

# Kaspersky Endpoint Security 8 für Smartphones

*für BlackBerry® OS*

The Kaspersky logo is displayed in a large, bold, teal font, slanted upwards from left to right. The word "KASPERSKY" is in teal, and the "lab" part is in red. The letters are stylized with small red triangles pointing downwards from the top of the 'A', 'P', and 'Y'.

Benutzerhandbuch

PROGRAMMVERSION: 8.0

Sehr geehrte Benutzerinnen und Benutzer!

Vielen Dank, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass Ihnen diese Dokumentation bei der Arbeit behilflich sein und auf die mit dem Produkt verbundenen Fragen antworten wird.

Achtung! Die Rechte für dieses Dokument liegen bei Kaspersky Lab ZAO (im Weiteren auch "Kaspersky Lab") und sind durch das Urheberrecht der Russischen Föderation und durch internationale Verträge geschützt. Illegale Vervielfältigung und Verbreitung des Dokuments und seiner Teile werden nach dem jeweils gültigen Zivilrecht, Verwaltungsrecht oder Strafrecht verfolgt.

Die Materialien dürfen nur mit schriftlicher Einwilligung von Kaspersky Lab auf elektronische, mechanische oder sonstige Weise kopiert, verbreitet oder übersetzt werden.

Das Dokument und die darin enthaltenen Bilder sind ausschließlich für informative, nicht gewerbliche und persönliche Zwecke bestimmt.

Das Dokument kann zukünftig ohne besondere Ankündigung geändert werden. Die aktuelle Version des Dokuments steht auf der Website von Kaspersky Lab unter der Adresse <http://www.kaspersky.com/de/docs> zur Verfügung.

Kaspersky Lab übernimmt keine Haftung für Inhalt, Qualität, Aktualität und Richtigkeit von in diesem Dokument verwendeten Materialien, deren Rechte bei anderen Eigentümern liegen, sowie für möglichen Schaden, der mit der Verwendung dieser Materialien verbunden ist.

Redaktionsdatum: 09.02.12

© 2012 Kaspersky Lab ZAO.

<http://www.kaspersky.de>  
<http://support.kaspersky.de>

# INHALT

ÜBER DIESES HANDBUCH.....	5
ZUSÄTZLICHE INFORMATIONSMQUELLEN.....	6
Informationsquellen zur selbständigen Recherche .....	6
Diskussion über die Programme von Kaspersky Lab im Webforum .....	7
Kontakt zur Abteilung für Handbücher und Hilfesysteme .....	7
KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES.....	8
HARD- UND SOFTWAREVORAUSSETZUNGEN.....	9
KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES INSTALLIEREN.....	10
Über die Programminstallation über eine Workstation.....	10
Programminstallation über eine Workstation .....	11
Über die Programminstallation nach dem Empfang einer E-Mail-Nachricht .....	13
Programminstallation nach dem Empfang einer E-Mail-Nachricht.....	13
PROGRAMMEINSTELLUNGEN VERWALTEN.....	15
PROGRAMM DEINSTALLIEREN .....	16
LIZENZVERWALTUNG.....	17
Über Lizenzen für Kaspersky Endpoint Security 8 für Smartphones .....	17
Lizenz installieren .....	18
Lizenz-Info anzeigen .....	18
SYNCHRONISIERUNG DES GERÄTS MIT DEM REMOTE-MANAGEMENT-SYSTEM .....	19
Synchronisierung manuell starten .....	19
Synchronisierungseinstellungen ändern.....	20
ERSTE SCHRITTE .....	21
Programm starten.....	21
Geheimcode festlegen.....	21
Programm-Infos anzeigen .....	22
PROGRAMMOBERFLÄCHE .....	23
Registerkarten des Programms .....	23
Fenster für den Schutzstatus.....	24
EINGEHENDE ANRUFEN UND SMS FILTERN .....	25
Über den Anruf- und SMS-Filter .....	25
Über die Modi für den Anruf- und SMS-Filter.....	26
Modus des Anruf- und SMS-Filters ändern.....	26
Schwarze Liste anlegen.....	27
Eintrag zur Schwarzen Liste hinzufügen .....	27
Eintrag der Schwarzen Liste ändern .....	28
Eintrag aus Schwarzer Liste löschen .....	29
Weiße Liste anlegen.....	29
Eintrag zur Weißen Liste hinzufügen .....	30
Eintrag der Weißen Liste ändern .....	31
Eintrag aus Weißer Liste löschen .....	31
Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen.....	32
Reaktion auf SMS von Nicht-Ziffern-Nummern.....	33
Aktion für eingehende SMS wählen.....	34
Aktion für eingehende Anrufe wählen .....	35
DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS .....	36
Über den Diebstahlschutz.....	36
Gerät blockieren .....	37
Persönliche Daten löschen.....	38
Liste der zu löschenden Ordner erstellen .....	40

Wechsel der SIM-Karte auf dem Gerät überwachen .....41  
Geografische Koordinaten des Geräts ermitteln .....43  
Diebstahlschutz-Funktionen ferngesteuert starten .....45  
PROGRAMMBERICHTE .....46  
    Berichte .....46  
    Berichtseinträge anzeigen .....46  
    Einträge aus Bericht löschen .....46  
ANPASSEN VON ERWEITERTEN EINSTELLUNGEN .....47  
    Geheimcode ändern .....47  
    Tooltips anzeigen .....47  
GLOSSAR .....48  
KASPERSKY LAB ZAO .....50  
INFORMATIONEN ZUM PROGRAMMCODE VON DRITTHHERSTELLERN .....51  
MARKENHINWEIS .....52  
SACHREGISTER .....53

# ÜBER DIESES HANDBUCH

Dieses Handbuch informiert über Installation, Konfiguration und Verwendung des Programms Kaspersky Endpoint Security 8 für Smartphones. Das Dokument ist für gewöhnliche Anwender gedacht.

Das Dokument soll:

- dem Anwender helfen, das Programm selbst auf einem mobilen Gerät zu installieren, es zu aktivieren und unter Berücksichtigung individueller Aufgaben optimal anzupassen.
- Fragen, die sich auf das Programm beziehen, schnell beantworten.
- auf alternative Informationsquellen über das Programm und auf Möglichkeiten des technischen Supports hinweisen.

# ZUSÄTZLICHE INFORMATIONSENQUELLEN

Zu Fragen über Installation oder Verwendung von Kaspersky Endpoint Security 8 für Smartphones stehen unterschiedliche Informationsquellen zur Verfügung. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

## IN DIESEM ABSCHNITT

---

Informationsquellen zur selbständigen Recherche.....	<a href="#">6</a>
Diskussion über die Programme von Kaspersky Lab im Webforum.....	<a href="#">7</a>
Kontakt zur Abteilung für Handbücher und Hilfesysteme .....	<a href="#">7</a>

## INFORMATIONSENQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Seite über das Programm auf der Website von Kaspersky Lab
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank)
- elektronisches Hilfesystem
- Dokumentationen

### Seite auf der Website von Kaspersky Lab

<http://www.kaspersky.com/de/endpoint-security-smartphone>

Auf dieser Seite finden Sie allgemeine Informationen über Kaspersky Endpoint Security 8 für Smartphones, seine Funktionen und Besonderheiten.

### Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

<http://support.kaspersky.com/de/kes8m>

Auf dieser Seite finden Sie Artikel, die von Spezialisten des Technischen Supports veröffentlicht wurden.

Diese Artikel bieten nützliche Informationen, Tipps und Antworten auf häufige Fragen zu Kauf, Installation und Verwendung von Kaspersky Endpoint Security 8 für Smartphones. Sie sind nach Themen wie "Arbeit mit Schlüsseldateien", "Datenbank-Update" oder "Beheben von Störungen bei der Arbeit" angeordnet. Die Artikel können außerdem Fragen behandeln, die nicht nur Kaspersky Endpoint Security 8 für Smartphones, sondern auch andere Produkte von Kaspersky Lab betreffen. Außerdem können sie Neuigkeiten über den Technischen Support enthalten.

### Elektronisches Hilfesystem

Bei Fragen zu einem speziellen Fenster oder zu einer Registerkarte von Kaspersky Endpoint Security 8 für Smartphones hilft Ihnen die Kontexthilfe.

Um die Kontexthilfe zu öffnen, öffnen Sie das entsprechende Programmfenster und klicken Sie auf **Hilfe** oder wählen Sie **Menü** → **Hilfe**.

### Dokumentation

Zum Lieferumfang von Kaspersky Endpoint Security 8 für Smartphones gehört das Dokument **Benutzerhandbuch** (im PDF-Format). Dieses Dokument beschreibt Installation und Deinstallation des Programms, Konfiguration der Programmeinstellungen, erste Schritte bei der Arbeit mit dem Programm und Konfiguration der Programmkomponenten. Das Handbuch bietet eine Beschreibung der Programmoberfläche und Lösungswege für typische Aufgaben, die sich dem Anwender bei der Arbeit mit dem Programm stellen.

## **DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM**

Wenn Ihre Frage nicht dringend ist, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse <http://forum.kaspersky.com> diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben, neue Themen eröffnen und die Hilfefunktion verwenden.

## **KONTAKT ZUR ABTEILUNG FÜR HANDBÜCHER UND HILFESYSTEME**

Wenn Sie Fragen zu dieser Dokumentation haben, einen Fehler darin gefunden haben oder Ihre Meinung über unsere Dokumentationen schreiben möchten, richten Sie sich bitte direkt an unsere Abteilung für Handbücher und Hilfesysteme. Die Abteilung für Handbücher und Hilfesysteme erreichen Sie unter der Adresse [docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com). Geben Sie folgenden Betreff an: "Kaspersky Help Feedback: Kaspersky Endpoint Security 8 for Smartphone".

# KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES

Kaspersky Endpoint Security 8 für Smartphones schützt mobile Geräte, die mit dem Betriebssystem BlackBerry® OS arbeiten. Das Programm erlaubt es, eingehende SMS und Anrufe zu überwachen, und die Informationen auf dem Gerät bei Diebstahl oder Verlust zu schützen. Jeder Bedrohungstyp wird von bestimmten Programmkomponenten verarbeitet. Dadurch wird erlaubt, die Programmeinstellungen flexibel an die Erfordernisse eines konkreten Benutzers anzupassen. Programminstallation, Konfiguration und Update werden vom Administrator mit Hilfe von Remote-Management-Systemen ausgeführt.

Kaspersky Endpoint Security 8 für Smartphones umfasst folgende Schutzkomponenten:

- **Anruf- und SMS-Filter.** Prüft alle eingehenden SMS und Anrufe auf Spam. Diese Komponente erlaubt es, das Blockieren von SMS und Anrufe, die als unerwünscht gelten, flexibel anzupassen.
- **Diebstahlschutz.** Schützt die Informationen auf dem Gerät vor unbefugtem Zugriff, wenn es verloren geht oder gestohlen wird, und hilft bei der Suche nach dem Gerät. Außerdem kann der Diebstahlschutz Ihr Gerät durch einen SMS-Befehl von einem anderen Gerät aus ferngesteuert blockieren, auf dem Gerät gespeicherte Daten löschen und das Gerät orten (falls Ihr Gerät einen GPS-Empfänger besitzt). Außerdem kann der Diebstahlschutz das Gerät blockieren, falls die SIM-Karte gewechselt oder das Gerät ohne SIM-Karte eingeschaltet wird.

Das Programm verfügt außerdem über eine Reihe von Servicefunktionen. Sie erlauben es, die Einsatzmöglichkeiten des Programms zu erweitern und den Benutzer bei der Arbeit zu unterstützen.

- **Schutzstatus.** Auf dem Display werden die Status der Programmkomponenten angezeigt. Auf Basis der angezeigten Informationen können Sie den aktuellen Schutzstatus für die Informationen auf Ihrem Gerät einschätzen.
- **Ereignisbericht.** Das Programm führt für jede Komponente einen separaten Ereignisbericht, der die Arbeit der Komponente dokumentiert (z.B. ferngesteuerter Start der Diebstahlschutz-Funktionen, Benachrichtigungen über die Gültigkeitsdauer der Programmlizenz). Die Berichte über die Arbeit der Komponenten werden an das Remote-Management-System weitergeleitet und dort gespeichert.
- **Programm deinstallieren.** Um einen Zugriff auf geschützte Informationen zu verhindern, ist die Deinstallation von Kaspersky Endpoint Security 8 für Smartphones nur über die Programmoberfläche möglich.

Kaspersky Endpoint Security 8 für Smartphones führt keine Datensicherung und anschließende Wiederherstellung aus.

# **HARD- UND SOFTWAREVORAUSSETZUNGEN**

Kaspersky Endpoint Security 8 für Smartphones kann auf mobilen Geräten installiert werden, die mit den Betriebssystemen BlackBerry 4.5, 4.6, 4.7, 5.0 und 6.0 arbeiten.

# KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES INSTALLIEREN

Für die Installation von Kaspersky Endpoint Security 8 für Smartphones verwendet der Administrator Remote-Management-Tools. Die Programminstallation erfordert eine Mitwirkung des Benutzers.

Die Programminstallation folgt einem der folgenden Schemata:

- Auf Ihrer Workstation wird das gleichnamige Installationstool für Kaspersky Endpoint Security 8 für Smartphones installiert. Mit diesem Tool können Sie Kaspersky Endpoint Security 8 für Smartphones auf Ihrem mobilen Gerät installieren.
- Sie erhalten per E-Mail eine Nachricht von Ihrem Administrator, die eine Programmdistribution oder einen Link für deren Download enthält. Mithilfe dieser Informationen installieren Sie Kaspersky Endpoint Security 8 für Smartphones auf dem mobilen Gerät.

