Kontrollkästchen **Kaspersky Network Agent Paket installieren** und setzen Sie das Häkchen neben dem Namen des gewünschten Installationspaketes. Bei Bedarf legen Sie ein neues Installationspaket mit der Schaltfläche **Neu** an.

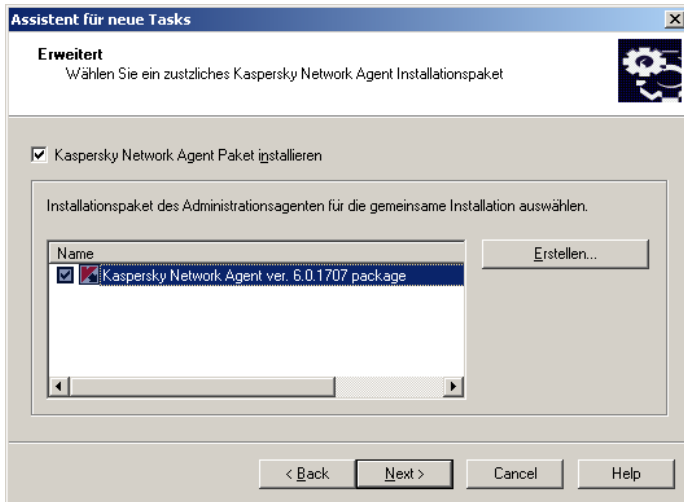


Abbildung 9. Gemeinsame Installation mit Administrationsagenten

9. In diesem Fenster bestimmen Sie die Computer, für die eine Aufgabe angelegt wird (s. Abb. 10):
- **Auf Basis von Daten, die sich aus dem Windows-Netzwerk ergeben.** In diesem Fall erfolgt die Auswahl der Computer zur Installation anhand von Daten, die der Administrationsserver beim Durchsuchen des Corporate-Windows-Netzwerkes gewonnen hat.
 - **Auf Basis von manuell einzugebenden IP-Adresse, NetBIOS-Name, oder DNS-Name.** In diesem Fall werden die Installationscomputer manuell ausgewählt.

Wenn die Computer anhand von Daten ausgewählt werden sollen, die beim Durchsuchen des Windows-Netzwerkes gewonnen wurden, wird die Liste im Fenster des Assistenten (s. Abb. 11) so gebildet wie beim Hinzufügen von Computern zu einem logischen Netzwerk (Details s. Benutzerhandbuch für Kaspersky Administration Kit). Zur Auswahl stehen Client-Computer des logischen Netzwerkes (Ordner **Gruppen**) oder Computer, die noch nicht dazu gehören (Ordner **Netzwerk**).

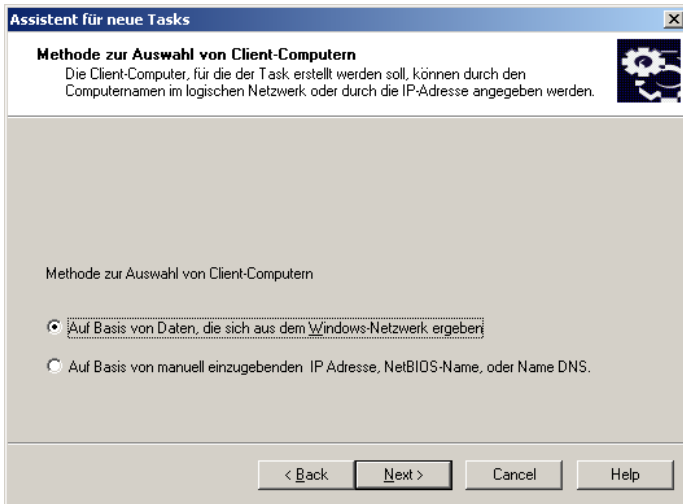


Abbildung 10. Auswahl von Client-Computern

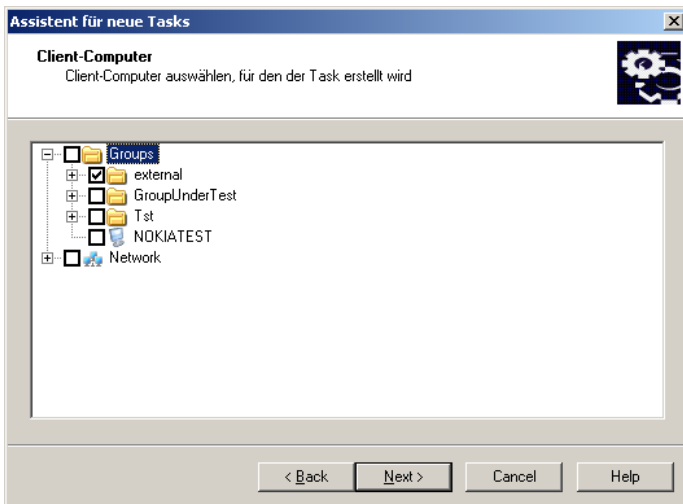


Abbildung 11. Erstellen einer Computerliste für die Installation anhand der Daten des Windows-Netzwerkes

Wenn die Computer manuell ausgesucht werden, wird die Liste anhand der NetBIOS- oder DNS-Namen, der IP-Adressen (oder eines Bereiches von IP-Adressen) für die Computer zusammengestellt, oder

durch Import der Liste aus einer *txt*-Datei, in der jede Adresse in einer neuen Zeile angegeben sein muss (s. Abb. 12).

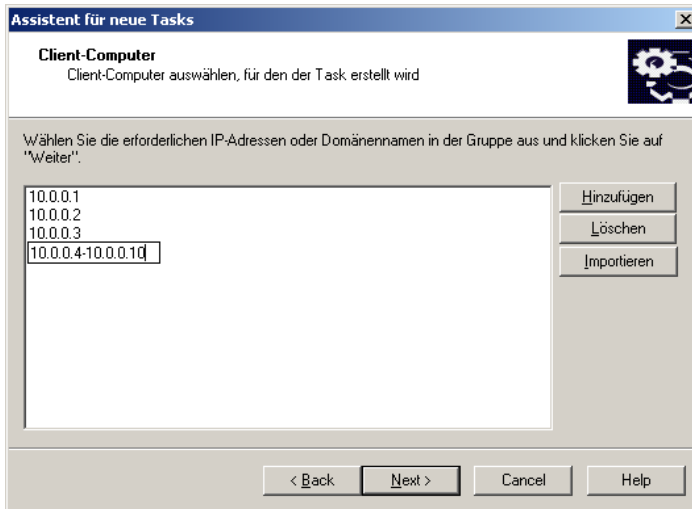


Abbildung 12. Liste der Computer für die Installation anhand der IP-Adressen

10. Geben Sie im nächsten Fenster des Assistenten an, mit den Rechten welches Benutzerkontos die Aufgabe zur Remote-Installation auf den Computern gestartet werden soll (s. Abb. 13).

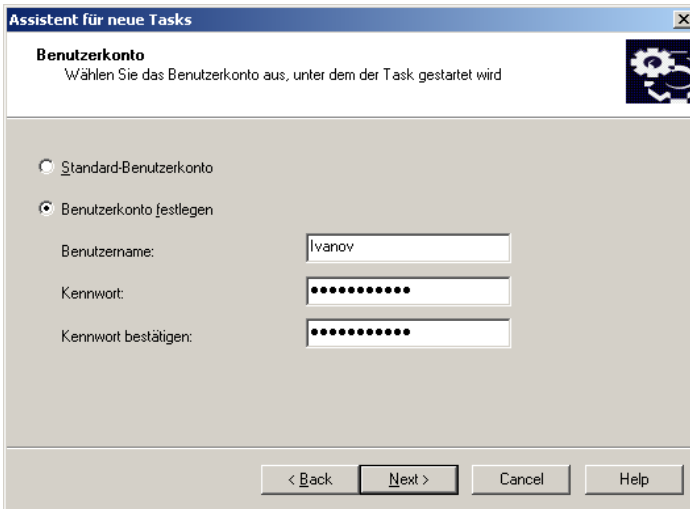


Abbildung 13. Benutzerkonto auswählen

Achtung!

Das Benutzerkonto muss über Administratorrechte auf allen Computern verfügen, auf denen die Remote-Installation der Anwendung geplant ist.

Bei der Installation von Programmen auf Computern, die zu unterschiedlichen Domänen gehören, müssen vertrauenswürdige Beziehungen zwischen diesen Domänen und der Domäne, in der der Administrationsserver arbeitet, bestehen.

Wählen Sie:

- **Standard-Benutzerkonto** – wenn der Administrationsserver unter dem Benutzerkonto eines Domänenbenutzers gestartet wird und das Konto über die zur Programminstallation erforderlichen Rechte verfügt.
- **Benutzerkonto festlegen** – wenn der Administrationsserver unter dem System-Benutzerkonto gestartet wird oder das Benutzerkonto des Administrationsservers nicht über Rechte zum Start des Tasks Remote-Installation verfügt.

Achtung!

Für eine Remote-Installation von Programmen auf Computern, die nicht zur Domäne gehören, muss der Task Remote-Installation unter dem Konto desjenigen Benutzers gestartet werden, der die Administratorenrechte auf diesen Computern hat.

Geben Sie in den unten angebrachten Feldern die Attribute des Benutzers ein, dessen Konto die geforderten Bedingungen erfüllt.

11. Erstellen Sie nun einen Zeitplan für den Aufgabenstart (s. Abb. 14).

- Wählen Sie in der Dropdown-Liste **Start nach Zeitplan** den gewünschten **Modus für den Task-Start** aus:
 - **Manuell**
 - **Jede N-te Stunde**
 - **Täglich**
 - **Wöchentlich**
 - **Monatlich**
 - **Einmal** (Aufgabe zur Remote-Installation wird dann auf den Computern nur einmal gestartet, egal, welches Resultat sich dabei ergeben hat)
 - **Sofort** (sofort nach dem Erstellen der Aufgabe, nach Abschluss des Assistenten)
 - **Nach Fertigstellung anderer Aufgabe** (Aufgabe zur Remote-Installation startet erst nach Abschluss der angegebenen Aufgabe)
- Richten Sie den Zeitplan in der Feldergruppe ein, die dem ausgewählten Modus entspricht (Näheres s. Benutzerhandbuch für Kaspersky Administration Kit).

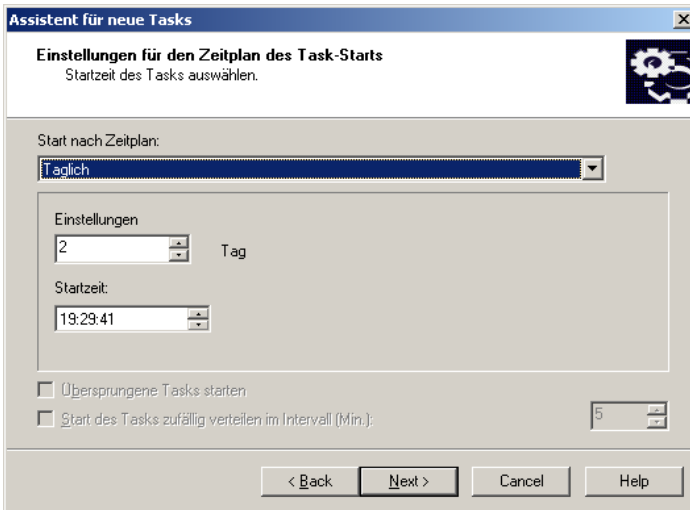


Abbildung 14. Täglicher Aufgabenstart

Nach Abschluss des Assistenten wird die neue Aufgabe zur Remote-Installation dem Element **Globale Tasks** hinzugefügt und im Ergebnisfenster angezeigt.

Um die Aufgabe zur Remote-Installation zu starten, machen Sie Folgendes:

Markieren Sie in der Konsolenstruktur das Element **Globale Tasks**, markieren Sie im Ergebnisfenster das gewünschte Installationspaket, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Installieren** oder auf den gleichnamigen Punkt im Menü **Aktion**.

Nach der Installation wird auf dem Computer im Hintergrund das Programm *kmlisten.exe* aufgerufen, das den Anschluss von mobilen Geräten an den Computer überwacht. Sollte ein angeschlossenes Gerät erkannt werden, öffnet sich ein Fenster (s. Abb. 15), in dem das Gerät angegeben wird, auf das das Programm installiert wird.

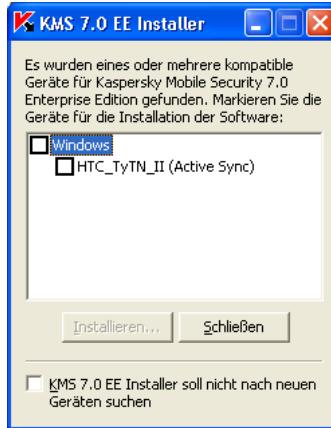


Abbildung 15. Fenster des Hilfsprogramms *KMListen.exe*

Klicken Sie auf die Schaltfläche **Installieren**, um das Installationspaket für das Programm auf das mobile Gerät zu laden. Nach dem Kopiervorgang befolgen Sie die Anweisungen des Installationsassistenten, der auf dem Gerät aufgerufen wird.

2.3. Programm über SMS installieren

Die Installation des Programms mit einer SMS kommt infrage, wenn mobile Geräte nicht mit den Computern des logischen Netzwerkes verbunden werden.

Achtung!

Um eine SMS zu versenden, muss ein GSM-Modem vorhanden sein, das eine Verbindung zum Administrationsserver aufbaut. Außerdem muss auf dem Server Microsoft .NET Framework 2.0 installiert sein. Sonst lassen sich keine SMS verschicken.

Um das Programm mit einer SMS zu installieren, machen Sie Folgendes:

1. Stellen Sie eine Verbindung zum Administrationsserver her.
2. Markieren Sie in der Konsolenstruktur das Element **Remote-Installation**.
3. Gehen Sie im Kontextmenü des angelegten Installationspakets für das Programm auf den Eintrag **Eigenschaften**.
4. Öffnen Sie die Registerkarte **Parameter** und klicken Sie auf die Schaltfläche **Über SMS installieren**.

5. Im sich öffnenden Fenster (s. Abb. 16) bestimmen Sie die Installationsparameter:
- a) Im Block **GSM-Modem** geben Sie die Parameter für die Modem-Verbindung an: Port und Geschwindigkeit.
 - b) Im Feld **URL-Distribution** tragen Sie die Adresse des öffentlichen Servers ein, auf dem die Installationsdateien von Kaspersky Mobile Security liegen und von dem das Programm installiert wird.

Beispiel:

ftp://ftp.domain.com/distrib/KMS7EE/kmsecurity_7_0_15_beta.sis

oder

http://domain.name.ru/distrib/KMS7EE/kmsecurity_ee_wm_sp_7_0_0_49_ru.cab

- b) Legen Sie eine Liste mit Nummern an, an die SMS-Nachrichten geschickt werden sollen. Tragen Sie dazu in das Eingabefeld die Nummer ein und klicken Sie auf die Schaltfläche **Nummer hinzufügen**. Die eingegebene Nummer wird in die Liste übernommen.

