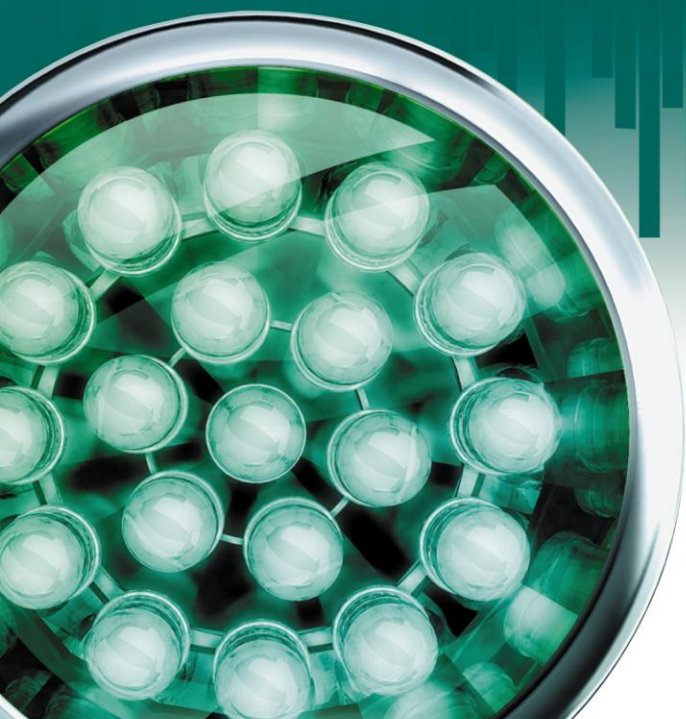


Kaspersky Endpoint Security 8 für Linux

INSTALLATIONSHAND BUCH

PROGRAMMVERSION: 8.0



KASPERSKY lab

Sehr geehrte Benutzerinnen und Benutzer!

Vielen Dank, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Achtung! Die Rechte an diesem Dokument liegen bei Kaspersky Lab ZAO (im Weiteren auch Kaspersky Lab) und sind durch die Urhebergesetze der Russischen Föderation und durch internationale Abkommen geschützt. Bei illegalem Vervielfältigen und Weiterverbreiten des Dokuments oder einzelner Teile daraus kann der Beschuldigte nach den Gesetzen der Russischen Föderation zivilrechtlich, verwaltungsrechtlich und strafrechtlich zur Verantwortung gezogen werden.

Das Kopieren in jeder Form, das Weiterverbreiten wie eine Übersetzung von Unterlagen ist nur mit einer schriftlichen Einwilligung von Kaspersky Lab erlaubt.

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

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

Für den Inhalt, die Qualität, die Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, deren Rechte anderen Rechteinhabern gehören, sowie für Schäden, die in Verbindung mit der Nutzung dieser Unterlagen entstehen, lehnt Kaspersky Lab die Haftung ab.

In diesem Dokument werden eingetragene Markenzeichen und Handelsmarken verwendet, die das Eigentum der jeweiligen Rechtsinhaber sind.

Redaktionsdatum: 11.05.11

© 1997-2011 Kaspersky Lab ZAO. Alle Rechte vorbehalten

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

INHALT

EINFÜHRUNG	5
Funktion des Programms.....	5
Hard- und Softwarevoraussetzungen für das System	5
Informationen zu Ereignissen für Kaspersky Endpoint Security anzeigen	6
Informationsquellen zur selbständigen Recherche	7
Kontaktaufnahme mit dem Technischen Support	8
Diskussion von Kaspersky-Lab-Programmen im Webforum.....	9
Was ist neu in Version 8.....	9
EINZELKOMPONENTEN DES PROGRAMMS	12
INSTALLATION VON KASPERSKY ENDPOINT SECURITY.....	13
Schritt 1. Pakete für Kaspersky Endpoint Security installieren	13
Schritt 2. Installation des Administrationsagenten	14
REMOTE-INSTALLATION VON KASPERSKY ENDPOINT SECURITY	15
Aufgabe zur Remote-Installation erstellen.....	15
Schritt 1. Aufgabennamen festlegen	16
Schritt 2. Aufgabenart auswählen	16
Schritt 3. Installationspaket auswählen	16
Schritt 4. Methode zur Remote-Installation auswählen	16
Schritt 5. Aufgabeneinstellungen bestimmen	17
Schritt 6. Installationspaket für gemeinsame Installation auswählen	17
Schritt 7. Einstellungen für den Neustart der Computer konfigurieren	17
Schritt 8. Art der Auswahl von Computern definieren	17
Schritt 9. Client-Computer auswählen.....	17
Schritt 10. Benutzerkonto für Aufgabenstart auswählen	18
Schritt 11. Zeitplan für Aufgabenstart erstellen	18
Schritt 12. Erstellen einer Aufgabe abschließen	19
Aufgabe zur Remote-Installation starten	19
Aufgabe zur Remote-Installation anzeigen und konfigurieren	19
Installationspaket erstellen	20
Schritt 1. Namen des Installationspakets festlegen.....	20
Schritt 2. Lieferumfang des Programms auswählen.....	20
Schritt 3. Laden des Installationspakets.....	21
Schritt 4. Aufgabeneinstellungen für den Echtzeitschutz anpassen.....	21
Schritt 5. Sonstige Einstellungen der Updateaufgabe konfigurieren	21
Schritt 6. Erstellen des Installationspakets abschließen	22
Einstellungen des Installationspakets anzeigen und konfigurieren.....	22
ERSTKONFIGURATION VON KASPERSKY ENDPOINT SECURITY	23
Schritt 1. Lizenzvereinbarung durchlesen.....	24
Schritt 2. Zeichensatz auswählen	24
Schritt 3. Schlüsseldatei installieren	25
Schritt 4. Proxyserver-Einstellungen anpassen	25
Schritt 5. Datenbanken von Kaspersky Endpoint Security herunterladen.....	25
Schritt 6. Automatisches Update der Antiviren-Datenbanken aktivieren.....	26
Schritt 7. Kernel-Modul kompilieren.....	26

Schritt 8. Mit Samba-Server integrieren.....	27
Schritt 9. Automatischer Start der grafischen Oberfläche.....	27
Schritt 10. Echtzeitschutzaufgabe starten.....	28
Schritt 11. Einstellungen für Administrationsagenten konfigurieren.....	28
Automatischer Start der Erstkonfiguration.....	28
Erlaubnisregeln in den Systemen SELinux und AppArmor anpassen.....	30
KASPERSKY ENDPOINT SECURITY DEINSTALLIEREN.....	31
REMOTE-DEINSTALLATION VON KASPERSKY ENDPOINT SECURITY.....	32
AKTIONEN NACH DER DEINSTALLATION VON KASPERSKY ENDPOINT SECURITY.....	33
FUNKTIONSPRÜFUNG FÜR AUFGABEN ZUM ECHTZEITSCHUTZ UND VIRENSUCHE.....	34
Funktionsprüfung für Echtzeitschutzaufgabe.....	34
Funktionsprüfung für Untersuchungsaufgabe.....	35
EICAR-"Testvirus" und seine Modifikationen.....	35
DATEISTRUKTUR VON KASPERSKY ENDPOINT SECURITY.....	37
KASPERSKY LAB.....	38

EINFÜHRUNG

Dieses Handbuch beschreibt die Installation des Programms Kaspersky Endpoint Security 8 für Linux (im Folgenden – *Kaspersky Endpoint Security* oder das *Programm*).

Alle Befehle, die im folgenden Text dieses Dokuments genannt werden, beziehen sich auf Linux-Systeme.

IN DIESEM ABSCHNITT

Funktion des Programms	5
Hard- und Softwarevoraussetzungen für das System	5
Informationen zu Ereignissen für Kaspersky Endpoint Security anzeigen	6
Was ist neu in Version 8.....	9

FUNKTION DES PROGRAMMS

Das Programm Kaspersky Anti-Virus 8 für Linux dient dem Virenschutz von Workstations bei Verwendung des Linux-Betriebssystems.

Kaspersky Endpoint Security bietet:

- Permanenten Schutz des Dateisystems vor schädlichem Programmcode: Erkennen und Abwehr von Zugriffsversuchen auf Dateien; Analyse von Zugriffsversuchen; Desinfektion und Löschen von infizierten Objekten;
- Überprüfen von Objekten auf der Workstation auf Anfrage: Suche nach infizierten und verdächtigen Objekten in ausgewählten Untersuchungsbereichen; Analyse von Objekten; Desinfizieren und Löschen infizierter Objekte;
- Verschieben verdächtiger und beschädigter Objekte in die Quarantäne;
- Anlegen von Kopien infizierter Objekte in einem speziellen Backup-Speicher vor der Desinfektion, um Objekte, die wichtige Informationen und Daten enthalten, bei Bedarf wiederherstellen zu können;
- Datenbanken aktualisieren (Als Ressource für die Aktualisierung der Datenbanken dienen die Updateserver oder der Administrationsserver von Kaspersky Lab. Kaspersky Endpoint Security kann auch so eingestellt werden, dass die Datenbanken aus einem lokalen Verzeichnis aktualisiert werden);
- Verwaltung des Programms und seiner Einstellungen mit Hilfe eines Verwaltungstools, dem Kaspersky Administration Kit.

HARD- UND SOFTWAREVORAUSSETZUNGEN FÜR DAS SYSTEM

Damit Sie Kaspersky Endpoint Security verwenden können, muss Ihr System folgende Hard- und Softwareanforderungen erfüllen:

- Mindestanforderungen für die Hardware:
 - CPU Intel Pentium® II 400 MHz oder höher;

- 512 MB RAM;
- Swap-Partition mit einer Größe von mindestens 1 GB;
- 2 GB freier Speicherplatz auf der Festplatte zur Installation des Programms sowie für temporäre Dateien und Protokolldateien.
- Softwareanforderungen:
 - für 32-Bit-Plattform folgender Betriebssysteme:
 - Red Hat Enterprise Linux 5.5 Desktop;
 - Fedora 13;
 - CentOS-5.5;
 - SUSE Linux Enterprise Desktop 10 SP3;
 - SUSE Linux Enterprise Desktop 11 SP1;
 - openSUSE Linux 11.3;
 - Mandriva Linux 2010 Spring;
 - Ubuntu 10.04 LTS Desktop Edition;
 - Debian GNU/Linux 5.0.5.
 - für 64-Bit-Plattform folgender Betriebssysteme:
 - Red Hat Enterprise Linux 5.5 Desktop;
 - Fedora 13;
 - CentOS-5.5;
 - SUSE Linux Enterprise Desktop 10 SP3;
 - SUSE Linux Enterprise Desktop 11 SP1;
 - openSUSE Linux 11.3;
 - Ubuntu 10.04 LTS Desktop Edition;
 - Debian GNU/Linux 5.0.5.
 - Interpreter für Perl 5.0 oder höher <http://www.perl.org>
 - Pakete für Programmkompilierung (gcc, binutils, glibc (für 64-Bit-Betriebssysteme wird 32-bit-Version von glibc verwendet), glibc-devel, make, ld) sowie Quellcode des BS-Kernels zur Kompilierung der Module von Kaspersky Endpoint Security.

