

Kaspersky Endpoint Security 10 Maintenance Release 1 für Windows

Build 10.2.1.23, 12.12.2013

Kaspersky Endpoint Security 10 für Windows (im Folgenden auch "Programm" oder "Kaspersky Endpoint Security" genannt) ist eine universelle Lösung, mit der Benutzer in Unternehmen vor Informationsbedrohungen geschützt werden.

MINDESTKONFIGURATION

Um die normale Funktionsfähigkeit des Programms zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Allgemeine Anforderungen:

- Prozessor Intel Pentium 1 GHz und höher
- 1 GB Arbeitsspeicher
- 2 GB freier Speicherplatz auf der Festplatte
- Microsoft Internet Explorer 7.0 und höher
- Microsoft Windows Installer 3.0 und höher
- Internetverbindung für die Aktivierung des Programms, Update der Datenbanken und Programm-Module

Zur vollständigen Datenträgerverschlüsselung von Geräten sind für den Authentifizierungsagenten im konventionellen Arbeitsspeicher des Computers (conventional memory) mindestens 60416 Byte erforderlich. Diese Voraussetzung wird vor dem Start der vollständigen Datenträgerverschlüsselung der Geräte automatisch überprüft. Ausführliche Informationen finden Sie über folgenden Link:

<http://support.kaspersky.com/de/9992>

Betriebssysteme:

- Microsoft Windows 8.1 Enterprise x86 / x64
- Microsoft Windows 8 Pro x86 / x64
- Microsoft Windows 8 Enterprise x86 / x64
- Microsoft Windows 7 Professional x86 / x64 SP1 und höher
- Microsoft Windows 7 Enterprise / Ultimate x86 / x64 SP1 und höher
- Microsoft Windows 7 Professional x86 / x64
- Microsoft Windows 7 Enterprise / Ultimate x86 / x64
- Microsoft Windows Vista x86 / x64 SP2 und höher
- Microsoft Windows XP Professional x86 SP3 und höher
- Windows Embedded POSReady 7 x86 / x64 (Die Funktionalität zur Verschlüsselung von Dateien (FLE) und von Festplatten (FDE) wird nicht unterstützt).
- Windows Embedded Standard 7 mit SP1 x86 / x64 (Die Funktionalität zur Verschlüsselung von Dateien (FLE) und von Festplatten (FDE) wird nicht unterstützt).

- Microsoft Small Business Server 2011 Essentials x64
- Microsoft Small Business Server 2011 Standard x64

- Microsoft Small Business Server 2008 Standard x64
- Microsoft Small Business Server 2008 Premium x64
- Microsoft Windows Server 2012 R2 Standard x64 (Die Konfigurationen Server Core und Cluster Mode werden nicht unterstützt, das Dateisystem ReFS wird mit Einschränkungen unterstützt).
- Microsoft Windows Server 2012 Foundation x64 (Das Dateisystem ReFS sowie die Konfigurationen Server Core und Cluster Mode werden nicht unterstützt).
- Microsoft Windows Server 2012 Essentials x64 (Das Dateisystem ReFS sowie die Konfigurationen Server Core und Cluster Mode werden nicht unterstützt).
- Microsoft Windows Server 2012 Standard x64 (Das Dateisystem ReFS sowie die Konfigurationen Server Core und Cluster Mode werden nicht unterstützt).
- Microsoft Windows MultiPoint Server 2011 x64
- Microsoft Windows Server 2008 R2 Standard x64 SP1 und höher
- Microsoft Windows Server 2008 R2 Standard x64
- Microsoft Windows Server 2008 R2 Enterprise x64 SP1 und höher
- Microsoft Windows Server 2008 R2 Enterprise x64
- Microsoft Windows Server 2008 R2 Foundation x64 SP1 und höher
- Microsoft Windows Server 2008 R2 Foundation x64
- Microsoft Windows Server 2008 Standard x86 / x64 SP2 und höher
- Microsoft Windows Server 2008 Enterprise x86 / x64 SP2 und höher
- Microsoft Windows Server 2003 R2 Standard x86 / x64 SP2 und höher
- Microsoft Windows Server 2003 R2 Enterprise x86 / x64 SP2 und höher
- Microsoft Windows Server 2003 Standard x86 / x64 SP2
- Microsoft Windows Server 2003 Enterprise x86 / x64 SP2 und höher

INSTALLATION

Um das Programm zu installieren, starten Sie die Installationsdatei und folgen den Anweisungen des Installationsassistenten.

Achtung! Wenn auf Ihrem Computer eine ältere Version von Kaspersky Endpoint Security 10 für Windows installiert war, müssen vor einem Upgrade zuerst alle verschlüsselten Festplatten entschlüsselt werden. Wurde auf Ihrem Computer die Programmversion Kaspersky Endpoint Security 10 Maintenance Release 1 für Windows (Beta) installiert, ist es erforderlich, vor der Installation von Kaspersky Endpoint Security 10 Maintenance Release 1 für Windows die Beta-Version des Programms zu deinstallieren. Vor der Deinstallation sollen auch die verschlüsselten Bereiche und Festplatten entschlüsselt werden.