Klicken Sie auf die Schaltflächen **In Datei speichern** und **Aus Datei hinzufügen**, um die Liste der Nummern in einer TXT-Datei zu speichern oder sie aus einer früher erstellten Datei zu laden.

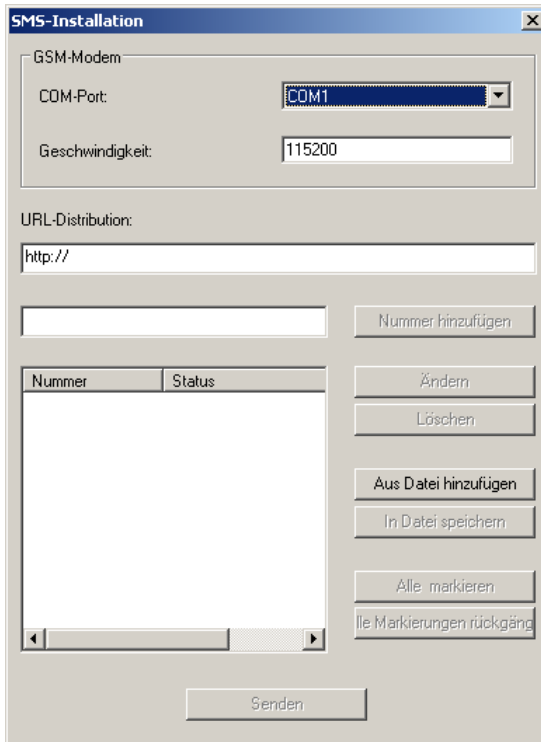


Abbildung 16. Parameter für SMS-Versand

6. Klicken Sie auf die Schaltfläche **Senden**, damit die SMS-Nachrichten für die Installation von Kaspersky Mobile Security an die eingegebenen Nummern gesendet werden.

Auf mobile Geräte, deren Nummern in der Liste stehen, werden SMS-Nachrichten mit der URL des Installationspaketes geschickt. Beim Öffnen der URL auf dem Gerät wird das Installationspaket für das Programm geladen. Nach dem Kopiervorgang befolgen Sie die Anweisungen des Installationsassistenten, der auf dem Gerät aufgerufen wird.

2.4. Gerät in Gruppe einfügen

Nach der Installation von Kaspersky Mobile Security werden beim Durchsuchen des Netzwerkes alle mobilen Geräte in die Domäne mit dem Namen verschoben, die beim Erstellen des Installationspaketes angegeben wurden (Standard lautet

PDAGroup). Auf das Gerät wird dabei nicht die Richtlinie angewendet, die für mobile Geräte angelegt wurde.

Anmerkung

Die Gruppe für mobile Geräte erscheint im Container **Netzwerk** (im Modus **Darstellung der Domänen**) nach der ersten Verbindung des mobilen Gerätes mit dem Administrationsserver, wenn auf dem Gerät Kaspersky Mobile Security vorhanden ist.

Zum Verschieben des mobilen Gerätes in eine Administrationsgruppe öffnen Sie die Administrationskonsole, wechseln Sie zum Container **Netzwerk** und gehen Sie auf den Modus **Darstellung der Domänen**. In der Liste der Netzwerkgruppen öffnen Sie die Gruppe **PDAGroup** und ziehen Sie das mobile Gerät in die gewünschte Administrationsgruppe.

Um mobile Geräte automatisch in die gewünschte Gruppe zu verschieben, machen Sie Folgendes:

1. Öffnen Sie die Konsolenstruktur und wechseln Sie zum Container **Netzwerk**.
2. Gehen Sie auf die Gruppe **PDAGroup** und öffnen Sie mit dem Kontextmenü das Eigenschaftfenster der Gruppe.
3. Öffnen Sie die Registerkarte **Client-Computer** (s. Abb. 17).

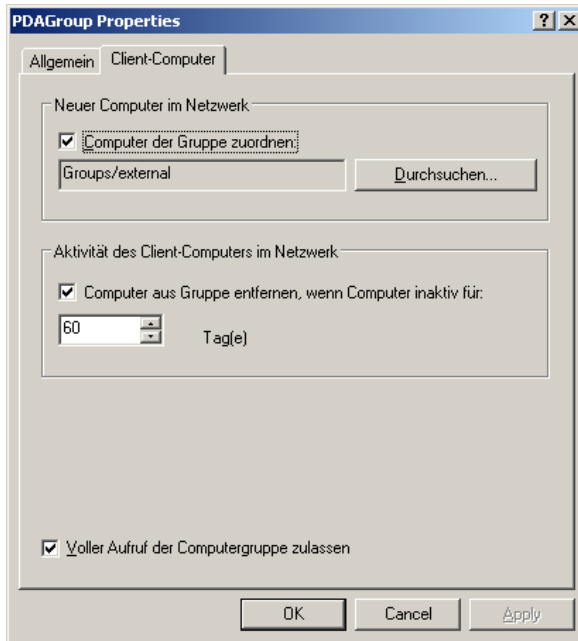


Abbildung 17. Gruppeneigenschaften

4. Im Block **Neuer Computer im Netzwerk** setzen Sie das Häkchen im Kontrollkästchen **Computer der Gruppe zuordnen**.
5. Klicken Sie auf die Schaltfläche **Durchsuchen** und markieren Sie im nächsten Fenster die Administrationsgruppe, zu der neu angeschlossene mobile Geräte verschoben werden sollen.
6. Speichern Sie die Änderungen.

KAPITEL 3. RICHTLINIENVERWA LTUNG

In diesem Abschnitt finden Sie Informationen über das Erstellen und Konfigurieren einer Richtlinie für Kaspersky Mobile Security 7.0 Enterprise Edition.

Eine Richtlinie wird in den folgenden Fällen angewendet:

- bei der ersten Verbindung des Gerätes mit dem Netzwerk
- bei nachfolgenden Verbindungen des Gerätes, wenn die Programm- oder Richtlinienparameter geändert worden sind
- bei Aufruf der manuellen Synchronisierung (s. Benutzerhandbuch von Kaspersky Mobile Security).


3.1. Erstellen einer Richtlinie

Um eine Richtlinie zu erstellen, führen Sie folgende Aktionen durch:

1. Markieren Sie in der Konsolenstruktur im Knoten **Gruppen** die Gruppe derjenigen mobilen Geräte, für die eine Richtlinie erstellt werden muss.
2. Markieren Sie den zur ausgewählten Gruppe gehörenden Ordner **Richtlinien**, öffnen Sie das Kontextmenü und gehen Sie auf den Eintrag **Neue→Richtlinie**.

Die Anlage einer Richtlinie erfolgt über einen Assistenten für Microsoft Windows (Windows Wizard) und besteht aus einer Abfolge von Fenstern, zwischen denen Sie mit den Schaltflächen **Zurück** und **Weiter** navigieren können. Der Assistent wird mit der Schaltfläche **Fertig** beendet, abrechen können Sie jederzeit mit der Schaltfläche **Abbrechen**.

Achtung!

In jedem Schritt für die Anlage einer Richtlinie lassen sich die eingegebenen Parameter mit der Schaltfläche  fixieren. Ist das Schloss in der Schaltfläche verschlossen, werden im Weiteren bei Verwendung der Richtlinie auf den mobilen Geräten Werte übernommen, die von der angelegten Richtlinie vorgegeben sind.

Schritt 1. Eingabe von allgemeinen Richtliniendaten

Im ersten Fenster des Assistenten müssen Sie einen Namen für die Richtlinie vergeben (Feld **Name**). Im zweiten Fenster wählen Sie das Programm **Kaspersky Mobile Security 7.0 Enterprise Edition** aus der Dropdown-Liste **Anwendungsname** aus. Damit die Richtlinieneinstellungen sofort nach dem Anlegen in Kraft treten, muss im dritten Fenster das Häkchen **Aktive Richtlinie** im Block **Richtlinienzustand** gesetzt werden.

Schritt 2. Parameter für Antiviren-Untersuchung bestimmen

In diesem Schritt werden die Parameter für die Antiviren-Untersuchung des mobilen Gerätes festgelegt: Untersuchungsbereich und Zeitplan für den Start der Untersuchung.

Im Block **Untersuchungsparameter** (s. Abb. 18) können Sie den Untersuchungsbereich auswählen, indem Sie die Dateitypen markieren, die untersucht werden sollen, und ob versucht werden soll, ein infiziertes Objekt zu desinfizieren:

- **Nur ausführbare Dateien untersuchen** – Untersucht werden ausführbare Programmdateien.
- **Archive** – Dateien untersuchen, die als Archiv gepackt sind
- **Versuch zur Desinfektion des infizierten Objektes** – Das infizierte Objekt wird versucht zu desinfizieren. Es lassen sich nicht alle Objekte reparieren.

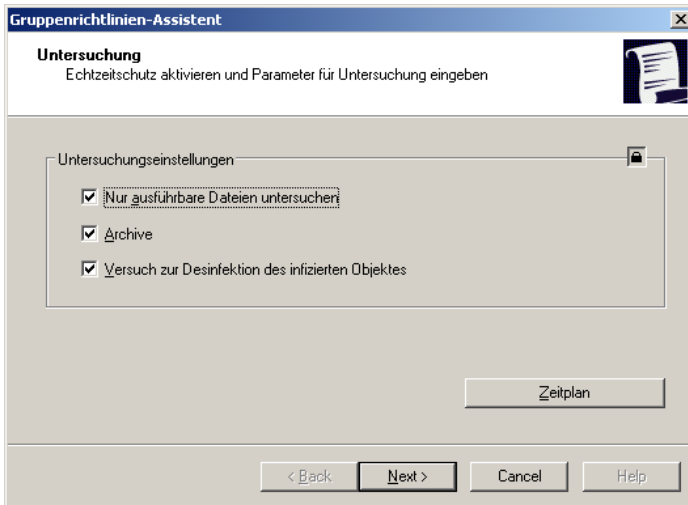


Abbildung 18. Parameter für Antiviren-Untersuchung konfigurieren

Um einen Zeitplan für einen Scan auf Befehl einzugeben, klicken Sie auf **Zeitplan**. Es öffnet sich ein Dialogfenster, in dem das Untersuchungsintervall eingegeben werden muss:

- **Manuell** – Die Aktion wird bei einem manuellen Start auf Wunsch des Benutzers ausgeführt.
- **Täglich** – Die Untersuchung erfolgt jeden Tag. In der Feldergruppe **Startzeit** geben Sie das Datum für den Aufgabenstart ein.
- **Wöchentlich** – Die Untersuchung erfolgt an einem bestimmten Wochentag. In der Feldergruppe **Startzeit** geben Sie die Zeit für die Aktion an und wählen einen Wochentag aus, wann der Scan auf Befehl ausgeführt werden soll.

Schritt 3. Parameter für Echtzeitschutz eingeben

In diesem Schritt werden die Echtzeitschutz-Parameter für das Dateisystem und für den Speicher des mobilen Gerätes festgelegt.

Setzen Sie das Häkchen im Kontrollkästchen **Echtzeitschutz aktivieren** (s. Abb. 19), damit das Programm alle ausführbaren Programme und Dateien untersucht, die der Benutzer öffnen kann.

Im Block **Untersuchungseinstellungen** können Sie den Untersuchungsbereich auswählen, indem Sie die Dateitypen markieren, die untersucht werden sollen.

- **Nur ausführbare Dateien untersuchen** – Untersucht werden nur ausführbare Programmdateien.

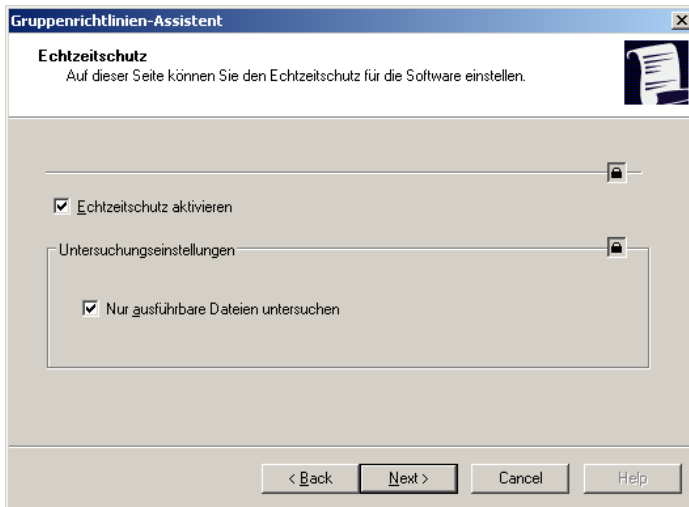


Abbildung 19. Parameter für Echtzeitschutz einrichten

Schritt 4. Auswahl der Updatequelle

In diesem Schritt wird die Updatequelle bestimmt und ein Zeitplan für die Updates aktiviert.

Im Block **Updatequelle** (s. Abb. 20) geben Sie die Adresse des Servers an, von dem Updates erfolgen.

Damit Updates von den Kaspersky-Lab-Updateservern erfolgen, lassen Sie das Feld **Geben Sie den HTTP- oder FTP-Update-Server ein** leer.

Werden Updates von einer anderen Ressource geladen, geben Sie im Block **Updatequelle** die Adresse der Updatequelle ein. Es muss eine komplette URL der Datei *mobile.xml* eingetragen werden.

Beispiel: <http://domain.com/index/mobile.xml>

Achtung!

Die Ordnerstruktur in der Updatequelle muss mit der Struktur auf den Updateservern von Kaspersky Lab übereinstimmen.

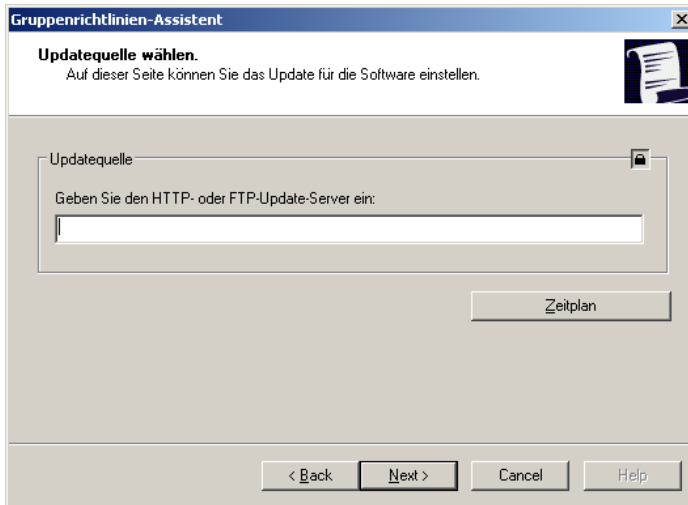


Abbildung 20. Auswahl der Updatequelle

Außerdem können Sie einen Zeitplan für den Update-Start eingeben. Klicken Sie dazu auf die Schaltfläche **Zeitplan**. Es öffnet sich ein Fenster, in dem das Untersuchungsintervall eingegeben werden muss:

- **Manuell** – Die Aktion wird bei einem manuellen Start auf Wunsch des Benutzers ausgeführt.
- **Täglich** – Die Untersuchung erfolgt jeden Tag. In der Feldergruppe **Startzeit** geben Sie das Datum für den Aufgabenstart ein.
- **Wöchentlich** – Die Untersuchung erfolgt an einem bestimmten Wochentag. In der Feldergruppe **Startzeit** geben Sie die Zeit für die Aktion an und wählen einen Wochentag aus, an dem der Scan auf Befehl ausgeführt werden soll.