INFORMATIONEN ZU EREIGNISSEN FÜR KASPERSKY ENDPOINT SECURITY ANZEIGEN

Kaspersky Lab bietet Ihnen verschiedene Informationsquellen zur Arbeit mit dem Programm. Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage aus diesen Quellen wählen.

Nachdem Sie Kaspersky Endpoint Security käuflich erworben haben, wenden Sie sich an unseren Technischen Support. Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Mitarbeitern von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse <http://forum.kaspersky.com> diskutieren.

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Es stehen Ihnen folgende Informationsquellen zu Kaspersky Endpoint Security zur Verfügung:

- Programm Kaspersky Endpoint Security auf der Homepage von Kaspersky Lab;
- Dokumentation;
- Manual pages.

Programm-Website auf der Homepage von Kaspersky Lab

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

Auf dieser Seite finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten. In unserem Online-Shop können Sie Kaspersky Endpoint Security kaufen oder die Nutzungsdauer verlängern.

Dokumentation

Das **Installationshandbuch** beschreibt die Funktion des Programms, die Hard- und Softwareanforderungen zur Installation von Kaspersky Endpoint Security sowie das Vorgehen zur Installation, Funktionsprüfung und Erstkonfiguration des Programms.

Das **Administratorhandbuch** enthält Informationen zur Steuerung von Kaspersky Endpoint Security mit dem Befehlszeilentool und dem Kaspersky Administration Kit.

Im Lieferumfang sind diese Unterlagen als PDF-Dateien enthalten. Außerdem stehen die Dokumente auf der Website für das Programm Kaspersky Endpoint Security auf der Homepage von Kaspersky Lab zum Download bereit.

Manual Pages

Auf folgenden Manual Pages finden Sie Informationen zu Kaspersky Endpoint Security:

- Kaspersky Endpoint Security über die Befehlszeile verwalten:

`/opt/kaspersky/kes4lwks/share/man/man1/kes4lwks-control.1.gz;`

- Allgemeine Einstellungen von Kaspersky Endpoint Security anpassen:

`/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks.conf.5.gz;`

- Echtzeitschutzaufgabe anpassen:

`/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-oas.conf.5.gz;`

- Untersuchungsaufgaben anpassen:

`/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-ods.conf.5.gz;`

- Updateaufgaben anpassen:

`/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-update.conf.5.gz;`

- Anpassen der Einstellungen für Quarantäne und Backup (Sicherungskopien von desinfizierten und gelöschten Objekten):

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-quarantine.conf.5.gz;

- Einstellungen für den Ereignisspeicher anpassen:

/opt/kaspersky/kes4lwks/share/man/man5/kes4lwks-events.conf.5.gz;

- Beschreibung des Tools zum Ändern der Einstellungen für die Verbindung mit dem Administrationsserver von Kaspersky Administration Kit:

/opt/kaspersky/klnagent/share/man/man1/klmover.1.gz;

- Beschreibung des Tools zum Prüfen der Einstellungen für die Verbindung mit dem Administrationsserver von Kaspersky Administration Kit:

/opt/kaspersky/klnagent/share/man/man1/klnagchk.1.gz;

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Nachdem Sie das Programm käuflich erworben haben, können Sie von den Spezialisten des Technischen Supports per Telefon oder über das Internet Informationen über das Programm erhalten.

Bitte lesen Sie die Supportrichtlinien (<http://support.kaspersky.com/de/support/rules>), bevor Sie sich an den Technischen Support wenden.

E-Mail-Anfrage an den Technischen Support

Sie können Ihre Frage auch an die Spezialisten des Technischen Supports richten. Füllen Sie dazu das Webformular für die Bearbeitung von Kundenanfragen Helpdesk aus (<http://support.kaspersky.ru/helpdesk.html?LANG=de>).

Die Anfrage kann in deutscher, englischer, französischer, spanischer oder russischer Sprache gestellt werden.

Um eine E-Mail-Anfrage zu stellen, ist die Angabe der **Kundennummer**, die Sie bei der Anmeldung auf der Webseite des Technischen Supports erhalten haben, und des **Keywords** erforderlich.

Wenn Sie noch nicht als Benutzer eines Kaspersky-Lab-Programms registriert sind, können Sie das Anmeldeformular ausfüllen (<https://support.kaspersky.com/de/personalcabinet/registration/form/>). Geben Sie bitte während der Registrierung den Dateinamen für die Schlüsseldatei ein.

Die Spezialisten des Technischen Supports werden Ihre Frage per E-Mail an die in der Anfrage angegebene Adresse beantworten sowie in Ihrem Personal Cabinet (<https://support.kaspersky.com/de/PersonalCabinet>).

Beschreiben Sie im Webformular das aufgetretene Problem möglichst genau. Machen Sie in den obligatorisch auszufüllenden Feldern folgende Angaben:

- **Typ der Anfrage.** Wählen Sie bitte aus der Themenliste das Thema aus, das Ihr Problem am besten beschreibt, z.B. "Probleme beim Installieren/Deinstallieren des Programms" oder "Probleme beim Suchen/Löschen von Viren".
- **Name und Versionsnummer des Programms.**
- **Anfragetext.** Beschreiben Sie bitte das aufgetretene Problem möglichst detailliert.
- **Kundennummer und Kennwort.** Geben Sie die Kundennummer und das Kennwort an, die Sie bei der Anmeldung auf der Support-Webseite erhalten haben.

- **E-Mail-Adresse.** An diese Adresse werden die Support-Spezialisten Ihre Anfrage beantworten.

Technischer Support am Telefon

Zur Lösung dringender Probleme können Sie den Technischen Support in Ihrem Land direkt anrufen. Wenn Sie sich an die Spezialisten des lokalen (http://support.kaspersky.com/support/support_local) oder internationalen (<http://support.kaspersky.com/de/support/international>) technischen Supports wenden, vergessen Sie bitte nicht, uns die erforderlichen Informationen über Kaspersky Endpoint Security (<http://support.kaspersky.com/de/support/details>), mitzuteilen.

DISKUSSION VON KASPERSKY-LAB-PROGRAMMEN IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Mitarbeitern 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.

WAS IST NEU IN VERSION 8

Nachfolgend sind alle Neuerungen in der Programmversion Kaspersky Anti-Virus 8 für Linux detailliert beschrieben.

Neuerungen im Schutz:

- Das Programm vereint die Funktionen früherer Programmversionen, Kaspersky Anti-Virus 5.7 for Linux Workstations und Kaspersky Anti-Virus 5.5 for SAMBA Servers, durch Einsatz von zwei neuen Abfangmodulen für Dateiaktionen: im Kernel-Modul sowie in der SAMBA-Umgebung;
- Erweiterte Optionen für Quarantäne / Backup, die Ihnen erlaubt:
 - Manuelles Hinzufügen von Objekten zur Quarantäne;
 - Suche nach Quarantäneobjekten (anhand von bestimmten Objektattributen);
 - Löschen gefundener Objekte;
 - Wiederherstellen gefundener Objekte;
 - Mehrmalige Untersuchung von Objekten;
 - Speichern von Teilen des Quarantäne-/Backup-Speichers als Archivdatei (Einsparung von Speicherplatz);
 - Import von Objekten aus einem Archiv in den Quarantäne- oder Backup-Speicher.

Neuerungen bei der Verwaltung von Kaspersky Endpoint Security:

- Möglichkeit zur zentralen Steuerung des gesamten Produktzyklus von Kaspersky Endpoint Security und Ausführung der Aufgaben zur Virensuche, zum Echtzeitschutz und zum Datenbank-Update von Kaspersky Endpoint Security.
- Zentrale Speicherung der Funktionseinstellungen für Kaspersky Endpoint Security.
- Zur Speicherung der Funktionseinstellungen von Kaspersky Endpoint Security werden keine Konfigurationsdateien in Textform mehr benötigt. Textdateien werden lediglich noch zum Speichern und Abrufen von Programmeinstellungen aus dem zentralen Speicherverzeichnis für Programmeinstellungen benötigt.

- Es gibt die Möglichkeit, mehrere Untersuchungsbereiche für eine einzelne Aufgabe anzugeben. Dabei sind möglich:
 - Individuelle Auswahl der Untersuchungseinstellungen für jeden Untersuchungsbereich;
 - Verschiedene Möglichkeiten zur Vorgabe der Untersuchungsbereiche:
 - Konventionelle Suche und Auswahl im Dateisystem;
 - Auswahl anhand des Gerätenamens;
 - Auswahl anhand der Zugriffsrechte im Netzwerk; (Shared, Mounted);
 - Auswahl anhand des Netzwerkprotokolls (SMB / CIFS, NFS);
 - Auswahl anhand des Namens der Netzwerkressourcen (Samba share name, NFS shared folder);
 - Zur Beschreibung der Untersuchungsbereiche werden Standardausdrücke im Format ECMA-262 unterstützt;
- Für einzelne Untersuchungsbereiche können Benutzernamen / Benutzergruppen vorgegeben werden, deren Dateioperationen durch den permanenten Virenschutz des Programms überwacht werden sollen.
- Es ist die Möglichkeit vorgesehen, mehrere Ausnahmeregeln für denselben Untersuchungsbereich festzulegen.
- Die Remote-Verwaltung mit Hilfe von Kaspersky Administration Kit ist möglich.
- Die Verwaltung mit Hilfe einer lokalen Benutzeroberfläche ist möglich. Dabei können Sie die folgenden Aufgaben ausführen:
 - Schutzstatus des Computers anzeigen, auf dem Kaspersky Endpoint Security installiert ist;
 - Aufgaben zur Untersuchung des Computers auf Viren und zum Datenbankupdate starten und diese Aufgaben steuern;
 - Statistik für die Aufgaben zur Virensuche und zum Echtzeitschutz aufrufen;
 - Ereignisse im Ereignisjournal einsehen.
- Es können Aktionen für einzelne Objekte je nach Art der gefundenen Bedrohung festgelegt werden.
- Es besteht die Möglichkeit, einen genauen Zeitplan für den Start / das Beenden von Aufgaben einzustellen.

Neuerungen in Programmüberwachung, Protokollierung und Statistik von Kaspersky Endpoint Security:

- Erweiterte Möglichkeiten zur Überwachung der Funktionen von Kaspersky Endpoint Security:
 - Neue Programmfunktionen zum Abrufen folgender Informationen:
 - Allgemeine Informationen über das Programm;
 - Informationen zur Version der Datenbanken von Kaspersky Endpoint Security;
 - Informationen zum Lizenzstatus;
 - Statusinformationen für die einzelnen Komponenten von Kaspersky Endpoint Security;
 - Ergebnisinformationen zur Ausführung von Aufgaben;
 - Statusinformationen für Quarantäne / Backup;

- Tools zur retrospektiven Analyse der Arbeit von Kaspersky Endpoint Security mit folgenden Optionen:
 - Sammeln, Berechnen und Protokollieren statistischer Daten zur Programmausführung;
 - Grafische Aufbereitung statistischer Daten zur Programmausführung für ausgewählte Zeiträume;
 - Ereignissuche nach bestimmten Benutzerkriterien;
 - Audit für folgende Aspekte der Arbeit von Kaspersky Endpoint Security: Erstellen / Start / Beenden von Aufgaben, Ändern von Funktionseinstellungen für das Programm, Benutzeraktionen mit Objekten im Quarantäne- / Backup-Speicher usw.;
- Programmfunktionen zum Erstellen und Exportieren statistischer Berichte (unterstützte Formate: HTML, CSV);
- Überwachung der Arbeit von Kaspersky Endpoint Security und der Virenaktivität. Diese Daten werden zentral im Verzeichnis für Ereignisse von Kaspersky Endpoint Security gespeichert. Die Suche, grafische Aufbereitung und Analyse von Daten zur Programmausführung können sowohl über spezielle integrierte Programmfunktionen als auch mit Hilfe externer Anwendungen erfolgen.