Dieser Abschnitt erläutert die erforderlichen Vorbereitungen für die Installation von Kaspersky Endpoint Security 8 für Smartphones. Außerdem werden Varianten für die Programminstallation auf einem mobilen Gerät beschrieben.

## IN DIESEM ABSCHNITT

Über die Programminstallation über eine Workstation .....	<a href="#">10</a>
Programminstallation über eine Workstation.....	<a href="#">10</a>
Über die Programminstallation nach dem Empfang einer E-Mail-Nachricht.....	<a href="#">12</a>
Programminstallation nach dem Empfang einer E-Mail-Nachricht .....	<a href="#">13</a>

## ÜBER DIE PROGRAMMINSTALLATION ÜBER EINE WORKSTATION

Wenn der Administrator das Übertragungstool für Kaspersky Endpoint Security 8 für Smartphones auf Ihrer Workstation installiert hat, können Sie Kaspersky Endpoint Security 8 für Smartphones auf den mobilen Geräten installieren, die an diesen Computer angeschlossen werden. Das Übertragungstool für Kaspersky Endpoint Security 8 für Smartphones enthält eine Programmdistribution und sendet diese an das mobile Gerät. Das Tool wird nach der Installation auf einer Workstations automatisch gestartet und überwacht die Verbindung von mobilen Geräten mit dem Computer. Jedes Mal, wenn ein mobiles Gerät mit der Workstation verbunden wird, prüft das Tool, ob das Gerät die Systemvoraussetzungen für Kaspersky Endpoint Security 8 für Smartphones erfüllt, und bietet an, das Programm darauf zu installieren.

Eine Installation ist nur möglich, wenn das Programm BlackBerry Desktop Manager auf der Workstation installiert ist.

## PROGRAMMINSTALLATION ÜBER EINE WORKSTATION

Wenn das Übertragungstool für Kaspersky Endpoint Security 8 für Smartphones auf Ihrer Workstation installiert ist, wird Ihnen bei jeder Verbindung mit mobilen Geräten, die die Systemanforderungen erfüllen, vorgeschlagen, Kaspersky Endpoint Security 8 für Smartphones darauf zu installieren.

Sie können verbieten, dass Kaspersky Endpoint Security 8 für Smartphones bei künftigen Verbindungen von Geräten mit dem Computer installiert wird.

➤ *Gehen Sie folgendermaßen vor, um das Programm über eine Workstation auf einem mobilen Gerät zu installieren:*

1. Verwenden Sie BlackBerry Desktop Manager, um das mobile Gerät mit der Workstation zu verbinden.

Erfüllt das Gerät die Systemanforderungen für die Installation der Anwendung, so öffnet das Fenster **KES 8** mit Informationen über das Tool (s. Abb. unten).

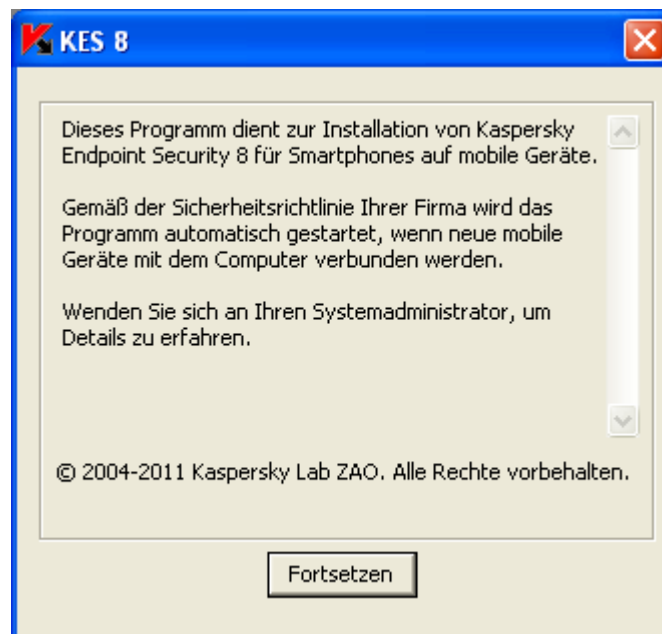


Abbildung 1: Installationsprogramm für Kaspersky Endpoint Security 8 für Smartphones

2. Klicken Sie auf die Schaltfläche **Weiter**.

Es öffnet sich das Fenster **KES 8** mit einer Liste der gefundenen angeschlossenen Geräte.

Wenn mehrere Geräte, die die Systemvoraussetzungen erfüllen, an die Workstation angeschlossen sind, werden diese im folgenden Fenster **KES 8** in einer Liste der gefundenen verbundenen Geräte angezeigt.

3. Wählen Sie ein oder mehrere Geräte aus der Liste der gefundenen verbundenen Geräte aus, auf denen das Programm installiert werden soll. Aktivieren Sie dazu die Kontrollkästchen für die Geräte (s. Abb. unten).



Abbildung 2: Auswahl der Geräte für die Installation von Kaspersky Endpoint Security 8 für Smartphones

4. Klicken Sie auf **Installieren**.

Auf der Workstation wird das Fenster **Assistent für den Programm-Download** geöffnet. Nachdem die Distribution auf die ausgewählten mobilen Geräte kopiert wurde, startet automatisch die Programminstallation. Klicken Sie beim Abschluss der Installation im Fenster **Assistent für den Programm-Download** auf **Schließen**.

Der Status der Übertragung der Programmdistribution auf das Gerät wird auch auf der Workstation im Fenster **KES 8** dargestellt.

Falls bei der Programminstallation Fehler auftreten sollten, wenden Sie sich an den Administrator.

- Um zu verhindern, dass Kaspersky Endpoint Security 8 für Smartphones bei künftigen Verbindungen von Geräten mit dem Computer installiert wird:

aktivieren Sie im Fenster **KES 8** das Kontrollkästchen **Automatischen Start des Installationsprogramms für Kaspersky Endpoint Security 8 für Smartphones deaktivieren**.

## ÜBER DIE PROGRAMMINSTALLATION NACH DEM EMPFANG EINER E-MAIL-NACHRICHT

Sie erhalten per E-Mail eine Nachricht von Ihrem Administrator. Die Nachricht enthält eine Programmdistribution oder einen Link für deren Download.

Die Nachricht enthält folgende Informationen:

- Anhang mit der Programmdistribution oder Link zum Download der Distribution
- Informationen über die Einstellungen für eine Verbindung des Programms mit dem Remote-Management-System

Bewahren Sie diese Nachricht auf, bis die Installation von Kaspersky Endpoint Security 8 für Smartphones auf dem Gerät abgeschlossen wurde.

## PROGRAMMINSTALLATION NACH DEM EMPFANG EINER E-MAIL-NACHRICHT

Wenn Sie eine E-Mail-Nachricht mit den Programmeinstellungen erhalten haben, können Sie das Programm nur vom mobilen Gerät aus installieren. Eine Installation von Kaspersky Endpoint Security 8 für Smartphones über die Workstations wird in diesem Fall nicht unterstützt.

➤ Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security 8 für Smartphones zu installieren:

1. Öffnen Sie auf dem mobilen Gerät die Nachricht des Administrators, die die Einstellungen für die Programminstallation enthält.
2. Führen Sie eine der folgende Aktionen aus:
  - Wenn die Nachricht einen Link enthält, folgen Sie dem Link und laden Sie die Programmdistribution herunter.
  - Wenn die Distribution an die Nachricht angehängt ist, laden Sie die Programmdistribution herunter.  
Die Programminstallation startet automatisch und das Programm wird auf dem Gerät installiert.

3. Öffnen Sie das Programm (s. Abschnitt "Programm starten" auf S. 21). Gehen Sie dazu auf **Menü** → **Download** → **KES 8** und starten Sie das Programm. Verwenden Sie dazu das Trackpad oder gehen Sie auf **Menü** → **Öffnen**.
4. Legen Sie einen Geheimcode für das Programm fest (s. Abschnitt "Geheimcode festlegen" auf S. 21). Füllen Sie dazu die Felder **Neuen Code eingeben** und **Code bestätigen** aus, und betätigen Sie die **EINGABE**-Taste.  
Das Fenster **Synchronisierungseinstellungen** wird geöffnet.

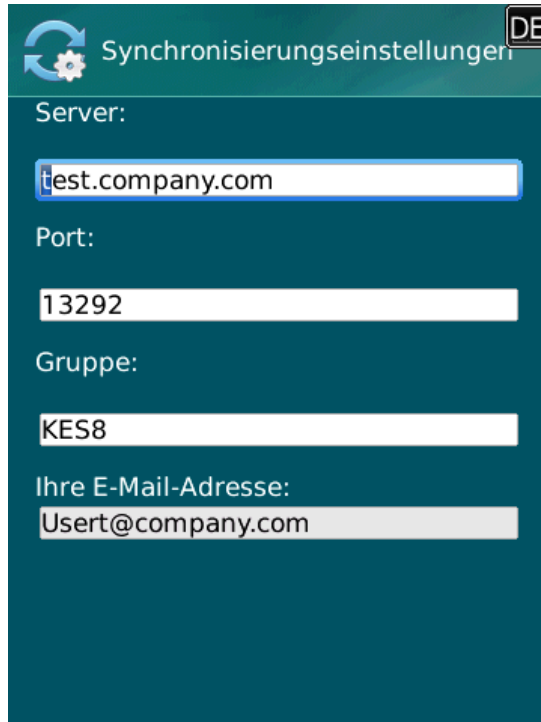


Abbildung 3: Synchronisierungseinstellungen

5. Passen Sie die Einstellungen für eine Verbindung mit dem Remote-Management-System an, wenn die entsprechenden Werte in der Nachricht des Administrators enthalten waren. Legen Sie Werte für folgende Einstellungen fest:
  - **Server**
  - **Port**
  - **Gruppe**

Falls es überflüssig ist, die Einstellungen für eine Verbindung mit dem Remote-Management-System anzupassen, wird dieser Schritt übersprungen.
6. Geben Sie im Feld **Ihre E-Mail-Adresse** Ihre geschäftliche E-Mail-Adresse ein und klicken Sie auf **OK**.  
Diese E-Mail-Adresse wird für die Anmeldung des Geräts im Remote-Management-System verwendet. Beachten Sie, dass die Adresse, die bei der Programminstallation angegeben wurde, nicht geändert werden kann.

Falls bei der Programminstallation Fehler auftreten sollten, wenden Sie sich an den Administrator.

# PROGRAMMEINSTELLUNGEN VERWALTEN

Alle Einstellungen für die Arbeit von Kaspersky Endpoint Security 8 für Smartphones, einschließlich der Lizenz, werden vom Administrator über ein Remote-Management-System angepasst. Dabei kann der Administrator dem Benutzer erlauben oder verbieten, diese Einstellungen zu ändern.

Sie können die Funktionseinstellungen für das Programm auf dem mobilen Gerät ändern, falls der Administrator dies nicht untersagt hat.

Wenn im oberen Bereich des Konfigurationsfensters einer Komponente ein Schlosssymbol und eine Warnmeldung vorhanden sind, können die Programmeinstellungen auf dem mobilen Gerät nicht geändert werden.

Wenn der Administrator die Programmeinstellungen geändert hat, werden sie über das Remote-Management-System an das Gerät übertragen. Dabei werden auf dem Gerät die Werte der Programmeinstellungen geändert, die vom Administrator gesperrt wurden. Einstellungen, die vom Administrator nicht gesperrt wurden, bleiben unverändert und behalten die zuvor eingestellten Werte bei.

Wenn das Gerät keine Programmeinstellungen empfangen hat oder Sie die vom Administrator festgelegten Einstellungen wiederherstellen möchten, verwenden Sie die Funktion zur Synchronisierung des Geräts mit dem Remote-Management-System (s. Abschnitt "Synchronisierung manuell starten" auf S. [19](#)).

# PROGRAMM DEINSTALLIEREN

Das Programm kann nur manuell durch den Benutzer vom Gerät entfernt werden.

➔ Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security 8 für Smartphones manuell zu entfernen:

1. Auf der Registerkarte **Erweitert** wählen Sie den Punkt **Deinstallation des Programms** (s. Abb. unten).



Abbildung 4: Deinstallation des Programms

Ein Fenster zum Bestätigen des Löschens wird geöffnet.

2. Bestätigen Sie die Deinstallation von Kaspersky Endpoint Security 8 für Smartphones mit **Ja**.  
Die Deinstallation des Programms beginnt.
3. Starten Sie das Gerät neu, um die Deinstallation des Programms abzuschließen.

# LIZENZVERWALTUNG

Dieser Abschnitt informiert über die Programmlizenz, die Lizenzaktivierung und die Anzeige von Lizenzinformationen.

## IN DIESEM ABSCHNITT

Über Lizenzen für Kaspersky Endpoint Security 8 für Smartphones.....	<a href="#">17</a>
Lizenz installieren.....	<a href="#">17</a>
Lizenz-Info anzeigen .....	<a href="#">18</a>

## ÜBER LIZENZEN FÜR KASPERSKY ENDPOINT SECURITY 8 FÜR SMARTPHONES

Die *Lizenz* verleiht das Recht zur Nutzung von Kaspersky Endpoint Security 8 für Smartphones und der zum Programm gehörenden Zusatzleistungen, die von Kaspersky Lab und seinen Partnern angeboten werden.

Um das Programm zu nutzen, muss eine Lizenz installiert sein.

Jede Lizenz wird durch Gültigkeitsdauer und Typ charakterisiert.

Die *Gültigkeitsdauer einer Lizenz* ist die Zeitspanne, für die Ihnen der technische Support zur Verfügung steht.

Der Umfang der angebotenen Leistungen ist vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen:

- *Test* – Kostenlose Lizenz mit begrenzter Gültigkeitsdauer (z. B. 30 Tage) zum Kennenlernen von Kaspersky Endpoint Security 8 für Smartphones.