Schritt 5. Parameter für Anti-Spam festlegen

In diesem Schritt können Sie die Parameter für das Anti-Spam-Modul einrichten (s. Abb. 21).

Geben Sie einen Funktionsmodus für Anti-Spam im Block **Schutz vor unerwünschter Post** ein:

- **Deaktiviert.** Anti-Spam ist deaktiviert.
- **Nur Nachrichten aus weißer Liste zulässig.** In diesem Modus überspringt Anti-Spam Nachrichten, die auf der "weißen" Liste stehen. Die übrigen Nachrichten werden gesperrt.
- **Nur Nachrichten aus schwarzer Liste sperren.** In diesem Modus sperrt Anti-Spam den Empfang von Nachrichten, die auf der "schwarzen" Liste stehen. Die übrigen Nachrichten werden übersprungen.
- **Standard.** In diesem Modus filtert Anti-Spam eingehende Nachrichten anhand der „schwarzen“ und „weißen“ Liste. Geht eine Nachricht von einer Telefonnummer ein, die in keiner Liste steht, benachrichtigt Anti-Spam den Benutzer und schlägt das Sperren oder Zulassen des Nachrichtenempfangs vor und empfiehlt außerdem die Übernahme der Telefonnummer in die „weiße“ oder „schwarze“ Liste.

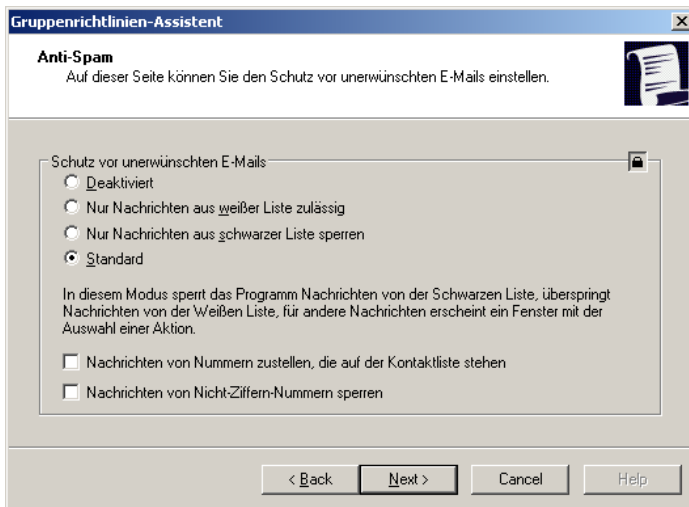


Abbildung 21. Parameter für Anti-Spam festlegen

Setzen Sie das Häkchen im Kontrollkästchen **Nachrichten von Nummern zustellen, die auf der Kontaktliste stehen**, damit Anti-Spam Nachrichten von Nummern aus der Kontaktliste überspringt.

Setzen Sie das Häkchen im Kontrollkästchen **Nachrichten von Nicht-Ziffer-Nummern sperren**, damit Anti-Spam Nachrichten von Nummern, die nicht ausschließlich Ziffern enthalten, sperrt.

Schritt 6. Zusätzliche Parameter eingeben

In diesem Schritt können Sie die Sicherheitsstufe für das Firewall-Modul eingeben und außerdem die Synchronisierung mit dem Administrationsserver einstellen.

Im Block **Firewall** (s. Abb. 22) richten Sie die Sicherheitsstufe für das Firewall-Modul ein. Die Firewall gewährleistet den Schutz des mobilen Gerätes auf einer der folgenden Stufen:

- **Deaktiviert.** Die Firewall ist deaktiviert.
- **Niedrig.** Die Firewall sperrt alle eingehenden Verbindungen, jede ausgehende Verbindung ist zugelassen.
- **Mittel.** Die Firewall sperrt alle eingehenden Verbindungen. Die ausgehenden Verbindungen können über die HTTP-, HTTPS-, SMTP-, IMAP- und SSH-Protokolle hergestellt werden.
- **Hoch.** Die Firewall sperrt jede Netzwerkaktivität, außer Verbindungen mit dem Administrationsserver und Updates der Programm-Datenbanken.

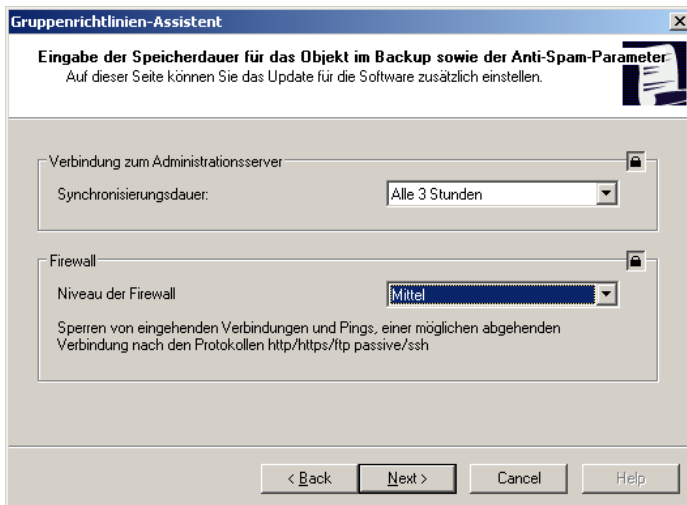


Abbildung 22. Zusätzliche Programmeinstellungen

Im Block **Verbindung zum Administrationsserver** geben Sie das Intervall des Verbindungsaufbaus ein, indem Sie den gewünschten Wert in der Dropdown-Liste **Synchronisierungsdauer** markieren. Standardmäßig initiiert das mobile Gerät alle 6 Stunden den Verbindungsaufbau mit dem Administrationsserver.


Schritt 7. Auswahl einer Schlüsseldatei

In diesem Schritt können Sie die Schlüsseldatei angeben, die zur Aktivierung von Kaspersky Mobile Security dient.

Klicken Sie auf die Schaltfläche **Ändern** und geben im nächsten Fenster die Schlüsseldatei an. Im Fenster des Assistenten werden danach die folgenden Informationen zum Lizenzschlüssel angezeigt:

- Nummer
- Schlüsseltyp
- Ablaufdatum für die Gültigkeit
- Lizenzbeschränkungen


Achtung!

Damit die Schlüsseldatei auf mobile Geräte geladen wird, muss die Wahl mit der Schaltfläche  fixiert werden. Sonst kann Kaspersky Mobile Security nicht aktiviert werden.

Schritt 8. Richtlinienerstellung abschließen

Das letzte Fenster des Assistenten informiert Sie über den erfolgreichen Abschluss für die Erstellung der Richtlinie (s. Abb. 23).

Nach Fertigstellung des Assistenten wird die Richtlinie für Kaspersky Mobile Security 7.0 Enterprise Edition im Ordner **Richtlinien** der entsprechenden Gruppe eingefügt und im Ergebnisfenster angezeigt.

Die angelegte Richtlinie und deren Einstellungen können Sie bearbeiten und Einschränkungen für die Änderung der Parameter mithilfe der Schaltfläche  für jede Gruppeneinstellung festlegen. Der Benutzer des mobilen Gerätes kann die Einstellungen nicht ändern, die auf diese Weise fixiert worden sind. Die Verbreitung der Richtlinie auf mobile Geräte erfolgt bei der ersten Synchronisierung der Clients mit dem Server unmittelbar nach dem Hinzufügen des mobilen Geräts in die Administrationsgruppe.

Sie können Richtlinien aus einer Gruppe in eine andere Gruppe übertragen und mit den Standardbefehlen des Kontextmenüs **Kopieren / Einfügen**, **Ausschneiden / Einfügen** und **Löschen** oder der analogen Einträge im Menü **Aktion** einfügen beziehungsweise löschen.

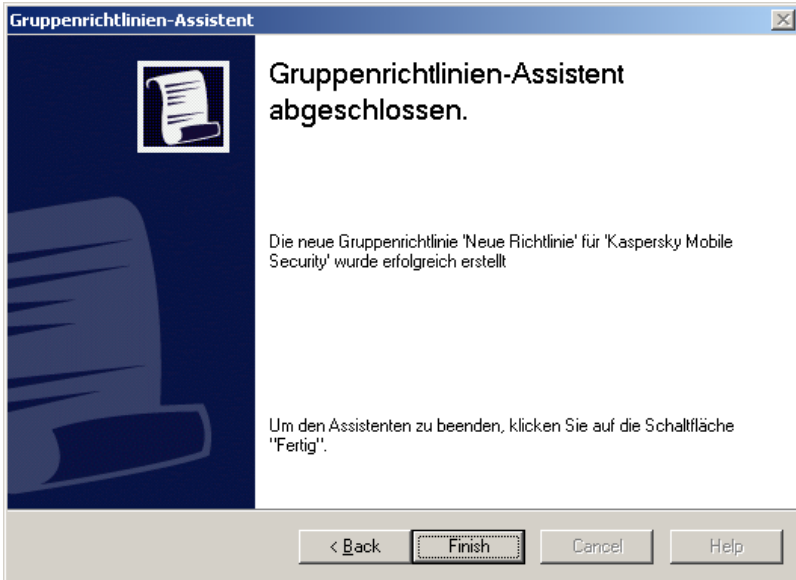


Abbildung 23. Richtlinienerstellung abschließen

3.2. Richtlinienparameter anzeigen und bearbeiten

Beim Bearbeiten können Sie eine Richtlinie ändern, das Ändern der Parameter in den Richtlinien der untergeordneten Gruppen und in den Programm- und Aufgabeneinstellungen unterbinden.


1. Markieren Sie die Gruppe, zu der die mobilen Geräte gehören, in der Konsolenstruktur im Ordner **Gruppen**, für die die Parameter bearbeitet werden sollen.
2. Markieren Sie den zu dieser ausgewählten Gruppe gehörenden Ordner **Richtlinien**, dabei werden im Ergebnisfenster alle Richtlinien angezeigt, die für die Gruppe erzeugt worden sind.
3. Markieren Sie in der Richtlinienliste die gewünschte Richtlinie für **Kaspersky Mobile Security 7.0 Enterprise Edition** (Programmname steht im Feld **Anwendung**).
4. Gehen Sie im Kontextmenü der ausgewählten Richtlinie auf den Eintrag **Eigenschaften**.

Es öffnet sich das Fenster zur Einstellung der Richtlinie für das Programm, das mehrere Registerkarten enthält.

Die Registerkarten **Allgemein**, **Übernehmen** und **Ereignisse** sind Standard für das Programm Kaspersky Administration Kit (Details s. Administratorhandbuch von Kaspersky Administration Kit).

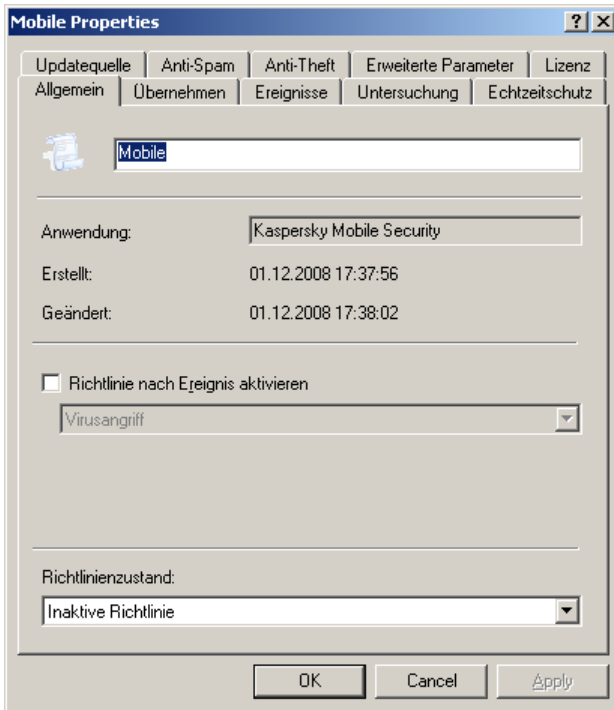
Die übrigen Registerkarten enthalten die Einstellungen für die Parameter von Kaspersky Mobile Security 7.0 Enterprise Edition. Weiter unten wird jede Registerkarte beschrieben.

Anmerkung

Beim Bearbeiten der Richtlinienparameter verwenden Sie die Schaltfläche , um die eingegebenen Richtliniendaten zu fixieren. Im Weiteren kann der Benutzer des mobilen Gerätes die Richtlinieneinstellungen nicht ändern, die auf diese Weise fixiert worden sind.

3.2.1. Programm-Informationen anzeigen

Auf der Registerkarte **Allgemein** (s. Abb. 24) stehen die folgenden Informationen über die Richtlinie: Name der Richtlinie, Name des Programms, für das sie erstellt wurde, Datum und Uhrzeit für die Erstellung der Richtlinie, Datum und Uhrzeit der letzten Änderung.

Abbildung 24. Registerkarte **Allgemein**

In dem Fenster können Sie den Namen der Richtlinie ändern, sie aktivieren oder deaktivieren sowie die Aktivierung der Richtlinie bei Eintreten eines Ereignisses konfigurieren.

3.2.2. Ergebnisse der Richtlinienübernahme anzeigen

Auf der Registerkarte **Übernehmen** (s. Abb. 25) stehen Hilfestellungen zur Übernahme der Richtlinie auf mobilen Geräten der Gruppe. Es wird dabei die Menge der Geräte angegeben, auf denen:

- die Richtlinie nicht festgelegt wurde
- sie ausgeführt wird
- sie noch nicht ausgeführt wird

- die Richtlinie aufgrund eines Fehlers nicht übernommen werden konnte.

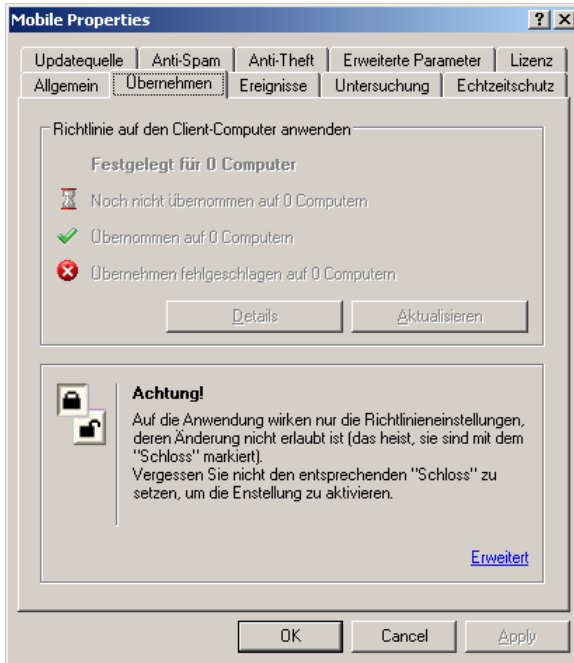


Abbildung 25. Registerkarte **Übernehmen**

Details zu den Ergebnissen der Richtlinienübernahme auf jedem Client-Computer der Gruppe lassen sich im Fenster anzeigen, das Sie mit einem Klick auf **Details** öffnen (Details s. Administratorhandbuch des Kaspersky Administration Kit).