EINZELKOMPONENTEN DES PROGRAMMS

Die Einzelkomponenten des Programms sind in nachstehender Tabelle aufgeführt.

Tabelle 1. Pakete für Kaspersky Endpoint Security

PAKET	FUNKTION
kes4lwks-<Versionsnummer>.i386.rpm kes4lwks_<Versionsnummer>_i386.deb	Enthält die wichtigsten Dateien für Kaspersky Endpoint Security. Das Paket kann auf 32- und 64-Bit-Betriebssystemen installiert werden.
klnagent-<Versionsnummer>.i386.rpm klnagent_<Versionsnummer>_i386.deb	Enthält den Administrationsagenten (Dienstprogramm für die Anbindung von Kaspersky Endpoint Security an das Kaspersky Administration Kit).
kes4lwks-rpm.tar.gz kes4lwks-deb.tar.gz	Enthält die Dateien kes4lwks.kpd und akinstall.sh, die bei der Remote-Installation von Kaspersky Endpoint Security mit Hilfe des Kaspersky Administration Kit verwendet werden.
klnagent-rpm.tar.gz klnagent-deb.tar.gz	Enthält die Dateien klnagent.kpd und akinstall.sh, die bei der Remote-Installation des Administrationsagenten mit Hilfe des Kaspersky Administration Kit verwendet werden.

INSTALLATION VON KASPERSKY ENDPOINT SECURITY

Kaspersky Endpoint Security wird in den Paketen in den Formaten `.deb` und `.rpm` geliefert.

Die Installation erfolgt in mehreren Einzelschritten:

1. Pakete für Kaspersky Endpoint Security installieren.
2. Paket des Administrationsagenten installieren (Die Installation dieses Pakets ist notwendig, um Kaspersky Endpoint Security mit Hilfe von Kaspersky Administration Kit zu verwalten zu können).

IN DIESEM ABSCHNITT

Schritt 1. Pakete für Kaspersky Endpoint Security installieren [13](#)

Schritt 2. Installation des Administrationsagenten [14](#)

SCHRITT 1. PAKETE FÜR KASPERSKY ENDPOINT SECURITY INSTALLIEREN

Löschen Sie vor der Installation von Kaspersky Anti-Virus 8 für Linux eventuell auf dem Computer installierte Versionen von Kaspersky Anti-Virus 5.5 for Samba-Server oder Kaspersky Anti-Virus 5.7 for Linux File Server.

Um das Paket Kaspersky Endpoint Security zu installieren, müssen Sie über **root**-Benutzerrechte verfügen.

Vor der Installation von Kaspersky Endpoint Security soll das Paket `glibc` installiert werden (für 64-Bit-Betriebssysteme ist die 32-bit-Version von `glibc` erforderlich).

➤ Um Kaspersky Endpoint Security aus einem `.rpm`-Paket zu installieren, führen Sie folgenden Befehl aus:

```
# rpm -i kes4lwks-<Versionsnummer>_i386.rpm
```

➤ Um Kaspersky Endpoint Security aus einem `.deb`-Paket zu installieren, führen Sie folgenden Befehl aus:

```
# dpkg -i kes4lwks_<Versionsnummer>_i386.deb
```

➤ Um Kaspersky Endpoint Security aus einem `.deb`-Paket auf ein 64-Bit-Betriebssystem zu installieren, führen Sie folgenden Befehl aus:

```
# dpkg -i --force-architecture kes4lwks_<Versionsnummer>_i386.deb
```

Nach Ausführung des Befehls erfolgt die weitere Installation automatisch.

Nach Abschluss der Installation von Kaspersky Endpoint Security aus dem `rpm`-Paket müssen Sie das Skript zur Konfiguration des Programms nach der Installation starten (s. Abschnitt "Erstkonfiguration von Kaspersky Endpoint Security" auf S. [23](#)).

SCHRITT 2. INSTALLATION DES ADMINISTRATIONSAGENTEN

Falls Sie Kaspersky Endpoint Security über Kaspersky Administration Kit verwalten wollen, müssen Sie den Administrationsagenten installieren.

Um den Administrationsagenten zu installieren, müssen Sie über **root**-Benutzerrechte verfügen.

➤ Um den Administrationsagenten aus einem *.rpm*-Paket zu installieren, führen Sie folgenden Befehl aus:

```
# rpm -i klnagent-<Versionsnummer>.i386.rpm
```

➤ Um den Administrationsagenten aus einem *.deb*-Paket zu installieren, führen Sie folgenden Befehl aus:

```
# dpkg -i klnagent_<Versionsnummer>_i386.deb
```

➤ Um den Administrationsagenten aus einem *.deb*-Paket auf ein 64-Bit-Betriebssystem zu installieren, führen Sie folgenden Befehl aus:

```
# dpkg -i --force-architecture klnagent_<Versionsnummer>_i386.deb
```

Nach Ausführung des Befehls erfolgt die weitere Installation automatisch.

Nach Abschluss der Installation aus dem rpm-Paket müssen Sie das Skript zur Konfiguration des Programms nach der Installation starten.

REMOTE-INSTALLATION VON KASPERSKY ENDPOINT SECURITY

Sie können Kaspersky Endpoint Security im Remote-Betrieb über die Administrationskonsole des Kaspersky Administration Kit installieren. Für eine Remote-Installation von Kaspersky Endpoint Security erstellen Sie eine Aufgabe zur Remote-Installation (s. Abschnitt "Aufgabe zur Remote-Installation erstellen" auf S. [15](#)) für eine Gruppe von Computern.

Die Installation erfolgt durch *Push-Installation* (s. "Handbuch zur Einführung von Kaspersky Administration Kit"). Die Push-Installation erlaubt die Remote-Installation eines Programms auf konkreten Client-Computern des logischen Netzwerks. Beim Start der Aufgabe kopiert der Administrationsserver aus dem gemeinsamen Ordner die Installationsdateien des Programms auf jeden Client-Computer in einen temporären Ordner und startet die jeweiligen Installationsprogramme.

Die Kommunikation des Administrationsservers mit den Client-Computern wird durch die Komponente Administrationsagent sichergestellt. Er muss daher unbedingt installiert und konfiguriert sein. Um die Aufgabe zur Remote-Installation erfolgreich auszuführen, muss der Administrationsagent auf dem geschützten Computer gestartet sein.

Beim Erstellen einer Aufgabe zur Remote-Installation werden Installationspakete eingesetzt (s. Abschnitt „Installationspaket erstellen“ auf S. [20](#)). Ein Installationspaket entspricht einer Sammlung von Dateien, die für die Installation benötigt werden. Es enthält sowohl die Parameter für den eigentlichen Installationsvorgang als auch eine Anfangskonfiguration (s. S. [23](#)) der zu installierenden Anwendung (insbesondere eine Datei mit Anti-Virus-Parametern). Das Installationspaket kann vor oder während der Erstellung der Aufgabe zur Remote-Installation erstellt werden. Dabei kann ein Installationspaket mehrmals verwendet werden.

Beachten Sie, dass Installationspakete für Betriebssysteme, die dpkg verwenden auf Basis des deb-Pakets, und für die Betriebssysteme, die RPM verwenden auf Basis des rpm-Pakets erstellt werden müssen.

Alle für einen Administrationsserver erstellten Installationspakete liegen in der Konsolenstruktur im Ordner **Datenverwaltung** → **Installationspakete**.

IN DIESEM ABSCHNITT

Aufgabe zur Remote-Installation erstellen.....	15
Aufgabe zur Remote-Installation starten	19
Aufgabe zur Remote-Installation anzeigen und konfigurieren	19
Installationspaket erstellen	20
Parameter des Installationspakets anzeigen und konfigurieren	22

AUFGABE ZUR REMOTE-INSTALLATION ERSTELLEN

► Um eine Aufgabe zur Remote-Installation für eine Zusammenstellung von Computern mittels Push-Installation zu erstellen, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben für eine Zusammenstellung von Computern** aus.

3. Wählen Sie im entsprechenden Kontextmenü den Punkt **Neu** → **Aufgabe** oder im Menü **Aktion** die gleichnamige Option aus.

Daraufhin wird der Assistent für die Erstellung einer Aufgabe gestartet. Befolgen Sie die Anweisungen.

SCHRITTE DES ASSISTENTEN

Schritt 1. Aufgabennamen festlegen	16
Schritt 2. Aufgabenart auswählen	16
Schritt 3. Installationspaket auswählen	16
Schritt 4. Methode zur Remote-Installation auswählen	16
Schritt 5. Aufgabeneinstellungen bestimmen	17
Schritt 6. Installationspaket für gemeinsame Installation auswählen	17
Schritt 7. Einstellungen für den Neustart der Computer konfigurieren	17
Schritt 8. Art der Auswahl von Computern definieren	17
Schritt 9. Client-Computer auswählen	17
Schritt 10. Benutzerkonto für Aufgabenstart auswählen	18
Schritt 11. Zeitplan für Aufgabenstart erstellen	18
Schritt 12. Erstellen einer Aufgabe abschließen	19

SCHRITT 1. AUFGABENNAMEN FESTLEGEN

Geben Sie in das Feld **Name** den Aufgabennamen ein.

SCHRITT 2. AUFGABENART AUSWÄHLEN

Wählen Sie im Knoten **Kaspersky Administration Kit** die Aufgabenart **Remote-Installation der Anwendung** aus.

SCHRITT 3. INSTALLATIONSPAKET AUSWÄHLEN

Geben Sie das Installationspaket an, dessen Installation mit dieser Aufgabe verbunden ist. Wählen Sie aus den vorhandenen, für diesen Administrationsserver angelegten Paketen das gewünschte Paket aus, oder erstellen Sie ein neues Paket, indem Sie auf die Schaltfläche **Neu** klicken. Daraufhin wird mit dem Assistenten ein neues Installationspaket erstellt (s. Abschnitt „Installationspaket erstellen“ auf S. [20](#)).

SCHRITT 4. METHODE ZUR REMOTE-INSTALLATION AUSWÄHLEN

Wählen Sie die Variante **Push-Installation** aus.

SCHRITT 5. AUFGABENEINSTELLUNGEN BESTIMMEN

Sie können bestimmen, ob die Anwendung erneut installiert werden soll, wenn sie bereits auf dem Client-Computer installiert ist. Aktivieren Sie das Kontrollkästchen **Anwendung nicht installieren, wenn sie schon installiert ist**, damit keine neue Installation der Anwendung auf den Computern erfolgt.

SCHRITT 6. INSTALLATIONSPAKET FÜR GEMEINSAME INSTALLATION AUSWÄHLEN

Wenn Sie den Administrationsagenten zusammen mit der Anwendung installieren wollen, aktivieren Sie das Kontrollkästchen **Administrationsagenten gemeinsam mit dieser Anwendung installieren** und wählen dann das gewünschte Installationspaket aus.

