kaspersky

Kaspersky Endpoint Security 12.1 for Windows

© 2024 AO Kaspersky Lab

جدول المحتويات

تعليمات Kaspersky Endpoint Security for Windows

ما الجديد

الأسئلة الأكثر تكرارًا

Kaspersky Endpoint Security for Windows

حزمة التوزيع

متطلبات الأجهزة والبرامج

إجراء مقارنة بين ميزات التطبيق المتاحة تبعًا لنوع نظام التشغيل

مقارنة بين وظائف التطبيق اعتمادا على أدوات الإدارة

التوافق مع التطبيقات الأخرى

تثبيت التطبيق وإزالته

النشر من خلال Kaspersky Security Center

التثبيت القياسي للتطبيق

إنشاء حزمة التثبيت

تحديث قواعد البيانات في حزمة التثبيت

إنشاء مهمة تثبيت عن بعد

تثبيت التطبيق محليًا باستخدام المعالج

تثبيت التطبيق عن بعد باستخدام مدير تكوين مركز النظام

وصف إعدادات تثبيت ملف setup.ini

تغيير مكونات التطبيق

الترقية من إصدار سابق للتطبيق

إزالة التطبيق

ترخيص التطبيق

حول اتفاقية ترخيص المستخدم النهائي

حول الترخيص

حول شهادة الترخيص

حول الاشتراك

حول مفتاح الترخيص

حول رمز التفعيل

حول الملف الرئيسي

مقارنة بين وظائف التطبيق حسب نوع الترخيص لمحطات العمل

مقارنة بين وظائف التطبيق حسب نوع الترخيص للخوادم

تفعيل التطبيق

تنشيط التطبيق من خلال Kaspersky Security Center

استخدام معالج التفعيل لتفعيل التطبيق

عرض معلومات الترخيص

شراء الترخيص

تجديد الاشتراك

توفير البيانات

توفير البيانات بموجب اتفاقية ترخيص المستخدم النهائي

حول توفير البيانات عند استخدام Kaspersky Security Network

توفير البيانات عند استخدام حلول Detection and Response

Kaspersky Endpoint Detection and Response

Kaspersky Sandbox

(Kaspersky Anti Targeted Attack Platform (EDR

الامتثال لتشريعات الاتحاد الأوروبي (GDPR)

بدء الاستخدام

نبذة عن المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows
اعتبارات خاصة عند العمل مع إصدارات مختلفة لمكونات الإدارة الإضافية
اعتبارات خاصة عند استخدام البروتوكولات المشفرة للتفاعل مع الخدمات الخارجية
واجهة التطبيق
رمز التطبيق في منطقة إخطار شريط المهام
واجهة التطبيق المبسطة
تكوين عرض واجهة التطبيق
بدء الاستخدام
إدارة السياسات
إدارة المهام
تكوين إعدادات التطبيق المحلية
بدء وإيقاف تشغيل برنامج Kaspersky Endpoint Security
التوقف المؤقت واستئناف حماية الكمبيوتر ومراقبته
إنشاء ملف تكوين واستخدامه
استعادة إعدادات التطبيق الافتراضية
فحص البرامج الضارة
فحص الكمبيوتر
فحص محركات الأقراص القابلة للإزالة عند توصيلها بالكمبيوتر
فحص في الخلفية
الفحص من قائمة السياق
مراقبة تكامل التطبيق
تحرير نطاق الفحص
إجراء فحص مجدول
إجراء فحص كمستخدم مختلف
تحسين الفحص
تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق
سيناريوهات تحديثات وحدات التطبيق وقواعد البيانات
التحديث من مستودع الخادم
التحديث من مجلد مشترك
التحديث باستخدام برنامج Kaspersky Update Utility
التحديث أثناء الوضع المتنقل
بدء مهمة تحديث وإيقافها
بدء مهمة تحديث تحت حقوق حساب مستخدم مختلف
تحديد وضع تشغيل مهام التحديث
إضافة مصدر تحديث
تكوين تحديثات من مجلد مشترك
تحديث الوحدات النمطية للتطبيق
استخدام الخادم الوكيل للتحديثات
استرجاع آخر تحديث
التعامل مع التهديدات النشطة
تنظيف التهديدات النشطة على محطات العمل
تنظيف التهديدات النشطة على الخوادم
تمكين أو تعطيل تقنية التنظيف المتقدمة
معالجة التهديدات النشطة
حماية الكمبيوتر
الحماية من تهديدات الملفات
تمكين وتعطيل الحماية من تهديدات الملفات
الإيقاف التلقائي المؤقت للحماية من تهديدات الملفات

تغيير الإجراءات التي تتخذها الملفات المصابة بواسطة مكون الحماية من تهديدات الملفات
تشكيل نطاق الحماية لمكون الحماية من تهديدات الملفات
استخدام طرق الفحص
استخدام تقنيات الفحص في تشغيل مكون الحماية من تهديدات الملفات
تحسين فحص الملفات
فحص الملفات المركبة
تغيير وضع الفحص
الحماية من تهديدات الويب
تمكين وتعطيل الحماية من تهديدات الويب
تكوين طرق اكتشاف عناوين الويب الخبيثة
مكافحة الاحتيال
إنشاء قائمة عناوين الويب الموثوقة
تصدير واستيراد قائمة عناوين الويب الموثوقة
الحماية من تهديدات البريد
تمكين وتعطيل الحماية من تهديدات البريد
تغيير الإجراء الذي تود اتخاذه بشأن رسائل البريد الإلكتروني المصابة
تشكيل نطاق الحماية لمكون الحماية من تهديدات البريد
فحص الملفات المركبة المرفقة برسائل البريد الإلكتروني
تصفية مرفقات رسائل البريد الإلكتروني
تصدير واستيراد ملحقات لتصفية المرفقات
فحص رسائل البريد الإلكتروني في Microsoft Office Outlook
الحماية من تهديدات الشبكة
تمكين وتعطيل الحماية من تهديدات الشبكة
منع الكمبيوتر المهاجم
تكوين عناوين الاستثناءات من المنع
تصدير واستيراد قائمة الاستثناءات من المنع
تكوين الحماية ضد هجمات شبكة الاتصال حسب النوع
جدار الحماية
تمكين أو تعطيل جدار الحماية
تغيير حالة اتصال الشبكة
إدارة قواعد حزم الشبكة
إنشاء قاعدة حزمة الشبكة
تمكين أو تعطيل قاعدة حزمة الشبكة
تغيير إجراء جدار الحماية لقاعدة حزمة الشبكة
تغيير أولوية قاعدة حزمة الشبكة
تصدير واستيراد قواعد حزمة الشبكة
تحديد قواعد حزم الشبكة في XML
إدارة قواعد الشبكة للتطبيق
إنشاء قاعدة شبكة للتطبيق
تمكين وتعطيل قعدة شبكة التطبيق
تغيير إجراء جدار الحماية الخاص بقاعدة شبكة اتصال لتطبيق
تغيير أولوية قاعدة شبكة تطبيق
مراقبة شبكة الاتصال
منع هجمات BadUSB
تمكين "منع هجمات BadUSB" أو تعطيلها
استخدام لوحة المفاتيح على الشاشة للمصادقة على أجهزة USB
حماية AMSI
تمكين حماية AMSI وتعطيلها

استخدام حماية AMSI لفحص الملفات المركبة
منع الاستغلال
تمكين وتعطيل منع الاستغلال
تحديد إجراء لاتخاذه عند اكتشاف استغلال
حماية ذاكرة عمليات النظام
اكتشاف السلوك
تمكين وتعطيل اكتشاف السلوك
تحديد الإجراء الذي سيتم اتخاذه عند اكتشاف نشاط برمجيات ضارة
حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي
تمكين وتعطيل حماية المجلدات المشتركة ضد التشفير الخارجي
تحديد الإجراء الذي يمكن اتخاذه عند اكتشاف تشفير خارجي للمجلدات التي تتم مشاركتها
إنشاء استثناء لحماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي
تكوين عناوين الاستثناءات من حماية المجلدات المشتركة ضد التشفير الخارجي
تصدير واستيراد قائمة استثناءات من حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي
منع اختراق المضيف
تمكين وتعطيل منع اختراق المضيف
إدارة المجموعات الموثوقة للتطبيق
تغيير مجموعة الثقة لتطبيق
تكوين حقوق مجموعة الثقة
تحديد مجموعة ثقة للتطبيقات التي تم بدؤها قبل Kaspersky Endpoint Security
تحديد مجموعة ثقة للتطبيقات غير المعروفة
تحديد مجموعة ثقة للتطبيقات الموقعة رقمياً
إدارة حقوق التطبيق
حماية موارد نظام التشغيل والبيانات الشخصية
حذف معلومات حول التطبيقات غير المستخدمة
مراقبة منع اختراق المضيف
حماية الوصول إلى الصوت والفيديو
محرك المعالجة
Kaspersky Security Network
تمكين وتعطيل استخدام Kaspersky Security Network
قيود Kaspersky Private Security Network
تمكين وتعطيل وضع السحابة لمكونات الحماية
إعدادات وكيل KSN
التحقق من سمعة أحد الملفات في شبكة Kaspersky Security Network
فحص الاتصالات المشفرة
تمكين فحص الاتصالات المشفرة
تثبيت شهادات الجذر الموثوق بها
فحص الاتصالات المشفرة التي تتضمن شهادة غير موثوقة
فحص الاتصالات المشفرة في Firefox وThunderbird
استثناء الاتصالات المشفرة من الفحص
مسح البيانات
التحكم في الكمبيوتر
التحكم في الويب
تمكين وتعطيل التحكم في الويب
الإجراءات المتبعة مع قواعد الوصول إلى موارد الويب
إضافة قاعدة وصول إلى موارد الويب
تعيين أولويات لقواعد الوصول إلى موارد الويب
تمكين وتعطيل قاعدة الوصول إلى مورد ويب

تصدير واستيراد قواعد التحكم في الويب
اختبار قواعد الوصول إلى موارد الويب
تصدير واستيراد قائمة عناوين موارد الويب
مراقبة نشاط إنترنت المستخدم
تحرير قوالب رسائل التحكم في الويب
تحرير أقنعة عناوين مصادر الويب
التحكم في الجهاز
تمكين وتعطيل التحكم في الجهاز
حول قواعد الوصول
تحرير قاعدة الوصول للجهاز
تحرير قاعدة الوصول إلى ناقل الاتصال
إدارة الوصول إلى الأجهزة المحمولة
التحكم في الطباعة
التحكم في اتصالات Wi-Fi
مراقبة استخدام محركات الأقراص القابلة للإزالة
تغيير مدة التخزين المؤقت
الإجراءات المصاحبة للأجهزة الموثوقة
إضافة جهاز إلى القائمة الموثوقة من واجهة التطبيق
إضافة جهاز إلى القائمة الموثوقة من Kaspersky Security Center
تصدير واستيراد قائمة بالأجهزة الموثوقة
الوصول إلى جهاز ممنوع
وضع الاتصال بالإنترنت لمنح صلاحية الوصول
والوضع غير متصل بالإنترنت لمنح صلاحية الوصول
تحرير قوالب رسائل التحكم في الجهاز
منع تعدد الاتصال
تمكين منع تعدد الاتصال
تغيير حالة قاعدة اتصال
تغيير أولوية قاعدة اتصال
مراقبة عيوب التكيف
تمكين وتعطيل مراقبة عيوب التكيف
تمكين وتعطيل قاعدة مراقبة عيوب التكيف
تعديل الإجراء المتخذ عند إطلاق قاعدة مراقبة عيوب التكيف
إنشاء استثناء لقاعدة التحكم غير الطبيعي التكيفي
تصدير واستيراد الاستثناءات لقواعد التحكم غير الطبيعي التكيفي
تطبيق التحديثات لقواعد مراقبة عيوب التكيف
تحرير قالب رسالة مراقبة عيوب التكيف
عرض تقارير مراقبة عيوب التكيف
التحكم في التطبيقات
قيود وظيفة التحكم في التطبيق
استلام المعلومات حول التطبيقات المثبَّتة على أجهزة كمبيوتر المستخدمين
تمكين وتعطيل التحكم في التطبيق
تحديد وضع التحكم في التطبيق
إدارة قواعد التحكم في التطبيق
إضافة شرط تشغيل لقاعدة التحكم في التطبيقات
إضافة الملفات التنفيذية من مجلد الملفات التنفيذية إلى فئة التطبيق
إضافة الملفات التنفيذية ذات الصلة بالحدث إلى فئة التطبيق
إضافة قاعدة التحكم في التطبيقات
تغيير حالة قاعدة التحكم في التطبيق عبر Kaspersky Security Center

تصدير واستيراد قواعد التحكم في التطبيقات
عرض الأحداث الناتج عن تشغيل مكون التحكم في التطبيقات
عرض تقرير حول التطبيقات المحجوبة
اختبار قواعد التحكم في التطبيق
تمكين وتعطيل اختبار قاعدة التحكم في التطبيقات
لعرض التقرير الخاص بالتطبيقات المحجوبة في وضع الاختبار
عرض الأحداث الناتجة عن عملية اختبار مكون التحكم في التطبيقات
مراقبة نشاط التطبيقات
قواعد لإنشاء أقنعة أسماء للملفات أو المجلدات
تحرير قوالب رسالة التحكم في التطبيقات
أفضل الممارسات لتنفيذ قائمة التطبيقات المسموح بها
تكوين وضع قائمة السماح للتطبيقات
اختبار وضع قائمة السماح
دعم وضع قائمة السماح
مراقبة منافذ الشبكة
تمكين مراقبة جميع منافذ الشبكة
إنشاء قائمة بمنافذ الشبكة المراقبة
إنشاء قائمة بالتطبيقات التي يتم مراقبة كافة منافذ الشبكة من أجلها
تصدير واستيراد قوائم المنافذ قيد المراقبة
فحص السجل
تكوين القواعد المحددة مسبقًا
إضافة قواعد مخصصة
مراقبة سلامة الملف
تحرير نطاق المراقبة
عرض معلومات سلامة النظام
الحماية بكلمة مرور
تمكين الحماية بكلمة مرور
منح أذونات للمستخدمين الأفراد أو المجموعات
استخدام كلمة مرور مؤقتة لمنح الأذونات
الجوانب الخاصة لأذونات الحماية بكلمة المرور
إعادة تعيين كلمة مرور KLAdmin
منطقة موثوقة
إنشاء استثناء من الفحص
تحديد أنواع الكائنات القابلة للاكتشاف
تحرير قائمة التطبيقات الموثوقة
تصدير واستيراد المنطقة الموثوقة
استخدام مخزن شهادات النظام الموثوق
إدارة النسخ الاحتياطي
تكوين أقصى فترة تخزين للملفات في النسخ الاحتياطي
تكوين أقصى حجم للنسخ الاحتياطي
استعادة الملفات من النسخ الاحتياطي
حذف النسخ الاحتياطية للملفات من النسخ الاحتياطي
خدمة الإخطارات
تكوين إعدادات سجل الحدث
تكوين عرض وتسليم الإخطارات
تكوين عرض التحذيرات حول حالة التطبيق في منطقة الإخطارات
تبادل الرسائل بين المستخدمين والمدير
إدارة التقارير

عرض التقارير
تكوين الفترة الزمنية القصوى لتخزين التقرير
تكوين الحجم الأقصى لملف التقرير
حفظ التقرير إلى ملف
مسح التقارير
الدفاع الذاتي لبرنامج Kaspersky Endpoint Security
تمكين وتعطيل الدفاع الذاتي
تمكين دعم AM-PPL وتعطيله
حماية خدمات التطبيق من الإدارة الخارجية
دعم تطبيقات الإدارة عن بعد
أداء Kaspersky Endpoint Security والتوافق مع التطبيقات الأخرى
تمكين أو تعطيل وضع توفير الطاقة
تمكين أو تعطيل منح الموارد للتطبيقات الأخرى
أفضل الممارسات لتحسين أداء Kaspersky Endpoint Security
تشفير البيانات
قيود وظيفة التشفير
تغيير طول مفتاح التشفير (AES56 / AES256)
تشفير القرص من Kaspersky
ميزات خاصة لتشفير محرك أقراص SSD
بدء تشفير القرص من Kaspersky
إنشاء قائمة بمحركات الأقراص الصلبة التي تم استثناؤها من التشفير
تصدير واستيراد قائمة بمحركات الأقراص الصلبة التي تم استثناؤها من التشفير
تمكين تقنية تسجيل الدخول الأحادي (SSO)
إدارة حسابات وكيل المصادقة
استخدام رمز مميز وبطاقة ذكية مع وكيل المصادقة
فك تشفير محرك الأقراص الصلبة
استعادة الوصول إلى محرك محمي بواسطة تقنية تشفير القرص من Kaspersky
تسجيل الدخول باستخدام حساب خدمة وكيل المصادقة
تحديث نظام التشغيل
استبعاد الأخطاء الخاصة بتحديث وظيفة التشفير
تحديد مستوى تتبع وكيل المصادقة
تحرير نصوص تعليمات وكيل المصادقة
إزالة الكائنات والبيانات الباقية بعد اختبار تشغيل وكيل المصادقة
إدارة BitLocker
بدء تشغيل تشفير محرك الأقراص من BitLocker
فك تشفير محرك أقراص محمي بتقنية BitLocker
استعادة الوصول إلى محرك محمي باستخدام BitLocker
إيقاف حماية BitLocker مؤقتًا لتحديث البرنامج
التشفير على مستوى الملف على محركات الأقراص الثابتة المحلية
تشفير الملفات على محركات أقراص الكمبيوتر المحلية
تشكيل قواعد الوصول إلى الملفات المشفرة للتطبيقات
تشفير الملفات التي تم إنشاؤها أو تعديلها بواسطة تطبيقات محددة
إنشاء قاعدة فك تشفير
فك تشفير الملفات على محركات أقراص الكمبيوتر المحلية
إنشاء حزم مشفرة
طلب الوصول إلى الملفات المشفرة
استعادة الوصول إلى البيانات المشفرة بعد فشل نظام التشغيل
تحرير قوالب رسائل الوصول إلى الملفات المشفرة

تشفير محركات الأقراص القابلة للإزالة
بدء تشفير محركات الأقراص القابلة للإزالة
إضافة قاعدة تشفير لمحركات الأقراص القابلة للإزالة
تصدير واستيراد قائمة بقواعد التشفير لمحركات الأقراص القابلة للإزالة
الوضع المحمول للوصول إلى الملفات المشفرة على محركات الأقراص القابلة للإزالة
فك تشفير محركات الأقراص القابلة للإزالة
عرض تفاصيل تشفير البيانات
عرض حالة التشفير
عرض إحصائيات عن لوحات تحكم Kaspersky Security Center
عرض أخطاء تشفير الملفات على محركات أقراص الكمبيوتر المحلية
عرض تقرير تشفير البيانات
استخدام الأجهزة المشفرة في حالة عدم توافر الوصول إليها
استرداد البيانات باستخدام الأداة المساعدة FDERT
إنشاء قرص إنقاذ نظام تشغيل
حلول Detection and Response
Kaspersky Endpoint Agent
ترحيل السياسة والمهام لـ Kaspersky Endpoint Agent
ترحيل تكوين [KES+KEA] إلى تكوين [KES+العامل المضمن]
Managed Detection and Response
التكامل مع MDR
الترحيل من Kaspersky Endpoint Agent
Endpoint Detection and Response
التكامل مع Kaspersky Endpoint Detection and Response
الترحيل من Kaspersky Endpoint Agent
الفحص للبحث عن مؤشرات الاختراق (مهمة قياسية)
نقل الملف إلى العزل
الحصول على الملف
حذف الملف
بدء العملية
إنهاء العملية
منع التنفيذ
عزل شبكة الاتصال
Cloud Sandbox
Kaspersky Sandbox
التكامل مع Kaspersky Sandbox
الترحيل من Kaspersky Endpoint Agent
إضافة شهادة TLS
إضافة خوادم Kaspersky Sandbox
الفحص للبحث عن مؤشرات الاختراق (مهمة مستقلة)
(Kaspersky Anti Targeted Attack Platform (EDR
التكامل مع KATA) EDR)
تكوين القياس عن بعد
دليل الترحيل من KEA إلى KES لحل KATA) EDR)
إدارة العزل
تكوين الحد الأقصى لحجم العزل
إرسال بيانات عن الملفات المعزولة إلى Kaspersky Security Center
استعادة الملفات من العزل
دليل الترحيل من KSWS إلى KES

مطابقة مكونات KSWS و KES
مطابقة إعدادات KSWS و KES
ترحيل مكونات KSWS
ترحيل مهام وسياسات KSWS
تثبيت KES بدلاً من KSWS
ترحيل تكوين [KSWS+KEA] إلى تكوين [KES+العامل المضمن]
التأكد من إزالة Kaspersky Security for Windows Server بنجاح
تفعيل KES بمفتاح KSWS
اعتبارات خاصة لترحيل الخوادم عالية التحميل
مثال على الترحيل من [KSWS + KEA] إلى KES
إدارة التطبيق على خادم Core Mode
لإدارة التطبيق من سطر الأوامر
تثبيت التطبيق
تفعيل التطبيق
إزالة التطبيق
أوامر AVP
SCAN. فحص البرامج الضارة
UPDATE. تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق
ROLLBACK. استرجاع آخر تحديث
TRACES. التتبع
START. بدء ملف التعريف
STOP. إيقاف ملف التعريف
STATUS. حالة ملف التعريف
STATISTICS. إحصائيات عملية تشغيل ملف التعريف
RESTORE. استعادة الملفات من النسخ الاحتياطي
EXPORT. تصدير إعدادات التطبيق
IMPORT. استيراد إعدادات التطبيق
ADDKEY. تطبيق ملف المفتاح
LICENSE. الترخيص
التجديد. شراء الترخيص
PBATESTRESET. إعادة ضبط نتائج التحقق من القرص قبل تشفير القرص
EXIT. إنهاء التطبيق
EXITPOLICY. تعطيل السياسة
STARTPOLICY. تمكين السياسة
DISABLE. تعطيل الحماية
SPYWARE. الكشف عن برامج التجسس
KSN. التبديل بين KSN / KPSN
أوامر KESCLI
فحص. فحص البرامج الضارة
GetScanState. حالة اكتمال الفحص
GetLastScanTime. تحديد وقت إكمال الفحص
GetThreats. الحصول على بيانات عن التهديدات المكتشفة
UpdateDefinitions. تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق
GetDefinitionState. تحديد وقت إكمال التحديث
EnableRTP. تمكين الحماية
GetRealTimeProtectionState. حالة الحماية من تهديدات الملفات
الإصدار. تحديد إصدار التطبيق
أوامر إدارة Detection and Response

SANDBOX. إدارة Kaspersky Sandbox
المنع. إدارة منع التنفيذ
العزل. إدارة عزل شبكة الاتصال
RESTORE. استعادة الملفات من العزل
IOCSCAN. فحص مؤشرات الاختراق (IOC)
MDRLICENSE. تفعيل MDR
EDRKATA. التكامل مع KATA) EDR)
رموز الخطأ
الملحق. ملفات تعريف التطبيق
إدارة التطبيق من خلال REST API
تثبيت التطبيق مع REST API
العمل باستخدام واجهة برمجة التطبيقات (API)
مصادر المعلومات المتعلقة بالتطبيق
الاتصال بالدعم الفني
محتويات وتخزين ملفات التتبع
تتبع تشغيل التطبيق
تتبع أداء التطبيق
تفريغ الكتابة
حماية ملفات التفريغ وملفات التتبع
القيود والتحذيرات
المصطلحات
IOC
OpenIOC
إدارة الملفات المحمولة
إنذار خاطئ
الأرشيف
القناع
المفتاح الإضافي
الملف القابل للإصابة
المهمة
الوحدة النمطية للنظام الأساسي الموثوق به
تنظيف
جهة إصدار الشهادة
شهادة الترخيص
عميل الشبكة
قاعدة بيانات عناوين الويب الاحتيالية
قاعدة بيانات عناوين الويب الضارة
قواعد بيانات مكافحة الفيروسات
كائن OLE
مجموعة الإدارة
مفتاح نشط
ملف IOC
ملف مصاب
نطاق الحماية
نطاق الفحص
نموذج تمت معايرته من عنوان مصدر ويب
وكيل المصادقة
الملحقات

الملحق رقم 1. إعدادات التطبيق
الحماية من تهديدات الملفات
الحماية من تهديدات الويب
الحماية من تهديدات البريد
الحماية من تهديدات الشبكة
جدار الحماية
منع هجمات BadUSB
حماية AMSI
منع الاستغلال
اكتشاف السلوك
منع اختراق المضيف
محرك المعالجة
Kaspersky Security Network
فحص السجل
التحكم في الويب
التحكم في الجهاز
التحكم في التطبيقات
مراقبة عيوب التكيف
مراقبة سلامة الملف
أداة استشعار نقطة النهاية
Kaspersky Sandbox
Endpoint Detection and Response
(Endpoint Detection and Response (KATA
تشفير القرص بالكامل
التشفير على مستوى الملف
تشفير محركات الأقراص القابلة للإزالة
قوالب (تشفير البيانات)
الاستثناءات
إعدادات التطبيق
التقارير والمخزن
إعدادات الشبكة
الواجهة
إدارة الإعدادات
تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق
الملحق رقم 2. المجموعات الموثوقة للتطبيقات
الملحق رقم 3. امتدادات الملفات لفحص محركات الأقراص القابلة للإزالة
الملحق رقم 4. نوع الملف لعامل تهديدات للحماية من تهديدات البريد
الملحق رقم 5. إعدادات الشبكة للتفاعل مع الخدمات الخارجية
الملحق رقم 6. أحداث التطبيق
حرج
خلل وظيفي
تحذير
رسائل معلوماتية
الملحق رقم 7. امتدادات الملفات المدعومة لمنع التنفيذ
الملحق رقم 8. مترجمو النصوص المدعومون لمنع التنفيذ
الملحق رقم 9. نطاق فحص IOC في التسجيل (Registryltem)
الملحق رقم 10. متطلبات ملف IOC
معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

تعليمات Kaspersky Endpoint Security for Windows

ما الجديد في الإصدار 12.1

- تمت إضافة عامل مضمن لإدارة مكون Kaspersky Endpoint Detection and Response الذي يعد جزءًا من حل Kaspersky Anti Targeted Attack Platform. لم تعد بحاجة إلى Kaspersky Endpoint Agent لاستخدام EDR (KATA). ويستطيع برنامج Kaspersky Endpoint Security تنفيذ كل وظائف Kaspersky Endpoint Agent.
- الجديد في كل إصدار من Kaspersky Endpoint Security for Windows

بدء الاستخدام

- نشر Kaspersky Endpoint Security for Windows
- الإعداد المبدئي لتطبيق Kaspersky Endpoint Security for Windows
- ترخيص Kaspersky Endpoint Security for Windows

القضاء على التهديدات

- على محطات العمل
- على الخوادم
- التفاعل مع اكتشاف مؤشر التسوية (عزل شبكة الاتصال ← العزل ← منع التنفيذ)

استخدام KES كجزء من حلول أخرى

- Kaspersky EDR
- Kaspersky Sandbox
- Kaspersky MDR

توفير البيانات

- تحن اتفاقية ترخيص المستخدم النهائي
- عند استخدام KSN

- اللائحة العامة لحماية البيانات

ما الجديد

التحديث 12.1

يوفر برنامج Kaspersky Endpoint Security 12.1 for Windows الميزات والتحسينات التالية:

1. تمت إضافة العامل المُضمن لحل Kaspersky Anti Targeted Attack Platform. لم تعد بحاجة إلى Kaspersky Endpoint Agent لاستخدام EDR (KATA). وسيتم تنفيذ جميع وظائف Kaspersky Endpoint Agent بواسطة Kaspersky Endpoint Security. ولترحيل سياسات Kaspersky Endpoint Agent، استخدم معالج الترحيل. وبعد تحديث التطبيق، يتحول Kaspersky Endpoint Security إلى استخدام العامل المضمن ويزيل Kaspersky Endpoint Agent. تمت إضافة Kaspersky Endpoint Agent إلى قائمة البرامج غير المتوافقة. يحتوي Kaspersky Endpoint Security على عوامل مدمجة لجميع حلول Detection and Response، لذلك لم يعد تثبيت Kaspersky Endpoint Agent للتكامل مع هذه الحلول ضروريًا.

2. يتم دعم وضع التوافق مع Azure WVD الآن. تتيح هذه الميزة عرض حالة جهاز Azure الظاهري بشكل صحيح في وحدة التحكم لتطبيق Kaspersky Anti Targeted Attack Platform. ويسمح وضع التوافق مع Azure WVD بتعيين معرف مستشعر فريد دائم لهذه الأجهزة الظاهرية.

3. يمكنك الآن تكوين وصول المستخدم إلى الأجهزة المحمولة في iTunes أو التطبيقات المماثلة. وهذا يعني أنه يمكنك، على سبيل المثال، السماح باستخدام الجهاز المحمول فقط في iTunes وحظر استخدام الجهاز المحمول كمحرك أقراص قابل للإزالة. ويدعم التطبيق أيضًا هذه القواعد لتطبيق Android Debug Bridge (ADB).

4. لم يعد الإصدار 11 من Kaspersky Security Center مدعومًا. قم ترقية Kaspersky Security Center إلى أحدث إصدار.

التحديث 12.0

يوفر برنامج Kaspersky Endpoint Security 12.0 for Windows الميزات والتحسينات التالية:

1. تم تحسين تشغيل Kaspersky Endpoint Security على الخوادم. ويمكنك الآن الترحيل من Kaspersky Security for Windows Server إلى Kaspersky Endpoint Security for Windows واستخدام حل واحد لحماية محطات العمل والخوادم. ولترحيل إعدادات التطبيق، قم بتشغيل معالج تحويل تصحيح المهام والسياسات. ويمكن استخدام مفتاح ترخيص KSWS لتفعيل KES. بعد الترحيل إلى KES، لن تحتاج حتى إلى إعادة تشغيل الخادم. وللمزيد من المعلومات عن الترحيل إلى KES، راجع دليل الترحيل.

2. تم تحسين ترخيص التطبيق كجزء من صورة جهاز افتراضي مدفوع الثمن في Amazon Machine Image (AMI). وليست هناك حاجة لتفعيل التطبيق بشكل منفصل. وفي هذه الحالة، يستخدم Kaspersky Security Center مفتاح الترخيص لبيئة السحابة التي تمت إضافتها بالفعل إلى التطبيق.

3. تم تحسين التحكم في الجهاز:

- بالنسبة للأجهزة المحمولة (MTP)، يمكنك تكوين قواعد الوصول (قراءة/كتابة)، أو تحديد مستخدمين أو مجموعة مستخدمين لديهم حق الوصول إلى الأجهزة، أو تكوين جدول وصول للجهاز. ويمكنك الآن إنشاء قواعد وصول للأجهزة المحمولة بالطريقة نفسها لإنشاء محركات الأقراص القابلة للإزالة.
- يمكنك الآن تكوين وصول المستخدم إلى الأجهزة المحمولة في Android Debug Bridge (ADB) أو التطبيقات المماثلة. وهذا يعني أنه يمكنك، على سبيل المثال، السماح باستخدام الجهاز المحمول فقط في ADB وحظر استخدام الجهاز المحمول كمحرك أقراص قابل للإزالة.
- يمكنك الآن إعادة شحن جهاز محمول عن طريق توصيله بمنفذ USB بالكمبيوتر حتى في حالة حظر الوصول إلى الجهاز المحمول.
- بالنسبة للطابعات، يمكنك الآن تكوين أذونات الطباعة للمستخدمين. يدعم Kaspersky Endpoint Security التحكم في الوصول إلى الطابعات المحلية وطابعات الشبكة. ويمكنك الآن السماح بالطباعة أو حظرها على الطابعات المحلية أو طابعات الشبكة للمستخدمين الفرديين.

- تمت إضافة دعم بروتوكول WPA3 للتحكم في الاتصالات بشبكات Wi-Fi. ويمكنك الآن تحديد استخدام بروتوكول WPA3 في إعدادات شبكة Wi-Fi الموثوقة ورفض الاتصال بالشبكة باستخدام بروتوكول أقل أمانًا.

التحديث 11.11.0

يوفر برنامج Kaspersky Endpoint Security 11.11.0 for Windows الميزات والتحسينات التالية:

1. تمت إضافة مكون فحص السجل للخوادم. ويراقب سجل الفحص سلامة البيئة المحمية استنادًا إلى نتائج تحليل سجل أحداث Windows. وعندما يكتشف التطبيق علامات سلوك غير نمطي في النظام، فإنه يُبلغ المسؤول، لأن هذا السلوك قد يشير إلى محاولة هجوم إلكتروني.

2. تمت إضافة مكون مراقبة سلامة الملف للخوادم. ويكتشف مكون مراقبة سلامة الملف التغييرات في الكائنات (الملفات والمجلدات) في منطقة مراقبة معينة. وقد تشير هذه التغييرات إلى حدوث خرق لأمان الكمبيوتر. وعند اكتشاف تغييرات الكائن، يُبلغ التطبيق المسؤول.

3. تم تحسين واجهة تفاصيل الاكتشاف لحل Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). وتمت محاذاة عناصر سلسلة تطور التهديد، ولم تعد الروابط بين العمليات في السلسلة متداخلة. ويسهل هذا تحليل تطور التهديد.

4. تم تحسين أداء التطبيق. ولهذا الغرض، تم تحسين معالجة حركة مرور شبكة الاتصال بواسطة مكون الحماية من تهديدات الشبكة.

5. تمت إضافة خيار ترقية Kaspersky Endpoint Security بدون إعادة التشغيل. ويتيح لك هذا ضمان تشغيل الخوادم دون انقطاع عند ترقية التطبيق. يمكنك ترقية التطبيق دون إعادة التشغيل بدءًا من الإصدار 11.10.0. يمكنك أيضًا تثبيت التصحيحات دون إعادة التشغيل بدءًا من الإصدار 11.11.0.

6. تمت إعادة تسمية مهمة Virus Scan في Kaspersky Security Center Console. وتسمى هذه المهمة الآن Malware Scan.

التحديث 11.10.0

يوفر برنامج Kaspersky Endpoint Security 11.10.0 for Windows الميزات والتحسينات التالية:

1. تمت إضافة دعم موفري بيانات الاعتماد الخارجيين لتسجيل الدخول الأحادي باستخدام Kaspersky Full Disk Encryption. يراقب Kaspersky Endpoint Security كلمة مرور المستخدم لتطبيق ADSelfService Plus ويتولى تحديث بيانات وكيل المصادقة إذا قام المستخدم، على سبيل المثال، بتغيير كلمة مروره.

2. تمت إضافة خيار تمكين عرض التهديدات المكتشفة بواسطة تقنية Cloud Sandbox. وهذه التقنية متاحة لمستخدمي حلول Endpoint Detection and Response Optimum) EDR) أو Cloud Sandbox (EDR Expert. هي تقنية تتيح لك اكتشاف التهديدات المتقدمة على جهاز كمبيوتر. ويعيد Kaspersky Endpoint Security تلقائيًا توجيه الملفات المكتشفة إلى Cloud Sandbox لتحليلها. ويقوم Cloud Sandbox بتشغيل هذه الملفات في بيئة معزولة لتحديد النشاط الضار وتحديد سمعتها.

3. تمت إضافة معلومات إضافية عن الملفات إلى تفاصيل التنبيه لمستخدمي EDR Optimum. وتتضمن تفاصيل التنبيه الآن معلومات عن مجموعة الثقة والتوقيع الرقمي وتوزيع الملف ومعلومات أخرى. وستتمكن أيضا من الانتقال إلى وصف الملف التفصيلي على بوابة Kaspersky Threat Intelligence Portal (KL TIP) مباشرة من تفاصيل التنبيه.

4. تم تحسين أداء التطبيق. ولفعل ذلك، أجرينا تحسينات على عملية الفحص في الخلفية وأضفنا القدرة على إضافة مهام الفحص إلى قائمة الانتظار إذا كان الفحص قيد التشغيل بالفعل.

التحديث 11.9.0

يوفر برنامج Kaspersky Endpoint Security 11.9.0 for Windows الميزات والتحسينات التالية:

1. تستطيع الآن إنشاء حساب خدمة وكيل المصادقة عند استخدام تشفير القرص من Kaspersky. ويعد حساب الخدمة ضروريًا للوصول إلى الكمبيوتر، على سبيل المثال، عندما ينسى المستخدم كلمة المرور. ويمكنك أيضًا استخدام حساب الخدمة كحساب احتياطي.

2. لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من ملف مجموعة توزيع التطبيق. ولدعم حلول Detection and Response، يمكنك استخدام العميل المدمج في Kaspersky Endpoint Security. وإذا لزم الأمر، يمكنك تنزيل حزمة توزيع Kaspersky Endpoint Agent من مجموعة توزيع Kaspersky Anti Targeted Attack Platform.

3. تم تحسين واجهة تفاصيل الاكتشاف لحل Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). وتحتوي ميزات الاستجابة للتهديد الآن على تلميحات أدوات. ويتم أيضًا عرض إرشادات تفصيلية لضمان أمان البنية التحتية للشركة عند اكتشاف مؤشرات الاختراق.

4. يمكنك الآن تفعيل Kaspersky Endpoint Security for Windows باستخدام مفتاح ترخيص Kaspersky Hybrid Cloud Security.

5. تمت إضافة أحداث جديدة حول إنشاء اتصال بالمجالات التي تحتوي على شهادات غير موثوقة وأخطاء فحص الاتصالات المشفرة الأخطاء.

التحديث 11.8.0

يوفر برنامج Kaspersky Endpoint Security 11.8.0 for Windows الميزات والتحسينات التالية:

1. تمت إضافة العامل المدمج لدعم تشغيل حل Kaspersky Endpoint Detection and Response Expert. ويعد Kaspersky Endpoint Detection and Response Expert حلاً لحماية البنية التحتية لتكنولوجيا المعلومات في الشركة من التهديدات الإلكترونية المتقدمة. وتجمع وظيفة الحل بين الاكتشاف التلقائي للتهديدات والقدرة على الرد على هذه التهديدات لمواجهة الهجمات المتقدمة بما في ذلك عمليات الاستغلال الجديدة وبرامج الفدية والهجمات الخالية من الملفات، بالإضافة إلى الأساليب التي تستخدم أدوات النظام المشروعة. ويوفر EDR Expert وظائف أكثر لرصد التهديدات والاستجابة لها من EDR Optimum. وللمزيد من المعلومات عن الحل، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Expert.

2. تم الآن تحسين واجهة مراقبة شبكة الاتصال. ويعرض مراقبة شبكة الاتصال الآن بروتوكول UDP بالإضافة إلى TCP.

3. تم تحسين مهمة فحص الفيروسات. إذا قمت بإعادة تشغيل الكمبيوتر أثناء الفحص، يقوم Kaspersky Endpoint Security بتشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقف عندها الفحص.

4. يمكنك الآن تعيين حد لوقت تنفيذ المهمة. ويمكنك تحديد وقت التنفيذ لمهمتي فحص الفيروسات وفحص IOC. وبعد مدة زمنية معينة، يوقف Kaspersky Endpoint Security المهمة. لتقليل وقت تنفيذ مهمة فحص الفيروسات، يمكنك على سبيل المثال، تكوين نطاق الفحص أو تحسين الفحص.

5. يتم رفع قيود الأنظمة الأساسية للخادم للتطبيق المثبت على جلسات متعددة لنظام التشغيل Windows 10 Enterprise. ويعتبر Kaspersky Endpoint Security الآن أن الجلسات المتعددة لنظام التشغيل Windows 10 Enterprise هو نظام تشغيل محطة عمل، وليس نظام تشغيل خادم. وفي المقابل، لم تعد قيود النظام الأساسي للخادم تنطبق على التطبيق في جلسات المتعددة لنظام التشغيل Windows 10 Enterprise. ويستخدم التطبيق أيضًا مفتاح ترخيص محطة عمل للتفعيل بدلاً من مفتاح ترخيص خادم.

التحديث 11.7.0

يوفر Kaspersky Endpoint Security for Windows 11.7.0 الميزات والتحسينات الجديدة التالية:

1. تحديث واجهة Kaspersky Endpoint Security for Windows.

2. دعم أنظمة التشغيل Windows 11 وWindows 10 21H2 وWindows Server 2022.

3. تمت إضافة مكونات جديدة:

- تمت إضافة عامل مضمن للتكامل مع Kaspersky Sandbox. ويكتشف حل Kaspersky Sandbox ويمنع تلقائيًا التهديدات المتقدمة على أجهزة الكمبيوتر. ويحلل Kaspersky Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Kaspersky Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Kaspersky Sandbox). وللحصول على تفاصيل حول الحل، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

  لم تعد بحاجة إلى Kaspersky Endpoint Agent لاستخدام Kaspersky Sandbox. وسيتم تنفيذ جميع وظائف Kaspersky Endpoint Agent بواسطة Kaspersky Endpoint Security. ولترحيل سياسات Kaspersky Endpoint Agent، استخدم معالج الترحيل. وتحتاج إلى برنامج Kaspersky Security Center 13.2 لكي تعمل جميع وظائف Kaspersky Sandbox. وللحصول على تفاصيل عن الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows، يرجى الرجوع إلى تعليمات التطبيق.

- تمت إضافة العامل المدمج لدعم تشغيل حل Kaspersky Endpoint Detection and Response Optimum. ويعد Kaspersky Endpoint Detection and Response Optimum حلاً لحماية البنية التحتية لتكنولوجيا المعلومات في المؤسسة من التهديدات الإلكترونية المتقدمة. وتجمع وظيفة الحل بين الاكتشاف التلقائي للتهديدات والقدرة على الرد على هذه التهديدات لمواجهة الهجمات المتقدمة بما في ذلك عمليات الاستغلال الجديدة وبرامج الفدية والهجمات الخالية من الملفات، بالإضافة إلى الأساليب التي تستخدم أدوات النظام المشروعة. وللمزيد من المعلومات عن الحل، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum.

  لم تعد بحاجة إلى Kaspersky Endpoint Agent لاستخدام Kaspersky Endpoint Detection and Response. وسيتم تنفيذ جميع وظائف Kaspersky Endpoint Agent بواسطة Kaspersky Endpoint Security. ولترحيل سياسات ومهام Kaspersky Endpoint Agent، استخدم معالج الترحيل. ولاستخدام جميع الوظائف، يتطلب Kaspersky Endpoint Detection and Response Optimum 13.2 وجود Kaspersky Security Center. وللحصول على تفاصيل عن الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows، يرجى الرجوع إلى تعليمات التطبيق.

4. تمت إضافة معالج ترحيل لسياسات ومهام Kaspersky Endpoint Agent. وينشئ مع سياسات ومهام مدمجة جديدة لتطبيق Kaspersky Endpoint Security for Windows. ويسمح المعالج بتبديل حلول Detection and Response من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security. وتشمل حلول Detection and Response كلاً من Kaspersky Sandbox وKaspersky Endpoint Detection and Response Optimum (EDR Optimum) وKaspersky Managed Detection and Response (MDR).

5. تم تحديث Kaspersky Endpoint Agent، المدرج في حزمة التوزيع، إلى الإصدار 3.11.

   عند ترقية Kaspersky Endpoint Security، يكتشف التطبيق إصدار Kaspersky Endpoint Agent والغرض المحدد منه. وفي حالة تخصيص Kaspersky Endpoint Agent لتشغيل Kaspersky Sandbox وKaspersky Managed Detection and Response (MDR) وKaspersky Endpoint Detection and Response Optimum (EDR Optimum)، فإن Kaspersky Endpoint Security يحول تشغيل هذه الحلول إلى العامل المدمج للتطبيق. وفيما يتعلق بحلي Kaspersky Sandbox وEDR Optimum، سوف يغلي التطبيق تلقائيًا تثبيت Kaspersky Endpoint Agent. وبالنسبة إلى MDR، يمكنك إلغاء تثبيت Kaspersky Endpoint Agent يدويًا. وإذا كان التطبيق مخصصًا لتشغيل Kaspersky Endpoint Detection and Response Expert (EDR Expert)، فسوف يقوم Kaspersky Endpoint Security بترقية إصدار Kaspersky Endpoint Agent. وللمزيد من التفاصيل حول التطبيق، يرجى الرجوع إلى وثائق حلول Kaspersky التي تدعم Kaspersky Endpoint Agent.

6. تم تحسين وظيفة تشفير BitLocker:

- يمكن الآن استخدام رمز PIN محسّن مع تشفير محرك الأقراص من BitLocker. ويسمح رمز PIN المحسّن باستخدام أحرف أخرى بالإضافة إلى الأحرف الرقمية: الأحرف اللاتينية الكبيرة والصغيرة والأحرف الخاصة والمسافات.

- تمت إضافة ميزة لتعطيل مصادقة BitLocker لترقية نظام التشغيل أو تثبيت حزم التحديث. وقد يتطلب تثبيت التحديثات إعادة تشغيل الكمبيوتر عدة مرات. ولتثبيت التحديثات بشكل صحيح، يمكنك إيقاف تشغيل مصادقة BitLocker مؤقتًا وإعادة تمكين المصادقة بعد تثبيت التحديثات.

- تستطيعُ الآن تعيين وقت انتهاء صلاحية لكلمة مرور تشفير BitLocker أو رمز PIN. وعند انتهاء صلاحية كلمة المرور أو رمز PIN، يطالب Kaspersky Endpoint Security المستخدم بكلمة مرور جديدة.

7. يمكنك الآن تكوين الحد الأقصى لعدد محاولات مصادقة لوحة المفاتيح لمنع هجمات BadUSB. وعند الوصول إلى العدد الذي تم تكوينه للمحاولات الفاشلة لإدخال رمز المصادقة، يتم قفل جهاز USB مؤقتًا.

8. تم تحسين وظائف جدار الحماية:

- يمكنك الآن تكوين مجموعة من عناوين IP لأجل قواعد حزمة جدار الحماية. ويمكنك إدخال نطاق من العناوين بتنسيق IPv4 أو IPv6. على سبيل المثال، `192.168.1.1-192.168.1.100` أو `2::12:34-99::12:34`.
- يمكنك الآن إدخال أسماء DNS لأجل قواعد حزمة جدار الحماية بدلاً من عناوين IP. ويجب عليك استخدام أسماء DNS فقط لأجهزة كمبيوتر الشبكة المحلية (LAN) أو الخدمات الداخلية. ويجب التعامل مع التفاعل مع الخدمات السحابية (مثل Microsoft Azure) وموارد الإنترنت الأخرى بواسطة مكون التحكم في الويب.

9. تحسين البحث في قاعدة التحكم في الويب. وللبحث في قاعدة وصول إلى موارد الويب، بالإضافة إلى اسم القاعدة، يمكنك استخدام عنوان URL لموقع الويب أو اسم مستخدم أو فئة محتوى أو نوع بيانات.

10. تحسين مهمة فحص الفيروسات:

- تم تحسين مهمة فحص الفيروسات في الوضع الخامل. إذا قمت بإعادة تشغيل الكمبيوتر أثناء الفحص، يقوم Kaspersky Endpoint Security بتشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقف عندها الفحص.
- تم تحسين مهمة فحص الفيروسات. وافتراضيًا، يقوم Kaspersky Endpoint Security بتشغيل الفحص فقط عندما يكون الكمبيوتر خاملاً. ويمكنك التكوين عند تشغيل فحص الكمبيوتر في خصائص المهمة.

11. يمكنك الآن تقييد وصول المستخدم إلى البيانات التي توفرها مراقبة نشاط التطبيقات. مراقبة نشاط التطبيقات أداة مصممة لعرض معلومات حول نشاط التطبيقات على كمبيوتر المستخدم في الوقت الحقيقي. ويستطيع المسؤول إخفاء مراقبة نشاط التطبيقات عن المستخدم في خصائص سياسة التطبيق.

12. تحسين أمان إدارة التطبيق من خلال REST API. يتحقق Kaspersky Endpoint Security الآن من توقيع الطلبات المرسلة عبر REST API. ولإدارة البرنامج، تحتاج إلى تثبيت شهادة تعريف الطلب.

يوفر برنامج Kaspersky Endpoint Security 11.4.0 for Windows الميزات والتحسينات التالية:

1. تصميم جديد لرمز التطبيق في منطقة إخطار شريط المهام. يتم الآن عرض الرمز الجديد بدلاً من الرمز القديم. إذا كان يجب على المستخدم اتخاذ إجراء (مثل إعادة تشغيل الكمبيوتر بعد تحديث التطبيق)، فإن الرمز سيتغير إلى . إذا كانت مكونات الحماية للتطبيق غير مفعلة أو بها خطأ، فإن الرمز سوف يتغير إلى أو . إذا مررت بالسهم فوق الرمز، فإن Kaspersky Endpoint Security سوف يعرض وصفًا للمشكلة في حماية الكمبيوتر.

2. قد تم تحديث Kaspersky Endpoint Agent، الموجود ضمن حزمة التوزيع، إلى الإصدار 3.9. 3.9 Kaspersky Endpoint Agent يدعم التكامل مع حلول Kaspersky الجديدة. وللمزيد من التفاصيل حول التطبيق، يرجى الرجوع إلى وثائق حلول Kaspersky التي تدعم Kaspersky Endpoint Agent.

3. إضافة حالة غير مدعوم من الترخيص لمكونات Kaspersky Endpoint Security. ويمكنك عرض حالة المكونات في قائمة المكونات في نافذة التطبيق الرئيسية.

4. تم إضافة أحداث جديدة من منع الاستغلال إلى التقارير.

5. محركات الأقراص لتقنية تشفير القرص من Kaspersky الآن تُضاف بشكل آلي إلى بيئة استرداد نظام Windows (WinRE) عند بدء تشفير القرص. الإصدار السابق من Kaspersky Endpoint Security كان يضيف المحركات عند تثبيت التطبيق. إضافة أجهزة إلى WinRE يمكن أن يحسِّن من ثبات التطبيق عند استعادة نظام التشغيل على أجهزة كمبيوتر محمية بتقنية Kaspersky Disk Encryption.

تم إزالة مكون أداة استشعار نقطة النهاية من Kaspersky Endpoint Security. لا يزال بإمكانك تكوين إعدادات أداة استشعار نقطة النهاية في سياسة شريطة أن يكون Kaspersky Endpoint Security بالإصدار 11.0.0 إلى 11.3.0 مثبتًا على الكمبيوتر.

يوفر برنامج Kaspersky Endpoint Security 11.5.0 for Windows الميزات والتحسينات التالية:

1. دعم نظام التشغيل Windows 10 20H2. للحصول على تفاصيل حول دعم نظام التشغيل Microsoft Windows 10، الرجاء الرجوع إلى قاعدة معارف الدعم الفني.

2. تم تحديث واجهة التطبيق. تم أيضًا تحديث رمز التطبيق في مساحة الإخطارات وإخطارات التطبيق ومربعات الحوار.

3. واجهة مُحسَّنة للمكوِّن الإضافي للويب لتطبيق Kaspersky Endpoint Security لمكونات التحكم في التطبيقات والتحكم في الجهاز ومكونات التحكم غير الطبيعي التكيفي.

4. وظيفة مضافة لاستيراد وتصدير قوائم القواعد والاستثناءات بتنسيق XML. يسمح لك تنسيق XML بتحرير القوائم بعد تصديرها. يمكنك إدارة القوائم فقط في وحدة تحكم Kaspersky Security Center. القوائم التالية متاحة للتصدير / الاستيراد:

   - اكتشاف السلوك (قائمة الاستثناءات).
   - الحماية من تهديدات الويب (قائمة عناوين الويب الموثوقة).
   - الحماية من تهديدات البريد (قائمة ملحقات تصفية المرفقات).
   - الحماية من تهديدات الشبكة (قائمة الاستثناءات).
   - جدار الحماية (قائمة قواعد حزمة الشبكة).
   - التحكم في التطبيقات (قائمة القواعد).
   - التحكم في الويب (قائمة القواعد).
   - مراقبة منفذ شبكة الاتصال (قوائم المنافذ والتطبيقات التي يراقبها Kaspersky Endpoint Security).
   - تشفير القرص من Kaspersky (قائمة الاستثناءات).
   - تشفير محركات الأقراص القابلة للإزالة (قائمة القواعد).

5. تمت إضافة معلومات MD5 الخاصة بالكائن إلى تقرير اكتشاف التهديد. في الإصدارات السابقة من التطبيق، عرض Kaspersky Endpoint Security فقط SHA256 لكائن.

6. تمت إضافة إمكانية تعيين الأولوية لقواعد الوصول إلى الجهاز في إعدادات التحكم في الجهاز. يتيح تعيين الأولوية تكوينًا أكثر مرونة لوصول المستخدم إلى الأجهزة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 0 لمجموعة المسؤولين وقم بتعيين أولوية من 1 لمجموعة "الجميع". يمكنك تكوين الأولوية فقط للأجهزة التي تحتوي على نظام ملفات. يتضمن ذلك محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة والأقراص المرنة ومحركات أقراص CD/DVD والأجهزة المحمولة (MTP).

7. تمت إضافة وظيفة جديدة:

   - إدارة الإخطارات الصوتية.
   - يقيد Kaspersky Endpoint Security لاتصالات الشبكة المراعية للتكلفة حركة شبكة الاتصال إذا كان اتصال الإنترنت محدودًا (على سبيل المثال، من خلال اتصال محمول).
   - يمكنك إدارة إعدادات Kaspersky Endpoint Security عبر تطبيقات الإدارة عن بُعد الموثوقة (مثل TeamViewer وLogMeIn وRemotely Anywhere). يمكنك استخدام تطبيقات الإدارة عن بُعد لبدء تشغيل Kaspersky Endpoint Security وإدارة الإعدادات في واجهة التطبيق.
   - يمكنك إدارة إعدادات فحص حركة المرور الآمنة في Firefox وThunderbird. ويمكنك تحديد مخزن الشهادة الذي ستستخدمه Mozilla: مخزم شهادة Windows أو مخزن شهادة Mozilla. هذه الوظيفة متاحة فقط لأجهزة الكمبيوتر التي تُطبق عليها سياسة. وفي حالة عدم تطبيق سياسة

على جهاز كمبيوتر، فإن Kaspersky Endpoint Security يقوم تلقائيًا بتمكين استخدام مخزن شهادة Windows في Firefox وThunderbird.