Während der Gültigkeitsdauer der Testlizenz sind alle Programmfunktionen verfügbar. Nach Ablauf der Gültigkeitsdauer einer Testlizenz stellt Kaspersky Endpoint Security 8 für Smartphones alle Funktionen ein. In diesem Fall sind nur folgende Aktionen möglich:

- Hilfesystem für das Programm anzeigen
- Synchronisierung mit dem Remote-Management-System.

- *Kommerziell* – Gekaufte Lizenz, die eine begrenzte Gültigkeitsdauer (z.B. 1 Jahr) besitzt und beim Kauf von Kaspersky Endpoint Security 8 für Smartphones zur Verfügung gestellt wird.

Während der Laufzeit einer kommerziellen Lizenz sind alle Programmfunktionen und zusätzliche Services verfügbar.

Nach Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz kommt es zu einer Einschränkung des Funktionsumfangs von Kaspersky Endpoint Security 8 für Smartphones. In diesem Modus sind folgende Aktionen möglich:

- Komponente Diebstahlschutz deaktivieren
- Hilfesystem für das Programm anzeigen
- Synchronisierung mit dem Remote-Management-System.

## LIZENZ INSTALLIEREN

Die Lizenz wird vom Administrator über das Remote-Management-System installiert.

Ohne Lizenz funktioniert Kaspersky Endpoint Security 8 für Smartphones innerhalb von drei Tagen nach der Programminstallation in vollem Funktionsumfang. Innerhalb dieser Frist installiert der Administrator über das Remote-Management-System eine Lizenz und das Programm wird aktiviert.

Wenn innerhalb von drei Tagen keine Lizenz installiert wurde, wird die Funktionalität des Programms eingeschränkt. In diesem Modus sind folgende Aktionen möglich:

- Alle Komponenten deaktivieren
- Hilfesystem für das Programm anzeigen

Wenn innerhalb von drei Tagen nach der Installation keine Lizenz installiert wurde, verwenden Sie zur Lizenzinstallation die Funktion zur Synchronisierung des Geräts mit dem Remote-Management-System (s. Abschnitt "Synchronisierung manuell starten" auf S. [19](#)).

## LIZENZ-INFO ANZEIGEN

Sie können folgende Informationen zur Lizenz lesen: Nummer und Typ der Lizenz, Aktivierungsdatum, Ablaufdatum, verbleibende Gültigkeitsdauer und PIN des Geräts.

➡ *Gehen Sie folgendermaßen vor, um Informationen zur Lizenz anzuzeigen:*

1. Wählen Sie die Registerkarte **Erweitert** aus.
2. Wählen Sie **Lizenz-Info**.

Das Fenster **Lizenz-Info** wird geöffnet.

# SYNCHRONISIERUNG DES GERÄTS MIT DEM REMOTE-MANAGEMENT-SYSTEM

Bei der Synchronisierung werden die vom Administrator festgelegten Programmeinstellungen auf das Gerät übertragen. Vom Gerät werden Berichte über die Arbeit der Programmkomponenten an das Remote-Management-System übertragen.

Die Synchronisierung des Geräts mit dem Remote-Management-System erfolgt automatisch.

Falls die Synchronisierung nicht automatisch ausgeführt wird, können Sie sie manuell starten.

Eine manuelle Synchronisierung ist erforderlich, wenn innerhalb von drei Tagen nach der Programminstallation keine Lizenz installiert wurde.

Abhängig vom Remote-Management-System, das der Administrator zur Programmverwaltung einsetzt, kann der Benutzer bei der Programminstallation aufgefordert werden, die Einstellungen für eine Verbindung zu dem Remote-Management-System einzugeben. In diesem Fall können die Werte, die der Benutzer manuell festgelegt hat, vom Programm aus geändert werden (s. Abschnitt "Synchronisierungseinstellungen ändern" auf S. [20](#)).

## IN DIESEM ABSCHNITT

Synchronisierung manuell starten .....	<a href="#">19</a>
Synchronisierungseinstellungen ändern.....	<a href="#">20</a>

## SYNCHRONISIERUNG MANUELL STARTEN

➔ Gehen Sie folgendermaßen vor, um das Gerät manuell mit dem Remote-Management-System zu synchronisieren:

1. Wählen Sie die Registerkarte **Erweitert**.
2. Gehen Sie auf **Synchronisierung** (s. Abb. unten).



Abbildung 5: Manuelle Synchronisierung

Wenn der Benutzer bei der Programminstallation nicht aufgefordert wurde, die Einstellungen für eine Verbindung zum Remote-Management-System einzugeben, so öffnet sich ein Fenster zur Bestätigung der Internetverbindung. Erlauben Sie die Verbindung mit **Ja**. Es wird eine Verbindung mit dem Remote-Management-System hergestellt.

Wenn der Benutzer bei der Programminstallation aufgefordert wurde, die Einstellungen für eine Verbindung zum Remote-Management-System einzugeben, dann wird in diesem Fall das Fenster **Synchronisierung** geöffnet. Wählen Sie den Punkt **Synchronisierung starten** aus. Es wird eine Verbindung mit dem Remote-Management-System hergestellt.

## SYNCHRONISIERUNGSEINSTELLUNGEN ÄNDERN

Ändern Sie die Einstellungen für eine Verbindung zu dem Remote-Management-System nur auf Anweisung des Administrators.

➤ Gehen Sie folgendermaßen vor, um die Einstellungen für eine Verbindung mit dem Remote-Management-System zu ändern:

1. Wählen Sie die Registerkarte **Erweitert**.
2. Gehen Sie auf **Synchronisierung**.  
Das Fenster **Synchronisierung** wird geöffnet.
3. Wählen Sie den Punkt **Synchronisierungseinstellungen** aus.
4. Ändern Sie die Werte für folgende Einstellungen (s. Abb. unten):
  - **Server**
  - **Port**
  - **Gruppe**

The screenshot shows a dialog box titled 'Synchronisierungseinstellungen' with a 'DE' language indicator in the top right corner. The dialog contains the following fields:

- Server:** test.company.com
- Port:** 13292
- Gruppe:** KES8
- Ihre E-Mail-Adresse:** User@company.com

Abbildung 6: Synchronisierungseinstellungen ändern

5. Gehen Sie auf **Menü** → **Speichern**.

# ERSTE SCHRITTE

Dieser Abschnitt informiert über die ersten Schritte bei der Arbeit mit Kaspersky Endpoint Security 8 für Smartphones: Geheimcode für das Programm festlegen, Programm starten und Informationen zum Programm anzeigen.

## IN DIESEM ABSCHNITT

Programm starten .....	<a href="#">21</a>
Geheimcode festlegen .....	<a href="#">21</a>
Programm-Infos anzeigen .....	<a href="#">22</a>

## PROGRAMM STARTEN

➔ *Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security 8 für Smartphones zu starten:*

1. Öffnen Sie das Hauptmenü des Geräts.
2. Wählen Sie den Ordner **Download** → **KES 8**.

Der Installationsordner für das Programm kann je nach Modell des mobilen Geräts variieren.

3. Starten Sie das Programm. Verwenden Sie dazu auf das Trackpad oder gehen Sie auf **Menü** → **Öffnen**.
4. Geben Sie den Geheimcode des Programms an (s. Abschnitt "Geheimcode festlegen" auf S. [21](#)) und betätigen Sie die **ENTER**-Taste.

Die Bestätigungsmethode für den angegebenen Geheimcode kann je nach Modell des mobilen Geräts variieren.

Auf dem Bildschirm öffnet sich ein Fenster mit dem Schutzstatus von Kaspersky Endpoint Security 8 für Smartphones (s. Abschnitt "Fenster für den Schutzstatus" auf S. [23](#)).

## GEHEIMCODE FESTLEGEN

Nachdem das Programm gestartet wurde, werden Sie aufgefordert, den Geheimcode des Programms einzugeben. Der *Geheimcode des Programms* verhindert einen unautorisierten Zugriff auf die Programmeinstellungen. Der aktuelle Geheimcode des Programms kann später geändert werden.

Der Geheimcode des Programms wird in folgenden Fällen abgefragt:

- für den Zugriff auf das Programm
- wenn von einem anderen mobilen Gerät aus ein SMS-Befehl gesendet wird, um folgende Funktionen ferngesteuert zu starten: SMS-Block, SMS-Clean, SIM-Watch, GPS-Find, Privatsphäre.

**Merken Sie sich den Geheimcode des Programms, Wenn Sie ihn vergessen, ist es nicht mehr möglich, die Funktionen von Kaspersky Endpoint Security 8 für Smartphones zu verwalten und das Programm zu entfernen.**

Der Geheimcode des Programms besteht aus Ziffern, Er muss aus mindestens vier Zeichen bestehen.

➤ *Gehen Sie folgendermaßen vor, um den Geheimcode festzulegen:*

1. Bestätigen Sie das Erstellen eines Geheimcodes für das Programm. Klicken Sie dazu nach dem ersten Programmstart im Benachrichtigungsfenster auf **OK**.

Ein Fenster für die Eingabe des Geheimcodes für das Programm wird geöffnet.

2. Geben Sie im Feld **Neuen Code eingeben** die Ziffern für Ihren Code ein.
3. Wiederholen Sie die Eingabe im Feld **Code bestätigen**.
4. Drücken Sie die Taste **ENTER**.

Ein eingegebener Code wird automatisch auf seine Sicherheit geprüft.

Wenn der eingegebene Geheimcode sicher ist, öffnet sich das Fenster für den Schutzstatus.

Wenn die Prüfung ergibt, dass ein Code unsicher ist, erfolgt eine Warnung und das Programm erfragt eine Bestätigung. Klicken Sie auf **Ja**, um den aktuellen Code zu verwenden.

Klicken Sie auf **Nein**, um einen neuen Code festzulegen. Die Felder **Neuen Code eingeben** und **Code bestätigen** werden geleert. Geben Sie den Geheimcode für das Programm erneut ein.

## PROGRAMM-INFOS ANZEIGEN

Sie können allgemeine Informationen über das Programm Kaspersky Endpoint Security 8 für Smartphones und seine Version anzeigen.

➤ *Um Informationen über das Programm anzuzeigen,*

auf der Registerkarte **Erweitert** den Punkt **Programm-Infos**.

# PROGRAMMOBERFLÄCHE

Dieser Abschnitt informiert über die wichtigsten Elemente der Benutzeroberfläche von Kaspersky Endpoint Security 8 für Smartphones.

## IN DIESEM ABSCHNITT

---

Registerkarten des Programms.....	<a href="#">23</a>
Fenster für den Schutzstatus .....	<a href="#">23</a>

## REGISTERKARTEN DES PROGRAMMS

Die Programmkomponenten sind logisch angeordnet und stehen auf den Registerkarten des Programms zur Verfügung. Jede Registerkarte bietet Zugriff auf die Einstellungen der gewählten Komponente und ihre Aufgaben.

Kaspersky Endpoint Security 8 für Smartphones besitzt folgende Registerkarten:

- **Schutzstatus** – Status für alle Programmkomponenten anzeigen.
- **Diebstahlschutz** – Schutz für die Informationen auf dem Gerät bei Diebstahl oder Verlust.
- **Anruf- und SMS-Filter** – Filterung von unerwünschten eingehenden Anrufen und SMS.
- **Erweitert** – allgemeine Programmeinstellungen, Start der Synchronisierung des Geräts mit dem Remote-Management-System, Deinstallation des Programms, Informationen zum Programm und zur Lizenz.

Zur Navigation zwischen den Registerkarten dient das Trackpad.

## FENSTER FÜR DEN SCHUTZSTATUS

Der Status der wichtigsten Programmkomponenten wird im Fenster für den Schutzstatus angezeigt (s. Abb. unten).

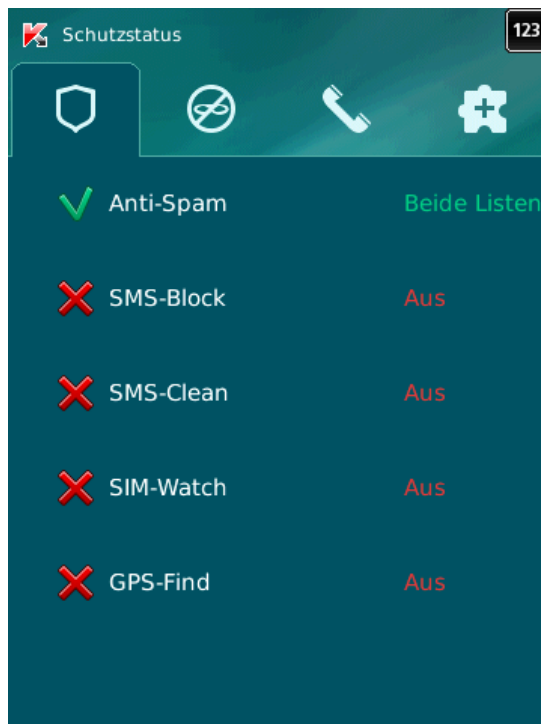


Abbildung 7: Fenster für den Schutzstatus

Das Fenster für den Schutzstatus ist nach dem Programmstart verfügbar und bietet folgende Informationen:

- **Anti-Spam** – Modus für die Filterung von Anrufen und SMS (s. Abschnitt "Eingehende Anrufe und SMS filtern" auf S. [25](#)).
- **SMS-Block**, **SMS-Clean**, **SIM-Watch**, **GPS-Find** – Status der Diebstahlschutz-Funktionen (s. Abschnitt "Datenschutz bei Verlust oder Diebstahl des Geräts" auf S. [36](#)).

Der Status **An** bedeutet, dass die Diebstahlschutz-Funktion aktiviert ist. Der Status **Aus** bedeutet, dass die Diebstahlschutz-Funktion deaktiviert ist.