➔ *Um ein neues Installationspaket für den Administrationsagenten zu erstellen,*

klicken Sie auf **Erstellen**.

Es wird daraufhin der Assistent für die Erstellung eines Installationspakets aufgerufen (s. Abschnitt „Installationspaket erstellen“ auf S. [20](#)). Befolgen Sie die Anweisungen.

SCHRITT 7. EINSTELLUNGEN FÜR DEN NEUSTART DER COMPUTER KONFIGURIEREN

Definieren Sie Aktionen, die auszuführen sind, wenn nach der Installation des Programms der Computer neu gestartet werden muss. Es stehen die folgenden Varianten zur Verfügung:

- **Computer nicht neu starten;**
- **Computer neu starten** – Bei dieser Variante wird das Betriebssystem nur im Bedarfsfall neu gestartet;
- **Benutzer fragen** – Bei dieser Variante müssen die Einstellungen für die Benachrichtigung des Benutzers über einen Neustart konfiguriert werden.

Wählen Sie die Variante **Computer nicht neu starten**.

SCHRITT 8. ART DER AUSWAHL VON COMPUTERN DEFINIEREN

Definieren Sie die Art der Auswahl von Computern, für die eine Aufgabe erstellt wird:

- **Auf Basis von Daten aus der Windows-Netzwerkabfrage** – In diesem Fall erfolgt die Auswahl der Computer für die Installation aufgrund von Daten, die der Administrationsserver beim Durchsuchen des Netzwerks des Unternehmens empfangen hat;
- **Auf Basis von manuell einzugebenden Adressen (IP-Adresse, NetBIOS-Name oder DNS-Name)** – In diesem Fall müssen die Namen oder IP-Adressen der Client-Computer manuell ausgewählt und eingegeben werden.

SCHRITT 9. CLIENT-COMPUTER AUSWÄHLEN

Wenn die Computer anhand von Daten ausgewählt werden, die beim Durchsuchen des Netzwerks gewonnen worden sind, wird die Liste im Fenster des Assistenten gebildet. Aktivieren Sie die Kontrollkästchen neben den Namen der Client-Computer in den Administrationsgruppen (Knoten **Verwaltete Computer**) oder der noch nicht zu den Administrationsgruppen hinzugefügten Computer (Knoten **Nicht zugeordnete Computer**), um sie auszuwählen.

Beim manuellen Auswählen der Computer wird die Liste anhand der Eingabe von NetBIOS- und DNS-Namen, IP-Adressen (oder eines Bereiches von IP-Adressen) von Computern erstellt oder durch Import einer Liste aus einer txt-Datei, in der jede Adresse in einer neuen Zeile angegeben sein muss. Sie können die Adressliste durch Klicken auf die Schaltflächen **Hinzufügen**, **Entfernen** und **IP-Intervall hinzufügen** erstellen oder durch Klicken auf die Schaltfläche **Importieren** aus einer Textdatei importieren. Als Computeradresse können Sie die IP-Adresse (oder den IP-Adressbereich), den NetBIOS- oder den DNS-Namen verwenden. Um die Liste aus einer Datei zu importieren, müssen Sie eine txt-Datei mit den Adressen der hinzuzufügenden Computer angeben.

SCHRITT 10. BENUTZERKONTO FÜR AUFGABENSTART AUSWÄHLEN

Wenn der Administrationsagent die Dateien für die Client-Computer bereitstellt, wird das Benutzerkonto nicht verwendet. Alle Kopiervorgänge und die Installation der Dateien erledigt der Administrationsagent unter dem Benutzerkonto **Lokales System**.

SCHRITT 11. ZEITPLAN FÜR AUFGABENSTART ERSTELLEN

Erstellen Sie nun einen Zeitplan für den Aufgabenstart.

- Wählen Sie in der Dropdown-Liste **Start nach Zeitplan** den gewünschten Modus für den Aufgabenstart aus:
 - **Manuell**;
 - **Jede N-te Stunde**;
 - **Täglich**;
 - **Wöchentlich**;
 - **Monatlich**;
 - **Einmal** – Die Aufgabe zur Remote-Installation wird auf den Computern nur einmal gestartet, und zwar unabhängig vom Ergebnis der Ausführung;
 - **Sofort** – Sofort nach dem Erstellen der Aufgabe (nach Abschluss des Assistenten);
 - **Nach Beenden einer anderen Aufgabe** – In diesem Fall wird die Aufgabe Remote-Installation erst nach Abschluss der angegebenen Aufgabe gestartet.
- Richten Sie den Zeitplan in der Feldgruppe ein, die dem ausgewählten Modus entspricht.
- Konfigurieren Sie zusätzliche Einstellungen für den Aufgabenstart (ihre Zusammensetzung hängt vom ausgewählten Startmodus ab). Gehen Sie dazu folgendermaßen vor:
 - Geben Sie die Reihenfolge des Aufgabenstarts vor, wenn innerhalb der durch den Zeitplan festgelegten Zeitdauer der Client-Computer nicht erreichbar ist (ausgeschaltet, nicht im Netzwerk erreichbar usw.) oder die Anwendung nicht gestartet wurde.
 - Aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**, damit beim folgenden Start der Anwendung auf diesem Client-Computer versucht wird, die Aufgabe zu starten. Für die Varianten **Manuell**, **Einmal** und **Sofort** wird die Aufgabe gestartet, sobald der Computer im Netzwerk erkannt wird.
 - Wenn kein Kontrollkästchen aktiviert ist, erfolgt der Aufgabenstart auf den Client-Computern nur nach Zeitplan und für die Varianten **Manuell**, **Einmal** und **Sofort** nur auf den Computern, die im Netzwerk sichtbar sind. Dieses Kontrollkästchen ist standardmäßig deaktiviert.

SCHRITT 12. ERSTELLEN EINER AUFGABE ABSCHLIEßEN

Nach Abschluss des Assistenten wird die neue Aufgabe Remote-Installation zum Ordner **Aufgaben für Zusammenstellungen von Computern** hinzugefügt und im Ergebnisbereich angezeigt. Bei Bedarf können Sie ihre Einstellungen ändern (s. Abschnitt „Aufgabe Remote-Installation konfigurieren“ auf S. [19](#)).

AUFGABE ZUR REMOTE-INSTALLATION STARTEN

➤ Um die Aufgabe Remote-Installation für eine Zusammenstellung von Computern manuell zu starten, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben für eine Zusammenstellung von Computern** aus.
3. Wählen Sie im Ergebnisbereich die gewünschte Aufgabe aus.
4. Wählen Sie im entsprechenden Kontextmenü den Befehl **Start** oder im Menü **Aktion** die gleichnamige Option aus.

AUFGABE ZUR REMOTE-INSTALLATION ANZEIGEN UND KONFIGURIEREN

➤ Um die Eigenschaften der Aufgabe zur Remote-Installation anzuzeigen und ihre Einstellungen zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben für eine Zusammenstellung von Computern** aus.
2. Wählen Sie im Ergebnisbereich die gewünschte Aufgabe aus.
3. Wählen Sie im entsprechenden Kontextmenü den Befehl **Eigenschaften** oder im Menü **Aktion** die gleichnamige Option aus.

Dadurch wird das Fenster **Eigenschaften: <Aufgabenname>**, geöffnet, das die folgenden Registerkarten enthält: **Allgemein**, **Benachrichtigung**, **Client-Computer**, **Zeitplan**, **Parameter**, **Benutzerkonto** und **Neustart des Betriebssystems**.

Die Aufgabe Remote-Installation wird wie jede andere Aufgabe konfiguriert. Es werden die für diese Aufgabenart speziellen Einstellungen erläutert, die auf der Registerkarte **Einstellungen** angegeben sind. Auf dieser Registerkarte können Sie folgende Einstellungen festlegen:

- Auf welche Weise die für die Installation des Programms benötigten Dateien auf die Client-Computer gelangen und wie viele Verbindungen höchstens gleichzeitig vorhanden sein dürfen;
- Anzahl der Versuche für die Installation beim zeitplangesteuerten Start der Aufgabe;
- Ob die Anwendung erneut installiert werden soll, wenn sie bereits auf dem Client-Computer installiert ist;
- Ob die laufenden Anwendungen vor der Installation beendet werden müssen;
- Ob vor der Installation des Programms die Version des Betriebssystems auf Kompatibilität mit den Softwarevoraussetzungen für das System geprüft werden muss.

INSTALLATIONSPAKET ERSTELLEN

Vor der Erstellung des Installationspakets müssen die Programmdateien von Kaspersky Endpoint Security vorbereitet werden.

➤ *Gehen Sie folgendermaßen vor, um Kaspersky Endpoint Security zum Installieren vorzubereiten:*

1. Entpacken Sie das Archiv kes4lwks-rpm.tar.gz oder kes4lwks-deb.tar.gz (abhängig vom Paket-Manager, der im Betriebssystem des geschützten Servers verwendet wird) im Ordner, der für den Administrationsserver von Kaspersky Administration Kit verfügbar ist.
2. Kopieren Sie das Paket kes4lwks-<Versionsnummer>.i386.rpm oder kes4lwks-<Versionsnummer>_i386.deb in den gleichen Ordner (abhängig vom Paket-Manager, der im Betriebssystem des geschützten Computers verwendet wird).

➤ *Um ein Installationspaket zu erstellen, gehen Sie wie folgt vor:*

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur den Ordner **Datenverwaltung** → **Installationspakete** aus.
3. Wählen Sie im Kontextmenü den Befehl **Neu** → **Installationspaket** oder im Menü **Aktion** die gleichnamige Option aus.

Daraufhin wird der Assistent für die Erstellung eines Installationspakets aufgerufen. Befolgen Sie die Anweisungen.

SCHRITTE DES ASSISTENTEN

Schritt 1. Namen des Installationspakets festlegen	20
Schritt 2. Lieferumfang des Programms auswählen	20
Schritt 3. Laden des Installationspakets	21
Schritt 4. Aufgabeneinstellungen für den Echtzeitschutz anpassen	21
Schritt 5. Sonstige Einstellungen der Updateaufgabe konfigurieren	21
Schritt 6. Erstellen des Installationspakets abschließen	22

SCHRITT 1. NAMEN DES INSTALLATIONSPAKETS FESTLEGEN

Geben Sie in das Feld **Name** den Namen des Installationspakets ein.

SCHRITT 2. LIEFERUMFANG DES PROGRAMMS AUSWÄHLEN

In diesem Fenster können Sie das Programm für die Installation festlegen.

Wählen Sie in der Liste die Variante **Installationspaket für Kaspersky-Lab-Anwendung anlegen**. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie die Datei mit Erweiterung .kpd aus. Daraufhin werden die Felder mit dem Namen und der Versionsnummer des Programms automatisch ausgefüllt.

Die Parameter des Installationspakets werden standardmäßig angelegt und passen zu dem Programm, das installiert werden soll. Sie können diese Einstellungen nach dem Anlegen des Pakets im Eigenschaftfenster ändern (s. S. [22](#)).

SCHRITT 3. LADEN DES INSTALLATIONSPAKETS

Um das erstellte Installationspaket auf den Administrationsserver zu laden, klicken Sie auf **Weiter**.