8. تمت إضافة إمكانية تكوين وضع فحص حركة المرور الآمنة: افحص دائمًا حركة المرور حتى في حالة تعطيل مكونات الحماية، أو افحص حركة المرور عند طلب مكونات الحماية ذلك.

9. الإجراء المنقح لحذف المعلومات من التقارير. يستطيع المستخدم حذف كل التقارير فقط. في الإصدارات السابقة من التطبيق، يستطيع المستخدم تحديد مكونات تطبيق معينة سيتم حذف معلوماتها من التقارير.

10. الإجراء المنقح لاستيراد ملف تكوين يحتوي على إعدادات Kaspersky Endpoint Security، والإجراء المنقح لاستعادة إعدادات التطبيق. قبل الاستيراد أو الاستعادة، يعرض Kaspersky Endpoint Security تحذيرًا فقط. في الإصدارات السابقة من التطبيق، كان بإمكانك عرض قيم الإعدادات الجديدة قبل تطبيقها.

11. إجراء مبسط لاستعادة الوصول إلى محرك أقراص تم تشفيره بواسطة BitLocker. بعد إكمال إجراء استرداد الوصول، يطالب Kaspersky Endpoint Security المستخدم بتعيين كلمة مرور جديدة أو رمز PIN جديد. بعد تعيين كلمة مرور جديدة، سوف يشفر BitLocker محرك الأقراص. في الإصدار السابق من التطبيق، كان على المستخدم إعادة تعيين كلمة المرور يدويًا في إعدادات BitLocker.

12. يتمتع المستخدمون الآن بالقدرة على إنشاء منطقتهم الموثوقة المحلية لجهاز كمبيوتر محدد. وبهذه الطريقة، يستطيع المستخدمون إنشاء قوائم محلية من الاستثناءات والتطبيقات الموثوقة الخاصة بهم بالإضافة إلى المنطقة العامة الموثوقة في سياسة ما. ويستطيع المسؤول باستخدام الاستثناءات المحلية أو التطبيقات الموثوقة المحلية أو منعها. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر.

13. تمت إضافة إمكانية لإدخال التعليقات في خصائص التطبيقات الموثوقة. تساعد التعليقات في تبسيط عمليات البحث وفرز التطبيقات الموثوقة.

14. إدارة التطبيق من خلال REST API:

- توجد قدرة الآن على تكوين إعدادات ملحق الحماية من تهديدات البريد لبرنامج Outlook.
- يحظر تعطيل اكتشاف الفيروسات والفيروسات المتنقلة وفيروسات حصان طروادة.

يوفر برنامج Kaspersky Endpoint Security 11.6.0 for Windows الميزات والتحسينات التالية:

1. دعم نظام التشغيل Windows 10 21H1. للحصول على تفاصيل حول دعم نظام التشغيل Microsoft Windows 10، الرجاء الرجوع إلى قاعدة معارف الدعم الفني.

2. تم إضافة مكون Managed Detection and Response. يسهل هذا المكون التفاعل مع الحل المعروف باسم Kaspersky Managed Detection and Response. ويوفر Kaspersky Managed Detection and Response (MDR) الحماية على مدار الساعة من عدد متزايد من التهديدات القادرة على تجاوز آليات الحماية الآلية للمؤسسات التي تواجه صعوبة في العثور على خبراء مؤهلين تأهيلاً عالياً أو تمتلك موارد داخلية محدودة. وللحصول على معلومات مفصلة حول طريقة عمل الحل، يرجى الرجوع إلى تعليمات Kaspersky Managed Detection and Response.

3. تم تحديث Kaspersky Endpoint Agent، الموجود ضمن حزمة التوزيع، إلى الإصدار 3.10. ويوفر Kaspersky Endpoint Agent 3.10 ميزات جديدة ويحل بعض المشكلات السابقة ويحسّن الاستقرار. وللمزيد من التفاصيل حول التطبيق، يرجى الرجوع إلى وثائق حلول Kaspersky التي تدعم Kaspersky Endpoint Agent.

4. يوفر الآن القدرة على إدارة الحماية ضد الهجمات مثل إغراق الشبكة وفحص المنافذ في إعدادات الحماية من تهديدات الشبكة.

5. تمت إضافة طريقة جديدة لإنشاء قواعد الشبكة لجدار الحماية. ويمكنك إضافة قواعد الحزمة وقواعد التطبيق للاتصالات التي يتم عرضها في نافذة مراقبة شبكة الاتصال. ومع ذلك، سيتم تكوين إعدادات اتصال قاعدة الشبكة تلقائيًا.

6. تم الآن تحسين واجهة مراقبة شبكة الاتصال. تمت إضافة المعلومات حول نشاط الشبكة: معرف العملية، الذي يبدأ نشاط الشبكة؛ ونوع الشبكة (الشبكة المحلية أو الإنترنت)؛ والمنافذ المحلية. وبشكل افتراضي، تكون المعلومات المتعلقة بنوع شبكة الاتصال مخفية.

7. توجد الآن إمكانية لإنشاء حسابات وكيل المصادقة تلقائيًا لمستخدمي Windows الجدد. ويسمح الوكيل للمستخدم بإكمال المصادقة للوصول إلى محركات الأقراص التي تم تشفيرها باستخدام تقنية تشفير القرص من Kaspersky، وتحميل نظام التشغيل. ويتحقق التطبيق من المعلومات حول حسابات مستخدمي Windows على الكمبيوتر. إذا اكتشف Kaspersky Endpoint Security حساب مستخدم Windows ليس له حساب وكيل مصادقة، فسوف ينشئ التطبيق حسابًا جديدًا للوصول إلى محركات الأقراص المشفرة. ويعني ذلك أنك لا تحتاج إلى إضافة حسابات وكيل المصادقة يدويًا لأجهزة الكمبيوتر التي تحتوي على محركات أقراص مشفرة بالفعل.

8. توجد الآن إمكانية لمراقبة عملية تشفير القرص في واجهة التطبيق على أجهزة كمبيوتر المستخدمين (تشفير القرص من Kaspersky وBitLocker). يمكنك تشغيل أداة مراقبة التشفير من نافذة التطبيق الرئيسية.

الأسئلة الأكثر تكرارًا

عام

على أي أجهزة كمبيوتر يمكن أن يعمل برنامج Kaspersky Endpoint Security؟

ماذا تغير منذ الإصدار الأخير؟

ما هي تطبيقات Kaspersky الأخرى التي يمكن أن يعمل معها برنامج Kaspersky Endpoint Security؟

كيف يمكنني الحفاظ على موارد جهاز الكمبيوتر أثناء تشغيل برنامج Kaspersky Endpoint Security؟

توزيع

كيف أقوم بتثبيت برنامج Kaspersky Endpoint Security على كل أجهزة الكمبيوتر في مؤسسة ما؟

ما هي إعدادات التثبيت التي يمكن تكوينها في سطر الأوامر؟

الإنترنت

هل يقوم برنامج Kaspersky Endpoint Security بفحص الاتصالات المشفرة (HTTPS)؟

كيف أسمح للمستخدمين بالاتصال بشبكات Wi-Fi الموثوقة فقط؟

كيف أقوم بحظر الشبكات الاجتماعية؟

تطبيقات

كيف يمكنني معرفة التطبيقات التي تم تثبيتها على جهاز كمبيوتر مستخدم ما (المخزون)؟

كيف أمنع تشغيل ألعاب الكمبيوتر؟

كيف أتحقق من أن التحكم في التطبيقات قد تم تكوينه بشكل صحيح؟

كيف أقوم بإضافة تطبيق إلى القائمة الموثوقة؟

كيف أقوم بإلغاء تثبيت برنامج Kaspersky Endpoint Security عن بُعد؟

تحديث

ما هي الطرق المتاحة لتحديث قواعد البيانات؟

ماذا يجب علي أن أفعل إذا ظهرت مشاكل بعد التحديث؟

كيف أقوم بتحديث قواعد البيانات خارج شبكة الشركة؟

هل من الممكن استخدام الخادم الوكيل لإجراء التحديثات؟

الأمان

كيف يفحص برنامج Kaspersky Endpoint Security البريد الإلكتروني؟

كيف أستبعد ملف موثوق من عمليات الفحص؟

كيف أحمي جهاز كمبيوتر ما من الفيروسات التي تأتي من محركات الأقراص المحمولة؟

كيف أقوم بتشغيل فحص البرامج الضارة بحيث يكون مخفي عن المستخدم؟

كيف أقوم بإيقاف حماية برنامج Kaspersky Endpoint Security بشكل مؤقت؟

كيف يمكنني استعادة ملف قام برنامج Kaspersky Endpoint Security بحذفه عن طريق الخطأ؟

كيف يمكنني حماية برنامج Kaspersky Endpoint Security من قيام المستخدم بإلغاء تثبيته؟

الأجهزة

كيف أقوم بحظر استخدام محركات الأقراص المحمولة؟

كيف أقوم بإضافة جهاز إلى القائمة الموثوقة؟

هل من الممكن الحصول على إمكانية الوصول إلى جهاز محظور؟

التشفير

تحت أي ظروف يكون التشفير مستحيلًا؟

كيف أستخدم كلمة مرور لتقييد الوصول إلى الأرشيف؟

هل من الممكن استخدام البطاقات الذكية وأجهزة التحقق من الهوية مع التشفير؟

هل من الممكن الحصول على صلاحية الوصول إلى البيانات المشفرة إذا لم يكن هناك اتصال مع Kaspersky Security Center؟

ماذا يجب علي أن أفعل إذا فشل نظام تشغيل جهاز الكمبيوتر ولكن البيانات لا تزال مشفرة؟

الدعم

أين يتم تخزين ملف التقرير؟

كيف أقوم بإنشاء ملف التتبع؟

كيف أقوم بتمكين كتابة التفريغ؟

Kaspersky Endpoint Security for Windows

يوفر برنامج Kaspersky Endpoint Security for Windows (المشار إليه أيضًا فيما بعد باسم Kaspersky Endpoint Security) حماية متكاملة للكمبيوتر ضد أنواع مختلفة من التهديدات وهجمات الشبكات والهجمات الاحتيالية.

لا يُقصد من التطبيق استخدامه في العمليات التقنية التي تتضمن أنظمة تحكم مؤتمتة. ولحماية الأجهزة في مثل هذه الأنظمة، فمن المستحسن استخدام تطبيق Kaspersky Industrial CyberSecurity for Nodes.

تقنيات اكتشاف التهديدات

التعلم الآلي

يستخدم Kaspersky Endpoint Security نموذجًا يعتمد على التعلم الآلي. وقد طور خبراء Kaspersky هذا النموذج. بعد ذلك، يتم تغذية الطراز باستمرار ببيانات التهديد من KSN (تدريب النموذج).

التحليل السحابي

يتلقى Kaspersky Endpoint Security بيانات التهديد من Kaspersky Security Network. تعتبر شبكة Kaspersky Security Network (KSN) بنية تحتية من الخدمات السحابية التي توفر الوصول إلى قاعدة معارف Kaspersky على الإنترنت والتي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج.

تحليل الخبراء

يستخدم Kaspersky Endpoint Security بيانات التهديد المضافة بواسطة محللي الفيروسات في Kaspersky. ويتولى محللو الفيروسات تقييم الكائنات في حالة عدم التمكن من تحديد سمعة أي كائن تلقائيًا.

تحليل السلوك

يحلل Kaspersky Endpoint Security نشاط الكائن في الوقت الحقيقي.

التحليل التلقائي

يتلقى Kaspersky Endpoint Security البيانات من نظام تحليل الكائنات التلقائي. ويعالج النظام جميع الكائنات التي يتم إرسالها إلى Kaspersky. ثم يحدد النظام سمعة الكائن ويضيف البيانات إلى قواعد بيانات مكافحة الفيروسات. وإذا لم يتمكن النظام من تحديد سمعة الكائن ، يستفسر النظام من محللي الفيروسات من Kaspersky.

Kaspersky Sandbox

يعالج Kaspersky Endpoint Security الكائن في جهاز ظاهري. ويحلل Kaspersky Sandbox سلوك الكائن ويتخذ قرارًا بشأن سمعته. وتكون هذه التقنية متاحة فقط إذا كنت تستخدم حل Kaspersky Sandbox.

Cloud Sandbox

يفحص Kaspersky Endpoint Security الكائنات الموجودة في بيئة معزولة توفرها Kaspersky. يتم تمكين تقنية Cloud Sandbox بشكل دائم وهي متاحة لجميع مستخدمي Kaspersky Security Network بغض النظر عن نوع الترخيص الذي يستخدمونه. وإذا نشرت بالفعل Endpoint Detection and Response Optimum، يمكنك تمكين عداد منفصل للتهديدات المكتشفة بواسطة Cloud Sandbox.

شجرة التحديد

وتتم معالجة كل نوع من التهديدات بواسطة مكون تطبيق مخصص. ويمكن تمكين المكونات أو تعطيلها بصورة مستقلة، ويمكن تكوين الإعدادات الخاصة بها.

شجرة التحديد

القسم	المكون
الحماية من التهديدات الأساسية	**الحماية من تهديدات الملفات** يتيح لك مكون الحماية من تهديدات الملفات منع إصابة نظام الملفات في جهاز الكمبيوتر. بشكل افتراضي، يوجد مكون الحماية من تهديدات الملفات بشكل دائم في ذاكرة الوصول العشوائي للكمبيوتر. يقوم المكون بفحص الملفات على كافة محركات الأقراص للكمبيوتر وكذلك على محركات الأقراص المتصلة. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

الحماية من تهديدات الويب

يمنع مكون الحماية من تهديدات الويب تنزيلات الملفات الضارة عبر الإنترنت، ويحظر أيضًا مواقع الويب الضارة والاحتيالية. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

الحماية من تهديدات البريد

يفحص مكون الحماية من تهديدات البريد مرفقات رسائل البريد الإلكتروني الصادرة والواردة للحماية من الفيروسات والتهديدات الأخرى. بشكل افتراضي، يوجد مكون الحماية من تهديدات البريد بشكل دائم في ذاكرة الوصول العشوائي للكمبيوتر ويقوم بفحص جميع الرسائل المستلمة أو المرسلة باستخدام بروتوكولات POP3 أو SMTP أو IMAP أو NNTP أو عميل بريد Microsoft Office Outlook (MAPI). يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

الحماية من تهديدات الشبكة

يراقب مكون الحماية من تهديدات الشبكة (يسمى أيضًا نظام اكتشاف التطفل) حركة شبكة الاتصال\ الواردة للبحث عن خاصية النشاط لهجمات الشبكة. عندما يكتشف Kaspersky Endpoint Security محاولة هجوم على الشبكة على كمبيوتر المستخدم، فإنه يحظر اتصال الشبكة مع الكمبيوتر المهاجم. تتوفر أوصاف لأنواع هجمات الشبكة المعروفة حاليًا وطرق إبطالها في قواعد بيانات Kaspersky Endpoint Security. يتم تحديث قائمة هجمات الشبكة التي يكتشفها مكون الحماية من تهديدات الشبكة أثناء تحديثات قاعدة البيانات والوحدة النمطية للتطبيق.

جدار الحماية

يقوم جدار الحماية بحظر الاتصالات غير المصرح بها للكمبيوتر أثناء العمل على الإنترنت أو الشبكة المحلية. يتحكم جدار الحماية كذلك في نشاط الشبكة للتطبيقات على الكمبيوتر. يسمح لك هذا بحماية الشبكة المحلية الخاصة بشركتك من سرقة الهوية والهجمات الأخرى. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك قواعد الشبكة المحددة مسبقًا.

منع هجمات BadUSB

يمنع المكون "منع هجمات BadUSB" أجهزة USB المصابة من محاكاة لوحة المفاتيح للاتصال بالكمبيوتر.

حماية AMSI

يكون مكون حماية AMSI مخصصًا لدعم واجهة فحص البرمجيات الضارة من Microsoft. تتيح واجهة فحص البرمجيات الضارة (AMSI) للتطبيقات الخارجية التي تتمتع بدعم AMSI إرسال الكائنات (على سبيل المثال، البرامج النصية PowerShell) إلى برنامج Kaspersky Endpoint Security لإجراء عملية فحص إضافية واستقبال نتائج الفحص لهذه الكائنات.

الحماية من التهديدات المتقدمة

Kaspersky Security Network

تعتبر شبكة Kaspersky Security Network (KSN) بنية تحتية من الخدمات السحابية التي توفر الوصول إلى قاعدة معارف Kaspersky على الإنترنت والتي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج. ويعد استخدام البيانات من Kaspersky Security Network ضمانًا لسرعة وقت استجابات Kaspersky Endpoint Security عند مواجهة تهديدات جديدة، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية ويقلل من خطر وقوع الحالات الإيجابية الزائفة. إذا كنت تشارك في شبكة Kaspersky Security Network، فإن خدمات شبكة KSN تقوم بتزويد برنامج Kaspersky Endpoint Security بمعلومات حول فئة وسمعة الملفات التي تم فحصها، بالإضافة إلى معلومات حول سمعة عناوين الويب التي تم فحصها.

اكتشاف السلوك

يتلقى مكون اكتشاف السلوك بيانات حول إجراءات التطبيقات على جهاز الكمبيوتر الخاص بك ويقدم هذه المعلومات إلى مكونات الحماية الأخرى لتحسين أدائها. يستخدم مكون اكتشاف السلوك توقيعات تدفق السلوك (BSS) للتطبيقات. إذا كان نشاط تطبيق متطابقًا مع توقيع تدفق سلوك، ينفذ Kaspersky Endpoint Security إجراء الاستجابة المحدد. ويوفر الأداء الوظيفي لبرنامج Kaspersky Endpoint Security المستند إلى توقيعات تدفق السلوك دفاعًا وقائيًا للكمبيوتر.

منع الاستغلال

مكون منع الاستغلال يكتشف رمز البرنامج الذي يستفيد من الثغرات الأمنية الموجودة على جهاز الكمبيوتر لاستغلال امتيازات المسؤول أو لتنفيذ أنشطة ضارة. على سبيل المثال، يمكن أن يستخدم المستغلون هجوم تجاوز سعة المخزن المؤقت. للقيام بذلك، يُرسل المستغل كمية كبيرة من البيانات إلى تطبيق معرض للاختراق. عند معالجة هذه البيانات، ينفذ التطبيق المعرض للاختراق تعليمات برمجية ضارة. كنتيجة لهذا الهجوم، يمكن أن يبدأ المستغل عملية تثبيت مُصرح بها للبرمجيات الضارة. عند اكتشاف محاولة لتشغيل الملف التنفيذي من تطبيق قابل للاختراق والتي لم يتم تنفيذها من قبل المستخدم، يحظر برنامج Kaspersky Endpoint Security تشغيل هذا الملف ويقوم بإخطار المستخدم.

منع اختراق المضيف

	يمنع مكون منع اختراق المضيف التطبيقات من تنفيذ الإجراءات التي قد تكون خطرة على نظام التشغيل ويضمن التحكم في الوصول إلى موارد نظام التشغيل والبيانات الشخصية. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network. **محرك المعالجة** يتيح محرك المعالجة لبرنامج Kaspersky Endpoint Security التراجع عن الإجراءات التي تم تنفيذها باستخدام برمجيات ضارة في نظام التشغيل.
ضوابط الأمان	**التحكم في التطبيقات** يدير التحكم في التطبيقات بدء تشغيل التطبيقات على أجهزة كمبيوتر المستخدمين. يتيح لك هذا تنفيذ سياسة أمان الشركة عند استخدام التطبيقات. التحكم في التطبيقات يقلل أيضًا من خطر إصابة الكمبيوتر بتقييد الوصول إلى التطبيقات. **التحكم في الجهاز** يعمل التحكم في الجهاز على إدارة إمكانية وصول المستخدم إلى الأجهزة المثبت عليها أو المتصلة بجهاز الكمبيوتر (على سبيل المثال، الأقراص الصلبة أو الكاميرات أو وحدات شبكة Wi-Fi). يتيح لك هذا حماية جهاز الكمبيوتر من الإصابة بالفيروسات عند اتصال مثل هذه الأجهزة به بالإضافة إلى الوقاية من فقدان البيانات أو تسريبها. **التحكم في الويب** يقوم المكون التحكم في الويب بإدارة وصول المستخدمين إلى موارد الويب. هذا يساعد على تقليل حركة المرور والاستخدام غير المناسب لوقت العمل. عندما يحاول مستخدم فتح موقع ويب محظور من التحكم في الويب، يحظر Kaspersky Endpoint Security الوصول إلى ذلك الموقع أو يعرض تحذيرًا. **مراقبة عيوب التكيف** يراقب مكون مراقبة عيوب التكيف ويمنع الإجراءات التي لا تعتبر معتادة لأجهزة الكمبيوتر الموجودة في شبكة الشركة. يستخدم نظام مراقبة عيوب التكيف مجموعة من القواعد لتتبع السلوك غير النموذجي (على سبيل المثال، قاعدة بدء تشغيل Windows PowerShell من خلال تطبيق Office). تم إنشاء القواعد من قِبل متخصصي Kaspersky استنادًا إلى سيناريوهات نموذجية للنشاط الضار. تستطيع تكوين كيفية قيام نظام مراقبة عيوب التكيف بمعالجة كل قاعدة، وعلى سبيل المثال، يسمح بتنفيذ نصوص PowerShell التي تقوم بالتشغيل التلقائي لبعض مهام سير العمل. يقوم Kaspersky Endpoint Security بتحديث مجموعة القواعد إلى جانب قواعد بيانات التطبيق. **فحص السجل** ويراقب سجل الفحص سلامة البيئة المحمية استنادًا إلى نتائج تحليل سجل أحداث Windows. وعندما يكتشف التطبيق علامات سلوك غير نمطي في النظام، فإنه يُبلغ المسؤول، لأن هذا السلوك قد يشير إلى محاولة هجوم إلكتروني. **مراقبة سلامة الملف** ويكتشف مكون مراقبة سلامة الملف التغييرات في الكائنات (الملفات والمجلدات) في منطقة مراقبة معينة. وقد تشير هذه التغييرات إلى حدوث خرق لأمان الكمبيوتر. وعند اكتشاف تغييرات الكائن، يُبلغ التطبيق المسؤول.
المهام	**فحص البرامج الضارة** يفحص Kaspersky Endpoint Security الكمبيوتر للبحث عن الفيروسات والتهديدات الأخرى. ويساعد فحص البرامج الضارة على إلغاء احتمالية نشر البرامج الضارة التي لم يتم اكتشافها بواسطة مكونات الحماية، على سبيل المثال، بسبب وجود مستوى أمان منخفض. **تحديث** يقوم برنامج Kaspersky Endpoint Security بتنزيل قواعد البيانات والوحدات النمطية المحدثة الخاصة بالتطبيق. يحافظ التحديث على استمرار حماية الكمبيوتر ضد أحدث الفيروسات والتهديدات الأخرى. ويتم تحديث التطبيق تلقائيًا بشكل افتراضي، ومع هذا، فمن الضروري أن تقوم بتحديث قواعد البيانات والوحدات النمطية للتطبيق يدويًا. **استرجاع آخر تحديث** يتراجع Kaspersky Endpoint Security عن التحديث الأخير لقواعد البيانات والوحدات النمطية. يتيح لك هذا الأمر إرجاع قواعد البيانات والوحدات النمطية للتطبيق إلى إصداراتها السابقة عند اللزوم، على سبيل المثال، عند احتواء إصدار قاعدة البيانات الجديد على توقيع غير صالح يتسبب في أن يقوم برنامج Kaspersky Endpoint Security بمنع تشغيل تطبيق آمن. **التحقق من السلامة** يتحقق Kaspersky Endpoint Security من الوحدات النمطية للتطبيق في مجلد تثبيت التطبيق بحثًا عن أية تلفيات أو تعديلات. في حالة وجود توقيع رقمي غير صحيح لإحدى الوحدات النمطية للتطبيق، يتم اعتبار الوحدة النمطية تالفة.
تشفير البيانات	**File Level Encryption** يسمح المكون بإنشاء قواعد تشفير الملفات. ويمكنك تحديد مجلدات محددة مسبقًا للتشفير، أو تحديد مجلد يدويًا، أو تحديد الملفات حسب الملحق.

	تشفير القرص بالكامل يسمح المكون بتشفير القرص الصلب باستخدام تشفير القرص من Kaspersky أو تشفير محرك الأقراص من BitLocker. **Encryption of removable drives** يسمح المكون بحماية البيانات الموجودة على محركات الأقراص القابلة للإزالة. ويمكنك استخدام تشفير القرص بالكامل (FDE) أو التشفير على مستوى الملف (FLE).
Detection and Response	**Endpoint Detection and Response Optimum** عامل مضمن لحل Kaspersky Endpoint Detection and Response Optimum (يُشار إليه فيما يلي أيضًا باسم "EDR Optimum"). ويعد Kaspersky Endpoint Detection and Response حلاً لحماية البنية التحتية لتكنولوجيا المعلومات في الشركة من التهديدات الإلكترونية المتقدمة. وتجمع وظيفة الحل بين الاكتشاف التلقائي للتهديدات والقدرة على الرد على هذه التهديدات لمواجهة الهجمات المتقدمة بما في ذلك عمليات الاستغلال الجديدة وبرامج الفدية والهجمات الخالية من الملفات، بالإضافة إلى الأساليب التي تستخدم أدوات النظام المشروعة. وللمزيد من المعلومات عن الحل، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum. **Endpoint Detection and Response Expert** عامل مضمن لحل Kaspersky Endpoint Detection and Response Expert (يُشار إليه فيما يلي أيضًا باسم "EDR Expert"). ويوفر EDR Expert وظائف أكثر لرصد التهديدات والاستجابة لها من EDR Optimum. وللمزيد من المعلومات عن الحل، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Expert. **Kaspersky Sandbox** عامل مضمن لحل Kaspersky Sandbox. ويكتشف حل Kaspersky Sandbox ويمنع تلقائيًا التهديدات المتقدمة على أجهزة الكمبيوتر. ويحلل Kaspersky Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Kaspersky Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Kaspersky Sandbox). وللحصول على تفاصيل حول الحل، يرجى الرجوع إلى تعليمات Kaspersky Sandbox. **Managed Detection and Response** عامل مدمج لدعم تشغيل حل Kaspersky Managed Detection and Response. يكتشف حل Kaspersky Managed Detection and Response (MDR) تلقائيًا ويحلل الحوادث الأمنية في البنية التحتية الخاصة بك. ولفعل ذلك، يستخدم MDR بيانات القياس عن بُعد الواردة من نقاط النهاية والتعلم الآلي. ويرسل MDR بيانات الحادث إلى خبراء Kaspersky. ويستطيع الخبراء بعد ذلك معالجة الحادث، وعلى سبيل المثال، إضافة إدخال جديد إلى قواعد بيانات مكافحة الفيروسات. وبدلاً من ذلك، يستطيع الخبراء إصدار توصيات بشأن معالجة الحادث، وعلى سبيل المثال، اقتراح عزل الكمبيوتر من الشبكة. وللحصول على معلومات مفصلة حول طريقة عمل الحل، يرجى الرجوع إلى تعليمات Kaspersky Managed Detection and Response.

حزمة التوزيع

تتضمن مجموعة التوزيع حزم التوزيع التالية:

- **تشفير قوي (AES256)**

  تحتوي حزمة التوزيع هذه على أدوات التشفير التي تقوم بتنفيذ خوارزمية التشفير AES (معيار التشفير المتقدم) باستخدام طول مفتاح فعال 256 بت.

- **تشفير خفيف (AES56)**

  تحتوي حزمة التوزيع هذه على أدوات التشفير التي تقوم بتنفيذ خوارزمية التشفير AES باستخدام طول مفتاح فعال 56 بت.

تحتوي كل حزمة من حزم التوزيع على الملفات التالية:

`kes_win.msi`	حزمة تثبيت برنامج Kaspersky Endpoint Security.
`setup_kes.exe`	الملفات المطلوبة لتثبيت التطبيق باستخدام أي من الطرق المتاحة.

kes_win.kud	ملف لإنشاء حزم التثبيت لبرنامج Kaspersky Endpoint Security.
klcfginst.msi	حزمة تثبيت المكون الإضافي لإدارة برنامج Kaspersky Endpoint Security لبرنامج Kaspersky Security Center.
bases.cab	تحديث ملفات الحزمة التي تستخدم في أثناء عملية التثبيت.
cleaner.cab	ملفات لإزالة البرامج غير المتوافقة.
incompatible.txt	الملف الذي يحتوي على قائمة بالبرامج غير المتوافقة.
ksn_<language_ID>.txt	ملف يمكنك من خلاله قراءة شروط المشاركة في شبكة Kaspersky Security Network.
license.txt	ملف تستطيع من خلاله قراءة اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية.
installer.ini	الملف الذي يحتوي على الإعدادات الداخلية لحزمة التثبيت.
keswin_web_plugin.zip	أرشيف يحتوي على الملفات المطلوبة لتثبيت المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security.

من غير المستحسن تغيير قيم هذه الإعدادات. إذا كنت تريد خيارات التثبيت، فاستخدم الملف setup.ini.

متطلبات الأجهزة والبرامج

لضمان أفضل تشغيل لبرنامج Kaspersky Endpoint Security، يجب أن يلبي جهاز الكمبيوتر الخاص بك المتطلبات التالية:

الحد الأدنى من المتطلبات العامة:

- مساحة قرص خالية تبلغ 2 جيجابايت على محرك القرص الثابت؛
- وحدة المعالجة المركزية:
  - محطة العمل: 1 جيجا هرتز؛
  - الخادم: 1.4 جيجا هرتز؛
  - دعم مجموعة تعليمات SSE2.
- ذاكرة الوصول العشوائي (RAM):
  - محطة العمل (x86): 1 جيجابايت؛
  - محطة العمل (x64): 2 جيجابايت؛
  - الخادم: 2 جيجابايت.

محطات العمل

أنظمة التشغيل المدعومة لمحطات العمل:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 أو أحدث؛
- Windows 8 Professional / Enterprise؛

- Windows 8.1 Professional / Enterprise؛
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise متعدد الجلسات؛
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise.

للحصول على تفاصيل حول دعم نظام التشغيل Microsoft Windows 10، الرجاء الرجوع إلى قاعدة معارف الدعم الفني.

للحصول على تفاصيل حول دعم نظام التشغيل Microsoft Windows 11، الرجاء الرجوع إلى قاعدة معارف الدعم الفني.

الخوادم

يدعم Kaspersky Endpoint Security المكونات الأساسية للتطبيق على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows للخوادم. ويمكنك استخدام Kaspersky Endpoint Security for Windows بدلاً من Kaspersky Security for Windows Server على الخوادم والمجموعات في مؤسستك (وضع المجموعة). يدعم التطبيق أيضا الوضع الأساسي (راجع المشكلات المعروفة).

أنظمة التشغيل المدعومة للخوادم:

- Windows Small Business Server 2011 Essentials / Standard (64 بت)؛

يتم دعم Microsoft Small Business Server 2011 Standard (64 بت) فقط في حالة تثبيت Service Pack 1 لنظام التشغيل Microsoft Windows Server 2008 R2.

- Windows MultiPoint Server 2011 (64 بت)؛
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 أو أحدث؛
- Windows Web Server 2008 R2 Service Pack 1 أو أحدث؛
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2016 Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2019 Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (بما في ذلك Core Mode).

للحصول على تفاصيل حول الدعم لأنظمة تشغيل Windows Server 2016 و Microsoft Windows Server 2019، الرجاء الرجوع إلى قاعدة معارف الدعم الفني.

للحصول على تفاصيل حول دعم نظام التشغيل Microsoft Windows Server 2022، الرجاء الرجوع إلى قاعدة معارف الدعم الفني.

أنظمة التشغيل غير المدعومة للخوادم:

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 أو أحدث؛

- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 أو أحدث؛
- Windows Server 2008 Standard / Enterprise / Datacenter SP2 أو أحدث؛
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP2 أو أحدث؛
- Microsoft Small Business Server 2008 Standard / Premium SP2 أو أحدث.

الأنظمة الأساسية الافتراضية

الأنظمة الأساسية الافتراضية المدعومة:

- VMware Workstation 17.0 Pro؛
- VMware ESXi 8.0a؛
- Microsoft Hyper-V Server 2019؛
- Citrix Virtual Apps and Desktops 7 2212؛
- Citrix Provisioning 2212؛
- Citrix Hypervisor 8.2 (التحديث التراكمي 1).

الخوادم الطرفية

أنواع الخوادم الطرفية المدعومة:

- Microsoft Remote Desktop Services المعتمد على Windows Server 2008 R2 SP1؛
- Microsoft Remote Desktop Services المعتمد على Windows Server 2012؛
- Microsoft Remote Desktop Services المعتمد على Windows Server 2012 R2؛
- Microsoft Remote Desktop Services المعتمد على Windows Server 2016؛
- Microsoft Remote Desktop Services المعتمد على Windows Server 2019؛
- Microsoft Remote Desktop Services المعتمد على Windows Server 2022.

دعم Kaspersky Security Center

يدعم Kaspersky Endpoint Security الإصدارات التالية من Kaspersky Security Center:

- Kaspersky Security Center 12
- Kaspersky Security Center 13
- Kaspersky Security Center 13.1
- Kaspersky Security Center 13.2

- Kaspersky Security Center 13.2.2
- Kaspersky Security Center 14
- Kaspersky Security Center 14.1
- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2

إجراء مقارنة بين ميزات التطبيق المتاحة تبعًا لنوع نظام التشغيل

تعتمد مجموعة المزايا المتاحة بتطبيقKaspersky Endpoint Security على نوع نظام التشغيل: محطة عمل أو خادم (انظر الجدول أدناه).

مقارنة بين مزايا برنامج Kaspersky Endpoint Security

المزايا	محطة عمل	خادم
الحماية من التهديدات المتقدمة		
Kaspersky Security Network	✓	✓
اكتشاف السلوك	✓	✓
منع الاستغلال	✓	✓
منع اختراق المضيف	✓	–
محرك المعالجة	✓	✓
الحماية من التهديدات الأساسية		
الحماية من تهديدات الملفات	✓	✓
الحماية من تهديدات الويب	✓	✓
الحماية من تهديدات البريد	✓	✓
جدار الحماية	✓	✓
الحماية من تهديدات الشبكة	✓	✓
منع هجمات BadUSB	✓	✓
حماية AMSI	✓	✓
ضوابط الأمان		
فحص السجل	–	✓
التحكم في التطبيقات	✓	✓
التحكم في الجهاز	✓	✓
التحكم في الويب	✓	✓
مراقبة عيوب التكيف	✓	–
مراقبة سلامة الملف	–	✓
تشفير البيانات		
تشفير القرص من Kaspersky	✓	–

تشفير محرك الأقراص من BitLocker	✓	✓
التشفير على مستوى الملف	✓	–
تشفير محركات الأقراص القابلة للإزالة	✓	–
Detection and Response		
Endpoint Detection and Response Optimum	✓	✓
Endpoint Detection and Response Expert	✓	✓
(Endpoint Detection and Response (KATA	✓	✓
Kaspersky Sandbox	✓	✓
(MDR) Managed Detection and Response	✓	✓

مقارنة بين وظائف التطبيق اعتمادا على أدوات الإدارة

تعتمد مجموعة الوظائف المتاحة في Kaspersky Endpoint Security على أدوات الإدارة (انظر الجدول أدناه).

يمكنك إدارة التطبيق باستخدام وحدات التحكم التالية على Kaspersky Security Center:

- وحدة تحكم الإدارة. تم تثبيت الأداة الإضافية لوحدة تحكم Microsoft Management Console (MMC) في محطة عمل المسؤول.
- وحدة تحكم الويب. تم تثبيت مكون Kaspersky Security Center في خادم الإدارة. يمكنك العمل في وحدة التحكم Web Console من خلال مستعرض ويب بأي كمبيوتر يمكن الوصول من خلاله إلى خادم الإدارة.

ويمكنك أيضًا إدارة التطبيق باستخدام وحدة التحكم Kaspersky Security Center Cloud Console. تعد Kaspersky Security Center Cloud Console هي النسخة السحابية من Kaspersky Security Center. هذا يعني أنه تم تثبيت خادم الإدارة والمكونات الأخرى لـ Kaspersky Security Center في البنية الأساسية السحابية لـ Kaspersky. وللمزيد من المعلومات عن إدارة التطبيق باستخدام Kaspersky Security Center Cloud Console، يُرجى الرجوع إلى تعليمات Kaspersky Security Center Cloud Console.

مقارنة بين مزايا برنامج Kaspersky Endpoint Security

المزايا	Kaspersky Security Center		Kaspersky Security Center
	وحدة تحكم الإدارة	وحدة تحكم الويب	وحدة تحكم السحابة
الحماية من التهديدات المتقدمة			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
اكتشاف السلوك	✓	✓	✓
منع الاستغلال	✓	✓	✓
منع اختراق المضيف	✓	✓	✓
محرك المعالجة	✓	✓	✓
الحماية من التهديدات الأساسية			
الحماية من تهديدات الملفات	✓	✓	✓
الحماية من تهديدات الويب	✓	✓	✓
الحماية من تهديدات البريد	✓	✓	✓

جدار الحماية	✓	✓	✓
الحماية من تهديدات الشبكة	✓	✓	✓
منع هجمات BadUSB	✓	✓	✓
حماية AMSI	✓	✓	✓
ضوابط الأمان			
فحص السجل	✓	✓	✓
التحكم في التطبيقات	✓	✓	✓
التحكم في الجهاز	✓	✓	✓
التحكم في الويب	✓	✓	✓
مراقبة عيوب التكيف	✓	✓	✓
مراقبة سلامة الملف	✓	✓	✓
تشفير البيانات			
تشفير القرص من Kaspersky	✓	✓	–
تشفير محرك الأقراص من BitLocker	✓	✓	✓
التشفير على مستوى الملف	✓	✓	–
تشفير محركات الأقراص القابلة للإزالة	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert	–	–	✓
(Endpoint Detection and Response (KATA	✓	✓	–
Kaspersky Sandbox	–	✓	–
(MDR) Managed Detection and Response	✓	✓	✓
المهام			
إضافة مفتاح	✓	✓	✓
تغيير مكونات التطبيق	✓	✓	✓
المخزون	✓	✓	✓
تحديث	✓	✓	✓
تراجع عن التحديث	✓	✓	✓
فحص البرامج الضارة	✓	✓	✓
التحقق من السلامة	✓	✓	–
مسح البيانات	✓	✓	✓
إدارة حسابات وكيل المصادقة (تشفير القرص من Kaspersky)	✓	✓	–
فحص IOC (EDR)	–	✓	✓
نقل الملف إلى العزل (EDR)	–	✓	✓
الحصول على ملف (EDR)	–	✓	✓
حذف الملف (EDR)	–	✓	✓

بدء المعالجة (EDR)	–	✓	✓
إنهاء العملية (EDR)	–	✓	✓

التوافق مع التطبيقات الأخرى

قبل التثبيت، يقوم برنامج Kaspersky Endpoint Security بالتحقق من جهاز الكمبيوتر بحثًا عن وجود تطبيقات Kaspersky. يفحص التطبيق أيضًا الكمبيوتر للبحث عن البرامج غير المتوافقة.

التوافق مع تطبيقات الطرف الثالث

تتوفر قائمة البرامج غير المتوافقة في ملف incompatible.txt المضمن في حزمة التوزيع.

تنزيل ملف INCOMPATIBLE.TXT

التوافق مع تطبيقات Kaspersky

لا يتوافق برنامج Kaspersky Endpoint Security مع تطبيقات Kaspersky التالية:

- تطبيق Kaspersky Small Office Security.
- تطبيق Kaspersky Internet Security.
- تطبيق Kaspersky Anti-Virus.
- تطبيق Kaspersky Total Security.
- تطبيق Kaspersky Safe Kids.
- تطبيق Kaspersky Free.
- تطبيق Kaspersky Anti-Ransomware Tool.
- منصة Kaspersky Anti Targeted Attack Platform (بما في ذلك مكون مستشعر Endpoint).
- Kaspersky Sandbox (يشمل Kaspersky Endpoint Agent).
- Kaspersky Endpoint Detection and Response (يشمل مكون أداة استشعار نقطة النهاية).

إذا كان مكون وكيل نقطة النهاية مثبتًا على كمبيوتر يستخدم أدوات نشر خاصة لتطبيقات أخرى من Kaspersky، فسيتم تلقائيًا إزالة المكون أثناء تثبيت Kaspersky Endpoint Security. وربما يشتمل أيضًا Kaspersky Endpoint Security على مكون أداة استشعار نقطة النهاية/وكيل نقطة النهاية من Kaspersky إذا حددت وكيل نقطة النهاية في قائمة مكونات التطبيق.

- تطبيق Kaspersky Security for Virtualization Light Agent.
- تطبيق Kaspersky Fraud Prevention for Endpoint.
- تطبيق Kaspersky Embedded Systems Security.

إذا كانت تطبيقات Kaspersky الواردة في هذه القائمة مثبتة على جهاز الكمبيوتر، سيقوم برنامج Kaspersky Endpoint Security بإزالة تلك التطبيقات. يُرجى الانتظار حتى انتهاء هذه العملية قبل متابعة تثبيت برنامج Kaspersky Endpoint Security.

تخطي فحص البرامج غير المتوافقة

إذا اكتشف Kaspersky Endpoint Security وجود برامج غير متوافقة على الكمبيوتر، فلن يواصل تثبيت التطبيق. ولمتابعة التثبيت، يجب إزالة البرنامج غير المتوافق. ومع ذلك، إذا أشار مورد برنامج خارجي في وثائقه إلى أن برامجه متوافقة مع Endpoint Protection Platforms (EPP)، فيمكنك تثبيت Kaspersky Endpoint Security على جهاز كمبيوتر يحتوي على تطبيق من هذا البائع. على سبيل المثال، قد يعلن موفر حلول Endpoint Detection and Response (EDR) عن توافقه مع أنظمة EPP الخاصة بجهات خارجية. وإذا كانت هذه هي الحالة، فأنت بحاجة إلى بدء تثبيت Kaspersky Endpoint Security دون إجراء فحص للبرامج غير المتوافقة. ولفعل ذلك، قم بتمرير المعلمات التالية إلى المُثبت:

- `SKIPPRODUCTCHECK=1`. تعطيل التحقق من البرامج غير المتوافقة. تتوفر قائمة البرامج غير المتوافقة في ملف incompatible.txt المضمن في حزمة التوزيع. في حال عدم تحديد قيمة هذه المعلمة وتم اكتشاف برنامج غير متوافق، فسوف يتم إلغاء تثبيت Kaspersky Endpoint Security.
- `SKIPPRODUCTUNINSTALL=1`. تعطيل الإزالة التلقائية للبرامج غير المتوافقة التي تم اكتشافها. في حال عدم تحديد قيمة لهذه المعلمة، فإن Kaspersky Endpoint Security سوف يحاول إزالة البرنامج غير المتوافق.
- `CLEANERSIGNCHECK=0`. تعطيل التحقق من التوقيع الرقمي للبرامج غير المتوافقة المكتشفة. وإذا لم يتم تعيين هذه المعلمة، فسيتم تعطيل التحقق من التوقيعات الرقمية عند نشر التطبيق عبر Kaspersky Security Center. وعند تثبيت التطبيق محليًا، يتم تمكين التحقق من التوقيع الرقمي افتراضيًا.

يمكنك تمرير المعلمات في سطر الأوامر عند تثبيت التطبيق محليًا.

مثال:

```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1
/pSKIPPRODUCTUNINSTALL=1 /pCLEANERSIGNCHECK=0 /s
```

لتثبيت Kaspersky Endpoint Security عن بُعد، تحتاج إلى إضافة المعلمات المناسبة إلى ملف إنشاء حزمة التثبيت المسمى `kes_win.kud` في `[Setup]` (انظر أدناه). ويتم تضمين الملف `kes_win.kud` في مجموعة التوزيع.

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1
/pSKIPPRODUCTUNINSTALL=1 /pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

تثبيت التطبيق وإزالته

يمكن تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر بالطرق التالية:

- محليًا، عن طريق استخدام معالج الإعداد.
- محليًا من سطر الأوامر.
- عن بُعد باستخدام Kaspersky Security Center.
- عن بُعد من خلال استخدام محرر إدارة نهج مجموعة Microsoft Windows (للحصول على المزيد من التفاصيل، يرجى زيارة موقع ويب الدعم الفني لشركة Microsoft).
- عن بُعد، من خلال استخدام System Center Configuration Manager.

يمكنك تكوين إعدادات تثبيت التطبيق بعدة طرق. إذا كنت تستخدم طرقًا متعددة في نفس الوقت لتكوين الإعدادات، فإن برنامج Kaspersky Endpoint Security يقوم بتطبيق الإعدادات ذات الأولوية القصوى. يستخدم برنامج Kaspersky Endpoint Security الترتيب التالي للأولويات:

1. الإعدادات التي تم استلامها من ملف setup.ini.
2. الإعدادات التي تم استلامها من ملف installer.ini.
3. الإعدادات التي تم استلامها من سطر الأوامر.

نوصي بغلق جميع التطبيقات قيد التشغيل قبل بدء تثبيت برنامج Kaspersky Endpoint Security (بما في ذلك التثبيت عن بعد).

النشر من خلال Kaspersky Security Center

يمكن نشر برنامج Kaspersky Endpoint Security على أجهزة الكمبيوتر الموجودة داخل الشبكة الخاصة بالشركة بعدة طرق. يمكنك اختيار سيناريو النشر الأكثر ملاءمة للمؤسسة الخاصة بك أو دمج العديد من سيناريوهات النشر في نفس الوقت. يدعم Kaspersky Security Center طرق النشر الرئيسية التالية:

- تثبيت التطبيق باستخدام معالج نشر الحماية.

  طريقة التثبيت القياسية هي الأكثر ملاءمة في حال كنت راضيًا عن الإعدادات الافتراضية الخاصة ببرنامج Kaspersky Endpoint Security وإذا كانت المؤسسة التابع إليها تحتوي على بنية أساسية بسيطة لا تتطلب تكوينات خاصة.

- تثبيت التطبيق باستخدام مهمة التثبيت عن بعد.

  طريقة التثبيت الشاملة، والتي تتيح لك تكوين إعدادات برنامج Kaspersky Endpoint Security وإدارة مهام التثبيت عن بُعد بمرونة. يتكون التثبيت الخاص ببرنامجKaspersky Endpoint Security من الخطوات التالية:

  1. إنشاء حزمة التثبيت.
  2. إنشاء مهمة تثبيت عن بعد.

يدعم Kaspersky Security Center أيضًا طرقًا أخرى لتثبيت برنامج Kaspersky Endpoint Security مثل النشر داخل صورة نظام التشغيل. وللحصول على تفاصيل حول طرق النشر الأخرى، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

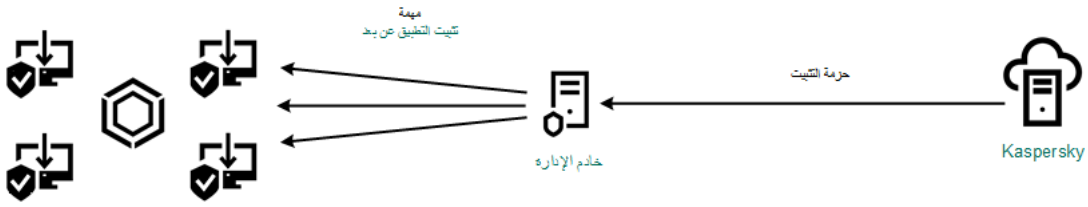
التثبيت القياسي للتطبيق

Kaspersky Security Center يوفر معالج نشر حماية لتثبيت التطبيق على أجهزة كمبيوتر الشركة. يتضمن معالج نشر الحماية الإجراءات الرئيسية التالية:

1. حدد حزمة التثبيت الخاصة ببرنامج Kaspersky Endpoint Security.

   حزمة التثبيت هي مجموعة من الملفات التي تم إنشاؤها للتثبيت عن بعد لتطبيق Kaspersky عبر Kaspersky Security Center. تحتوي حزمة التثبيت على مجموعة من الإعدادات المطلوبة لتثبيت التطبيق وتشغيله فورًا بعد التثبيت. يتم إنشاء حزمة التثبيت باستخدام الملفات ذات الامتدادات kpd. وkud. في حزمة توزيع التطبيق. تعد حزمة تثبيت Kaspersky Endpoint Security ميزة شائعة لجميع الإصدارات المدعومة لأنظمة تشغيل Windows وأنواع بنية المعالج.

2. إنشاء المهمة تثبيت التطبيق عن بُعد الخاصة بخادم الإدارة Kaspersky Security Center.



نشر Kaspersky Endpoint Security

كيفية تشغيل معالج نشر الحماية في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى المجلد **خادم الإدارة** ← **إضافي** ← **التثبيت عن بُعد**.

2. انقر فوق الرابط **نشر حزمة التثبيت على الأجهزة المُدارة (محطات العمل)**.

سوف يؤدي هذا إلى بدء معالج نشر الحماية. اتبع تعليمات المعالج.

يجب فتح منافذ TCP 139 و 445 ومنافذ UDP 137 و 138 على جهاز كمبيوتر عميل.

الخطوة 1. تحديد حزمة تثبيت

حدد حزمة تثبيت Kaspersky Endpoint Security من القائمة. إذا كانت القائمة لا تحتوي على حزمة التثبيت الخاصة ببرنامج Kaspersky Endpoint Security، فيمكنك إنشاء الحزمة في المعالج.

يمكنك تكوين إعدادات حزمة التثبيت في Kaspersky Security Center. علي سبيل المثال يمكنك تحديد مكونات التطبيق التي سيتم تثبيتها على جهاز الكمبيوتر.

سيتم أيضًا تثبيت وكيل الشبكة مع Kaspersky Endpoint Security. يسهل عميل الشبكة التفاعل بين خادم الإدارة وجهاز العميل. إذا كان عميل الشبكة مثبتًا بالفعل على جهاز الكمبيوتر، فلن يتم تثبيته مرة أخرى.

الخطوة الثانية: اختيار أجهزة الكمبيوتر للتثبيت

حدد أجهزة الكمبيوتر لتثبيت برنامج Kaspersky Endpoint Security. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. لم يتم تثبيت عميل الشبكة على الأجهزة غير المخصصة. في هذه الحالة يتم تعيين المهمة لأجهزة محددة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الثالثة: تعريف إعدادات مهمة التثبيت عن بُعد

قم بتكوين إعدادات التطبيق الإضافية التالية:

- **تنزيل حزمة التثبيت الإجباري**. حدد طريقة تثبيت التطبيق:
  - **استخدام عميل الشبكة**. إذا لم يتم تثبيت عميل الشبكة على الكمبيوتر فسيتم تثبيت عميل الشبكة الأول باستخدام أدوات نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.
  - **استخدام موارد نظام التشغيل عبر نقاط التوزيع**. يتم تسليم حزمة التثبيت إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل عبر نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت هناك نقطة توزيع واحدة على الأقل في الشبكة. وللمزيد من التفاصيل حول نقاط التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.
  - **استخدام موارد نظام التشغيل من خلال خادم الإدارة**. سيتم تسليم الملفات إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل من خلال خادم الإدارة. يمكنك تحديد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على جهاز الكمبيوتر العميل، ولكن جهاز الكمبيوتر العميل يتواجد على نفس الشبكة باعتباره خادم إدارة.

- **السلوك المخصص للأجهزة المُدارة من خلال خوادم الإدارة الأخرى**. حدد حزمة التثبيت الخاصة ببرنامج Kaspersky Endpoint Security. إذا كانت الشبكة تحتوي على أكثر من خادم إدارة مثبت فقد تري خوادم الإدارة نفس أجهزة الكمبيوتر العميلة. قد يتسبب ذلك على سبيل المثال، في تثبيت تطبيق عن بُعد على جهاز العميل نفسه عدة مرات من خلال خوادم إدارة مختلفة، أو حدوث تعارضات أخرى.

- **لا تقم بإعادة تثبيت التطبيق إذا كان مثبتًا بالفعل**. قم بمسح مربع الاختيار هذا إذا كنت تريد تثبيت إصدار سابق من التطبيق على سبيل المثال.

- **تعيين تثبيت عميل الشبكة في سياسات مجموعة Active Directory**. التثبيت اليدوي لعميل الشبكة باستخدام موارد Active Directory. لتثبيت عميل الشبكة يجب تشغيل مهمة التثبيت عن بعد مع امتيازات مسؤول المجال.

الخطوة 4. اختيار عميل الشبكة

أضف مفتاحًا لحزمة التثبيت لتفعيل التطبيق. تعتبر هذه الخطوة اختيارية. إذا كان خادم الإدارة يحتوي على مفتاح ترخيص مع وظيفة التوزيع التلقائي، فسيتم إضافة المفتاح تلقائيًا لاحقًا. يمكنك أيضًا تفعيل التطبيق لاحقًا باستخدام مهمة إضافة مفتاح.

الخطوة الخامسة: تحديد إعداد إعادة تشغيل نظام التشغيل

حدد الإجراء المراد تنفيذه إذا كانت إعادة تشغيل جهاز الكمبيوتر مطلوبة. إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. إعادة التشغيل مطلوبة فقط إذا كان يجب عليك إزالة التطبيقات غير المتوافقة قبل التثبيت. قد تكون إعادة التشغيل مطلوبة أيضًا عند تحديث إصدار التطبيق.

الخطوة السادسة: إزالة التطبيقات غير المتوافقة قبل تثبيت التطبيق

في هذه الخطوة، اقرأ بعناية قائمة التطبيقات غير المتوافقة واسمح بإزالة هذه التطبيقات. في حالة تثبيت تطبيقات غير متوافقة على الكمبيوتر ينتهي تثبيت Kaspersky Endpoint Security بخطأ (انظر الشكل أدناه).