3.2.3. Parameter für Ereignisregistrierung im Programmverlauf konfigurieren

Kaspersky Mobile Security generiert während des Programmablaufs einen bestimmten Bestand an Ereignissen. Jedes Ereignis hat Merkmale, die dessen Prioritätsstufe darstellen. Es gibt vier Prioritätsstufen: Kritisches Ereignis, Funktionsausfall, Warnung und informative Mitteilung.

Ereignisse des gleichen Typs können verschiedene Prioritätsstufen besitzen, was von der Situation abhängig ist, in der das Ereignis eingetreten ist.

Auf der Registerkarte **Ereignisse** (s. Abb. 26) stehen die Ereignistypen, die im Programmablauf eintreten und im Bericht fixiert werden, sowie der Speicherort des Berichtes und die Art der Benachrichtigung vom Administrator und / oder anderer Benutzer.

Um Ereignistypen anzuzeigen, wählen Sie die gewünschte Prioritätsstufe aus der Dropdown-Liste **Prioritätsstufe** aus. Die Ereignistypen für die ausgewählte Priorität werden im Informationsfeld dargestellt, das sich unten befindet.

Für jedes Ereignis können Sie wählen, ob es in den Bericht aufgenommen werden soll und können eine Benachrichtigung des Administrators über das Ereignis konfigurieren.

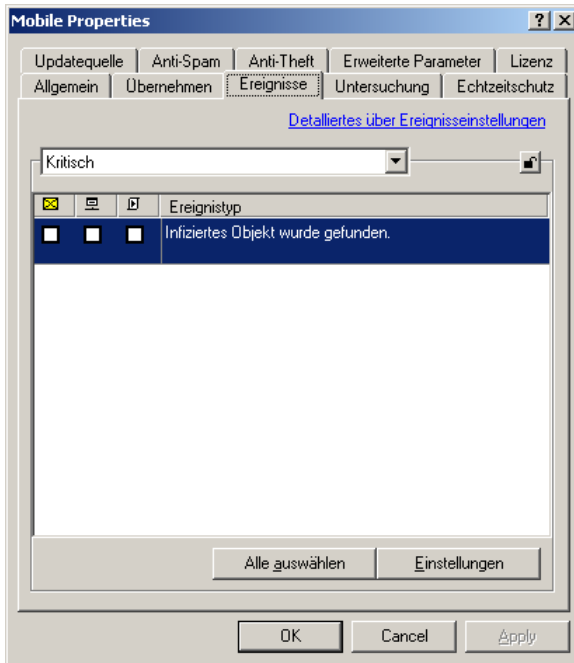


Abbildung 26. Registerkarte **Ereignisse**

Details zu den übrigen Einstellungen der Registerkarte **Ereignisse** finden Sie im Administratorhandbuch des Kaspersky Administration Kit.

3.2.4. Parameter für Antiviren-Untersuchung bestimmen

Auf der Registerkarte **Untersuchung** (s. Abb. 27) werden die Parameter für den Scan auf Befehl angepasst: Untersuchungsbereich, Aktion für infizierte Objekte sowie einen Zeitplan, nach dem die Untersuchung erfolgen wird.

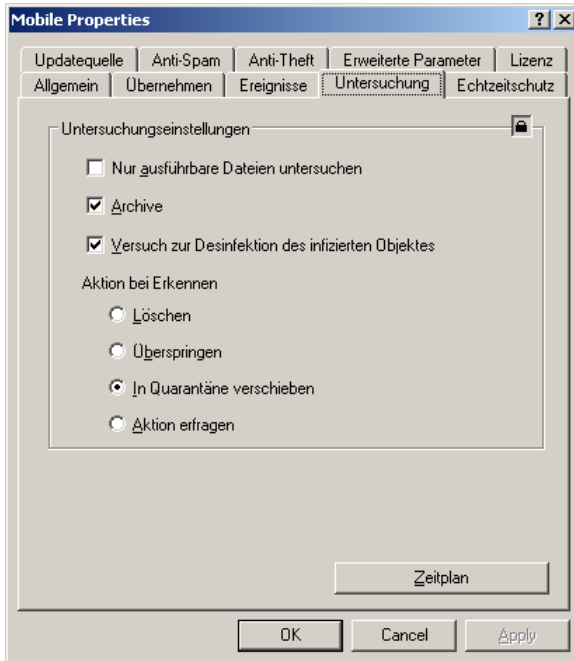


Abbildung 27. Registerkarte **Untersuchung**

Im Block **Aktion bei Erkennen** geben Sie die Aktion an, die beim Erkennen eines infizierten Objektes ausgeführt wird:

- **Löschen**
- **Überspringen** – Die erkannten infizierten Objekte werden ohne Änderung belassen.
- **In Quarantäne verschieben** – Die erkannten infizierten Objekte werden in die Quarantäne verschoben.

- **Aktion erfragen** – Meldung über erkannten Virus machen und vorschlagen, das infizierte Objekt zu löschen, es in die Quarantäne zu verschieben oder ohne Änderung zu belassen.

Wenn der Parameter **Versuch zur Desinfektion des infizierten Objektes** gesetzt ist, wird die gewählte Aktion dann ausgeführt, wenn das Objekt nicht desinfiziert werden konnte.

Die übrigen Parameter sind analog zu den oben in Pkt. 3.1 auf S. 26 beschriebenen Einstellungen.

3.2.5. Parameter für Echtzeitschutz festlegen

Auf der Registerkarte **Echtzeitschutz** (s. Abb. 28) werden die Parameter für den Echtzeitschutz festgelegt: Untersuchungsbereich, Aktionen für infizierte Objekte.

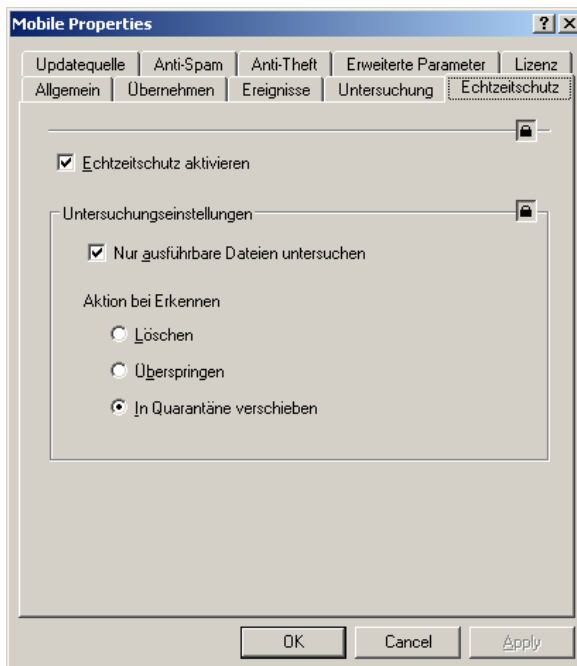


Abbildung 28. Registerkarte **Echtzeitschutz**

3.2.6. Updatequelle für Programm-Datenbanken bestimmen

Auf der Registerkarte **Updatequelle** (s. Abb. 29) wird die Updatequelle angegeben, von der die Updates der Antiviren-Datenbanken geladen werden. Außerdem kann auf der Registerkarte ein Zeitplan für den Update-Start eingegeben werden.

Damit Updates von den Kaspersky-Lab-Updateservern erfolgen, lassen Sie das Feld **Geben Sie den http- oder FTP-Update-Server ein** leer.

Wird ein Update von einer anderen Ressource geladen, geben Sie im Block **Updatequelle** die Adresse der Updatequelle ein. Es muss eine komplette URL der Datei *mobile.xml* eingetragen werden.

Beispiel: <http://domain.com/index/mobile.xml>

Achtung!

Die Ordnerstruktur in der Updatequelle muss mit der Struktur auf den Updateservern von Kaspersky Lab übereinstimmen.

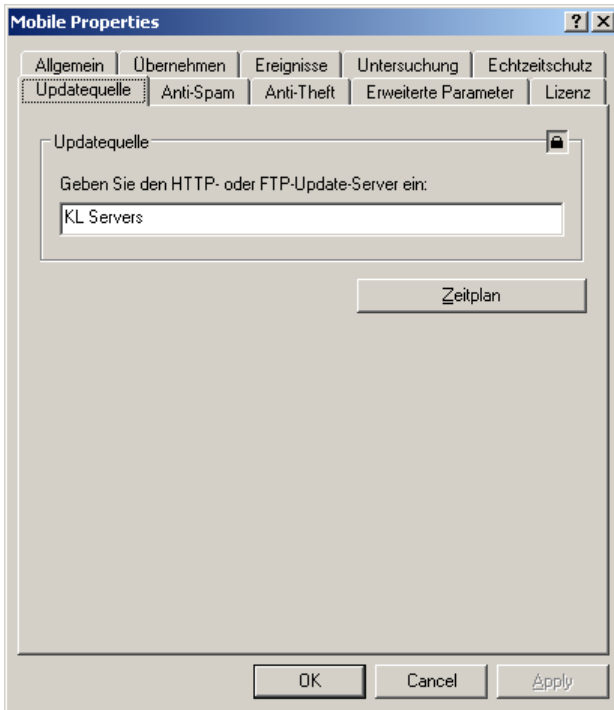


Abbildung 29. Registerkarte **Updatequelle**

3.2.7. Parameter für Anti-Spam festlegen

Auf der Registerkarte **Anti-Spam** (s. Abb. 30) werden die Parameter für den Schutz vor unerwünschter Post eingegeben.

Im Block **Schutz vor unerwünschten E-Mails** gehen Sie auf den Modus für das Anti-Spam-Modul:

- **Deaktiviert** – Beenden von Anti-Spam
- **Nur Nachrichten auf weißer Liste zulässig** – Anti-Spam prüft eine Nachricht, ob sie mit der weißen Liste übereinstimmt. Stimmt die

Absendernummer oder der Nachrichtentext mit einem Listenelement überein, überspringt Anti-Spam die Nachricht.

- **Nur Nachrichten auf schwarzer Liste sperren** – Anti-Spam prüft eine Nachricht, ob sie mit der schwarzen Liste übereinstimmt. Stimmt die Absendernummer oder der Nachrichtentext mit einem Listenelement überein, sperrt Anti-Spam die Nachricht.
- **Standard** – Anti-Spam sperrt Nachrichten von der "schwarzen" Liste, überspringt Nachrichten von der "weißen" Liste, für alle übrigen Nachrichten erscheint ein Fenster, in dem der Benutzer des Gerätes eine Aktion für die Nachricht bestimmen kann.

Setzen Sie das Häkchen im Kontrollkästchen **Nachrichten von Nummern zustellen, die auf der Kontaktliste stehen**, damit Anti-Spam Nachrichten von Nummern aus der Kontaktliste überspringt.

Setzen Sie das Häkchen im Kontrollkästchen **Nachrichten von Nicht-Ziffer-Nummern sperren**, damit Anti-Spam Nachrichten von Nummern, die nicht ausschließlich aus Ziffern bestehen, sperrt.

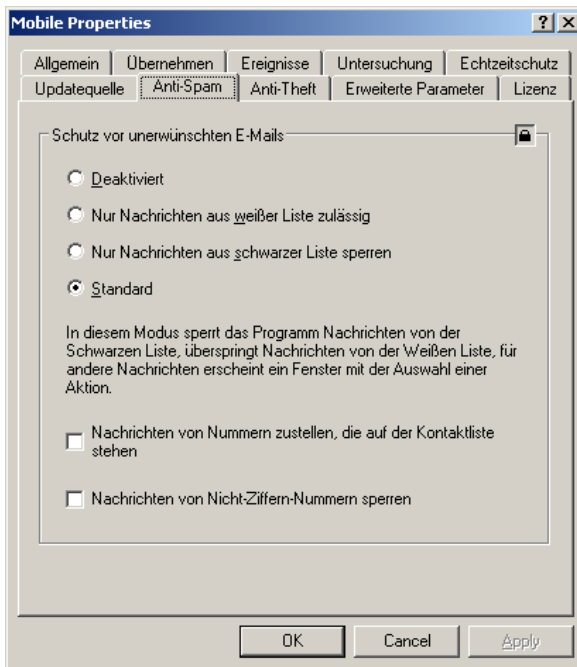


Abbildung 30. Registerkarte **Anti-Spam**

3.2.8. Parameter für Anti-Theft festlegen

Auf der Registerkarte **Anti-Theft** (s. Abb. 31) werden die Parameter für das Anti-Theft-Modul eingegeben, das Daten, die auf dem mobilen Gerät gespeichert sind, vor dem unautorisierten Zugriff schützt, falls das Gerät gestohlen wird oder verloren geht.

Setzen Sie das Häkchen im Kontrollkästchen **SMSClean**, um SMS-Clean einzuschalten. Diese Funktion löscht persönliche Benutzerdaten (Kontakte, Nachrichten, Benutzerdateien, Speicherkartendaten, Netzwerkeinstellungen). Um die Funktion SMS-Clean einzuschalten, schicken Sie auf das Gerät eine SMS mit dem Text: «clean:Code».

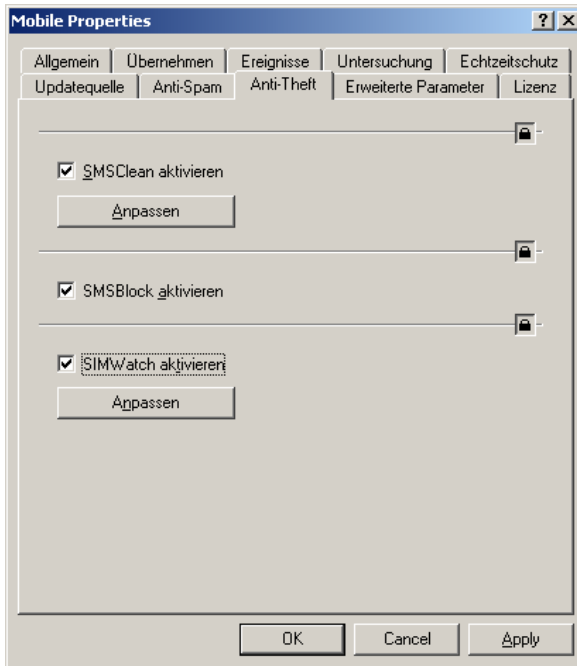
Klicken Sie auf Schaltfläche **Einrichten** und geben im nächsten Fenster die Datenkategorien an, die mit SMS-Clean gelöscht werden sollen:

- **Kontakte löschen** – Löschen des Telefonbuches
- **E-Mail löschen** – Löschen von Nachrichten
- **Dokumente löschen** – Löschen von persönlichen Daten
- **Daten von Speicherkarte löschen** – Löschen von Dateien auf Speichererweiterungskarte
- **Netzwerkeinstellungen und Access Points löschen** – Löschen von persönlichen Netzwerkeinstellungen.