Bei der Installation erkennt und entfernt Kaspersky Endpoint Security 10 für Windows Programme, die zu einer Verlangsamung (bis hin zur vollen Funktionsuntüchtigkeit) des Benutzercomputers führen können. Das Programm kann von einem Remote-Standort mit Kaspersky Security Center installiert werden.

Achtung! Das Programm ist mit Kaspersky Security Center 10.0 und höher kompatibel. Das Programm kann im Silent-Modus (ohne Beteiligung des Benutzers) installiert werden.

Damit die Verschlüsselungsfunktionalität in Kaspersky Endpoint Security 10 für Windows funktioniert, muss ein Verschlüsselungsmodul installiert werden.

NEUERUNGEN VON KASPERSKY ENDPOINT SECURITY 10 MAINTENANCE RELEASE 1 FÜR WINDOWS

- Verschlüsselung von Festplatten:
 - Die Liste der im Authentifizierungsagenten unterstützten Tastaturlayouts wurde erweitert.
 - Neu: Automatische Kompatibilitätsprüfung des Boot-Laufwerks mit dem Authentifizierungsagenten vor dem Start der Festplattenverschlüsselung. Details finden Sie über den Link: <http://support.kaspersky.com/de/9992>
 - Neu: Mit dem Reparatur-Tool FDE Recovery Tool können Diagnose-Informationen über ein verschlüsseltes Gerät ermittelt werden.
 - Die Funktionalität zur automatischen Benutzeranmeldung am Betriebssystem nach erfolgreicher Authentifizierung im Authentifizierungsagenten wurde verbessert.
 - Die Leistungsfähigkeit der Verschlüsselung von Dateien (FLE) und von Festplatten (FDE) wurde verbessert.
- Zur Erhöhung des Schutzniveaus wurde die Funktionalität zur Aktivitätsüberwachung von Programmen in den Basisschutz (Core) aufgenommen.
- Neu: Verzögerung beim Zugriff auf den Aktivierungsserver. Dadurch wird die Belastung bei der Programmaktivierung mithilfe eines Aktivierungscodes unter Verwendung von Kaspersky Security Center sowie bei der Programmaktivierung mithilfe eines Reserveschlüssels minimiert.
- Die Funktionalität der übrigen Komponenten wurde optimiert.
- Neu: Unterstützung der Betriebssysteme Microsoft Windows 8.1 und Microsoft Windows Server 2012 R2.

Eine Liste der behobenen Fehler finden Sie auf der Seite <http://support.kaspersky.com/de/10578>.

EINSCHRÄNKUNGEN UND BEKANNTE FEHLER

- Wenn Kaspersky Endpoint Security installiert ist, ist ein Upgrade des Betriebssystems auf Microsoft Windows 8.1 / Microsoft Windows Server 2012 R2 nicht möglich. Um das Betriebssystem aufzupgraden, muss vorher das Programm entfernt werden.
- Verschlüsselung von Dateien (FLE):
 - Die Funktionalität zur Dateiverschlüsselung wird für die Betriebssysteme der Produktfamilie Microsoft Windows Embedded nicht unterstützt.
 - Das Betriebssystem muss nach der Programminstallation neu gestartet werden, damit die Verschlüsselung für Dateien und Ordner funktioniert.
 - Wird von einem Computer ohne Verschlüsselungsfunktionalität von Kaspersky Endpoint Security auf eine Datei eines Computers mit Verschlüsselungsfunktionalität zugegriffen, die dort verschlüsselt wurde und gespeichert ist, wird direkter Zugriff auf diese Datei gewährt. Wird eine Datei, die auf einem Computer mit Verschlüsselungsfunktionalität von Kaspersky Endpoint Security verschlüsselt wurde und gespeichert ist, aus einem Netzwerkordner auf einen Computer ohne Verschlüsselungsfunktionalität kopiert, wird diese Datei unverschlüsselt kopiert.
 - Es wird empfohlen, die mithilfe von Encrypting File System verschlüsselten Dateien zu entschlüsseln, bevor sie mit Kaspersky Endpoint Security verschlüsselt werden.
 - Die Größe einer Datei erhöht sich nach der Verschlüsselung um 4 KB.
 - Nach der Verschlüsselung erhält eine Datei in den Eigenschaften das Attribut "Archiv".
 - Beim Entpacken eines verschlüsselten Archivs werden die im Ordner vorhandenen Dateien mit gleichen Namen durch die Dateien des verschlüsselten Archivs überschrieben. Der Überschreibvorgang wird dem Benutzer nicht gemeldet.
 - Auf der Oberfläche des portablen Dateimanagers werden keine Meldungen über Fehler angezeigt, die in diesem Dateimanager auftreten.