الخطوة السابعة: تحديد حساب للوصول إلى الأجهزة

حدد في هذه الخطوة الحساب المستخدم لتثبيت عميل الشبكة باستخدام أدوات نظام التشغيل. في هذه الحالة، تكون حقوق المسؤول مطلوبة للوصول إلى جهاز الكمبيوتر. يمكنك إضافة حسابات عديدة. إذا لم يكن للحساب حقوق كافية يستخدم معالج التثبيت الحساب التالي. إذا قمت بتثبيت برنامج Kaspersky Endpoint Security باستخدام أدوات عميل الشبكة فلا يلزم تحديد حساب.

الخطوة الثامنة: بدء التثبيت

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية بدء معالج نشر الحماية في Web Console وCloud Console

في نافذة Web Console الرئيسية، حدد **Protection** ← **Deployment & Assignment** ← **Discovery & Deployment** **Deployment Wizard**.

سوف يؤدي هذا إلى بدء معالج نشر الحماية. اتبع تعليمات المعالج.

يجب فتح منافذ TCP 139 و 445 ومنافذ UDP 137 و 138 على جهاز كمبيوتر عميل.

الخطوة 1. تحديد حزمة تثبيت

حدد حزمة تثبيت Kaspersky Endpoint Security من القائمة. إذا كانت القائمة لا تحتوي على حزمة التثبيت الخاصة ببرنامج Kaspersky Endpoint Security، فيمكنك إنشاء الحزمة في المعالج. لإنشاء حزمة التثبيت، لا تحتاج إلى البحث عن حزمة التوزيع وحفظها في ذاكرة جهاز الكمبيوتر. في Kaspersky Security Center، يمكنك عرض قائمة حزم التوزيع الموجودة على خوادم Kaspersky، ويتم إنشاء حزمة التثبيت تلقائيًا. تقوم Kaspersky بتحديث القائمة بعد تنزيل إصدارات جديدة من التطبيقات.

يمكنك تكوين إعدادات حزمة التثبيت في Kaspersky Security Center. على سبيل المثال يمكنك تحديد مكونات التطبيق التي سيتم تثبيتها على جهاز الكمبيوتر.

الخطوة 2. اختيار عميل الشبكة

أضف مفتاحًا لحزمة التثبيت لتفعيل التطبيق. تعتبر هذه الخطوة اختيارية. إذا كان خادم الإدارة يحتوي على مفتاح ترخيص مع وظيفة التوزيع التلقائي، فسيتم إضافة المفتاح تلقائيًا لاحقًا. يمكنك أيضًا تفعيل التطبيق لاحقًا باستخدام مهمة إضافة مفتاح.

الخطوة 3. اختيار عميل الشبكة

حدد إصدار عميل الشبكة الذي سيتم تثبيته مع برنامج Kaspersky Endpoint Security. يسهل عميل الشبكة التفاعل بين خادم الإدارة وجهاز العميل. إذا كان عميل الشبكة مثبتًا بالفعل على جهاز الكمبيوتر، فلن يتم تثبيته مرة أخرى.

الخطوة الرابعة: اختيار أجهزة الكمبيوتر للتثبيت

حدد أجهزة الكمبيوتر لتثبيت برنامج Kaspersky Endpoint Security. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. لم يتم تثبيت عميل الشبكة على الأجهزة غير المخصصة. في هذه الحالة يتم تعيين المهمة لأجهزة محددة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة 5. تكوين الإعدادات المتقدمة

قم بتكوين إعدادات التطبيق الإضافية التالية:

- **Force installation package download**. اختيار طريقة تثبيت التطبيق:
  - **استخدام عميل الشبكة**. إذا لم يتم تثبيت عميل الشبكة على الكمبيوتر فسيتم تثبيت عميل الشبكة الأول باستخدام أدوات نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.

- **استخدام موارد نظام التشغيل عبر نقاط التوزيع**. يتم تسليم حزمة التثبيت إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل عبر نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت هناك نقطة توزيع واحدة على الأقل في الشبكة. وللمزيد من التفاصيل حول نقاط التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

- **استخدام موارد نظام التشغيل من خلال خادم الإدارة**. سيتم تسليم الملفات إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل من خلال خادم الإدارة. يمكنك تحديد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على جهاز الكمبيوتر العميل، ولكن جهاز الكمبيوتر العميل يتواجد على نفس الشبكة باعتباره خادم إدارة.

- **لا تقم بإعادة تثبيت التطبيق إذا كان مثبتًا بالفعل**. قم بمسح مربع الاختيار هذا إذا كنت تريد تثبيت إصدار سابق من التطبيق على سبيل المثال.

- **Assign package installation in Active Directory group policies**. يتم تثبيت برنامج Kaspersky Endpoint Security عن طريق عميل الشبكة أو يدويًا عن طريق Active Directory. لتثبيت عميل الشبكة يجب تشغيل مهمة التثبيت عن بعد مع امتيازات مسؤول المجال.

الخطوة السادسة: تحديد إعداد إعادة تشغيل نظام التشغيل

حدد الإجراء المراد تنفيذه إذا كانت إعادة تشغيل جهاز الكمبيوتر مطلوبة. إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. إعادة التشغيل مطلوبة فقط إذا كان يجب عليك إزالة التطبيقات غير المتوافقة قبل التثبيت. قد تكون إعادة التشغيل مطلوبة أيضًا عند تحديث إصدار التطبيق.

الخطوة السابعة: إزالة التطبيقات غير المتوافقة قبل تثبيت التطبيق

في هذه الخطوة، اقرأ بعناية قائمة التطبيقات غير المتوافقة واسمح بإزالة هذه التطبيقات. في حالة تثبيت تطبيقات غير متوافقة على الكمبيوتر ينتهي تثبيت Kaspersky Endpoint Security بخطأ (انظر الشكل أدناه).

الخطوة 8. تعيين مجموعة الإدارة

حدد مجموعة الإدارة التي سيتم نقل الكمبيوتر إليها بعد تثبيت عميل الشبكة. تحتاج أجهزة الكمبيوتر إلى النقل إلى مجموعة إدارة حتى يمكن تطبيق السياسات والمهام الجماعية. إذا كان الكمبيوتر في أي مجموعة إدارة بالفعل، فلن يتم نقل الكمبيوتر. إذا لم تقم بتحديد مجموعة إدارة، فستتم إضافة أجهزة الكمبيوتر إلى المجموعة **الأجهزة غير المخصصة**.

الخطوة التاسعة: تحديد حساب للوصول إلى الأجهزة

حدد في هذه الخطوة الحساب المستخدم لتثبيت عميل الشبكة باستخدام أدوات نظام التشغيل. في هذه الحالة، تكون حقوق المسؤول مطلوبة للوصول إلى جهاز الكمبيوتر. يمكنك إضافة حسابات عديدة. إذا لم يكن للحساب حقوق كافية يستخدم معالج التثبيت الحساب التالي. إذا قمت بتثبيت برنامج Kaspersky Endpoint Security باستخدام أدوات عميل الشبكة فلا يلزم تحديد حساب.

الخطوة 10. بدء التثبيت

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

إنشاء حزمة التثبيت

حزمة التثبيت هي مجموعة من الملفات التي تم إنشاؤها للتثبيت عن بعد لتطبيق Kaspersky عبر Kaspersky Security Center. تحتوي حزمة التثبيت على مجموعة من الإعدادات المطلوبة لتثبيت التطبيق وتشغيله فورًا بعد التثبيت. يتم إنشاء حزمة التثبيت باستخدام الملفات ذات الامتدادات kpd. وkud. في حزمة توزيع التطبيق. تعد حزمة تثبيت Kaspersky Endpoint Security ميزة شائعة لجميع الإصدارات المدعومة لأنظمة تشغيل Windows وأنواع بنية المعالج.

كيفية إنشاء حزمة تثبيت في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى المجلد **خادم الإدارة** ← **إضافي** ← **التثبيت عن بُعد** ← **حزم التثبيت**.
   يؤدي ذلك إلى فتح قائمة بحزم التثبيت التي تم تنزيلها إلى Kaspersky Security Center.
2. انقر فوق الزر **إنشاء حزمة التثبيت**.

يبدأ معالج الحزمة الجديدة. اتبع تعليمات المعالج.

الخطوة 1. تحديد نوع حزمة التثبيت

حدد الخيار **إنشاء حزمة تثبيت لتطبيق Kaspersky**.

الخطوة الثانية: تحديد اسم نوع حزمة التثبيت

أدخل اسم حزمة التثبيت، مثل Kaspersky Endpoint Security for Windows 12.1.

الخطوة الثالثة: حدد حزمة التوزيع للتثبيت

حدد الزر **استعراض** ثم حدد الملف `kes_win.kud` المُدرج في حزمة التوزيع.

إذا كان ذلك ضروريًا، قم بتحديث قواعد بيانات مكافحة الفيروسات في حزمة التثبيت عن طريق استخدام خانة الاختيار **نسخ التحديثات من المستودع إلى حزمة التثبيت**.

الخطوة الرابعة: اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية

اقرأ شروط اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية ووافق عليهما.

سيتم إنشاء حزمة التثبيت وإضافتها إلى Kaspersky Security Center. باستخدام حزمة التثبيت، يمكنك تثبيت برنامج Kaspersky Endpoint Security على أجهزة الكمبيوتر الخاصة بشبكة الشركة أو تحديث إصدار التطبيق. في إعدادات حزمة التثبيت، يمكنك أيضًا تحديد مكونات التطبيق وتكوين إعدادات تثبيت التطبيق (انظر الجدول أدناه). تحتوي حزمة التثبيت على قواعد بيانات مكافحة الفيروسات المستمدة من مستودع خادم الإدارة. يمكنك تحديث قواعد البيانات في حزمة التثبيت للحد من استخدام حركة المرور عند تحديث قواعد البيانات بعد تثبيت Kaspersky Endpoint Security.

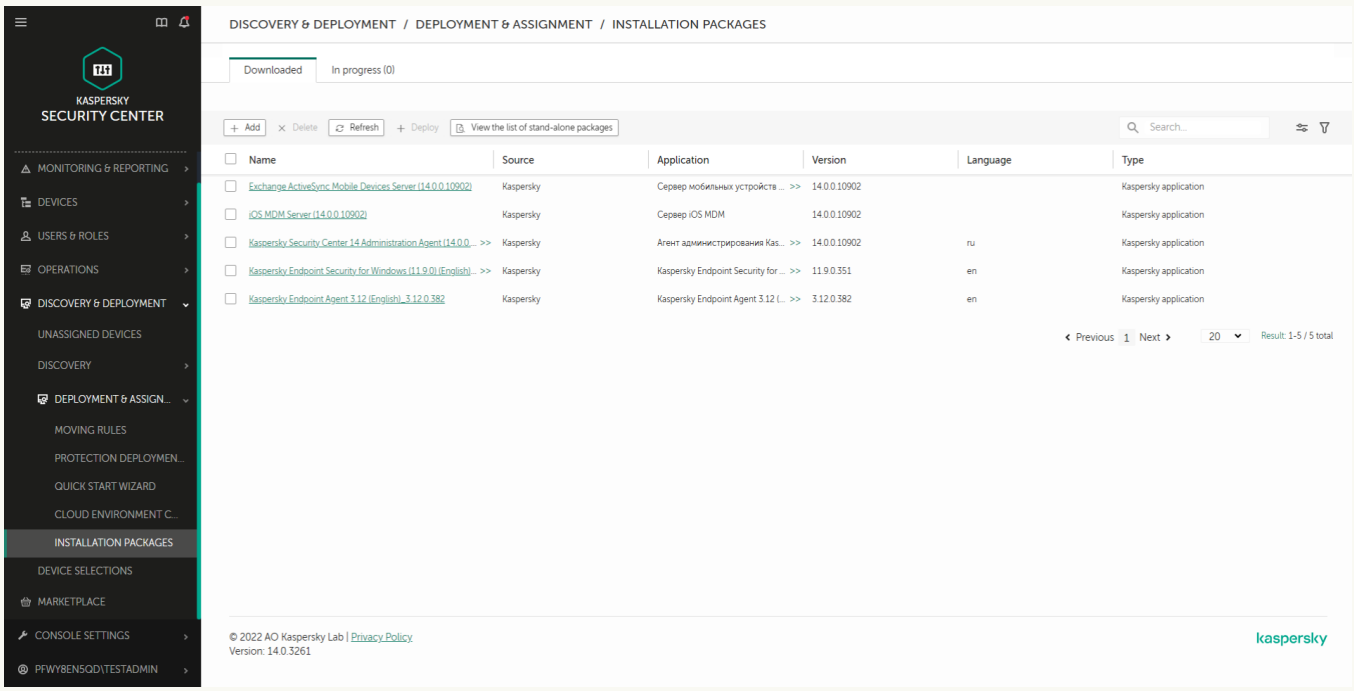
كيفية إنشاء حزمة تثبيت في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Discovery & Deployment ← Deployment & Assignment ← Installation packages**.

يؤدي ذلك إلى فتح قائمة بحزم التثبيت التي تم تنزيلها إلى Kaspersky Security Center.

2. انقر على الزر **Add**.

يبدأ معالج الحزمة الجديدة. اتبع تعليمات المعالج.



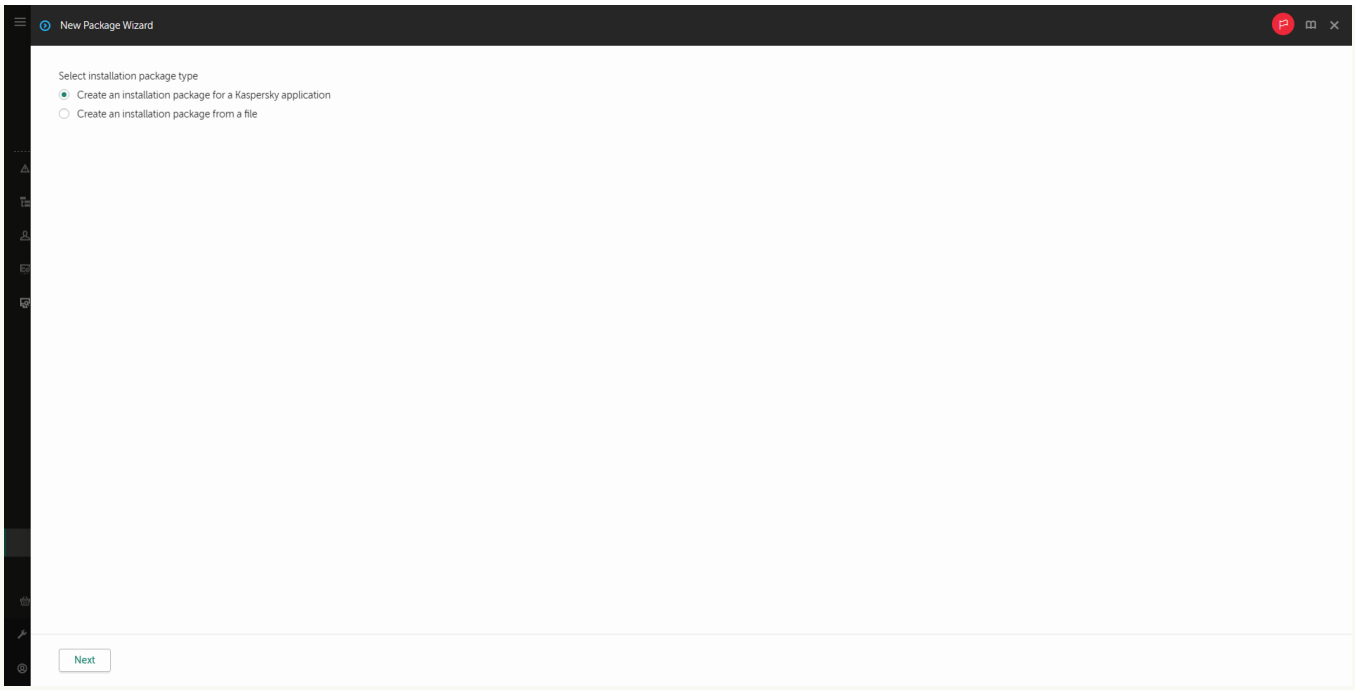
قائمة حزم التثبيت

الخطوة 1. تحديد نوع حزمة التثبيت

فحدد الخيار **Create an installation package for a Kaspersky application**.

سيقوم المعالج بإنشاء حزمة التثبيت من حزمة التوزيع الموجودة على خوادم Kaspersky. يتم تحديث القائمة تلقائيًا حيث يتم إطلاق إصدارات جديدة من التطبيقات. يُوصى بتحديد هذا الخيار لتثبيت برنامج Kaspersky Endpoint Security.

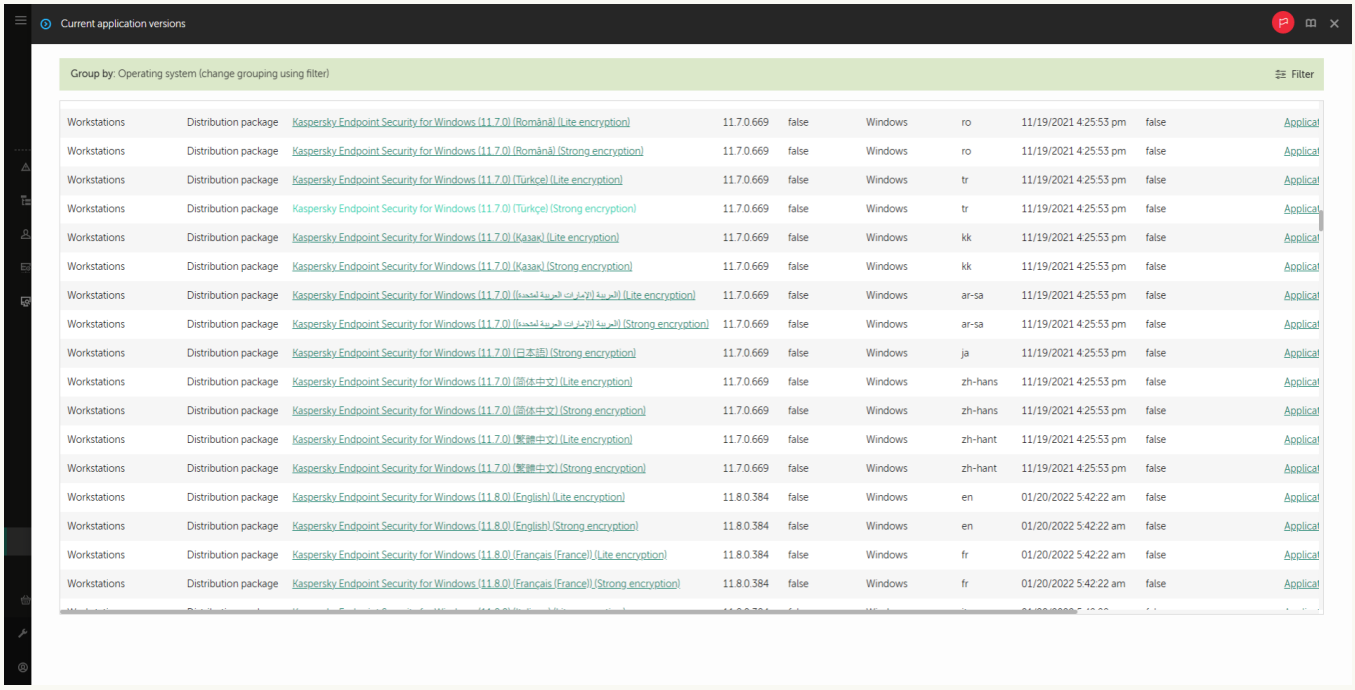
يمكنك أيضًا إنشاء حزمة التثبيت من ملف.



أنواع حزم التثبيت

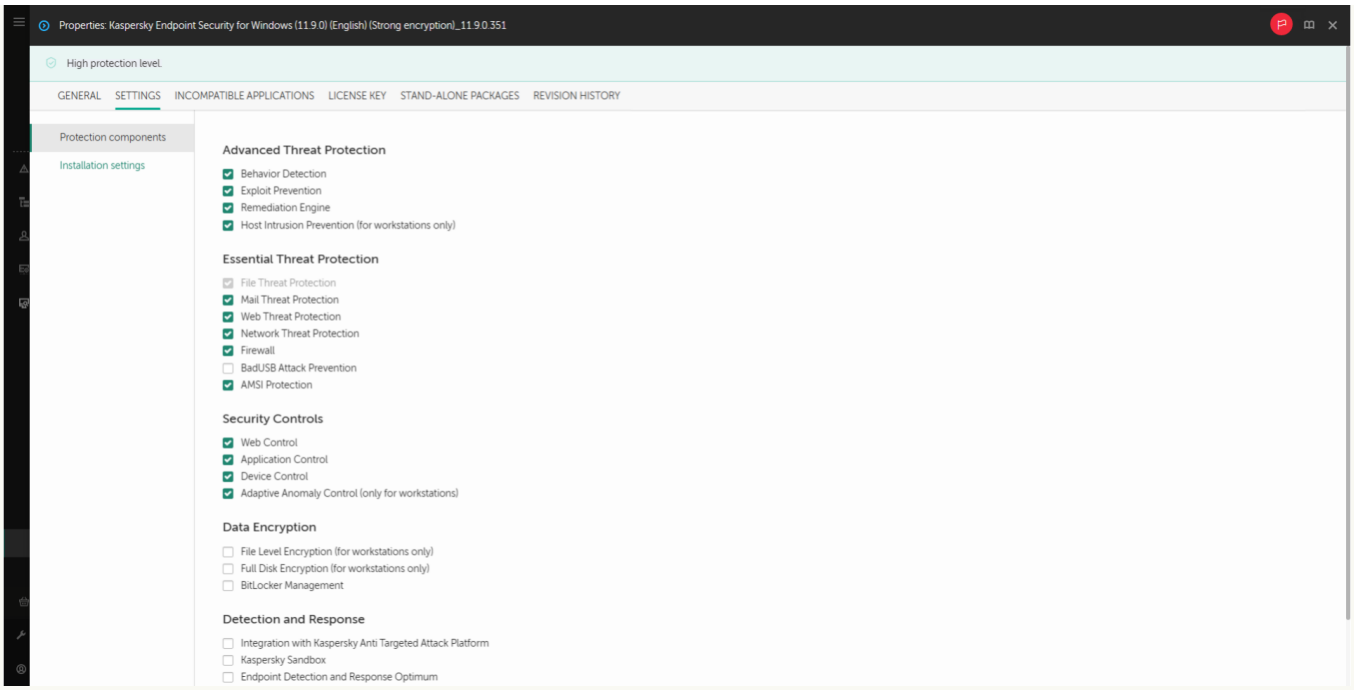
الخطوة 2. حزم التثبيت

حدد حزمة تثبيت Kaspersky Endpoint Security for Windows. بدء عملية إنشاء حزمة التثبيت. أثناء إنشاء حزمة التثبيت، يجب عليك أن تقبل شروط اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية.

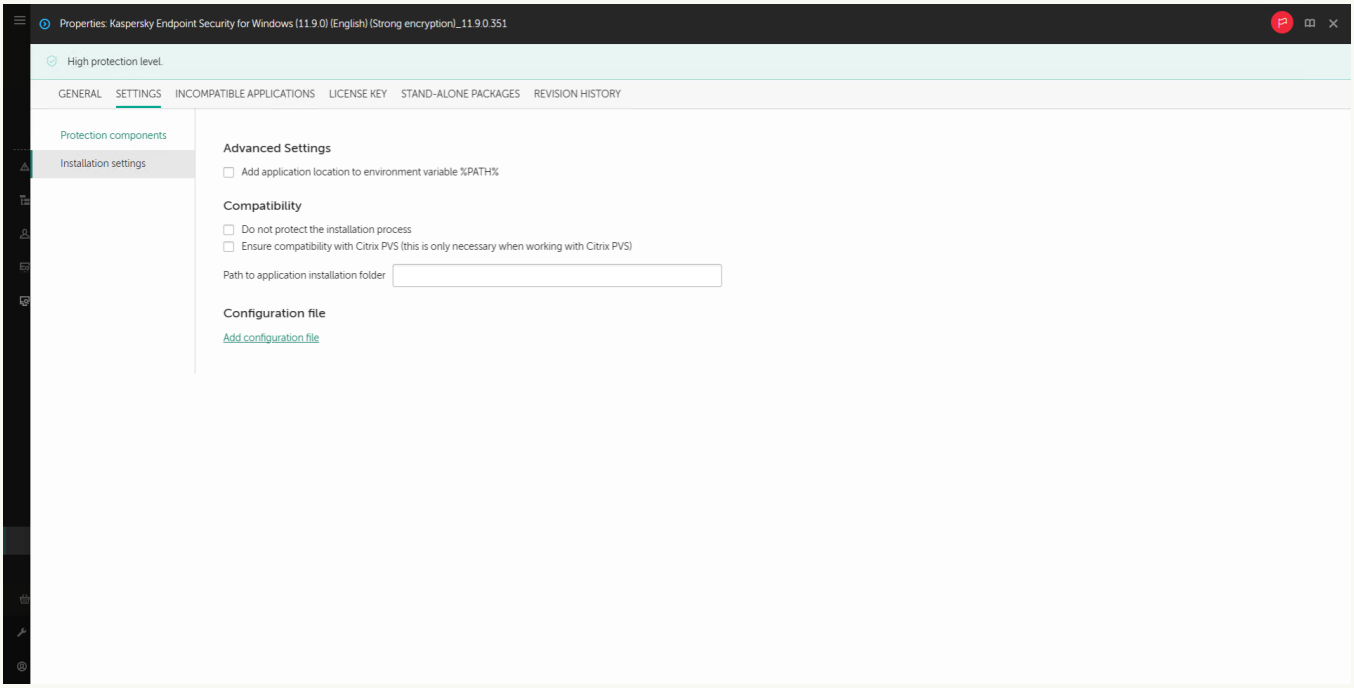


قائمة حزم التثبيت على خوادم Kaspersky

سيتم إنشاء حزمة التثبيت وإضافتها إلى Kaspersky Security Center. باستخدام حزمة التثبيت، يمكنك تثبيت برنامج Kaspersky Endpoint Security على أجهزة الكمبيوتر الخاصة بشبكة الشركة أو تحديث إصدار التطبيق. في إعدادات حزمة التثبيت، يمكنك أيضًا تحديد مكونات التطبيق وتكوين إعدادات تثبيت التطبيق (انظر الجدول أدناه). تحتوي حزمة التثبيت على قواعد بيانات مكافحة الفيروسات المستمدة من مستودع خادم الإدارة. يمكنك تحديث قواعد البيانات في حزمة التثبيت للحد من استخدام حركة المرور عند تحديث قواعد البيانات بعد تثبيت Kaspersky Endpoint Security.



المكونات المضمنة في حزمة التثبيت



إعدادات تثبيت حزمة التثبيت

إعدادات حزمة التثبيت

القسم	الوصف
Protection components	في هذا القسم يمكنك تحديد مكونات التطبيق التي ستكون متاحة. يمكنك تغيير مجموعة مكونات التطبيق في وقت لاحق من خلال استخدام المهمة تغيير مكونات التطبيق. لم يتم تثبيت مكون منع هجمات BadUSB ومكون Detection and Response ومكونات تشفير البيانات بشكل افتراضي. ويمكن إضافة هذه المكونات في إعدادات حزمة التثبيت. إذا كنت بحاجة إلى تثبيت مكونات Detection and Response، يدعم Kaspersky Endpoint Security التكوينات التالية: • Endpoint Detection and Response Optimum فقط • Endpoint Detection and Response Expert فقط

	• Endpoint Detection and Response (KATA) فقط • Kaspersky Sandbox فقط • Endpoint Detection and Response Optimum وKaspersky Sandbox • Endpoint Detection and Response Expert وKaspersky Sandbox • Endpoint Detection and Response (KATA) وKaspersky Sandbox يتحقق Kaspersky Endpoint Security من تحديد المكونات قبل تثبيت التطبيق. وفي حالة عدم دعم التكوين المحدد لمكونات Detection and Response، يمكن تثبيت Kaspersky Endpoint Security.
License key	في هذا القسم، يمكنك تفعيل التطبيق. ولتفعيل التطبيق، يجب عليك تحديد مفتاح ترخيص. وقبل فعل ذلك ،يجب عليك إضافة المفتاح إلى خادم الإدارة. للمزيد من التفاصيل حول إضافة المفاتيح إلى خادم إدارة Kaspersky Security Center، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.
Incompatible Applications	في هذه الخطوة، اقرأ بعناية قائمة التطبيقات غير المتوافقة واسمح بإزالة هذه التطبيقات. في حالة تثبيت تطبيقات غير متوافقة على الكمبيوتر ينتهي تثبيت Kaspersky Endpoint Security بخطأ.
Installation settings	**إضافة مسار إلى الملف avp.com إلى متغير النظام %PATH%**. يمكنك إضافة مسار التثبيت إلى المتغير %PATH% من أجل الاستخدام السهل لواجهة سطر الأوامر. **Do not protect the installation process**. تتضمن حماية التثبيت الحماية من استبدال حزمة التوزيع باستخدام التطبيقات الضارة ومنع الوصول إلى مجلد تثبيت برنامج Kaspersky Endpoint Security ومنع الوصول إلى قسم تسجيل النظام الذي يحتوي على مفاتيح التطبيق. وعلى الرغم من ذلك، إذا تعذر تثبيت التطبيق (على سبيل المثال، عند إجراء التثبيت عن بُعد باستخدام تعليمات Windows Remote Desktop)، ينصح حينئذ بتعطيل حماية عملية التثبيت. **تأكيد التوافق مع Citrix PVS (يعتبر هذا الخيار ضروريًا فقط عند العمل مع Citrix PVS)**. يمكنك تمكين دعم خدمات Citrix التزويد لتثبيت برنامج Kaspersky Endpoint Security إلى جهاز ظاهري. **استخدم وضع التوافق مع Azure WVD**. تتيح هذه الميزة عرض حالة جهاز Azure الظاهري بشكل صحيح في وحدة التحكم لتطبيق Kaspersky Anti Targeted Attack Platform. ولمراقبة أداء الكمبيوتر، يرسل Kaspersky Endpoint Security بيانات القياس عن بُعد إلى خوادم KATA. ويتضمن القياس عن بعد معرف الكمبيوتر (معرف المستشعر). ويسمح وضع التوافق مع Azure WVD بتعيين معرف مستشعر فريد دائم لهذه الأجهزة الظاهرية. وفي حالة إيقاف تشغيل وضع التوافق، يمكن أن يتغير معرف المستشعر بعد إعادة تشغيل الكمبيوتر بسبب كيفية عمل أجهزة Azure الظاهرية. ومن الممكن أن يتسبب هذا في ظهور نسخ مكررة من الأجهزة الظاهرية على وحدة التحكم. **Path to application installation folder**. يمكنك تغيير مسار تثبيت برنامج Kaspersky Endpoint Security على كمبيوتر العميل. افتراضيًا، يتم تثبيت التطبيق في المجلد `%ProgramFiles%\Kaspersky Lab\KES`. **Configuration file**. يمكنك تحميل ملف يحدد إعدادات برنامج Kaspersky Endpoint Security. يمكنك إنشاء ملف تكويني في الواجهة المحلية للتطبيق.

تحديث قواعد البيانات في حزمة التثبيت

تحتوي حزمة التثبيت على قواعد بيانات مكافحة الفيروسات المستمدة من مستودع خادم الإدارة والتي تشتمل على بيانات حديثة وقت إنشاء حزمة التثبيت. بعد إنشاء حزمة التثبيت، يمكنك تحديث قواعد بيانات مكافحة الفيروسات في حزمة التثبيت. سيتيح لك ذلك تقليل استخدام حركة المرور عند تحديث قواعد بيانات مكافحة الفيروسات بعد تثبيت Kaspersky Endpoint Security.

لتحديث قواعد بيانات مكافحة الفيروسات في مستودع خادم الإدارة، استعن بمهمة تنزيل تحديثات لمستودع خادم الإدارة الخاصة بخادم الإدارة. وللمزيد من المعلومات عن تحديث قواعد بيانات مكافحة الفيروسات في مستودع خادم الإدارة، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

يمكنك تحديث قواعد البيانات في حزمة التثبيت فقط في وحدة تحكم الإدارة ووحدة تحكم Kaspersky Security Center. لا يمكن تحديث قواعد البيانات في حزمة التثبيت في وحدة التحكم Kaspersky Security Center Cloud Console.

كيفية تحديث قواعد بيانات مكافحة الفيروسات في حزمة التثبيت من خلال وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى المجلد **خادم الإدارة** ← **إضافي** ← **التثبيت عن بُعد** ← **حزم التثبيت**.

يؤدي ذلك إلى فتح قائمة بحزم التثبيت التي تم تنزيلها إلى Kaspersky Security Center.

2. افتح خصائص حزمة التثبيت.

3. في قسم **عام**، انقر فوق زر **تحديث قواعد البيانات**.

نتيجةً لذلك، سيتم تحديث قواعد بيانات مكافحة الفيروسات في حزمة التثبيت من مستودع خادم الإدارة. سيتم استبدال ملف `bases.cab` الموجود في مجموعة التوزيع بمجلد `bases`. ستكون ملفات حزمة التحديث داخل المجلد.

كيفية تحديث قواعد بيانات مكافحة الفيروسات في حزمة تثبيت من خلال Web Control

1. في نافذة Web Console الرئيسية، حدد **Installation** ← **Deployment & Assignment** ← **Discovery & Deployment** ← **packages**.

يؤدي هذا إلى فتح قائمة حزم التثبيت التي تم تنزيلها لـ Web Console.

2. انقر فوق اسم حزمة التثبيت الخاصة بـ Kaspersky Endpoint Security التي تريد تحديث قواعد بيانات مكافحة الفيروسات بها.

سيتم فتح نافذة خصائص حزمة التثبيت.

3. في علامة التبويب **General information**، انقر فوق الرابط **Update databases**.

نتيجةً لذلك، سيتم تحديث قواعد بيانات مكافحة الفيروسات في حزمة التثبيت من مستودع خادم الإدارة. سيتم استبدال ملف `bases.cab` الموجود في مجموعة التوزيع بمجلد `bases`. ستكون ملفات حزمة التحديث داخل المجلد.

إنشاء مهمة تثبيت عن بعد

مهمة تثبيت التطبيق عن بُعد مصممة لتثبيت تطبيق Kaspersky Endpoint Security عن بُعد. تسمح لك مهمة تثبيت التطبيق عن بُعد بنشر حزمة تثبيت التطبيق على جميع أجهزة الكمبيوتر في المؤسسة. قبل نشر حزمة التثبيت، يمكنك تحديث قواعد بيانات مكافحة الفيروسات داخل الحزمة وتحديد مكونات التطبيق المتاحة في خصائص حزمة التثبيت.

كيفية إنشاء مهمة تثبيت عن بُعد في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **خادم إدارة Kaspersky Security Center** ← **تثبيت التطبيق عن بُعد**.

الخطوة 2. تحديد حزمة تثبيت

حدد حزمة تثبيت Kaspersky Endpoint Security من القائمة. إذا كانت القائمة لا تحتوي على حزمة التثبيت الخاصة ببرنامج Kaspersky Endpoint Security، فيمكنك إنشاء الحزمة في المعالج.

يمكنك تكوين إعدادات حزمة التثبيت في Kaspersky Security Center. علي سبيل المثال يمكنك تحديد مكونات التطبيق التي سيتم تثبيتها على جهاز الكمبيوتر.

سيتم أيضًا تثبيت وكيل الشبكة مع Kaspersky Endpoint Security. يسهل عميل الشبكة التفاعل بين خادم الإدارة وجهاز العميل. إذا كان عميل الشبكة مثبتًا بالفعل على جهاز الكمبيوتر، فلن يتم تثبيته مرة أخرى.

الخطوة الثالثة: إضافي

حدد حزمة تثبيت عميل الشبكة. سيتم تثبيت الإصدار المُحدد من عميل الشبكة مع برنامج Kaspersky Endpoint Security.

الخطوة 4. الإعدادات

قم بتكوين إعدادات التطبيق الإضافية التالية:

- **تنزيل حزمة التثبيت الإجباري**. حدد طريقة تثبيت التطبيق:
  - **استخدام عميل الشبكة**. إذا لم يتم تثبيت عميل الشبكة على الكمبيوتر فسيتم تثبيت عميل الشبكة الأول باستخدام أدوات نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.
  - **استخدام موارد نظام التشغيل عبر نقاط التوزيع**. يتم تسليم حزمة التثبيت إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل عبر نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت هناك نقطة توزيع واحدة على الأقل في الشبكة. وللمزيد من التفاصيل حول نقاط التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.
  - **استخدام موارد نظام التشغيل من خلال خادم الإدارة**. سيتم تسليم الملفات إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل من خلال خادم الإدارة. يمكنك تحديد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على جهاز الكمبيوتر العميل، ولكن جهاز الكمبيوتر العميل يتواجد على نفس الشبكة باعتباره خادم إدارة.
- **السلوك المخصص للأجهزة المُدارة من خلال خوادم الإدارة الأخرى**. حدد حزمة التثبيت الخاصة ببرنامج Kaspersky Endpoint Security. إذا كانت الشبكة تحتوي على أكثر من خادم إدارة مثبت فقد تري خوادم الإدارة نفس أجهزة الكمبيوتر العميلة. قد يتسبب ذلك على سبيل المثال، في تثبيت تطبيق عن بُعد على جهاز العميل نفسه عدة مرات من خلال خوادم إدارة مختلفة، أو حدوث تعارضات أخرى.
- **لا تقم بإعادة تثبيت التطبيق إذا كان مثبتًا بالفعل**. قم بمسح مربع الاختيار هذا إذا كنت تريد تثبيت إصدار سابق من التطبيق على سبيل المثال.

الخطوة الخامسة: تحديد إعداد إعادة تشغيل نظام التشغيل

حدد الإجراء المراد تنفيذه إذا كانت إعادة تشغيل جهاز الكمبيوتر مطلوبة. إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. إعادة التشغيل مطلوبة فقط إذا كان يجب عليك إزالة التطبيقات غير المتوافقة قبل التثبيت. قد تكون إعادة التشغيل مطلوبة أيضًا عند تحديث إصدار التطبيق.

الخطوة السادسة: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر لتثبيت برنامج Kaspersky Endpoint Security. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. لم يتم تثبيت عميل الشبكة على الأجهزة غير المخصصة. في هذه الحالة يتم تعيين المهمة لأجهزة محددة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة السابعة: اختيار الحساب لتشغيل المهمة

حدد في هذه الخطوة الحساب المستخدم لتثبيت عميل الشبكة باستخدام أدوات نظام التشغيل. في هذه الحالة، تكون حقوق المسؤول مطلوبة للوصول إلى جهاز الكمبيوتر. يمكنك إضافة حسابات عديدة. إذا لم يكن للحساب حقوق كافية يستخدم معالج التثبيت الحساب التالي. إذا قمت بتثبيت برنامج Kaspersky Endpoint Security باستخدام أدوات عميل الشبكة فلا يلزم تحديد حساب.

الخطوة الثامنة: تكوين جدول بدء المهمة

قم بتكوين جدول لبدء المهمة، على سبيل المثال يدويًا أو عندما يكون الكمبيوتر خاملاً.

الخطوة التاسعة: تحديد اسم المهمة

أدخل اسمًا للمهمة، على سبيل المثال تثبيت Kaspersky Endpoint Security for Windows 12.1.

الخطوة 10. الانتهاء من إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة. سيتم تثبيت التطبيق في الوضع الصامت. بعد التثبيت، ستتم إضافة الرمز إلى منطقة إخطارات جهاز كمبيوتر المستخدم. إذا كان الرمز يشبه هذا ، تأكد أنك قد قمت بتفعيل التطبيق.

كيفية إنشاء حزمة تثبيت عن بُعد في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة 1. تكوين إعدادات المهمة العامة

تكوين إعدادات المهمة:

1. في القائمة المنسدلة **Application** حدد **Kaspersky Security Center**.
2. في القائمة المنسدلة **Task type** حدد **Install application remotely**.
3. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، تثبيت Kaspersky Endpoint Security for Managers.
4. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

الخطوة 2. اختيار أجهزة الكمبيوتر للتثبيت

في هذه الخطوة، حدد أجهزة الكمبيوتر المراد تثبيت برنامج Kaspersky Endpoint Security عليها وفقًا لخيار نطاق المهمة المُحدد.

الخطوة 3. تكوين حزمة التثبيت

كوّن في هذه الخطوة حزمة التثبيت:

1. حدد حزمة تثبيت (Kaspersky Endpoint Security for Windows (12.1.

2. حدد حزمة تثبيت عميل الشبكة.

سيتم تثبيت الإصدار المُحدد من عميل الشبكة مع برنامج Kaspersky Endpoint Security. يسهل عميل الشبكة التفاعل بين خادم الإدارة وجهاز العميل. إذا كان عميل الشبكة مثبتًا بالفعل على جهاز الكمبيوتر، فلن يتم تثبيته مرة أخرى.

3. في القسم **Force installation package download**، حدد طريقة تثبيت التطبيق:

- **استخدام عميل الشبكة**. إذا لم يتم تثبيت عميل الشبكة على الكمبيوتر فسيتم تثبيت عميل الشبكة الأول باستخدام أدوات نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.
- **استخدام موارد نظام التشغيل عبر نقاط التوزيع**. يتم تسليم حزمة التثبيت إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل عبر نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت هناك نقطة توزيع واحدة على الأقل في الشبكة. وللمزيد من التفاصيل حول نقاط التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.
- **استخدام موارد نظام التشغيل من خلال خادم الإدارة**. سيتم تسليم الملفات إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل من خلال خادم الإدارة. يمكنك تحديد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على جهاز الكمبيوتر العميل، ولكن جهاز الكمبيوتر العميل يتواجد على نفس الشبكة باعتباره خادم إدارة.

4. في الحقل **Maximum number of concurrent downloads** قم بتعيين حد لعدد طلبات تنزيل حزم التثبيت التي تم إرسالها إلى خادم الإدارة. سيساعد وجود حد لعدد الطلبات في منع التحميل الزائد على الشبكة.

5. في الحقل **Maximum number of installation attempts** قم بتعيين حد لعدد محاولات تثبيت التطبيق. إذا انتهي تثبيت Kaspersky Endpoint Security مع حدوث خطأ فستبدأ المهمة في التثبيت مرة أخري تلقائيًا.

6. إذا لزم الأمر، امسح خانة الاختيار **Do not re-install application if it is already installed**. فهذا الأمر على سبيل المثال، يتيح تثبيت أحد الإصدارات السابقة للتطبيق.

7. إذا لزم الأمر، امسح خانة الاختيار **Verify operating system type before downloading**. يتيح لك ذلك تجنب تحميل حزمة توزيع التطبيق إذا لم يستوف نظام تشغيل الكمبيوتر متطلبات البرنامج. إذا كنت متأكدًا من أن نظام التشغيل الخاص بالكمبيوتر يلبي متطلبات البرامج فيمكنك تخطي هذا التحقق.

8. وإذا لزم الأمر، حدد خانة الاختيار **Assign package installation in Active Directory group policies**. يتم تثبيت برنامج Kaspersky Endpoint Security عن طريق عميل الشبكة أو يدويًا عن طريق Active Directory. لتثبيت عميل الشبكة يجب تشغيل مهمة التثبيت عن بعد مع امتيازات مسؤول المجال.

9. وإذا لزم الأمر، حدد خانة الاختيار **Prompt users to close running applications**. تثبيت Kaspersky Endpoint Security يستهلك موارد الكمبيوتر. تيسيرًا على المستخدم، يطالب معالج تثبيت التطبيق بإغلاق التطبيقات قيد التشغيل قبل بدء التثبيت. هذا يساعد على منع الاضطرابات في تشغيل التطبيقات الأخرى ويمنع الأعطال المحتملة للكمبيوتر.

10. في القسم **Behavior for devices managed through other Administration Servers**، حدد طريقة تثبيت Kaspersky Endpoint Security. إذا كانت الشبكة تحتوي على أكثر من خادم إدارة مثبت فقد تري خوادم الإدارة نفس أجهزة الكمبيوتر العميلة. قد يتسبب ذلك على سبيل المثال، في تثبيت تطبيق عن بُعد على جهاز العميل نفسه عدة مرات من خلال خوادم إدارة مختلفة، أو حدوث تعارضات أخرى.

الخطوة الرابعة: اختيار الحساب لتشغيل المهمة

حدد في هذه الخطوة الحساب المستخدم لتثبيت عميل الشبكة باستخدام أدوات نظام التشغيل. في هذه الحالة، تكون حقوق المسؤول مطلوبة للوصول إلى جهاز الكمبيوتر. يمكنك إضافة حسابات عديدة. إذا لم يكن للحساب حقوق كافية يستخدم معالج التثبيت الحساب التالي. إذا قمت بتثبيت برنامج Kaspersky Endpoint Security باستخدام أدوات عميل الشبكة فلا يلزم تحديد حساب.

الخطوة 5 إكمال إنشاء المهمة

قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**. سيتم عرض مهمة جديدة في قائمة المهام. لتشغيل المهمة، حدد خانة الاختيار المقابلة لها وانقر فوق الزر **Start**. سيتم تثبيت التطبيق في الوضع الصامت. بعد التثبيت، ستتم إضافة الرمز إلى منطقة إخطارات جهاز كمبيوتر المستخدم. إذا كان الرمز يشبه هذا ، تأكد أنك قد قمت بتفعيل التطبيق.

تثبيت التطبيق محليًا باستخدام المعالج

تتكون واجهة معالج إعداد التطبيق من سلسلة من النوافذ تتوافق مع خطوات تثبيت التطبيق.

لتثبيت التطبيق أو ترقية التطبيق من إصدار سابق عن طريق استخدام معالج الإعداد:

1. انسخ مجلد حزمة التوزيع إلى كمبيوتر المستخدم.

2. قم بتشغيل setup_kes.exe.

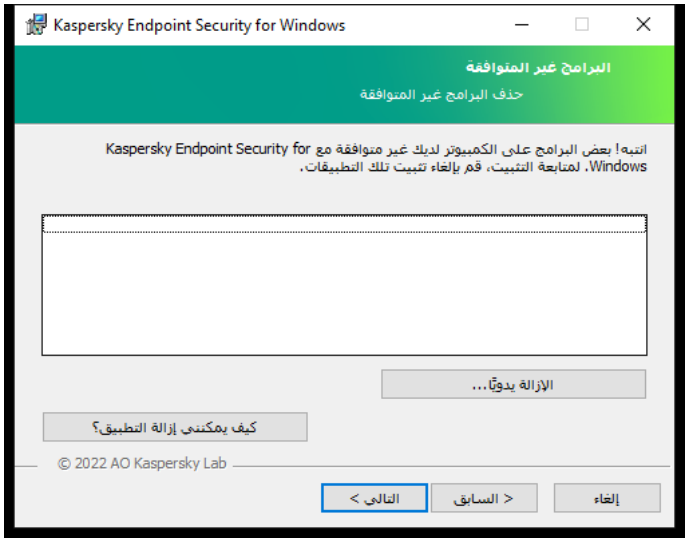
يبدأ معالج الإعداد.

التحضير للتثبيت

قبل تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر أو ترقيته من إصدار سابق، يتم التحقق من الشروط التالية:

- وجود البرامج غير المتوافقة المثبتة (تتوفر قائمة البرامج غير المتوافقة في ملف incompatible.txt المضمن في حزمة التوزيع).
- سواء تم الوفاء بمتطلبات الأجهزة والبرامج أم لا.
- سواء كان المستخدم يتمتع بحقوق تثبيت البرنامج أم لا.

في حالة عدم استيفاء أي من المتطلبات السابقة، يتم عرض إخطار على الشاشة يفيد بذلك. على سبيل المثال، إشعار حول البرامج غير المتوافقة (انظر الشكل أدناه).



حذف البرامج غير المتوافقة

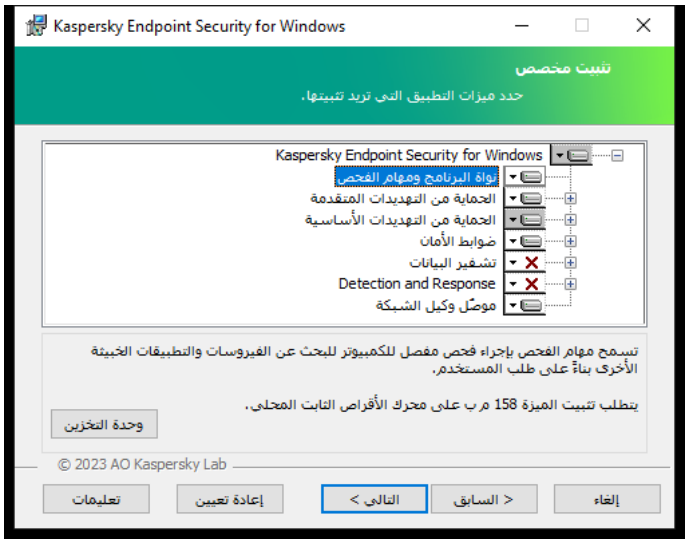
في حالة وفاء الكمبيوتر بالمتطلبات الواردة، يقوم معالج الإعداد بالبحث عن تطبيقات Kaspersky التي قد تؤدي إلى تعارضات عند تشغيلها في نفس وقت تثبيت التطبيق. وفي حالة وجود تلك التطبيقات، سوف يطلب منك إزالتها يدويًا.

إذا تضمنت التطبيقات المكتشفة إصدارات سابقة من Kaspersky Endpoint Security، فإنه يتم الاحتفاظ بجميع البيانات التي يمكن ترحيلها (مثل بيانات التفعيل وإعدادات التطبيق) واستخدامها أثناء تثبيت برنامج Kaspersky Endpoint Security 12.1 for Windows، وتتم إزالة الإصدار السابق من التطبيق تلقائيًا. وهذا ينطبق على إصدارات التطبيق التالية:

- Kaspersky Endpoint Security 11.6.0 for Windows (الإصدار 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (الإصدار 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 for Windows (الإصدار 11.8.0.384).
- Kaspersky Endpoint Security 11.9.0 for Windows (الإصدار 11.9.0.351).
- Kaspersky Endpoint Security 11.10.0 for Windows (الإصدار 11.10.0.399).
- Kaspersky Endpoint Security 11.11.0 for Windows (الإصدار 11.11.0.452).
- Kaspersky Endpoint Security 12.0 for Windows (الإصدار 12.0.0.465).

مكونات برنامج Kaspersky Endpoint Security

أثناء عملية التثبيت، يمكنك تحديد مكونات برنامج Kaspersky Endpoint Security التي ترغب في تثبيتها (انظر الشكل أدناه). مكون الحماية من تهديدات الملفات مكون إلزامي يجب تثبيته. ولا يمكنك إلغاء تثبيته.



تحديد مكونات التطبيق المطلوب تثبيتها

وبشكل افتراضي، يتم تحديد كل مكونات التطبيق للتثبيت باستثناء المكونات التالية:

- منع هجمات BadUSB.
- مكونات تشفير البيانات.
- مكونات Detection and Response.

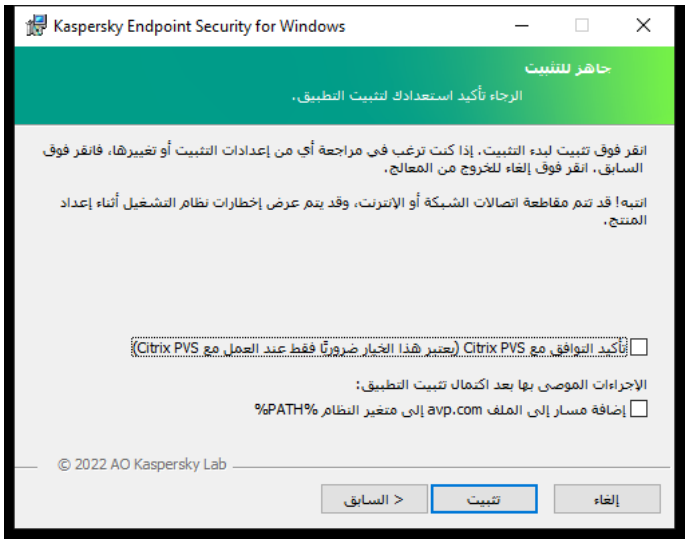
يمكنك تغيير مكونات التطبيقات المتاحة بعد تثبيت التطبيق. لفعل ذلك، سوف تحتاج إلى تشغيل معالج الإعداد مرة أخرى واختيار تغيير المكونات المتاحة.

إذا كنت بحاجة إلى تثبيت مكونات Detection and Response، يدعم Kaspersky Endpoint Security التكوينات التالية:

- Endpoint Detection and Response Optimum فقط
- Endpoint Detection and Response Expert فقط
- Endpoint Detection and Response (KATA) فقط
- Kaspersky Sandbox فقط
- Endpoint Detection and Response Optimum وKaspersky Sandbox
- Endpoint Detection and Response Expert وKaspersky Sandbox
- Endpoint Detection and Response (KATA) وKaspersky Sandbox

يتحقق Kaspersky Endpoint Security من تحديد المكونات قبل تثبيت التطبيق. وفي حالة عدم دعم التكوين المحدد لمكونات Detection and Response، يمكن تثبيت Kaspersky Endpoint Security.

إعدادات متقدمة



إعدادات تثبيت التطبيق المتقدمة

حماية عملية تثبيت التطبيق. تتضمن حماية التثبيت الحماية من استبدال حزمة التوزيع باستخدام التطبيقات الضارة ومنع الوصول إلى مجلد تثبيت برنامج Kaspersky Endpoint Security ومنع الوصول إلى قسم تسجيل النظام الذي يحتوي على مفاتيح التطبيق. وعلى الرغم من ذلك، إذا تعذر تثبيت التطبيق (على سبيل المثال، عند إجراء التثبيت عن بُعد باستخدام تعليمات Windows Remote Desktop)، ينصح حينئذ بتعطيل حماية عملية التثبيت.

تأكيد التوافق مع Citrix PVS (يعتبر هذا الخيار ضروريًا فقط عند العمل مع Citrix PVS). يمكنك تمكين دعم خدمات Citrix التزويد لتثبيت برنامج Kaspersky Endpoint Security إلى جهاز ظاهري.