Setzen Sie das Häkchen im Kontrollkästchen **SMSBlock**, um SMS-Block einzuschalten. Diese Funktion sperrt das Gerät. Es kann nur nach Eingabe eines Kennwortes entsperrt werden. Um das Gerät mit der Funktion SMS-Block zu sperren, schicken Sie auf Ihr Gerät eine SMS mit dem Text: «block:Code».

Setzen Sie das Häkchen im Kontrollkästchen **SIMWatch**, um SIM-Watch einzuschalten. Diese Funktion schickt an eingegebene Nummern die neue Telefonnummer und sperrt außerdem das Gerät, wenn die SIM-Karte im gestohlenen Gerät gewechselt wird.

Klicken Sie auf die Schaltfläche **Anpassen** und geben im nächsten Fenster die Parameter für SMS-Clean ein. In den Feldern **Basistelefon** und **Zusatztelefon** geben Sie diejenigen Telefonnummern ein, an die beim Wechsel der SIM-Karte eine SMS geschickt werden soll, in der die neue Telefonnummer steht. Außerdem können Sie eine Sperre des Gerätes beim Wechsel der SIM-Karte mit dem entsprechenden Häkchen setzen.

Abbildung 31. Registerkarte **Anti-Theft**

3.2.9. Zusätzliche Parameter eingeben

Auf der Registerkarte **Erweiterte Parameter** (s. Abb. 32) wird die Sicherheitsstufe der Firewall eingegeben und der Synchronisierungszeitraum mit dem Administrationsserver festgelegt.

Im Block **Verbindung zum Administrationsserver** geben Sie das Intervall des Verbindungsaufbaus ein, indem Sie den gewünschten Wert in der Dropdown-Liste **Synchronisierungsdauer** markieren.

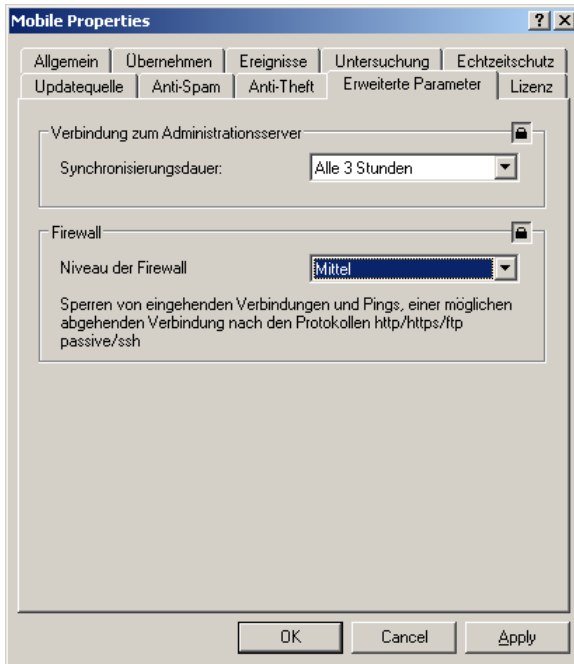


Abbildung 32. Registerkarte **Erweiterte Parameter**

Im Block **Firewall** richten Sie die Sicherheitsstufe für die Firewall ein:

- **Aktiviert** – Beenden der Firewall
- **Niedrig** – Die Firewall sperrt alle eingehenden Verbindungen, jede ausgehende Verbindung ist zugelassen.
- **Mittel** – Die Firewall sperrt alle eingehenden Verbindungen. Die ausgehenden Verbindungen können über die HTTP-, HTTPS-, SMTP-, IMAP- und SSH-Protokolle hergestellt werden.
- **Hoch** – Die Firewall sperrt jede Netzwerkaktivität, außer Verbindungen mit dem Administrationsserver und Updates der Programm-Datenbanken.

KAPITEL 4. VERWALTUNG DER PARAMETER FÜR PROGRAMMFUNKTIONEN

Mit den Programmeinstellungen können Sie die Parameter von Kaspersky Mobile Security für einzelne mobile Geräte ändern. Es lassen sich nur nicht von einer Richtlinie fixierte Parameter ändern (Details s. Pkt. 3.1 auf S. 6).

Um die Parameter in den Programmfunktionen zu ändern, machen Sie Folgendes:

1. Markieren Sie den Ordner mit dem Namen der Gruppe, zu der das mobile Gerät gehört, im Ordner **Gruppen**.
2. Markieren Sie im Ergebnisfenster das Gerät, für das Sie die Parameter der Programmfunktionen ändern müssen. Im Kontextmenü oder im Menü **Aktionen** gehen Sie auf den Eintrag **Eigenschaften**.
3. Im Programmhauptfenster öffnet sich daraufhin das Dialogfenster **Eigenschaften: Computername**. Gehen Sie auf die Registerkarte **Anwendungen** (s. Abb. 33).

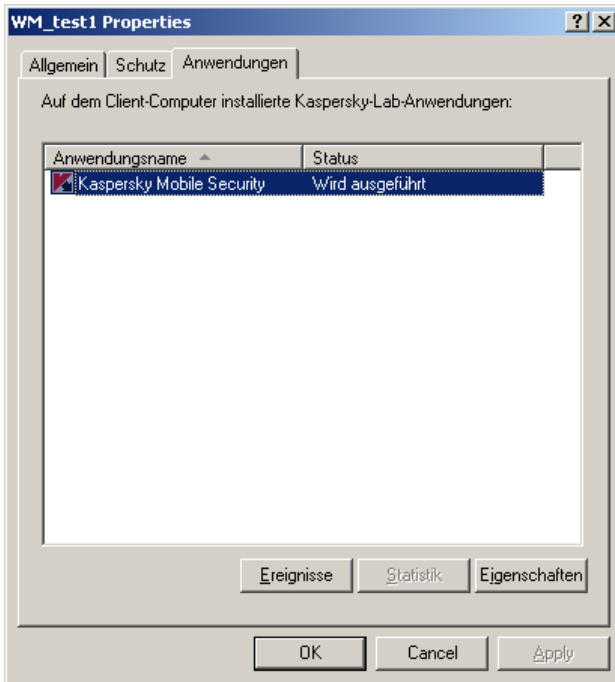


Abbildung 33. Fenster **Eigenschaften** des mobilen Gerätes anzeigen.
Registerkarte **Anwendungen**

4. Markieren Sie das Programm **Kaspersky Mobile Security 7.0 Enterprise Edition**. Im unteren Teil des Fensters befinden sich die folgenden Schaltflächen:
 - **Ereignisse** – Ereignisse im Programmablauf anzeigen, die auf dem mobilen Gerät eingetreten und auf dem Administrationsserver registriert worden sind.
 - **Statistik** - allgemeine Informationen über das Programm anzeigen.
 - **Eigenschaften** – Programm im geöffneten Fenster **Einstellungen von Anwendung Kaspersky Mobile Security 7.0 Enterprise Edition** einstellen.

4.1. Programm-Informationen anzeigen

Auf der Registerkarte **Allgemein** (s. Abb. 34) können Sie Informationen über das Programm Kaspersky Mobile Security 7.0 Enterprise Edition anzeigen lassen.

Im oberen Fensterteil steht der Name des installierten Programms, die Version, das Installationsdatum, dessen Status (ob das Programm auf dem mobilen Gerät gestartet oder beendet ist) sowie Angaben über den Zustand der Programm-Datenbanken.

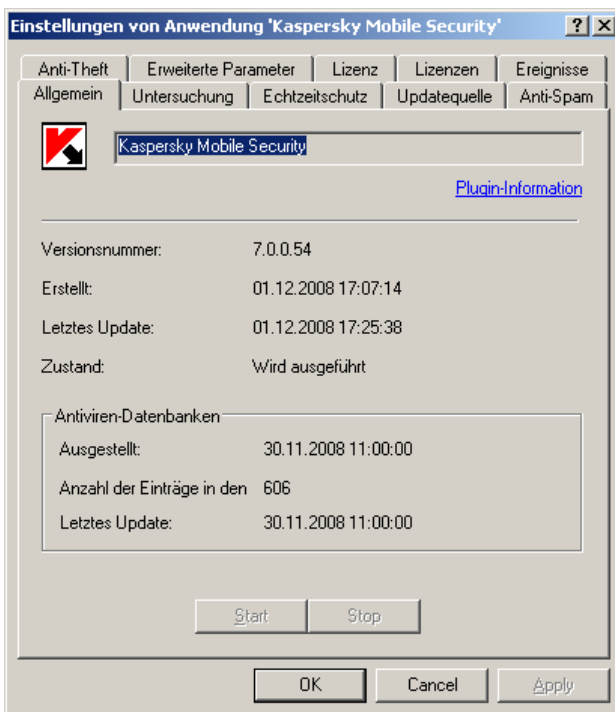


Abbildung 34. Einstellungsfenster für Anwendungseigenschaften. Registerkarte **Allgemein**

4.2. Informationen über Parameter für Antiviren-Untersuchung anzeigen

Auf der Registerkarte **Untersuchung** (s. Abb. 35) können Sie Änderungen in den Parametern für den Scan auf Befehl anzeigen lassen und vornehmen: Den Untersuchungsbereich, die Aktion für infizierte Objekte sowie den Zeitplan, dem zufolge die Untersuchung erfolgen wird.

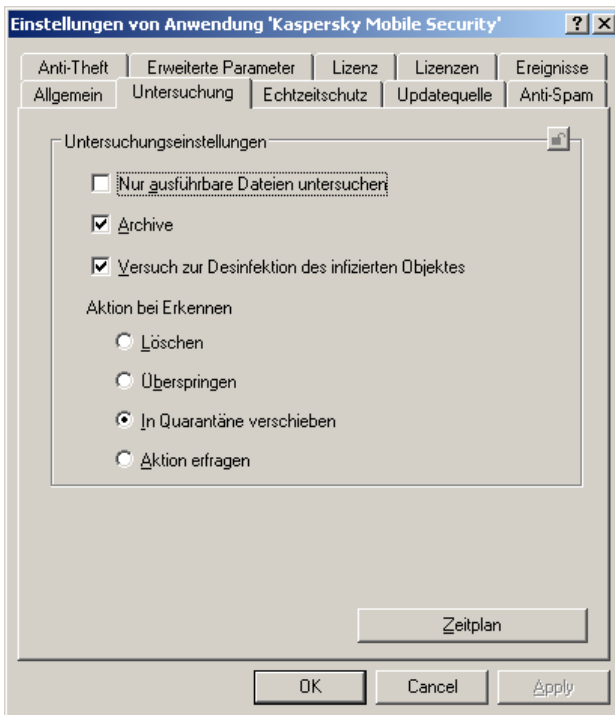


Abbildung 35. Registerkarte **Untersuchung**

4.3. Informationen über Parameter für Echtzeitschutz anzeigen

Auf der Registerkarte **Echtzeitschutz** (s. Abb. 36) können Sie Änderungen in den Parametern für den Echtzeitschutz anzeigen lassen und vornehmen: Untersuchungsbereich und Aktionen für infizierte Objekte.

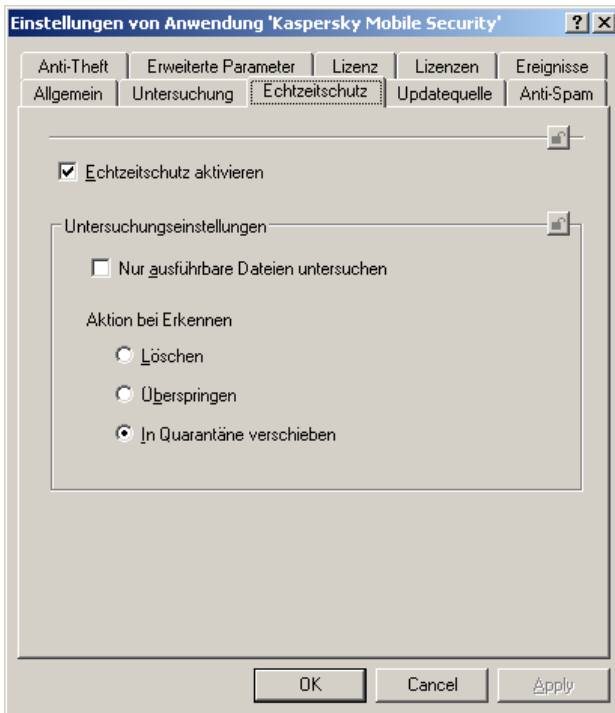
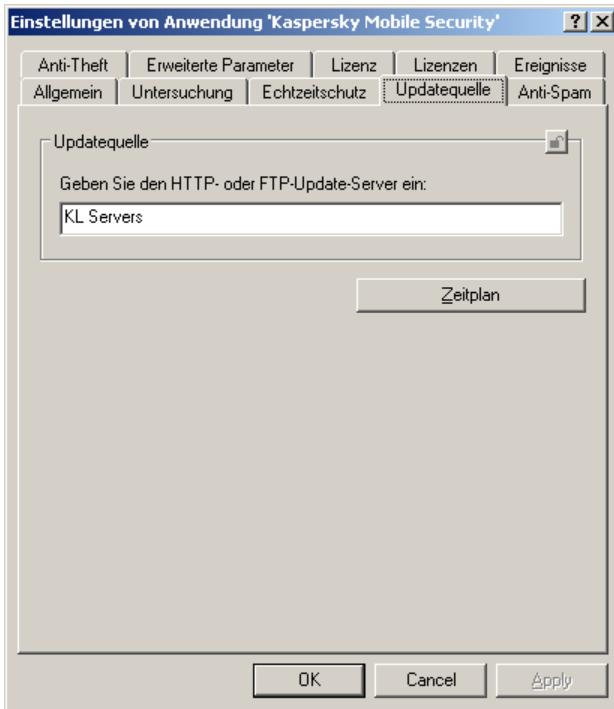


Abbildung 36. Registerkarte **Echtzeitschutz**

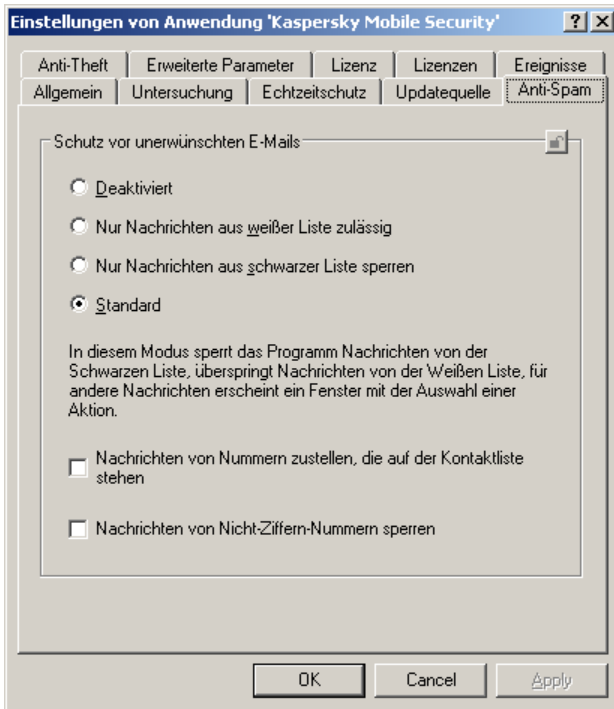
4.4. Informationen über Updatequelle anzeigen

Auf der Registerkarte **Updatequelle** (s. Abb. 37) können Sie Änderungen in den Parametern für den Update-Download zu diesem mobilen Gerät anzeigen lassen und vornehmen.