Das Fenster für den Schutzstatus wird nach dem Programmstart angezeigt. In das Fenster für den Schutzstatus können Sie auch durch Auswahl der Registerkarte **Schutzstatus** wechseln.

# EINGEHENDE ANRUF- UND SMS FILTERN

Dieser Abschnitt informiert über den Anruf- und SMS-Filter. Diese Komponente verhindert die Zustellung von unerwünschten Anrufen und SMS und verwendet dazu eine benutzerdefinierte Schwarze und Weiße Liste. Außerdem wird in diesem Abschnitt beschrieben, wie ein Modus ausgewählt wird, nach dem der Anruf- und SMS-Filter eingehende Anrufe und SMS untersuchen soll, wie erweiterte Einstellungen für die Filterung von eingehenden SMS und Anrufen vorgenommen werden, und wie die Schwarze und Weiße Liste erstellt werden.

## IN DIESEM ABSCHNITT

Über den Anruf- und SMS-Filter .....	<a href="#">25</a>
Über die Modi für den Anruf- und SMS-Filter .....	<a href="#">25</a>
Modus des Anruf- und SMS-Filters ändern .....	<a href="#">26</a>
Schwarze Liste anlegen .....	<a href="#">27</a>
Weißer Liste anlegen .....	<a href="#">29</a>
Reaktion auf SMS-Nachrichten und Anrufe von Kontakten, die nicht im Telefonbuch stehen .....	<a href="#">32</a>
Reaktion auf SMS von Nicht-Ziffern-Nummern .....	<a href="#">32</a>
Aktion für eingehende SMS wählen .....	<a href="#">33</a>
Aktion für eingehende Anrufe wählen .....	<a href="#">34</a>

## ÜBER DEN ANRUF- UND SMS-FILTER

Der Anruf- und SMS-Filter verhindert die Zustellung von unerwünschten Anrufen und SMS und verwendet dazu eine benutzerdefinierte Schwarze und Weiße Liste.

Die Listen bestehen aus Einträgen. Jeder Listeneintrag enthält folgende Informationen:

- Telefonnummer, von der der Anruf- und SMS-Filter für die Schwarze Liste Informationen blockieren und für die Weiße Liste zustellen soll.
- Typ der Ereignisse, die der Anruf- und SMS-Filter für die Schwarze Liste blockieren und für die Weiße Liste erlauben soll. Folgende Informationstypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der der Anruf- und SMS-Filter erwünschte und unerwünschte SMS unterscheidet. Für die Schwarze Liste blockiert der Anruf- und SMS-Filter die SMS-Nachrichten, die diese Phrase enthalten, und stellt SMS zu, in denen diese Schlüsselphrase nicht enthalten ist. Für die Weiße Liste stellt der Anruf- und SMS-Filter die SMS zu, die diese Phrase enthalten, und blockiert die SMS, in denen diese Schlüsselphrase nicht enthalten ist.

Der Anruf- und SMS-Filter filtert die Nachrichten und Anrufe nach dem ausgewählten Modus (s. Abschnitt "Über die Modi für den Anruf- und SMS-Filter" auf S. [25](#)). Nach diesem Modus untersucht Anruf- und SMS-Filter alle eingehenden Anrufe und Nachrichten, und stuft sie als erwünscht oder unerwünscht (Spam) ein. Sobald Anruf- und SMS-Filter einen Anruf oder eine SMS als erwünscht oder unerwünscht einstuft, wird die Untersuchung abgeschlossen.

Informationen über blockierte SMS und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmberichte" auf S. [46](#)).

## ÜBER DIE MODI FÜR DEN ANRUF- UND SMS-FILTER

Der Modus bestimmt die Regeln, nach denen der Anruf- und SMS-Filter die eingehenden Anrufe und SMS prüft.

Für den Anruf- und SMS-Filter sind folgende Modi vorgesehen:

- **Aus** – Alle eingehenden SMS-Nachrichten und Anrufe werden zugestellt.
- **Schwarze Liste** - Anrufe und SMS werden von allen Nummern unter Ausnahme der Schwarzen Liste zugestellt.
- **Weißer Liste** - Anrufe und SMS werden nur von Nummern aus der Weißen Liste zugestellt.
- **Beide Listen** – Eingehende Anrufe und SMS-Nachrichten werden von Nummern aus der Weißen Liste zugestellt und von Nummern aus der Schwarzen Liste blockiert. Nach einem Gespräch oder nach dem Empfang einer SMS von einer Nummer, die auf keiner Liste steht, schlägt Anruf- und SMS-Filter vor, die Nummer in eine der Listen aufzunehmen.

Sie können den Modus des Anruf- und SMS-Filters ändern (s. Abschnitt "Modus des Anruf- und SMS-Filters ändern" auf S. 26). Der aktuelle Modus des Anruf- und SMS-Filters wird auf der Registerkarte **Anruf- und SMS-Filter** neben dem Punkt **Modus** angezeigt.

## MODUS DES ANRUF- UND SMS-FILTERS ÄNDERN

➔ Gehen Sie folgendermaßen vor, um den Modus des Anruf- und SMS-Filters zu ändern:

1. Auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Modus**.  
Das Fenster **Anruf- und SMS-Filter** wird geöffnet.
2. Wählen Sie einen Wert für **Modus für Anruf- und SMS-Filter** aus (s. Abb. unten).

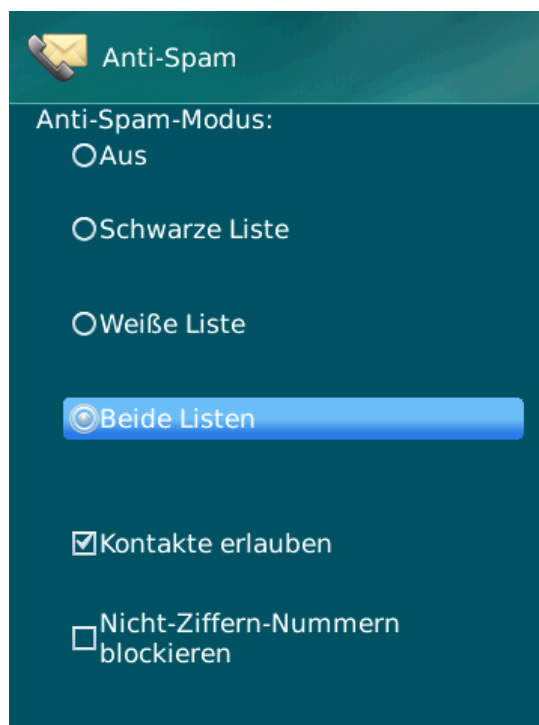


Abbildung 8: Modus des Anruf- und SMS-Filters ändern

3. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## SCHWARZE LISTE ANLEGEN

Die Schwarze Liste enthält Einträge über verbotene Nummern, d.h. jene Nummern, von denen Anrufe und SMS durch den Anruf- und SMS-Filter blockiert werden. Jeder Eintrag enthält folgende Informationen:

- Telefonnummer, von der der Anruf- und SMS-Filter Anrufe und (oder) SMS blockieren soll.
- Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer blockieren soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter zugestellt.

Der Anruf- und SMS-Filter blockiert die Anrufe und SMS, die alle Kriterien eines Eintrags aus der Schwarzen Liste erfüllen. Anrufe und SMS-Nachrichten, die auch nur ein Kriterium eines Eintrags aus der Schwarzen Liste nicht erfüllen, werden vom Anruf- und SMS-Filter zugestellt.

Eine Nummer mit identischen Filterkriterien kann nicht gleichzeitig auf der Schwarzen und Weißen Liste stehen.

Informationen über blockierte SMS und Anrufe werden in einem Bericht erfasst (s. Abschnitt "Programmierberichte" auf S. 46).

### IN DIESEM ABSCHNITT

Eintrag zur Schwarzen Liste hinzufügen .....	<a href="#">27</a>
Eintrag der Schwarzen Liste ändern .....	<a href="#">28</a>
Eintrag aus Schwarzer Liste löschen .....	<a href="#">29</a>

## EINTRAG ZUR SCHWARZEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für den Anruf- und SMS-Filter stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Endpoint Security 8 für Smartphones eine entsprechende Meldung an.

➤ Zum Hinzufügen eines Eintrags zur Schwarzen Liste des Anruf- und SMS-Filters:

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Schwarze Liste**.  
Das Fenster **Schwarze Liste** wird geöffnet.
2. Gehen Sie auf **Menü** → **Hinzufügen**.  
Das Fenster **Neuer Eintrag** wird geöffnet.
3. Nehmen Sie folgende Einstellungen vor (s. Abb. unten):
  - **Eingehende verbieten** – Typ von Ereignissen einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Schwarzen Liste blockiert werden:
    - **Anrufe und SMS** – eingehende SMS und Anrufe blockieren.
    - **Nur Anrufe** – nur eingehende Anrufe blockieren.
    - **Nur SMS** - nur eingehende SMS blockieren.
  - **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "\*" und "?" möglich (wobei "\*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer \*1234? aus der Schwarzen Liste. Der Anruf- und SMS-Filter blockiert Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.

- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS unerwünscht (Spam) ist. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Alle übrigen SMS werden zugestellt.

Wenn alle SMS von einer beliebigen Nummer aus der Schwarzen Liste blockiert werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

Abbildung 9: Einstellungen für einen Eintrag der Schwarzen Liste

4. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## EINTRAG DER SCHWARZEN LISTE ÄNDERN

Für die Einträge aus der Schwarzen Liste können alle Einstellungen geändert werden.

➔ *Zum Ändern eines Eintrags in der Schwarzen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Schwarze Liste**.  
Das Fenster **Schwarze Liste** wird geöffnet.
2. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.  
Das Fenster **Eintrag ändern** wird geöffnet..
3. Ändern Sie die erforderlichen Parameter:
  - **Eingehende verbieten** – Typ von Ereignissen einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Schwarzen Liste blockiert werden:
    - **Anrufe und SMS** – eingehende SMS und Anrufe blockieren.
    - **Nur Anrufe** – nur eingehende Anrufe blockieren.
    - **Nur SMS** - nur eingehende SMS blockieren.
  - **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "\*" und "?" möglich (wobei "\*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer \*1234? aus der Schwarzen Liste. Der Anruf- und SMS-Filter blockiert Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.

- **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS unerwünscht (Spam) ist. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Alle übrigen SMS werden zugestellt.

Wenn alle SMS von einer beliebigen Nummer aus der Schwarzen Liste blockiert werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

4. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## EINTRAG AUS SCHWARZER LISTE LÖSCHEN

Eine Nummer kann aus der Schwarzen Liste gelöscht werden. Außerdem können Sie die Schwarze Liste des Anruf- und SMS-Filters leeren, d.h. alle Einträge daraus löschen.

➤ *Zum Löschen eines Eintrags aus der Schwarzen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Schwarze Liste**.  
Das Fenster **Schwarze Liste** wird geöffnet.
2. Markieren Sie in der Liste den Eintrag, den Sie löschen möchten, und gehen Sie dann auf **Menü** → **Löschen**.  
Ein Bestätigungsfenster wird geöffnet.
3. Bestätigen Sie die Deinstallation mit **Ja**.

➤ *Zum Leeren der Schwarzen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Schwarze Liste**.  
Das Fenster **Schwarze Liste** wird geöffnet.
2. Gehen Sie auf **Menü** → **Alle löschen**.  
Ein Bestätigungsfenster wird geöffnet.
3. Bestätigen Sie die Deinstallation mit **Ja**.

Die Liste wird geleert.

## WEIßE LISTE ANLEGEN

Die Weiße Liste enthält Einträge über erlaubte Nummern, d.h. jene Nummern, von denen Anrufe und SMS durch den Anruf- und SMS-Filter zugestellt werden. Jeder Eintrag enthält folgende Informationen:

- Telefonnummer, von der der Anruf- und SMS-Filter Anrufe und (oder) SMS zustellen soll.
- Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer zustellen soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter stellt nur SMS zu, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter blockiert.

Der Anruf- und SMS-Filter stellt nur die Anrufe und SMS zu, die alle Kriterien eines Eintrags aus der Weißen Liste erfüllen. Anrufe und SMS-Nachrichten, die auch nur ein Kriterium eines Eintrags aus der Weißen Liste nicht erfüllen, werden vom Anruf- und SMS-Filter blockiert.

### IN DIESEM ABSCHNITT

Eintrag zur Weißen Liste hinzufügen .....	<a href="#">30</a>
Eintrag der Weißen Liste ändern .....	<a href="#">31</a>
Eintrag aus Weißer Liste löschen.....	<a href="#">31</a>

## EINTRAG ZUR WEIßEN LISTE HINZUFÜGEN

Beachten Sie, dass eine Nummer mit identischen Filterkriterien nicht gleichzeitig auf der Schwarzen und Weißen Liste der Telefonnummern für den Anruf- und SMS-Filter stehen kann. Wenn eine Nummer mit identischen Filterkriterien bereits in einer der Listen vorhanden ist, zeigt Kaspersky Endpoint Security 8 für Smartphones eine entsprechende Meldung an.

➤ Zum Hinzufügen eines Eintrags zur Weißen Liste des Anruf- und SMS-Filters:

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Weiße Liste**.  
Das Fenster **Weiße Liste** wird geöffnet.
2. Gehen Sie auf **Menü** → **Hinzufügen**.
3. Legen Sie folgende Parameter für den neuen Eintrag fest (s. Abb. unten):
  - **Eingehende erlauben** – Typ von Ereignissen von einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Weißen Liste erlaubt werden:
    - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
    - **Nur Anrufe** – nur eingehende Anrufe erlauben.
    - **Nur SMS** - nur eingehende SMS erlauben.
  - **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "\*" und "?" möglich (wobei "\*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer \*1234? aus der Weißen Liste. Der Anruf- und SMS-Filter stellt Anrufe und SMS von einer Nummer zu, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
  - **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS erwünscht ist. Für Nummern aus der Weißen Liste stellt der Anruf- und SMS-Filter nur die SMS zu, die die Schlüsselphrase enthalten. Alle übrigen SMS von dieser Nummer werden blockiert.