إضافة مسار إلى الملف avp.com إلى متغير النظام %PATH%. يمكنك إضافة مسار التثبيت إلى المتغير %PATH% من أجل الاستخدام السهل لواجهة سطر الأوامر.

تثبيت التطبيق عن بعد باستخدام مدير تكوين مركز النظام

تنطبق هذه الإرشادات على مدير تكوين مركز النظام 2012 R2.

لتثبيت تطبيق عن بعد باستخدام مدير تكوين مركز النظام:

1. افتح وحدة تحكم مدير التكوين.
2. في الجزء الأيسر من وحدة التحكم، في القسم **App management**، حدد **Packages**.
3. في الجزء العلوي من وحدة التحكم في لوحة التحكم، انقر فوق الزر **Create package**.
   يؤدي ذلك لبدء معالج حزمة وتطبيق جديد.
4. في معالج حزمة وتطبيق جديد:
   a. في القسم **Package**:
   - في الحقل **Name** ، أدخل اسم حزمة التثبيت.
   - في الحقل **Source folder**، حدد المسار إلى المجلد الذي يحتوي على حزمة توزيع Kaspersky Endpoint Security.

   b. في القسم **Application type**، حدد الخيار **Standard program**.

c. في القسم **Standard program**:

- في الحقل **Name**، أدخل الاسم الفريد لحزمة التثبيت (على سبيل المثال، اسم التطبيق متضمن الإصدار).
- في الحقل **Command line**، حدد خيارات تثبيت Kaspersky Endpoint Security من سطر الأوامر.
- انقر فوق الزر **Browse** لتحديد المسار إلى الملف التنفيذي للتطبيق.
- تأكد من أن قائمة **Run mode** تتضمن تحديد عنصر **Run with administrative rights**.

d. في القسم **Requirements**:

- حدد خانة الاختيار **Run another program first** إذا كنت تريد بدء تطبيق مختلف قبل تثبيت Kaspersky Endpoint Security.
  حدد التطبيق من القائمة المنسدلة **Application** أو حدد المسار إلى الملف التنفيذي لهذا التطبيق عبر النقر فوق الزر **Browse**.
- حدد الخيار **This program can run only on specified platforms** في القسم **Platform requirements** إذا كنت تريد تثبيت التطبيق في أنظمة التشغيل المحددة فقط.
  في القائمة أدناه، حدد خانات الاختيار المقابلة لأنظمة التشغيل التي سيتم فيها تثبيت Kaspersky Endpoint Security.

تعتبر هذه الخطوة اختيارية.

e. في القسم **Summary**، تحقق من كل قيم الإعدادات التي تم إدخالها وانقر فوق **Next**.

سوف تظهر حزمة التثبيت التي تم إنشاؤها في القسم **Packages** في قائمة حزم التثبيت المتوفرة.

5. في قائمة السياق الخاصة بحزمة التثبيت، حدد **Deploy**.
يؤدي ذلك إلى بدء معالج النشر.

6. في معالج النشر:

a. في القسم **General**:

- في الحقل **Software**، أدخل الاسم الفريد لحزمة التثبيت أو حدد حزمة التثبيت من القائمة عبر النقر فوق الزر **Browse**.
- في الحقل **Collection**، أدخل اسم مجموعة أجهزة الكمبيوتر التي سيتم تثبيت التطبيق عليها، أو حدد المجموعة عبر النقر فوق الزر **Browse**.

b. في القسم **Contains**، قم بإضافة نقاط التوزيع (للحصول على مزيد من المعلومات التفصيلية، الرجاء الرجوع إلى مستندات التعليمات الخاصة بمدير تكوين مركز النظام).

c. إذا لزم الامر، حدد قيم الإعدادات الأخرى في معالج النشر. تعتبر هذه الإعدادات اختيارية للتثبيت البعيد لتطبيق Kaspersky Endpoint Security.

d. في القسم **Summary**، تحقق من كل قيم الإعدادات التي تم إدخالها وانقر فوق **Next**.

بعد انتهاء معالج النشر، سيتم إنشاء مهمة لتثبيت Kaspersky Endpoint Security عن بعد.

وصف إعدادات تثبيت ملف setup.ini

يتم استخدام الملف setup.ini عند تثبيت التطبيق من سطر الأوامر أو استخدام محرر سياسة المجموعة الخاصة بـ Microsoft Windows. لتطبيق الإعدادات من ملف setup.ini، ضع هذا الملف في المجلد الذي يحتوي على حزمة توزيع Kaspersky Endpoint Security.

قم بتنزيل ملف SETUP.INI

يتكون ملف setup.ini من الأقسام التالية:

- `[Setup]` - إعدادات عامة لتثبيت التطبيق.
- `[Components]` – مجموعة مكونات التطبيق التي سيتم تثبيتها. في حالة عدم تحديد أي مكونات، سيتم تثبيت جميع مكونات النظام المتوفرة لنظام التشغيل. تمثل الحماية من تهديدات الملفات مكونًا إجباريًا ويتم تثبيته على الكمبيوتر بغض النظر عن أي إعدادات موضحة في هذا القسم. ولا يتضمن هذا القسم مكون Managed Detection and Response كذلك. لتثبيت هذا المكون، يجب عليك تفعيل Managed Detection and Response في Kaspersky Security Center Console.
- `[Tasks]` - مجموعة من المهام المطلوب تضمينها في قائمة مهامKaspersky Endpoint Security. في حالة عدم تحديد أي مهام، سيتم تضمين جميع المهام الموجودة في قائمة مهام Kaspersky Endpoint Security.

تتمثل القيم البديلة للقيمة `1` هي القيم `yes` و`on` و`enable` و`enabled`.

تتمثل القيم البديلة للقيمة `0` هي القيم `no` و `off` و `disable` و `disabled`.

إعدادات ملف setup.ini

القسم	المعلمة	الوصف
`[Setup]`	`InstallDir`	المسار المؤدي لمجلد تثبيت التطبيق.
	`ActivationCode`	رمز تفعيل Kaspersky Endpoint Security.
	`EULA=1`	قبول شروط اتفاقية ترخيص المستخدم النهائي. يتم تضمين نص اتفاقية الترخيص في حKaspersky Endpoint Security. يعد قبول شروط اتفاقية ترخيص المستخدم النهائي أمرًا ضروريًا لتثبيت التطبيق أو إصداره.
	`PrivacyPolicy=1`	قبول سياسة الخصوصية. ويتم تضمين نص سياسة الخصوصية في حزمة توزيع rskyEndpoint Security. لتثبيت التطبيق أو ترقية إصدار التطبيق، يجب عليك قبول سياسة الخصوصية.
	`KSN`	قبول أو رفض المشاركة في Kaspersky Security Network (KSN). إذا لم يتلهذه المعلمة، فسوف يطالب Kaspersky Endpoint Security بتأكيد موافقتك أو المشاركة في KSN عند بدء تشغيل Kaspersky Endpoint Security لأول مرة المتاحة: • `1` – قبول المشاركة في KSN. • `0` – رفض المشاركة في KSN (القيمة الافتراضية). يتم تحسين حزمة توزيع Kaspersky Endpoint Security للاستخدام معersky Security Network. وإذا اخترت عدم المشاركة في sky Security Networkفينبغي عليك تحديث Kaspersky Endpoint Security على الفور بعد اكتمال الت
	`تسجيل الدخول`	قم بتعيين اسم المستخدم للوصول إلى ميزات وإعدادات rsky Endpoint Security(مكون حماية كلمة المرور). يتم تعيين اسم المستخدم بالإضافة إلى المعلمتين `ssword` `PasswordArea`. تم استخدام اسم المستخدم KLAdmin بشكل افتراضي.
	`كلمة المرور`	حدد كلمة مرور للوصول إلى ميزات وإعدادات aspersky Endpoint Security

		تحديد كلمة المرور بالإضافة إلى المعلمتين `Login` و`PasswordArea`). إذا قمت بتحديد كلمة مرور ولم تحدد اسم مستخدم بمعلمة تسجيل دخول، فسيتم اس KLAdmin كاسم مستخدم افتراضيًا.
	`PasswordArea`	حدد نطاق كلمة المرور للوصول إلى Kaspersky Endpoint Security. عندما ي مستخدم تنفيذ إجراء تم تضمينه في هذا النطاق، فسيطالب ky Endpoint Security ببيانات اعتماد حساب المستخدم (معلمتا تسجيل الدخول وكلمة المرو الحرف " `;` " لتحديد قيم متعددة. القيم المتاحة: • `SET` - تعديل إعدادات التطبيق. • `EXIT` - الخروج من التطبيق. • `DISPROTECT` - تعطيل مكونات الحماية وإيقاف مهام الفحص. • `DISPOLICY` - تعطيل سياسة Kaspersky Security Center. • `UNINST` - إزالة التطبيق من الكمبيوتر. • `DISCTRL` - تعطيل مكونات المراقبة. • `REMOVELIC` - إزالة المفتاح. • `REPORTS` - عرض تقارير. على سبيل المثال، `rdArea=SET;PasswordArea=UNINST;PasswordArea=EXIT`
	`SelfProtection`	تمكين آلية حماية تثبيت التطبيق أو تعطيلها. القيم المتاحة: • `1` – تم تمكين آلية حماية تثبيت التطبيق (القيمة الافتراضية). • `0` – تم تعطيل آلية حماية تثبيت التطبيق. تتضمن حماية التثبيت الحماية من استبدال حزمة التوزيع باستخدام التطبيقات الضارة و الوصول إلى مجلد تثبيت برنامج Kaspersky Endpoint Security ومنع الوصو تسجيل النظام الذي يحتوي على مفاتيح التطبيق. وعلى الرغم من ذلك، إذا تعذر تثبيت ال سبيل المثال، عند إجراء التثبيت عن بُعد باستخدام تعليمات ws Remote Desktop ينصح حينئذ بتعطيل حماية عملية التثبيت.
	`EnableAzureSupport`	تمكين أو تعطيل وضع التوافق مع Azure WVD. القيم المتاحة: • `1` - تم تمكين وضع التوافق مع Azure WVD. • `0` - تم تعطيل وضع التوافق مع Azure WVD (القيمة الافتراضية). تتيح هذه الميزة عرض حالة جهاز Azure الظاهري بشكل صحيح في وحدة التحكم لتط Kaspersky Anti Targeted Attack Platform. ولمراقبة أداء الكمبيوتر، ير Kaspersky Endpoint Security بيانات القياس عن بُعد إلى خوادم KATA. ويتـ القياس عن بعد معرف الكمبيوتر (معرف المستشعر). ويسمح وضع التوافق مع WVD بتعيين معرف مستشعر فريد دائم لهذه الأجهزة الظاهرية. وفي حالة إيقاف تشغيل وضع يمكن أن يتغير معرف المستشعر بعد إعادة تشغيل الكمبيوتر بسبب كيفية عمل أجهزة e الظاهرية. ومن الممكن أن يتسبب هذا في ظهور نسخ مكررة من الأجهزة الظاهرية على التحكم.
	`Reboot=1`	إعادة التشغيل التلقائي للكمبيوتر، إذا لزم الامر بعد تثبيت التطبيق أو ترقيته. إذا كان لا ي محددة لهذا المعامل، فإن إعادة التشغيل التلقائي للكمبيوتر غير مدعومة.

		إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. التشغيل مطلوبة فقط إذا كان يجب عليك إزالة التطبيقات غير المتوافقة قبل التثبيت. قد تك التشغيل مطلوبة أيضًا عند تحديث إصدار التطبيق.
	`AddEnvironment`	في متغير النظام %PATH%، أضف المسار إلى الملفات القابلة للتنفيذ الموجودة في مج Kaspersky Endpoint Security. القيم المتاحة: • `1` – يتم تزويد متغير النظام %PATH% بمسار الملفات القابلة للتنفيذ الموجودة في إعداد Kaspersky Endpoint Security. • `0` – لن يتم تزويد متغير النظام %PATH% بمسار الملفات القابلة للتنفيذ الموجود إعداد Kaspersky Endpoint Security.
	`AMPPL`	يؤدي إلى تمكين أو تعطيل إجراءات الحماية الخاصة Kaspersky Endpoint Security باستخدام تقنية AM-PPL (Antimalware Protected Process Light). للح المزيد من التفاصيل حول تقنية AM-PPL، يُرجى زيارة موقع ويب Microsoft. إن تقنية AM-PPL متاحة للإصدار 1703 من نظام التشغيل Windows 10 (RS2) أحدث، ونظام التشغيل Windows Server 2019. القيم المتاحة: • `1` – تم تمكين إجراءات الحماية الخاصة بـ Kaspersky Endpoint Security تقنية AM-PPL. • `0` – تم تعطيل إجراءات الحماية الخاصة بـ Kaspersky Endpoint Security باستخدام تقنية AM-PPL.
	`UPGRADEMODE`	وضع ترقية التطبيق: • سلس يعني ترقية التطبيق مع إعادة تشغيل الكمبيوتر (القيمة الافتراضية). • إجباري يعني ترقية التطبيق دون إعادة التشغيل. يمكنك ترقية التطبيق دون إعادة التشغيل بدءًا من الإصدار 11.10.0. ولترقية إصدار سابق التطبيق، يجب إعادة تشغيل الكمبيوتر. يمكنك أيضًا تثبيت التصحيحات دون إعادة التشغ الإصدار 11.11.0. إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. سيتم تحديد وضع الترقية للتطبيق في إعدادات التطبيق. ويمكنك تغيير هذه المعلمة في إع التطبيق أو في السياسة. عند ترقية التطبيق المُثبت بالفعل، تكون أولوية المعلمة المحددة في ملف setup.ini أع الخاصة بالمعلمة المحددة في application settings أو في سطر الأوامر. على سبي في حالة تحديد وضع الترقية `Force` في ملف setup.ini وتحديد وضع `Seamless` إعدادات التطبيق، سيتم تثبيت الترقية دون إعادة تشغيل(`Force`). وإذا كنت تستخدم م setup.ini، حيث لم يتم تحديد المعلمة `UPGRADEMODE`، سيستخدم المُثبت قيمة افتر (`Seamless`) وسوف يُثبت الترقية مع إعادة تشغيل الكمبيوتر.
	`SetupReg`	تمكن من كتابة مفاتيح السجل من ملف setup.reg إلى السجل. `SetupReg:` `setup.reg` قيمة معلمة.
	`EnableTraces`	تمكين أو تعطيل تتبع التطبيق. بعد بدء تشغيل Kaspersky Endpoint Security، ملفات التتبع في المجلد `%ProgramData%\Kaspersky Lab\KES.21.13\Traces`. القيم المتاحة: • `1` – تم تمكين التتبع. • `0` – تم تعطيل التتبع (القيمة الافتراضية).
	`TracesLevel`	مستوى تفاصيل عمليات التتبع. القيم المتاحة:

		• `100` (حرجة). فقط رسائل حول الأخطاء الفادحة. • `200` (عالي). رسائل حول جميع الأخطاء، بما في ذلك الأخطاء الفادحة. • `300` (تشخيصية). رسائل حول جميع الأخطاء، وكذلك التحذيرات. • `400` (هامة). رسائل حول جميع الأخطاء، والتحذيرات، وكذلك المعلومات الإضا • `500` (عادية). رسائل حول جميع الأخطاء، والتحذيرات، وكذلك المعلومات المفص تشغيل التطبيق في الوضع العادي (الافتراضي). • `600` (قليلة). جميع الرسائل.
	`RESTAPI`	إدارة التطبيق من خلال REST API. لإدارة التطبيق من خلال REST API، يجب عل اسم المستخدم (`RESTAPI_User`). القيم المتاحة: • `1` – الإدارة عبر REST API مسموح بها. • `0` - تم حظر الإدارة عبر REST API (القيمة الافتراضية). لإدارة التطبيق من خلال REST API، يجب السماح بالإدارة باستخدام الأنظمة الإداري بذلك، قم بتعيين المعلمة `AdminKitConnector=1`. إذا كنت تدير التطبيق من خ REST API، فمن المستحيل إدارة التطبيق باستخدام أنظمة الإدارة الخاصة بـ ersky
	`RESTAPI_User`	اسم المستخدم الخاص بحساب المجال المستخدم لإدارة التطبيق من خلال REST API. التطبيق من خلال REST API متاحة فقط لهذا المستخدم. أدخل اسم المستخدم `\<IN>` `<UserName>` (على سبيل المثال، `RESTAPI_User=COMPANY\Administrator`). يمكنك تحديد مستخدم و للعمل باستخدام REST API. إن إضافة اسم مستخدم شرط للتمكن من إدارة التطبيق من خلال REST API.
	`RESTAPI_Port`	المنفذ المستخدم لإدارة التطبيق من خلال REST API. يُستخدم المنفذ 6782 بشكل افتر أن المنفذ خالٍ.
	`RESTAPI_Certificate`	شهادة لتحديد الطلبات (على سبيل المثال، `RESTAPI_Certificate=C:\cert.pem`). يتطلب التفاعل الآمن لبرنامج Kaspersky Endpoint Security مع عميل REST تكوين تعريف الطلب. ولفعل يجب عليك تثبيت شهادة ثم بعد ذلك التوقيع على حمولة كل طلب.
`[Components]`	`ALL`	تثبيت جميع المكونات. إذا تم تحديد قيمة المعلمة `1`، فسيتم تثبيت كل المكونات بغض الن إعدادات تثبيت المكونات الفردية. نظرًا للطريقة التي تُدعم بها حلول Detection and Response، يتم تثبيت Endpoint Detection and Response Optimum بالإضافة إلى مكونا Kaspersky Sandbox على الكمبيوتر. لا يتوافق مكون Endpoint Detection and Response Expert مع هذا التكوين.
	`MailThreatProtection`	الحماية من تهديدات البريد.
	`WebThreatProtection`	الحماية من تهديدات الويب.
	`AMSI`	حماية AMSI.
	`HostIntrusionPrevention`	منع اختراق المضيف.
	`BehaviorDetection`	اكتشاف السلوك.

	ExploitPrevention	منع الاستغلال.
	RemediationEngine	محرك المعالجة.
	Firewall	جدار الحماية.
	NetworkThreatProtection	الحماية من تهديدات الشبكة.
	WebControl	التحكم في الويب.
	DeviceControl	التحكم في الجهاز.
	ApplicationControl	التحكم في التطبيقات.
	AdaptiveAnomaliesControl	مراقبة عيوب التكيف.
	LogInspector	فحص السجل
	FileIntegrityMonitor	مراقبة سلامة الملف
	FileEncryption	أقسام التشفير على مستوى الملف.
	DiskEncryption	مكتبات تشفير القرص بالكامل.
	BadUSBAttackPrevention	منع هجمات BadUSB.
	EDR	Endpoint Detection and Response Optimum (EDR Optimum). المكون غير متوافق مع مكوني EDRCloud (EDR Expert) وEDR KATA (EDRKATA).
	EDRCloud	Endpoint Detection and Response Expert (EDR Expert). المكون غير متوافق مع مكوني EDR (EDR Optimum) وEDR KATA (EDRKATA).
	AntiAPTFeature	Endpoint Detection and Response (KATA). المكون غير متوافق مع مكوني EDRCloud (EDR Expert) وR Optimum (EDR).
	SB	Kaspersky Sandbox.
	AdminKitConnector	إدارة التطبيقات باستخدام نظم الإدارة. تشمل أنظمة الإدارة، على سبيل المثال، ersky Security Center. بالإضافة إلى أنظمة إدارة Kaspersky، يمكنك استخدام حلول جهات خارجية. يوفر Kaspersky Endpoint Security واجهة برمجة تطبيقات الغرض. القيم المتاحة: • 1 – مسموح بإدارة التطبيقات بمساعدة أنظمة الإدارة (القيمة الافتراضية). • 0 – مسموح بإدارة التطبيقات من خلال الواجهة المحلية فقط.
[Tasks]	ScanMyComputer	مهمة الفحص الكامل. القيم المتاحة: • 1 – يتم تضمين المهمة في قائمة مهام Kaspersky Endpoint Security.

		• 0 – لا يتم تضمين المهمة في قائمة مهام Kaspersky Endpoint Security
	ScanCritical	مهمة فحص المناطق الحرجة. القيم المتاحة: • 1 – يتم تضمين المهمة في قائمة مهام Kaspersky Endpoint Security. • 0 – لا يتم تضمين المهمة في قائمة مهام Kaspersky Endpoint Security
	Updater	مهمة التحديث. القيم المتاحة: • 1 – يتم تضمين المهمة في قائمة مهام Kaspersky Endpoint Security. • 0 – لا يتم تضمين المهمة في قائمة مهام Kaspersky Endpoint Security

تغيير مكونات التطبيق

أثناء تثبيت التطبيق، يمكنك اختيار المكونات التي ستكون متاحة. يمكنك تغيير مكونات التطبيقات المتاحة بالطرق التالية:

- محليًا، عن طريق استخدام معالج الإعداد.

  يتم تغيير مكونات التطبيقات باستخدام الطريقة العادية لنظام التشغيل Windows، والذي تتم من خلال لوحة التحكم. قم بتشغيل معالج إعداد التطبيق وحدد خيار تغيير مكونات التطبيق المتاح. اتبع التعليمات الموجودة على الشاشة.

- عن بُعد باستخدام Kaspersky Security Center.

  تتيح لك المهمة تغيير مكونات التطبيق القيام بتغيير مكونات برنامج Kaspersky Endpoint Security بعد تثبيت التطبيق.

يرجى مراعاة الاعتبارات الخاصة التالية عند تغيير مكونات التطبيق:

- على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows Server لا يمكنك تثبيت جميع مكونات Kaspersky Endpoint Security (مثلًا مكون مراقبة عيوب التكيف غير متاح).

- إذا كانت محركات الأقراص الصلبة في الكمبيوتر لديك محميةً من خلال تشفير القرص بالكامل (FDE)، فيمكنك إزالة مكون تشفير القرص بالكامل. لإزالة مكون تشفير القرص بالكامل، قم بفك تشفير كل محركات الأقراص الصلبة بالكمبيوتر.

- إذا كان بالكمبيوتر ملفات مشفرة (FLE) أو كان المستخدم يستعين بمحركات أقراص مشفرة قابلة للإزالة (FDE أو FLE)، فسيصير الوصول إلى الملفات ومحركات الأقراص القابلة للإزالة مستحيلًا بعد إزالة مكونات تشفير البيانات. يمكنك الوصول إلى الملفات ومحركات الأقراص القابلة للإزالة عن طريق إعادة تثبيت مكونات تشفير البيانات.

كيفية إضافة مكونات تطبيق أو حذفها في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (12.1)** ← **حدد المكونات المراد تثبيتها**.

الخطوة الثانية: إعدادات المهمة لتغيير مكونات التطبيق

حدد مكونات التطبيق التي ستكون متاحة على كمبيوتر المستخدم.

قم بتكوين الإعدادات المتقدمة للمهمة (انظر الجدول أدناه).

الخطوة الثالثة: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الرابعة: تكوين جدول بدء المهمة

قم بتكوين جدول لبدء المهمة، على سبيل المثال يدويًا أو عندما يكون الكمبيوتر خاملاً.

الخطوة الخامسة: تحديد اسم المهمة

أدخل اسم المهمة، مثل إضافة مكون التحكم في التطبيقات.

الخطوة 6 إكمال إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

وكنتيجة لذلك، سيتم تغيير مجموعة مكونات برنامج Kaspersky Endpoint Security على أجهزة المستخدمين في الوضع الصامت. سيتم عرض مجموعة المكونات المتاحة في الواجهة المحلية الخاصة بالتطبيق. سيتم تعطيل المكونات التي لم تكن مُضمّنة في التطبيق، ولن تكون إعدادات تلك المكونات متاحة.

كيفية إضافة أو إزالة مكونات التطبيقات في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة 1. تكوين إعدادات المهمة العامة

تكوين إعدادات المهمة:

1. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.
2. في القائمة المنسدلة **Task type** حدد **Change application components**.
3. في الحقل **Task name**، أدخل وصفًا موجزًا علي سبيل المثال، إضافة مكون التحكم في التطبيقات.
4. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

الخطوة الثانية: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. على سبيل المثال: حدد مجموعة إدارة منفصلة أو أنشئ تحديدًا.

الخطوة 3 إكمال إنشاء المهمة

حدد خانة الاختيار **Open task details when creation is complete** وقم بإنهاء المعالج. في خصائص المهمة، حدد نافذة **Application Settings** واختر مكونات التطبيق التي ستكون متاحة. قم بتكوين الإعدادات المتقدمة للمهمة (انظر الجدول أدناه).

احفظ التغييرات وشغل المهمة.

وكنتيجة لذلك، سيتم تغيير مجموعة مكونات برنامج Kaspersky Endpoint Security على أجهزة المستخدمين في الوضع الصامت. سيتم عرض مجموعة المكونات المتاحة في الواجهة المحلية الخاصة بالتطبيق. سيتم تعطيل المكونات التي لم تكن مُضمّنة في التطبيق، ولن تكون إعدادات تلك المكونات متاحة.

الإعدادات المتقدمة للمهمة

المعلمة	الوصف
إزالة تطبيقات الجهات الخارجية غير المتوافقة	يمكن عرض قائمة بالتطبيقات غير المتوافقة في `incompatible.txt` التي توجد في حزمة التوزيع. في حالة تثبيت تطبيقات غير متوافقة على الكمبيوتر ينتهي تثبيت Kaspersky Endpoint Security بخطأ.
استخدام كلمة مرور لتعديل مجموعة مكونات التطبيق	يقوم المسؤولون عادة بتمكين الحماية بكلمة مرور لتقييد الوصول إلى Kaspersky Endpoint Security. أي لتعديل تحديد مكونات التطبيق، يجب عليك إدخال بيانات اعتماد مستخدم لديه إذن **إزالة / تعديل / استعادة التطبيق**. على سبيل المثال، يمكنك استخدام حساب KLAdmin.
استخدم وضع التوافق مع Azure WVD	تتيح هذه الميزة عرض حالة جهاز Azure الظاهري بشكل صحيح في وحدة التحكم لتطبيق Kaspersky Anti Targeted Attack Platform. ولمراقبة أداء الكمبيوتر، يرسل Kaspersky Endpoint Security بيانات القياس عن بُعد إلى خوادم KATA. ويتضمن القياس عن بعد معرف الكمبيوتر (معرف المستشعر). ويسمح وضع التوافق مع Azure WVD بتعيين معرف مستشعر فريد دائم لهذه الأجهزة الظاهرية. وفي حالة إيقاف تشغيل وضع التوافق، يمكن أن يتغير معرف المستشعر بعد إعادة تشغيل الكمبيوتر بسبب كيفية عمل أجهزة Azure الظاهرية. ومن الممكن أن يتسبب هذا في ظهور نسخ مكررة من الأجهزة الظاهرية على وحدة التحكم.

استخدام كلمة المرور لإلغاء تثبيت Kaspersky Endpoint Agent وKaspersky Security for Windows Server	يقوم المسؤولون عادةً بتمكين الحماية بكلمة مرور في إعدادات هذه المهام لتقييد الوصول إلى Kaspersky Endpoint Agent (KEA) وKaspersky Security for Windows Server (KSWS). أي، إذا كنت تقوم بالترحيل من تكوين [KES+KEA] إلى [KES+العامل المدمج]، أو إذا كنت تقوم بالترحيل من KSWS إلى KES، فيجب عليك إدخال كلمة مرور لإزالة هذه التطبيقات.

الترقية من إصدار سابق للتطبيق

عند قيامك بإجراء تحديث لإصدار سابق من التطبيق إلى إصدار أحدث، عليك وضع الأمور التالية في الاعتبار:

- يجب أن تتوافق ترجمة الإصدار الجديد من Kaspersky Endpoint Security مع ترجمة الإصدار المُثبت من التطبيق. وإذا لم تتطابق ترجمات التطبيقات، ستكتمل ترقية التطبيق مع وجود خطأ.
- نوصي بالخروج من جميع التطبيقات النشطة قبل بدء تشغيل التحديث.
- قبل إجراء التحديث، يقوم Kaspersky Endpoint Security بحظر وظيفة تشفير القرص بالكامل. وإذا تعذر فك تشفير القرص بالكامل، فسوف تتم مقاطعة تثبيت الترقية. بعد عملية تحديث التطبيق، سوف تتم استعادة وظيفة تشفير القرص بالكامل.

يدعم Kaspersky Endpoint Security تحديثات الإصدارات التالية من التطبيق:

- Kaspersky Endpoint Security 11.6.0 for Windows (الإصدار 11.6.0.394).
- Kaspersky Endpoint Security 11.7.0 for Windows (الإصدار 11.7.0.669).
- Kaspersky Endpoint Security 11.8.0 for Windows (الإصدار 11.8.0.384).
- Kaspersky Endpoint Security 11.9.0 for Windows (الإصدار 11.9.0.351).
- Kaspersky Endpoint Security 11.10.0 for Windows (الإصدار 11.10.0.399).
- Kaspersky Endpoint Security 11.11.0 for Windows (الإصدار 11.11.0.452).
- Kaspersky Endpoint Security 12.0 for Windows (الإصدار 12.0.0.465).

طرق ترقية التطبيق

يمكن تحديث Kaspersky Endpoint Security على جهاز الكمبيوتر بطرق التالية:

- محليًا، عن طريق استخدام معالج الإعداد.
- محليًا من سطر الأوامر.
- عن بُعد باستخدام Kaspersky Security Center.
- عن بُعد من خلال استخدام محرر إدارة نهج مجموعة Microsoft Windows (للحصول على المزيد من التفاصيل، يرجى زيارة موقع ويب الدعم الفني لشركة Microsoft).
- عن بُعد، من خلال استخدام System Center Configuration Manager.

إذا كان التطبيق المطبق في شبكة الشركة يتميز بمجموعة من المكونات مختلفة عن المجموعة الافتراضية، فإن تحديث التطبيق من خلال وحدة تحكم الإدارة (MMC) أمر مختلف عن تحديث التطبيق من خلال Web Console وCloud Console. فكر فيما يلي عند تحديث Kaspersky Endpoint Security:

- Kaspersky Security Center Web Console أو Kaspersky Security Center Cloud Console.

إذا أنشأت حزمة تثبيت للإصدار الجديد من التطبيق باستخدام مجموعة المكونات الافتراضية، فإن مجموعة المكونات على جهاز كمبيوتر المستخدم لن تتغير. لاستخدام Kaspersky Endpoint Security مع مجموعة المكونات الافتراضية، سوف تحتاج إلى فتح خصائص حزمة التثبيت وتغيير مجموعة المكونات، وبعدها العودة إلى مجموعة المكونات الأصلية وحفظ التغييرات.

- Kaspersky Security Center Administration Console.

مجموعة مكونات التطبيق بعد التحديث سوف تطابق مجموعة المكونات في حزمة التثبيت. وإذا كان الإصدار الجديد من التطبيق به المجموعة الافتراضية من المكونات، فعندها -على سبيل المثال- سوف يتم إزالة "منع هجمات BadUSB" من على جهاز الكمبيوتر لأن هذا المكون مستثنى من المجموعة الافتراضية. للاستمرار في استخدام التطبيق بنفس مجموعة المكونات كما كان قبل التحديث، اختر المكونات التي تحتاج إليها في إعدادات حزمة التثبيت.

ترقية التطبيق دون إعادة التشغيل

توفر ترقية التطبيق دون إعادة التشغيل عملية خادم دون مقاطعة عند تحديث إصدار التطبيق.

تتضمن ترقية التطبيق دون إعادة تشغيل القيود التالية:

- يمكنك ترقية التطبيق دون إعادة التشغيل بدءًا من الإصدار 11.10.0. ولترقية إصدار سابق من التطبيق، يجب إعادة تشغيل الكمبيوتر.
- يمكنك تثبيت التصحيحات دون إعادة التشغيل بدءًا من الإصدار 11.11.0. لتثبيت تصحيحات للإصدارات السابقة من التطبيق، قد يلزم إعادة تشغيل الكمبيوتر.
- لا تتوفر ترقية التطبيق بدون إعادة التشغيل على أجهزة الكمبيوتر المزودة بتشفير بيانات تمكينه (تشفير Kaspersky (FDE) وBitLocker والتشفير على مستوى الملف (FLE)). ولترقية التطبيق على أجهزة الكمبيوتر التي تم تمكين تشفير البيانات عليها، يجب إعادة تشغيل الكمبيوتر.
- بعد تغيير مكونات التطبيق أو إصلاح التطبيق، يجب إعادة تشغيل الكمبيوتر.

كيفية تحديد وضع ترقية التطبيق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.
5. في القسم **إعدادات متقدمة**، حدد أو امسح خانة الاختيار **تثبيت تحديثات التطبيق دون إعادة التشغيل** لتكوين وضع ترقية التطبيق.
6. احفظ تغييراتك.

كيفية تحديد وضع ترقية التطبيق في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Application Settings**.

5. في القسم **Advanced settings**، حدد أو امسح خانة الاختيار **Install application updates without restart** لتكوين وضع ترقية التطبيق.

6. احفظ تغييراتك.

كيفية تحديد وضع ترقية التطبيق في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.

إعدادات Kaspersky Endpoint Security for Windows

3. في القسم **وضع التشغيل**، حدد أو امسح خانة الاختيار **تثبيت التحديثات دون إعادة تشغيل الكمبيوتر** لتكوين وضع ترقية التطبيق.

4. احفظ تغييراتك.

نتيجة لذلك، بعد ترقية التطبيق دون إعادة التشغيل، سيتم تثبيت نسختين من التطبيق على الكمبيوتر. ويقوم المُثبت بتثبيت الإصدار الجديد من التطبيق لفصل المجلدات الفرعية في مجلدات Program Files وProgram Data. ويقوم المُثبت أيضًا بإنشاء مفتاح تسجيل منفصل للإصدار الجديد من التطبيق. ولا يتعين عليك إزالة الإصدار السابق من التطبيق يدويًا. وستتم إزالة الإصدار السابق تلقائيًا عند إعادة تشغيل الكمبيوتر.

يمكنك التحقق من ترقية Kaspersky Endpoint Security باستخدام تقرير إصدار تطبيق Kaspersky في وحدة تحكم Kaspersky Security Center.

إزالة التطبيق

تؤدي إزالة برنامج Kaspersky Endpoint Security إلى ترك الكمبيوتر وبيانات المستخدم عرضةً للتهديدات.

إزالة التطبيق عن بعد باستخدام Kaspersky Security Center

يُمكنك إلغاء تثبيت التطبيق عن بُعد عن طريق استخدام مهمة إلغاء تثبيت التطبيق عن بُعد. عند تنفيذ المهمة، سيقوم برنامج Kaspersky Endpoint Security بتنزيل أداة إلغاء تثبيت التطبيق على جهاز كمبيوتر المستخدم. بعد الانتهاء من إلغاء تثبيت التطبيق، ستتم إزالة الأداة تلقائيًا.

كيفية إزالة التطبيق من حلال وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **خادم إدارة Kaspersky Security Center** ← **إضافي** ← **إلغاء تثبيت التطبيق عن بُعد**.

الخطوة الثانية: اختيار التطبيق الذي ترغب في إزالته

حدد **إلغاء تثبيت التطبيق المدعوم من قِبل Kaspersky Security Center**.

الخطوة الثالثة: إعدادات المهمة لإلغاء تثبيت التطبيق

حدد **Kaspersky Endpoint Security for Windows (12.1)**.

الخطوة الرابعة: إلغاء تثبيت إعدادات الأداة المساعدة

قم بتكوين إعدادات التطبيق الإضافية التالية:

- **فرض التحميل الخاص بالأداة المساعدة لإلغاء التثبيت**. حدد طريقة تسليم الأداة المساعدة:
  - **استخدام عميل الشبكة**. إذا لم يتم تثبيت عميل الشبكة على الكمبيوتر فسيتم تثبيت عميل الشبكة الأول باستخدام أدوات نظام التشغيل. عند ذلك يتم إلغاء تثبيت برنامج Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.
  - **استخدام موارد نظام التشغيل من خلال خادم الإدارة**. سيتم تسليم الأداة إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل من خلال خادم الإدارة. يمكنك تحديد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على جهاز الكمبيوتر العميل، ولكن جهاز الكمبيوتر العميل يتواجد على نفس الشبكة باعتباره خادم إدارة.
  - **استخدام موارد نظام التشغيل عبر نقاط التوزيع**. يتم تسليم الأداة إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل عبر نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت هناك نقطة توزيع واحدة على الأقل في الشبكة. وللمزيد من التفاصيل حول نقاط التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.
- **تحقق من نوع نظام التشغيل قبل التنزيل**. الغ تحديد خانة الاختيار هذه إذا كان ذلك ضروريًا. يُتيح لك ذلك تجنب تنزيل أداة إلغاء التثبيت إذا لم يستوف نظام تشغيل الكمبيوتر متطلبات البرنامج. إذا كنت متأكدًا من أن نظام التشغيل الخاص بالكمبيوتر يلبي متطلبات البرامج فيمكنك تخطي هذا التحقق.

إذا كانت عملية إلغاء تثبيت التطبيق محمية بكلمة مرور، اتبع الخطوات التالية:

1. حدد خانة الاختيار **استخدام كلمة مرور إلغاء التثبيت**.

2. انقر فوق الزر **تحرير**.

3. أدخل كلمة المرور الخاصة بحساب KLAdmin .

الخطوة الخامسة: تحديد إعداد إعادة تشغيل نظام التشغيل

بعد إلغاء تثبيت التطبيق سوف يُطلب منك إعادة التشغيل. حدد الإجراء الذي سيتم لإعادة تشغيل الكمبيوتر.

الخطوة السادسة: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة السابعة: اختيار الحساب لتشغيل المهمة

حدد في هذه الخطوة الحساب المستخدم لتثبيت عميل الشبكة باستخدام أدوات نظام التشغيل. في هذه الحالة، تكون حقوق المسؤول مطلوبة للوصول إلى جهاز الكمبيوتر. يمكنك إضافة حسابات عديدة. إذا لم يكن للحساب حقوق كافية يستخدم معالج التثبيت الحساب التالي. إذا قمت بإلغاء تثبيت برنامج Kaspersky Endpoint Security باستخدام أدوات عميل الشبكة، فلا يلزم تحديد حساب.

الخطوة الثامنة: تكوين جدول بدء المهمة

قم بتكوين جدول لبدء المهمة، على سبيل المثال يدويًا أو عندما يكون الكمبيوتر خاملاً.

الخطوة التاسعة: تحديد اسم المهمة

أدخل اسمًا للمهمة، مثل إزالة Kaspersky Endpoint Security 12.1.

الخطوة 10. الانتهاء من إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

سيتم إلغاء تثبيت التطبيق في الوضع الصامت.

كيفية إزالة التطبيق من خلال Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة 1. تكوين إعدادات المهمة العامة

تكوين إعدادات المهمة:

1. في القائمة المنسدلة **Application** حدد **Kaspersky Security Center**.

2. في القائمة المنسدلة **Task type** حدد **Uninstall application remotely**.

3. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، إلغاء تثبيت برنامج Kaspersky Endpoint Security من أجهزة كمبيوتر الدعم الفني.

4. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

الخطوة الثانية: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. على سبيل المثال: حدد مجموعة إدارة منفصلة أو أنشئ تحديدًا.

الخطوة 3. تكوين إعدادات إلغاء تثبيت التطبيق

في هذه الخطوة، قم بتكوين إعدادات إلغاء تثبيت التطبيق:

1. حدد **Uninstall managed application**.

2. حدد **Kaspersky Endpoint Security for Windows (12.1)**.

3. **Force download of the uninstallation utility**. حدد طريقة تسليم الأداة المساعدة:

- **Using Network Agent**. إذا لم يتم تثبيت عميل الشبكة على الكمبيوتر فسيتم تثبيت عميل الشبكة الأول باستخدام أدوات نظام التشغيل. عند ذلك يتم إلغاء تثبيت برنامج Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.
- **Using operating system resources through Administration Server**. سيتم تسليم الأداة إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل من خلال خادم الإدارة. يمكنك تحديد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على جهاز الكمبيوتر العميل، ولكن جهاز الكمبيوتر العميل يتواجد على نفس الشبكة باعتباره خادم إدارة.
- **Using operating system resources through distribution points**. يتم تسليم الأداة إلى أجهزة الكمبيوتر العميلة باستخدام موارد نظام التشغيل عبر نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت هناك نقطة توزيع واحدة على الأقل في الشبكة. وللمزيد من التفاصيل حول نقاط التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

4. في الحقل **Maximum number of concurrent downloads**، قم بتعيين حد لعدد الطلبات التي تم إرسالها إلى خادم الإدارة لتنزيل أداة إلغاء تثبيت التطبيق. سيساعد وجود حد لعدد الطلبات في منع التحميل الزائد على الشبكة.

5. في الحقل **Maximum number of uninstallation attempts** قم بتعيين حد لعدد محاولات إلغاء تثبيت التطبيق. إذا انتهي إلغاء تثبيت برنامج Kaspersky Endpoint Security مع حدوث خطأ، فستبدأ المهمة في إلغاء التثبيت مرة أخري تلقائيًا.

6. إذا لزم الأمر، امسح خانة الاختيار **Verify operating system type before downloading**. يُتيح لك ذلك تجنب تنزيل أداة إلغاء التثبيت إذا لم يستوف نظام تشغيل الكمبيوتر متطلبات البرنامج. إذا كنت متأكدًا من أن نظام التشغيل الخاص بالكمبيوتر يلبي متطلبات البرامج فيمكنك تخطي هذا التحقق.

الخطوة الرابعة: اختيار الحساب لتشغيل المهمة

حدد في هذه الخطوة الحساب المستخدم لتثبيت عميل الشبكة باستخدام أدوات نظام التشغيل. في هذه الحالة، تكون حقوق المسؤول مطلوبة للوصول إلى جهاز الكمبيوتر. يمكنك إضافة حسابات عديدة. إذا لم يكن للحساب حقوق كافية يستخدم معالج التثبيت الحساب التالي. إذا قمت بإلغاء تثبيت برنامج Kaspersky Endpoint Security باستخدام أدوات عميل الشبكة، فلا يلزم تحديد حساب.

الخطوة 5 إكمال إنشاء المهمة

قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**. سيتم عرض مهمة جديدة في قائمة المهام.

لتشغيل المهمة، حدد خانة الاختيار المقابلة لها وانقر فوق الزر **Start**. سيتم إلغاء تثبيت التطبيق في الوضع الصامت. بعد اكتمال عملية إلغاء التثبيت، يعرض برنامج Kaspersky Endpoint Security مطالبة لإعادة تشغيل جهاز الكمبيوتر.

إذا كانت عملية إلغاء تثبيت التطبيق هي محمي بكلمة المرور، أدخل كلمة المرور الخاصة بحساب KLAdmin في خصائص المهمة إلغاء تثبيت التطبيق عن بُعد. دون إدخال كلمة المرور، لن يتم تنفيذ المهمة.

لاستخدام كلمة المرور الخاصة بحساب KLAdmin في مهمة إلغاء تثبيت التطبيق عن بُعد:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.
   تفتح قائمة المهام.
2. انقر فوق المهمة **Uninstall application remotely** Kaspersky Security Center.
   نافذة خصائص المهمة.
3. حدد علامة التبويب **Application settings**.
4. حدد خانة الاختيار **Use uninstallation password**.
5. أدخل كلمة المرور الخاصة بحساب KLAdmin .
6. احفظ تغييراتك.

أعد تشغيل الكمبيوتر لإكمال التثبيت. ولفعل ذلك، يعرض عميل الشبكة نافذة منبثقة.

إزالة التطبيق عن بُعد باستخدام Active Directory

يمكنك إلغاء تثبيت التطبيق عن بُعد باستخدام سياسة مجموعة Microsoft Windows. لإلغاء تثبيت التطبيق، تحتاج إلى فتح Group Policy Management Console (gpmc.msc) واستخدام Group Policy Editor لإنشاء مهمة إزالة التطبيق (للمزيد من التفاصيل، يرجى زيارة موقع ويب الدعم الفني لشركة Microsoft).

إذا كانت عملية إلغاء تثبيت التطبيق محمية بكلمة مرور، تحتاج إلى فعل ما يلي:

1. إنشاء ملف BAT بالمحتويات التالية:

```
msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
```

<GUID> هو المعرف الفريد للتطبيق. يمكنك معرفة GUID لأي تطبيق باستخدام الأمر التالي:

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name,
IdentifyingNumber
```

مثال:

```
msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin
KLPASSWD=!Password1 /qn
```

2. إنشاء سياسة Microsoft Windows جديدة لأجهزة الكمبيوتر في gpmc.msc) Group Policy Management Console).

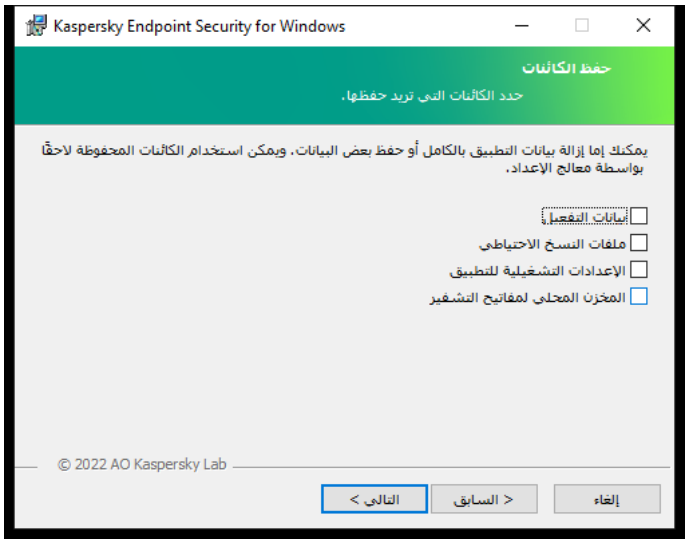
3. استخدام السياسة الجديدة لتشغيل ملف BAT الذي تم إنشاؤه على أجهزة الكمبيوتر.

إزالة التطبيق محليًا

يمكنك إزالة التطبيق محليًا باستخدام معالج الإعداد. تتم إزالة برنامج Kaspersky Endpoint Security باستخدام الطريقة العادية لنظام التشغيل Windows، والذي تتم من خلال لوحة التحكم. يبدأ معالج الإعداد. اتبع التعليمات الموجودة على الشاشة.

تحديد عملية إزالة التطبيق

يمكنك تحديد أي من البيانات التي يستخدمها التطبيق الذي تريد حفظه للاستخدام في المستقبل، أثناء إجراء التثبيت التالي للتطبيق (مثل عند الترقية إلى إصدار أحدث من التطبيق). إذا لم تحدد أي بيانات، فسيتم إزالة التطبيق بالكامل (انظر الشكل أدناه).



حفظ البيانات بعد الإزالة

يمكنك حفظ البيانات التالية:

- **بيانات التفعيل**، التي تتيح لك تجنب الاضطرار إلى تفعيل التطبيق مرة أخرى. يضيف برنامج Kaspersky Endpoint Security مفتاح ترخيص تلقائيًا إذا لم تنته فترة الترخيص قبل التثبيت.

- **ملفات النسخ الاحتياطي** – ملفات يفحصها التطبيق ويضعها في النسخ الاحتياطي.

لا يمكن الوصول إلى ملفات النسخ الاحتياطي التي تم حفظها بعد إزالة التطبيق إلا عن طريق نفس إصدار التطبيق الذي تم استخدامه لحفظ هذه الملفات.

إذا كنت تنوي استخدام كائنات النسخ الاحتياطي بعد إزالة التطبيق، فيجب عليك استعادة هذه الكائنات قبل إزالة التطبيق. ومع ذلك، لا يوصي خبراء Kaspersky باستعادة الكائنات من النسخ الاحتياطي، لأن هذا يلحق الضرر بالكمبيوتر.

- **الإعدادات التشغيلية للتطبيق** – قيم إعدادات التطبيق التي تم تحديدها خلال تكوين التطبيق.

- **المخزن المحلي لمفاتيح التشفير** – البيانات التي توفر وصولاً إلى الملفات ومحركات الأقراص التي تم تشفيرها قبل إزالة التطبيق. لضمان الوصول إلى الملفات ومحركات الأقراص التي تم تشفيرها، تأكد أنك قمت بتحديد وظيفة تشفير البيانات عند إعادة تثبيت برنامج Kaspersky Endpoint Security. لا يلزم اتخاذ أي إجراء آخر للوصول إلى الملفات ومحركات الأقراص التي تم تشفيرها من قبل.

يمكنك أيضًا حذف التطبيق محليًا باستخدام سطر الأوامر.

ترخيص التطبيق

يوضح هذا القسم معلومات حول المفاهيم العامة المتعلقة بترخيص Kaspersky Endpoint Security.

حول اتفاقية ترخيص المستخدم النهائي

اتفاقية ترخيص المستخدم النهائي هي اتفاقية إلزامية بينك وبين AO Kaspersky Lab تحدد البنود التي يمكنك بموجبها استخدام التطبيق.

نوصي بقراءة بنود "اتفاقية الترخيص" بحرص قبل استخدام التطبيق.

يمكنك مراجعة بنود "اتفاقية الترخيص" بالطرق التالية:

- عند تثبيت Kaspersky Endpoint Security في الوضع التفاعلي.
- بقراءة ملف الترخيص .txt. هذا المستند موجود ضمن مجموعة توزيع التطبيق وموجود أيضًا في مجلد تثبيت التطبيق %ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES.

وبتأكيد أنك توافق على اتفاقية ترخيص المستخدم النهائي عند تثبيت التطبيق، توقع على قبولك شروط اتفاقية ترخيص المستخدم النهائي. إذا لم تكن موافقًا على بنود اتفاقية ترخيص المستخدم النهائي، يمكنك إلغاء التثبيت.

حول الترخيص

الترخيص هو حق استخدام التطبيق لفترة زمنية محدودة، والذي يتم منحه بموجب اتفاقية ترخيص المستخدم النهائي.

يمنحك الترخيص حق استخدام التطبيق وفقًا لشروط اتفاقية ترخيص المستخدم النهائي، والحق في تلقي الدعم الفني. ويعتمد نطاق المزايا المتاحة واستخدام التطبيقات على نوع الترخيص المستخدم في تفعيل التطبيق.

يتم توفير أنواع الترخيص التالية:

- تجريبي – ترخيص مجاني مُعد لتجريب التطبيق.

  يحتوي الترخيص التجريبي عادة على فترة قصيرة. بمجرد انتهاء الترخيص التجريبي، فسيتم تعطيل كل ميزات برنامج Kaspersky Endpoint Security. للاستمرار في استخدام التطبيق، يجب شراء ترخيص تجاري.

  يمكنك استخدام الترخيص التجريبي لتفعيل التطبيق لمرة واحدة فقط.

- تجاري – ترخيص مدفوع ثمنه مُقدم عند شراء Kaspersky Endpoint Security.

  تتوقف وظائف التطبيق المتاحة بموجب الترخيص التجاري على اختيار المنتج. تم توضيح المنتج المحدد في شهادة الترخيص. يمكن الاطلاع على المعلومات المتعلقة بالمنتجات المتوفرة على موقع ويب Kaspersky.

  عند انتهاء صلاحية الترخيص التجاري، يتم تعطيل الميزات الرئيسية للتطبيق. للاستمرار في استخدام التطبيق، يجب تجديد الترخيص التجاري. وإذا كنت لا تخطط لتجديد ترخيصك، فيجب عليك إزالة التطبيق من الكمبيوتر الخاص بك.

حول شهادة الترخيص

إن شهادة الترخيص هي مستند يتم إرساله إلى المستخدم إضافة إلى ملف مفتاح أو رمز تفعيل.

تتضمن شهادة الترخيص معلومات الترخيص التالية:

- مفتاح الترخيص أو رقم الطلب.
- تفاصيل المستخدم الذي تم منح الترخيص إليه.
- تفاصيل التطبيق الذي يمكن تفعيله باستخدام الترخيص.
- القيود على عدد وحدات الترخيص (على سبيل المثال، عدد الأجهزة التي يمكن استخدام التطبيق عليها بموجب الترخيص).
- تاريخ بدء فترة الترخيص.
- تاريخ انتهاء صلاحية الترخيص أو فترة الترخيص.
- نوع الترخيص.

حول الاشتراك

يعد الاشتراك في Kaspersky Endpoint Security بمثابة أمر شراء للتطبيق مع معلمات محددة (مثل تاريخ انتهاء صلاحية الاشتراك وعدد الأجهزة المحمية). يمكنك طلب اشتراك في Kaspersky Endpoint Security من مزود الخدمة الخاص بك (مثل مزود خدمة الإنترنت). يمكن تجديد الاشتراك يدويًا أو تلقائيًا، أو يمكنك إلغاء الاشتراك الخاص بك. يمكنك إدارة الاشتراك الخاص بك على موقع ويب مزود الخدمة.

يمكن أن يكون الاشتراك محدودًا (لمدة عام، على سبيل المثال) أو غير محدود (بدون تاريخ انتهاء صلاحية). لاستمرار عمل Kaspersky Endpoint Security عقب انتهاء مدة الاشتراك المحدود، ستحتاج إلى تجديد الاشتراك. يتم تجديد الاشتراك غير المحدود تلقائيًا إذا تم الدفع المسبق لخدمات البائع في الوقت المحدد.

عند انتهاء صلاحية اشتراك محدود، فقد يتم تزويدك بفترة سماح لتجديد الاشتراك يواصل التطبيق العمل خلالها. ويتحدد توافر ومدة فترة السماح هذه بواسطة مزود الخدمة.

لاستخدام Kaspersky Endpoint Security بموجب الاشتراك، يجب عليك تطبيق رمز التفعيل الوارد من مزود الخدمة. عقب تطبيق رمز التفعيل، يتم إضافة المفتاح النشط. يحدد المفتاح النشط الترخيص لاستخدام التطبيق بموجب الاشتراك. لا يمكنك تفعيل التطبيق تحت الاشتراك باستخدام ملف مفتاح. ويستطيع مزود الخدمة توفير رمز تفعيل فقط. لا يمكن إضافة مفتاح احتياطي تحت اشتراك.

قد لا يتم استخدام رموز التفعيل التي تم شراؤها بموجب الاشتراك لتفعيل إصدارات سابقة من Kaspersky Endpoint Security.

حول مفتاح الترخيص

مفتاح الترخيص هو تسلسل من البتات التي يمكنك استخدامها في تفعيل التطبيق ثم استخدامه وفق شروط اتفاقية ترخيص المستخدم النهائي.

لا يتم توفير شهادة الترخيص لمفتاح مضاف تحت اشتراك.

يمكنك إضافة مفتاح ترخيص إلى التطبيق إما بتطبيق ملف مفتاح أو إدخال رمز تفعيل.

يمكن منع المفتاح بواسطة Kaspersky، إذا تم انتهاك بنود اتفاقية ترخيص المستخدم النهائي. إذا تم حجب المفتاح، فستحتاج إلى إضافة مفتاح مختلف لمتابعة استخدام التطبيق.

هناك نوعان من المفاتيح: مفتاح نشط ومفتاح احتياطي.

المفتاح النشط هو المفتاح المستخدم حاليًا بواسطة التطبيق. يمكن إضافة مفتاح تجريبي أو تجاري كالمفتاح النشط. لا يمكن أن يتضمن التطبيق أكثر من مفتاح نشط.

المفتاح الاحتياطي هو مفتاح يخول المستخدم من استخدام التطبيق لكنه ليس قيد الاستخدام حاليًا. عند انتهاء صلاحية المفتاح النشط، يصبح المفتاح الاحتياطي نشطًا. لا يمكن إضافة مفتاح احتياطي إلا في حالة توفر المفتاح النشط.

يمكن إضافة مفتاح لترخيص تجريبي كمفتاح نشط فقط. ولا يمكن إضافته كمفتاح احتياطي. لا يمكن أن يحل مفتاح ترخيص تجريبي محل مفتاح نشط في الترخيص التجاري.

في حالة إضافة مفتاح إلى قائمة المفاتيح الممنوعة، فإن وظيفة التطبيق المحددة بواسطة الترخيص المستخدم لتفعيل التطبيق تظل متاحة لمدة ثمانية أيام. يخطر التطبيق المستخدم بإضافة المفتاح إلى قائمة المفاتيح الممنوعة. بعد ثمانية أيام، فإن عمل التطبيق يصبح محدودًا على مستوى الوظيفية المتوفر بعد انتهاء صلاحية الترخيص. يمكنك استخدام مكونات الحماية والمراقبة وإجراء فحص باستخدام قواعد بيانات التطبيق التي تم تثبيتها قبل انتهاء صلاحية الترخيص. يستمر التطبيق أيضًا بتشفير الملفات التي تم تعديلها وتشفيرها قبل انتهاء صلاحية الترخيص، لكن لا يتم تشفير الملفات الجديدة. استخدام شبكة Kaspersky Security Network غير متوفر.

حول رمز التفعيل

رمز التفعيل هو متتالية فريدة من 20 رمز حرفي عددي. أنت تدخل رمز التفعيل لإضافة مفتاح ترخيص يقوم بتفعيل Kaspersky Endpoint Security. أنت تستلم رمز تفعيل على عنوان البريد الإلكتروني الذي خصصته بعد شراء Kaspersky Endpoint Security.

لتفعيل التطبيق باستخدام رمز التفعيل، يلزم وجود اتصال بالإنترنت للاتصال بخوادم تفعيل Kaspersky.

عند تفعيل التطبيق باستخدام رمز التفعيل، يتم تحميل المفتاح النشط. ولا يمكن إضافة مفتاح ترخيص احتياطي إلا باستخدام رمز تفعيل، ولا يمكن إضافته باستخدام ملف مفتاح.

في حالة فقدان رمز التفعيل بعد تفعيل التطبيق، يمكنك استعادة رمز التفعيل. قد تحتاج إلى رمز التفعيل، على سبيل المثال، لتسجيل حساب Kaspersky CompanyAccount. وفي حالة فقدان رمز التفعيل بعد تفعيل التطبيق، اتصل بشريك Kaspersky الذي اشتريت الترخيص منه.

حول الملف الرئيسي

ملف المفتاح هو ملف بامتداد .key تحصل عليه من Kaspersky. ويكمن الغرض من ملف المفتاح في إضافة مفتاح ترخيص لتفعيل التطبيق.

سوف تحصل على ملف المفتاح على عنوان البريد الإلكتروني الذي كتبته عند شرائك Kaspersky Endpoint Security أو طلبت إصدار النسخة التجريبية من Kaspersky Endpoint Security.

لا تحتاج إلى الاتصال بخوادم تفعيل Kaspersky لتفعيل التطبيق باستخدام ملف مفتاح.

يمكنك استعادة ملف مفتاح إذا تم حذفه عن طريق الخطأ. قد تحتاج إلى ملف مفتاح لتسجيل Kaspersky CompanyAccount، على سبيل المثال.

لاستعادة ملف مفتاح، قم بإجراء أي مما يلي:

- اتصل بجهة بيع الترخيص.
- احصل على ملف مفتاح من موقع Kaspersky على الويب اعتمادًا على رمز التفعيل الموجود لديك.

عند تفعيل التطبيق باستخدام ملف مفتاح، يتم تحميل مفتاح نشط. لا يمكن إضافة مفتاح ترخيص احتياطي إلا باستخدام ملف مفتاح، ولا يمكن إضافته باستخدام رمز تفعيل.

مقارنة بين وظائف التطبيق حسب نوع الترخيص لمحطات العمل

تعتمد مجموعة الوظائف المتاحة في Kaspersky Endpoint Security على محطات العمل على نوع الترخيص (انظر الجدول أدناه).

انظر أيضًا مقارنة بين وظائف التطبيق للخوادم

المزايا	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	spersky ybrid Cloud curity erprise
الحماية من التهديدات المتقدمة								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
اكتشاف السلوك	✓	✓	✓	✓	✓	✓	✓	✓
منع الاستغلال	✓	✓	✓	✓	✓	✓	✓	✓
منع اختراق المضيف	✓	✓	✓	✓	✓	✓	✓	✓
محرك المعالجة	✓	✓	✓	✓	✓	✓	✓	✓
الحماية من التهديدات الأساسية								
الحماية من تهديدات الملفات	✓	✓	✓	✓	✓	✓	✓	✓
الحماية من تهديدات الويب	✓	✓	✓	✓	✓	✓	✓	✓
الحماية من تهديدات البريد	✓	✓	✓	✓	✓	✓	✓	✓
جدار الحماية	✓	✓	✓	✓	✓	✓	✓	✓
الحماية من تهديدات الشبكة	✓	✓	✓	✓	✓	✓	✓	✓
منع هجمات BadUSB	✓	✓	✓	✓	✓	✓	✓	✓
حماية AMSI	✓	✓	✓	✓	✓	✓	✓	✓
ضوابط الأمان								
فحص السجل	–	–	–	–	–	–	–	–
التحكم في التطبيقات	✓	✓	✓	✓	✓	✓	✓	✓
التحكم في الجهاز	✓	✓	✓	✓	✓	✓	✓	✓
التحكم في الويب	✓	✓	✓	✓	✓	✓	✓	✓
مراقبة عيوب	–	✓	✓	✓	✓	✓	–	✓

التكيف								
مراقبة سلامة الملف	–	–	–	–	–	–	–	–
تشفير البيانات								
تشفير القرص من Kaspersky	–	✓	✓	✓	✓	✓	–	✓
تشفير محرك الأقراص من BitLocker	–	✓	✓	✓	✓	✓	–	✓
التشفير على مستوى الملف	–	✓	✓	✓	✓	✓	–	✓
تشفير محركات الأقراص القابلة للإزالة	–	✓	✓	✓	✓	✓	–	✓
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–	–	–
Endpoint Detection and Response Expert	–	–	✓	–	–	–	–	–
Kaspersky Sandbox (يجب شراء ترخيص Kaspersky Sandbox بشكل منفصل)	✓	✓	✓	✓	✓	✓	✓	✓

مقارنة بين وظائف التطبيق حسب نوع الترخيص للخوادم

تعتمد مجموعة الوظائف المتاحة في Kaspersky Endpoint Security على الخوادم على نوع الترخيص (انظر الجدول أدناه).

انظر أيضًا مقارنة بين وظائف التطبيق لمحطات العمل

مقارنة بين مزايا برنامج Kaspersky Endpoint Security

المزايا	Kaspersky Endpoint Security for	Kaspersky Endpoint Security for	Kaspersky Total Security	Kaspersky Endpoint Detection and	Kaspersky Optimum Security	Kaspersky Endpoint Detection and	Kaspersky Hybrid Cloud	spersky ybrid Cloud

curity erprise	Security Standard	Response Expert		Response Optimum		Business Advanced	Business Select	
								الحماية من التهديدات المتقدمة
✓	✓	✓	✓	✓	✓	✓	✓	Kaspersky Security Network
✓	✓	✓	✓	✓	✓	✓	✓	اكتشاف السلوك
✓	✓	✓	✓	✓	✓	✓	✓	منع الاستغلال
–	–	–	–	–	–	–	–	منع اختراق المضيف
✓	✓	✓	✓	✓	✓	✓	✓	محرك المعالجة
								الحماية من التهديدات الأساسية
✓	✓	✓	✓	✓	✓	✓	✓	الحماية من تهديدات الملفات
✓	✓	✓	✓	✓	✓	✓	–	الحماية من تهديدات الويب
✓	✓	✓	✓	✓	✓	✓	–	الحماية من تهديدات البريد
✓	✓	✓	✓	✓	✓	✓	✓	جدار الحماية
✓	✓	✓	✓	✓	✓	✓	✓	الحماية من تهديدات الشبكة
✓	✓	✓	✓	✓	✓	✓	✓	منع هجمات BadUSB
✓	✓	✓	✓	✓	✓	✓	✓	حماية AMSI
								ضوابط الأمان
✓	–	–	–	–	–	–	–	فحص السجل
✓	–	✓	✓	✓	✓	✓	–	التحكم في التطبيقات
✓	✓	✓	✓	✓	✓	✓	–	التحكم في الجهاز
✓	✓	✓	✓	✓	✓	✓	–	التحكم في الويب
–	–	–	–	–	–	–	–	مراقبة عيوب التكيف
✓	–	–	–	–	–	–	–	مراقبة سلامة الملف
								تشفير البيانات

تشفير القرص من Kaspersky	–	–	–	–	–	–	–	–
تشفير محرك الأقراص من BitLocker	–	✓	✓	✓	✓	✓	–	✓
التشفير على مستوى الملف	–	–	–	–	–	–	–	–
تشفير محركات الأقراص القابلة للإزالة	–	–	–	–	–	–	–	–
Detection and Response								
Endpoint Detection and Response Optimum	–	–	–	–	✓	✓	–	–
Endpoint Detection and Response Expert	–	–	✓	–	–	–	–	–
Kaspersky Sandbox (يجب شراء ترخيص Kaspersky Sandbox بشكل منفصل)	✓	✓	✓	✓	✓	✓	✓	✓

تفعيل التطبيق

التفعيل هي عملية تفعيل التطبيق تتيح لك استخدام إصدار كامل الوظائف من التطبيق حتى انتهاء صلاحية الترخيص. يتضمن تفعيل التطبيق إضافة مفتاح ترخيص.

يمكنك تفعيل التطبيق بإحدى الطرق التالية:

- محليًا من واجهة التطبيق باستخدام معالج التفعيل يمكنك إضافة المفتاح النشط والمفتاح الاحتياطي بهذه الطريقة.
- عن بُعد باستخدام مجموعة برامج Kaspersky Security Center عن طريق إنشاء ثم بدء مهمة إضافة مفتاح ترخيص. يمكنك إضافة المفتاح النشط والمفتاح الاحتياطي بهذه الطريقة.
- عن بُعد عن طريق توزيع ملفات المفتاح ورموز التفعيل المخزنة في مخزن مفاتيح خادم إدارة Kaspersky Security Center إلى أجهزة كمبيوتر العملاء. وللمزيد من التفاصيل حول مفاتيح التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center. يمكنك إضافة المفتاح النشط والمفتاح الاحتياطي بهذه الطريقة.

يتم توزيع رمز التفعيل الذي تم شراؤه بموجب الاشتراك في المقام الأول.

- استخدام سطر الأوامر.

قد تنتظر لبعض الوقت حتى يتم تفعيل التطبيق باستخدام رمز تفعيل (أثناء التثبيت عن بُعد أو التثبيت غير التفاعلي)، وذلك نظرًا لتوزيع الأحمال عبر خوادم التفعيل في Kaspersky. إذا كنت تريد تفعيل التطبيق في الحال، فيمكنك مقاطعة عملية التفعيل الجارية وبدء التفعيل باستخدام "معالج التفعيل".

تنشيط التطبيق من خلال Kaspersky Security Center

يمكنك تفعيل الإدارة عن بُعد من خلال Kaspersky Security Center Security Center بالطرق التالية:

- استخدام مهمة إضافة مفتاح.

  تتيح لك هذه الطريقة القيام بإضافة مفتاح لجهاز كمبيوتر معين أو لأجهزة الكمبيوتر التي تُعد جزءًا من مجموعة الإدارة.

- عن طريق توزيع المفتاح الذي تم تخزينه في خادم الإدارة Kaspersky Security Center على أجهزة الكمبيوتر.

  تتيح لك هذه الطريقة إضافة مفتاح إلى أجهزة الكمبيوتر المتصلة بالفعل بمركز Kaspersky Security Center وإلى أجهزة الكمبيوتر الجديدة. لاستخدام هذه الطريقة، ستحتاج أولاً ان تضيف المفتاح إلى خادم إدارة Kaspersky Security Center. للمزيد من التفاصيل حول إضافة المفاتيح إلى خادم إدارة Kaspersky Security Center، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

- عن طريق إضافة المفتاح إلى حزمة تثبيت Kaspersky Endpoint Security.

  تتيح لك هذه الطريقة إضافة المفتاح في خصائص حزمة التثبيت أثناء نشر Kaspersky Endpoint Security. ولا يتم تفعيل التطبيق تلقائيًا بعد التثبيت.

يتم توفير إصدار تجريبي من Kaspersky Security Center Cloud Console. الإصدار التجريبي هو إصدار خاص من Kaspersky Security Center Cloud Console مصمم لتعريف المستخدم على مزايا التطبيق. يمكنك في ذلك الإصدار أن تتخذ إجراءات في مساحة عمل لفترة 30 يومًا. جميع التطبيقات المدارة تعمل بموجب ترخيص تجريبي لـ Kaspersky Security Center Cloud Console، بما في ذلك Kaspersky Endpoint Security. رغم ذلك، لا يمكنك تفعيل Kaspersky Endpoint Security باستخدام ترخيصه التجريبي عندما تنتهي صلاحية الترخيص التجريبي من Kaspersky Security Center Cloud Console. للحصول على معلومات تفصيلية عن ترخيص Kaspersky Security Center، يُرجى الرجوع إلى تعليمات Kaspersky Security Center Cloud Console.

الإصدار التجريبي من Kaspersky Security Center Cloud Console لا يسمح لك بالانتقال إلى إصدار تجاري في النهاية. سوف يتم حذف أي مساحة عمل تجريبية بجميع محتوياتها بعد انتهاء الفترة البالغة 30 يومًا.

يمكنك مراقبة استخدام التراخيص بالطرق التالية:

- عرض تقرير استخدام المفتاح للبنية التحتية للمؤسسة (**Monitoring and reporting** ← **Reports**).
- عرض حالات أجهزة الكمبيوتر في علامة التبويب **الأجهزة** ← **الأجهزة المدارة**. إذا لم يتم تفعيل التطبيق، فستكون حالة الكمبيوتر ⚠ لم يتم تفعيل التطبيق.
- عرض معلومات الترخيص في خصائص الكمبيوتر.
- عرض خصائص المفتاح (**Licensing** ← **Operations**).

كيفية تفعيل التطبيق في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (12.1)** ← **إضافة مفتاح**.

الخطوة الثانية: إضافة مفتاح

أدخل رمز التفعيل أو حدد ملف مفتاح.

للمزيد من التفاصيل حول إضافة المفاتيح إلى مستودع Kaspersky Security Center، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

الخطوة الثالثة: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الرابعة: تكوين جدول بدء المهمة

قم بتكوين جدول لبدء المهمة، على سبيل المثال يدويًا أو عندما يكون الكمبيوتر خاملاً.

الخطوة الخامسة: تحديد اسم المهمة

أدخل اسمًا للمهمة، مثل تفعيل برنامج Kaspersky Endpoint Security for Windows.

الخطوة 6 إكمال إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة. ونتيجة لذلك، سيتم تفعيل Kaspersky Endpoint Security على أجهزة كمبيوتر المستخدمين في الوضع الصامت.

كيفية تفعيل التطبيق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة 1. تكوين إعدادات المهمة العامة

تكوين إعدادات المهمة:

1. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.
2. في القائمة المنسدلة **Task type** حدد **Add key**.
3. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، تفعيل برنامج Kaspersky Endpoint Security for Windows للمدراء.
4. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة. انتقل إلى الخطوة التالية.

الخطوة الثانية: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الثالثة: اختيار ترخيص

حدد الترخيص الذي ترغب في استخدامه لتفعيل التطبيق. انتقل إلى الخطوة التالية.

يمكنك إضافة مفاتيح إلى **Licensing** ← **Operations** (Web Console).

الخطوة 4 إكمال إنشاء المهمة

قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**. سيتم عرض مهمة جديدة في قائمة المهام. لتشغيل المهمة، حدد خانة الاختيار المقابلة لها وانقر فوق الزر **Start**. ونتيجة لذلك، سيتم تفعيل Kaspersky Endpoint Security على أجهزة كمبيوتر المستخدمين في الوضع الصامت.

في خصائص مهمة إضافة مفتاح، يمكنك إضافة مفتاح احتياطي إلى الكمبيوتر. يصبح المفتاح الإضافي نشطًا عند انتهاء صلاحية المفتاح النشط أو حذفه. وجود مفتاح إضافي يتيح لك إمكانية تجنب قيود وظائف التطبيق عندما تنتهي صلاحية الترخيص.

كيفية إضافة مفتاح ترخيص بشكل آلي إلى أجهزة الكمبيوتر من خلال وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **تراخيص Kaspersky** .

ستفتح قائمة بمفاتيح الترخيص.

2. افتح خصائص مفتاح الترخيص.

3. في قسم **عام**، حدد خانة الاختيار **مفتاح ترخيص موزع تلقائيًا**.

4. احفظ تغييراتك.

ونتيجة لذلك، سيتم توزيع المفتاح تلقائيًا على أجهزة الكمبيوتر المناسبة. أثناء التوزيع التلقائي للمفتاح باعتباره مفتاح نشط أو احتياطي، تتم مراعاة حد الترخيص (المحدد في خصائص المفتاح) الذي ينطبق على عدد أجهزة الكمبيوتر. إذا تم الوصول إلى حد الترخيص يتم إيقاف توزيع هذا المفتاح على أجهزة الكمبيوتر تلقائياً. يمكنك عرض عدد أجهزة الكمبيوتر التي تمت إضافة المفتاح إليها وبيانات أخرى في خصائص المفتاح في قسم **الأجهزة**.

كيفية إضافة مفتاح ترخيص بشكل آلي إلى أجهزة الكمبيوتر من خلال Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Operations** ← **Licensing** ← **Kaspersky Licenses**.

ستفتح قائمة بمفاتيح الترخيص.

2. افتح خصائص مفتاح الترخيص.

3. من النافذة **General**، قم بتفعيل زر **Deploy license key automatically**.

4. احفظ تغييراتك.

ونتيجة لذلك، سيتم توزيع المفتاح تلقائيًا على أجهزة الكمبيوتر المناسبة. أثناء التوزيع التلقائي للمفتاح باعتباره مفتاح نشط أو احتياطي، تتم مراعاة حد الترخيص (المحدد في خصائص المفتاح) الذي ينطبق على عدد أجهزة الكمبيوتر. إذا تم الوصول إلى حد الترخيص يتم إيقاف توزيع هذا المفتاح على أجهزة الكمبيوتر تلقائياً. يمكنك عرض عدد أجهزة الكمبيوتر التي تمت إضافة المفتاح إليها وبيانات أخرى في خصائص المفتاح في علامة التبويب **Devices**.

استخدام معالج التفعيل لتفعيل التطبيق

لتفعيل Kaspersky Endpoint Security باستخدام "معالج الإعداد":

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **الترخيص**.

2. انقر على **تفعيل التطبيق باستخدام ترخيص جديد**.

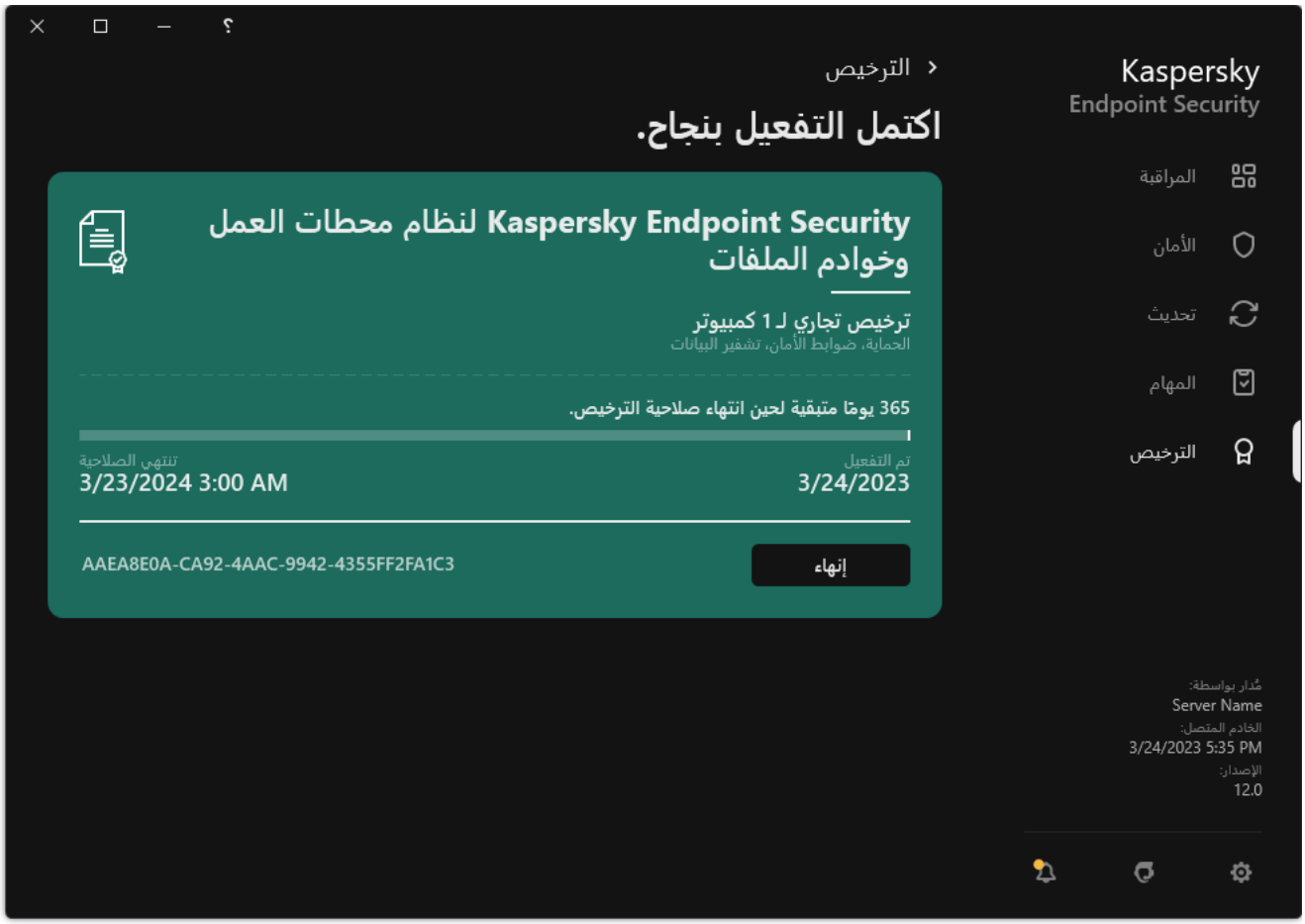
يبدأ معالج تفعيل التطبيق. اتبع تعليمات معالج التفعيل.

تفعيل التطبيق

عرض معلومات التراخيص

لعرض المعلومات بشأن التراخيص:

في نافذة التطبيق الرئيسية ، انتقل إلى القسم **التراخيص** (انظر الشكل أدناه).



نافذة الترخيص

يعرض القسم التفاصيل التالية:

- حالة المفتاح. يمكن تخزين عدة مفاتيح على جهاز الكمبيوتر. هناك نوعان من المفاتيح: مفتاح نشط ومفتاح احتياطي. لا يمكن أن يتضمن التطبيق أكثر من مفتاح نشط. قد يصبح المفتاح الاحتياطي مفعلاً فقط عند انتهاء صلاحية المفتاح المفعل أو بعد حذف المفتاح بالنقر فوق **حذف**.
- اسم التطبيق. الاسم الكامل لتطبيق Kaspersky الذي تم شراءه.
- نوع الترخيص. أنواع التراخيص التالية متاحة تجريبيًا أو تجاريًا.
- الوظيفة. ميزات التطبيق المتاحة تحت رخصتك. قد تتضمن الميزات الحماية وضوابط الأمان وتشفير البيانات وغيرها. ويتم أيضًا توفير قائمة بالمزايا المتاحة في شهادة الترخيص.
- معلومات إضافية حول الترخيص. تاريخ البدء وتاريخ انتهاء فترة الترخيص (فقط للمفتاح المفعل)، والمدة المتبقية من فترة الترخيص.

يتم عرض وقت انتهاء صلاحية الترخيص وفقًا للمنطقة الزمنية التي تم تكوينها في نظام التشغيل.

- المفتاح. المفتاح هو تسلسل أبجدي رقمي فريد يتم إنشاؤه من رمز التفعيل أو ملف مفتاح.

في نافذة الترخيص قم بأحد الإجراءات التالية:

- **شراء ترخيص / تجديد الترخيص**. قم بفتح موقع ويب متجر Kaspersky عبر الإنترنت حيث يمكنك شراء أو تجديد الترخيص. يُرجى إدخال معلومات شركتك ودفع ثمن الطلب.
- **تفعيل التطبيق باستخدام ترخيص جديد**. يبدأ معالج تفعيل التطبيق. في هذا المعالج يمكنك إضافة مفتاح باستخدام رمز التفعيل أو ملف مفتاح. يسمح لك معالج تفعيل التطبيق بإضافة مفتاح نشط ومفتاح احتياطي واحد فقط.

شراء الترخيص

يمكنك شراء ترخيص بعد تثبيت التطبيق. عند شراء ترخيص، تحصل على رمز تفعيل أو ملف مفتاح لتفعيل التطبيق.

لشراء ترخيص:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **الترخيص**.

2. قم بأحد الإجراءات التالية:

- في حال عدم إضافة أي مفاتيح أو تمت إضافة مفتاح للترخيص التجريبي، انقر فوق الزر **شراء ترخيص**.
- إذا تمت إضافة مفتاح للترخيص التجاري، انقر فوق الزر **تجديد الترخيص**.

تفتح نافذة بها موقع متجر Kaspersky على الإنترنت، حيث يمكنك شراء الترخيص.

تجديد الاشتراك

عندما تستخدم التطبيق بموجب الاشتراك، يقوم Kaspersky Endpoint Security تلقائيًا بالاتصال بخادم التفعيل في فترات زمنية محددة حتى انتهاء صلاحية الاشتراك الخاص بك.

إذا قمت باستخدام التطبيق بموجب الاشتراك، يقوم Kaspersky Endpoint Security تلقائيًا بالتحقق من خادم التفعيل للمفاتيح المجددة في وضع الخلفية. إذا كان المفتاح نشطًا على خادم التفعيل، يقوم التطبيق بإضافته عن طريق استبدال المفتاح السابق. بهذه الطريقة، يتم تجديد الاشتراك غير المحدود لـ Kaspersky Endpoint Security دون تدخل المستخدم.

إذا كنت تستخدم التطبيق بموجب اشتراك محدود، فسوف يخطرك Kaspersky Endpoint Security في تاريخ انتهاء الاشتراك (أو في تاريخ انتهاء فترة السماح لتجديد الاشتراك)حول هذا ويتوقف عن محاولة تجديد الاشتراك تلقائيًا. في هذه الحالة، يعمل Kaspersky Endpoint Security بنفس الطريقة كما يحدث عند انتهاء صلاحية الترخيص التجاري للتطبيق: يعمل التطبيق بدون تحديثات كما لا تتوفر شبكة Kaspersky Security Network.

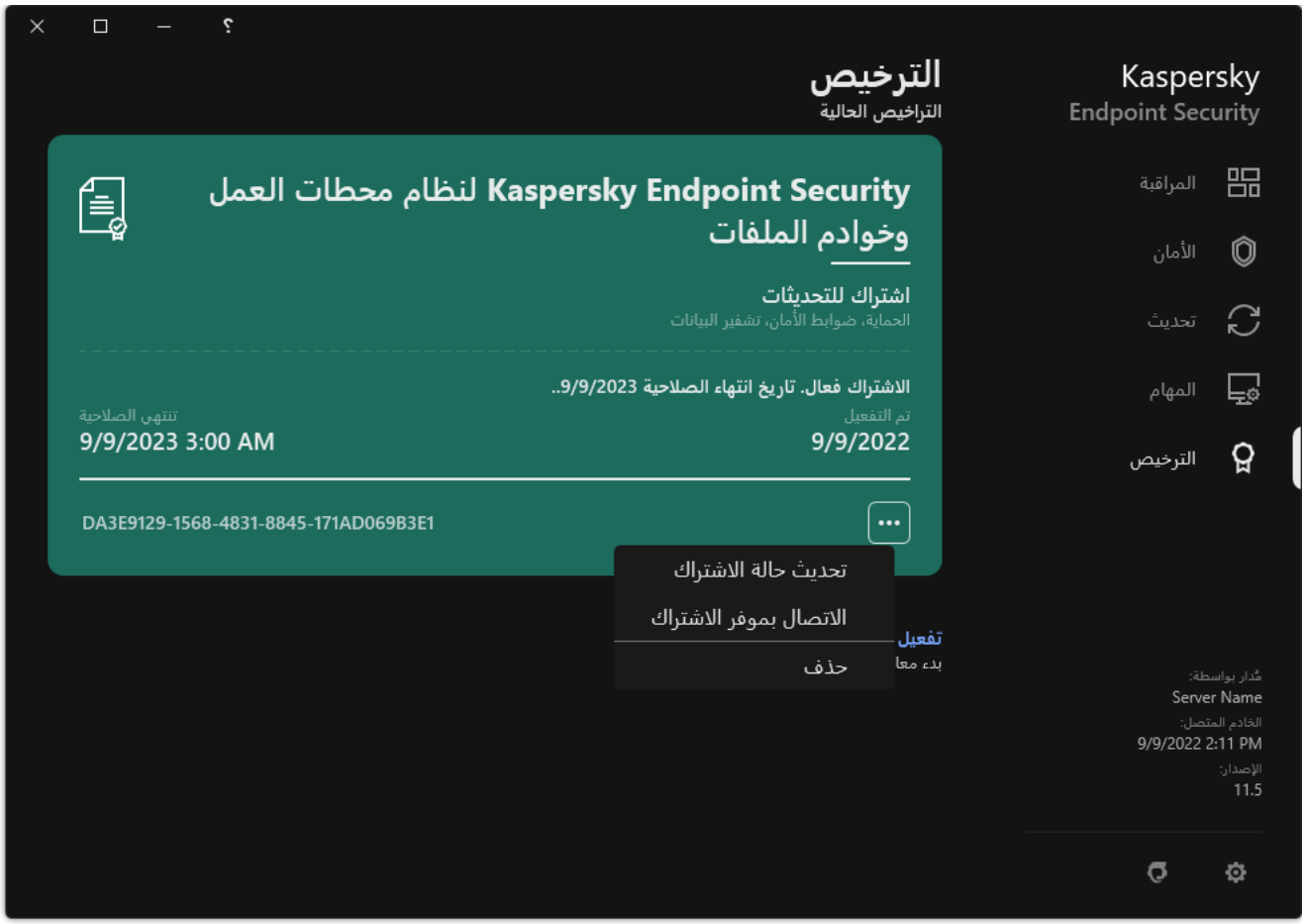
يمكنك تجديد الاشتراك على موقع ويب مزود الخدمة.

لزيارة موقع ويب مزود الخدمة من واجهة التطبيق:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **الترخيص**.

2. انقر على **الاتصال بموفر الاشتراك**.

يمكنك تحديث حالة الاشتراك يدويًا. قد يكون ذلك مطلوبًا في حالة تجديد الاشتراك عقب فترة السماح ولم يقم التطبيق بتحديث حالة الاشتراك تلقائيًا.



تجديد الاشتراك

توفير البيانات بموجب اتفاقية ترخيص المستخدم النهائي

في حالة استخدام رمز تفعيل لتفعيل Kaspersky Endpoint Security، فإنك توافق على إرسال المعلومات التالية بشكل دوري تلقائيًا إلى Kaspersky لأغراض التحقق من الاستخدام الصحيح للتطبيق:

- نوع وإصدار وترجمة Kaspersky Endpoint Security؛
- إصدارات التحديثات المثبتة لتطبيق Kaspersky Endpoint Security؛
- معرف الكمبيوتر ومعرف تثبيت Kaspersky Endpoint Security المحدد على الكمبيوتر؛
- الرقم المسلسل ومُعرّف المفتاح المفعل؛
- نوع وإصدار ومعدل بت نظام التشغيل واسم البيئة الظاهرية (في حالة تثبيت Kaspersky Endpoint Security في بيئة ظاهرية)؛
- معرفات مكونات Kaspersky Endpoint Security الفعالة عند إرسال المعلومات.

قد تستخدم Kaspersky أيضًا هذه المعلومات لتوليد الإحصاءات المتعلقة بنشر واستعمال برامج Kaspersky.

عن طريق استخدام رمز التفعيل، فإنك توافق على نقل البيانات المذكورة أعلاه تلقائيًا. إذا كنت لا توافق على إرسال هذه المعلومات إلى Kaspersky، فينبغي أن تستخدم ملف مفتاح لتفعيل Kaspersky Endpoint Security.

عن طريق قبول بنود اتفاقية ترخيص المستخدم النهائي، فإنك توافق على إرسال المعلومات التالية تلقائيًا:

- عند ترقية Kaspersky Endpoint Security:
  - إصدار Kaspersky Endpoint Security؛
  - معرف Kaspersky Endpoint Security؛
  - مفتاح نشط؛
  - المعرف الفريد لبدء مهمة الترقية؛
  - المعرف الفريد لتثبيت Kaspersky Endpoint Security.
- عند اتباع الروابط من واجهة Kaspersky Endpoint Security:
  - إصدار Kaspersky Endpoint Security؛
  - إصدار نظام التشغيل؛
  - تاريخ تفعيل Kaspersky Endpoint Security؛
  - تاريخ انتهاء صلاحية الترخيص؛
  - تاريخ إنشاء المفتاح؛
  - تاريخ تثبيت Kaspersky Endpoint Security؛
  - معرف Kaspersky Endpoint Security؛

- معرف الثغرة الأمنية المكتشفة في نظام التشغيل؛
- معرف آخر تحديث مثبت لتطبيق Kaspersky Endpoint Security؛
- تجزئة الملف المكتشف الخاضع للتهديد، واسم هذا التهديد وفقًا لتصنيف Kaspersky؛
- فئة خطأ تفعيل Kaspersky Endpoint Security؛
- رمز خطأ تفعيل Kaspersky Endpoint Security؛
- عدد الأيام المتبقية حتى انتهاء صلاحية المفتاح؛
- عدد الأيام التي انقضت منذ إضافة المفتاح؛
- عدد الأيام التي انقضت منذ انتهاء صلاحية الترخيص؛
- عدد أجهزة الكمبيوتر التي يتم تطبيق الترخيص الحالي عليها؛
- مفتاح نشط؛
- فترة ترخيص Kaspersky Endpoint Security؛
- الحالة الحالية للترخيص؛
- نوع الترخيص الحالي؛
- نوع التطبيق؛
- المعرف الفريد لبدء مهمة الترقية؛
- المعرف الفريد لتثبيت Kaspersky Endpoint Security على الكمبيوتر؛
- لغة واجهة Kaspersky Endpoint Security.

تتم حماية المعلومات التي يتم الحصول عليها بواسطة Kaspersky بما يتفق مع القانون والمتطلبات واللوائح المعمول بها الخاصة بـ Kaspersky. يتم نقل البيانات عبر قنوات تواصل مشفرة.

اقرأ اتفاقية ترخيص المستخدم النهائي وتفضل بزيارة موقع ويب Kaspersky لمعرفة المزيد حول كيفية تلقي المعلومات المتعلقة باستخدام التطبيق ومعالجتها وتخزينها وتدميرها بعد قبول اتفاقية ترخيص المستخدم النهائي والموافقة على بيان Kaspersky Security Network. يحتوي ملفا license.txt وksn_<language ID>.txt على نص اتفاقية ترخيص المستخدم النهائي وبيان Kaspersky Security Network التي تتضمنها حزمة التوزيع.

حول توفير البيانات عند استخدام Kaspersky Security Network

تعتمد مجموعة البيانات التي يرسلها Kaspersky Endpoint Security إلى Kaspersky على نوع الترخيص وإعدادات استخدام Kaspersky Security Network.

استخدام KSN بموجب ترخيص على ما لا يزيد عن 4 أجهزة كمبيوتر

عن طريق قبول بيان Kaspersky Security Network، فإنك توافق على إرسال المعلومات التالية تلقائيًا:

- معلومات حول تحديثات تكوين شبكة KSN: مُعرّف التكوين النشط، مُعرّف التكوين الذي تم استلامه، رمز الخطأ الخاص بتحديث التكوين؛

- معلومات حول الملفات وعناوين URL المراد فحصها: المجاميع الاختبارية للملف الذي خضع للفحص (MD5، SHA2-256، SHA1) وأنماط الملفات (MD5)، وحجم النمط، ونوع التهديد المكتشف واسمه وفقًا لتصنيف المالك، والمُعرّف المخصص لقواعد بيانات مكافحة الفيروسات، وعنوان URL الذي يتم طلب السمعة من أجله، فضلاً عن عنوان URL المُوجّه، ومُعرّف بروتوكول الاتصال ورقم المنفذ قيد الاستخدام؛

- معرف مهمة الفحص التي اكتشفت التهديد؛

- معلومات حول الشهادات الرقمية قيد الاستخدام والضرورية للتحقق من صحتها وأصالتها: المجاميع الاختبارية (SHA256) الخاصة بالشهادة المستخدمة لتوقيع الكائن الذي خضع للفحص والمفتاح العام للشهادة؛

- مُعرّف مكون البرامج الذي يقوم بإجراء الفحص؛

- المُعرّفات الخاصة بقواعد بيانات مكافحة الفيروسات والخاصة بالسجلات الموجودة في قواعد بيانات مكافحة الفيروسات هذه؛

- معلومات حول تفعيل البرامج على جهاز الكمبيوتر: مقدمة التذكرة الموقعة من خدمة التفعيل (مُعرّف مركز التفعيل الإقليمي، المجموع الاختباري لرمز التفعيل، المجموع الاختباري للتذكرة، تاريخ إنشاء التذكرة، المُعرّف الفريد من نوعه للتذكرة، إصدار التذكرة، حالة الترخيص، تاريخ ووقت بدء/إنهاء صلاحية التذكرة، المُعرّف الفريد من نوعه للترخيص، إصدار الترخيص)، مُعرّف الشهادة المستخدمة لتوقيع مقدمة التذكرة، المجموع الاختباري (MD5) لملف المفتاح؛

- معلومات حول برنامج صاحب الحق: الإصدار الكامل والنوع وإصدار البروتوكول المستخدم للاتصال بخدمات Kaspersky.

استخدام KSN بموجب ترخيص على 5 أجهزة كمبيوتر أو أكثر

عن طريق قبول بيان Kaspersky Security Network، فإنك توافق على إرسال المعلومات التالية تلقائيًا:

في حالة تحديد خانة الاختيار **Kaspersky Security Network** ومسح خانة الاختيار **تمكين وضع KSN الموسع**، يرسل التطبيق المعلومات التالية:

- معلومات حول تحديثات تكوين شبكة KSN: مُعرّف التكوين النشط، مُعرّف التكوين الذي تم استلامه، رمز الخطأ الخاص بتحديث التكوين؛

- معلومات حول الملفات وعناوين URL المراد فحصها: المجاميع الاختبارية للملف الذي خضع للفحص (MD5، SHA2-256، SHA1) وأنماط الملفات (MD5)، وحجم النمط، ونوع التهديد المكتشف واسمه وفقًا لتصنيف المالك، والمُعرّف المخصص لقواعد بيانات مكافحة الفيروسات، وعنوان URL الذي يتم طلب السمعة من أجله، فضلاً عن عنوان URL المُوجّه، ومُعرّف بروتوكول الاتصال ورقم المنفذ قيد الاستخدام؛

- معرف مهمة الفحص التي اكتشفت التهديد؛

- معلومات حول الشهادات الرقمية قيد الاستخدام والضرورية للتحقق من صحتها وأصالتها: المجاميع الاختبارية (SHA256) الخاصة بالشهادة المستخدمة لتوقيع الكائن الذي خضع للفحص والمفتاح العام للشهادة؛

- مُعرّف مكون البرامج الذي يقوم بإجراء الفحص؛

- المُعرّفات الخاصة بقواعد بيانات مكافحة الفيروسات والخاصة بالسجلات الموجودة في قواعد بيانات مكافحة الفيروسات هذه؛

- معلومات حول تفعيل البرامج على جهاز الكمبيوتر: مقدمة التذكرة الموقعة من خدمة التفعيل (مُعرّف مركز التفعيل الإقليمي، المجموع الاختباري لرمز التفعيل، المجموع الاختباري للتذكرة، تاريخ إنشاء التذكرة، المُعرّف الفريد من نوعه للتذكرة، إصدار التذكرة، حالة الترخيص، تاريخ ووقت بدء/إنهاء صلاحية التذكرة، المُعرّف الفريد من نوعه للترخيص، إصدار الترخيص)، مُعرّف الشهادة المستخدمة لتوقيع مقدمة التذكرة، المجموع الاختباري (MD5) لملف المفتاح؛

- معلومات حول برنامج صاحب الحق: الإصدار الكامل والنوع وإصدار البروتوكول المستخدم للاتصال بخدمات Kaspersky.

في حالة تحديد خانة الاختيار **تمكين وضع KSN الموسع** بالإضافة إلى خانة الاختيار **Kaspersky Security Network**، يرسل التطبيق المعلومات التالية كذلك بالإضافة إلى المعلومات المذكورة أعلاه:

- معلومات حول نتائج تصنيف موارد الويب المطلوبة، التي تحتوي على عنوان URL الذي تمت معالجته وعنوان IP الخاص بالمضيف، وإصدار مكون البرامج الذي قام بتنفيذ التصنيف، وطريقة التصنيف، ومجموعة الفئات المحددة لموارد الويب؛

- معلومات حول البرامج المثبتة على جهاز الكمبيوتر: أسماء تطبيقات البرامج وبائعي البرامج، ومفاتيح السجل وقيمها، معلومات حول ملفات مكونات البرامج المثبتة (أسماء المجاميع الاختبارية (MD5، SHA2-256، SHA1)، والمسار المؤدي إلى الملف على جهاز الكمبيوتر، والحجم، والإصدار، والتوقيع

الرقمي)؛

- معلومات حول حالة الحماية من الفيروسات للكمبيوتر: الإصدارات والطوابع الزمنية لإصدار قواعد بيانات مكافحة الفيروسات المستخدمة، ومعرف المهمة ومعرف البرنامج الذي يجري الفحص؛

- معلومات حول الملفات التي يتم تنزيلها من جانب المستخدم النهائي: عناوين URL و IP الخاصة بعملية التنزيل وصفحات التنزيل، مُعرّف بروتوكول التنزيل ورقم منفذ الاتصال، حالة عناوين URL باعتبارها ضارة أم لا، سمات الملف، الحجم والمجاميع الاختبارية (MD5، SHA2-256، SHA1)، معلومات حول العملية التي قامت بتنزيل الملف (المجاميع الاختبارية (MD5، SHA2-256، SHA1)، تاريخ ووقت الإنشاء/البناء، وحالة التشغيل التلقائي، والسمات، وأسماء منشئي الحزم، معلومات حول التوقيعات، علامة الملف القابل للتنفيذ، ومُعرّف التنسيق، والإن روبيا)، اسم الملف والمسار المؤدي له على جهاز الكمبيوتر، التوقيع الرقمي للملف والطابع الزمني لعملية إنشائه، عنوان URL حيث وقعت عملية الاكتشاف، رقم البرنامج النصي على الصفحة التي يبدو أنه مشكوك فيها أو ضارة، معلومات حول طلبات HTTP التي تم إنشاؤها والاستجابة لها؛

- معلومات حول التطبيقات قيد التشغيل والوحدات النمطية لها: البيانات بشأن العمليات قيد التشغيل على النظام (مُعرّف العملية (PID)، اسم العملية، معلومات حول الحساب الذي بدأت العملية منه، التطبيق والأمر الذي بدأ العملية، توقيع البرنامج أو العملية الموثوقة، المسار الكامل المؤدي إلى ملفات العملية والمجاميع الاختبارية (MD5، SHA2-256، SHA1)، وسطر الأوامر لبداية العملية، ومستوى تكامل العملية، ووصف المنتج الذي تنتمي العملية له (اسم المنتج والمعلومات حول الناشر)، فضلاً عن الشهادات الرقمية قيد الاستخدام والمعلومات المطلوبة للتحقق من أصالتها وصحتها أو المعلومات حول غياب التوقيع الرقمي للملف)، والمعلومات حول الوحدات النمطية التي تم تحميلها داخل العمليات (أسمائها، وأحجامها، وأنواعها، وتواريخ إنشائها، وسماتها، والمجاميع الاختبارية (MD5، SHA2-256، SHA1)، والمسارات المؤدية لها على جهاز الكمبيوتر)، معلومات مقدمة الملف التنفيذي المحمول، أسماء منشئي الحزم (في حال كان الملف مضمن في حزمة)؛

- معلومات حول جميع الكائنات والأنشطة المحتمل أن تكون ضارة: اسم الكائن المكتشف والمسار الكامل المؤدي إلى الكائن على جهاز الكمبيوتر، والمجاميع الاختبارية للملفات التي تمت معالجتها (MD5، SHA2-256، SHA1)، وتاريخ ووقت الاكتشاف، وأسماء وأحجام الملفات المصابة والمسارات المؤدية إليها، ورمز قالب المسار، وعلامة الملف التنفيذي، ومؤشر على ما إذا كان الكائن عبارة عن حاوية، وأسماء منشئ الحزمة (إذا كان الملف مضغوطًا)، ورمز نوع الملف، ومُعرّف تنسيق الملف، وقائمة الإجراءات التي تنفذها البرمجيات الضارة والقرار الذي اتخذه البرنامج والمستخدم للاستجابة لها، ومُعرّفات قواعد بيانات مكافحة الفيروسات ومُعرّفات السجلات الموجودة في قواعد بيانات مكافحة الفيروسات هذه التي تم استخدامها لاتخاذ القرار، ومؤشر لكائن محتمل أن يكون ضارًا، واسم التهديد المكتشف وفقًا لتصنيف المالك، ومستوى الخطر، وحالة الاكتشاف وطريقة الاكتشاف، وسبب الإدراج في السياق الذي تم تحليله ورقم تسلسل الملف في السياق، والمجاميع الاختبارية (MD5، SHA2-256، SHA1)، واسم وسمات الملف التنفيذي للتطبيق الذي تم إرسال الرسالة المصابة أو الارتباط المصاب من خلاله، وعناوين IP غير الشخصية (IPv4 و IPv6) الخاصة بمضيف الكائن الممنوع، وإنتروبيا الملف، ومؤشر التشغيل التلقائي للملف، ووقت اكتشاف الملف لأول مرة في النظام، وعدد مرات تشغيل الملف منذ إرسال الإحصاءات الأخيرة، ومعلومات حول الاسم، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) وحجم عميل البريد الذي تم استلام الكائن الضار من خلاله، ومُعرّف مهمة البرنامج الذي أجرى الفحص، ومؤشر حول ما إذا تم التحقق من سمعة الملف أو التوقيع، ونتيجة معالجة الملف، والمجموع الاختباري (MD5) للنمط الذي تم جمعه للكائن، وحجم النمط بالبايت، والمواصفات الفنية لتقنيات الاكتشاف المطبقة؛

- معلومات حول الكائنات التي تم فحصها: مجموعة الثقة المخصصة التي تم وضع الملف فيها و/أو نقل الملف منها، وسبب وضع الملف في تلك الفئة، ومُعرّف الفئة، ومعلومات حول مصدر الفئات والإصدار الخاص بقاعدة بيانات الفئة، وعلامة شهادة الثقة الخاصة بالملف، واسم مورّد الملف، وإصدار الملف، واسم وإصدار تطبيق البرنامج الذي يتضمن الملف؛

- معلومات حول الثغرات الأمنية المكتشفة: مُعرّف الثغرة الأمنية في قاعدة بيانات الثغرات الأمنية، درجة خطورة الثغرة الأمنية؛

- معلومات حول محاكاة الملف القابل للتنفيذ: حجم الملف والمجاميع الاختبارية (MD5، SHA2-256، SHA1) له، وإصدار مكون المحاكاة، وعمق المحاكاة، ومجموعة الخصائص للكتل المنطقية والوظائف داخل الكتل المنطقية التي تم الحصول عليها أثناء عملية المحاكاة، والبيانات من عناوين PE للملف القابل للتنفيذ؛

- عناوين IP الخاصة بجهاز الكمبيوتر المهاجم (IPv4 وIPv6)، ورقم المنفذ الموجود في جهاز الكمبيوتر الذي تم توجيه هجوم شبكة الاتصال له، ومُعرّف البروتوكول الخاص بحزمة IP الذي يحتوي على الهجوم، وهدف الهجوم (اسم المؤسسة، وموقع الويب)، والعلامة المعبرة عن رد الفعل على الهجوم، وحجم تأثير الهجوم، ومستوى الثقة؛

- معلومات حول الهجمات المرتبطة بموارد الشبكة التي تعرضت للخداع، وعناوين نظام أسماء النطاقات (DNS) وعناوين IP (IPv4 و IPv6) للمواقع الإلكترونية التي تمت زيارتها؛

- عناوين نظام أسماء النطاقات (DNS) وعناوين IP (IPv4 أو IPv6) الخاصة بمورد الويب المطلوب، ومعلومات حول الملف وعميل الويب الذي يتمتع بإمكانية الوصول إلى مورد الويب، والاسم، والحجم والمجاميع الاختبارية (MD5، SHA2-256، SHA1) للملف، والمسار الكامل المؤدي إلى الملف ورمز قالب المسار، ونتيجة فحص توقيعه الرقمي، وحالته في شبكة KSN؛

- معلومات حول التراجع عن إجراءات البرمجيات الضارة: بيانات حول الملف الذي تم التراجع عن أنشطته (اسم الملف، والمسار الكامل المؤدي إلى الملف، وحجم الملف والمجاميع الاختبارية (MD5، SHA2-256، SHA1)، وبيانات عن الإجراءات الناجحة وغير الناجحة لحذف وإعادة تسمية ونسخ الملفات واستعادة القيم في السجل (أسماء مفاتيح السجل وقيمها)، ومعلومات حول ملفات النظام المُعدّلة بواسطة البرمجيات الضارة، قبل وبعد التراجع؛

- معلومات حول الاستثناءات المعينة للمكون الخاص بالتحكم غير الطبيعي التكيفي: مُعرّف وحالة القاعدة التي تم تشغيلها، والإجراء الذي تم تنفيذه بواسطة البرنامج عند تشغيل القاعدة، ونوع حساب المستخدم الذي تقوم من خلاله العملية أو الترابط بإجراء نشاط مشكوك فيه، فضلاً عن معلومات حول العملية التي كان يتم تنفيذها أو عرضة لنشاط مشكوك فيه (مُعرّف البرنامج النصي أو اسم ملف العملية، والمسار الكامل المؤدي إلى ملف العملية، ورمز قالب المسار، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) الخاصة بملف العملية)؛ ومعلومات حول الكائن الذي قام بتنفيذ الإجراءات المشكوك فيها فضلاً عن معلومات حول الكائن الذي كان عرضة للإجراءات المشكوك فيها (اسم مفتاح سجل أو اسم ملف، والمسار الكامل المؤدي إلى الملف، ورمز قالب المسار، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) الخاصة بالملف)؛

- معلومات حول الوحدات النمطية للبرنامج التي تم تحميلها: الاسم والحجم والمجاميع الاختبارية (MD5، SHA2-256، SHA1) لملف الوحدة النمطية، والمسار الكامل المؤدي له ورمز قالب المسار، وإعدادات التوقيع الرقمي لملف الوحدة النمطية، وبيانات ووقت إنشاء التوقيع، واسم الموضوع والمؤسسة التي قامت بالتوقيع على ملف الوحدة النمطية، ومُعرّف العملية التي تم تحميل الوحدة النمطية فيها، واسم مورد الوحدة النمطية، والرقم التسلسلي للوحدة النمطية في قائمة انتظار التحميل؛

- معلومات حول جودة تفاعل البرنامج مع خدمات KSN: تاريخ ووقت البداية والنهاية للفترة الزمنية عند إنشاء الإحصائيات، ومعلومات حول جودة الطلبات والاتصال بكل خدمة من خدمات KSN المستخدمة (مُعرّف خدمة KSN)، وعدد الطلبات الناجحة، وعدد الطلبات التي تتضمن استجابات من التخزين المؤقت، وعدد الطلبات غير الناجحة (مشكلات الشبكة، وتعطيل KSN في إعدادات البرنامج، والتوجيه الخاطئ)، والفترة الزمنية للطلبات التي تجاوزت حد الوقت، وعدد الاتصالات بشبكة KSN المأخوذة من التخزين المؤقت، وعدد الاتصالات الناجحة بشبكة KSN، وعدد الاتصالات غير الناجحة بشبكة KSN، وعدد المعاملات الناجحة، وعدد المعاملات غير الناجحة، والفترة الزمنية للاتصالات الناجحة بشبكة KSN، والفترة الزمنية للاتصالات غير الناجحة بشبكة KSN، والفترة الزمنية للمعاملات الناجحة، والفترة الزمنية للمعاملات غير الناجحة)؛

- في حال اكتشاف كائن محتمل أن يكون ضارًا، فإنه يتم توفير معلومات حول البيانات الموجودة في ذاكرة العمليات: عناصر المستوى التدريجي لكائنات النظام (ObjectManager)، والبيانات الموجودة في ذاكرة UEFI BIOS، وأسماء مفاتيح السجل وقيمها؛

- معلومات حول الأحداث في سجلات الأنظمة: الطابع الزمني للحدث، واسم السجل الذي تم العثور على الحدث فيه، ونوع وفئة الحدث، واسم مصدر الحدث ووصف الحدث؛