- Auf einem Computer, auf dem die Funktionalität zur Dateiverschlüsselung installiert ist, startet Kaspersky Endpoint Security den portablen Dateimanager nicht.
 - Bei der Verwendung der Dateiverschlüsselung ist das Programm nicht mit dem Mail-Client Sylpheed kompatibel.
 - Die Einstellungen der Auslagerungsdatei können nicht geändert werden: Statt der festgelegten Einstellungen verwendet das Betriebssystem die Standardwerte.
 - Wenn die Funktionalität zur Dateiverschlüsselung auf einem Computer mit Microsoft Windows XP installiert ist, werden die Funktionen für die Verzeichnisstruktur (Erstellen / Umbenennen) in einem verteilten DFS-Dateisystem nicht unterstützt.
 - Es wird davor gewarnt, die Funktionalität zur Dateiverschlüsselung (FLE) zu verwenden, um auf einem Computer mit Microsoft Windows XP das gesamte Systemlaufwerk zu verschlüsseln, da dadurch Störungen im Betriebssystem auftreten können. Für die Verschlüsselung eines Systemlaufwerks mit NTFS-Dateisystem auf einem Computer mit Microsoft Windows XP sollte die Funktionalität zur Festplattenverschlüsselung (FDE) verwendet werden.
 - Wenn mit verschlüsselten Wechselmedien gearbeitet wird, muss unbedingt die Funktion zum sicheren Entfernen verwendet werden. Wenn ein Wechselmedium nicht durch sicheres Entfernen getrennt wird, kann die Datenintegrität auf dem Wechselmedium nicht garantiert werden.
 - Nach der Dateiverschlüsselung werden die unverschlüsselten Originale auf sichere Weise gelöscht.
- Verschlüsselung von Festplatten und Wechselmedien (FDE):
 - Die Funktionalität zur Festplattenverschlüsselung wird für die Betriebssysteme der Produktfamilie Microsoft Windows Embedded nicht unterstützt.
 - Im Authentifizierungsagenten werden nur folgende Tastaturlayouts unterstützt: QWERTY (USA), AZERTY (Frankreich), QWERTZ (Deutschland) und QWERTZ (Schweiz). In den Tastaturlayouts AZERTY (Frankreich), QWERTZ (Deutschland) und QWERTZ (Schweiz) werden nur jene Zeichen unterstützt, die im Tastaturlayout QWERTY (USA) verfügbar sind, unter Ausnahme der Zeichen | und \. Alle übrigen Zeichen, einschließlich Sonderzeichen und sprachspezifische Zeichen, werden nicht unterstützt.
 - Wenn Prozesse vorhanden sind, die auf verschlüsselte Geräte zugreifen, bevor das Programm den ungehinderten Zugriff auf diese Geräte gewährt hat, zeigt das Programm eine Warnung darüber an, dass diese Prozesse beendet werden müssen. Wenn nicht alle derartigen Prozesse beendet werden können, müssen die verschlüsselten Geräte erneut angeschlossen werden.
 - Unikale Festplatten-IDs werden in der Statistik zur Geräteverschlüsselung in umgekehrter Form angezeigt.
 - Es wird davor gewarnt, logische Partitionen einer Festplatte zu formatieren, während die Festplatte verschlüsselt wird.
 - Wenn gleichzeitig mehrere Wechselmedien mit einem Computer verbunden sind, kann es vorkommen, dass die Verschlüsselungsrichtlinie nur auf ein Wechselmedium angewendet wird. Wenn die übrigen Wechselmedien erneut verbunden werden, wird die Verschlüsselungsrichtlinie korrekt angewendet.
 - Wenn auf einem Computer alle Benutzerkonten für den Authentifizierungsagenten gesperrt sind, ist auf diesem Computer keine Anmeldung am Betriebssystem möglich.
 - Auf einer stark fragmentierten Festplatte kann der Verschlüsselungsvorgang nicht gestartet werden. In diesem Fall muss die Festplatte defragmentiert werden.
 - Bei der Festplattenverschlüsselung wird der Ruhezustand folgendermaßen gesperrt: ab dem Start der Verschlüsselungsaufgabe bis zum ersten Neustart des Computers in den

Betriebssystemen Microsoft Windows XP / 7 / 8 / 8.1, und nach der Installation der Funktionalität zur Festplattenverschlüsselung bis zum ersten Neustart der Betriebssysteme Microsoft Windows 8 und Microsoft Windows 8.1. Bei der Entschlüsselung von Festplatten wird der Ruhezustand ab dem Zeitpunkt der vollständigen Entschlüsselung des Boot-Laufwerks bis zum ersten Neustart des Betriebssystems gesperrt.