Wenn alle SMS von einer bestimmten Nummer aus der Weißen Liste zugestellt werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

Abbildung 10: Einstellungen für einen Eintrag der Weißen Liste

4. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## EINTRAG DER WEIßEN LISTE ÄNDERN

Alle Einstellungen der Einträge aus der Weißen Liste können geändert werden.

➔ *Zum Ändern eines Eintrags in der Weißen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Weiße Liste**.  
Das Fenster **Weiße Liste** wird geöffnet.
2. Wählen Sie aus der Liste ein Element, das geändert werden soll, und gehen Sie dann auf **Menü** → **Ändern**.  
Das Fenster **Eintrag ändern** wird geöffnet..
3. Ändern Sie die erforderlichen Parameter:
  - **Eingehende erlauben** – Typ von Ereignissen von einer Telefonnummer, die vom Anruf- und SMS-Filter für Nummern aus der Weißen Liste erlaubt werden:
    - **Anrufe und SMS** – eingehende Anrufe und SMS erlauben.
    - **Nur Anrufe** – nur eingehende Anrufe erlauben.
    - **Nur SMS** - nur eingehende SMS erlauben.
  - **Telefonnummer** – Telefonnummer, für die der Anruf- und SMS-Filter eingehende Informationen zustellen soll. Die Nummer kann mit einer Ziffer, einem Buchstaben oder dem Zeichen "+" beginnen und darf Ziffern und / oder Buchstaben enthalten. Zur Angabe von Nummern sind auch die Masken "\*" und "?" möglich (wobei "\*" für eine beliebige Zeichenfolge steht, "?" für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer \*1234? aus der Weißen Liste. Der Anruf- und SMS-Filter stellt Anrufe und SMS von einer Nummer zu, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.
  - **Mit Text** – Schlüsselphrase, die darauf hinweist, dass eine empfangene SMS erwünscht ist. Für Nummern aus der Weißen Liste stellt der Anruf- und SMS-Filter nur die SMS zu, die die Schlüsselphrase enthalten. Alle übrigen SMS von dieser Nummer werden blockiert.

Wenn alle SMS von einer bestimmten Nummer aus der Weißen Liste zugestellt werden sollen, lassen Sie das Feld **Mit Text** für diesen Eintrag leer.

4. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## EINTRAG AUS WEIßER LISTE LÖSCHEN

Sie können einen Eintrag aus der Weißen Liste löschen oder die Liste vollständig leeren.

➔ *Zum Löschen eines Eintrags aus der Weißen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Weiße Liste**.  
Das Fenster **Weiße Liste** wird geöffnet.
2. Markieren Sie in der Liste den Eintrag, den Sie löschen möchten, und gehen Sie dann auf **Menü** → **Löschen**.  
Ein Bestätigungsfenster wird geöffnet.
3. Bestätigen Sie die Deinstallation mit **Ja**.

➔ *Zum Leeren der Weißen Liste des Anruf- und SMS-Filters:*

1. Wählen Sie auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Weiße Liste**.  
Das Fenster **Weiße Liste** wird geöffnet.
2. Klicken Sie auf **Menü** → **Alle löschen**.  
Ein Bestätigungsfenster wird geöffnet.
3. Bestätigen Sie die Deinstallation mit **Ja**.

Die Weiße Liste wird geleert.

## REAKTION AUF SMS-NACHRICHTEN UND ANRUFEN VON KONTAKTEN, DIE NICHT IM TELEFONBUCH STEHEN

Im Modus **Beide Listen** oder **Weißer Liste** (s. Abschnitt "Über die Modi für den Anruf- und SMS-Filter" auf S. 25) können Sie zusätzlich festlegen, wie der Anruf- und SMS-Filter auf SMS und Anrufe von Nummern reagieren soll, die sich nicht in den Kontakten befinden. Die Weiße Liste des Anruf- und SMS-Filters lässt sich durch Aufnahme der Nummern aus den Kontakten erweitern.

- *Gehen Sie folgendermaßen vor, um festzulegen, wie der Anruf- und SMS-Filter auf eine Nummer reagieren soll, die nicht im Telefonbuch des Geräts steht:*
  1. Auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Modus**.  
Das Fenster **Anruf- und SMS-Filter** wird geöffnet.
  2. Wählen Sie einen Wert für **Kontakte erlauben** (s. Abb. unten):
    - Aktivieren Sie das Kontrollkästchen **Kontakte erlauben**, damit der Anruf- und SMS-Filter die Nummern aus den Kontakten als zusätzliche Weiße Liste betrachtet und die SMS und Anrufe von Nummern blockiert, die nicht in den Kontakten stehen.
    - Wählen Sie **Kontakte erlauben**, damit der Anruf- und SMS-Filter die Anrufe und Nachrichten nur nach dem festgelegten Modus filtert.

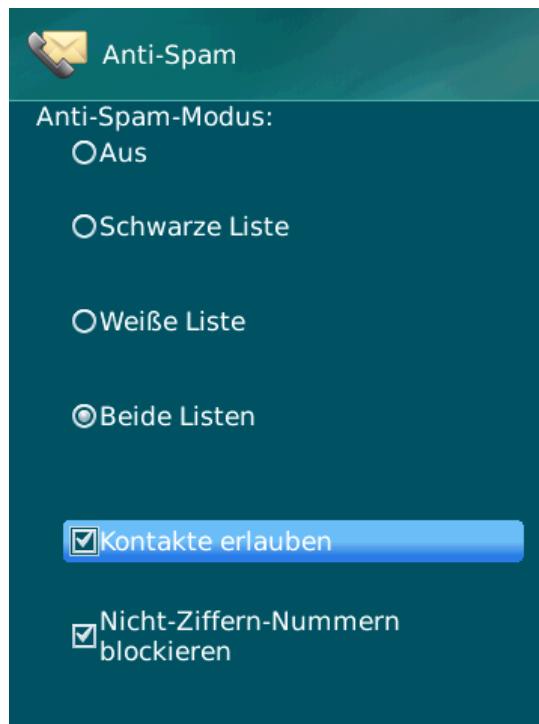


Abbildung 11: Reaktion des Anruf- und SMS-Filters auf Nummern, die nicht in den Kontakten stehen.

3. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## REAKTION AUF SMS VON NICHT-ZIFFERN-NUMMERN

Für den Modus des Anruf- und SMS-Filters **Beide Listen** oder **Schwarze Liste** (s. Abschnitt "Über die Modi für den Anruf- und SMS-Filter" auf S. 25) können Sie die Schwarze Liste durch Aufnahme aller Nicht-Ziffern-Nummern (Nummern, die Buchstaben enthalten) erweitern. In diesem Fall behandelt der Anruf- und SMS-Filter die SMS, die von Nicht-Ziffern-Nummern stammen, als würden diese Nummern auf der Schwarzen Liste stehen.

➤ Gehen Sie folgendermaßen vor, um festzulegen, wie der Anruf- und SMS-Filter auf eingehende SMS von Nicht-Ziffern-Nummern reagieren soll:

1. Auf der Registerkarte **Anruf- und SMS-Filter** den Punkt **Modus**.

Das Fenster **Anruf- und SMS-Filter** wird geöffnet.

2. Wählen Sie einen Wert für den Parameter **Nicht-Ziffern-Nummern blockieren** (s. Abb. unten):

- Aktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**, damit der Anruf- und SMS-Filter die SMS von Nicht-Ziffern-Nummern automatisch blockiert.
- Deaktivieren Sie das Kontrollkästchen **Nicht-Ziffern-Nummern blockieren**, damit der Anruf- und SMS-Filter die SMS von Nicht-Ziffern-Nummern nur auf Basis des für den Anruf- und SMS-Filter ausgewählten Modus filtert.

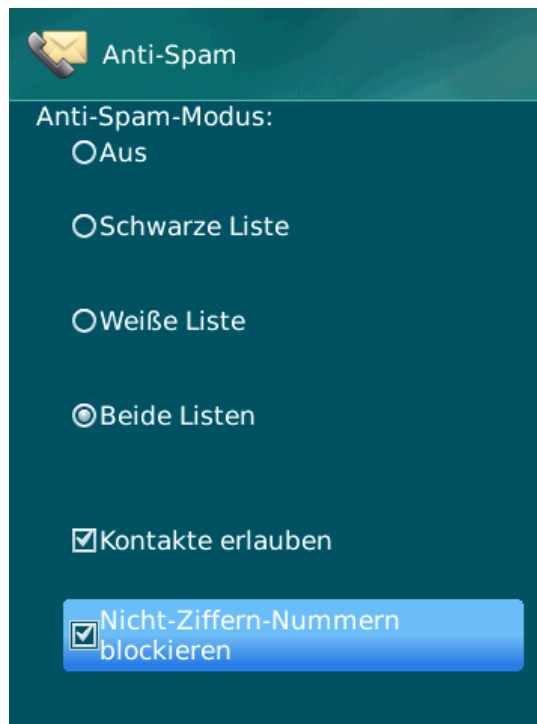


Abbildung 12: Aktion des Anruf- und SMS-Filters für eingehende SMS von Nicht-Ziffern-Nummern auswählen

3. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## AKTION FÜR EINGEHENDE SMS WÄHLEN

Im Modus **Beide Listen** (s. Abschnitt "**Über die Modi für den Anruf- und SMS-Filter**" auf S. [25](#)) prüft der Anruf- und SMS-Filter eingehende SMS auf Übereinstimmungen mit der Schwarzen und Weißen Liste.

Nach dem Empfang einer SMS von einer Nummer, die auf keiner Liste steht, schlägt der Anruf- und SMS-Filter vor, die Nummer in eine der Listen aufzunehmen (s. Abb. unten):

Sie können eine der folgenden Aktionen für eine SMS wählen:

- Um eine SMS zu blockieren und die Telefonnummer des Absenders in die Schwarze Liste aufzunehmen, wählen Sie **Zur Schwarzen Liste hinzuf.**
- Um eine SMS zu erlauben und die Telefonnummer des Absenders in die Weiße Liste aufzunehmen, wählen Sie **Zur Weißen Liste hinzuf.**
- Klicken Sie auf **Überspringen**, damit die SMS zugestellt und die Telefonnummer des Absenders nicht in eine Liste eingetragen wird.

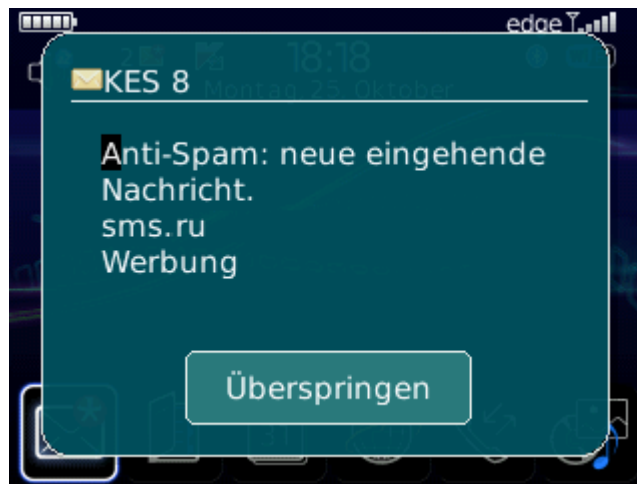


Abbildung 13: Meldung vom Anruf- und SMS-Filter über den Empfang einer SMS

Informationen über blockierte SMS werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [46](#)).

## AKTION FÜR EINGEHENDE ANRUF WÄHLEN

Im Modus **Beide Listen** (s. Abschnitt "**Über die Modi für den Anruf- und SMS-Filter**" auf S. 25) prüft der Anruf- und SMS-Filter eingehende Anrufe auf Übereinstimmungen mit der Schwarzen und Weißen Liste. Nach einem Anruf von einer Nummer, die auf keiner Liste steht, schlägt der Anruf- und SMS-Filter vor, die Nummer in eine der Listen aufzunehmen (s. Abb. unten):

Für eine Nummer, von der ein Anruf erfolgte, können Sie eine der folgenden Aktionen wählen:

- Um die Telefonnummer des Anrufers in die Schwarze Liste aufzunehmen, wählen Sie **Zur Schwarzen Liste hinzuf.**
- Um die Telefonnummer des Anrufers in die Weiße Liste aufzunehmen, wählen Sie **Zur Weißen Liste hinzuf.**
- Klicken Sie auf **Überspringen**, damit die Telefonnummer des Anrufers nicht in eine Liste eingetragen wird.

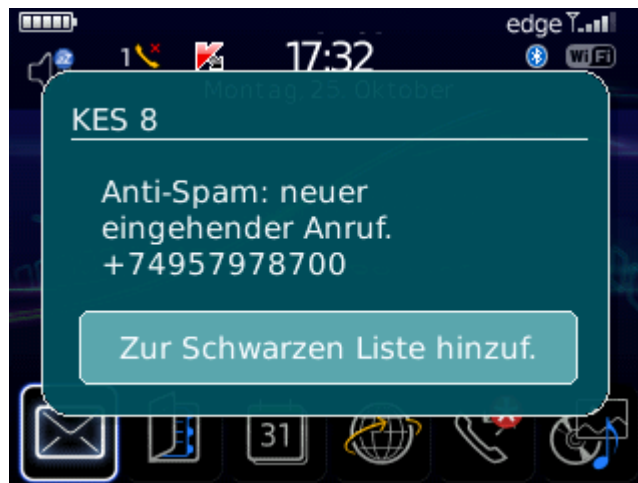


Abbildung 14: Meldung vom Anruf- und SMS-Filter über den Empfang einer SMS

Informationen über blockierte Anrufe werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. 46).