- معلومات حول اتصالات الشبكة: الإصدار والمجاميع الاختبارية (MD5، SHA2-256، SHA1) لملف العملية الذي بدأت العملية منه والتي أدت إلى فتح المنفذ، والمسار المؤدي إلى ملف العملية وتوقيعه الرقمي، وعناوين IP المحلية والبعيدة، وعدد منافذ الاتصال المحلية والبعيدة، وحالة الاتصال، والطابع الزمني لفتح المنفذ؛

- معلومات حول تاريخ تثبيت البرنامج وتفعيله على الكمبيوتر: معرّف الشريك الذي باع الترخيص، والرقم التسلسلي للترخيص، والعنوان الموقّع للتذكرة من خدمة التفعيل (معرّف مركز التفعيل الإقليمي، و المجموع الاختباري لرمز التفعيل، والمجموع الاختباري للتذكرة، وتاريخ إنشاء التذكرة، والمعرف الفريد للتذكرة، وإصدار التذكرة، وحالة الترخيص، وتاريخ ووقت بدء / انتهاء التذكرة، والمعرف الفريد للترخيص، وإصدار الترخيص)، ومعرف الشهادة المستخدمة لتوقيع رأس التذكرة، والمجموع الاختباري (MD5) لملف المفتاح، والمعرف الفريد لتثبيت البرنامج على الكمبيوتر، ونوع ومعرف التطبيق الذي يتم تحديثه، ومعرف مهمة التحديث؛

- معلومات حول تعيين جميع التحديثات المثبتة، وتعيين معظم التحديثات التي تم تثبيتها/إزالتها مؤخرًا، ونوع الحدث الذي تسبب في إرسال معلومات التحديث، والمدة الزمنية منذ تثبيت آخر تحديث، ومعلومات حول أية قواعد بيانات مثبتة مؤخرًا لمكافحة الفيروسات؛

- معلومات حول تشغيل البرنامج على جهاز الكمبيوتر: بيانات عن استخدام وحدة المعالجة المركزية (CPU)، وبيانات عن استخدام الذاكرة (وحدات البايت الخاصة، والتجمّع غير المُرحّل، والتجمّع المُرحّل)، وعدد مؤشرات الترابط النشطة في عمليات البرنامج ومؤشرات الترابط المعلقة، والمدة الزمنية لتشغيل البرنامج قبل حدوث الخطأ؛

- عدد مرات تفريغ البرنامج وتفريغ النظام (BSOD) منذ تثبيت البرنامج ومنذ إجراء آخر تحديث، ومُعرّف وإصدار الوحدة النمطية للبرنامج التي حدث فيها الخلل، وتكديس الذاكرة في عمليات البرنامج، ومعلومات حول قواعد بيانات مكافحة الفيروسات في وقت حدوث العطل؛

- بيانات عن تفريغ النظام (BSOD): علامة تشير إلى حدوث حالة تفريغ للنظام (BSOD) على جهاز الكمبيوتر، واسم برنامج التشغيل الذي تسبب في حدوث حالة تفريغ للنظام (BSOD)، والعنوان وتكديس الذاكرة في برنامج التشغيل، وعلامة تشير إلى المدة الزمنية لجلسة نظام التشغيل (OS) قبل حدوث حالة تفريغ للنظام (BSOD)، وتكديس الذاكرة لبرنامج التشغيل الذي حدث الخلل به، ونوع تفريغ الذاكرة المحفوظ، وعلامة تشير إلى أن جلسة نظام التشغيل استمرت أكثر من 10 دقائق قبل حدوث تفريغ للنظام (BSOD)، والمُعرّف الفريد للتفريغ، والطابع الزمني لتفريغ النظام (BSOD)؛

- معلومات حول الأخطاء أو مشكلات الأداء التي حدثت أثناء تشغيل مكونات البرنامج: مُعرّف الحالة للبرنامج، ونوع الخطأ، والرمز والسبب فضلاً عن الوقت الذي حدث الخطأ فيه، ومُعرّفات المكون، والوحدة النمطية والعملية الخاصة بالمنتج التي حدث الخطأ فيها، ومُعرّف المهمة أو فئة التحديث أثناء حدوث الخطأ خلالها، وسجلات برامج التشغيل المستخدمة من جانب البرنامج (رمز الخطأ، واسم الوحدة النمطية، واسم ملف المصدر والسطر حيث حدث الخطأ)؛

- معلومات حول تحديثات قواعد بيانات مكافحة الفيروسات ومكونات البرنامج: الاسم، وتاريخ ووقت تنزيل ملفات الفهرس أثناء التحديث الأخير والتي يجري تنزيلها أثناء التحديث الحالي؛

- معلومات حول إنهاء تشغيل البرنامج بصورة غير طبيعية: الطابع الزمني لإنشاء التفريغ، ونوعه، ونوع الحدث الذي تسبب في إنهاء تشغيل البرنامج بصورة غير طبيعية (إيقاف التشغيل بصورة غير متوقعة (حدوث خلل في التطبيق الخارجي)، وتاريخ ووقت إيقاف التشغيل بصورة غير متوقعة؛

- معلومات حول مدى توافق برامج التشغيل الخاصة بالبرنامج مع الأجهزة والبرامج: معلومات حول خصائص نظام التشغيل (OS) التي تقوم بتقييد وظائف مكونات البرنامج (التمهيد الآمن، وعزل لائحة النواة (KPTI)، وفرض WHQL، و BitLocker، والتحسس لحالة الأحرف)، ونوع برنامج التنزيل المثبت (UEFI، BIOS)، ومُعرّف الوحدة النمطية للنظام الأساسي الموثوق به (TPM)، وإصدار مواصفات الوحدة النمطية للنظام الأساسي الموثوق به (TPM)، ومعلومات حول وحدة المعالجة المركزية (CPU) الموجودة داخل جهاز الكمبيوتر، ووضع التشغيل ومعلمات تكامل الرموز وحماية الجهاز، ووضع التشغيل الخاص ببرامج التشغيل وسبب استخدام الوضع الحالي، وإصدار برامج التشغيل الخاصة بالبرنامج، وحالة دعم الوضع الظاهري في البرامج والأجهزة الخاصة بجهاز الكمبيوتر؛

- معلومات حول التطبيقات الخارجية التي تسببت في حدوث الخطأ: أسمائها، والإصدار والترجمة، ورمز الخطأ والمعلومات حول الخطأ من سجل تطبيقات النظام، وعنوان الخطأ وتكديس الذاكرة للتطبيق الخارجي، وعلامة تشير إلى حدوث الخطأ في مكون البرنامج، ومقدار الوقت الذي عمل فيه التطبيق الخارجي قبل حدوث الخطأ، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) لصورة عملية التطبيق التي حدث فيها الخطأ، والمسار المؤدي إلى صورة عملية التطبيق ورمز قالب المسار، ومعلومات من سجل النظام تحمل وصفًا للخطأ المرتبط بالتطبيق، ومعلومات حول الوحدة النمطية للتطبيق التي حدث فيها الخطأ (مُعرّف الاستثناء، وعنوان ذاكرة العطل كإزاحة في الوحدة النمطية للتطبيق، واسم وإصدار الوحدة النمطية، ومُعرّف عطل التطبيق في المكون الإضافي للمالك وتكديس ذاكرة العطل، ومقدار الوقت الذي عمل فيه التطبيق قبل حدوث العطل)؛

- إصدار مكون أداة التحديث للبرنامج، وعدد الأعطال في مكون أداة التحديث أثناء تشغيل مهام التحديث على مدار العمر التشغيلي للمكون، ومُعرّف نوع مهمة التحديث، وعدد المحاولات الفاشلة لمكون أداة التحديث من أجل إكمال مهام التحديث؛

- معلومات حول تشغيل مكونات مراقبة نظام البرنامج: الإصدارات الكاملة للمكونات، والتاريخ والوقت عند بدء تشغيل المكونات، ورمز الحدث الذي تجاوز سعة قائمة انتظار الحدث وعدد مثل تلك الأحداث، والعدد الإجمالي لأحداث تجاوز سعة قائمة الانتظار، ومعلومات حول ملف العملية الخاصة بمنشئ الحدث (اسم الملف والمسار المؤدي له على جهاز الكمبيوتر، ورمز القالب لمسار الملف، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) للعملية المرتبطة بالملف، وإصدار الملف)، ومُعرّف اعتراض الحدث الذي حدث، والإصدار الكامل لعامل تصفية الاعتراض، ومُعرّف نوع الحدث الذي تم اعتراضه، وحجم قائمة الانتظار وعدد الأحداث المتواجدة ما بين الحدث الأول في قائمة الانتظار والحدث الحالي، وعدد الأحداث المتأخرة في قائمة الانتظار، ومعلومات حول ملف العملية الخاصة بمنشئ الحدث الحالي (اسم الملف والمسار المؤدي له على جهاز الكمبيوتر، ورمز القالب لمسار الملف، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) للعملية المرتبطة بالملف)، والمدة الزمنية لمعالجة الحدث، والحد الأقصى للمدة الزمنية المخصصة لمعالجة الحدث، واحتمالية إرسال الإحصاءات، ومعلومات حول أحداث نظام التشغيل التي تم تجاوز حد وقت المعالجة من أجلها (تاريخ ووقت الحدث، وعدد عمليات التهيئة المتكررة لقواعد بيانات مكافحة الفيروسات، وتاريخ ووقت عملية التهيئة الأخيرة المتكررة لقواعد بيانات مكافحة الفيروسات بعد تحديثها، ووقت تأخير معالجة الحدث لكل مكون لمراقبة النظام، وعدد الأحداث الموجودة في قائمة الانتظار، وعدد الأحداث التي تمت معالجتها، وعدد الأحداث المتأخرة للنوع الحالي، ووقت التأخير الإجمالي لجميع الأحداث)؛

- معلومات من أداة تعقب الأحداث لنظام Windows (خاصية تعقب الأحداث لنظام Windows، ETW) في حالة وجود مشكلات بأداء البرنامج، وموردي أحداث WinSATAssessment / SysConfigEx / SysConfig من Microsoft: معلومات حول جهاز الكمبيوتر (الطراز، والشركة المصنعة، وعامل النموذج للهيكل الداخلي، والإصدار)، ومعلومات حول مقاييس أداء Windows (تقييمات WinSAT ومؤشر أداء Windows)، واسم المجال، ومعلومات حول أجهزة المعالجة المادية والمنطقية (عدد أجهزة المعالجة المادية والمنطقية، والشركة المصنعة، والطراز، ومستوى التخطي، وعدد مراكز المعالجات، وتردد الساعة، ومُعرّف وحدة المعالجة المركزية (CPUID)، وخصائص ذاكرة التخزين المؤقتة، وخصائص جهاز المعالجة المنطقي، والمؤشرات للأوضاع المدعومة والإرشادات)، ومعلومات حول الوحدات النمطية لذاكرة التخزين العشوائي (النوع، وعامل النموذج، والشركة المصنعة، والطراز، والسعة، والتنفيذ المتكرر لتخصيص الذاكرة)، ومعلومات حول واجهات الشبكة (عناوين IP و MAC، والاسم، والوصف، وتكوين واجهات الشبكة، وتصنيف عدد وحجم حزم الشبكة بحسب النوع، وسرعة تبادل الشبكة، وتصنيف عدد أخطاء الشبكة بحسب النوع)، وتكوين وحدة تحكم IDE، وعناوين IP لخوادم نظام أسماء النطاقات (DNS)، ومعلومات حول بطاقة الفيديو (الاسم، والوصف، والشركة المصنعة، وإمكانية التوافق، وسعة ذاكرة الفيديو، والإذن للشاشة، وعدد وحدات البت لكل بكسل، وإصدار BIOS)، ومعلومات حول أجهزة التوصيل والتشغيل (الاسم، والوصف، ومُعرّف الجهاز [PnP، ACPI]، ومعلومات حول الأقراص وأجهزة التخزين (عدد الأقراص أو محركات الأقراص المحمولة، والشركة المصنعة، والطراز، وسعة القرص، وعدد الاسطوانات، وعدد المسارات لكل اسطوانة، وعدد المقاطع لكل مسار، وسعة المقطع، وخصائص التخزين المؤقت، والرقم التسلسلي، وعدد الأقسام، وتكوين وحدة التحكم SCSI)، ومعلومات حول الأقراص المنطقية (الرقم التسلسلي، وسعة القسم، وسعة وحدة التخزين، وحرف وحدة التخزين، ونوع القسم، ونوع نظام الملف، وعدد المجموعات، وحجم المجموعة، وعدد المقاطع لكل مجموعة، وعدد المجموعات الخالية والمشغولة، وحرف وحدة التخزين القابلة للتشغيل، وعنوان الإزاحة للقسم بما يتعلق بتشغيل القرص)، ومعلومات حول اللوحة الأم BIOS (الشركة المصنعة، وتاريخ الإطلاق، والإصدار)، ومعلومات حول اللوحة الأم (الشركة المصنعة، والطراز، والنوع)، ومعلومات حول الذاكرة المادية (السعة المشتركة والخالية)، ومعلومات حول خدمات نظام التشغيل (الاسم، والوصف، والحالة، والعلامة، والمعلومات حول العمليات [الاسم ومُعرّف العملية (PID)])، ومعلمات استهلاك الطاقة لجهاز الكمبيوتر، وتكوين وحدة تحكم المقاطعة، والمسار المؤدي إلى مجلدات نظام Windows (Windows و System32)، ومعلومات حول نظام التشغيل (الإصدار، والبناء، وتاريخ الإطلاق، والاسم، والنوع، وتاريخ التثبيت)، وحجم ملف ترحيل الصفحات، ومعلومات حول شاشات العرض (العدد، والشركة المصنعة، والإذن للشاشة، وسعة دقة العرض، والنوع)، ومعلومات حول برنامج التشغيل الخاص ببطاقة الفيديو (الشركة المصنعة، وتاريخ الإطلاق، والإصدار)؛

- معلومات من خاصية تعقب الأحداث في نظام Windows، وموردو أحداث EventTrace / EventMetadata من Microsoft: معلومات عن تسلسل أحداث النظام (النوع، والوقت، والتاريخ، والمنطقة الزمنية)، والبيانات الوصفية للملف مع نتائج التتبع (الاسم، والبنية، ومعلمات التتبع، وتصنيف عدد عمليات التتبع حسب النوع)، ومعلومات حول نظام التشغيل (الاسم، والنوع، والإصدار، والنسخة، وتاريخ الإصدار، ووقت بدء التشغيل)؛

- معلومات من خاصية تعقب الأحداث في نظام Windows، وموردي أحداث Microsoft Windows Kernel Process / Microsoft Windows Kernel Processor Power من Microsoft: معلومات حول العمليات التي تم بدء تشغيلها وإكمالها (الاسم، ومُعرّف العملية (PID)،

ومعلمات بدء التشغيل، وسطر الأوامر، ورمز الرجوع، ومعلمات إدارة الطاقة، ووقت بدء التشغيل والاكتمال، ونوع رمز الوصول المميز، و SID، ومُعرّف الجلسة، وعدد عناصر الوصف المثبتة)، ومعلومات حول التغييرات في أولويات مؤشر الترابط (مُعرّف مؤشر الترابط (TID)، والأولوية، والوقت)، ومعلومات حول عمليات تشغيل القرص الخاصة بالعملية (النوع، والوقت، والسعة، والعدد)، وسجل التغييرات في البنية والسعة لعمليات الذاكرة القابلة للاستخدام؛

- معلومات من خاصية تعقب الأحداث في نظام Windows (ETW)، وموردي أحداث StackWalk / Perfinfo من Microsoft: معلومات حول عدّادات الأداء (أداء مقاطع التعليمة البرمجية الفردية، وتسلسل استدعاءات الدالة، ومُعرّف العملية (PID)، ومُعرّف مؤشر الترابط (TID)، وعناوين وسمات روتينيات خدمة المقاطعة (ISR) واستدعاءات الإجراءات المؤجلة (DPC)؛

- معلومات من خاصية تعقب الأحداث في نظام Windows (ETW)، ومورد أحداث KernelTraceControl-ImageID من Microsoft: معلومات حول الملفات القابلة للتنفيذ والمكتبات الديناميكية (الاسم، وحجم الصورة، والمسار الكامل)، ومعلومات حول ملفات PDB (الاسم، والمُعرّف)، وبيانات مصدر VERSIONINFO للملفات القابلة للتنفيذ (الاسم، والوصف، والمنشئ، والموقع، وإصدار ومُعرّف التطبيق، وإصدار ومُعرّف الملف)؛

- معلومات من خاصية تعقب الأحداث في نظام Windows (ETW)، وموردي أحداث Windows Kernel Disk / Image / Disklo / Filelo من Microsoft: معلومات عن عمليات تشغيل الملف والقرص (النوع، والسعة، ووقت البدء، ووقت الاكتمال، والمدة الزمنية، وحالة الاكتمال، ومُعرّف العملية (PID)، ومُعرّف مؤشر الترابط (TID)، وعناوين استدعاء دالة برنامج التشغيل، وحزمة طلب I/O (IRP)، وسمات كائن ملف Windows)، معلومات حول الملفات المرتبطة بعمليات تشغيل الملف والقرص (الاسم، والإصدار، والحجم، والمسار الكامل، والسمات، والإزاحة، والمجموع الاختباري للصورة، وخيارات الفتح والوصول)؛

- معلومات من خاصية تعقب الأحداث في نظام Windows (ETW)، ومورد أحداث PageFault من Microsoft: معلومات عن أخطاء الوصول إلى صفحة الذاكرة (العنوان، والوقت، والسعة، ومُعرّف العملية (PID)، ومُعرّف مؤشر الترابط (TID)، وسمات كائن ملف Windows، ومعلمات تخصيص الذاكرة)؛

- معلومات من خاصية تعقب الأحداث في نظام Windows (ETW)، ومورد أحداث مؤشر الترابط Thread من Microsoft: معلومات عن إنشاء/اكتمال مؤشر الترابط، ومعلومات عن مؤشرات الترابط التي تم بدء تشغيلها (مُعرّف العملية (PID)، ومُعرّف مؤشر الترابط (TID)، وحجم التكديس، وأولويات وتخصيص موارد وحدة المعالجة المركزية (CPU)، وموارد I/O، وصفحات الذاكرة بين مؤشرات الترابط، وعنوان التكديس، وعنوان الدالة init، وعنوان حظر بيئة مؤشر الترابط (TEB)، وعلامة خدمة Windows)؛

- معلومات من خاصية تعقب الأحداث في نظام Windows، مورد أحداث ذاكرة Microsoft Windows Kernel Memory من Microsoft: معلومات حول عمليات إدارة الذاكرة (حالة الاكتمال، والوقت، والكمية، ومُعرّف العملية (PID))؛

- معلومات حول تشغيل البرنامج في حالة وجود مشكلات بالأداء: مُعرّف تثبيت البرنامج، ونوع وقيمة الانخفاض في الأداء، ومعلومات حول تسلسل الأحداث داخل البرنامج (الوقت، والمنطقة الزمنية، والنوع، وحالة الاكتمال، ومُعرّف مكون البرنامج، ومُعرّف سيناريو تشغيل البرنامج، ومُعرّف مؤشر الترابط (TID)، ومُعرّف العملية (PID)، وعناوين استدعاء الدالة)، ومعلومات حول اتصالات الشبكة المراد التحقق منها (URL، واتجاه الاتصال، وحجم حزمة الشبكة)، ومعلومات حول ملفات PDB (الاسم، والمُعرّف، وحجم الصورة للملف التنفيذي)، ومعلومات حول الملفات المراد التحقق منها (الاسم، والمسار الكامل، والمجموع الاختباري)، ومعلمات مراقبة أداء البرنامج؛

- معلومات حول آخر إعادة تشغيل غير ناجحة لنظام التشغيل: عدد مرات إعادة التشغيل غير الناجحة منذ تثبيت نظام التشغيل، وبيانات عن تفريغ النظام (رمز ومعلمات الخطأ، والاسم، والإصدار والمجموع الاختباري (CRC32) للوحدة النمطية التي تسببت في حدوث الخطأ في تشغيل نظام التشغيل، وعنوان الخطأ كإزاحة في الوحدة النمطية، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) لتفريغ النظام)؛

- معلومات للتحقق من صحة وأصالة الشهادات الرقمية التي يجري استخدامها لتوقيع الملفات: بصمة الشهادة، وخوارزمية المجموع الاختباري، والمفتاح العام والرقم المسلسل للشهادة، واسم جهة الإصدار للشهادة، ونتيجة التحقق من الشهادة ومُعرّف قاعدة بيانات الشهادة؛

- معلومات حول العملية التي شنت الهجوم على الدفاع الذاتي للبرنامج: اسم وحجم ملف العملية، والمجاميع الاختبارية (MD5، SHA2-256، SHA1) له، والمسار الكامل المؤدي إلى ملف العملية ورمز قالب مسار الملف، والطوابع الزمنية للإنشاء/البناء، وعلامة الملف التنفيذي، وسمات ملف العملية، ومعلومات حول الشهادة المستخدمة للتوقيع على ملف العملية، ورمز الحساب المستخدم لبدء تشغيل العملية، ومُعرّف العمليات التي تم تنفيذها للوصول إلى العملية، ونوع المورد الذي يتم تنفيذ العملية به (العملية، الملف، كائن السجل، نافذة البحث باستخدام الدالة FindWindow)، واسم المورد الذي يتم تنفيذ العملية به، وعلامة تشير إلى نجاح العملية، وحالة ملف العملية وتوقيعه وفقًا لشبكة KSN؛

- معلومات حول برنامج صاحب الحق: الإصدار الكامل، والنوع، والترجمة وحالة تشغيل البرنامج المستخدم، وإصدارات مكونات البرنامج المثبتة وحالة تشغيلها، ومعلومات حول تحديثات البرامج المثبتة، وقيمة عامل التصفية TARGET، وإصدار البروتوكول المستخدم للاتصال بخدمات صاحب الحق؛

- معلومات حول الأجهزة التي تم تركيبها على جهاز الكمبيوتر: النوع، والاسم، واسم الطراز، وإصدار البرنامج الثابت، ومعلمات الأجهزة المدمجة والمتصلة، والمُعرّف الفريد لجهاز الكمبيوتر مع البرنامج المثبت؛

- معلومات حول إصدارات نظام التشغيل والتحديثات المثبتة، وحجم الكلمات، وإصدار ومعلمات وضع التشغيل لنظام التشغيل، والإصدار والمجاميع الاختبارية (MD5، SHA2-256، SHA1) لملف نواة kernel لنظام التشغيل، وتاريخ ووقت بدء تشغيل نظام التشغيل؛

- الملفات القابلة للتنفيذ وغير القابلة للتنفيذ، كليًا أو جزئيًا؛
- أجزاء من ذاكرة الوصول العشوائي (RAM) للكمبيوتر؛
- القطاعات المشتركة في عملية إقلاع نظام التشغيل؛
- حزم بيانات مرور شبكة الاتصال؛
- صفحات الويب ورسائل البريد الإلكتروني التي تحتوي على مواد مشكوك فيها وخبيثة؛
- وصف الفئات وحالات فئات مستودع WMI؛
- تقارير نشاط التطبيقات:

- اسم الملف الذي يجري إرساله وحجمه وإصداره، ووصفه ومجاميعه الاختبارية (MD5، SHA2-256، SHA1)، ومعرف تنسيق الملف، واسم بائع الملف، واسم المنتج الذي ينتمي إليه الملف، والمسار الكامل إلى الملف الموجود على الكمبيوتر ، ورمز القالب للمسار، وإنشاء وتعديل الطوابع الزمنية للملف؛
- تاريخ ووقت بداية وانتهاء فترة صلاحية الشهادة (إذا كان للملف توقيع رقمي)، وتاريخ ووقت التوقيع، واسم جهة إصدار الشهادة، ومعلومات حول صاحب الشهادة، وبصمة الإصبع، وشهادة المفتاح العام والخوارزميات المناسبة، والرقم المسلسل للشهادة؛
- اسم الحساب الجاري تشغيل العملية منه؛
- المجاميع الاختيارية (MD5، SHA2-256، SHA1) لاسم الكمبيوتر الذي يتم تشغيل العملية عليه؛
- عناوين نوافذ العملية؛
- معرّف قواعد بيانات مكافحة الفيروسات، واسم التهديد المكتشف طبقًا لتصنيف مالك الحق؛
- بيانات حول الترخيص المثبّت، ومعرّفه ونوعه وتاريخ انتهاء صلاحيته؛
- التوقيت المحلي للكمبيوتر لحظة تقديم المعلومات؛
- أسماء ومسارات الملفات التي تم الوصول إليها من قبل العملية؛
- أسماء مفاتيح التسجيل والقيم الخاصة بها التي تم الوصول إليها من قبل العملية؛
- عنوان URL وعناوين IP التي تم الوصول إليها من قبل العملية؛
- عنوان URL وعناوين IP التي تم تنزيل الملف قيد التشغيل منها.

توفير البيانات عند استخدام حلول Detection and Response

على أجهزة الكمبيوتر المُثبت عليها Kaspersky Endpoint Security، يتم تخزين البيانات المعدة للإرسال التلقائي إلى Kaspersky Endpoint Detection and Response و Kaspersky Sandbox و Kaspersky Anti Targeted Attack Platform. يتم تخزين الملفات على أجهزة الكمبيوتر في شكل عادي غير مشفر.

تعتمد مجموعة البيانات المحددة على الحل الذي يُستخدم Kaspersky Endpoint Security من خلاله.

Kaspersky Endpoint Detection and Response

يتم حذف كل البيانات التي يخزنها التطبيق محليًا على الكمبيوتر من الكمبيوتر عند إلغاء تثبيت Kaspersky Endpoint Security.

البيانات المستلمة نتيجة لتنفيذ مهمة فحص IOC (مهمة قياسية)

يرسل Kaspersky Endpoint Security تلقائيًا البيانات المتعلقة بنتائج تنفيذ مهمة فحص IOC إلى Kaspersky Security Center.

قد تحتوي البيانات في نتائج تنفيذ مهمة فحص IOC على المعلومات التالية:

- عنوان IP من جدول ARP
- العنوان الفعلي من جدول ARP
- نوع سجل DNS واسمه
- عنوان IP للكمبيوتر المحمي
- العنوان الفعلي (عنوان MAC) للكمبيوتر المحمي
- المعرف في إدخال سجل الأحداث
- اسم مصدر البيانات في السجل
- اسم السجل
- وقت الحدث
- تجزئات MD5 وSHA256 للملف
- الاسم الكامل للملف (بما في ذلك المسار)
- حجم الملف
- عنوان ومنفذ IP البعيد الذي تم إنشاء الاتصال به أثناء الفحص
- عنوان IP للمحول المحلي
- المنفذ المفتوح على المحول المحلي
- البروتوكول كرقم (وفقًا لمعيار IANA)
- اسم العملية
- وسائط العملية
- المسار إلى ملف العملية
- معرف Windows (PID) للعملية
- معرف Windows (PID) للعملية الأصل
- حساب المستخدم الذي بدأ العملية
- تاريخ ووقت بدء العملية

- اسم الخدمة
- وصف الخدمة
- مسار واسم خدمة DLL (لأجل svchost)
- مسار واسم ملف الخدمة القابل للتنفيذ
- معرف Windows (PID) للخدمة
- نوع الخدمة (على سبيل المثال، برنامج تشغيل أو محول نواة)
- حالة الخدمة
- وضع بدء تشغيل الخدمة
- اسم حساب المستخدم
- اسم المجلد
- حرف وحدة التخزين
- نوع وحدة التخزين
- ملفات تسجيل Windows
- قيمة خلية التسجيل
- مسار مفتاح التسجيل (بدون اسم الخلية والقيمة)
- إعداد التسجيل
- النظام (البيئة)
- اسم وإصدار نظام التشغيل المُثبت على الكمبيوتر
- اسم الشبكة للكمبيوتر المحمي
- المجال أو المجموعة التي ينتمي إليها الكمبيوتر المحمي
- اسم المستعرض
- إصدار المستعرض
- وقت الوصول إلى مورد الويب آخر مرة
- عنوان موقع الويب من طلب HTTP
- اسم الحساب المُستخدَم لطلب HTTP
- اسم ملف العملية التي قدمت طلب HTTP
- المسار الكامل لملف العملية التي قدمت طلب HTTP
- معرف Windows (PID) للعملية التي قدمت طلب HTTP

- مُحيل HTTP (عنوان موقع الويب لمصدر طلب HTTP)
- URI المورد المطلوب عبر HTTP
- معلومات عن عامل مستخدم HTTP (التطبيق الذي قدم طلب HTTP)
- وقت تنفيذ طلب HTTP
- المعرّف الفريد للعملية التي قدمت طلب HTTP

بيانات لإنشاء سلسلة تطور التهديد

يتم تخزين البيانات الخاصة بإنشاء سلسلة تطور التهديد بشكل افتراضي لمدة سبعة أيام. ويتم إرسال البيانات تلقائيًا إلى Kaspersky Security Center.

قد تحتوي البيانات الخاصة بإنشاء سلسلة تطور التهديد على المعلومات التالية:

- تاريخ ووقت الحادث
- اسم الاكتشاف
- وضع الفحص
- حالة الإجراء الأخير المتعلق بالاكتشاف
- سبب فشل معالجة الاكتشاف
- نوع الكائن المكتشف
- اسم الكائن المكتشف
- حالة التهديد بعد معالجة الكائن
- سبب فشل تنفيذ الإجراءات على الكائن
- الإجراءات التي تم تنفيذها للتراجع عن الإجراءات الضارة
- معلومات عن الكائن الذي تمت معالجته:
  - المعرّف الفريد للعملية
  - المعرّف الفريد للعملية الأصل
  - المعرّف الفريد لملف العملية
  - معرف عملية Windows (PID)
  - سطر أوامر العملية
  - حساب المستخدم الذي بدأ العملية
  - رمز جلسة تسجيل الدخول التي تعمل فيها العملية
  - نوع الجلسة التي تعمل فيها العملية
  - مستوى نزاهة العملية التي تتم معالجتها

- عضوية حساب المستخدم الذي بدأ العملية في المجموعات المحلية ومجموعات المجال ذات الامتيازات
- معرف الكائن الذي تتم معالجته
- الاسم الكامل للكائن الذي تتم معالجته
- معرّف الجهاز المحمي
- الاسم الكامل للكائن (اسم الملف المحلي أو عنوان الويب للملف الذي تم تنزيله)
- تجزئة MD5 أو SHA256 للكائن الذي تمت معالجته
- نوع الكائن الذي تم معالجته
- تاريخ إنشاء الكائن الذي تتم معالجته
- تاريخ إجراء آخر تعديل للكائن الذي تتم معالجته
- حجم الكائن الذي تتم معالجته
- سمات الكائن الذي تتم معالجته
- المؤسسة التي وقعت على الكائن الذي تتم معالجته
- نتيجة التحقق من الشهادة الرقمية للكائن الذي تتم معالجته
- معرّف الأمان (SID) للكائن الذي تتم معالجته
- معرف المنطقة الزمنية للكائن الذي تتم معالجته
- عنوان الويب لتنزيل الكائن الذي تتم معالجته (فقط للملفات الموجودة على القرص)
- اسم التطبيق الذي قام بتنزيل الملف
- تجزئات MD5 وSHA256 للتطبيق الذي قام بتنزيل الملف
- اسم التطبيق الذي قام بتعديل الملف آخر مرة
- تجزئات MD5 وSHA256 للتطبيق الذي قام بتعديل الملف آخر مرة
- عدد مرات بدء تشغيل الكائن الذي تتم معالجته
- تاريخ ووقت بدء تشغيل الكائن الذي تتم معالجته لأول مرة
- المعرفات الفريدة للملف
- الاسم الكامل للملف (اسم الملف المحلي أو عنوان الويب للملف الذي تم تنزيله)
- المسار إلى متغير تسجيل Windows الذي تتم معالجته
- اسم متغير تسجيل Windows الذي تتم معالجته
- قيمة متغير تسجيل Windows الذي تتم معالجته
- نوع متغير تسجيل Windows الذي تتم معالجته

- مؤشر عضوية مفتاح التسجيل الذي تتم معالجته في نقطة التشغيل التلقائي
- عنوان الويب لطلب الويب الذي تتم معالجته
- مصدر الارتباط لطلب الويب الذي تتم معالجته
- عامل المستخدم لطلب الويب الذي تتم معالجته
- نوع طلب الويب الذي تتم معالجته (GET أو POST).
- منفذ IP المحلي لطلب الويب الذي تتم معالجته
- منفذ IP البعيد لطلب الويب الذي تتم معالجته
- اتجاه الاتصال (وارد أو صادر) لطلب الويب الذي تتم معالجته
- معرّف العملية التي تم تضمين التعليمات البرمجية الضارة فيها

Kaspersky Sandbox

يتم حذف كل البيانات التي يخزنها التطبيق محليًا على الكمبيوتر من الكمبيوتر عند إلغاء تثبيت Kaspersky Endpoint Security.

بيانات الخدمة

يخزن Kaspersky Endpoint Security البيانات التالية التي تمت معالجتها أثناء الاستجابة التلقائية:

- الملفات والبيانات التي يجري معالجتها التي أدخلها المستخدم أثناء تكوين العامل المدمج في Kaspersky Endpoint Security:
  - الملفات المعزولة
  - المفتاح العام للشهادة المُستخدم للتكامل مع Kaspersky Sandbox
- ذاكرة التخزين المؤقت للعامل المدمج في Kaspersky Endpoint Security:
  - وقت كتابة نتائج الفحص في ذاكرة التخزين المؤقت
  - تجزئة MD5 لمهمة الفحص
  - معرف مهمة الفحص
  - نتيجة فحص الكائن
- قائمة انتظار طلبات فحص الكائن:
  - معرف الكائن في قائمة الانتظار
  - وقت وضع الكائن في قائمة الانتظار
  - حالة معالجة الكائن في قائمة الانتظار

- معرّف جلسة المستخدم في نظام التشغيل حيث تم إنشاء مهمة فحص الكائن
- معرّف النظام (SID) لمستخدم نظام التشغيل الذي تم استخدام حسابه لإنشاء المهمة
- تجزئة MD5 لمهمة فحص الكائن

- معلومات عن المهام التي ينتظر العامل المدمج في Kaspersky Endpoint Security نتائج فحصها من Kaspersky Sandbox:
  - وقت استلام مهمة فحص الكائن
  - حالة معالجة الكائن
  - معرّف جلسة المستخدم في نظام التشغيل حيث تم إنشاء مهمة فحص الكائن
  - معرّف مهمة فحص الكائن
  - تجزئة MD5 لمهمة فحص الكائن
  - معرّف النظام (SID) لمستخدم نظام التشغيل الذي تم استخدام حسابه لإنشاء المهمة
  - مخطط XML لمؤشر الاختراق الذي تم إنشاؤه تلقائيًا
  - تجزئة MD5 أو SHA256 للكائن الذي خضع للفحص
  - أخطاء المعالجة
  - أسماء الكائنات التي تم إنشاء المهمة لها
  - نتيجة فحص الكائن

البيانات الواردة في طلبات Kaspersky Sandbox

يتم تخزين البيانات التالية من الطلبات من العامل المدمج لحل Kaspersky Endpoint Security إلى Kaspersky Sandbox محليًا على الكمبيوتر:

- تجزئة MD5 لمهمة الفحص
- معرف مهمة الفحص
- الكائن الذي تم فحصه وجميع الملفات ذات الصلة

البيانات المستلمة نتيجة لتنفيذ مهمة فحص IOC (مهمة قائمة بذاتها)

يرسل Kaspersky Endpoint Security تلقائيًا البيانات المتعلقة بنتائج تنفيذ مهمة فحص IOC إلى Kaspersky Security Center.

قد تحتوي البيانات في نتائج تنفيذ مهمة فحص IOC على المعلومات التالية:

- عنوان IP من جدول ARP
- العنوان الفعلي من جدول ARP
- نوع سجل DNS واسمه
- عنوان IP للكمبيوتر المحمي

- العنوان الفعلي (عنوان MAC) للكمبيوتر المحمي
- المعرف في إدخال سجل الأحداث
- اسم مصدر البيانات في السجل
- اسم السجل
- وقت الحدث
- تجزئات MD5 وSHA256 للملف
- الاسم الكامل للملف (بما في ذلك المسار)
- حجم الملف
- عنوان ومنفذ IP البعيد الذي تم إنشاء الاتصال به أثناء الفحص
- عنوان IP للمحول المحلي
- المنفذ المفتوح على المحول المحلي
- البروتوكول كرقم (وفقًا لمعيار IANA)
- اسم العملية
- وسائط العملية
- المسار إلى ملف العملية
- معرف Windows (PID) للعملية
- معرف Windows (PID) للعملية الأصل
- حساب المستخدم الذي بدأ العملية
- تاريخ ووقت بدء العملية
- اسم الخدمة
- وصف الخدمة
- مسار واسم خدمة DLL (لأجل svchost)
- مسار واسم ملف الخدمة القابل للتنفيذ
- معرف Windows (PID) للخدمة
- نوع الخدمة (على سبيل المثال، برنامج تشغيل أو محول نواة)
- حالة الخدمة
- وضع بدء تشغيل الخدمة
- اسم حساب المستخدم

- اسم المجلد
- حرف وحدة التخزين
- نوع وحدة التخزين
- ملفات تسجيل Windows
- قيمة خلية التسجيل
- مسار مفتاح التسجيل (بدون اسم الخلية والقيمة)
- إعداد التسجيل
- النظام (البيئة)
- اسم وإصدار نظام التشغيل المُثبت على الكمبيوتر
- اسم الشبكة للكمبيوتر المحمي
- المجال أو المجموعة التي ينتمي إليها الكمبيوتر المحمي
- اسم المستعرض
- إصدار المستعرض
- وقت الوصول إلى مورد الويب آخر مرة
- عنوان موقع الويب من طلب HTTP
- اسم الحساب المُستخدَم لطلب HTTP
- اسم ملف العملية التي قدمت طلب HTTP
- المسار الكامل لملف العملية التي قدمت طلب HTTP
- معرف Windows (PID) للعملية التي قدمت طلب HTTP
- مُحيل HTTP (عنوان موقع الويب لمصدر طلب HTTP)
- URI المورد المطلوب عبر HTTP
- معلومات عن عامل مستخدم HTTP (التطبيق الذي قدم طلب HTTP)
- وقت تنفيذ طلب HTTP
- المعرّف الفريد للعملية التي قدمت طلب HTTP

(Kaspersky Anti Targeted Attack Platform (EDR

يتم حذف كل البيانات التي يخزنها التطبيق محليًا على الكمبيوتر من الكمبيوتر عند إلغاء تثبيت Kaspersky Endpoint Security.

بيانات الخدمة

يُخزن العامل المدمج في Kaspersky Endpoint Security البيانات التالية محليًا:

- الملفات والبيانات التي يجري معالجتها التي أدخلها المستخدم أثناء تكوين العامل المدمج في Kaspersky Endpoint Security:
  - الملفات المعزولة
  - إعدادات العامل المدمج في Kaspersky Endpoint Security:
    - المفتاح العام للشهادة المستخدمة للتكامل مع Central Node
    - بيانات الترخيص
- البيانات المطلوبة للتكامل مع Central Node:
  - قائمة انتظار حزمة حدث القياس عن بُعد
  - ذاكرة التخزين المؤقت لمعرفات ملف مؤشر الاختراق المستلمة من Central Node
  - الكائنات التي سيتم تمريرها إلى الخادم خلال مهمة الحصول على الملف
  - تقارير نتائج مهمة الحصول على التحقيق الجنائي

البيانات في الطلبات المقدمة إلى KATA (EDR)

عند الدمج مع Kaspersky Anti Targeted Attack Platform، يتم تخزين البيانات التالية محليًا على الكمبيوتر:

البيانات من العامل المدمج لطلبات Kaspersky Endpoint Security إلى مكون Central Node:

- في طلبات المزامنة:
  - المعرف الفريد
  - الجزء الأساسي من عنوان ويب الخادم
  - اسم الكمبيوتر
  - عنوان IP الكمبيوتر
  - عنوان MAC الكمبيوتر
  - التوقيت المحلي على الكمبيوتر
  - حالة الدفاع الذاتي في Kaspersky Endpoint Security
  - اسم وإصدار نظام التشغيل المُثبت على الكمبيوتر
  - إصدار Kaspersky Endpoint Security
  - إصدارات إعدادات التطبيق وإعدادات المهمة
  - حالات المهمة: معرفات المهام وحالات التنفيذ ورموز الخطأ

- في طلبات الحصول على الملفات من الخادم:
  - المعرفات الفريدة للملفات
  - معرّف Kaspersky Endpoint Security الفريد
  - المعرفات الفريدة للشهادات
  - الجزء الأساسي من عنوان ويب الخادم المُثبت عليه مكون Central Node
  - عنوان IP المضيف
- في تقارير نتائج تنفيذ المهمة:
  - عنوان IP المضيف
  - معلومات عن الكائنات التي تم اكتشافها أثناء فحص مؤشر الاختراق أو فحص YARA
  - علامات الإجراءات الإضافية التي يتم تنفيذها عند الانتهاء من المهام
  - أخطاء تنفيذ المهام ورموز الإرجاع
  - حالات إكمال المهمة
  - وقت إكمال المهمة
  - إصدارات الإعدادات المستخدمة لتنفيذ المهام
  - معلومات عن الكائنات المرسلة إلى الخادم والكائنات المعزولة والكائنات المستعادة من العزل: المسارات إلى الكائنات وتجزئات MD5 وSHA256 ومعرفات الكائنات المعزولة
  - معلومات عن العمليات التي بدأت أو توقفت على جهاز كمبيوتر بناءً على طلب الخادم: PID وUniquePID ورمز الخطأ وتجزئات MD5 وSHA256 للكائنات
  - معلومات غن الخدمات التي تم تشغيلها أو إيقافها على جهاز كمبيوتر بناءً على طلب الخادم: اسم الخدمة ونوع بدء التشغيل ورمز الخطأ وتجزئة MD5 وSHA256 لصور ملفات الخدمات
  - معلومات عن الكائنات التي تم إجراء تفريغ ذاكرة لأجلها لفحص YARA (المسارات، معرف ملف التفريغ)
  - الملفات المطلوبة من قبل الخادم
  - حزم القياس عن بعد
  - بيانات عن العمليات قيد التشغيل:
    - اسم الملف القابل للتنفيذ، بما في ذلك المسار الكامل والملحق
    - معلمات التشغيل التلقائي للعملية
    - معرف العملية
    - معرف جلسة تسجيل الدخول
    - اسم جلسة تسجيل الدخول
    - تاريخ ووقت بدء العملية

- تجزئات MD5 وSHA256 للكائن

- البيانات الموجودة في الملفات:
  - مسار الملف
  - اسم الملف
  - حجم الملف
  - سمات الملف
  - تاريخ ووقت إنشاء الملف
  - تاريخ ووقت آخر تعديل للملف
  - وصف الملف
  - اسم الشركة
  - تجزئات MD5 وSHA256 للكائن
  - مفتاح التسجيل (لنقاط التشغيل التلقائي)
- البيانات في الأخطاء التي تحدث عند استرداد معلومات عن الكائنات:
  - الاسم الكامل للكائن الذي تمت معالجته عند حدوث خطأ
  - رمز الخطأ
- بيانات القياس عن بعد:
  - عنوان IP المضيف
  - نوع البيانات في التسجيل قبل عملية التحديث الملتزم بها
  - البيانات الموجودة في مفتاح التسجيل قبل عملية التغيير الملتزم بها
  - نص البرنامج النصي الذي تمت معالجته أو جزء منه
  - نوع الكائن الذي تم معالجته
  - طريقة تمرير أمر إلى مترجم الأوامر

البيانات من طلبات مكون Central Node إلى العامل المدمج في Kaspersky Endpoint Security:

- إعدادات المهمة:
  - نوع المهمة
  - إعدادات جدولة المهمة
  - أسماء وكلمات مرور الحسابات التي يمكن تشغيل المهام تحتها
  - إصدارات الإعدادات

- معرفات الكائنات المعزولة
- المسارات إلى الكائنات
- تجزئات MD5 وSHA256 للكائنات
- سطر الأوامر لبدء العملية باستخدام الوسيطات
- علامات الإجراءات الإضافية التي يتم تنفيذها عند الانتهاء من المهام
- معرفات ملف مؤشر الاختراق التي سيتم استردادها من الخادم
- ملفات IOC
- اسم الخدمة
- نوع بدء تشغيل الخدمة
- المجلدات التي يجب استلام نتائج مهمة الحصول على التحقيق الجنائي لها
- أقنعة أسماء الكائنات وملحقاتها لمهمة الحصول على التحقيق الجنائي

- إعدادات عزل شبكة الاتصال:
  - أنواع الإعدادات
  - إصدارات الإعدادات
  - قوائم استثناءات عزل شبكة الاتصالات وإعدادات الاستثناء: اتجاه حركة المرور وعناوين IP والمنافذ والبروتوكولات والمسارات الكاملة إلى الملفات القابلة للتنفيذ
  - علامات الإجراءات الإضافية
  - وقت تعطيل العزل التلقائي
- إعدادات منع التنفيذ
  - أنواع الإعدادات
  - إصدارات الإعدادات
  - قوائم قواعد منع التنفيذ وإعدادات القواعد: المسارات إلى الكائنات وأنواع الكائنات وتجزئة MD5 وSHA256 للكائنات
  - علامات الإجراءات الإضافية
- إعدادات تصفية الأحداث:
  - أسماء الوحدات النمطية
  - المسارات الكاملة إلى الكائنات
  - تجزئات MD5 وSHA256 للكائنات
  - معرفات الإدخالات في سجل أحداث Windows
  - إعدادات الشهادة الرقمية

- اتجاه حركة المرور وعناوين IP والمنافذ والبروتوكولات والمسارات الكاملة إلى الملفات القابلة للتنفيذ
- أسماء المستخدمين
- أنواع تسجيل دخول المستخدم
- أنواع أحداث القياس عن بُعد التي يتم تطبيق عوامل التصفية عليها

البيانات في نتائج فحص YARA

ينقل العامل المدمج في Kaspersky Endpoint Security نتائج فحص YARA تلقائيًا إلى Kaspersky Anti Targeted Attack Platform لبناء سلسلة تطور التهديدات.

يتم تخزين البيانات مؤقتًا محليًا في قائمة الانتظار لإرسال نتائج تنفيذ المهمة إلى خادم Kaspersky Anti Targeted Attack Platform. ويتم حذف البيانات من التخزين المؤقت بمجرد إرسالها.

تحتوي نتائج فحص YARA على البيانات التالية:

- تجزئات MD5 وSHA256 للملف
- الاسم الكامل للملف
- مسار الملف
- حجم الملف
- اسم العملية
- وسائط العملية
- المسار إلى ملف العملية
- معرف Windows (PID) للعملية
- معرف Windows (PID) للعملية الأصل
- حساب المستخدم الذي بدأ العملية
- تاريخ ووقت بدء العملية

الامتثال لتشريعات الاتحاد الأوروبي (GDPR)

قد يرسل Kaspersky Endpoint Security البيانات إلى Kaspersky في ظل السيناريوهات التالية:

- استخدام Kaspersky Security Network.
- تفعيل التطبيق برمز تفعيل.
- تحديث الوحدة النمطية للتطبيق' وقواعد بيانات مكافحة الفيروسات.
- اتباع الروابط في واجهة التطبيق.

- تفريغ الكتابة.

بصرف النظر عن تصنيف البيانات والمنطقة التي يتم تلقي البيانات منها، تلتزم Kaspersky بمعايير عالية لأمن البيانات وتستخدم العديد من الإجراءات القانونية والتنظيمية والفنية لحماية بيانات المستخدمين، ولضمان أمن البيانات وسريتها، وكذلك لضمان الوفاء بحقوق المستخدمين على النحو الذي يضمنه التشريع المعمول به. تم تضمين نص سياسة الخصوصية في مجموعة توزيع التطبيق وهو متاح على موقع ويب Kaspersky.

قبل استخدام Kaspersky Endpoint Security، يُرجى قراءة وصف البيانات المرسلة بعناية في اتفاقية ترخيص المستخدم النهائي وبيان Kaspersky Security Network. إذا كانت البيانات المحددة المرسلة من Kaspersky Endpoint Security بموجب أي من السيناريوهات الموصوفة يمكن تصنيفها كبيانات شخصية وفقًا لتشريعاتك أو معاييرك المحلية، فيجب عليك التأكد من معالجة هذه البيانات بشكل قانوني والحصول على موافقة المستخدمين النهائيين لجمع ونقل مثل هذه البيانات.

اقرأ اتفاقية ترخيص المستخدم النهائي وتفضل بزيارة موقع ويب Kaspersky لمعرفة المزيد حول كيفية تلقي المعلومات المتعلقة باستخدام التطبيق ومعالجتها وتخزينها وتدميرها بعد قبول اتفاقية ترخيص المستخدم النهائي والموافقة على بيان Kaspersky Security Network. يحتوي ملفا license.txt وksn_<language ID>.txt على نص اتفاقية ترخيص المستخدم النهائي وبيان Kaspersky Security Network التي تتضمنها حزمة التوزيع.

إذا كنت لا ترغب في إرسال البيانات إلى Kaspersky، فيمكنك تعطيل توفير البيانات.

استخدام Kaspersky Security Network

باستخدام Kaspersky Security Network، فإنك توافق على تقديم البيانات المدرجة في بيان Kaspersky Security Network تلقائيًا. إذا كنت لا توافق على تقديم هذه البيانات إلى Kaspersky، استخدم Kaspersky Private Security Network (KPSN) أو قم بتعطيل استخدام KSN. للمزيد من التفاصيل عن شبكة KPSN، يُرجى الرجوع إلى الوثائق الموجودة على شبكة Kaspersky Private Security Network.

تفعيل التطبيق برمز تفعيل

باستخدام رمز التفعيل، فإنك توافق على تقديم البيانات المدرجة في اتفاقية ترخيص المستخدم النهائي تلقائيًا. إذا كنت لا توافق على توفير هذه البيانات إلى Kaspersky، فاستخدم ملف مفتاح لتفعيل Kaspersky Endpoint Security.

تحديث الوحدة النمطية للتطبيق' وقواعد بيانات مكافحة الفيروسات

باستخدام خوادم Kaspersky، فإنك توافق على تقديم البيانات المدرجة في اتفاقية ترخيص المستخدم النهائي تلقائيًا. يتطلب Kaspersky هذه المعلومات للتحقق من استخدام Kaspersky Endpoint Security بشكل قانوني. إذا كنت لا توافق على تقديم هذه المعلومات إلى Kaspersky، فاستخدم Kaspersky Security Center لتحديثات قاعدة البيانات أو أداة Kaspersky Update Utility.

اتباع الروابط في واجهة التطبيق

باستخدام الروابط الموجودة في واجهة التطبيق، فإنك توافق على تقديم البيانات المدرجة في اتفاقية ترخيص المستخدم النهائي تلقائيًا. تعتمد القائمة الدقيقة للبيانات المرسلة في كل رابط محدد على مكان الرابط في واجهة التطبيق والمشكلة التي يهدف إلى حلها. إذا كنت لا توافق على تقديم هذه البيانات إلى Kaspersky، فاستخدم واجهة التطبيق المبسطة أو قم بإخفاء واجهة التطبيق.

تفريغ الكتابة

إذا قمت بتمكين كتابة التفريغ، فسيقوم Kaspersky Endpoint Security بإنشاء ملف تفريغ يحتوي على جميع بيانات الذاكرة من عمليات التطبيق في وقت إنشاء ملف التفريغ هذا.

بدء الاستخدام

بعد تثبيت Kaspersky Endpoint Security، يمكنك إدارة التطبيق باستخدام الواجهات التالية:

- واجهة التطبيق المحلية.
- Kaspersky Security Center Administration Console.
- Kaspersky Security Center Web Console.
- Kaspersky Security Center Cloud Console.

Kaspersky Security Center Administration Console

يتيح لك Kaspersky Security Center تثبيت Kaspersky Endpoint Security وإلغاء تثبيته وإيقافه، وتكوين إعدادات التطبيق وتغيير مجموعة مكونات التطبيق المتاحة وإضافة مفاتيح وبدء وإيقاف التحديث وفحص المهام.

يمكن إدارة التطبيق بواسطة Kaspersky Security Center باستخدام مكون الإدارة الإضافي لبرنامج Kaspersky Endpoint Security.

للحصول على المزيد من التفاصيل حول إدارة التطبيق من خلال Kaspersky Security Center، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

Kaspersky Security Center Web Console وKaspersky Security Center Cloud Console

Kaspersky Security Center Web Console (ويشار إليه فيما بعد باسم "Web Console") هو تطبيق على الويب صمم خصيصًا لأداء المهام الرئيسية لإدارة وصيانة النظام الأمني لشبكة المؤسسة. Web Console هو أحد مكونات Kaspersky Security Center والذي يوفر واجهة مستخدم. للحصول على معلومات تفصيلية حولKaspersky Security Center Web Console، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

إن Kaspersky Security Center Cloud Console (المشار إليها فيما يلي باسم "Cloud Console") عبارة عن حل يستند إلى السحابة لحماية شبكة تابعة لمؤسسة ما وإدارتها. للحصول على معلومات تفصيلية حول Kaspersky Security Center Cloud Console، يُرجى الرجوع إلى دليل التعليمات الخاص بـ Kaspersky Security Center Cloud Console.

تتيح لك وحدتي التحكم Web Console وCloud Console إجراء ما يلي:

- مراقبة الحالة الخاصة بالنظام الأمني للمنظمة التابعة لك.
- تثبيت التطبيقات الخاصة بـ Kaspersky على الأجهزة الموجودة في الشبكة الخاصة بك.
- إدارة التطبيقات المثبتة.
- عرض التقارير عن حالة النظام الأمني.

إن إدارة Kaspersky Endpoint Security من خلال وحدة التحكم Web Console، ووحدة التحكم Cloud Console، ووحدة التحكم الخاصة بإدارة Kaspersky Security Center تتيح بكل وحدات التحكم تلك إمكانيات مختلفة للإدارة. وتتنوع أيضًا المكونات والمهام المتاحة باختلاف وحدات التحكم.

نبذة عن المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows

إن المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows يقوم بتفعيل التفاعل بين Kaspersky Endpoint Security وKaspersky Security Center. يتيح لك المكون الإضافي للإدارة التحكم في إدارة برنامج Kaspersky Endpoint security باستخدام السياسات والمهام وإعدادات التطبيق المحلية. التفاعل بين Kaspersky Security Center Web Console متوفر عن طريق مكون الويب.

قد يختلف إصدار مكون الإدارة الإضافي عن إصدار تطبيق Kaspersky Endpoint Security المثبت على كمبيوتر العميل. إذا كان الإصدار المثبت لمكون الإدارة الإضافي يتمتع بوظائف أقل من الإصدار المثبت لبرنامج Kaspersky Endpoint Security، فإنه لا يتم تنظيم إعدادات الوظائف المفقودة بواسطة مكون الإدارة الإضافي. ويمكن تعديل هذه الإعدادات بواسطة المستخدم في واجهة Kaspersky Endpoint Security المحلية.

لم يتم تثبيت المكون الإضافي للويب بشكل افتراضي على Kaspersky Security Center Web Console. على عكس المكوّن الإضافي للإدارة الخاص بـ Kaspersky Security Center Administration Console، الذي تم تثبيته على محطة عمل المسؤول، يجب تثبيت المكون الإضافي للويب على جهاز كمبيوتر مثبت عليه Kaspersky Security Center Web Console. إن وظيفة المكون الإضافي للويب متوفرة لجميع المسؤولين الذين لديهم إمكانية الوصول إلى Web Console في مستعرض. يمكنك عرض قائمة المكونات الإضافية للويب المثبتة في واجهة Web Console: **Console settings** ← **Web plug-ins**. لمزيد من التفاصيل حول توافق إصدارات المكون الإضافي للويب و Web Console، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