SCHRITT 4. AUFGABENEINSTELLUNGEN FÜR DEN ECHTZEITSCHUTZ ANPASSEN

Als nächstes können Sie die Kompilierung des Kernel-Moduls des Betriebssystems vornehmen. Das für die permanente Virenschutz-Funktion erforderliche Modul wird kompiliert. Sie können eine der folgenden Varianten auswählen:

- **Das Modul Echtzeitschutz nicht kompilieren;**
- **Das Modul kompilieren und automatisch nach Quellcodes suchen:** dabei werden die Kernel-Quellcodes automatisch gesucht;
- **Das Modul kompilieren und den Pfad der Quellcodes angeben:** dabei muss der vollständige Pfad der Kernel-Quellcodes des Betriebssystems manuell angegeben werden (Beispiel: */lib/modules/2.6.27.39-0.2-default*). Klicken Sie auf die Schaltfläche **Erweitert**, um den vollständigen Pfad des Kernel-Quellcodes anzugeben.

In diesem Schritt können Sie außerdem die Einstellungen für die Integration mit dem Samba-Server festlegen. Sie können eine der folgenden Varianten auswählen:

- **Samba-Abfangmodul nicht installieren;**
- **Automatische Integration mit dem Samba-Server:** dabei erfolgt die Integration von Kaspersky Endpoint Security mit dem Samba-Server automatisch;
- **Integration mit dem Samba-Server, Parameter manuell angeben:** Dabei müssen Sie die Einstellungen für die Integration mit dem Samba-Server manuell angeben. Klicken Sie auf die Schaltfläche **Erweitert**, um zusätzliche Einstellungen für die Integration mit dem Samba-Server festzulegen:
 - Den vollständigen Pfad zur Konfigurationsdatei des Samba-Servers (Beispiel: */etc/samba/smb.conf*);
 - Das Verzeichnis für das Samba-VFS-Modul (Beispiel: */usr/lib/samba/vfs*);
 - Den Namen des zu installierenden VFS-Moduls (Beispiel: */opt/kaspersky/kes4lwks/lib/samba/kes4lwks-smb-vfs21.so*).

Aktivieren Sie das Kontrollkästchen **Echtzeitschutzaufgabe nach der Installation starten**, wenn Sie möchten, dass die Aufgabe direkt nach der Installation gestartet wird.

SCHRITT 5. SONSTIGE EINSTELLUNGEN DER UPDATEAUFGABE KONFIGURIEREN

In diesem Fenster können Sie die Einstellungen für die Updateaufgaben festlegen. Sie können eine der folgenden Updatequellen auswählen:

- **Nicht ändern;**
- **Administrationsserver von Kaspersky Administration Kit;**
- **Updateserver von Kaspersky Lab;**
- **Andere Updatequellen.**

Klicken Sie dabei auf die Schaltfläche **Erweitert**, um eine benutzerdefinierte Updatequelle einzustellen. Als Updatequelle können HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner dienen.

Aktivieren Sie das Kontrollkästchen **Update nach der Installation starten**, wenn Sie möchten, dass die Updateaufgabe direkt nach der Installation gestartet wird.

SCHRITT 6. ERSTELLEN DES INSTALLATIONSPAKETS ABSCHLIEßEN

Das Installationspaket wird daraufhin erstellt und im Ergebnisbereich im Ordner **Datenverwaltung** → □ **Installationspakete** angezeigt. Sie können die Einstellungen des Installationspakets im entsprechenden Eigenschaftenfenster ändern.

EINSTELLUNGEN DES INSTALLATIONSPAKETS ANZEIGEN UND KONFIGURIEREN

➤ *Um die Einstellungen des Installationspakets anzuzeigen oder zu ändern, gehen Sie wie folgt vor:*

1. Wechseln Sie in der Administrationskonsole in den Ordner **Datenverwaltung** → **Installationspakete**.
2. Wählen Sie im Ergebnisbereich das Installationspaket der gewünschten Anwendung aus.
3. Wählen Sie im entsprechenden Kontextmenü den Befehl **Eigenschaften** oder im Menü **Aktion** die gleichnamige Option aus.
4. Daraufhin wird das Fenster **Eigenschaften <Name des Installationspakets>** geöffnet, das die folgenden Registerkarten enthält: **Allgemein**, **Echtzeitschutz**, **Update** und **Lizenz**.

Die Registerkarte **Allgemein** enthält allgemeine Informationen zum Paket. Dazu gehören folgende Daten:

- Name des Installationspakets (kann bei Bedarf geändert werden).
- Name und Version der Anwendung, für deren Installation das Paket erstellt wurde.
- Paketgröße.
- Erstellungsdatum.
- Pfad zum Speicherort des Installationspakets.

Die Registerkarte **Echtzeitschutz** enthält Einstellungen der Aufgabe zum Echtzeitschutz: Einstellungen für die Kompilierung des Kernel-Moduls des Betriebssystems, das für die permanente Virenschutz-Funktion erforderlich ist, und Einstellungen für die Integration mit dem Samba-Server. Diese Einstellungen werden bei der Erstellung eines Installationspakets festgelegt (s. Abschnitt „Installationspaket erstellen“[20](#) auf S.). Bei Bedarf können Sie sie ändern.

Die Registerkarte **Update** enthält Einstellungen der Aufgabe zum Update: Updatequelle auswählen und Benutzerdefinierte Updatequellen einstellen. Diese Einstellungen werden bei der Erstellung eines Installationspakets festgelegt (s. Abschnitt „Installationspaket erstellen“ auf S. [20](#)). Bei Bedarf können Sie sie ändern.

Die Registerkarte **Lizenz** enthält allgemeine Informationen über die Lizenz, die der Anwendung entspricht, für deren Installation das Paket erstellt wurde. Auf dieser Registerkarte können Sie eine Schlüsseldatei hinzufügen oder ändern.

ERSTKONFIGURATION VON KASPERSKY ENDPOINT SECURITY

Nachdem Sie Kaspersky Endpoint Security auf dem Server installiert haben, müssen Sie die Erstkonfiguration des Programms vornehmen.

Ohne diese Erstkonfiguration ist Ihr Computer nicht vor Viren geschützt.

Die Erstkonfiguration umfasst eine skriptbasierte Abfolge von Schritten, um die Handhabung durch den Benutzer zu erleichtern. Das Skript für die Erstkonfiguration wird automatisch gestartet, sobald die Installation des Programms auf dem Server abgeschlossen ist. Falls der Programm-Manager Ihres Systems die Ausführung von interaktiven Skripten blockiert, müssen Sie das Skript für die Erstkonfiguration manuell starten.

Nach Abschluss der Erstkonfiguration wird die Echtzeitschutz Aufgabe gestartet. Hierfür müssen Sie vorher folgende Aktionen ausführen:

- Schlüsseldatei installieren,
 - Datenbanken für Kaspersky Endpoint Security herunterladen,
 - Kompilierung des Kernel-Moduls.
- ➡ *Führen Sie folgenden Befehl aus, um das Skript zur Erstkonfiguration von Kaspersky Endpoint Security manuell zu starten:*

für Linux:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl
```

Die erforderlichen Aktionen zum Starten der Echtzeitschutz Aufgabe können Sie über das Steuerungsprogramm von Kaspersky Endpoint Security ausführen. Detaillierte Informationen hierzu finden Sie im "Administratorhandbuch" zu Kaspersky Endpoint Security 8 für Linux.

IN DIESEM ABSCHNITT

Schritt 1. Lizenzvereinbarung durchlesen	24
Schritt 2. Zeichensatz auswählen.....	24
Schritt 3. Schlüsseldatei installieren	25
Schritt 4. Proxyserver-Einstellungen anpassen.....	25
Schritt 5. Datenbanken von Kaspersky Endpoint Security herunterladen	25
Schritt 6. Automatisches Update der Datenbanken aktivieren	26
Schritt 7. Kernel-Modul kompilieren	26
Schritt 8. Mit Samba-Server integrieren	27
Schritt 9. Automatischer Start der grafischen Oberfläche.....	27
Schritt 10. Echtzeitschutzaufgabe starten	28
Schritt 11. Parameter für Administrationsagenten konfigurieren	28
Automatischer Start der Erstkonfiguration.....	28
Erlaubnisregeln in den Systemen SELinux und AppArmor anpassen.....	30

SCHRITT 1. LIZENZVEREINBARUNG DURCHLESEN

In diesem Schritt werden Sie aufgefordert, die Bedingungen des Lizenzvertrags zu akzeptieren oder abzulehnen.

Den Text können Sie über das Dienstprogramm `less` aufrufen. Um im Text zu scrollen, benutzen Sie bitte die Pfeiltasten oder die Tasten **b** (ein Bild zurück) bzw. **f** (ein Bild vor). Das Hilfemenü können Sie mit der Taste **h** aufrufen. Um den Lesemodus zu verlassen, drücken Sie bitte die Taste **q**.

Geben Sie bitte nach Verlassen des Lesemodus **yes** (oder **y**) ein, um die Lizenzvereinbarung zu akzeptieren. Falls Sie die Lizenzvereinbarung nicht akzeptieren möchten, geben Sie bitte **no** (oder **n**) ein.

Akzeptieren Sie die Lizenzvereinbarung nicht, wird die Konfiguration von Kaspersky Endpoint Security sofort abgebrochen.

SCHRITT 2. ZEICHENSATZ AUSWÄHLEN

In diesem Schritt muss der Name der Locale angegeben werden, die bei der Arbeit von Kaspersky Endpoint Security verwendet wird.

Der Zeichensatz wird im Format nach RFC 3066 angegeben.

➤ *Führen Sie folgenden Befehl aus, um die volle Liste der Namen von Zeichensätzen anzuzeigen.*