# DATENSCHUTZ BEI VERLUST ODER DIEBSTAHL DES GERÄTS

Dieser Abschnitt informiert über die Komponente Diebstahlschutz, die bei Diebstahl oder Verlust des Geräts die auf dem Gerät gespeicherten Informationen vor unbefugtem Zugriff schützt und das Auffinden des Geräts erleichtert.

Außerdem werden hier folgende Vorgänge beschrieben: Diebstahlschutz-Funktionen aktivieren / deaktivieren, Diebstahlschutz anpassen, Diebstahlschutz-Funktionen von einem anderen Gerät aus ferngesteuert starten.

## IN DIESEM ABSCHNITT

Über den Diebstahlschutz .....	<a href="#">36</a>
Gerät blockieren .....	<a href="#">36</a>
Persönliche Daten löschen .....	<a href="#">38</a>
Liste der zu löschenden Ordner erstellen .....	<a href="#">40</a>
Wechsel der SIM-Karte auf dem Gerät überwachen .....	<a href="#">41</a>
Geografische Koordinaten des Geräts ermitteln .....	<a href="#">42</a>
Diebstahlschutz-Funktionen ferngesteuert starten .....	<a href="#">44</a>

## ÜBER DEN DIEBSTAHLSCHEUTZ

Der Diebstahlschutz schützt die Informationen, die auf Ihrem mobilen Gerät gespeichert sind, vor unbefugtem Zugriff.

Der Diebstahlschutz umfasst folgende Funktionen:

- **SMS-Block** erlaubt es, das Gerät ferngesteuert zu blockieren und einen Text festzulegen, der auf dem Display des blockierten Geräts angezeigt wird.
- **SMS-Clean** erlaubt es, die persönlichen Benutzerdaten (Einträge in den Kontakten, Nachrichten, Bilder, Kalender, Berichte, Internet-Einstellungen) sowie Daten auf Speicherkarten und von Dateien aus der Lösch-Liste per Fernsteuerung vom Gerät zu löschen.
- **SIM-Watch** erlaubt es, die aktuelle Telefonnummer zu ermitteln, wenn die SIM-Karte gewechselt wurde. Außerdem kann das Gerät automatisch blockiert werden, wenn die SIM-Karte gewechselt oder das Gerät ohne SIM eingeschaltet wird. Informationen über die neue Telefonnummer werden als Nachricht an die von Ihnen angegebene Telefonnummer und / oder E-Mail-Adresse geschickt.
- Mit **GPS-Find** kann ein Gerät geortet werden. Die geografischen Koordinaten des Geräts werden als Nachricht an die Telefonnummer, von der der spezielle SMS-Befehl stammte, und an eine E-Mail-Adresse geschickt.

Die Diebstahlschutz-Funktionen von Kaspersky Endpoint Security 8 für Smartphones lassen sich durch einen SMS-Befehl von einem anderen Gerät aus starten (s. Abschnitt "Diebstahlschutz-Funktionen ferngesteuert starten" auf S. [44](#)).

Um die Diebstahlschutz-Funktionen ferngesteuert zu starten, ist der Geheimcode für das Programm erforderlich, der beim ersten Start von Kaspersky Endpoint Security 8 für Smartphones auf Ihrem Gerät festgelegt wurde.

Der aktuelle Status der einzelnen Funktionen wird im Fenster **Diebstahlschutz** neben der jeweiligen Funktion angezeigt.

Informationen über die Arbeit einer Komponente werden in einem Programmbericht erfasst (s. Abschnitt "Programmberichte" auf S. [46](#)).

## GERÄT BLOCKIEREN

Nach Empfang eines speziellen SMS-Befehls kann die Funktion SMS-Block per Fernsteuerung den Zugriff auf das Gerät und die darauf gespeicherten Daten sperren. Das Gerät kann nur durch Eingabe des Geheimcodes entsperrt werden.

Diese Funktion blockiert das Gerät nicht, sondern aktiviert eine Option für das ferngesteuerte Blockieren.

➔ Gehen Sie folgendermaßen vor, um die Funktion SMS-Block zu aktivieren:

1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **SMS-Block**.  
Das Fenster **SMS-Block** wird geöffnet.
2. Aktivieren Sie das Kontrollkästchen **SMS-Block aktivieren**.
3. Ändern Sie im Feld **Text beim Blockieren** den Text, der auf dem Display des blockierten Geräts angezeigt werden soll (s. Abb. unten). In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Telefonbesitzers hinzufügen können.

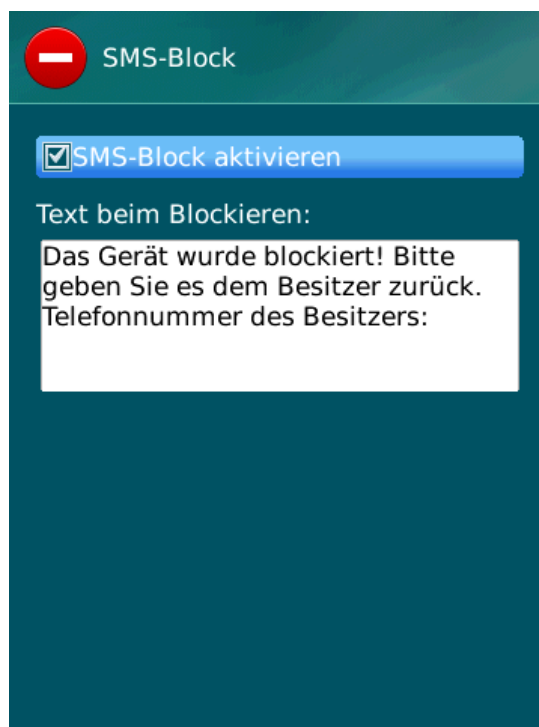


Abbildung 15: Einstellungen der Funktion SMS-Block

4. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

Ein anderes Gerät, auf dem die Funktion SMS-Block aktiviert ist, kann auf folgende Weise gesperrt werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z.B. in Kaspersky Endpoint Security 8 für Smartphones) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion **Befehl senden**. Dadurch erhält Ihr Gerät unbemerkt eine SMS und das Gerät wird blockiert.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um ein Gerät per Fernzugriff zu blockieren, wird die sichere Methode mit der Funktion Befehl senden empfohlen. In diesem Fall wird der Geheimcode für das Programm in verschlüsselter Form gesendet.

- *Gehen Sie folgendermaßen vor, um den SMS-Befehl mit Hilfe der Funktion **Befehl senden** an das andere Gerät zu senden:*
  1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Befehl senden** aus.  
Das Fenster **Befehl senden** wird geöffnet.
  2. Wählen Sie für **SMS-Befehl auswählen** den Wert **SMS-Block** aus.
  3. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.
  4. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode für das Programm ein, der für das Gerät gilt, an das der SMS-Befehl gerichtet ist.
  5. Gehen Sie auf **Menü** → **Senden**.
- *Um mit Hilfe der Standardfunktionen eines Telefons eine SMS zu erstellen,*  
schicken Sie an das andere Gerät eine SMS mit dem Text `block:<Code>`, wobei `<Code>` der Geheimcode des Programms ist, der auf dem anderen Gerät hinterlegt ist. Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

## PERSÖNLICHE DATEN LÖSCHEN

Nach Erhalt des speziellen SMS-Befehls ermöglicht es die Funktion SMS-Clean, die folgenden, auf dem Gerät gespeicherten Informationen zu löschen:

- persönliche Benutzerdaten (Einträge in den Kontakten, Kalender, E-Mails, Anrufliste)
- Informationen auf einer Speicherkarte
- Dateien aus der Liste der zu löschenden Ordner (s. Abschnitt "Liste der zu löschenden Ordner erstellen" auf S. 40).

Diese Funktion löscht die auf dem Gerät gespeicherten Daten nicht, sondern aktiviert eine Option zur Datenlöschung.

- *Gehen Sie folgendermaßen vor, um die Funktion SMS-Clean zu aktivieren:*
  1. Auf der Registerkarte **Diebstahlschutz** wählen Sie den Punkt **SMS-Clean**.  
Das Fenster **SMS-Clean** wird geöffnet.
  2. Gehen Sie auf **Modus**.  
Das Fenster **SMS-Clean** wird geöffnet.

3. Aktivieren Sie das Kontrollkästchen **SMS-Clean aktivieren**.
4. Wählen Sie die zu löschenden Informationen aus. Aktivieren Sie dazu im Block **Löschen** die entsprechenden Kontrollkästchen (s. Abb. unten):
  - Aktivieren Sie das Kontrollkästchen **Persönliche Daten**, damit persönliche Daten gelöscht werden.
  - Damit Dateien aus den Ordnern auf der Speicherkarte und aus der Lösch-Liste entfernt werden, aktivieren Sie das Kontrollkästchen **Ausgewählte Ordner**.

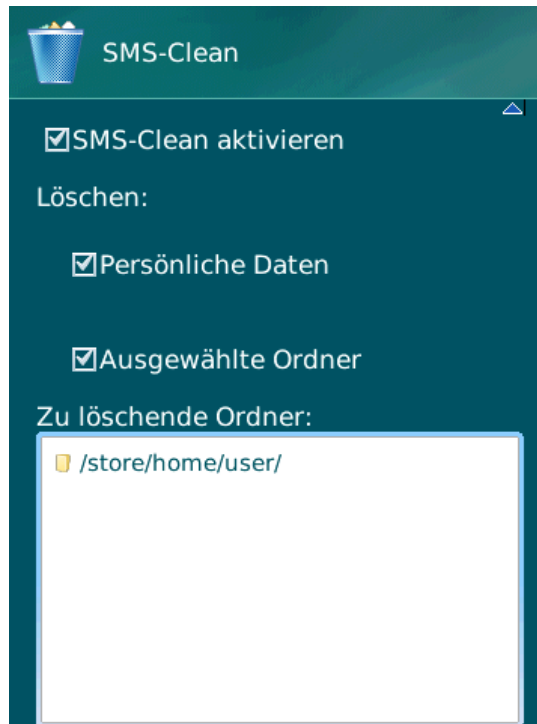


Abbildung 16: Einstellungen der Funktion SMS-Clean

5. Erstellen Sie nun die Liste der zu löschenden Ordner (s. Abschnitt "Liste der zu löschenden Ordner erstellen" auf S. 40).
6. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

Wenn die Funktion aktiviert ist, können persönliche Daten auf folgende Weise vom Gerät gelöscht werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z.B. in Kaspersky Endpoint Security 8 für Smartphones) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Dadurch erhält Ihr Gerät unbemerkt eine SMS und die Informationen werden gelöscht. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion **Befehl senden**.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät unbemerkt eine SMS und die Informationen werden gelöscht.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um per Fernsteuerung Daten vom Gerät zu löschen, wird die sichere Methode mit der Funktion **Befehl senden** empfohlen. In diesem Fall wird der Geheimcode für das Programm in verschlüsselter Form gesendet.

➔ Gehen Sie folgendermaßen vor, um den SMS-Befehl mit Hilfe der Funktion **Befehl senden** an das andere Gerät zu senden:

1. Auf der Registerkarte **Erweitert** wählen Sie den Punkt **Befehl senden** aus.  
Das Fenster **Befehl senden** wird geöffnet.
2. Wählen Sie für **SMS-Befehl auswählen** den Wert **SMS-Clean** aus.

3. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.
4. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode für das Programm ein, der für das Gerät gilt, an das der SMS-Befehl gerichtet ist.
5. Gehen Sie auf **Menü** → **Senden**.

➔ *Um mit Hilfe der Standardfunktionen eines Telefons eine SMS zu erstellen:*

schicken Sie an das andere Gerät eine SMS mit dem Text `wipe:<Code>` (wobei `<Code>` der Geheimcode für das Programm auf dem anderen Gerät ist). Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

## LISTE DER ZU LÖSCHENDEN ORDNER ERSTELLEN

Die Funktion SMS-Clean erlaubt es, eine Liste mit Ordnern anzulegen, die nach dem Empfang eines speziellen SMS-Befehls gelöscht werden sollen.

Damit der Diebstahlschutz die Ordner aus dieser Liste nach Empfang eines speziellen SMS-Befehls löscht, stellen Sie sicher, dass auf der Registerkarte **Diebstahlschutz** → **SMS-Clean** das Kontrollkästchen **Ausgewählte Ordner** aktiviert ist.

Die Liste der zu löschenden Ordner kann Ordner enthalten, die vom Administrator hinzugefügt wurden. Solche Ordner können nicht aus der Liste entfernt werden.

➔ *Gehen Sie folgendermaßen vor, um einen Ordner zur Liste der zu löschenden Ordner hinzuzufügen:*

1. Auf der Registerkarte **Diebstahlschutz** wählen Sie den Punkt **SMS-Clean**.  
Das Fenster **SMS-Clean** wird geöffnet.
2. Gehen Sie weiter zur Liste der zu löschenden Ordner.
3. Gehen Sie auf **Menü** → **Ordner hinzufügen** (s. Abb. unten).