تثبيت المكون الإضافي للويب

يمكنك تثبيت المكون الإضافي للويب على النحو التالي:

- قم بتثبيت المكون الإضافي للويب باستخدام معالج البدء السريع لتطبيق Kaspersky Security Center Web Console.

  يطالبك Web Console تلقائيًا ببدء تشغيل معالج البدء السريع عند توصيل Web Console بخادم الإدارة للمرة الأولى. تستطيع أيضا بدء تشغيل معالج البدء السريع في واجهة Web Console (**Discovery & Deployment** ← **Deployment & Assignment** ← **Quick Start Wizard**). كما يمكن لمعالج البدء السريع التحقق مما إذا كانت المكونات الإضافية للويب المثبتة محدثة و تنزيل التحديثات الضرورية. وللمزيد من التفاصيل حول معالج البدء السريع لتطبيق Kaspersky Security Center Web Console، يُرجي الرجوع إلى تعليمات Kaspersky Security Center.

- قم بتثبيت المكون الإضافي للويب من قائمة حزم التوزيع المتاحة في Web Console.

  لتثبيت المكون الإضافي للويب، حدد حزمة التوزيع للمكون الإضافي للويب لتطبيق Kaspersky Endpoint Security في واجهة Web Console: **Web plug-ins** ← **Console settings**. يتم تحديث قائمة حزم التوزيع المتوفرة تلقائيًا بعد تنزيل إصدارات جديدة من تطبيقات Kaspersky.

- قم بتنزيل حزمة التوزيع إلى Web Console من مصدر خارجي.

  لتثبيت المكوّن الإضافي للويب، قم بإضافة أرشيف ZIP لحزمة التوزيع المخصصة للمكوّن الإضافي للويب الخاص بـ Kaspersky Endpoint Security في واجهة Web Console: **Web plug-ins** ← **Console settings**. يمكن تنزيل حزمة توزيع المكون الإضافي على موقع Kaspersky على سبيل المثال.

تحديث المكون الإضافي للإدارة

لتحديث المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows، قم بتنزيل آخر إصدار من المكون (الموجود في حزمة التوزيع) ثم قم بتشغيل معالج تثبيت المكون.

إذا أصبح إصدار جديد من المكون الإضافي للويب متاحًا، ستقوم بـWeb Console عرض الإخطار التحديثات متاحة للمكونات الإضافية المستخدمة. يمكنك المتابعة لتحديث إصدار المكون الإضافي للويب من إخطار Web Console هذا. وكذلك يمكنك التحقق يدويًا من وجود تحديثات جديدة للمكون الإضافي للويب في واجهة Web Console (**Web plug-ins** ← **Console settings**). ستتم إزالة الإصدار السابق من المكون الإضافي للويب تلقائيًا في أثناء عملية التحديث.

عند تحديث المكون الإضافي للويب، يتم حفظ المكونات الموجودة بالفعل (مثل السياسات أو المهام). ستظهر الإعدادات الجديدة الخاصة بالمكونات التي تنفذ وظائف برنامج Kaspersky Endpoint Security الجديدة في المكونات الموجودة، وسيكون لها قيم افتراضية.

يمكنك تحديث المكون الإضافي للويب على النحو التالي:

- قم بتحديث المكون الإضافي للويب في قائمة المكونات الإضافية للويب في وضع على الاتصال بالإنترنت.

  لتحديث المكون الإضافي للويب، يجب عليك القيام بتحديد حزمة التوزيع للمكون الإضافي للويب الخاص بـ Kaspersky Endpoint Security في واجهة Web Console: **Web plug-ins** ← **Console settings**). تتحقق Web Console من التحديثات المتوفرة على خوادم Kaspersky وتقوم بتنزيل التحديثات ذات الصلة.

- تحديث المكون الإضافي للويب من ملف.

لتحديث المكوّن الإضافي للويب، يجب عليك تحديد أرشيف ZIP لحزمة التوزيع المخصصة للمكوّن الإضافي للويب الخاص بتطبيق Kaspersky Endpoint Security في واجهة Web Console: **Web plug-ins** ← **Console settings**. يمكن تنزيل حزمة توزيع المكون الإضافي على موقع Kaspersky على سبيل المثال. يمكنك تحديث المكون الإضافي للويب الخاص ببرنامج Kaspersky Endpoint Security في واحد أو أكثر من الإصدارات الأخيرة. يتعذر تحديث المكون الإضافي للويب لإصدار أقدم.

في حالة فتح أي مكون (مثل السياسة أو المهمة)، يقوم المكون الإضافي للويب بالتحقق من معلومات التوافق الخاصة به. إذا كان إصدار المكون الإضافي للويب مساويًا أو أحدث من الإصدار المحدد في معلومات التوافق، فيمكنك تغيير إعدادات هذا المكون. بخلاف ذلك، لا يمكنك استخدام المكون الإضافي للويب لتغيير إعدادات المكون المحدد. يُوصى بترقية المكون الإضافي للويب.

اعتبارات خاصة عند العمل مع إصدارات مختلفة لمكونات الإدارة الإضافية

لا يمكنك إدارة Kaspersky Endpoint Security عبر Kaspersky Security Center إلا إذا كان لديك مكون إضافي للإدارة يكون إصداره مساويًا للإصدار المحدد في المعلومات المتعلقة بتوافق Kaspersky Endpoint Security مع المكون الإضافي للإدارة أو أحدث منه. ويمكنك الاطلاع على الإصدار الأدنى المطلوب من المكون الإضافي للإدارة في ملف installer.ini المضمن في مجموعة التوزيع.

في حالة فتح أي عنصر (مثل فتح سياسة أو مهمة)، يقوم مكون الإدارة الإضافي بالتحقق من معلومات التوافق الخاصة به. إذا كان إصدار مكون الإدارة الإضافي مساويًا أو أحدث من الإصدار المحدد في معلومات التوافق، فيمكنك تغيير إعدادات هذا المكون. بخلاف ذلك، لا يمكنك استخدام مكون الإدارة الإضافي لتغيير إعدادات العنصر المحدد. يُوصى بترقية مكون الإدارة الإضافي.

إذا كان المكون الإضافي لإدارة Kaspersky Endpoint Security مثبتًا في وحدة تحكم الإدارة، يُرجى تذكر ما يلي عند تثبيت إصدار جديد من المكون الإضافي للإدارة:

- سيتم إزالة الإصدار السابق من المكون الإضافي لإدارة Kaspersky Endpoint Security.
- يدعم الإصدار الجديد للمكون الإضافي لإدارة Kaspersky Endpoint Security إدارة الإصدار السابق من برنامج Kaspersky Endpoint Security for Windows على أجهزة المستخدمين.
- يمكنك استخدام الإصدار الجديد للمكون الإضافي للإدارة للقيام بتغيير الإعدادات في السياسات والمهام والعناصر الأخرى التي تم إنشاؤها بواسطة الإصدار السابق من المكون الإضافي للإدارة.
- للإعدادات الجديدة، يقوم الإصدار الجديد من المكون الإضافي للإدارة بتعيين القيم الافتراضية عند حفظ سياسة، أو ملف تعريف سياسة، أو مهمة للمرة الأولى.

بعد ترقية المكون الإضافي للإدارة، يوصى بالتحقق من قيم الإعدادات الجديدة الموجودة في السياسات وملفات تعريف السياسات وحفظها. إذا لم تقم بذلك، فستقوم المجموعات الجديدة من إعدادات برنامج Kaspersky Endpoint Security الموجودة على كمبيوتر المستخدم باتخاذ القيم الافتراضية ويمكن تعديلها (السمة). يوصى بالتحقق من الإعدادات بدايةً من السياسات وملفات تعريف السياسات في أعلى مستوى للتسلسل الهرمي. وكذلك يوصى باستخدام حساب المستخدم الذي يمتلك حقوق الوصول إلى جميع المجالات الوظيفية لبرنامج Kaspersky Security Center.

للتعرف على الإمكانيات الجديدة للتطبيق، يُرجى الرجوع إلى ملاحظات الإصدار أو تعليمات التطبيق.

- إذا تمت إضافة معلمة جديدة إلى مجموعة الإعدادات في الإصدار الجديد للمكون الإضافي للإدارة، فلن يتم تغيير حالة السمة / المحددة مسبقًا لهذه المجموعة من الإعدادات.

اعتبارات خاصة عند استخدام البروتوكولات المشفرة للتفاعل مع الخدمات الخارجية

يستخدم Kaspersky Endpoint Security وKaspersky Security Center قناة اتصال مشفرة مع TLS (أمن طبقة النقل) للعمل مع الخدمات الخارجية من Kaspersky. يستخدم Kaspersky Endpoint Security خدمات خارجية للوظائف التالية:

- تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق؛
- تفعيل التطبيق برمز التفعيل (التفعيل 2.0)؛
- استخدام Kaspersky Security Network.

يؤدي استخدام TLS إلى تأمين التطبيق من خلال توفير الميزات التالية:

- التشفير. تكون محتويات الرسائل سرية ولا يتم الكشف عنها لمستخدمي الجهات الخارجية.
- السلامة. يتأكد مستلم الرسالة أن محتويات الرسالة لم يتم تعديلها منذ إعادة توجيه الرسالة بواسطة المرسل.
- المصادقة. يكون المستلم على يقين من أن الاتصال لا يتم إلا من خلال خادم Kaspersky موثوق.

يستخدم Kaspersky Endpoint Security شهادات المفاتيح العامة لمصادقة الخادم. مطلوب بنية تحتية للمفتاح العام (PKI) للعمل مع الشهادات. تكون جهة إصدار الشهادات الموثوقة جزءًا من PKI. تستخدم Kaspersky جهة إصدار الشهادات الموثوقة الخاصة بها لأن خدمات Kaspersky تقنية للغاية وليست عامة. وفي هذه الحالة، عندما يتم إبطال شهادات الجذر من Thawte وVerisign وGlobaltrust وغيرها، يظل Kaspersky PKI صالحًا للعمل دون انقطاع.

يعتبر Kaspersky Endpoint Security البيئات التي تحتوي على MITM (أدوات البرامج والأجهزة التي تدعم تحليل بروتوكول HTTPS) غير آمنة. قد تحدث أخطاء عند العمل مع خدمات Kaspersky. على سبيل المثال، قد توجد أخطاء تتعلق باستخدام الشهادات الموقعة ذاتيًا. وقد تحدث هذه الأخطاء لأن أداة فحص HTTPS من بيئتك لا تتعرف على Kaspersky PKI. ولتصحيح هذه المشاكل، يجب عليك تكوين استثناءات للتفاعل مع الخدمات الخارجية.

واجهة التطبيق

نافذة التطبيق الرئيسية

المراقبة	• **التقارير**. يمكنك عرض الأحداث التي حدثت أثناء تشغيل التطبيق، والمكونات الفردية والمهام.

	• **نسخ احتياطي**. يمكنك عرض قائمة بالنسخ المحفوظة من الملفات المصابة التي حذفها التطبيق. • **تقنيات اكتشاف التهديدات**. يمكنك عرض معلومات حول تقنيات اكتشاف التهديدات وعدد التهديدات التي تم اكتشافها بواسطة هذه التقنيات. • **Kaspersky Security Network**. حالة الاتصال بين Kaspersky Endpoint Security وKaspersky Security Network وإحصائيات KSN العالمية. تعتبر شبكة Kaspersky Security Network (KSN) بنية تحتية من الخدمات السحابية التي توفر الوصول إلى قاعدة معارف Kaspersky على الإنترنت والتي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج. ويعد استخدام البيانات من Kaspersky Security Network ضمانًا لسرعة وقت استجابات Kaspersky Endpoint Security عند مواجهة تهديدات جديدة، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية ويقلل من خطر وقوع الحالات الإيجابية الزائفة. إذا كنت تشارك في شبكة Kaspersky Security Network، فإن خدمات شبكة KSN تقوم بتزويد برنامج Kaspersky Endpoint Security بمعلومات حول فئة وسمعة الملفات التي تم فحصها، بالإضافة إلى معلومات حول سمعة عناوين الويب التي تم فحصها. • **مراقبة نشاط التطبيقات**. يمكنك عرض معلومات حول تشغيل التطبيقات المثبتة. ويتتبع مراقب النظام أحداث الملف والتسجيل ونظام التشغيل المتعلقة بتطبيق. • **مراقبة شبكة الاتصال**. يمكنك عرض معلومات عن نشاط الشبكة الخاصة بالكمبيوتر في الوقت الحقيقي. • **مراقبة التشفير**. يراقب عملية تشفير القرص أو فك تشفيره في الوقت الحقيقي. يتوفر مكون مراقبة التشفير في حالة تثبيت مكون تشفير القرص من Kaspersky Disk أو مكون تشفير محرك الأقراص من BitLocker.
الأمان	حالة تشغيل المكونات المثبتة. ويمكنك أيضًا المتابعة لتكوين المكونات أو عرض التقارير.
تحديث	يمكنك إدارة مهام تحديث Kaspersky Endpoint Security. ويمكنك تحديث قواعد البيانات والوحدات النمطية للتطبيق لمكافحة الفيروسات والتراجع عن التحديث الأخير. ويستطيع المسؤول إخفاء القسم عن المستخدم أو تقييد إدارة المهام.
المهام	يمكنك إدارة مهام الفحص لتطبيق Kaspersky Endpoint Security. يمكنك إجراء فحص البرامج الضارة والتحقق من سلامة التطبيق. يستطيع المسؤول إخفاء المهام عن مستخدم أو تقييد إدارة المهام.
الترخيص	ترخيص التطبيق. يمكنك شراء ترخيص أو تفعيل التطبيق أو تجديد اشتراك. يمكنك أيضًا عرض معلومات حول الترخيص الحالي.
	تكوين إعدادات التطبيق. يستطيع المسؤول منع إجراء تغييرات على الإعدادات في Kaspersky Security Center.
	معلومات حول التطبيق: الإصدار الحالي من Kaspersky Endpoint Security، وتاريخ إصدار قاعدة البيانات والمفتاح ومعلومات أخرى. ويمكنك أيضًا المتابعة إلى موارد معلومات Kaspersky التي توفر معلومات مفيدة وتوصيات وإجابات للأسئلة المتداولة حول كيفية شراء التطبيق وتثبيته واستخدامه.
	الرسائل التي تحتوي على معلومات حول التحديثات المتوفرة وطلبات الوصول إلى الملفات والأجهزة المشفرة.

رمز التطبيق في منطقة إخطار شريط المهام

بعد تثبيت برنامج Kaspersky Endpoint Security مباشرة، سيظهر رمز التطبيق في منطقة إخطار شريط مهام Microsoft Windows.

يخدم الرمز الأغراض التالية:

- يشير إلى نشاط التطبيق.
- يعمل كاختصار في القائمة السياقية ونافذة التطبيق الرئيسية.

يتم توفير حالات رمز التطبيق التالية لعرض معلومات حول تشغيل التطبيق:

- يحدد الرمز أنه تم تمكين مكونات حماية التطبيق المهمة للغاية. سيعرض Kaspersky Endpoint Security تحذيرًا إذا كان يجب على المستخدم أن يتخذ إجراءً، مثل إعادة تشغيل الكمبيوتر بعد تحديث التطبيق.

- يحدد الرمز أن مكونات حماية التطبيق المهمة للغاية إما معطلة أو بها خطأ. قد لا تعمل مكونات الحماية لعدة أسباب، مثل بسبب انتهاء الترخيص أو نتيجة وجود خطأ في التطبيق. Kaspersky Endpoint Security سوف يعرض تحذيرًا بوصف المشكلة في حماية الكمبيوتر.

تحتوي قائمة السياق لرمز التطبيق على العناصر التالية:

- **Kaspersky Endpoint Security for Windows**. يفتح نافذة التطبيق الرئيسية. في هذه النافذة، يمكنك ضبط تشغيل مكونات ومهام التطبيق، وعرض إحصائيات الملفات التي تمت معالجتها والتهديدات المكتشفة.

- **إيقاف الحماية مؤقتًا / استئناف الحماية**. قم بإيقاف التشغيل مؤقتًا لجميع مكونات الحماية والمراقبة التي لم يتم وضع علامة قفل () عليها في السياسة. قبل تنفيذ هذه العملية، يُوصى بتعطيل سياسة Kaspersky Security Center.

  قبل إيقاف التشغيل المؤقت لمكونات الحماية والمراقبة، يطلب التطبيق كلمة المرور الخاصة بالوصول إلى برنامج Kaspersky Endpoint Security (كلمة المرور الخاصة بالحساب أو كلمة مرور مؤقتة). يمكنك بعد ذلك تحديد فترة الإيقاف المؤقت: لمدة محددة من الوقت، أو حتى إعادة التشغيل، أو بناءً على طلب المستخدم.

  يتوفر عنصر قائمة السياق هذا إذا تم تمكين الحماية بكلمة المرور. ولاستئناف تشغيل مكونات الحماية والمراقبة، حدد **استئناف الحماية** في قائمة السياق الخاصة بالتطبيق.

> لا يؤثر إيقاف التشغيل المؤقت لمكونات الحماية والمراقبة على أداء مهام التحديث وفحص البرامج الضارة. يستمر التطبيق في استخدام Kaspersky Security Network.

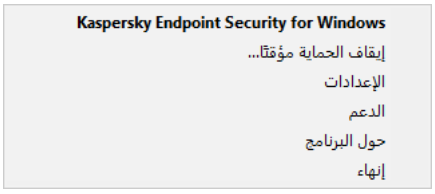
- **تعطيل السياسة / تمكين السياسة**. تعطيل سياسة Kaspersky Security Center على جهاز الكمبيوتر. تتوافر جميع إعدادات برنامج Kaspersky Endpoint Security للتكوين، بما في ذلك الإعدادات التي تحتوي على قفل مغلق في السياسة. (). علاوةً على ذلك، إذا كانت السياسة معطلة، فإن التطبيق يطلب كلمة المرور للوصول إلى Kaspersky Endpoint Security (كلمة المرور الخاصة بالحساب أو كلمة مرور مؤقتة). يتوفر عنصر قائمة السياق هذا إذا تم تمكين الحماية بكلمة المرور. لتمكين السياسة، حدد **تمكين السياسة** في قائمة السياق الخاصة بالتطبيق.

- **الإعدادات**. يفتح نافذة إعدادات التطبيق.

- **الدعم**. يفتح هذا نافذة تحتوي على المعلومات اللازمة للاتصال بالدعم الفني من Kaspersky.

- **حول البرنامج**. يفتح هذا العنصر نافذة معلومات تشتمل على تفاصيل التطبيق.

- **إنهاء**. يقوم هذا العنصر بإنهاء Kaspersky Endpoint Security. ويؤدي النقر فوق عنصر قائمة السياق هذه لإلغاء تحميل التطبيق من ذاكرة الوصول العشوائي (RAM) للكمبيوتر.



قائمة سياق رمز التطبيق

واجهة التطبيق المبسطة

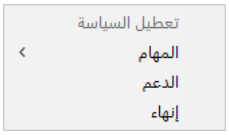
في حالة تكوين سياسة Kaspersky Security Center على عرض الواجهة المبسطة على كمبيوتر عميل مثبت عليه Kaspersky Endpoint Security، لا تتوافر نافذة التطبيق الرئيسية على هذا الكمبيوتر العميل. انقر بزر الماوس الأيمن لفتح قائمة سياق رمز Kaspersky Endpoint Security (انظر الشكل أدناه) التي تحتوي على العناصر التالية:

- **تعطيل السياسة / تمكين السياسة**. تعطيل سياسة Kaspersky Security Center على جهاز الكمبيوتر. تتوافر جميع إعدادات برنامج Kaspersky Endpoint Security للتكوين، بما في ذلك الإعدادات التي تحتوي على قفل مغلق في السياسة. (). علاوةً على ذلك، إذا كانت السياسة معطلة، فإن التطبيق يطلب كلمة المرور للوصول إلى Kaspersky Endpoint Security (كلمة المرور الخاصة بالحساب أو كلمة مرور مؤقتة). يتوفر عنصر قائمة السياق هذا إذا تم تمكين الحماية بكلمة المرور. لتمكين السياسة، حدد **تمكين السياسة** في قائمة السياق الخاصة بالتطبيق.

- **المهام**. القائمة المنسدلة التي تحتوي على العناصر التالية:

- **التحقق من السلامة**.
- **إعادة قواعد البيانات إلى إصدارها السابق**.
- **فحص كامل**.
- **فحص مخصص**.
- **فحص المناطق الحرجة**.
- **تحديث**.

- **الدعم**. يفتح هذا نافذة تحتوي على المعلومات اللازمة للاتصال بالدعم الفني من Kaspersky.
- **إنهاء**. يقوم هذا العنصر بإنهاء Kaspersky Endpoint Security. ويؤدي النقر فوق عنصر قائمة السياق هذه لإلغاء تحميل التطبيق من ذاكرة الوصول العشوائي (RAM) للكمبيوتر.



قائمة سياق رمز التطبيق عند عرض الواجهة المبسطة

تكوين عرض واجهة التطبيق

يمكنك تكوين وضع شاشة واجهة التطبيق لمستخدم. ويمكن لهذا المستخدم عندها التفاعل مع التطبيق بالطرق التالية:

- **عرض واجهة التطبيق المبسطة**. على جهاز كمبيوتر عميل، لا يمكن الوصول إلى نافذة التطبيق الرئيسية، وتكون الأيقونة الموجودة في منطقة إخطار Windows فقط متاحة. في قائمة السياق الخاصة بالرمز، يُمكن للمستخدم تنفيذ عدد محدود من العمليات مع برنامج Kaspersky Endpoint Security. يعرض أيضًا برنامج Kaspersky Endpoint Security إخطارات فوق رمز التطبيق.

- **عرض واجهة المستخدم**. على جهاز كمبيوتر عميل، النافذة الرئيسية لبرنامج Kaspersky Endpoint Security و الرمز الموجود في منطقة إخطار Windows يكونوا متاحين. في قائمة السياق الخاصة بالرمز، يُمكن للمستخدم تنفيذ العمليات مع برنامج Kaspersky Endpoint Security. يعرض أيضًا برنامج Kaspersky Endpoint Security إخطارات فوق رمز التطبيق.

- **عدم العرض**. على جهاز كمبيوتر عميل، لا يتم عرض أي علامات لعملية تشغيل برنامج Kaspersky Endpoint Security. الرمز الموجود في منطقة إخطار Windows والإخطارات غير متاحين.

كيفية تكوين وضع شاشة واجهة التطبيق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الواجهة**.

5. في القسم **التفاعل مع المستخدم**، نفذ أحد الإجراءات التالية:

- حدد خانة الاختيار **عرض واجهة المستخدم** إذا كنت تريد عرض عناصر الواجهة التالية على الكمبيوتر العميل:
  - مجلد يحتوي على اسم التطبيق في قائمة **ابدأ**
  - رمز Kaspersky Endpoint Security في منطقة إخطار شريط مهام Microsoft Windows
  - الإخطارات المنبثقة

  في حالة تحديد خانة الاختيار هذه، يستطيع المستخدم أن يعرض، حسب الحقوق المتاحة، ويغير إعدادات التطبيق من واجهة التطبيق.
- قم بإلغاء تحديد خانة الاختيار **عرض واجهة المستخدم** إذا كنت تريد إخفاء كل علامات Kaspersky Endpoint Security على الكمبيوتر العميل.

6. في القسم **التفاعل مع المستخدم**، حدد خانة الاختيار **عرض واجهة التطبيق المبسطة** إذا كنت تريد عرض simplified application interface على كمبيوتر عميل مُثبت عليه Kaspersky Endpoint Security.

كيفية تكوين وضع شاشة واجهة التطبيق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Interface**.

5. في القسم **Interaction with user**، قم بتكوين كيفية عرض واجهة التطبيق:

- **With simplified interface**. على جهاز كمبيوتر عميل، لا يمكن الوصول إلى نافذة التطبيق الرئيسية، وتكون الأيقونة الموجودة في منطقة إخطار Windows فقط متاحة. في قائمة السياق الخاصة بالرمز، يُمكن للمستخدم تنفيذ عدد محدود من العمليات مع برنامج Kaspersky Endpoint Security. يعرض أيضًا برنامج Kaspersky Endpoint Security إخطارات فوق رمز التطبيق.
- **With full interface**. على جهاز كمبيوتر عميل، النافذة الرئيسية لبرنامج Kaspersky Endpoint Security و الرمز الموجود في منطقة إخطار Windows يكونوا متاحين. في قائمة السياق الخاصة بالرمز، يُمكن للمستخدم تنفيذ العمليات مع برنامج Kaspersky Endpoint Security. يعرض أيضًا برنامج Kaspersky Endpoint Security إخطارات فوق رمز التطبيق.
- **No interface**. على جهاز كمبيوتر عميل، لا يتم عرض أي علامات لعملية تشغيل برنامج Kaspersky Endpoint Security. الرمز الموجود في منطقة إخطار Windows والإخطارات غير متاحين.

6. احفظ تغييراتك.

بدء الاستخدام

بعد نشر التطبيق على أجهزة الكمبيوتر العميلة، للعمل مع برنامج Kaspersky Endpoint Security من Kaspersky Security Center Web Console ستحتاج إلى تنفيذ الإجراءات التالية:

- قم بإنشاء السياسة وتكوينها.

  يمكنك استخدام السياسات لتطبيق إعدادات Kaspersky Endpoint Security المطابقة على جميع أجهزة الكمبيوتر العميلة داخل إحدى مجموعات الإدارة. يقوم معالج البدء السريع لتطبيق Kaspersky Security Center تلقائيًا بإنشاء سياسة لبرنامج Kaspersky Endpoint Security.

- إنشاء مهام تحديث وفحص البرامج الضارة.

  مهمة تحديثمطلوبة للحفاظ على أمان جهاز الكمبيوتر محدثًا. عند إجراء المهمة يقوم برنامج Kaspersky Endpoint Security بتحديث قواعد بيانات مكافحة الفيروسات والوحدات النمطية الخاصة بالتطبيق. يتم إنشاء مهمة تحديث تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

  مهمة فحص البرامج الضارة مطلوبة للكشف المناسب عن الفيروسات والبرمجيات الضارة الأخرى في الوقت المناسب. تحتاج إلى إنشاء المهمة فحص البرامج الضارة يدويًا.

كيفية إنشاء مهمة فحص البرامج الضارة في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (12.1)** ← **فحص البرامج الضارة**.

الخطوة الثانية: نطاق الفحص

قم بإنشاء قائمة الكائنات التي سيقوم Kaspersky Endpoint Security بفحصها أثناء تنفيذ مهمة الفحص.

الخطوة الثالثة: إجراء Kaspersky Endpoint Security

اختر الإجراء المطلوب اتخاذه عند اكتشاف تهديد:

- **تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات.
- **تنظيف؛ إبلاغ إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا تعذر التنظيف، يضيف Kaspersky Endpoint Security معلومات حول الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة.
- **إعلام**. في حالة تحديد هذا الخيار، يضيف Kaspersky Endpoint Security المعلومات حول الملفات المصابة إلى قائمة التهديدات النشطة عند اكتشاف هذه الملفات.
- **تشغيل التنظيف المتقدم على الفور**. في حال تحديد خانة الاختيار، سيستخدم Kaspersky Endpoint Security تقنية التنظيف المتقدم لمعالجة التهديدات النشطة أثناء الفحص.

  تقنية التنظيف المتقدمة تهدف إلى تطهير نظام التشغيل من التطبيقات الضارة التي بدأت بالفعل عملياتها في ذاكرة الوصول العشوائي والتي تمنع Kaspersky Endpoint Security من إزالتها باستخدام طرق أخرى. يتم إبطال التهديد كنتيجة. أثناء تقدم إجراء التنظيف المتقدم، ننصحك بعدم بدء أي عمليات جديدة أو تحرير تسجيل نظام التشغيل. تستخدم تقنية التنظيف المتقدمة موارد نظام التشغيل بدرجة كبيرة، وهو ما يبطئ من التطبيقات الأخرى. بعد اكتمال التنظيف المتقدم، سيقوم Kaspersky Endpoint Security بإعادة تشغيل الكمبيوتر دون مطالبة المستخدم بتأكيد ذلك.

قم بتكوين وضع تشغيل المهمة باستخدام **Run only when the computer is idle**. تؤدي خانة الاختيار هذه إلى تمكين/تعطيل وظيفة فحص البرامج الضارة عندما تكون موارد الكمبيوتر محدودة. يوقف Kaspersky Endpoint Security مهمة فحص البرامج الضارة مؤقتًا في حالة إيقاف تشغيل حافظة الشاشة وإلغاء قفل الكمبيوتر.

الخطوة الرابعة: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.

- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الخامسة: اختيار الحساب لتشغيل المهمة

حدد حسابًا لتشغيل مهمة فحص البرامج الضارة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي. إذا كان نطاق الفحص يشمل محركات الشبكة أو كائنات أخرى ذات وصول محظور، يجب تحديد حساب مستخدم له صلاحيات وصول كافية.

الخطوة السادسة: تكوين جدول بدء المهمة

قم بتكوين جدول لبدء المهمة، مثل يدويًا أو بعد تنزيل قواعد بيانات مكافحة الفيروسات على المستودع.

الخطوة السابعة: تحديد اسم المهمة

أدخل اسم المهمة، مثل فحص كامل يومي.

الخطوة 8 إكمال إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة. ونتيجة لذلك، سيتم تنفيذ مهمة فحص البرامج الضارة على أجهزة كمبيوتر المستخدم وفقًا للجدول المحدد.

كيفية إنشاء مهمة فحص البرامج الضارة في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.
تفتح قائمة المهام.

2. انقر على الزر **Add**.
يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type** حدد **Malware Scan**.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا علي سبيل المثال الفحص أسبوعيًا.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.

5. أغلق المعالج.
سيتم عرض مهمة جديدة في قائمة المهام.

6. لتكوين جدول المهام انتقل إلى خصائص المهمة.
من المستحسن أن تكون جدولة المهمة للتشغيل مرة واحدة على الأقل في الأسبوع.

7. حدد خانة الاختيار المجاورة للمهمة.

8. انقر على الزر **Run**.
يمكنك مراقبة حالة المهمة وعدد الأجهزة التي تم استكمال المهمة عليها بنجاح أو اكتمل تنفيذها مع وجود خطأ.

ونتيجة لذلك، سيتم تنفيذ مهمة فحص البرامج الضارة على أجهزة كمبيوتر المستخدم وفقًا للجدول المحدد.

إدارة السياسات

السياسة هي مجموعة من إعدادات التطبيق التي يتم تعريفها لمجموعة الإدارة. يمكنك تكوين سياسات متعددة مع قيم مختلفة لتطبيق واحد. يمكن تشغيل تطبيق تحت إعدادات مختلفة لمجموعات مختلفة من الإدارة. يمكن أن تحتوي كل مجموعة إدارة على سياستها الخاصة بالتطبيق.

يتم إرسال إعدادات السياسة إلى أجهزة الكمبيوتر العميلة عن طريق عميل الشبكة أثناء المزامنة. يقوم خادم الإدارة بإجراء المزامنة فورًا بشكل تلقائي بعد أن يتم تغيير إعدادات السياسة. يُستخدم منفذ UDP 15000 الموجود في كمبيوتر العميل لإجراء المزامنة. يقوم خادم الإدارة بإجراء المزامنة كل 15 دقيقة بشكل افتراضي. إذا فشلت المزامنة بعد تغيير إعدادات السياسة، فسيتم إجراء محاولة المزامنة التالية وفقًا للجدول الذي تم تكوينه.

السياسة النشطة وغير النشطة

السياسة مخصصة لمجموعة من أجهزة الكمبيوتر المدارة والتي يمكن أن تكون نشطة وغير نشطة. يتم حفظ الإعدادات الخاصة بالسياسة النشطة على أجهزة الكمبيوتر العميلة أثناء المزامنة. لا يمكنك تطبيق نُهج متعددة في وقت واحد على جهاز كمبيوتر واحد وبالتالي قد يكون هناك سياسة واحدة فقط نشطة في كل مجموعة.

يمكنك إنشاء عدد غير محدود من السياسات غير النشطة. لا تؤثر السياسة غير النشطة على إعدادات التطبيق الخاصة بأجهزة الكمبيوتر في الشبكة. الهدف من السياسات غير النشطة هو الاستعدادات لحالات الطوارئ مثل هجوم الفيروس. إذا كان هناك هجومًا عبر محركات الأقراص المحمولة، فيمكنك تفعيل السياسة التي تمنع الوصول إلى محركات الأقراص المحمولة. في هذه الحالة تصبح السياسة النشطة غير نشطة تلقائيًا.

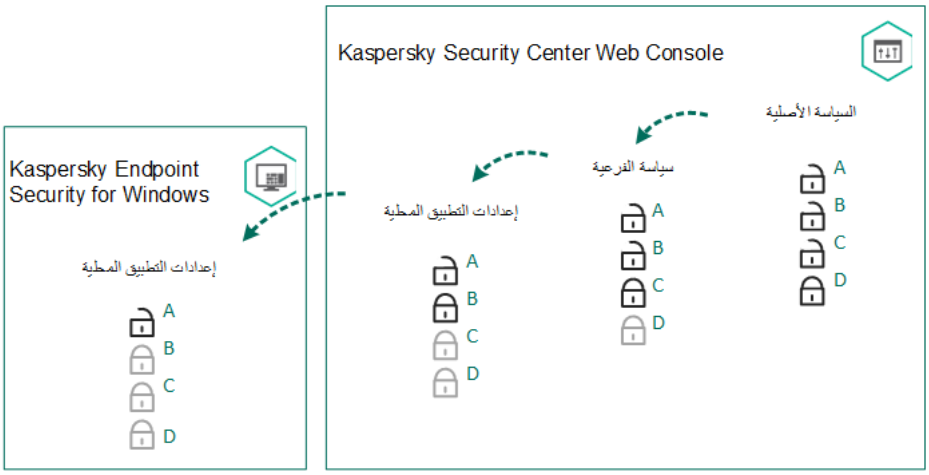
سياسة الوجود خارج المكتب

يتم تفعيل سياسة الوجود خارج المكتب عندما يترك الكمبيوتر شبكة المؤسسة المحيطة.

توريث الإعدادات

السياسات، مثل مجموعات الإدارة، تكون مرتبة في تسلسل هرمي. الوضع الافتراضي أن إعدادات السياسة الفرعية تورث من السياسة الأصلية. السياسة الفرعية هي سياسة مخصصة للمستويات الهرمية المتداخلة، أي أنها سياسة مخصصة لمجموعات الإدارة المتداخلة وخوادم الإدارة الثانوية. يمكنك تعطيل توريث الإعدادات من السياسة الأصلية.

يوجد لدى كل سياسة السمة، التي تشير إلى إذا كان بالإمكان تعديل الإعدادات في السياسات الفرعية أو في إعدادات التطبيق المحلية. لا يتم تمكين السمة إلا إذا تم تمكين توريث إعدادات السياسة الرئيسية في السياسة الفرعية. لا تؤثر سياسات الوجود خارج المكتب على السياسات الأخرى من خلال التسلسل الهيكلي لمجموعات الإدارة.



توريث الإعدادات

يتم تحديد حقوق الوصول إلى إعدادات السياسة (كتابة، قراءة، تنفيذ) لكل مستخدم لديه حق الوصول إلى خادم إدارة Kaspersky Security Center وبشكل منفصل لكل نطاق وظيفي لـ Kaspersky Endpoint Security. لتكوين حقوق الوصول إلى إعدادات السياسة، انتقل إلى القسم **الأمان** من نافذة خصائص خادم إدارة Kaspersky Security Center.

إنشاء سياسة

كيفية إنشاء سياسة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في مجلد **الأجهزة المدارة** الخاص بشجرة وحدة تحكم الإدارة، حدد المجلد الذي يحتوي على اسم مجموعة الإدارة التي تنتمي إليها أجهزة الكمبيوتر العميلة ذات الصلة.

3. في مساحة العمل، حدد علامة التبويب **سياسات**.

4. انقر فوق الزر **سياسة جديدة**.

   بدء تشغيل معالج السياسة.

5. اتبع تعليمات "معالج السياسات".

كيفية إنشاء سياسة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر على الزر **Add**.

   بدء تشغيل معالج السياسة.

3. حدد برنامج Kaspersky Endpoint Security وانقر على **Next**.

4. يُرجى القراءة والموافقة على الشروط الخاصة بكلمة مرور بيان شبكة Kaspersky Security Network (KSN) وانقر على **Next**.

5. في النافذة **General**تستطيع تنفيذ الإجراءات التالية:

   - قم بتغيير اسم السياسة.
   - حدد حالة السياسة:
     - **Active**. بعد إجراء المزامنة التالية، سيتم استخدام السياسة باعتبارها السياسة النشطة على جهاز الكمبيوتر.
     - **Inactive**. سياسة النسخ الاحتياطي. إذا لزم الأمر يمكن تحويل حالة السياسة من غير نشطة إلى نشطة.
     - **Out-of-office**. يتم تفعيل السياسة عندما يترك جهاز الكمبيوتر شبكة المؤسسة المحيطة.
   - تكوين توارث الإعدادات:
     - **Inherit settings from parent policy**. إذا تم تشغيل زر التبديل فإن القيم الخاصة بإعدادات السياسة يتم توريثها من السياسة ذات المستوى الأعلى. يتعذر تحرير إعدادات السياسة في حال تعيين للسياسة الرئيسية.
     - **Force inheritance of settings in child policies**. إذا تم تشغيل زر التبديل، فإنه يتم نشر القيم الخاصة بإعدادات السياسة إلى السياسات الفرعية. في خصائص السياسة الفرعية، سيكون زر **Inherit settings from parent policy** مفعلاً بشكل تلقائي ولا يمكن إيقاف تشغيله. يتم توريث إعدادات السياسة الفرعية من السياسة الرئيسية، باستثناء الإعدادات التي يتم تمييزها من خلال . يتعذر تحرير إعدادات السياسة الفرعية في حال تعيين للسياسة الرئيسية.

6. في علامة التبويب **Application settings**، يمكنك تكوين إعدادات سياسة Kaspersky Endpoint Security.

7. احفظ تغييراتك.

ونتيجة لذلك سيتم تكوين الإعدادات الخاصة بـ Kaspersky Endpoint على أجهزة الكمبيوتر العميلة أثناء المزامنة التالية. يمكنك عرض معلومات حول السياسة المطبقة على الكمبيوتر في واجهة Kaspersky Endpoint Security من خلال النقر على الزر على الشاشة الرئيسية (اسم السياسة على سبيل المثال). للقيام بذلك، في إعدادات سياسة وكيل الشبكة تحتاج إلى تمكين استلام بيانات السياسة الموسعة. وللمزيد من التفاصيل حول سياسة عميل الشبكة، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

مؤشر مستوى الأمان

يتم عرض مؤشر مستوى الأمان في الجزء العلوي من نافذة **الخصائص: <اسم السياسة>**. ومن الممكن أن يأخذ المؤشر أحد القيم التالية:

- **مستوى حماية مرتفع**. يأخذ المؤشر هذه القيمة ويتحول إلى اللون الأخضر في حالة تمكين كل مكونات من الفئات التالية:
  - **حرج**. تتضمن هذه الفئة المكونات التالية:
    - الحماية من تهديدات الملفات.
    - اكتشاف السلوك.
    - منع الاستغلال.
    - محرك المعالجة.
  - **هام**. تتضمن هذه الفئة المكونات التالية:
    - Kaspersky Security Network.
    - الحماية من تهديدات الويب.
    - الحماية من تهديدات البريد.
    - منع اختراق المضيف.
- **مستوى حماية متوسط**. يأخذ المؤشر هذه القيمة ويتحول إلى اللون الأصفر في حالة تعطيل أحد المكونات الهامة.
- **مستوى حماية منخفض**. يأخذ المؤشر هذه القيمة ويتحول إلى اللون الأحمر في الحالات التالية:
  - تعطيل مكون هام واحد أو أكثر.
  - تعطيل مكونين هامين أو أكثر.

إذا كان للمؤشر قيمة **مستوى حماية متوسط** أو **مستوى حماية منخفض**، سيظهر الرابط الذي يفتح نافذة **إعدادات متقدمة** على يسار المؤشر. وفي هذه النافذة، يمكنك تمكين أي من مكونات الحماية الموصى بها.

إدارة المهام

يمكنك إنشاء الأنواع التالية من المهام لإدارة البرنامج Kaspersky Endpoint Security من خلال Kaspersky Security Center:

- المهام المحلية التي تم تكوينها لكمبيوتر عميل فردي.
- المهام الجماعية التي تم تكوينها لأجهزة كمبيوتر عميلة ضمن مجموعات الإدارة.
- مهام مخصصة لمجموعة من أجهزة الكمبيوتر.

يمكنك إنشاء أي عدد من المهام الجماعية، أو المهام المخصصة لمجموعة من أجهزة الكمبيوتر، أو المهام المحلية. للمزيد من التفاصيل عن العمل مع مجموعات الإدارة ومجموعات من أجهزة الكمبيوتر، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

يدعم Kaspersky Endpoint Security المهام التالية:

- **فحص البرامج الضارة**. يقوم برنامج Kaspersky Endpoint Security بفحص مناطق الكمبيوتر المحددة في إعدادات المهمة لتحديد الفيروسات والتهديدات الأخرى. وتعتبر مهمة فحص البرامج الضارة مطلوبة لعملية لتشغيل برنامج Kaspersky Endpoint Security ويتم تكوينها أثناء معالج البدء السريع. من المستحسن أن تكون جدولة المهمة للتشغيل مرة واحدة على الأقل في الأسبوع.
- **إضافة مفتاح**. يقوم برنامج Kaspersky Endpoint Security بإضافة مفتاح لتفعيل التطبيقات، بما في ذلك المفتاح الإضافي. قبل تشغيل المهمة، تأكد من أن عدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها، لا يتجاوز عدد أجهزة الكمبيوتر المسموح بها بموجب الترخيص.
- **تغيير مكونات التطبيق**. يقوم Kaspersky Endpoint Security بتثبيت المكونات أو إزالتها على أجهزة الكمبيوتر العميلة وفقًا لقائمة المكونات المحددة في إعدادات المهمة. لا يمكن إزالة الملف الخاص بالحماية من تهديدات الملفات. تساعد المجموعة المثلى من مكونات Kaspersky Endpoint Security على الحفاظ على موارد الكمبيوتر.
- **المخزون**. يقوم برنامج Kaspersky Endpoint Security بجمع معلومات حول كل ملفات التطبيق التنفيذية والمخزنة على أجهزة الكمبيوتر. يتم تنفيذ مهمة المخزونبواسطة مكون التحكم في التطبيق. إذا لم يتم تثبيت مكون التحكم في التطبيقات فسيتم إنهاء المهمة مع ظهور خطأ.
- **تحديث**. يقوم برنامج Kaspersky Endpoint Security بتحديث قواعد البيانات والوحدات النمطية الخاصة بالتطبيق. وتعتبر مهمة تحديث مطلوبة لعملية لتشغيل برنامج Kaspersky Endpoint Security ويتم تكوينها أثناء معالج البدء السريع. يُوصى بتكوين جدول يقوم بتشغيل المهمة مرة واحدة في اليوم على الأقل.
- **مسح البيانات**. يقوم برنامج Kaspersky Endpoint Security بحذف الملفات والمجلدات من أجهزة كمبيوتر المستخدمين فورًا أو إذا لم يكن هناك اتصال مع Kaspersky Security Center لوقت طويل.
- **تراجع عن التحديث**. يتراجع Kaspersky Endpoint Security عن التحديث الأخير لقواعد البيانات والوحدات النمطية للتطبيق. قد يكون ذلك ضروريًا على سبيل المثال، إذا كانت قواعد البيانات الجديدة تحتوي على بيانات غير صحيحة قد تتسبب في قيام برنامج Kaspersky Endpoint Security بمنع تطبيق آمن.
- **التحقق من السلامة**. يقوم برنامج Kaspersky Endpoint Security بتحليل ملفات التطبيق، ويتحقق من ملفات التطبيق بحثًا عن أية تلفيات أو تعديلات، ويتحقق من التوقيعات الرقمية فيها.
- **إدارة حسابات وكيل المصادقة**. يقوم Kaspersky Endpoint Security بتكوين إعدادات حساب وكيل المصادقة. وكيل المصادقة ضروري للعمل مع المحركات المشفرة. قبل تحميل نظام التشغيل، يحتاج المستخدم إلى إكمال المصادقة مع الوكيل.

يتم تشغيل المهام على جهاز الكمبيوتر فقط إذا كان Kaspersky Endpoint Security قيد التشغيل.

إضافة مهمة جديدة

كيفية إنشاء مهمة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. حدد المجلد **المهام** في شجرة وحدة تحكم الإدارة.
3. انقر فوق زر **مهمة جديدة**.
   يبدأ معالج المهمة.
4. اتبع تعليمات معالج المهمة.

كيفية إنشاء مهمة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.
تفتح قائمة المهام.

2. انقر على الزر **Add**.
يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type**، حدد المهمة التي تريد تشغيلها على أجهزة كمبيوتر المستخدمين.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.

5. أغلق المعالج.

سيتم عرض مهمة جديدة في قائمة المهام. سيكون للمهمة الإعدادات الافتراضية. لتكوين إعدادات المهمة، تحتاج للانتقال إلى خصائص المهمة. لتشغيل المهمة، تحتاج إلى تحديد خانة الاختيار المقابلة لها والنقر فوق الزر **تشغيل**. بعد بدء تشغيل المهمة، يمكنك إيقافها مؤقتًا واستكمالها لاحقًا.

في قائمة المهام، يمكنك مراقبة نتائج المهمة، والتي تتضمن حالة المهمة وإحصائيات أداء المهمة على أجهزة الكمبيوتر. يمكنك أيضًا إنشاء مجموعة من الأحداث لمراقبة إكمال المهام (**Event selections** ← **Monitoring and reporting**). للمزيد من التفاصيل حول تحديد الحدث، يُرجى الرجوع إلى تعليمات Kaspersky Security Center. يتم كذلك حفظ نتائج تنفيذ المهام محليًا في سجل أحداث Windows وفي تقارير Kaspersky Endpoint Security.

التحكم في الوصول للمهمات

يتم تحديد حقوق الوصول إلى مهام Kaspersky Endpoint Security (قراءة، كتابة، تنفيذ) لكل مستخدم لديه حق الوصول إلى خادم إدارة Kaspersky Security Center من خلال إعدادات الوصول إلى المجالات الوظيفية لـ Kaspersky Endpoint Security. لتكوين الوصول إلى المجالات الوظيفية لـ Kaspersky Endpoint Security، انتقل إلى القسم **الأمان** من نافذة خصائص خادم إدارة Kaspersky Security Center. وللحصول المزيد من التفاصيل حول إدارة المهام من خلال Kaspersky Security Center، يرجى الرجوع إلى تعليمات Kaspersky Security Center.

يمكنك تكوين حقوق المستخدمين لمهام للوصول باستخدام سياسة (وضع إدارة المهام). على سبيل المثال: يمكنك إخفاء مهمة جماعية في واجهة Kaspersky Endpoint Security.

كيفية تكوين وضع إدارة المهام في واجهة Kaspersky Endpoint Security من خلال وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **المهام المحلية** ← **إدارة المهام**.

5. قم بتكوين وضع إدارة المهام (انظر الجدول أدناه).

6. احفظ تغييراتك.

كيفية تكوين وضع إدارة المهام في واجهة Kaspersky Endpoint Security من خلال ووحدة تحكم الويب

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Local Tasks** ← **Task management**.

5. قم بتكوين وضع إدارة المهام (انظر الجدول أدناه).

6. احفظ تغييراتك.

إعدادات إدارة المهام

المعلمة	الوصف
Allow use of local tasks	في حالة تحديد خانة الاختيار هذه، يتم عرض المهام المحلية في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. عند عدم وجود قيود إضافية على السياسة، يمكن للمستخدم تكوين المهام وتشغيلها. ومع ذلك، يظل تكوين برنامج جدولة المهام غير متاح للمستخدم. ويستطيع المستخدم تشغيل المهام يدويًا فقط. إذا تم إلغاء تحديد خانة الاختيار، يتم وقف استخدام المهام المحلية. وفي هذا الوضع، لا يتم تشغيل المهام المحلية وفقًا لجدول. ولا يمكن بدء المهام أو تكوينها في واجهة Kaspersky Endpoint Security المحلية، أو عند العمل مع سطر الأوامر. يظل بإمكان المستخدم بدء عملية فحص على ملف أو مجلد عن طريق تحديد الخيار **فحص للبحث عن الفيروسات** في قائمة السياق للملف أو المجلد. تبدء مهمة الفحص بالقيم الافتراضية لإعدادات مهمة فحص مخصص.
Allow group tasks to be displayed	في حالة تحديد خانة الاختيار هذه، يتم عرض المهام الجماعية في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. يمكن للمستخدم عرض قائمة بجميع المهام في واجهة التطبيق. في حالة إلغاء تحديد خانة الاختيار، فإن Kaspersky Endpoint Security يعرض قائمة مهام خالية.
Allow management of group tasks	في حالة تحديد خانة الاختيار، يمكن للمستخدمين بدء وإيقاف المهام الجماعية المحددة في Kaspersky Security Center. يمكن للمستخدمين بدء وإيقاف تشغيل المهام في واجهة التطبيق أو في واجهة التطبيق المبسطة. في حالة عدم تحديد خانة الاختيار، فإن Kaspersky Endpoint Security يبدأ المهام المجدولة آليًا، أو أن المدير يبدأ المهام يدويًا في Kaspersky Security Center.

تكوين إعدادات التطبيق المحلية

في Kaspersky Security Center، يمكنك تكوين إعدادات برنامج Kaspersky Endpoint Security على جهاز كمبيوتر معين. وهي تعد إعدادات تطبيق محلية. قد يتعذر الوصول إلى بعض الإعدادات للتحرير. يتم حظر هذه الإعدادات عن طريق السمة الموجودة في خصائص السياسة.

كيفية تكوين إعدادات التطبيق المحلي في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في المجلد **الأجهزة المدارة** الخاص بشجرة وحدة تحكم الإدارة، افتح المجلد الذي يحمل اسم مجموعة الإدارة التي ينتمي إليها جهاز الكمبيوتر العميل المناسب.
3. في مساحة العمل، حدد علامة تبويب **الأجهزة**.
4. حدد الكمبيوتر الذي تريد تكوين إعدادات البرنامج Kaspersky Endpoint Security فيه.
5. في قائمة سياق الكمبيوتر العميل، حدد **خصائص**.

   تفتح عندئذٍ نافذة خصائص كمبيوتر العميل.
6. في نافذة خصائص كمبيوتر العميل، حدد القسم **التطبيقات**.

   تظهر قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر العميل في الجزء الأيمن من نافذة خصائص الكمبيوتر العميل.
7. حدد Kaspersky Endpoint Security.
8. انقر فوق الزر **خصائص** أسفل قائمة تطبيقات Kaspersky.

   تفتح النافذة **إعدادات تطبيق Kaspersky Endpoint Security for Windows**.
9. في القسم **إعدادات عامة**، كوّن إعدادات Kaspersky Endpoint Security وكذلك التقارير والمخزن.

   تعتبر الأقسام الأخرى لنافذة **إعدادات تطبيق Kaspersky Endpoint Security for Windows** قياسية لتطبيق Kaspersky Security Center. يتم توفير وصف لتلك الأقسام في تعليمات Kaspersky Security Center.

   إذا كان أحد التطبيقات يخضع لسياسة تحظر إجراء تغييرات على إعدادات معينة، فلن تتمكن من تحرير تلك الإعدادات أثناء تكوين إعدادات التطبيق في القسم **الإعدادات العامة**.
10. احفظ تغييراتك.

كيفية تكوين التطبيق المحلي في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Managed devices** ← **Devices**.

2. حدد الكمبيوتر الذي تريد تكوين إعدادات التطبيق المحلية له.

   تقوم هذه الخطوة بفتح خصائص الكمبيوتر.

3. حدد علامة التبويب **Applications**.

4. انقر على **Kaspersky Endpoint Security for Windows**.

   تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.

5. حدد علامة التبويب **Application settings**.

6. قم بتكوين إعدادات التطبيق المحلية.

7. احفظ تغييراتك.

إعدادات التطبيقات المحلية هي نفسها إعدادات السياسة، باستثناء إعدادات التشفير.

بدء وإيقاف تشغيل برنامج Kaspersky Endpoint Security

بعد تثبيت Kaspersky Endpoint Security على جهاز الكمبيوتر الخاص بالمستخدم، يتم بدء التطبيق تلقائيًا. يتم بشكلٍ افتراضي بدء تشغيل برنامج Kaspersky Endpoint Security بعد بدء تشغيل نظام التشغيل. من غير الممكن تكوين بدء التشغيل التلقائي للتطبيق في إعدادات نظام التشغيل.

قد يستغرق تنزيل قواعد بيانات مكافحة فيروسات Kaspersky Endpoint Security بعد بدء نظام التشغيل مدة دقيقتين اعتمادًا على إمكانيات الكمبيوتر. وأثناء ذلك الوقت، يتم خفض مستوى حماية الكمبيوتر. لا يؤدي تنزيل قواعد بيانات مكافحة الفيروسات عند بدء Kaspersky Endpoint Security على نظام تشغيل تم تشغيله بالفعل إلى خفض مستوى حماية الكمبيوتر.

كيفية تكوين بدء تشغيل Kaspersky Endpoint Security في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.

5. استخدم خانة الاختيار **بدء Kaspersky Endpoint Security عند بدء تشغيل الكمبيوتر (مستحسن)** لتكوين بدء تشغيل التطبيق.

6. احفظ تغييراتك.