```
# locale -a
```

Als Standard wird der Zeichensatz **en_US.utf8** verwendet.

SCHRITT 3. SCHLÜSSELDATEI INSTALLIEREN

Als nächstes müssen Sie eine Schlüsseldatei installieren. Die Schlüsseldatei enthält notwendige Informationen zur Überprüfung der Benutzerrechte und der verbleibenden Nutzungsdauer für Kaspersky Endpoint Security.

➔ *Um eine Schlüsseldatei zu installieren,*

geben Sie bitte den Pfad zur gewünschten Schlüsseldatei bzw. den Pfad zum Verzeichnis vor, in dem Ihre Schlüsseldateien gespeichert sind.

Enthält das ausgewählte Verzeichnis mehrere Schlüsseldateien, dann wird die erste Datei installiert, die zu Kaspersky Endpoint Security 8.0 für Linux passt.

Wenn Sie keine Lizenz installieren, ist Ihr Server nicht durch Kaspersky Endpoint Security vor Viren geschützt.

Sie können die Schlüsseldatei auch installieren, ohne das Skript für die Erstkonfiguration zu verwenden. Detaillierte Informationen zur Installation von Schlüsseldateien finden Sie unter "Lizenzverwaltung" im "Administratorhandbuch" zu Kaspersky Endpoint Security 8.0 für Linux.

SCHRITT 4. PROXYSERVER-EINSTELLUNGEN ANPASSEN

Nehmen Sie in diesem Schritt die Einstellungen für den Proxyserver vor. Dies ist erforderlich, wenn der Internetzugang über einen Proxyserver erfolgt. Die Internetverbindung wird zum Herunterladen der Datenbank-Updates für Kaspersky Endpoint Security vom Update-Server benötigt.

➔ *Gehen Sie folgendermaßen vor, um die Proxyserver-Einstellungen anzupassen:*

- Wird für die Internetverbindung ein Proxy-Server verwendet, geben Sie bitte die Adresse des Proxy-Servers in einem der folgenden Formate ein:
 - `IP_Adresse_Proxy_Server:Port`, falls für die Anmeldung am Proxyserver keine Authentifizierung erforderlich ist;
 - `Benutzername:Passwort@IP_Adresse_Proxy_Server:Port`, falls für die Anmeldung am Proxyserver eine Authentifizierung erforderlich ist.
- Wird für die Internetverbindung kein Proxyserver verwendet, so wählen Sie die Antwort **no**.

Standardmäßig ist die Antwort **no** angegeben.

Sie können die Einstellungen für den Proxyserver auch konfigurieren, ohne das Skript für die Erstkonfiguration zu verwenden. Nähere Informationen zum Anpassen der Proxyserver-Einstellungen finden Sie unter "Update von Kaspersky Endpoint Security" im "Administratorhandbuch" zu Kaspersky Endpoint Security 8 für Linux.

SCHRITT 5. DATENBANKEN VON KASPERSKY ENDPOINT SECURITY HERUNTERLADEN

Als nächstes müssen Sie die Antiviren-Datenbanken von Kaspersky Endpoint Security auf den Computer laden. Der Schutz der Daten auf Ihrem Computer wird durch Antiviren-Datenbanken gewährleistet, in welchen die Beschreibungen der Bedrohungssignaturen und Verfahren zu deren Behandlung gespeichert sind. Kaspersky Endpoint Security verwendet diese Antiviren-Datenbanken, um gefährliche Objekte zu identifizieren und unschädlich zu machen. Die Antiviren-Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt.

- *Um die Antiviren-Datenbanken für Kaspersky Endpoint Security auf den Computer zu laden,*
wählen Sie die Antwort **yes**.

Falls Sie die Antiviren-Datenbanken jetzt nicht herunterladen möchten, geben Sie **no** ein.

Standardmäßig ist die Antwort **yes** angegeben.

Wenn die Antiviren-Datenbanken für Kaspersky Endpoint Security nicht heruntergeladen werden, ist der Virenschutz des Computers durch Kaspersky Endpoint Security nicht gewährleistet.

Sie können das Update der Antiviren-Datenbanken von Kaspersky Endpoint Security auch starten, ohne das Skript zu verwenden. Nähere Informationen zum Starten des Antiviren-Datenbank-Updates finden Sie unter "Update von Kaspersky Endpoint Security" im "Administratorhandbuch" zu Kaspersky Endpoint Security 8 für Linux.

SCHRITT 6. AUTOMATISCHES UPDATE DER ANTIVIREN-DATENBANKEN AKTIVIEREN

Als nächstes können Sie das automatische Update für Antiviren-Datenbanken aktivieren.

- *Um das automatische Antiviren-Datenbank-Update zu aktivieren,*
geben Sie bitte **yes** ein.

Standardmäßig werden die Antiviren-Datenbanken für Kaspersky Endpoint Security alle 30 Minuten automatisch aktualisiert.

Sie können das automatische Update für die Antiviren-Datenbanken auch aktivieren, ohne das Skript für die Erstkonfiguration zu verwenden. Nähere Informationen zur Konfiguration von Zeitplänen für das Update der Antiviren-Datenbanken finden Sie in den Abschnitten "Zeitplan-Einstellungen für die Aufgabe anpassen".

SCHRITT 7. KERNEL-MODUL KOMPILIEREN

Als nächstes können Sie die Kompilierung des Kernel-Moduls vornehmen. Das für die permanente Virenschutz-Funktion erforderliche Modul wird kompiliert.

Wenn das Skript im Standardverzeichnis des Betriebssystems Kernel-Quellcodes findet, wird der gefundene Pfad als Standardeinstellung verwendet. Andernfalls werden Sie aufgefordert, den richtigen Pfad des Kernel-Quellcodes einzugeben.

Sie können das Kernel-Modul kompilieren, ohne die vorherigen Schritte des Skripts zu wiederholen.

- *Um die Kompilierung des Kernel-Moduls auszuführen, ohne die Erstkonfiguration zu starten, geben Sie den folgenden Befehl ein:*

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl \  
  
--build=<Pfad des Kernel-Quellcodes>
```

Wenn das Kernel-Modul nicht kompiliert wurde, werden Operationen auf lokalen oder gemounteten Objekten des Computerdateisystems nicht von der Echtzeitschutzaufgabe verarbeitet.

SCHRITT 8. MIT SAMBA-SERVER INTEGRIEREN

Als nächstes erfolgt die Integration mit dem Samba-Server. Hierzu sind folgende Schritte erforderlich:

- Suche nach dem installierten Samba-Server und Prüfung der Version auf Kompatibilität mit dem Programm;
- Suchen und Anpassen der Konfigurationsdatei für den Samba-Server;
- Prüfung der Konfigurationsdatei für den Samba-Server auf eventuell vorhandene VFS-Module.

Enthält die Konfigurationsdatei für den Samba-Server zum Zeitpunkt der Installation von Kaspersky Endpoint Security VFS-Module, so werden diese deaktiviert.

Das Skript für die Erstkonfiguration sucht automatisch nach installierten Samba-Servern. Anschließend werden Sie aufgefordert, den Antivirenschutz für die gefundenen Server automatisch bzw. manuell zu konfigurieren. Geben Sie **Y** ein, um den Schutz für die Samba-Server automatisch zu konfigurieren. Dieser Modus wird standardmäßig verwendet. Geben Sie **N** ein, wenn Sie den Schutz des Samba-Servers manuell konfigurieren möchten.

➤ Um den Schutz für den Samba-Server manuell zu konfigurieren, gehen Sie wie folgt vor:

Wenn Sie als Antwort auf die Anfrage des Erstkonfigurations-Skripts eine Leerzeile eingeben, wird die Konfiguration des Schutzes für Samba-Server abgebrochen.

1. Geben Sie den Pfad zum Verzeichnis mit der Datei `smbd` ein.
2. Geben Sie den Pfad zum Verzeichnis mit der Konfigurationsdatei für den Samba-Server (`smb.conf`) ein.
3. Geben Sie den Pfad zum Verzeichnis mit den VFS-Modulen des Samba-Servers ein.

Nach Abschluss der Integration führen Sie den Neustart des Samba-Servers manuell aus.

Falls nach der Integration mit dem Samba-Server die Echtzeitschutzaufgabe gestoppt wurde, ist der Zugriff auf die Samba-Ressourcen blockiert.

➤ Um zu vermeiden, dass nach dem Anhalten der Echtzeitschutzaufgabe der Zugriff auf Samba-Ressourcen blockiert wird,

fügen Sie dem Abschnitt `[global]` der Konfigurationsdatei `/etc/samba/smb.conf` folgende Zeile hinzu:

```
kavsamba:access_on_error = yes
```

Sie können eine Integration mit dem Samba-Server ausführen, ohne die vorherigen Schritte des Skripts zu wiederholen.

➤ Um die Kompilierung des Kernel-Moduls auszuführen, ohne die Erstkonfiguration zu starten, geben Sie folgenden Befehl ein:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl --samba
```

SCHRITT 9. AUTOMATISCHER START DER GRAFISCHEN OBERFLÄCHE

Legen Sie nun fest, ob die grafische Benutzeroberfläche beim Systemstart automatisch gestartet werden soll.

- *Damit die grafische Oberfläche beim Systemstart automatisch gestartet wird,*
wählen Sie die Antwort **yes**.

Wenn beim Systemstart kein automatischer Start der grafischen Oberfläche erfolgen soll, wählen Sie **no**.

Standardmäßig ist die Antwort **yes** angegeben.

SCHRITT 10. ECHTZEITSCHUTZAUFGABE STARTEN

Als nächstes wird die Echtzeitschutzaufgabe gestartet, sofern vorher folgende Aktionen ausgeführt wurden:

- Installation einer Lizenz;
- Download der Antiviren-Datenbanken für Kaspersky Endpoint Security;
- Kompilierung der Kernel-Module oder Integration mit dem Samba-Server.

Detaillierte Informationen zur Verwaltung von Aufgaben finden Sie im Abschnitt "Aufgabenverwaltung" des "Administratorhandbuchs" zu Kaspersky Endpoint Security 8.0 für Linux.

SCHRITT 11. EINSTELLUNGEN FÜR ADMINISTRATIONSAGENTEN KONFIGURIEREN

Wenn Sie Kaspersky Endpoint Security mit Hilfe des Kaspersky Administration Kit verwalten wollen, müssen Sie die Einstellungen für den Administrationsagenten anpassen. Dieser Prozess wird über ein spezielles Skript ausgeführt.

- *Führen Sie folgenden Befehl aus, um das Skript zur Konfiguration des Administrationsagenten zu starten:*

```
# /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl
```

Während der Ausführung des Skripts werden Sie aufgefordert, folgende Eingaben zu machen:

1. DNS-Namen oder IP-Adresse des Administrationsservers.
2. Port-Adresse des Administrationsservers oder den standardmäßigen Port (14000).
3. SSL-Port-Adresse des Administrationsservers oder den standardmäßigen Port (13000).
4. SSL-Verbindung zur Datenübertragung verwenden/nicht verwenden. Standardmäßig ist die SSL-Verbindung aktiviert.

Nähere Informationen zur Konfiguration des Network Agent finden Sie im "Administratorhandbuch" für Kaspersky Administration Kit.

AUTOMATISCHER START DER ERSTKONFIGURATION

Die Erstkonfiguration von Kaspersky Endpoint Security kann automatisch erfolgen.

- *Um die Erstkonfiguration im Automatikmodus zu starten, führen Sie folgenden Befehl aus::*

Für Linux:

```
/opt/kaspersky/kes4lwks/bin/kes4lwks-setup.pl \
```

--auto-install=<vollständiger Pfad der Konfigurationsdatei für die Erstkonfiguration>

Für FreeBSD:

/usr/local/bin/kes4lwks-setup.pl \

--auto-install=<vollständiger Pfad der Konfigurationsdatei für die Erstkonfiguration>

Die folgende Tabelle enthält die Parameter der Konfigurationsdatei für die Erstkonfiguration.

Tabelle 2. Parameter der Konfigurationsdatei für die Erstkonfiguration

PARAMETER	BESCHREIBUNG	MÖGLICHE WERTE
EULA_AGREED	Obligatorischer Parameter. Zustimmung zu den Bedingungen des Lizenzvertrags	yes
SERVICE_LOCALE	Zeichensatz, der bei der Arbeit von Kaspersky Endpoint Security verwendet wird.	Locale im Format, das dem RFC 3066 entspricht.
INSTALL_KEY_FILE	Vollständiger Pfad der Schlüsseldatei	
UPDATER_SOURCE	Updatequelle	<ul style="list-style-type: none"> • AKServer – den Administrationsserver von Kaspersky Administration Kit als Updatequelle verwenden; • KLServers – die Kaspersky-Lab-Updateserver als Updatequelle verwenden; • URL des Updateservers;
UPDATER_PROXY	Adresse des Proxyserver, der für eine Internetverbindung verwendet wird.	<ul style="list-style-type: none"> • URL des Proxyserver; • no – keinen Proxyserver verwenden;
UPDATER_EXECUTE	Start der Aufgabe zum Datenbank-Update während des Konfigurationsvorgangs	<ul style="list-style-type: none"> • yes – Updateaufgabe starten; • no – Updateaufgabe nicht starten;
UPDATER_ENABLE_AUTO	Automatischen Start der Aufgabe zum Datenbank-Update aktivieren / deaktivieren.	<ul style="list-style-type: none"> • yes – automatischen Start der Updateaufgabe aktivieren; • no – automatischen Start der Updateaufgabe deaktivieren;
RTP_BUILD_KERNEL_MODULE	Obligatorischer Parameter. Start der Kompilation des Kernel-Moduls	<ul style="list-style-type: none"> • yes – Kernel-Modul kompilieren; • no – Kernel-Modul nicht kompilieren;
RTP_BUILD_KERNEL_SRCS	Pfad des Kernel-Quellcodes	<ul style="list-style-type: none"> • auto – automatische Suche; • Pfad des Quellcode;

PARAMETER	BESCHREIBUNG	MÖGLICHE WERTE
RTP_SAMBA_ENABLE	Obligatorischer Parameter. Mit Samba-Server integrieren	<ul style="list-style-type: none"> • yes – unter Verwendung der Parameterwerte RTP_SAMBA_CONF, RTP_SAMBA_VFS, RTP_SAMBA_VFS_MODULE integrieren; • no – nicht integrieren; • auto – Pfade der Samba-Server-Komponenten automatisch ermitteln;
RTP_SAMBA_CONF	Vollständiger Pfad der Konfigurationsdatei des Samba-Servers (<i>smb.conf</i>)	
RTP_SAMBA_VFS	Vollständiger Pfad des Verzeichnisses mit den VFS-Modulen des Samba-Servers	
RTP_SAMBA_VFS_MODULE	Vollständiger Pfad des VFS-Moduls von Kaspersky Endpoint Security, das als Modul-Handler installiert wird.	
RTP_START	Start der Echtzeitschutzaufgabe nach Abschluss der Konfiguration	<ul style="list-style-type: none"> • yes – Echtzeitschutzaufgabe starten; • no – Echtzeitschutzaufgabe nicht starten;
GUI_ENABLE	Automatischer Start der grafischen Oberfläche bei der Anmeldung im System.	<ul style="list-style-type: none"> • yes – grafische Oberfläche automatisch starten; • no – grafische Oberfläche nicht automatisch starten;

Geben Sie den Parameterwert im Format **Parametername=Wert** an (Leerzeichen im Namen und in den Werten eines Parameters werden nicht verarbeitet).

ERLAUBNISREGELN IN DEN SYSTEMEN SELINUX UND APPARMOR ANPASSEN

Kaspersky Endpoint Security ist nicht kompatibel mit SELinux und Novell AppArmor.

➤ Um SELinux in den Permissive-Modus umzuschalten, führen Sie folgenden Befehl aus:

```
# setenforce Permissive
```

➤ Um alle Regeln für AppArmor in den „schonenden“ Modus umzuschalten, führen Sie die folgenden Befehle aus:

```
# aa-complain /etc/apparmor.d/*
```

```
# /etc/init.d/apparmor reload
```

KASPERSKY ENDPOINT SECURITY DEINSTALLIEREN

Falls Sie Dateien aus der Quarantäne wiederherstellen möchten, müssen Sie dies vor der Deinstallation von Kaspersky Endpoint Security tun. Andernfalls können Dateien aus der Quarantäne nicht wiederhergestellt werden.

- Um Kaspersky Endpoint Security, das aus einem rpm-Paket installiert wurde, zu deinstallieren, führen Sie folgenden Befehl aus:

```
# rpm -e kes4lwks
```

- Um Kaspersky Endpoint Security, das aus einem deb-Paket installiert wurde, zu deinstallieren, führen Sie folgenden Befehl aus:

```
# dpkg -r kes4lwks
```

- Um die Anwendung auf einem Computer mit FreeBSD-Betriebssystem zu deinstallieren, führen Sie folgenden Befehl aus:

```
# pkg_delete kes4lwks
```

Dabei werden sämtliche Aufgaben von Kaspersky Endpoint Security beendet.

- Um den Administrationsagenten zu deinstallieren, wenn er aus einem .rpm-Paket installiert wurde, führen Sie folgenden Befehl aus:

```
# rpm -e klnagent
```

- Um den Administrationsagenten zu deinstallieren, wenn er aus einem .deb-Paket installiert wurde, führen Sie folgenden Befehl aus:

```
# dpkg -r klnagent
```

Die Deinstallation erfolgt automatisch. Nach Abschluss des Vorgangs erhalten Sie eine entsprechende Meldung über die Konsole.

REMOTE-DEINSTALLATION VON KASPERSKY ENDPOINT SECURITY

Die Remote-Deinstallation von Kaspersky Endpoint Security mit Hilfe des Kaspersky Administration Kit erfolgt über das Starten der Aufgabe zur Remote-Deinstallation.

◆ *Gehen Sie folgendermaßen vor, um die Aufgabe zur Remote-Deinstallation von Kaspersky Endpoint Security zu erstellen:*

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben für eine Zusammenstellung von Computern** aus.
3. Wählen Sie im entsprechenden Kontextmenü den Punkt **Neu** → **Aufgabe** oder im Menü **Aktion** die gleichnamige Option aus.

Daraufhin wird der Assistent für die Erstellung einer Aufgabe gestartet.

4. Geben Sie im Fenster **Aufgabenname** im Feld **Name** einen Namen für die Aufgabe ein.
5. Wählen Sie im Fenster **Aufgabentyp** die Anwendung **Kaspersky Administration Kit** aus, öffnen Sie den Unterordner **Erweitert**, und klicken Sie auf **Remote-Deinstallation der Anwendung**.
6. Geben Sie im Fenster **Einstellungen** die Anwendung an, die deinstalliert werden soll. Wählen Sie dazu in der Dropdown-Liste **Anwendung deinstallieren, die von Kaspersky Administration Kit unterstützt** wird die Variante **Kaspersky Endpoint Security 8 für Linux**.
7. Im Fenster **Typ der Remote-Deinstallation** wählen Sie die Variante **Erzwungene Deinstallation** aus.
8. Im Fenster **Einstellungen** im Block **Laden des Deinstallationstools erzwingen** aktivieren Sie das Kontrollkästchen **Mit Hilfe des Administrationsagenten**.
9. Beenden Sie das Erstellen der Aufgabe analog zur Aufgabe Remote-Installation (s. S. [15](#)).

Die angelegte Aufgabe wird je nach dem eingestellten Zeitplan aufgerufen.

◆ *Gehen Sie folgendermaßen vor, um die Aufgabe zur Remote-Deinstallation von Kaspersky Endpoint Security manuell zu starten:*

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie in der Konsolenstruktur den Ordner **Aufgaben für eine Zusammenstellung von Computern** aus.
3. Wählen Sie im Ergebnisbereich die gewünschte Aufgabe aus.
4. Wählen Sie im entsprechenden Kontextmenü den Befehl **Start** oder im Menü **Aktion** die gleichnamige Option aus.

AKTIONEN NACH DER DEINSTALLATION VON KASPERSKY ENDPOINT SECURITY

Nach der Deinstallation von Kaspersky Endpoint Security (s. S. [31](#)) bleiben folgende Informationen auf dem Computer gespeichert:

- Antiviren-Datenbanken von Kaspersky Endpoint Security;
- Datenbanken des Lizenz-Verzeichnisse;
- Datenbanken des Ereignis-Verzeichnisses;
- Datenbanken mit den Funktionseinstellungen für Kaspersky Endpoint Security;
- Dateien im Backup- und Quarantäne-Speicher;
- Protokolldateien.

Kaspersky Endpoint Security bietet Skripts, mit denen die nach der Deinstallation verbleibenden Dateien und Verzeichnisse vom Computer gelöscht werden können.

➡ *Gehen Sie wie folgt vor, um diese Skripts zu starten:*

1. Führen Sie folgenden Befehl aus:
 - für Linux: # `/var/opt/kaspersky/kes4lwks/cleanup.sh`
 - für FreeBSD: # `/var/db/kaspersky/kav4fs/cleanup.sh`
2. Geben Sie **yes** ein, um das Löschen der nach der Deinstallation von Kaspersky Endpoint Security verbliebenen Dateien zu bestätigen. Um das Löschen der Daten zu verhindern und das Skript anzuhalten, geben Sie **no** ein.

FUNKTIONSPRÜFUNG FÜR AUFGABEN ZUM ECHTZEITSCHUTZ UND VIRENSUCHE

Nach der Installation und Erstkonfiguration des Programms können Sie überprüfen, ob die Aufgaben für Echtzeitschutz und Virensuche ordnungsgemäß konfiguriert sind.

IN DIESEM ABSCHNITT

Funktionsprüfung für Echtzeitschutzaufgabe	34
Funktionsprüfung für Untersuchungsaufgabe	35
EICAR-Testvirus und seine Modifikationen	35

FUNKTIONSPRÜFUNG FÜR ECHTZEITSCHUTZAUFGABE

Dieser Abschnitt beschreibt, wie Sie überprüfen können, ob das Programm über die Echtzeitschutzaufgabe bei Zugriffsversuchen infizierte und verdächtige Objekte identifiziert und die für solche Objekte anhand der Aufgabeneinstellungen definierten Aktionen ordnungsgemäß ausführt.

➔ *Gehen Sie folgendermaßen vor, um die korrekte Funktion der Echtzeitschutzaufgabe zu überprüfen:*

1. Laden Sie die Datei *eicar.com* von der entsprechenden Seite der EICAR-Homepage http://www.eicar.org/anti_virus_test_file.htm herunter. Speichern Sie die Datei auf dem Computer.

Um zu prüfen, ob das Programm auch verdächtige Objekte richtig identifiziert, müssen Sie in der Textzeile den Präfix *SUSP-* hinzufügen (nähere Informationen hierzu finden Sie im Abschnitt "EICAR-Testvirus und seine Modifikationen").

2. Falls die Echtzeitschutzaufgabe gestoppt ist, führen Sie folgenden Befehl aus, um die Aufgabe erneut zu starten:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-control --start-task 8
```

3. Öffnen Sie die Datei *eicar.com* im Lesemodus mit dem Befehl:

```
# cat <vollständiger_Pfad_zu_eicar.com>
```

4. Kaspersky Endpoint Security fängt den Zugriff auf die Datei ab, untersucht sie und verweigert den Zugriff darauf. In der Konsole erscheint hierbei folgende Meldung:

```
"cat: <vollständiger_Pfad_zu_eicar.com>: Permission denied"
```

5. Führen Sie folgenden Befehl aus:

```
# echo $?
```

Wird nach Ausführung des Befehls ein Wert verschieden von Null angezeigt, bedeutet dies, dass der Zugriffsversuch auf die Datei *eicar.com* durch die Echtzeitschutzaufgabe erfolgreich verarbeitet wurde.

FUNKTIONSPRÜFUNG FÜR UNTERSUCHUNGSAUFGABE

Dieser Abschnitt beschreibt, wie Sie überprüfen können, ob Kaspersky Endpoint Security beim Ausführen einer Untersuchungsaufgabe infizierte und verdächtige Objekte in den ausgewählten Untersuchungsbereichen erfolgreich identifiziert und die für die Aufgabe definierten Aktionen für solche Objekte ordnungsgemäß ausführt.