Abbildung 37. Registerkarte **Updatequelle**

4.5. Informationen über Parameter für Anti-Spam anzeigen

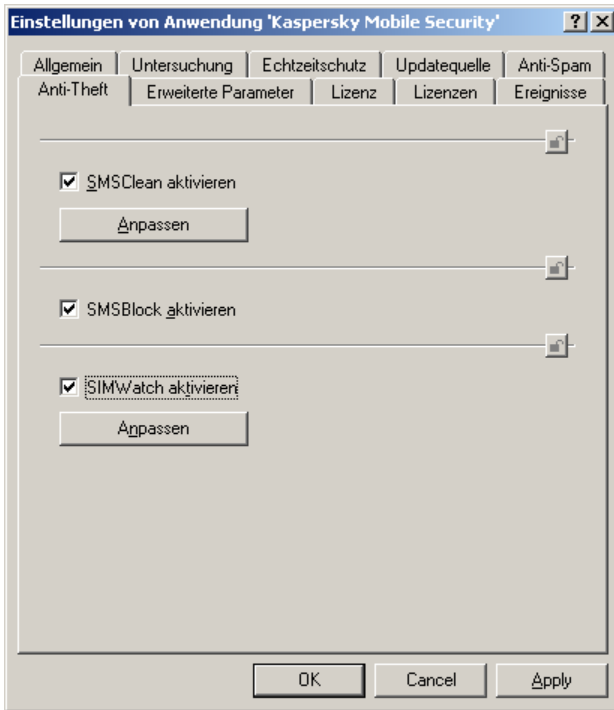
Auf der Registerkarte **Anti-Spam** (s. Abb. 38) können Sie Daten anzeigen lassen und Änderungen in den Parametern für den Schutz des mobilen Gerätes vor unerwünschter Post ändern.

Abbildung 38. Registerkarte **Anti-Spam**

4.6. Informationen über Parameter für Anti-Theft anzeigen

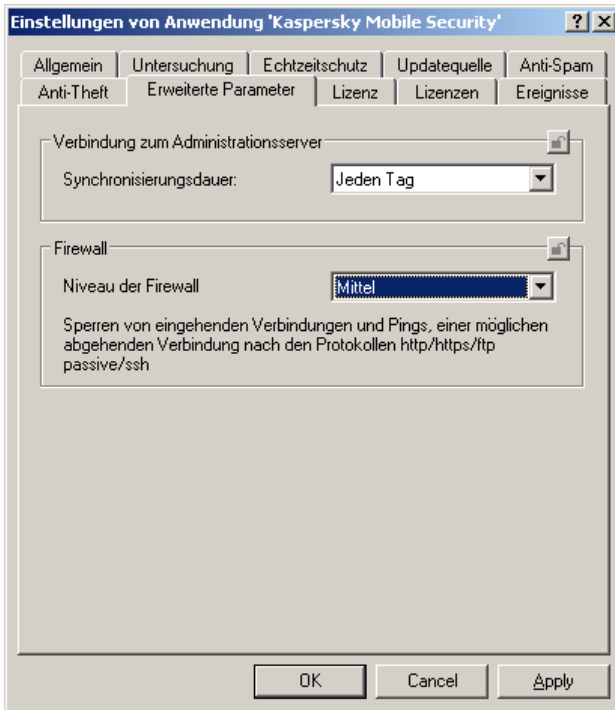
Auf der Registerkarte **Anti-Theft** (s. Abb. 39) können Sie Änderungen in den Parametern für das Anti-Theft-Modul anzeigen lassen und vornehmen: Hier können Sie:

- Modulfunktionen einschalten: SMS-Clean, SMS-Block, SIM-Watch
- Parameter für die Anti-Theft-Funktionen mit den Schaltflächen **Einrichten** in den entsprechenden Abschnitten einrichten.

Abbildung 39. Registerkarte **Anti-Theft**

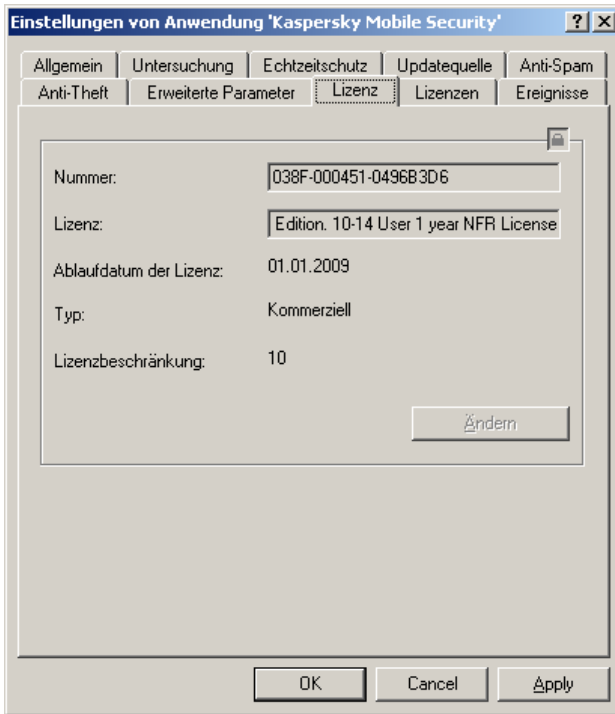
4.7. Informationen über zusätzliche Parameter anzeigen

Auf der Registerkarte **Erweiterte Parameter** (s. Abb. 40) können Sie Daten anzeigen und Änderungen an den Parametern für die Firewall ändern sowie das Intervall für den Verbindungsaufbau mit dem Administrationsserver ändern.

Abbildung 40. Registerkarte **Erweiterte Parameter**

4.8. Informationen über Schlüssel anzeigen

Auf der Registerkarte **Lizenz** (s. Abb. 41) stehen Informationen über den Schlüssel, der auf dem mobilen Gerät installiert ist.

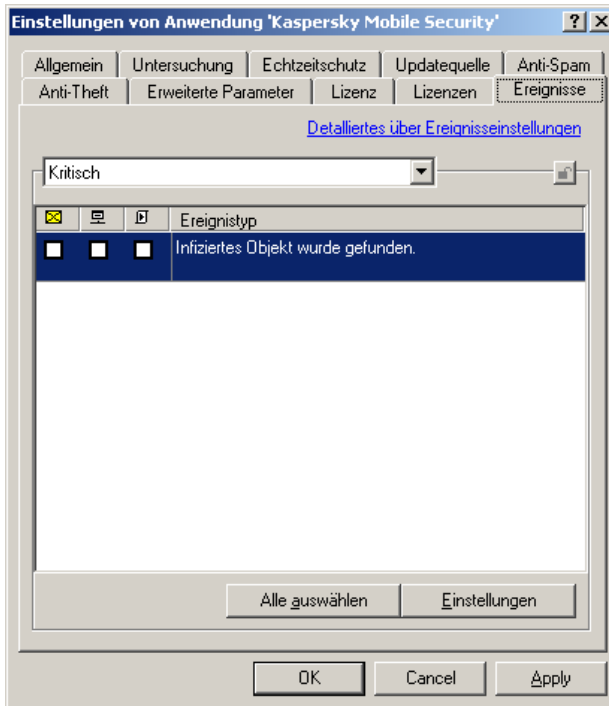
Abbildung 41. Registerkarte **Lizenzen**

4.9. Ereignis-Informationen anzeigen

Kaspersky Mobile Security generiert während des Programmablaufs einen bestimmten Bestand an Ereignissen. Jedes Ereignis hat Merkmale, die dessen Prioritätsstufe darstellen. Es gibt vier Prioritätsstufen: Kritisches Ereignis, Funktionsausfall, Warnung und informative Mitteilung.

Ereignisse des gleichen Typs können verschiedene Prioritätsstufen besitzen, was von der Situation abhängig ist, in der das Ereignis eingetreten ist.

Auf der Registerkarte **Ereignisse** (s. Abb. 42) stehen die Ereignistypen, die im Programmablauf eintreten und im Bericht festgehalten werden, sowie der Speicherort des Berichtes und die Art der Benachrichtigung des Administrators und / oder anderer Benutzer über das eingetretene Ereignis.

Abbildung 42. Registerkarte **Ereignisse**

ANHANG A. KASPERSKY LAB

Kaspersky Lab wurde 1997 gegründet. Die Firma ist heute das bekannteste Unternehmen für Datenschutz-Software in Russland und bietet eine breite Palette an IT-Sicherheitslösungen zum Schutz vor Viren, Spam und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Der Stammsitz befindet sich in Russland. Das Unternehmen unterhält Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Beneluxstaaten, in China, Polen, Rumänien und in den USA. In Frankreich wurde eine neue Filiale gegründet, das Europäische Zentrum für Antivirenforschung. Unser Partnernetzwerk verbindet weltweit mehr als 500 Unternehmen.

Kaspersky Lab – das ist heute mehr als tausend hoch qualifizierte Fachleute, von denen ein Dutzend MBA-Diplome, sechzehn einen Dokortitel haben. Die führenden Virusanalytiker von Kaspersky Lab gehören zur prestigeträchtigen Computer Anti-virus Researcher's Organization (CARO).

Das größte Kapital des Unternehmens besteht in dem einzigartigen Wissen und in der Erfahrung, die von den Mitarbeitern im Laufe des mehr als vierzehnjährigen kontinuierlichen Kampfes gegen Viren gesammelt wurden. Dank der permanenten Analyse von Virenaktivitäten sind wir in der Lage, Tendenzen in der Malware-Entwicklung zu prognostizieren und unseren Benutzern rechtzeitig zuverlässigen Schutz vor neuen Angriffen zu gewährleisten. Dieser Vorteil manifestiert sich in den Erzeugnissen und Leistungen von Kaspersky Lab. Wir sind unseren Konkurrenten stets einen Schritt voraus und bieten unseren Kunden Schutz von höchster Güte.

Aufgrund der jahrelangen Tätigkeit ist das Unternehmen jetzt ein führender Entwickler im Bereich der Virenschutztechnologien. Kaspersky Lab hat als erstes Unternehmen viele moderne Standards für Antiviren-Software gesetzt. Die Basisprodukt des Unternehmens heißt Kaspersky Anti-Virus®. Es bietet für alle Arten von Objekten zuverlässigen Schutz vor Virenangriffen: Arbeitsstationen, Dateiserver, Mailsysteme, Firewalls und Internet-Gateways, Handhelds. Bequeme Steuerelemente erlauben es dem Benutzer, den Antivirenschutz von Computern und Firmennetzwerken möglichst weitgehend zu automatisieren. Viele von Welt-Entwicklern verwenden in ihrer Software den Kern vom Kaspersky Anti-Virus®. Zu ihnen gehören u.a.: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab kommen in den Genuss eines breiten Spektrums von Zusatzleistungen, die das störungsfreie Funktionieren der Erzeugnisse und die genaue Kompatibilität mit speziellen Business-Vorgaben garantieren. Wir planen, realisieren und begleiten komplexe Antivirenlösungen für Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Rund um die Uhr steht

unseren Benutzern ein technischer Kundendienst in mehreren Sprachen zur Verfügung.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gerne telefonisch oder per E-Mail beraten. Alle Ihre Fragen werden umfassend beantwortet.

Webseite von Kaspersky Lab <http://www.kaspersky.com/de>

Viren-Enzyklopädie: <http://www.viruslist.com/de>

Kontakt: <http://www.kaspersky.de/kontakt>

Technischer Support: <http://support.kaspersky.de>

Feedback zu unseren Benutzerhandbüchern: docfeedback@kaspersky.de

Antiviren-Labor: newvirus@kaspersky.com
(nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de>
(für Fragen an die Virenanalysierer)

Webforum von Kaspersky Lab: <http://forum.kaspersky.com>

ANHANG B. KASPERSKY LAB

ENDNUTZERVERTRAG

WICHTIGER RECHTLICHER HINWEIS AN ALLE NUTZER: LESEN SIE BITTE DEN FOLGENDEN VERTRAG SORGFÄLTIG DURCH, BEVOR SIE DIE SOFTWARE NUTZEN.

DURCH ANKLICKEN DER SCHALTFLÄCHE „ANNEHMEN“ IM LIZENZVERTRAG ODER DURCH DIE EINGABE EINES ENTSPRECHENDEN ZEICHENS BZW. ENTSPRECHENDER ZEICHEN ERKLÄREN SIE SICH DAMIT EINVERSTANDEN, DASS SIE AN DIE BEDINGUNGEN DIESES VERTRAGES GEBUNDEN SIND. **DURCH EINE DERARTIGE HANDLUNG, DIE GLEICHBEDEUTEND IST MIT IHRER UNTERSCHRIFT, ERKLÄREN SIE SICH DAMIT EINVERSTANDEN, AN DIESEN VERTRAG GEBUNDEN ZU SEIN UND PARTEI DES VERTRAGES ZU WERDEN. SIE SIND AUSSERDEM DAMIT EINVERSTANDEN, DASS DIESER VERTRAG WIE JEDER SCHRIFTLICHE, VON IHNEN UNTERZEICHNETE VERTRAG DURCHSETZBAR IST.** FALLS SIE NICHT MIT ALLEN BEDINGUNGEN DIESES VERTRAGES EINVERSTANDEN SIND, BRECHEN SIE BITTE DIE INSTALLATION DER SOFTWARE AB UND INSTALLIEREN SIE DIE SOFTWARE NICHT.

NACH DEM ANKLICKEN DER SCHALTFLÄCHE „ANNEHMEN“ IM LIZENZVERTRAG BZW. NACH DER EINGABE EINES ENTSPRECHENDEN ZEICHENS / ENTSPRECHENDER ZEICHEN SIND SIE BERECHTIGT, DIE SOFTWARE GEMÄSS DEN BEDINGUNGEN DIESES VERTRAGES ZU NUTZEN.

1. **Begriffsbestimmungen**

- 1.1 **Software** bedeutet Software einschließlich aller Updates und zugehöriger Materialien.
- 1.2 **Rechteinhaber** (Inhaber aller ausschließlichen oder sonstigen Rechte an der Software) ist Kaspersky Lab ZAO, ein nach dem Recht der Russischen Föderation errichtetes Unternehmen.
- 1.3 **Computer** bedeutet Hardware wie Personal Computer, Laptops, Workstations, PDAs, Smartphones, Handhelds und andere elektronische Geräte, für die die Software entwickelt wurde und auf denen die Software installiert und/oder verwendet wird.
- 1.4 **Endnutzer (Sie)** sind Personen, die die Software im eigenen Namen installieren bzw. nutzen oder eine Kopie der Software rechtmäßig nutzen. Wurde die Software im Namen einer Organisation, etwa eines

Unternehmens, heruntergeladen oder installiert, bezieht sich „Sie“ außerdem auf die Organisation, für die die Software heruntergeladen oder installiert wurde. Es wird zugesichert, dass diejenige Person, die dem Vertrag zugestimmt hat, von der betreffenden Organisation hierzu bevollmächtigt ist. Der Ausdruck

„*Organisation*“ im Sinne dieses Vertrages umfasst insbesondere Partnerschaften, Gesellschaften mit beschränkter Haftung, Körperschaften, Aktiengesellschaften, Trusts, Joint Ventures, Arbeitnehmerorganisationen, Personengesellschaften oder staatliche Behörden.