- Es wird davor gewarnt, das Tool xbootmgr.exe mit aktivierten zusätzlichen Diensten zu verwenden (z. B. DISPATCHER, NETWORK, DRIVERS u. a.).
 - Nachdem die Funktion zur Verschlüsselung von Festplatten und Wechselmedien auf einem Computer mit Microsoft Windows XP installiert wurde, wird die Option des Betriebssystems "Schnelle Benutzerumschaltung" gesperrt.
 - Auf Computern mit Microsoft Windows XP und Microsoft Windows Vista wird die vollständige Verschlüsselung von Geräten mit FAT32-Dateisystem nicht unterstützt. Verwenden Sie zur Verschlüsselung solcher Geräte die Dateiverschlüsselung (FLE) oder formatieren Sie das Dateisystem in NTFS um.
- **Aktivitätsmonitor:** Es werden keine vollständigen Informationen über Prozesse angezeigt.
 - **Lizenzverwaltung:**
 - Bei Server-Betriebssystemen wird im Fenster "Lizenzverwaltung" des Programms die durch die Lizenz erlaubte Funktionalität angezeigt, nicht aber die installierten Programmkomponenten.
 - Die Aufgabe zum Hinzufügen von Schlüsseln mithilfe von Kaspersky Security Center kann mit Fehlern ausgeführt werden. Weitere Details können Sie der Wissensdatenbank für das Produkt (Artikel-ID 9648) entnehmen.
 - **Aktive Desinfektion:**
 - In Server-Betriebssystemen wird keine Warnung darüber angezeigt, dass eine aktive Desinfektion erforderlich ist.
 - In bestimmten Fällen wird das Programm auf Computern mit Microsoft Windows XP SP3 nach einem Reboot nicht automatisch gestartet. In diesem Fall muss der Computer neu gestartet werden.
 - Es kann vorkommen, dass eine Webadresse, die zur Liste der vertrauenswürdigen Webadressen hinzugefügt wurde, fehlerhaft verarbeitet wird.
 - Es kann vorkommen, dass in den Berichten von Kaspersky Security Center Programmereignisse fehlerhaft angezeigt werden.
 - Die Wiederherstellung von Objekten, die von Mail-Anti-Virus in die Quarantäne verschoben wurden, wird nicht unterstützt.
 - **Gerätekontrolle:**
 - Es kann vorkommen, dass ein Gerät des Typs "Drucker", das zur Liste für vertrauenswürdige Geräte hinzugefügt wurde, durch Sperrregeln für Geräte und Schnittstellen verboten wird.
 - Auf Computern mit Microsoft Windows 8.1 wird die Gerätesperre auf Basis einer Schnittstelle nicht unterstützt. Verwenden Sie in solchen Fällen eine dem Gerätetyp entsprechende Gerätesperre.
 - **Web-Kontrolle:**
 - Die Formate ogv und webm werden nicht unterstützt.
 - Das Protokoll RTMP wird nicht unterstützt.
 - **Programminstallation:**
 - Nach der Installation auf einem infizierten Computer benachrichtigt das Programm nicht darüber, dass eine Untersuchung des Computers erforderlich ist. Es können Probleme bei der Programmaktivierung auftreten. Um dieses Problem zu lösen, muss nach der Installation eine Untersuchung der wichtigen Bereiche gestartet werden.

- Wenn der Vorgang zum Upgrade auf Kaspersky Endpoint Security 10 für Windows abgebrochen wird, kann es sein, dass die zu aktualisierende Programmversion nicht mehr funktioniert.
- In bestimmten Fällen wird eine Überinstallation des Programms über Kaspersky Internet Security 2013 MP1 nicht ausgeführt. Es wird empfohlen, Kaspersky Internet Security 2013 MP1 zu entfernen und Kaspersky Endpoint Security neu zu starten.
- Bei einem Upgrade des Programms Kaspersky Anti-Virus 6.0 für Windows Workstations MP4 auf Kaspersky Endpoint Security 10 für Windows wird die automatische Installation des Verschlüsselungsmoduls zusammen mit dem Programm nicht unterstützt. Das Verschlüsselungsmodul muss einzeln installiert werden.
- Wenn das Verschlüsselungsmodul nach der Programminstallation separat installiert wird, ist die Verschlüsselungsfunktionalität des Programms erst verfügbar, nachdem der Computer neu gestartet wurde.
- Nachdem das Programm Kaspersky Endpoint Security 10 für Windows wiederhergestellt wurde, muss das Verschlüsselungsmodul separat wiederhergestellt werden, damit die Verschlüsselung einwandfrei funktioniert.
- Die Installation der Funktionalität zur Festplattenverschlüsselung wird auf Tablets mit Microsoft Windows 8 und Microsoft Windows 8.1 nicht unterstützt.