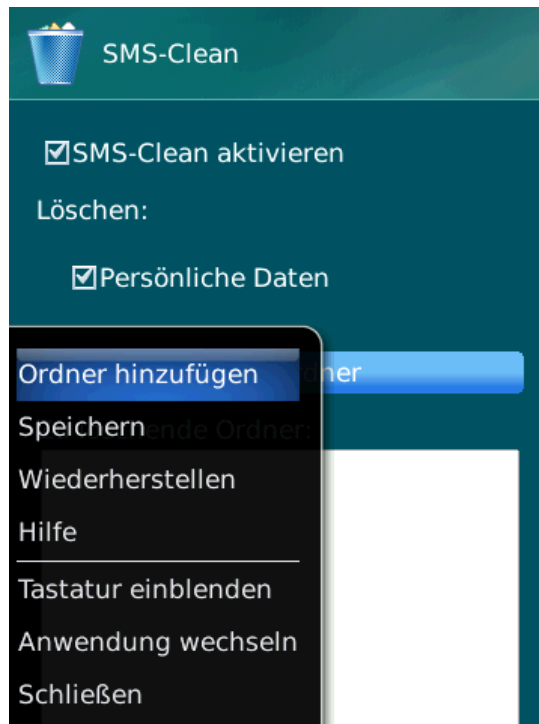


Abbildung 17: Ordner hinzufügen

4. Markieren Sie den entsprechenden Ordner in der Ordnerstruktur und gehen Sie auf **Menü** → **Auswählen**.  
Der Ordner wird zur Liste **Ausgewählte Ordner** hinzugefügt.
5. Gehen Sie auf **Menü** → **Speichern**.
- *Gehen Sie folgendermaßen vor, um einen Ordner aus der Liste zu löschen:*
  1. Auf der Registerkarte **Diebstahlschutz** wählen Sie den Punkt **SMS-Clean**.  
Das Fenster **SMS-Clean** wird geöffnet.
  2. Gehen Sie weiter zur Liste der zu löschenden Ordner.
  3. Markieren Sie einen Ordner in der Liste und gehen Sie dann auf **Menü** → **Ordner löschen**.  
Ein Bestätigungsfenster wird geöffnet.
  4. Bestätigen Sie das Löschen des Ordners mit **Ja**.  
Der Ordner wird aus der Liste **Ausgewählte Ordner** entfernt.
  5. Gehen Sie auf **Menü** → **Speichern**.

## WECHSEL DER SIM-KARTE AUF DEM GERÄT ÜBERWACHEN

Wenn die SIM-Karte ausgetauscht wird, kann SIM-Watch die neue Telefonnummer an eine vorgegebene Telefonnummer und (oder) E-Mail-Adresse schicken und das Gerät blockieren.

- *Gehen Sie folgendermaßen vor, um die Funktion SIM-Watch zu aktivieren und den Wechsel der SIM-Karte auf dem Gerät zu überwachen:*
  1. Wählen Sie auf der Registerkarte **Diebstahlschutz** den Punkt **SIM-Watch**.  
Das Fenster **SIM-Watch** wird geöffnet.
  2. Aktivieren Sie das Kontrollkästchen **SIM-Watch aktivieren**.
  3. Passen Sie folgende Parameter an, um den Wechsel der SIM-Karte auf dem Gerät zu kontrollieren (s. Abb. unten):
    - Um automatisch eine SMS mit der neuen Nummer Ihres Telefons zu erhalten, tragen Sie unter **Beim Wechsel der SIM-Karte neue Nummer senden** im Feld **SMS an Telefonnummer** die Telefonnummer ein, die per SMS benachrichtigt werden soll.  
Die Nummer kann mit einer Ziffer oder dem Zeichen "+" beginnen und darf nur Ziffern enthalten.
    - Wenn Sie per E-Mail über die neue Nummer Ihres Telefons informiert werden möchten, tragen Sie unter **Beim Wechsel der SIM-Karte neue Nummer senden** im Feld **Nachricht an E-Mail-Adresse** die entsprechende E-Mail-Adresse ein.

- Aktivieren Sie unter **Erweitert** das Kontrollkästchen **Gerät blockieren**, damit das Gerät blockiert wird, wenn die SIM-Karte ausgetauscht oder das Gerät ohne SIM eingeschaltet wird. Das Gerät kann durch Eingabe des Geheimcodes für das Programm entsperrt werden.
- Damit auf dem Display des blockierten Geräts eine Nachricht angezeigt wird, füllen Sie das Feld **Text beim Blockieren** aus. In der Grundeinstellung wird für die Meldung ein Standardtext verwendet, dem Sie die Nummer des Besitzers hinzufügen können.

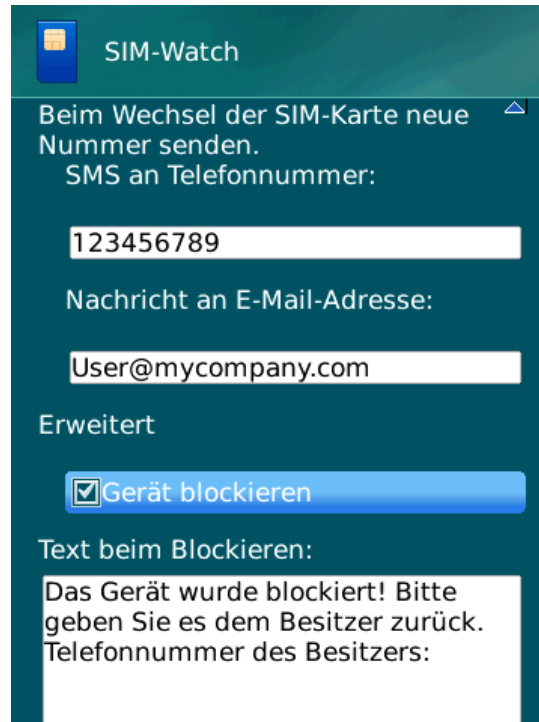


Abbildung 18: Einstellungen der Funktion SIM-Watch

4. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

## GEOGRAFISCHE KOORDINATEN DES GERÄTS ERMITTELN

Nach Empfang eines speziellen SMS-Befehls kann die Funktion GPS-Find die geografischen Koordinaten des Geräts ermitteln und diese mit einer SMS oder E-Mail an das anfragende Gerät und an eine E-Mail-Adresse schicken.

Für das Senden einer SMS fallen die tarifüblichen Gebühren an.

Diese Funktion eignet sich nur für Geräte mit integriertem GPS-Empfänger. Der GPS-Empfänger wird automatisch aktiviert, nachdem das Gerät einen speziellen SMS-Befehl erhalten hat. Wenn sich das Gerät im Empfangsbereich von Satelliten befindet, empfängt die Funktion GPS-Find die Gerätekoordinaten und leitet sie weiter. Besteht im Augenblick der Anfrage kein Satellitenempfang, dann versucht GPS-Find in regelmäßigen Abständen, das Gerät zu orten und die Suchergebnisse zu übermitteln.

➔ Gehen Sie folgendermaßen vor, um GPS-Find zu aktivieren:

1. Auf der Registerkarte **Diebstahlschutz** wählen Sie den Punkt **GPS-Find**.

Das Fenster **GPS-Find** wird geöffnet.

2. Aktivieren Sie das Kontrollkästchen **GPS-Find aktivieren**.

Beim Empfang eines speziellen SMS-Befehls schickt Kaspersky Endpoint Security 8 für Smartphones eine Antwort-SMS mit den Gerätekoordinaten.

3. Um die Koordinaten des Geräts auch per E-Mail zu erhalten, geben Sie bitte im Block **Geräte koordinaten senden** für den Parameter **Nachricht an E-Mail-Adresse** die entsprechende E-Mail-Adresse ein.

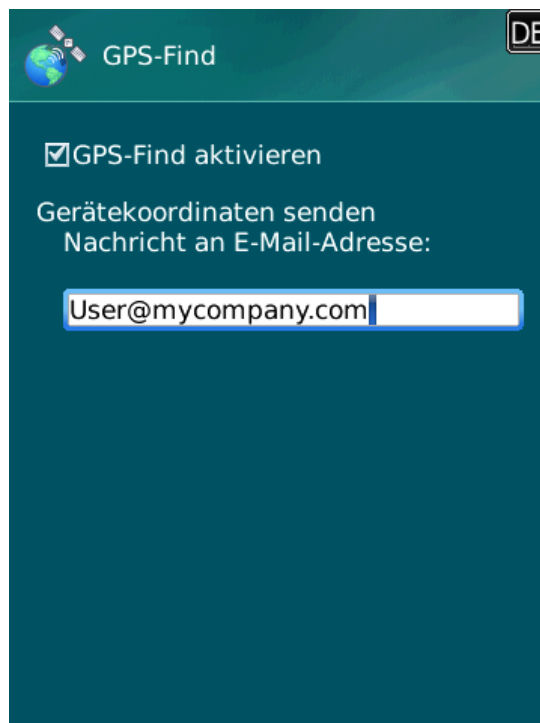


Abbildung 19: Einstellungen der Funktion GPS-Find

4. Gehen Sie auf **Menü** → **Speichern**, um die Änderungen zu speichern.

Wenn GPS-Find aktiviert ist, können die Koordinaten des Geräts auf folgende Weise ermittelt werden:

- Erstellen Sie auf einem anderen mobilen Gerät in einem Programm für mobile Endgeräte (z.B. in Kaspersky Endpoint Security 8 für Smartphones) einen speziellen SMS-Befehl und senden Sie diesen an Ihr Gerät. Dadurch erhält Ihr Gerät eine SMS und das Programm sendet die Gerätekoordinaten. Um einen speziellen SMS-Befehl zu erstellen, verwenden Sie bitte die Funktion Befehl senden.
- Erstellen Sie auf einem anderen mobilen Gerät eine SMS mit einem speziellen Text und dem Geheimcode des Geräts, an das die SMS geht, und senden Sie diese. Dadurch erhält Ihr Gerät eine SMS und das Programm sendet die Gerätekoordinaten.

Für das Senden einer SMS fallen für das sendende Gerät die tarifgemäßen Gebühren an.

Um die Gerätekoordinaten zu erhalten, wird die sichere Methode mit der Funktion Befehl senden empfohlen. In diesem Fall wird der Geheimcode in verschlüsselter Form gesendet.

➤ *Gehen Sie folgendermaßen vor, um den Befehl mit Hilfe der Funktion Befehl senden an das andere Gerät zu senden:*

1. Wählen Sie auf der Registerkarte **Erweitert** den Punkt **Befehl senden** aus.  
Das Fenster **Befehl senden** wird geöffnet.
2. Wählen Sie für **SMS-Befehl auswählen** den Wert **GPS-Find** aus.
3. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.
4. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode für das Programm ein, der für das Gerät gilt, an das der SMS-Befehl gerichtet ist.
5. Gehen Sie auf **Menü** → **Senden**.

➤ *Um mit Hilfe der Standardfunktionen eines Telefons eine SMS zu erstellen:*

schicken Sie an das andere Gerät eine SMS mit dem Text `find:<Code>`, wobei `<Code>` der Geheimcode des Programms ist, der auf dem anderen Gerät hinterlegt ist. Die Groß- und Kleinschreibung von Buchstaben und die Leerzeichen vor und nach dem Doppelpunkt sind irrelevant.

Eine SMS mit den Koordinaten des Geräts wird an die Nummer des Telefons gesendet, von dem aus der SMS-Befehl gesendet wurde, sowie an eine E-Mail-Adresse, sofern eine solche in den Einstellungen für GPS-Find hinterlegt wurde.

# DIEBSTAHLSCHUTZ-FUNKTIONEN FERNGESTEUERT

## STARTEN

Das Programm ermöglicht den Versand eines speziellen SMS-Befehls, um auf einem anderen Gerät, auf dem Kaspersky Endpoint Security 8 für Smartphones installiert ist, die Diebstahlschutz-Funktionen ferngesteuert zu starten. Der SMS-Befehl wird in Form einer verschlüsselten SMS gesendet und erhält den Geheimcode für das Programm, das auf dem anderen Gerät installiert ist. Der Empfang des SMS-Befehls bleibt auf dem anderen Gerät unbemerkt.

Für die SMS fallen die tarifgemäßen Gebühren an.

➤ Gehen Sie folgendermaßen vor, um einen SMS-Befehl an das andere Gerät zu senden:

1. Auf der Registerkarte **Erweitert** wählen Sie den Punkt **Befehl senden** aus.  
Das Fenster **Befehl senden** wird geöffnet.
2. Wählen Sie eine Funktion aus, die per Fernsteuerung auf einem anderen mobilen Gerät gestartet werden soll. Wählen Sie dazu einen der folgenden Werte für **SMS-Befehl auswählen** (s. Abb. unten):
  - SMS-Block (auf S. [36](#)).
  - SMS-Clean (s. Abschnitt "Persönliche Daten löschen" auf S. [38](#)).
  - GPS-Find (s. Abschnitt "Geografische Koordinaten des Geräts ermitteln" auf S. [42](#)).
  - Privatsphäre.

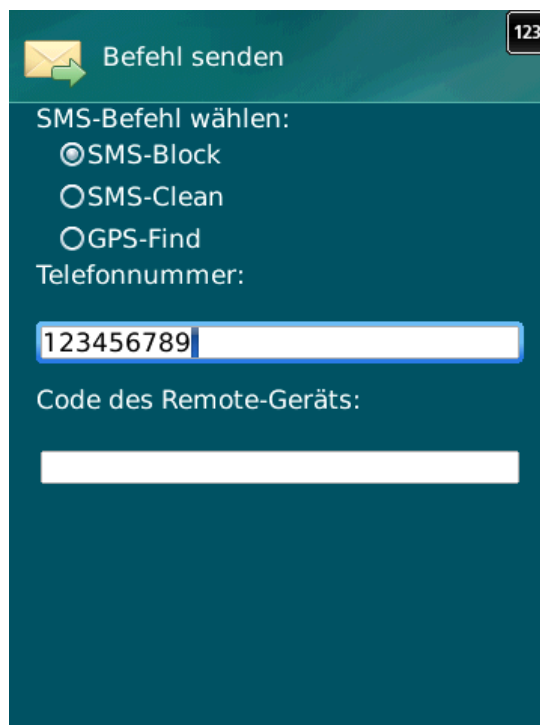


Abbildung 20: Ferngesteuerter Start der Diebstahlschutz-Funktionen

3. Geben Sie im Feld **Telefonnummer** die Telefonnummer des Geräts ein, an das der SMS-Befehl geschickt wird.
4. Geben Sie im Feld **Code des Remote-Geräts** den Geheimcode für das Programm ein, der für das Gerät gilt, an das der SMS-Befehl gerichtet ist.
5. Gehen Sie auf **Menü** → **Senden**.