- 1.5 **Partner** sind Organisationen oder Personen, denen der Rechteinhaber vertraglich gestattet hat, die Software zu vertreiben.
- 1.6 **Updates** sind Verbesserungen, Überarbeitungen, Korrekturen, Erweiterungen, Reparaturen, Modifizierungen, Reproduktionen, Ergänzungen oder Wartungspakete etc.
- 1.7 **Benutzerhandbuch** bezieht sich auf die Bedienungsanleitung, die Administrator-Anleitung, ein Nachschlagewerk und ähnliche erläuternde oder sonstige Materialien.

2. Lizenzerteilung

- 2.1 Der Rechteinhaber gewährt Ihnen hiermit die nicht ausschließliche Lizenz, die Software auf einer bestimmten Anzahl von Computern zu speichern, zu laden, zu installieren, auszuführen und anzuzeigen (zu „nutzen“), um dadurch Ihren Computer, auf dem die Software installiert wurde, vor den im Benutzerhandbuch beschriebenen Gefahren gemäß den technischen, im Benutzerhandbuch beschriebenen Anforderungen sowie gemäß den Bedingungen dieses Vertrages (der „Lizenz“) zu schützen. Sie nehmen diese Lizenz an.

Testversion. Falls Sie eine Testversion der Software erhalten, heruntergeladen und/oder installiert und damit eine Testlizenz für die Software erworben haben, können Sie sie nur zu Testzwecken sowie, falls nicht anderweitig angegeben, ausschließlich während des Testzeitraums ab dem Zeitpunkt der erstmaligen Installation nutzen. Eine Nutzung der Software zu anderen Zwecken oder über den Testzeitraum hinaus ist streng verboten.

Software für Mehrfachumgebungen; mehrsprachige Software; Dual-Media-Software; Mehrfachexemplare; Pakete. Falls Sie verschiedene Versionen oder verschiedensprachige Ausgaben der Software nutzen, die Software auf mehreren Medien oder sonst mehrere Exemplare der Software bzw. die Software im Paket mit anderer Software erhalten haben, entspricht die zulässige Gesamtzahl der Computer, auf denen

sämtliche Versionen der Software installiert sind, der Anzahl der Lizenzen, die Sie vom Rechteinhaber erworben haben. Dabei gibt Ihnen – vorbehaltlich abweichender Lizenzbestimmungen – jede erworbene Lizenz das Recht, die Software auf der in Ziff. 2.2 und 2.3 festgelegten Anzahl von Computern zu installieren und zu nutzen.

- 2.2 Wurde die Software auf einem Datenträger erworben, sind Sie berechtigt, die Software zum Schutz der auf der Software-Verpackung angegebenen Anzahl von Computern zu nutzen.
- 2.3 Wurde die Software über das Internet bezogen, sind Sie berechtigt, die Software zum Schutz der beim Erwerb der Software festgelegten Anzahl von Computern zu nutzen.
- 2.4 Sie dürfen die Software ausschließlich zu Sicherungszwecken als Ersatz für das rechtmäßig in Ihrem Besitz befindliche Exemplar für den Fall kopieren, dass dieses Exemplar verloren geht bzw. zerstört oder unbrauchbar wird. Für andere Zwecke darf die Sicherungskopie nicht verwendet werden. Sie ist zu zerstören, sobald Sie das Recht zur Nutzung der Software verlieren bzw. wenn Ihre Lizenz abläuft oder aus sonstigen Gründen nach den im Land Ihres Hauptwohnsitzes oder im Land der Softwarenutzung geltenden Gesetzen beendet wird.
- 2.5 Sie können die nicht ausschließliche Lizenz zur Nutzung der Software im Rahmen des Ihnen vom Rechteinhaber gewährten Umfangs auf andere natürliche oder juristische Personen übertragen. Der Erwerber muss anerkennen, dass er an alle Bedingungen dieses Vertrages gebunden ist und Ihnen als Inhaber der vom Rechteinhaber gewährten Lizenz in vollem Umfang nachfolgt. Falls Sie die vom Rechteinhaber gewährten Rechte zur Nutzung der Software in vollem Umfang übertragen, sind Sie verpflichtet, sämtliche Exemplare der Software einschließlich der Sicherungskopie zu zerstören. Als Erwerber einer übertragenen Lizenz müssen Sie sich verpflichten, alle Bedingungen dieses Vertrages einzuhalten. Falls Sie nicht anerkennen, dass Sie an alle Bedingungen dieses Vertrages gebunden sind, dürfen Sie die Software weder installieren noch nutzen. Als Erwerber einer übertragenen Lizenz erkennen Sie außerdem an, dass Sie keine weitergehenden oder besseren Rechte haben als der ursprüngliche Endnutzer, der die Software vom Rechteinhaber erworben hat.
- 2.6 Sobald die Software aktiviert bzw. die Lizenzschlüsseldatei installiert wurde (gilt nicht für eine Testversion der Software), sind Sie berechtigt, während des auf der Software-Verpackung angegebenen Zeitraums (beim Erwerb der Software auf einem Datenträger) bzw. des beim Erwerb festgelegten Zeitraums (falls die Software über das Internet bezogen wurde) die folgenden Leistungen in Anspruch zu nehmen:
 - Aktualisierungen der Software (Updates) über das Internet, sobald der Rechteinhaber sie auf seiner Website oder durch andere Online-Dienste herausgibt. Die von Ihnen bezogenen

- Updates werden Teil der Software. Die Bedingungen dieses Vertrages gelten auch für die Updates;
- Technischer Support über das Internet und technische Support-Hotline per Telefon.

3. Aktivierung und Laufzeit

- 3.1 Wenn Sie Ihren Computer modifizieren oder die darauf installierte Software anderer Anbieter verändern, kann es aufgrund von Vorgaben des Rechteinhabers erforderlich werden, die Aktivierung der Software bzw. die Installierung der Lizenzschlüsseldatei zu wiederholen. Der Rechteinhaber behält sich das Recht vor, die Gültigkeit der Lizenz und/oder die Rechtmäßigkeit einer Kopie der auf Ihrem Computer installierten bzw. genutzten Software mit allen zur Verfügung stehenden Mitteln und Nachweisverfahren zu überprüfen.
- 3.2 Wurde die Software auf einem Datenträger erworben, kann sie nach Ihrer Zustimmung zu diesem Vertrag während des auf der Verpackung angegebenen Zeitraums, beginnend mit dem Zeitpunkt der Vertragsannahme, genutzt werden.
- 3.3 Wurde die Software über das Internet bezogen, kann sie nach Ihrer Zustimmung zu diesem Vertrag während des beim Erwerb festgelegten Zeitraums genutzt werden.
- 3.4 Sie sind berechtigt, ab dem Zeitpunkt der Software-Aktivierung gemäß diesem Vertrag für einen einmaligen Testzeitraum von 30 Tagen eine Testversion der Software gemäß Ziff. 2.1 zu nutzen. Die Testversion berechtigt Sie nicht zum Bezug von Updates sowie zur Inanspruchnahme von technischem Support über das Internet bzw. über die technische Support-Hotline per Telefon.
- 3.5 Ihre Lizenz zur Nutzung der Software ist auf den in Ziff. 3.2 bzw. 3.3 angegebenen Zeitraum begrenzt. Die verbleibende Vertragslaufzeit kann auf die im Benutzerhandbuch beschriebene Weise abgefragt werden.
- 3.6 Haben Sie die Software zur Nutzung auf mehr als einem Computer erworben, beginnt der Zeitraum, auf den Ihre Lizenz zur Nutzung der Software begrenzt ist, am Tag der Aktivierung der Software bzw. der Installation der Lizenzschlüsseldatei auf dem ersten Computer.
- 3.7 Falls Sie eine Bestimmung dieses Vertrages verletzen, ist der Rechteinhaber unbeschadet sonstiger ihm nach Gesetz oder Billigkeit zustehender Rechtsmittel jederzeit berechtigt, diese Lizenz zur Nutzung der Software ohne vorherige Ankündigung fristlos zu kündigen. Eine Rückerstattung des Kaufpreises - ganz oder teilweise - ist in diesem Fall ausgeschlossen.
- 3.8 Bei der Nutzung der Software sowie bei der Verwendung von aus der Nutzung der Software herrührenden Informationen oder Daten verpflichten Sie sich zur Einhaltung aller einschlägigen internationalen,

nationalen, bundesstaatlichen, regionalen und lokalen Vorschriften. Hierzu zählen insbesondere Datenschutz-, Urheberrechts- und Ausführüberwachungsgesetze sowie gegen Obszönität gerichtete Gesetze.

- 3.9 Falls nicht ausdrücklich anderweitig bestimmt, dürfen Sie die Ihnen nach diesem Vertrag gewährten Rechte bzw. die sich hieraus ergebenden Pflichten nicht übertragen oder abtreten.

4. Technischer Support

Den in Ziff. 2.6 dieses Vertrages dargestellten technischen Support können Sie in Anspruch nehmen, wenn das neueste Update der Software installiert ist (gilt nicht für eine Testversion der Software).

Technischer Support: <http://support.kaspersky.com>

5. Einschränkungen

- 5.1 Sie dürfen die Software nicht emulieren, klonen, vermieten, verleihen, verleasen, verkaufen, verändern, dekompileieren oder zurückentwickeln. Ebenso wenig dürfen Sie auf der Software basierende, abgeleitete Werke disassemblieren oder erstellen, es sei denn, Sie sind hierzu durch eine gesetzliche Regelung unabdingbar berechtigt. Sie dürfen auch auf andere Weise keinen Teil der Software auf eine für den Menschen lesbare Form reduzieren oder die lizenzierte Software ganz oder teilweise übertragen bzw. Dritten die Übertragung gestatten, es sei denn, die Möglichkeit dieses Verbots wird durch einschlägige Gesetze ausdrücklich ausgeschlossen. Weder der Binärcode der Software noch der Quellcode darf dazu genutzt werden, den proprietären Programmalgorithmus nachzubilden. Alle nicht durch diesen Vertrag ausdrücklich gewährten Rechte bleiben dem Rechteinhaber und/oder dessen Lieferanten vorbehalten. Eine unbefugte Nutzung der Software hat die unverzügliche, automatische Beendigung des Vertrages und der darin erteilten Lizenz zur Folge. Außerdem müssen Sie mit strafrechtlicher und/oder zivilrechtlicher Verfolgung rechnen.
- 5.2 Sie dürfen die Rechte zur Nutzung der Software nur im Rahmen der in Ziff. 2.5 dieses Vertrages enthaltenen Bestimmungen auf Dritte übertragen.
- 5.3 Sie dürfen weder den Aktivierungscode noch die Lizenzschlüsseldatei an Dritte weitergeben oder Dritten Zugang zum Aktivierungscode und/oder der Lizenzschlüsseldatei gestatten. Diese gelten als vertrauliche Daten des Rechteinhabers. Können Sie den Aktivierungscode und/oder die Lizenzschlüsseldatei gemäß den in Ziff. 2.5 dieses Vertrages enthaltenen Bestimmungen auf Dritte übertragen,

- haben Sie die zum Schutz der Vertraulichkeit des Aktivierungs-codes bzw. der Lizenzschlüssel-datei angemessene Sorgfalt aufzuwenden.
- 5.4 Sie dürfen die Software an Dritte weder vermieten noch verleasen oder verleihen.
- 5.5 Es ist Ihnen nicht gestattet, die Software zur eigenen Erstellung von Daten bzw. von Software zur Entdeckung, Blockierung oder Bearbeitung der im Benutzerhandbuch beschriebenen Gefahren nutzen.
- 5.6 Falls Sie eine Bestimmung dieses Vertrages verletzen, ist der Rechteinhaber befugt, die Schlüssel-datei ohne Anspruch auf Rückerstattung zu blockieren oder Ihre Lizenz zu kündigen.
- 5.7 Wenn Sie die Testversion der Software nutzen, haben Sie keinen Anspruch auf den in Ziff. 4 dieses Vertrages dargestellten technischen Support. Außerdem sind Sie nicht berechtigt, die Lizenz bzw. die Rechte zur Nutzung der Software auf Dritte zu übertragen.

6. Eingeschränkte Gewährleistung und Haftungsausschluss

- 6.1 Der Rechteinhaber steht dafür ein, dass die Software im Wesentlichen gemäß den im Benutzerhandbuch niedergelegten Angaben und Beschreibungen funktioniert. Diese eingeschränkte Gewährleistung gilt allerdings nicht, falls einer der folgenden Fälle vorliegt: (w) Mängel an Ihrem Computer und ähnliche Unregelmäßigkeiten, für die der Rechteinhaber ausdrücklich keine Gewähr übernimmt; (x) Fehlfunktionen, Mängel oder Defekte aufgrund fehlerhafter Anwendung; Missbrauch; Störfälle; Nachlässigkeit; unsachgemäße Installation, Handhabung oder Wartung; Diebstahl; Vandalismus; höhere Gewalt; terroristische Aktionen; Stromausfälle oder Überspannungen; Unfälle; Änderungen, nicht gestattete Modifizierungen oder Instandsetzungen durch andere als den Rechteinhaber; durch Sie vorgenommene Handlungen oder Handlungen Dritter; Umstände, die der Rechteinhaber nicht zu vertreten hat; (y) Mängel, die Sie dem Rechteinhaber nicht so schnell wie möglich nach dem erstmaligen Auftreten angezeigt haben; (z) Inkompatibilitäten, die von auf Ihrem Computer installierten Hardware- und/oder Softwarekomponenten verursacht wurden.
- 6.2 Sie erkennen an, akzeptieren und bestätigen, dass keine Software frei von Fehlern ist. Es wird empfohlen, den Computer mit der für Ihre Zwecke angemessenen Häufigkeit und Zuverlässigkeit zu sichern.
- 6.3 Bei Verletzungen der im Benutzerhandbuch bzw. in diesem Vertrag enthaltenen Bestimmungen gewährt der Rechteinhaber keine Garantie dafür, dass die Software korrekt funktioniert.
- 6.4 Wenn Sie die in Ziff. 2.6 des Vertrages geregelten Updates nicht regelmäßig herunterladen, übernimmt der Rechteinhaber keine Garantie dafür, dass die Software korrekt funktioniert.