Sie können die Funktion "Virensuche" bei der Ausführung sowohl der standardmäßig voreingestellten Aufgabe **Vollständige Untersuchung des Computers** als auch einer beliebigen benutzerdefinierten Untersuchungsaufgabe prüfen.

Hierzu müssen Sie die Datei *eicar.com* auf dem betreffenden Computer speichern.

➤ *Gehen Sie folgendermaßen vor, um die korrekte Funktion einer Untersuchungsaufgabe zu überprüfen:*

1. Stoppen Sie die Aufgabe zum Echtzeitschutz mit folgendem Befehl:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-control --stop-task 8
```

2. Laden Sie die Datei *eicar.com* von der entsprechenden Website auf der EICAR-Homepage herunter: http://www.eicar.org/anti_virus_test_file.htm, und speichern Sie die Datei auf dem Computer.

Während der Untersuchung wird die Datei vom Programm als **Infiziert** gekennzeichnet, wenn Sie keine Änderungen an der Datei *eicar.com* vornehmen. Die Datei erhält vom Programm den Status **Verdächtig**, wenn Sie in der Textzeile der Datei *eicar.com* den Präfix **SUSP-** einfügen (genauere Informationen hierzu finden Sie im Abschnitt "EICAR-Testvirus und seine Modifikationen" (s. S. 35)).

3. Erstellen Sie eine Untersuchungsaufgabe, indem Sie folgenden Befehl ausführen:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-control \  
--create-task <Aufgabenname> --use-task-type=ODS
```

Die Aufgaben-ID wird in der Konsole angezeigt.

4. Fügen Sie das Verzeichnis, in dem sich die Datei *eicar.com* befindet, über folgenden Befehl zum Untersuchungsbereich für die neu erstellte Aufgabe hinzu:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-control \  
--set-settings <Aufgaben-ID> \  
ScanScope.AreaPath.Path=<Pfad_zum_Verzeichnis_von_eicar.com>
```

5. Starten Sie die neu erstellte Aufgabe über folgenden Befehl:

```
# /opt/kaspersky/kes4lwks/bin/kes4lwks-control \  
--start-task <ID_der_neuen_Aufgabe> -W
```

6. Das Ergebnis der Ausführung können Sie über die Konsole prüfen.

Wenn die Datei *eicar.com* vom Computer entfernt wurde, ist die Untersuchungsaufgabe richtig konfiguriert (sofern in den Aufgabeneinstellungen **Desinfizieren, falls nicht möglich** - Löschen als Aktion für infizierte Objekte eingestellt ist).

EICAR-"TESTVIRUS" UND SEINE MODIFIKATIONEN

Der "Testvirus" dient lediglich zur Funktionsprüfung für Virenschutzprogramme. Er wurde vom European Institute for Computer Anti-Virus Research (EICAR) entwickelt.

Der "Testvirus" ist kein schädliches Programm. Er enthält keine Programmcodes, die potenziell Ihren Computer gefährden könnten; die Virenschutzprogramme der meisten Anbieter identifizieren ihn jedoch als potenzielle Bedrohung.

Der Name der Datei mit dem "Testvirus" ist eicar.com. Diese Datei können Sie von der offiziellen Homepage des EICAR unter http://www.eicar.org/anti_virus_test_file.htm herunterladen.

Bevor Sie die Datei in einem Verzeichnis auf dem Computer speichern, überzeugen Sie sich, dass der permanente Virenschutz für dieses Verzeichnis deaktiviert ist.

Die Datei eicar.com enthält eine Textzeile. Während der Untersuchung der Datei identifiziert Kaspersky Endpoint Security in dieser Textzeile eine "Bedrohung", kennzeichnet die Datei als **Infiziert** und führt die durch die Aufgabeneinstellungen vorgegebene Aktion aus.

Mit der Datei eicar.com können Sie auch die ordnungsgemäße Funktion des Programms beim Auffinden anderer Dateitypen prüfen. Öffnen Sie hierzu die Datei mit einem Textverarbeitungsprogramm, fügen Sie in der Datei eines der unten aufgeführten Präfixe hinzu, und speichern Sie die Datei unter einem anderen Namen.

Tabelle 3. Präfixe

PRÄFIX	STATUS DER DATEI NACH DER UNTERSUCHUNG UND AKTIONEN VON KASPERSKY ENDPOINT SECURITY
Ohne Präfix	Kaspersky Endpoint Security ordnet dem Objekt den Status Infiziert zu.
WARN-	Kaspersky Endpoint Security ordnet dem gefundenen Objekt den Status Warnung zu (der Code des Objekts stimmt teilweise mit dem Code einer bekannten Bedrohung).
ERRO-	Bei der Untersuchung des Objekts ist ein Fehler aufgetreten. Die Anwendung erhielt keinen Zugriff auf das Objekt: Die Integrität des Objekts ist beschädigt (z. B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird).
SUSP-	Kaspersky Endpoint Security kennzeichnet die Objekte als Verdächtig (auf Grund der heuristischen Untersuchung).
CURE-	Kaspersky Endpoint Security kennzeichnet die Objekte als Infiziert und versucht eine Desinfektion. Nach erfolgreicher Desinfektion wird der Virenkörper durch das Wort "CURE" ersetzt.
CORR-	Kaspersky Endpoint Security ordnet dem Objekt den Status Beschädigt zu.

DATEISTRUKTUR VON KASPERSKY ENDPOINT SECURITY

Nach der Installation von Kaspersky Endpoint Security auf einer Linux-Workstation sind die Programmdateien standardmäßig wie folgt angeordnet:

/opt/kaspersky/kes4lwks/ – Hauptverzeichnis von Kaspersky Endpoint Security mit folgenden Unterverzeichnissen:

bin/ – Verzeichnis der ausführbaren Dateien für sämtliche Programmkomponenten von Kaspersky Endpoint Security:

kes4lwks-control – ausführbare Datei für die Verwaltungskomponente für Kaspersky Endpoint Security;

kes4lwks-qtgui – ausführbare Datei der grafischen Oberfläche;

kes4lwks-setup.pl – Skript für die Erstkonfiguration nach Installation von Kaspersky Endpoint Security.

lib/ – Speicherverzeichnis für Zusatzmodule von Kaspersky Endpoint Security:

samba/ – Speicherverzeichnis für die kompilierten Samba-Module.

lib64/ – Speicherverzeichnis für Zusatzmodule der 64-Bit-Module von Kaspersky Endpoint Security:

samba/ – Speicherverzeichnis für die kompilierten 64-Bit-Samba-Module.

libexec/ – Speicherverzeichnis für Dienstdateien von Kaspersky Endpoint Security;

src/ – Speicherverzeichnis für Quellcodes der Module von Kaspersky Endpoint Security:

kernel/ – Speicherverzeichnis für Bibliotheken des Kernels von Kaspersky Endpoint Security;

samba/ – Speicherverzeichnis für Bibliotheken des Samba-Moduls von Kaspersky Endpoint Security.

/opt/kaspersky/kes4lwks/share/doc/ – Dokumentation von Kaspersky Endpoint Security:

LICENSE – Lizenzvereinbarung.

LICENSE.GPL – Lizenzvereinbarung für Kernel-Modul und Samba-Modul.

/opt/kaspersky/kes4lwks/share/man/ – Speicherverzeichnis für man-Dateien.

/etc/init.d/ – Verzeichnis für Verwaltungsskript für den Dienst Kaspersky Lab Framework:

kav4fs-supervisor – Verwaltungsskript für den Dienst Kaspersky Lab Framework.

/etc/opt/kaspersky/ – Verzeichnis für die Konfigurationsdatei für Kaspersky Lab Framework:

kes4lwks-supervisor.conf – Konfigurationsdatei für Kaspersky Lab Framework.

/var/opt/kaspersky/kes4lwks/ – Verzeichnis für Daten von Kaspersky Endpoint Security:

db/ – Datenbanken für Kaspersky Endpoint Security;

update/ – Speicherverzeichnis für Updates von Kaspersky Endpoint Security;

quarantine/ – Quarantänespeicher.

/var/log/kaspersky/kes4lwks/ – Speicherverzeichnis für Log-Dateien von Kaspersky Endpoint Security;

/var/run/kes4lwks/ – Speicherverzeichnis für Dienstdateien von Kaspersky Endpoint Security.

Zur Verbindung mit dem Hilfesystem von Kaspersky Endpoint Security (manual pages) fügen Sie in der Konfigurationsdatei *snmpd.conf* folgende Zeile hinzu:

```
MANPATH="$MANPATH:/opt/kaspersky/kes4lwks/share/man/:"  
export MANPATH
```

KASPERSKY LAB

Die Firma Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Die Zentrale befindet sich in Russland, es gibt Niederlassungen in Großbritannien, Frankreich, Deutschland, Japan, in den Benelux-Ländern, China, Polen, Rumänien und in den USA (Kalifornien). In Frankreich wurde eine neue Tochtergesellschaft gegründet, das Europäische Zentrum für Antiviren-Forschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Unternehmen.

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

Das größte Kapital des Unternehmens sind das einzigartige Wissen und die Erfahrung, die die Mitarbeiter im Laufe des mehr als vierzehnjährigen ununterbrochenen Kampfes gegen Viren gesammelt haben. Dank der ständigen Analyse von Virenaktivitäten können wir Tendenzen bei der Malware-Entwicklung vorhersagen und frühzeitig Benutzern einen zuverlässigen Schutz vor neuen Angriffen an die Hand geben. Dieser Vorteil manifestiert sich in den Erzeugnissen und Leistungen von Kaspersky Lab. Wir sind unseren Wettbewerbern stets einen Schritt voraus und bieten unseren Kunden den besten Schutz.

Aufgrund der jahrelangen Tätigkeit wurde das Unternehmen zum führenden Entwickler von Technologien zum Schutz vor Viren. Viele moderne Standards für Virenschutzprogramme wurden erstmals von Kaspersky Lab entwickelt. Die Basis-Software des Unternehmens heißt Kaspersky Anti-Virus und sie sorgt für einen zuverlässigen Schutz aller Objekte vor Virenangriffen: Arbeitsstationen, Dateiserver, Mail-Systeme, Firewalls und Internet-Gateways sowie Taschencomputer. Bequeme Steuerelemente versetzen die Benutzer in die Lage, den Antivirenschutz von Computern und Unternehmensnetzwerken maximal zu automatisieren. Viele internationale Developer verwendeten in ihrer Software den Kernel von Kaspersky Anti-Virus, beispielsweise: Nokia ICG (USA), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab erhalten ein breites Spektrum zusätzlicher Dienstleistungen, welche die störungsfreie Funktion der Produkte und die präzise Abstimmung auf spezifische Anforderungen garantieren. Wir projektieren, realisieren und begleiten Antiviren-Komplettlösungen von Unternehmen. Unsere Datenbanken werden stündlich aktualisiert. Wir haben für unsere Benutzer einen technischen Kundendienst in mehreren Sprachen eingerichtet.

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir beraten Sie gern detailliert über das Telefon oder E-Mail. Auf Ihre Fragen bekommen Sie eine vollständige und erschöpfende Antwort.

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

Viren-Enzyklopädie: <http://www.securelist.com/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 Virenanalytiker)