# PROGRAMMBERICHTE

Dieser Abschnitt informiert über die Berichte, in denen die Arbeit der einzelnen Komponenten und die Ausführung aller Aufgaben (z.B. Synchronisierung mit dem Remote-Management-System, Empfang eines SMS-Befehls von einem anderen Gerät) protokolliert werden.

## IN DIESEM ABSCHNITT

---

Berichte .....	<a href="#">46</a>
Berichtseinträge anzeigen.....	<a href="#">46</a>
Einträge aus Bericht löschen.....	<a href="#">46</a>

## BERICHTE

In Berichten werden Ereignisse gespeichert, die bei der Arbeit der einzelnen Komponenten von Kaspersky Endpoint Security 8 für Smartphones auftreten. Für jede Komponente wird ein eigener Ereignisbericht geführt. Sie können einen Bericht über die Ereignisse auswählen und ansehen, die bei der Arbeit der Komponente eingetreten sind. Die Einträge werden im Bericht chronologisch in absteigender Reihenfolge angeordnet.

## BERICHTSEINTRÄGE ANZEIGEN

- *Um die Einträge im Bericht einer Komponente anzuzeigen,*

Wählen Sie auf der Registerkarte der entsprechenden Komponente den Punkt **Ereignisbericht**.

Ein Bericht für die ausgewählte Komponente wird geöffnet.

Verwenden Sie zur Navigation innerhalb eines Berichts das Trackpad.

- *Um ausführliche Informationen über einen Berichtseintrag anzuzeigen,*

wählen Sie den gewünschten Eintrag und betätigen Sie die Taste **ENTER**.

## EINTRÄGE AUS BERICHT LÖSCHEN

Sie können alle Berichte leeren. Dabei werden die Informationen über die Arbeit aller Komponenten von Kaspersky Endpoint Security 8 für Smartphones gelöscht.

- *Gehen Sie folgendermaßen vor, um alle Berichte zu leeren:*

1. Wählen Sie auf der Registerkarte einer beliebigen Komponente den Punkt **Ereignisbericht**.  
Das Fenster **Ereignisbericht** wird geöffnet.
2. Gehen Sie auf **Menü** → **Bericht leeren**.
3. Bestätigen Sie die Deinstallation mit **Ja**.

Es werden sämtliche Einträge aus den Berichten aller Komponenten gelöscht.

# ANPASSEN VON ERWEITERTEN EINSTELLUNGEN

Dieser Abschnitt informiert über zusätzliche Optionen von Kaspersky Endpoint Security 8 für Smartphones: Geheimcode für das Programm ändern, Tooltips aktivieren / deaktivieren (Tooltips anzeigen, wenn eine Komponente angepasst werden soll).

## IN DIESEM ABSCHNITT

Geheimcode ändern.....	47
Tooltips anzeigen.....	47

## GEHEIMCODE ÄNDERN

Der Geheimcode für das Programm, der nach dem ersten Start des Programms festgelegt wurde, kann geändert werden.

➤ *Gehen Sie folgendermaßen vor, um den Geheimcode des Programms zu ändern:*

1. Auf der Registerkarte **Erweitert** wählen Sie den Punkt **Erweiterte Einstellungen** aus.  
Das Fenster **Erweiterte Einstellungen** wird geöffnet.
2. Wählen Sie den Punkt **Code eingeben**.
3. Tragen Sie den aktuellen Geheimcode des Programms im Feld **Geheimcode eingeben** ein.
4. Geben Sie in den Feldern **Neuen Code eingeben** und **Code bestätigen** einen neuen Geheimcode für das Programm ein.

Ein eingegebener Code wird automatisch auf seine Sicherheit geprüft.

Wenn der eingegebene Geheimcode sicher ist, wird er gespeichert.

Wenn die Prüfung ergibt, dass ein Code unsicher ist, erscheint eine Warnung auf dem Bildschirm und das Programm erfragt eine Bestätigung. Klicken Sie auf **Ja**, um den aktuellen Code zu verwenden.

Klicken Sie auf **Nein**, um einen neuen Code festzulegen. Die Felder **Neuen Code eingeben** und **Code bestätigen** werden geleert. Geben Sie den Geheimcode für das Programm erneut ein.

## TOOLTIPS ANZEIGEN

Während Sie die Einstellungen der Komponenten anpassen, zeigt Kaspersky Endpoint Security 8 für Smartphones standardmäßig kurze Tooltips für die jeweilige Funktion an. Sie können die Anzeige von Tooltips für Kaspersky Endpoint Security 8 für Smartphones anpassen.

➤ *Gehen Sie folgendermaßen vor, um die Anzeige von Tooltips anzupassen:*

1. Auf der Registerkarte **Erweitert** wählen Sie den Punkt **Erweiterte Einstellungen** aus.  
Das Fenster **Erweiterte Einstellungen** wird geöffnet.
2. Aktivieren / deaktivieren Sie die Anzeige von Tooltips. Wählen Sie dazu den Punkt **Tooltips** aus.

Der aktuelle Status der Tooltips wird neben dem Punkt **Tooltips** angezeigt. Der rechts angebrachte Auswahlschalter ändert sein Aussehen abhängig davon, welchen Status die Tooltips-Anzeige besitzt.

# GLOSSAR

## A

### **AKTIVIERUNG DES PROGRAMMS**

Freischaltung aller Programmfunktionen. Der Benutzer kann das Programm während oder nach der Installation aktivieren. Zur Aktivierung wird ein Aktivierungscode oder eine Schlüsseldatei benötigt.

## G

### **GEHEIMCODE FÜR DAS PROGRAMM**

Der Geheimcode des Programms verhindert einen unbefugten Zugriff auf Programmeinstellungen und geschützte Informationen, die sich auf dem Gerät befinden. Er wird beim ersten Programmstart vom Benutzer festgelegt und muss aus mindestens vier Ziffern bestehen. Der Geheimcode des Programms wird in folgenden Fällen abgefragt:

- für den Zugriff auf die Programmeinstellungen
- wenn von einem anderen mobilen Gerät aus ein SMS-Befehl gesendet wird, um folgende Funktionen ferngesteuert zu starten: SMS-Block, SMS-Clean, SIM-Watch, GPS-Find und Privatsphäre.

## L

### **LÖSCHEN VON SMS**

Verarbeitungsmethode für SMS, die Spam-Merkmale aufweisen. Dabei wird die Nachricht physikalisch gelöscht. Diese Methode wird für SMS empfohlen, die eindeutig als Spam gelten.

## M

### **MASKE FÜR EINE TELEFONNUMMER**

Platzhalter für eine Telefonnummer in der Schwarzen oder Weißen Liste. Die beiden wichtigsten Zeichen in Masken für Telefonnummern sind \* und ? (wobei \* für eine beliebige Anzahl von beliebigen Zeichen steht und ? für ein beliebiges Einzelzeichen). Zum Beispiel: Nummer \*1234? aus der Schwarzen Liste. Der Anruf- und SMS-Filter blockiert die Anrufe und SMS von einer Nummer, in der auf die Ziffern 1234 ein beliebiges Zeichen folgt.

## N

### **NICHT-ZIFFERN-NUMMERN**

Eine Nicht-Ziffern-Nummer (auch Buchstabenwahl-, Wortwahlrufnummer oder Vanity-Rufnummer) ist eine Telefonnummer, die teilweise oder vollständig aus Buchstaben besteht.

## R

### **REMOTE-MANAGEMENT-SYSTEM**

System, mit dem Geräte ferngesteuert und in Echtzeit verwaltet werden können.

## S

### **SCHWARZE LISTE**

Die Einträge dieser Liste enthalten folgende Informationen:

- Telefonnummer, von der der Anruf- und SMS-Filter Anrufe und (oder) SMS blockieren soll.

- Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer blockieren soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter blockiert nur jene SMS, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter zugestellt.

## **SYNCHRONISIERUNG**

Vorgang, bei dem eine Verbindung zwischen dem mobilen Gerät und dem Remote-Management-System hergestellt wird, um Daten zu übertragen. Bei der Synchronisierung werden die vom Administrator festgelegten Programmeinstellungen auf das Gerät übertragen. Vom Gerät werden Berichte über die Arbeit der Programmkomponenten an das Remote-Management-System übertragen.

## **W**

### **WEIßE LISTE**

Die Einträge dieser Liste enthalten folgende Informationen:

- Telefonnummer, von der der Anruf- und SMS-Filter Anrufe und (oder) SMS zustellen soll.
- Typ der Ereignisse, die der Anruf- und SMS-Filter von dieser Nummer zustellen soll. Folgende Ereignistypen sind vorhanden: Anrufe und SMS, nur Anrufe, nur SMS.
- Schlüsselphrase, nach der der Anruf- und SMS-Filter eine SMS als unerwünscht (Spam) einstufen soll. Der Anruf- und SMS-Filter stellt nur SMS zu, die diese Schlüsselphrase enthalten. Die übrigen SMS werden vom Anruf- und SMS-Filter blockiert.

# KASPERSKY LAB ZAO

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, vor Spam sowie vor Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

**Produkte.** Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Anwendungen für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Dienste für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert, die Anti-Spam-Datenbanken im 5-Minuten-Takt.*

**Technologien.** Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (Großbritannien), CommuniGate Systems (USA), Critical Path (Irland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Frankreich), NETGEAR (USA), Parallels (Russland), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

**Auszeichnungen.** Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in einem Test des anerkannten österreichischen Antiviren-Labors AV-Comparatives mit mehreren Premium-Awards Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Website von Kaspersky Lab:

<http://www.kaspersky.de>

Viren-Enzyklopädie:

<http://www.securelist.com/de>

Antiviren-Labor:

newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden)

<http://support.kaspersky.de/helpdesk.html>

(für Fragen an die Virenanalysiker)

Webforum von Kaspersky Lab:

<http://forum.kaspersky.com>

# INFORMATIONEN ZUM PROGRAMMCODE VON DRITTHERSTELLERN

Bei der Programmentwicklung wurde der Code von Drittherstellern verwendet.

Für das Erstellen und die Überprüfung elektronischer digitaler Signaturen wird die Programmbibliothek für den Informationsschutz (PBSI) "Crypto-C" verwendet, die von CryptoEx OOO entwickelt wurde.

Webseite von CryptoEx OOO: <http://www.cryptoex.ru>.

# MARKENHINWEIS

Die registrierten Markenzeichen und Dienstleistungszeichen sind Eigentum der rechtmäßigen Besitzer.

Das Markenzeichen Blackberry ist Eigentum von Research In Motion Limited, ist in der USA registriert und kann in anderen Ländern angemeldet oder registriert sein.

# SACHREGISTER

## A

Aktivieren	
Anruf- und SMS-Filter .....	26

## Ä

Ändern	
Schwarze Liste des Anruf- und SMS-Filters .....	28
Weiße Liste des Anruf- und SMS-Filters .....	31

## A

Anruf- und SMS-Filter.....	25
Aktion für Anruf.....	35
Aktion für SMS.....	34
Modi.....	26
Nicht-Ziffern-Nummern .....	33
Nummer, die nicht in den Kontakten steht.....	32
Schwarze Liste .....	27
Weiße Liste.....	29

## B

Bildschirm	
Fenster für den Schutzstatus .....	24

## C

Code	
Geheimcode für das Programm.....	21

## D

Daten	
ferngesteuertes Löschen .....	38
Deaktivieren	
Anruf- und SMS-Filter.....	26
Diebstahlschutz.....	36
GPS-Find.....	43
SIM-Watch.....	41
SMS-Block.....	37
SMS-Clean .....	38, 40

## E

Eintrag	
Schwarze Liste des Anruf- und SMS-Filters .....	27
Weiße Liste des Anruf- und SMS-Filters .....	30
Ereignisberichte	
Einträge anzeigen.....	46
Einträge löschen .....	46
Erlauben	
eingehende Anrufe .....	30
eingehende SMS .....	30

## F

FILTERUNG	
EINGEHENDE ANRUFEN .....	25
EINGEHENDE SMS .....	25

**G**

Geheimcode für das Programm .....21, 47  
 Gerät orten .....43

**H**

HARDWAREVORAUSSETZUNGEN .....9  
 Hinzufügen  
     Schwarze Liste des Anruf- und SMS-Filters .....27  
     Weiße Liste des Anruf- und SMS-Filters .....30

**K**

KASPERSKY LAB.....50

**L**

Lizenz  
     Informationen.....18  
 Löschen  
     Berichtseinträge.....46  
     Informationen, die auf dem Gerät gespeichert sind .....38  
     Schwarze Liste des Anruf- und SMS-Filters .....29  
     Weiße Liste des Anruf- und SMS-Filters .....31  
 LÖSCHEN  
     PROGRAMM .....16

**M**

Modi  
     Anruf- und SMS-Filter .....26

**P**

PROGRAMM INSTALLIEREN .....10  
 PROGRAMMOBERFLÄCHE .....23  
 Programm-Tooltips.....47

**R**

Registerkarten des Programms.....23

**S**

Schlüssel  
     Installation .....18  
 Schutzstatus.....24  
 Schwarze Liste  
     Anruf- und SMS-Filter .....27  
 SMS-Befehl senden .....45  
 SMS-Block  
     Eingehende Anrufe .....27, 29  
     eingehende SMS .....27  
     Gerät .....37  
 Start  
     Programm.....21

**W**

Weiße Liste  
     Anruf- und SMS-Filter .....29

**Z**

ZAO KASPERSKY LAB.....50