- 6.5 Nach Ablauf des in den Ziff. 3.2 bzw. 3.3 dieses Vertrages geregelten Zeitraums sowie nach einer Beendigung der Lizenz zur Nutzung der Software aus anderen Gründen garantiert der Rechteinhaber keinen Schutz vor den im Benutzerhandbuch beschriebenen Gefahren.
- 6.6 DIE SOFTWARE WIRD GELIEFERT WIE BESEHEN. DER RECHTEINHABER GIBT HINSICHTLICH IHRER NUTZUNG ODER FUNKTION KEINE ZUSICHERUNG AB UND LEISTET KEINE GEWÄHR. GARANTIEEN SOWIE ENTSPRECHENDE BEDINGUNGEN, ZUSICHERUNGEN ODER BESTIMMUNGEN WERDEN DURCH DEN RECHTEINHABER UND SEINE PARTNER AUSGESCHLOSSEN BZW. BESCHRÄNKT, SOWEIT DIES GESETZLICH MÖGLICH IST; SIE WERDEN WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND BZW. DURCH GESETZ, GEWOHNHEITSRECHT, (HANDELS-)BRAUCH ODER AUF ANDERE WEISE ABGEGEBEN. DIES GILT INSBESONDERE FÜR DIE BEACHTUNG VON RECHTEN DRITTER, DIE VERKEHRSFÄHIGKEIT, EINE ZUFRIEDENSTELLENDENDE QUALITÄT, DIE INTEGRATIONSFÄHIGKEIT SOWIE DIE VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. NEBEN DER GEFAHR VON MÄNGELN TRAGEN SIE DAS GESAMTE RISIKO IM HINBLICK AUF DIE FUNKTION DER SOFTWARE. AUSSERDEM SIND SIE VERANTWORTLICH FÜR DIE AUSWAHL DER SOFTWARE IM HINBLICK AUF DIE GEEIGNETHEIT ZUR ERREICHUNG IHRER ZWECKE SOWIE FÜR DIE INSTALLATION, DIE NUTZUNG UND DIE AUS DER SOFTWARE ERZIELTEN ERGEBNISSE. UNBESCHADET DER VORANGEGANGENEN BESTIMMUNGEN GIBT DER RECHTEINHABER KEINE ZUSICHERUNG AB UND LEISTET KEINE GEWÄHR DAFÜR, DASS DIE SOFTWARE FEHLER- UND UNTERBRECHUNGSFREI ARBEITET UND SONST FREI VON MÄNGELN IST ODER DASS DIE SOFTWARE IHRE ANFORDERUNGEN GANZ ODER TEILWEISE ERFÜLLT, SEIEN SIE DEM RECHTEINHABER BEKANNTGEGEBEN ODER NICHT.

7. Ausschluss und Beschränkung der Haftung

SOWEIT GESETZLICH ZULÄSSIG, LEISTEN DER RECHTEINHABER UND SEINE PARTNER KEINEN ERSATZ FÜR KONKRETE SCHÄDEN, EVENTUALSCHÄDEN, STRAFSCHADENSERSATZBETRÄGE, MITTELBARE SCHÄDEN ODER FOLGESCHÄDEN ALLER ART (INSBESONDERE FÜR ENTGANGENEN GEWINN SOWIE FÜR DEN VERLUST VERTRAULICHER ODER SONSTIGER DATEN, FÜR GESCHÄFTSUNTERBRECHUNGEN, FÜR DIE VERLETZUNG DER PRIVATSPHÄRE, FÜR DIE VERFÄLSCHUNG, BESCHÄDIGUNG UND DEN VERLUST VON DATEN ODER PROGRAMMEN, FÜR DIE NICHTERFÜLLUNG VON PFLICHTEN WIE ETWA GESETZLICHER VERPFLICHTUNGEN, TREUEPFLICHTEN ODER SORGFALTSPFLICHTEN, FÜR FAHRLÄSSIGKEIT, FÜR WIRTSCHAFTLICHE VERLUSTE SOWIE FÜR

ANDERE MATERIELLE ODER SONSTIGE VERLUSTE ALLER ART), DIE IM ZUSAMMENHANG MIT ODER AUFGRUND EINES DER FOLGENDEN UMSTÄNDE ENTSTEHEN: VERWENDUNG ODER UNMÖGLICHKEIT DER VERWENDUNG DER SOFTWARE, GEWÄHRUNG ODER VERSAGUNG VON SUPPORT- UND SONSTIGEN LEISTUNGEN, BEREITSTELLUNG VON DATEN SOWIE VON SOFTWARE- UND ÄHNLICHEN INHALTEN DURCH DIE SOFTWARE ODER ANLÄSSLICH IHRER NUTZUNG SOWIE SONST IM ZUSAMMENHANG MIT DER DURCHFÜHRUNG DIESES VERTRAGES, VERTRAGSVERLETZUNG ODER UNERLAUBTE HANDLUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT, ARGLIST UND VERSCHULDENSUNABHÄNGIGER HAFTUNG), VERLETZUNG GESETZLICHER PFLICHTEN ODER GEWÄHRLEISTUNGSVERLETZUNG DURCH DEN RECHTEINHABER ODER SEINE PARTNER; UND ZWAR AUCH DANN NICHT, WENN DER RECHTEINHABER ODER SEINE PARTNER AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDEN.

SIE ERKLÄREN SICH DAMIT EINVERSTANDEN, DASS BEI ANSPRÜCHEN GEGEN DEN RECHTEINHABER UND/ODER SEINE PARTNER DIE HAFTUNG DES RECHTEINHABERS UND/ODER SEINER PARTNER AUF DEN BETRAG DER FÜR DIE SOFTWARE AUFGEWANDTEN KOSTEN BEGRENZT IST. IN KEINEM FALL ÜBERSTEIGT DIE HAFTUNG DES RECHTEINHABERS UND/ODER SEINER PARTNER DIE FÜR DIE SOFTWARE AN DEN RECHTEINHABER BZW. AN SEINE PARTNER GEZAHLTEN GEBÜHREN.

ANSPRÜCHE AUFGRUND DER TÖTUNG ODER VERLETZUNG EINER PERSON WERDEN DURCH DIESEN VERTRAG WEDER AUSGESCHLOSSEN NOCH EINGESCHRÄNKT. IST EIN AUSSCHLUSS ODER EINE BESCHRÄNKUNG DER HAFTUNG DURCH DIESEN VERTRAG NACH DEN JEWEILS GELTENDEN GESETZEN IM EINZELFALL NICHT ZULÄSSIG, GILT DER AUSSCHLUSS ODER DIE BESCHRÄNKUNG DER HAFTUNG NUR FÜR DIESEN FALL NICHT. DIE ÜBRIGEN HAFTUNGSAUSSCHLÜSSE UND - BESCHRÄNKUNGEN GELTEN WEITERHIN.

8. GNU und sonstige Lizenzen Dritter

Die Software kann Software-Programme enthalten, für die der Nutzer eine (Unter-) Lizenz gemäß der GNU General Public License (GPL) bzw. ähnliche kostenlose Software-Lizenzen erhalten hat, die den Nutzer unter anderem dazu berechtigen, bestimmte Programme oder Teile davon zu kopieren, zu ändern und weiterzugeben und die den Zugang zum Quellcode gestatten („Open Source Software“). Sofern diese Lizenzen erfordern, dass der Quellcode für eine in einem ausführbaren, binären Format weitergegebene Software dem Nutzer ebenfalls zugänglich gemacht wird, wird der Quellcode nach einer entsprechenden Anforderung an source@kaspersky.com zur Verfügung gestellt bzw. mit der Software geliefert. Erfordern Lizenzen für Open Source Software,

dass der Rechteinhaber Rechte zur Nutzung, zum Kopieren oder zur Änderung eines Open Source Software-Programms gewährt, die weiter gehen als die in diesem Vertrag gewährten Rechte, haben jene Rechte Vorrang vor den in diesem Vertrag enthaltenen Rechten und Beschränkungen.

9. Geistiges Eigentum

- 9.1 Sie erkennen an, dass die Software, die Urheberschaft, Systeme, Ideen, Handhabungsmethoden, Dokumentationen und sonstige in der Software enthaltene Daten geistiges Eigentum und/oder wertvolle Geschäftsgeheimnisse des Rechteinhabers oder seiner Partner sind und der Rechteinhaber bzw. seine Partner durch Zivil- und Strafgesetze sowie durch internationale Verträge ebenso geschützt werden wie durch die Gesetze der Russischen Föderation, der Europäischen Union, der Vereinigten Staaten und anderer Länder über Urheberrechte, Geschäftsgeheimnisse, Warenzeichen und Patente. Dieser Vertrag verleiht Ihnen keine Rechte an geistigem Eigentum einschließlich der Waren- und Dienstleistungszeichen des Rechteinhabers und/oder seiner Partner („Warenzeichen“). Sie dürfen die Warenzeichen nur zur Kennzeichnung von durch die Software erstellten Ausdrucken gemäß anerkannter Warenzeichenpraxis nutzen. Hierzu zählt auch die Kennzeichnung mit dem Namen des Warenzeicheninhabers. Die derartige Nutzung eines Warenzeichens gewährt Ihnen kein Eigentumsrecht an diesem Warenzeichen. Der Rechteinhaber und/oder seine Partner besitzen und behalten alle Rechte, Ansprüche und Anteile an der Software, insbesondere in Bezug auf Fehlerbehebung, Verbesserungen, Updates und sonstige Änderungen der Software durch den Rechteinhaber oder Dritte sowie sämtliche Urheberrechte, Patente, Geschäftsgeheimnisse, Warenzeichen und sonstige geistigen Eigentumsrechte nach diesem Vertrag. Durch Besitz, Installierung und Nutzung der Software haben Sie keinen Anspruch auf das geistige Eigentum an der Software. Sie erwerben nur die in diesem Vertrag ausdrücklich festgelegten Rechte an der Software. Alle gemäß diesem Vertrag gefertigten Kopien der Software müssen Eigentumsangaben enthalten, die den auf und in der Software erkennbaren Angaben entsprechen. Dieser Vertrag gewährt Ihnen keine anderen als die vertraglich genannten geistigen Eigentumsrechte an der Software. Sie erkennen an, dass Ihnen die vertraglich erteilte Lizenz, wie unten näher erläutert, lediglich ein begrenztes Nutzungsrecht gemäß den Bedingungen dieses Vertrages verleiht. Rechte, die Ihnen nicht ausdrücklich durch diesen Vertrag verliehen werden, behält sich der Rechteinhaber vor.
- 9.2 Sie erkennen an, dass der Quellcode, der Aktivierungscode und/oder die Lizenzschlüsseldatei Eigentum des Rechteinhabers sind und Geschäftsgeheimnisse des Rechteinhabers darstellen. Sie verpflichten

sich, den Quellcode der Software keinesfalls zu verändern, anzupassen, zurückzuentwickeln, zu dekompileieren, zu disassemblieren oder auf sonstige Weise seine Entschlüsselung zu versuchen.

- 9.3 Sie verpflichten sich, die Software selbst in keiner Weise zu modifizieren oder zu ändern. Auf Kopien der Software angebrachte Urheberrechts- und sonstige Eigentumsangaben dürfen Sie nicht entfernen oder verändern.

10. Anwendbares Recht; Schiedsgerichtsbarkeit

Der vorliegende Vertrag unterliegt dem Recht der Russischen Föderation und ist nach diesem Recht auszulegen. Das Kollisionsrecht bleibt unberücksichtigt. Der Vertrag unterliegt nicht dem Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf, dessen Geltung ausdrücklich ausgeschlossen wird. Für die Entscheidung von aus der Auslegung bzw. Anwendung von Bestimmungen dieses Vertrages oder deren Verletzung entstehenden Streitigkeiten, die nicht durch direkte Verhandlungen beigelegt werden können, ist das Gericht der internationalen Handelsschiedsgerichtsbarkeit bei der Industrie- und Handelskammer der Russischen Föderation (Tribunal of International Commercial Arbitration at the Russian Federation Chamber of Commerce and Industry) in Moskau zuständig. Ein Schiedsspruch des Schiedsgerichts ist endgültig und für die Parteien bindend. Das Schiedsgerichtsurteil kann vor dem zuständigen Gericht durchgesetzt werden. Unbeschadet der Vorschriften dieses Abschnitts ist es jeder Partei gestattet, bei einem zuständigen Gericht vor, während oder nach dem Schiedsverfahren einen Rechtsbehelf aus Billigkeitsgründen einzulegen.

11. Frist für gerichtliche Geltendmachung

Ansprüche, die sich aus der Durchführung dieses Vertrages ergeben, sind spätestens ein (1) Jahr nach ihrer Entstehung bzw. Feststellung gerichtlich geltend zu machen. Für Klagen wegen einer Verletzung geistigen Eigentums gilt jedoch die gesetzliche Höchstfrist.

12. Vollständigkeit der Vereinbarung; salvatorische Klausel; Abdingbarkeit

Dieser Vertrag stellt die gesamte Vereinbarung zwischen Ihnen und dem Rechteinhaber dar. Er ersetzt alle früheren mündlichen oder schriftlichen Vereinbarungen, Angebote, Mitteilungen oder Anzeigen in Bezug auf die Software bzw. den Vertragsgegenstand.

Sie erklären, dass Sie den Vertrag gelesen haben, ihn verstehen und sich an seine Bestimmungen gebunden halten. Falls ein zuständiges Gericht eine

Bestimmung dieses Vertrages aus irgendeinem Grund ganz oder teilweise für ungültig, nichtig oder nicht durchsetzbar erachtet, ist der betreffenden Bestimmung durch engere Auslegung zu Rechtsgültigkeit und Durchsetzbarkeit zu verhelfen. Der Vertrag insgesamt wird hierdurch nicht gefährdet; vielmehr bleibt der Rest des Vertrages in vollem Umfang wirksam, soweit nach Gesetz oder Billigkeit zulässig. Der ursprüngliche Vertragszweck ist so weit wie möglich beizubehalten. Eine Bestimmung bzw. Klausel dieses Vertrages kann nur in schriftlicher Form durch ein von Ihnen und einem bevollmächtigten Vertreter des Rechteinhabers unterzeichnetes Dokument abbedungen werden. Sieht eine Partei davon ab, sich auf die Verletzung einer Bestimmung dieses Vertrags zu berufen, stellt dies keinen Verzicht auf die Geltendmachung früherer, gleichzeitiger oder späterer Vertragsverletzungen dar. Unterlässt es der Rechteinhaber, auf der strikten Durchführung einer Bestimmung dieses Vertrages oder auf der Durchsetzung eines Rechts zu bestehen, so gilt dies nicht als Verzicht auf die Geltendmachung der Bestimmung bzw. des Rechts.

13. Kontaktdaten

Haben Sie Fragen zu diesem Vertrag oder möchten Sie mit dem Rechteinhaber aus anderen Gründen in Kontakt treten, wenden Sie sich bitte an unsere Kundendienstabteilung:

Kaspersky Lab ZAO, 1 Volokolamsky Proezd, d. 10, str. 1
Moskau, 123060
Russische Föderation
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
E-Mail: info@kaspersky.com
Website: www.kaspersky.com

© 1997-2009 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Die Software ist mit der gesamten Begleitdokumentation durch Urheberrechtsgesetze und internationale Urheberrechtsverträge sowie andere Gesetze und Verträge zum Schutz geistigen Eigentums urheberrechtlich geschützt.