كيفية تكوين بدء تشغيل Kaspersky Endpoint Security في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Application Settings**.

5. استخدم خانة الاختيار **Start Kaspersky Endpoint Security on computer startup (recommended)** لتكوين بدء تشغيل التطبيق.

6. احفظ تغييراتك.

كيفية تكوين بدء تشغيل Kaspersky Endpoint Security في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.

إعدادات Kaspersky Endpoint Security for Windows

3. استخدم خانة الاختيار **بدء Kaspersky Endpoint Security عند بدء تشغيل الكمبيوتر (مستحسن)** لتكوين بدء تشغيل التطبيق.

4. احفظ تغييراتك.

لا يوصي خبراء Kaspersky بإيقاف برنامج Kaspersky Endpoint Security يدويًا، لأن ذلك يُعرّض الكمبيوتر وبياناتك الشخصية للتهديدات. إذا لزم الأمر، يمكنك إيقاف وظيفة حماية الكمبيوتر مؤقتًا، للمدة التي تريدها، دون إيقاف التطبيق.

يمكنك مراقبة حالة التطبيق باستخدام عنصر **Protection Status**.

كيفية تكوين بدء أو إيقاف Kaspersky Endpoint Security في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في المجلد **الأجهزة المدارة** الخاص بشجرة وحدة تحكم الإدارة، افتح المجلد الذي يحمل اسم مجموعة الإدارة التي ينتمي إليها جهاز الكمبيوتر العميل المناسب.
3. في مساحة العمل، حدد علامة تبويب **الأجهزة**.
4. حدد الكمبيوتر الذي ترغب في بدء تشغيل التطبيق أو إيقاف تشغيله عليه.
5. انقر بزر الماوس الأيمن فوق القائمة السياقية الخاصة بالكمبيوتر العميل وحدد **الخصائص**.
6. في نافذة خصائص كمبيوتر العميل، حدد القسم **التطبيقات**.
   تظهر قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر العميل في الجزء الأيمن من نافذة خصائص الكمبيوتر العميل.
7. حدد Kaspersky Endpoint Security.
8. نفذ ما يلي:
   - لبدء التطبيق، انقر فوق الزر الموجود إلى يمين قائمة تطبيقات Kaspersky.
   - لإيقاف التطبيق، انقر فوق الزر الموجود إلى يمين قائمة تطبيقات Kaspersky.

كيفية تكوين بدء أو إيقاف Kaspersky Endpoint Security في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Managed devices** ← **Devices**.
2. انقر فوق اسم الكمبيوتر الذي تريد بدء أو إيقاف Kaspersky Endpoint Securityعليه.
   تفتح عندئذٍ نافذة خصائص الكمبيوتر.
3. حدد علامة التبويب **Applications**.
4. حدد خانة الاختيار المقابلة لتطبيق **Kaspersky Endpoint Security for Windows**.
5. انقر فوق الزر **Start** أو **Stop**.

كيفية تكوين بدء أو إيقاف Kaspersky Endpoint Security من سطر الأوامر

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.

2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.

3. لبدء تشغيل التطبيق من سطر الأوامر، اكتب `klpsm.exe start_avp_service`.

4. لإيقاف تشغيل التطبيق من سطر الأوامر، اكتب `klpsm.exe stop_avp_service`.

لإيقاف التطبيق من سطر الأوامر، يتعين عليك تمكين الإدارة الخارجية لخدمات النظام.

بدء التطبيق وإيقافه من خلال سطر الأوامر

التوقف المؤقت واستئناف حماية الكمبيوتر ومراقبته

يُقصد بإيقاف مكون الحماية والمراقبة بالكمبيوتر مؤقتًا تعطيل كل مكونات الحماية والمراقبة الخاصة ببرنامج Kaspersky Endpoint Security لبعض الوقت.

يتم عرض حالة التطبيق باستخدام رمز التطبيق في منطقة إخطارات شريط المهام.

- يدل الرمز على إيقاف تشغيل مكون الحماية والمراقبة بجهاز الكمبيوتر مؤقتًا.
- الرمز يدل على تفعيل مكون الحماية والمراقبة بجهاز الكمبيوتر.

لا يؤثر الإيقاف المؤقت لمكون الحماية والمراقبة بجهاز الكمبيوتر واستئناف تشغيله على مهام الفحص والتحديث.

في حالة تأسيس أي من اتصالات الشبكة فعليًا عند الإيقاف المؤقت لمكون الحماية والمراقبة بجهاز الكمبيوتر واستئناف تشغيله، فسوف يظهر إخطار يشير إلى قطع هذه الاتصالات.

لإيقاف مكون الحماية والمراقبة بجهاز الكمبيوتر مؤقتًا:

1. انقر بزر الماوس الأيمن لإظهار القائمة السياقية الخاصة بأيقونة التطبيق في منطقة إعلام شريط المهام.

2. في قائمة السياق، حدد **إيقاف الحماية مؤقتًا** (انظر الشكل أدناه).
يتوفر عنصر قائمة السياق هذا إذا تم تمكين الحماية بكلمة المرور.

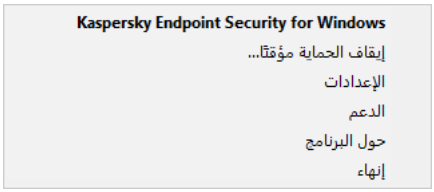
3. حدد أحد الخيارات التالية:

- **إيقاف مؤقت لمدة <الفترة المحددة>** – سوف يتم استئناف حماية ومراقبة جهاز الكمبيوتر بعد مرور الفترة الزمنية التي تم تحديدها في القائمة المنسدلة أدناه.
- **إيقاف مؤقت إلى أن تتم إعادة تشغيل التطبيق** – سوف يتم استئناف حماية ومراقبة جهاز الكمبيوتر بعد إعادة تشغيل التطبيق أو إعادة تشغيل نظام التشغيل. يجب تمكين بدء التشغيل التلقائي للتطبيق لاستخدام هذا الخيار.

- **إيقاف مؤقت** – سوف يستأنف مكون الحماية والمراقبة بجهاز الكمبيوتر عمله عندما تقرر إعادة تمكينه.

4. انقر على **إيقاف الحماية مؤقتًا**.

Kaspersky Endpoint Security سوف يوقف بشكل موقت تشغيل جميع مكونات الحماية والمراقبة التي لم يتم وضع علامة قفل (🔒) عليها في السياسة. قبل تنفيذ هذه العملية، يُوصى بتعطيل سياسة Kaspersky Security Center.



قائمة سياق رمز التطبيق

لاستئناف تشغيل مكون الحماية والمراقبة بجهاز الكمبيوتر:

1. انقر بزر الماوس الأيمن لإظهار القائمة السياقية الخاصة بأيقونة التطبيق في منطقة إعلام شريط المهام.

2. في قائمة السياق، حدد **استئناف الحماية**.

يمكنك استئناف تشغيل مكون الحماية والمراقبة بجهاز الكمبيوتر في أي وقت بغض النظر عن تحديدك مُسبقًا لخيار الإيقاف المؤقت لمكون الحماية والمراقبة.

إنشاء ملف تكوين واستخدامه

يتيح لك ملف التكوين مع إعدادات Kaspersky Endpoint Security إنجاز المهام التالية:

- نفذ التثبيت المحلي لتطبيق Kaspersky Endpoint Security عبر سطر الأوامر باستخدام الإعدادات مسبقة التحديد.
  لفعل ذلك، يجب حفظ ملف التكوين في المجلد نفسه الذي توجد فيه حزمة التوزيع.
- قم بإجراء تثبيت عن بعد لتطبيق Kaspersky Endpoint Security عبر Kaspersky Security Center باستخدام الإعدادات مسبقة التحديد.
- قم بترحيل إعدادات Kaspersky Endpoint Security من جهاز كمبيوتر إلى آخر (انظر التعليمات أدناه).

لإنشاء ملف تكوين:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إدارة الإعدادات**.

3. انقر على **تصدير**.

4. في النافذة التي تفتح، حدد المسار الذي تريد حفظ ملف التكوين فيه، وأدخل اسمه.

لاستخدام ملف التكوين لتثبيت Kaspersky Endpoint Security محليًا أو عن بعد، يجب عليك تسميته install.cfg.

5. احفظ الملف.

لاستيراد إعدادات Kaspersky Endpoint Security من ملف تكوين:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إدارة الإعدادات**.

3. انقر على **استيراد**.

4. في النافذة التي تفتح، أدخل المسار المؤدي إلى ملف التكوين.

5. افتح الملف.

سيتم تعيين كل قيم إعدادات Kaspersky Endpoint Security وفقًا لملف التكوين المحدد.

إدارة إعدادات التطبيق

استعادة إعدادات التطبيق الافتراضية

يمكنك استعادة إعدادات التطبيق التي توصي بها Kaspersky في أي وقت تريد. عند استعادة الإعدادات، يتم تعيين مستوى الأمان **مستحسن** لجميع مكونات الحماية.

لاستعادة إعدادات التطبيق الافتراضية:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إدارة الإعدادات**.

3. انقر على **استعادة**.

4. احفظ تغييراتك.

إدارة إعدادات التطبيق

فحص البرامج الضارة

فحص البرامج الضارة أمر حيوي لأمان الكمبيوتر. قم بإجراء فحص البرامج الضارة بانتظام للقضاء على احتمال انتشار البرامج الضارة التي لم يتم اكتشافها بواسطة مكونات الحماية بسبب تعيين مستوى أمان منخفض أو لأسباب أخرى.

لا يفحص Kaspersky Endpoint Security الملفات التي يوجد محتواها على التخزين السحابي لموقع OneDrive، بل ينشئ مدخلات سجل توضح أن هذه الملفات لم يتم فحصها.

فحص كامل

فحص شامل للكمبيوتر بأكمله. يقوم برنامج Kaspersky Endpoint Security بفحص الكائنات التالية:

- ذاكرة Kernel؛
- الكائنات التي يتم تحميلها عند بدء تشغيل نظام التشغيل
- قطاعات التمهيد؛
- النسخ الاحتياطي لنظام التشغيل
- جميع المحركات الثابتة ومحركات الأقراص القابلة للإزالة

ينصحك خبراء Kaspersky بعدم تغيير نطاق الفحص لمهمة الفحص الكامل.

للحفاظ على موارد جهاز الكمبيوتر، يوصى بتشغيل مهمة فحص في الخلفية بدلاً من مهمة الفحص الكامل. لن يؤثر ذلك على مستوى أمان الكمبيوتر.

فحص المناطق الحرجة

بشكلٍ افتراضي، يفحص Kaspersky Endpoint Security ذاكرة kernel والعمليات قيد التشغيل وقطاعات تمهيد القرص.

ينصحك خبراء Kaspersky بعدم تغيير نطاق الفحص لمهمة فحص المناطق الحرجة.

فحص مخصص

يفحص برنامج Kaspersky Endpoint Security الكائنات التي يحددها المستخدم. يمكنك فحص أي كائن من القائمة التالية:

- ذاكرة النظام
- الكائنات التي يتم تحميلها عند بدء تشغيل نظام التشغيل
- النسخ الاحتياطي لنظام التشغيل
- صندوق بريد Microsoft Outlook
- محركات الأقراص الصلبة والقابلة للإزالة ومحركات الشبكة

- أي ملف محدد

فحص في الخلفية

الفحص في الخلفية هو وضع فحص من Kaspersky Endpoint Security لا يقوم بعرض إخطارات للمستخدم. تتطلب عملية الفحص في الخلفية استخدام موارد أقل من جهاز الكمبيوتر بخلاف أنواع الفحص الأخرى (مثل الفحص الكامل). وفي هذا الوضع يفحص برنامج Kaspersky Endpoint Security كائنات بدء التشغيل ومقطع التمهيد وذاكرة النظام وقسم النظام.

التحقق من السلامة

يتحقق Kaspersky Endpoint Security من الوحدات النمطية للتطبيق بحثًا عن وجود تلف أو تعديلات.

فحص الكمبيوتر

الفحص أمر حيوي لأمان الكمبيوتر. قم بإجراء فحص البرامج الضارة بانتظام للقضاء على احتمال انتشار البرامج الضارة التي لم يتم اكتشافها بواسطة مكونات الحماية بسبب تعيين مستوى أمان منخفض أو لأسباب أخرى. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

يحتوي Kaspersky Endpoint Security على المهام القياسية التالية المحددة مسبقًا: فحص كاملوفحص المناطق الحرجةوفحص مخصص. وإذا كان نظام إدارة Kaspersky Security Center منشور في مؤسستك، يمكنك إنشاء مهمة فحص البرامج الضارة وتكوين الفحص. وتتوفر أيضًا المهمة فحص في الخلفية في Kaspersky Security Center. ولا يمكن تكوين الفحص في الخلفية.

كيفية تشغيل مهمة فحص في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **المهام**.
3. حدد مهمة الفحص وانقر نقرًا مزدوجًا لفتح خصائص المهمة.
   إذا لزم الأمر، أنشئ مهمة فحص البرامج الضارة.
4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.
5. كوّن مهمة الفحص (انظر الجدول أدناه).
   اذا كان ضروريًا، كوّن جدول مهام الفحص.
6. احفظ تغييراتك.
7. قم بتشغيل مهمة الفحص.

سيبدأ Kaspersky Endpoint Security فحص الكمبيوتر. إذا قاطع المستخدم تنفيذ المهمة (على سبيل المثال عن طريق إيقاف تشغيل الكمبيوتر)، يقوم Kaspersky Endpoint Security بتشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقف فيها الفحص.

كيفية تشغيل مهمة فحص في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.

نافذة خصائص المهمة.

3. حدد علامة التبويب **Application settings**.

4. كوّن مهمة الفحص (انظر الجدول أدناه).

اذا كان ضروريًا، كوّن جدول مهام الفحص.

5. احفظ تغييراتك.

6. قم بتشغيل مهمة الفحص.

سيبدأ Kaspersky Endpoint Security فحص الكمبيوتر. إذا قاطع المستخدم تنفيذ المهمة (على سبيل المثال عن طريق إيقاف تشغيل الكمبيوتر)، يقوم Kaspersky Endpoint Security بتشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقف فيها الفحص.

كيفية تشغيل مهمة فحص في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. في قائمة المهام، حدد مهمة الفحص وانقر فوق ⚙.

3. كوّن مهمة الفحص (انظر الجدول أدناه).

اذا كان ضروريًا، كوّن جدول مهام الفحص.

4. احفظ تغييراتك.

5. قم بتشغيل مهمة الفحص.

سيبدأ Kaspersky Endpoint Security فحص الكمبيوتر. سيعرض التطبيق تقدم الفحص، وعدد الملفات التي تم فحصها، والوقت المتبقي للفحص. يمكنك إيقاف المهمة في أي وقت بالنقر فوق الزر **إيقاف**. إذا لم يتم عرض مهمة الفحص، فيعني هذا أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

نتيجة لذلك، يفحص Kaspersky Endpoint Security الكمبيوتر وفي حالة اكتشاف تهديد، ينفذ الإجراء الذي تم تكوينه في إعدادات التطبيق. ويحاول التطبيق عادة تنظيف الملفات المصابة. ونتيجة لذلك، يمكن أن تتلقى الملفات المصابة الحالات التالية:

- **تم التأجيل**. لا يمكن تنظيف الملف المصاب. ويحذف التطبيق الملف المصاب بعد إعادة تشغيل الكمبيوتر.
- **تم تسجيل الدخول**. لا يمكن تنظيف الملف المصاب. ويضيف التطبيق معلومات عن الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة.
- **الكتابة غير مدعمة** أو **خطأ في الكتابة**. لا يمكن تنظيف الملف المصاب. لا يمتلك التطبيق حق الوصول للكتابة.
- **تمت المعالجة بالفعل**. اكتشف التطبيق ملفًا مصابًا في وقت سابق. وينظف التطبيق أو يحذف الملف المصاب بعد إعادة تشغيل الكمبيوتر.

إعدادات الفحص

المعلمة	الوصف
مستوى الأمان	من الممكن أن يستخدم Kaspersky Endpoint Security مجموعات مختلفة من الإعدادات لإجراء فحص. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان:

	• **مرتفع**. يفحص Kaspersky Endpoint Security كل أنواع الملفات. عند فحص الملفات المركبة، يفحص التطبيق ملفات تنسيق البريد أيضًا. • **مستحسن**. لا يقوم Kaspersky Endpoint Security إلا بفحص تنسيقات ملفات محددة على جميع محركات الأقراص الثابتة وأقراص الشبكة ووسائط التخزين القابلة للإزالة الخاصة بالكمبيوتر، وكذلك كائنات OLE المضمنة. لا يفحص التطبيق الأرشيفات أو حزم التثبيت. • **منخفض**. يفحص Kaspersky Endpoint Security الملفات الجديدة أو المعدلة فقط والتي تحمل الامتدادات الموضحة فقط على جميع محركات الأقراص الثابتة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة على الكمبيوتر. ولا يفحص التطبيق الملفات المركبة. يمكنك تحديد أحد مستويات الأمان المعدة مسبقًا أو تكوين إعدادات مستوى الأمان يدويًا. في حالة تغيير إعدادات مستوى الأمان، يمكنك دائمًا العودة إلى إعدادات مستوى الأمان الموصى بها.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات. **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا تعذر التنظيف، يضيف Kaspersky Endpoint Security معلومات حول الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة. **إخطار**. في حالة تحديد هذا الخيار، يضيف Kaspersky Endpoint Security المعلومات حول الملفات المصابة إلى قائمة التهديدات النشطة عند اكتشاف هذه الملفات. قبل محاولة تنظيف ملف مصاب أو حذفه، ينشئ التطبيق نسخة احتياطية من الملف في حال احتجت إلى استعادة الملف أو إذا كان من الممكن تنظيفه في المستقبل. عند اكتشاف ملفات مصابة تعتبر جزءًا من تطبيق Windows Store ، يحاول Kaspersky Endpoint Security حذف الملف.
تشغيل التنظيف المتقدم على الفور (متوفر فقط في Kaspersky Security Center (Console	يتم تنفيذ التنظيف المتقدم أثناء مهمة فحص فيروسات على جهاز كمبيوتر فقط في حالة تمكين ميزة التنظيف المتقدم في خصائص السياسة المطبقة على هذا الكمبيوتر. في حالة تحديد خانة الاختيار، ينظف Kaspersky Endpoint Security الإصابة النشطة فور اكتشافها أثناء تنفيذ مهمة فحص الفيروسات. بعد تنظيف الإصابة النشطة، يعيد Kaspersky Endpoint Security تشغيل الكمبيوتر دون مطالبة المستخدم. في حالة إلغاء تحديد خانة الاختيار، ينظف Kaspersky Endpoint Security الإصابة النشطة فور اكتشافها أثناء تنفيذ مهمة فحص الفيروسات. ينشئ Kaspersky Endpoint Security أحداث الإصابة النشطة في تقارير التطبيقات المحلية وعلى جانب Kaspersky Security Center. ويمكن تنظيف الإصابة النشطة عند تشغيل مهمة فحص الفيروسات مرة أخرى مع تشغيل ميزة التنظيف المتقدم. وبهذه الطريقة، يستطيع مسؤول النظام اختيار الوقت المناسب لإجراء التنظيف المتقدم وإعادة تشغيل أجهزة الكمبيوتر تلقائيًا.
نطاق الفحص	قائمة الكائنات التي يفحصها Kaspersky Endpoint Security أثناء تنفيذ مهمة فحص. قد تشتمل الكائنات في نطاق الفحص على ذاكرة قلب نظام التشغيل، أو العمليات قيد التشغيل، أو قطاعات التمهيد، أو مخزن النسخ الاحتياطي للنظام، أو قواعد بيانات البريد، أو محركات الأقراص الصلبة، أو محركات الأقراص القابلة للإزالة أو محركات أقراص الشبكة، أو مجلد أو ملف.
جدولة الفحص	**يدويًا**. وضع التشغيل الذي يمكنك فيه بدء الفحص يدويًا في الوقت الذي يناسبك. **حسب الجدولة**. في وضع تشغيل مهمة الفحص هذه، يبدأ التطبيق تشغيل مهمة الفحص حسب الجدول الذي قمت بإنشائه. في حالة تحديد وضع تشغيل مهمة الفحص هذه، يمكنك أيضًا بدء تشغيل مهمة الفحص يدويًا.
تأجيل التشغيل بعد بدء التطبيق لمدة N دقيقة	تأجيل بدء مهمة الفحص بعد بدء تشغيل التطبيق. عند بدء تشغيل نظام التشغيل، يتم تشغيل العديد من العمليات، لذلك من المفيد تأجيل تشغيل مهمة الفحص بدلاً من تشغيلها فور بدء تشغيل Kaspersky Endpoint Security.

تشغيل المهام التي تم تخطيها	في حالة تحديد خانة الاختيار، يبدأ Kaspersky Endpoint Security في تشغيل مهمة الفحص التي تم تخطيها بمجرد أن يكون هذا الأمر ممكنًا. يمكن تخطي مهمة الفحص، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء مهمة الفحص المجدولة. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل مهام الفحص التي تم تخطيها. كبديل، سيقوم بتشغيل مهمة الفحص التالية بما يتوافق مع الجدول الحالي.
التشغيل فقط عندما يكون الكمبيوتر خاملاً	تأجيل بدء مهمة الفحص عندما تكون موارد الكمبيوتر مشغولة. يبدأ Kaspersky Endpoint Security مهمة الفحص إذا كان الكمبيوتر مقفلاً أو إذا كانت شاشة التوقف قيد التشغيل. إذا قاطعت تنفيذ المهمة، على سبيل المثال بواسطة إلغاء تأمين الكمبيوتر، يجري Kaspersky Endpoint Security تشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقفت عندها.
تشغيل الفحص باسم	بشكل افتراضي، يتم تشغيل مهمة الفحص باسم المستخدم الذي سجلتَ باستخدام حقوقه في نظام التشغيل. وقد يشمل نطاق الحماية محركات أقراص الشبكة أو كائنات أخرى تتطلب حقوقًا خاصة للوصول. يمكنك تحديد مستخدم يمتلك الحقوق المطلوبة في إعدادات التطبيق وتشغيل مهمة الفحص تحت حساب هذا المستخدم.
أنواع الملفات	يعتبر برنامج Kaspersky Endpoint Security الملفات التي بدون امتدادات الملفات القابلة للتنفيذ. ويفحص التطبيق الملفات القابلة للتنفيذ دومًا بغض النظر عن أنواع الملفات التي اخترتها للفحص. **كل الملفات**. إذا تم تمكين هذا الإعداد، فإن Kaspersky Endpoint Security يفحص كل الملفات دون استثناء (كل التنسيقات والامتدادات). **الملفات التي تم فحصها حسب التنسيق**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. قبل فحص أحد الملفات بحثًا عن التعليمات البرمجية الضارة، يتم تحليل العنوان الداخلي للملف لتحديد تنسيق الملف (على سبيل المثال، .txt أو .doc أو .exe). ويبحث الفحص أيضًا عن الملفات بملحقات ملف معينة. **الملفات التي تم فحصها حسب الامتداد**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. ويتم تحديد تنسيق الملف عندئذٍ استنادًا إلى امتداد الملف. افتراضيًا، يفحص Kaspersky Endpoint Security الملفات حسب تنسيقها. يعد فحص الملفات حسب الملحق أقل أمانًا لأن الملف الضار يمكن أن يكون بملحق غير مدرج في قائمة المواد القابلة للإصابة (على سبيل المثال، `123.`).
فحص الملفات الجديدة والتي تم تغييرها فقط	يفحص فقط الملفات الجديدة والملفات التي تم تعديلها منذ آخر مرة لفحصها. هذا يساعد على تقليل فترة الفحص. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.
تخطي الملفات إذا استغرق فحصها أكثر من N من الثواني	ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.
عدم تشغيل مهام فحص متعددة في الوقت نفسه	يتم تأجيل بدء مهام الفحص إذا كان الفحص قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص الجديدة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، لنفترض أن التطبيق بدأ مهمة فحص كامل وفقًا للجدولة. إذا حاول المستخدم بدء فحص سريع من واجهة التطبيق، سوف يُدرج Kaspersky Endpoint Security مهمة الفحص السريع هذه في قائمة الانتظار ثم يبدأ هذه المهمة تلقائيًا بعد انتهاء مهمة الفحص الكامل. مع ذلك، يبدأ Kaspersky Endpoint Security على الفور مهمة فحص حتى إذا كانت إحدى مهام الفحص التالية قيد التشغيل: • فحص محركات الأقراص القابلة للإزالة عند توصيلها. • الفحص من قائمة السياق. • فحص المناطق الحرجة الذي بدأ عند اكتشاف مؤشر اختراق (IoC). في حالة إلغاء تحديد مربع الاختيار هذا، يتيح لك Kaspersky Endpoint Security تشغيل مهام فحص متعددة في الوقت نفسه. ويتطلب تشغيل مهام فحص متعددة المزيد من موارد الكمبيوتر.
فحص الأرشيفات	فحص تنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE وتنسيقات الأرشيفات الأخرى. يفحص التطبيق الأرشيفات ليس فقط حسب الملحق، لكن أيضًا حسب التنسيق. عند التحقق من الأرشيفات، ينفذ التطبيق عملية تفريغ متكررة. ويسمح هذا باكتشاف التهديدات داخل أرشيفات متعددة المستويات (أرشيف داخل أرشيف).
فحص حزم	تقوم خانة الاختيار هذه بتمكين/تعطيل فحص حزم التوزيع التابعة لجهة خارجية.

التوزيع	
فحص الملفات بتنسيقات Microsoft Office	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
فحص تنسيقات البريد الإلكتروني	فحص ملفات تنسيق البريد الإلكتروني وقاعدة بيانات البريد الإلكتروني. يفحص التطبيق ملفات PST وOST المستخدمة بواسطة برنامجي البريد MS Outlook وWindows Mail بالإضافة إلى ملفات EML. لا يدعم Kaspersky Endpoint Security إصدار 64 بت من عميل البريد MS Outlook. وهذا يعني أن Kaspersky Endpoint Security لا يفحص ملفات MS Outlook (ملفات PST وOST) في حالة تثبيت إصدار 64 بت من MS Outlook على الكمبيوتر، حتى إذا كان البريد مضمنًا في نطاق الفحص. وإذا تم تحديد خانة الاختيار، فإن Kaspersky Endpoint Security يقسم ملف تنسيق البريد إلى مكوناته (عنوان ونص ومرفقات) ويقوم بفحصها بحثًا عن التهديدات. إذا تم إلغاء تحديد خانة الاختيار هذه، فإن Kaspersky Endpoint Security يفحص ملف تنسيق البريد على أنه ملف فردي.
فحص الأرشيفات المحمية بكلمة مرور	في حالة تحديد خانة الاختيار، يفحص التطبيق الأرشيفات المحمية بكلمات مرور. قبل فحص الملفات الموجودة في الأرشيف، تتم مطالبتك بإدخال كلمة مرور. في حالة مسح خانة الاختيار، يتخطى التطبيق فحص الأرشيفات المحمية بكلمة مرور.
عدم فك ضغط الملفات المركبة كبيرة الحجم	في حالة تحديد هذا المربع، لا يفحص التطبيق الملفات المركبة إذا كان حجمها يتجاوز القيمة المحددة. في حالة عدم تحديد خانة الاختيار هذه، يفحص التطبيق الملفات المركبة من جميع الأحجام. يفحص التطبيق الملفات الكبيرة التي يتم استخراجها من الأرشيفات بغض النظر عما إذا كانت خانة الاختيار محددة أو لا.
التعلّم الآلي وتحليل التوقيع	تستخدم طريقة التعلّم الآلي وتحليل التوقيع قواعد بيانات Kaspersky Endpoint Security التي تحتوي على وصف للتهديدات المعروفة وطرق إبطالها. وتوفر الحماية التي تستخدم هذه الطريقة الحد الأدنى المقبول لمستوى الأمان. بناءً على توصيات خبراء Kaspersky، يتم تمكين التعلّم الآلي وتحليل التوقيع دائمًا.
التحليل المساعد على الاكتشاف	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف. عند فحص الملفات للبحث عن تعليمات برمجية ضارة، ينفذ المحلل المساعد على الاكتشاف الإرشادات الواردة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
تقنية iSwift (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.
تقنية iChecker (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).

فحص محركات الأقراص القابلة للإزالة عند توصيلها بالكمبيوتر

يفحص Kaspersky Endpoint Security جميع الملفات التي تقوم بتشغيلها أو نسخها، حتى إذا كان الملف موجودًا على محرك أقراص قابل للإزالة (مكون الحماية من تهديدات الملفات). ولمنع انتشار الفيروسات والبرامج الضارة الأخرى، يمكنك تكوين عمليات الفحص التلقائي لمحركات الأقراص القابلة للإزالة عند توصيلها بالكمبيوتر. ويحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل عملية التنظيف، يقوم Kaspersky Endpoint Security بحذف الملفات. ويحافظ المكون على الكمبيوتر آمنًا عن طريق إجراء عمليات الفحص التي تنفذ التعلم الآلي والتحليل المساعد على الاكتشاف (المستوى العالي) وتحليل التوقيع. يستخدم Kaspersky Endpoint Security أيضا تقنيتي تحسين الفحص iSwift وiChecker. وتكون هاتان التقنيتان قيد التشغيل دائمًا ولا يمكن تعطيلهما.

كيفية تكوين فحص محركات الأقراص القابلة للإزالة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **المهام المحلية** ← **فحص محركات الأقراص القابلة للإزالة**.
5. في القائمة المنسدلة **الإجراء عند توصيل محرك أقراص قابل للإزالة**، حدد **فحص مفصل** أو **فحص سريع**.
6. كوّن الخيارات المتقدمة لفحص محركات الأقراص القابلة للإزالة (انظر الجدول أدناه).
7. احفظ تغييراتك.

كيفية تكوين فحص محركات الأقراص القابلة للإزالة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Local Tasks** ← **Removable drives scan**.
5. في القائمة المنسدلة **Action when a removable drive is connected**، حدد **Detailed Scan** أو **Quick Scan**.
6. كوّن الخيارات المتقدمة لفحص محركات الأقراص القابلة للإزالة (انظر الجدول أدناه).
7. احفظ تغييراتك.

كيفية تكوين فحص تشغيل محركات الأقراص القابلة للإزالة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. في قائمة المهام، حدد مهمة الفحص وانقر فوق ⚙.

3. استخدم مفتاح التبديل **فحص محركات الأقراص القابلة للإزالة** لتمكين أو تعطيل عمليات فحص محركات الأقراص القابلة للإزالة عند الاتصال بالكمبيوتر.

4. كوّن الخيارات المتقدمة لفحص محركات الأقراص القابلة للإزالة (انظر الجدول أدناه).

5. احفظ تغييراتك.

نتيجة لذلك، يفحص Kaspersky Endpoint Security محركات الأقراص القابلة للإزالة للبحث عن محركات الأقراص القابلة للإزالة التي لا تزيد عن الحجم الأقصى المحدد. إذا لم يتم عرض المهمة فحص محركات الأقراص القابلة للإزالة، فهذا يعني أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

إعدادات مهمة فحص محركات الأقراص القابلة للإزالة

المعلمة	الوصف
الإجراء عند توصيل محرك أقراص قابل للإزالة	**فحص مفصل**. في حالة تحديد هذا العنصر، عند توصيل محرك أقراص قابل للإزالة، يفحص Kaspersky Endpoint Security كل الملفات الموجودة على محرك الأقراص القابل للإزالة، بما في ذلك الملفات المضمنة في الكائنات المركبة والأرشيفات وحزم التوزيع والملفات بتنسيقات Office. ولا يفحص Kaspersky Endpoint Security الملفات بتنسيقات البريد أو الأرشيفات المحمية بكلمة مرور. **فحص سريع**. في حالة تحديد هذا الخيار، بعد توصيل محرك الأقراص القابل للإزالة، يفحص Kaspersky Endpoint Security الملفات من تنسيقات محددة فقط التي تكون أكثر عرضة للإصابة، ولا يفك ضغط الكائنات المركبة.
الحد الأقصى لحجم الأقراص القابلة للإزالة	في حالة تحديد خانة الاختيار هذه، ينفذ Kaspersky Endpoint Security الإجراء المحدد في القائمة المنسدلة **الإجراء عند توصيل محرك أقراص قابل للإزالة** على محركات الأقراص القابلة للإزالة ذات حجم لا يزيد عن الحد الأقصى لحجم محرك الأقراص المحدد. في حالة إلغاء تحديد خانة الاختيار، ينفذ Kaspersky Endpoint Security الإجراء المحدد في القائمة المنسدلة **الإجراء عند توصيل محرك أقراص قابل للإزالة** على محركات الأقراص القابلة للإزالة من أي حجم.
إظهار تقدم الفحص	في حالة تحديد خانة الاختيار، يعرض Kaspersky Endpoint Security مدى تقدم فحص محركات الأقراص القابلة للإزالة في نافذة منفصلة وفي القسم **المهام**. في حالة إلغاء تحديد خانة الاختيار، فإنKaspersky Endpoint Security يجري فحص محركات الأقراص القابلة للإزالة في الخلفية.
منع إيقاف مهمة الفحص	في حالة تحديد خانة الاختيار هذه، فإن مهمة فحص محركات الأقراص القابلة للإزالة في الواجهة المحلية لتطبيق Kaspersky Endpoint Security لا يتوافر بها الزر **إيقاف** في القسم **المهام** والزر **إيقاف** في نافذة فحص محركات الأقراص القابلة للإزالة.

فحص في الخلفية

الفحص في الخلفية هو وضع فحص من Kaspersky Endpoint Security لا يقوم بعرض إخطارات للمستخدم. تتطلب عملية الفحص في الخلفية استخدام موارد أقل من جهاز الكمبيوتر بخلاف أنواع الفحص الأخرى (مثل الفحص الكامل). وفي هذا الوضع يفحص برنامج Kaspersky Endpoint Security كائنات بدء التشغيل ومقطع التمهيد وذاكرة النظام وقسم النظام.

للحفاظ على موارد جهاز الكمبيوتر، يوصى بتشغيل مهمة فحص في الخلفي بدلاً من مهمة الفحص الكاملة. لن يؤثر ذلك على مستوى أمان الكمبيوتر. وهذه المهام تتضمن نطاق الفحص نفسه. ولتحسين الحمل على الكمبيوتر، لا يقوم التطبيق بتشغيل مهمة الفحص الكامل ومهمة الفحص في الخلفية في الوقت نفسه. وإذا قمت بالفعل بتشغيل مهمة فحص كامل، فلن يبدأ Kaspersky Endpoint Security مهمة الفحص في الخلفية لمدة سبعة أيام بعد اكتمال مهمة الفحص الكامل.

تبدأ عملية الفحص في الخلفية في الحالات التالية:

- بعد تحديث قاعدة بيانات مكافحة الفيروسات.
- 30 دقيقة بعد بدء Kaspersky Endpoint Security.
- كل ست ساعات.
- عندما يكون الكمبيوتر في وضع الخمول لمدة خمس دقائق أو أكثر (الكمبيوتر مقفل أو شاشة التوقف قيد التشغيل).

تتم مقاطعة عملية الفحص في الخلفية عندما يكون جهاز الكمبيوتر في وضع الخمول إذا كانت أحد الشروط التالية صحيحة:

- انتقال جهاز الكمبيوتر إلى الوضع النشط.

لا تتم مقاطعة عملية الفحص، إذا لم يتم تشغيل عملية الفحص في الخلفية لمدة تتجاوز العشرة أيام.

- تحول جهاز الكمبيوتر (الكمبيوتر المحمول) إلى وضع البطارية.

عند القيام بعملية الفحص في الخلفية، لا يقوم Kaspersky Endpoint Security بفحص ملفات تم وضع محتوياتها في المحزن السحابي لـ OneDrive.

كيفية تمكين الفحص في الخلفية في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **المهام المحلية** ← **فحص في الخلفية**.
5. استخدم خانة الاختيار **تمكين الفحص في الخلفية** لتمكين عمليات الفحص في الخلفية أو تعطيله.
6. احفظ تغييراتك.

كيفية تمكين الفحص في الخلفية في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Local Tasks** ← **Background scan**.
5. استخدم خانة الاختيار **Enable background scan** لتمكين عمليات الفحص في الخلفية أو تعطيله.
6. احفظ تغييراتك.

كيفية تمكين الفحص في الخلفية في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.
2. في قائمة المهام، حدد مهمة الفحص وانقر فوق ⚙.
3. استخدم مفتاح التبديل **فحص في الخلفية** لتمكين عمليات الفحص في الخلفية أو تعطيلها.
4. احفظ تغييراتك.

إذا لم يتم عرض فحص في الخلفية، فهذا يعني أن المسؤول حظر استخدام المهام المحلية في السياسة.

الفحص من قائمة السياق

يتيح لك برنامج Kaspersky Endpoint Security تشغيل فحص الملفات الفردية من قائمة السياق لفحص الفيروسات والبرمجيات الضارة الأخرى (انظر الشكل أدناه).

عند القيام بعملية الفحص من قائمة السياق، لا يقوم Kaspersky Endpoint Security بفحص ملفات تم وضع محتوياتها في التخزين السحابي لـ OneDrive.

الفحص من قائمة السياق

كيفية تكوين الفحص من قائمة السياق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **المهام المحلية** ← **الفحص من قائمة السياق**.
5. تكوين الفحص من قائمة السياق (انظر الجدول أدناه).
6. احفظ تغييراتك.

كيفية تكوين الفحص من قائمة السياق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Local Tasks** ← **Scan from Context Menu**.

5. تكوين الفحص من قائمة السياق (انظر الجدول أدناه).

6. احفظ تغييراتك.

كيفية تكوين فحص من قائمة السياق في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. في قائمة المهام، حدد مهمة الفحص وانقر فوق ⚙.

3. تكوين الفحص من قائمة السياق (انظر الجدول أدناه).

4. احفظ تغييراتك.

إذا لم يتم عرض مهمة الفحص من قائمة السياق، فهذا يعني أن المسؤول حظر استخدام المهام المحلية في السياسة.

إعدادات الفحص من قائمة سياق المهمة

المعلمة	الوصف
مستوى الأمان	من الممكن أن يستخدم Kaspersky Endpoint Security مجموعات مختلفة من الإعدادات لإجراء فحص. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان: • **مرتفع**. يفحص Kaspersky Endpoint Security كل أنواع الملفات. عند فحص الملفات المركبة، يفحص التطبيق ملفات تنسيق البريد أيضًا. • **مستحسن**. لا يقوم Kaspersky Endpoint Security إلا بفحص تنسيقات ملفات محددة على جميع محركات الأقراص الثابتة وأقراص الشبكة ووسائط التخزين القابلة للإزالة الخاصة بالكمبيوتر، وكذلك كائنات OLE المضمنة. لا يفحص التطبيق الأرشيفات أو حزم التثبيت. • **منخفض**. يفحص Kaspersky Endpoint Security الملفات الجديدة أو المعدلة فقط والتي تحمل الامتدادات الموضحة فقط على جميع محركات الأقراص الثابتة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة على الكمبيوتر. ولا يفحص التطبيق الملفات المركبة.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات. **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا تعذر التنظيف، يضيف Kaspersky Endpoint Security معلومات حول الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة. **إخطار**. في حالة تحديد هذا الخيار، يضيف Kaspersky Endpoint Security المعلومات حول الملفات المصابة إلى قائمة التهديدات النشطة عند اكتشاف هذه الملفات.
أنواع الملفات	

	يعتبر برنامج Kaspersky Endpoint Security الملفات التي بدون امتدادات الملفات القابلة للتنفيذ. ويفحص التطبيق الملفات القابلة للتنفيذ دومًا بغض النظر عن أنواع الملفات التي اخترتها للفحص. **كل الملفات**. إذا تم تمكين هذا الإعداد، فإن Kaspersky Endpoint Security يفحص كل الملفات دون استثناء (كل التنسيقات والامتدادات). **الملفات التي تم فحصها حسب التنسيق**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. قبل فحص أحد الملفات بحثًا عن التعليمات البرمجية الضارة، يتم تحليل العنوان الداخلي للملف لتحديد تنسيق الملف (على سبيل المثال، .txt أو .doc أو .exe). ويبحث الفحص أيضًا عن الملفات بملحقات ملف معينة. **الملفات التي تم فحصها حسب الامتداد**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. ويتم تحديد تنسيق الملف عندئذٍ استنادًا إلى امتداد الملف. افتراضيًا، يفحص Kaspersky Endpoint Security الملفات حسب تنسيقها. يعد فحص الملفات حسب الملحق أقل أمانًا لأن الملف الضار يمكن أن يكون بملحق غير مدرج في قائمة المواد القابلة للإصابة (على سبيل المثال، `.123`).
فحص الملفات الجديدة والتي تم تغييرها فقط	يفحص فقط الملفات الجديدة والملفات التي تم تعديلها منذ آخر مرة لفحصها. هذا يساعد على تقليل فترة الفحص. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.
تخطي الملفات إذا استغرق فحصها أكثر من N من الثواني	ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.
فحص الأرشيفات	فحص تنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE وتنسيقات الأرشيفات الأخرى. يفحص التطبيق الأرشيفات ليس فقط حسب الملحق، لكن أيضًا حسب التنسيق. عند التحقق من الأرشيفات، ينفذ التطبيق عملية تفريغ متكررة. ويسمح هذا باكتشاف التهديدات داخل أرشيفات متعددة المستويات (أرشيف داخل أرشيف).
فحص حزم التوزيع	تقوم خانة الاختيار بتمكين أو تعطيل فحص حزم التوزيع.
فحص الملفات بتنسيقات Microsoft Office	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
فحص تنسيقات البريد الإلكتروني	فحص ملفات تنسيق البريد الإلكتروني وقاعدة بيانات البريد الإلكتروني. يفحص التطبيق ملفات PST وOST المستخدمة بواسطة برنامجي البريد MS Outlook وWindows Mail بالإضافة إلى ملفات EML. لا يدعم Kaspersky Endpoint Security إصدار 64 بت من عميل البريد MS Outlook. وهذا يعني أن Kaspersky Endpoint Security لا يفحص ملفات MS Outlook (ملفات PST وOST) في حالة تثبيت إصدار 64 بت من MS Outlook على الكمبيوتر، حتى إذا كان البريد مضمنًا في نطاق الفحص. وإذا تم تحديد خانة الاختيار، فإن Kaspersky Endpoint Security يقسم ملف تنسيق البريد إلى مكوناته (عنوان ونص ومرفقات) ويقوم بفحصها بحثًا عن التهديدات. إذا تم إلغاء تحديد خانة الاختيار هذه، فإن Kaspersky Endpoint Security يفحص ملف تنسيق البريد على أنه ملف فردي.
فحص الأرشيفات المحمية بكلمة مرور	في حالة تحديد خانة الاختيار، يفحص التطبيق الأرشيفات المحمية بكلمات مرور. قبل فحص الملفات الموجودة في الأرشيف، تتم مطالبتك بإدخال كلمة مرور. في حالة مسح خانة الاختيار، يتخطى التطبيق فحص الأرشيفات المحمية بكلمة مرور.
عدم فك ضغط الملفات المركبة كبيرة الحجم	في حالة تحديد هذا المربع، لا يفحص التطبيق الملفات المركبة إذا كان حجمها يتجاوز القيمة المحددة. في حالة عدم تحديد خانة الاختيار هذه، يفحص التطبيق الملفات المركبة من جميع الأحجام. يفحص التطبيق الملفات الكبيرة التي يتم استخراجها من الأرشيفات بغض النظر عما إذا كانت خانة الاختيار محددة أو لا.
التعلّم الآلي	تستخدم طريقة التعلّم الآلي وتحليل التوقيع قواعد بيانات Kaspersky Endpoint Security التي تحتوي على وصف للتهديدات

وتحليل التوقيع	المعروفة وطرق إبطالها. وتوفر الحماية التي تستخدم هذه الطريقة الحد الأدنى المقبول لمستوى الأمان. بناءً على توصيات خبراء Kaspersky، يتم تمكين التعلّم الآلي وتحليل التوقيع دائمًا.
التحليل المساعد على الاكتشاف	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف. عند فحص الملفات للبحث عن تعليمات برمجية ضارة، ينفذ المحلل المساعد على الاكتشاف الإرشادات الواردة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
تقنية iSwift	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.
تقنية iChecker	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).

مراقبة تكامل التطبيق

يتحقق Kaspersky Endpoint Security من الوحدات النمطية للتطبيق بحثًا عن وجود تلف أو تعديلات. على سبيل المثال، في حالة وجود توقيع رقمي غير صحيح لإحدى مكتبات التطبيق، يتم اعتبار المكتبة تالفة. مهمة التحقق من السلامة مُخصصة للتحقق من ملفات التطبيق. قم بتشغيل مهمة التحقق من السلامة إذا اكتشف برنامج Kaspersky Endpoint Security كائن ضار ولكنه لم يقوم بإبطال مفعوله.

يمكنك إنشاء التحقق من السلامة في Kaspersky Security Center Web Console وفي وحدة تحكم الإدارة. لا يمكن إنشاء مهمة في وحدة التحكم Kaspersky Security Center Cloud Console.

قد تظهر حالات اختراق في سلامة التطبيق وذلك في الحالات التالية:

- قيام كائن ضار بتعديل ملفات خاصة ببرنامج Kaspersky Endpoint Security. في هذه الحالة، قم بالإجراء لاستعادة استخدام الأدوات الخاصة بنظام تشغيل برنامج Kaspersky Endpoint Security. بعد عملية الاستعادة، قم بتشغيل فحص كامل للكمبيوتر وتكرار التحقق من السلامة.
- انتهت صلاحية التوقيع الرقمي. في هذه الحالة، قم بتحديث برنامج Kaspersky Endpoint Security.

كيفية تشغيل فحص التحقق من السلامة لتطبيق من خلال وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (12.1)** ← **التحقق من السلامة**.

الخطوة الثانية: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الثالثة: تكوين جدول بدء المهمة

قم بتكوين جدول لبدء المهمة، على سبيل المثال يدويًا أو عند اكتشاف تفشي فيروس.

الخطوة الرابعة: تحديد اسم المهمة

أدخل اسم المهمة، مثل التحقق من السلامة بعد أن كان الكمبيوتر مصابًا.

الخطوة 5 إكمال إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة. كنتيجة لذلك، سيقوم برنامج Kaspersky Endpoint Security بالتحقق من سلامة التطبيق. ويمكنك أيضًا تكوين جدولة التحقق من سلامة التطبيق في خصائص المهمة (انظر الجدول أدناه).

كيفية تشغيل فحص التحقق من السلامة لتطبيق من خلال وحدة تحكم الويب

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type** حدد **Integrity check**.

c. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، التحقق من سلامة التطبيق بعد إصابة الكمبيوتر.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.

5. أغلق المعالج.

سيتم عرض مهمة جديدة في قائمة المهام.

6. حدد خانة الاختيار المجاورة للمهمة.

كنتيجة لذلك، سيقوم برنامج Kaspersky Endpoint Security بالتحقق من سلامة التطبيق. ويمكنك أيضًا تكوين جدولة التحقق من سلامة التطبيق في خصائص المهمة (انظر الجدول أدناه).

كيفية تشغيل التحقق من السلامة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. يفتح هذا قائمة المهام؛ وحدد مهمة Integrity check وانقر فوق **تشغيل**.

كنتيجة لذلك، سيقوم برنامج Kaspersky Endpoint Security بالتحقق من سلامة التطبيق. ويمكنك أيضًا تكوين جدولة التحقق من سلامة التطبيق في خصائص المهمة (انظر الجدول أدناه). وإذا لم يتم عرض التحقق من السلامة، فهذا يعني أن المسؤول حظر استخدام المهام المحلية في السياسة.

إعدادات مهمة التحقق من السلامة

المعلمة	الوصف
جدولة الفحص	**يدويًا**. وضع التشغيل الذي يمكنك فيه بدء الفحص يدويًا في الوقت الذي يناسبك. **حسب الجدولة**. في وضع تشغيل مهمة الفحص هذه، يبدأ التطبيق تشغيل مهمة الفحص حسب الجدول الذي قمت بإنشائه. في حالة تحديد وضع تشغيل مهمة الفحص هذه، يمكنك أيضًا بدء تشغيل مهمة الفحص يدويًا.
تشغيل المهام التي تم تخطيها	في حالة تحديد خانة الاختيار، يبدأ Kaspersky Endpoint Security في تشغيل مهمة الفحص التي تم تخطيها بمجرد أن يكون هذا الأمر ممكنًا. يمكن تخطي مهمة الفحص، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء مهمة الفحص المجدولة. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل مهام الفحص التي تم تخطيها. كبديل، سيقوم بتشغيل مهمة الفحص التالية بما يتوافق مع الجدول الحالي.
التشغيل فقط عندما يكون	تأجيل بدء مهمة الفحص عندما تكون موارد الكمبيوتر مشغولة. يبدأ Kaspersky Endpoint Security مهمة الفحص إذا كان الكمبيوتر مقفلاً أو إذا كانت شاشة التوقف قيد التشغيل. إذا قاطعت تنفيذ المهمة، على سبيل المثال بواسطة إلغاء تأمين الكمبيوتر، يجري Kaspersky Endpoint Security تشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقفت عندها.

الكمبيوتر خاملاً	

تحرير نطاق الفحص

نطاق الفحص عبارة عن قائمة بالمسارات إلى المجلدات والمسارات التي يفحصها Kaspersky Endpoint Security عند تنفيذ المهمة. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع.

لتحرير نطاق الفحص، نوصي باستخدام المهمة فحص مخصص. وينصحك خبراء Kaspersky بعدم تغيير نطاق الفحص لمهام فحص كامل وفحص المناطق الحرجة.

يحتوي Kaspersky Endpoint Security على الكائنات التالية المحددة مسبقًا كجزء من نطاق الفحص:

- **بريدي الإلكتروني**.

  الملفات ذات الصلة بعميل بريد Outlook: ملفات البيانات (PST)، ملفات البيانات غير المتصلة (OST).

- **ذاكرة النظام**.

- **كائنات بدء التشغيل**.

  الذاكرة التي تَشغلها العمليات والملفات القابلة للتنفيذ الخاصة بالتطبيق والتي يتم تشغيلها عند بدء تشغيل النظام.

- **مقاطع تمهيد القرص**.

  القرص الصلب وقطاعات تمهيد القرص القابل للإزالة.

- **النسخ الاحتياطي للنظام**.

  محتويات المجلد System Volume Information.

- **جميع الأجهزة الخارجية**.

- **كل محركات الأقراص الثابتة**.

- **كل محركات أقراص الشبكة**.

نوصي بإنشاء مهمة فحص منفصلة لفحص محركات أقراص الشبكة أو المجلدات المشتركة. في مهمة فحص البرامج الضارة، حدد مستخدمًا يمتلك حق الوصول للكتابة إلى محرك الأقراص هذا؛ وهذا ضروري للتخفيف من التهديدات المكتشفة. وإذا كان الخادم الذي يوجد به محرك أقراص الشبكة يحتوي على أدوات أمان خاصة به، فلا تقم بتشغيل مهمة الفحص لمحرك الأقراص هذا. وبهذه الطريقة، يمكنك تجنب فحص الكائن مرتين وتحسين أداء الخادم.

لاستبعاد المجلدات أو الملفات من نطاق الفحص، أضف المجلد أو الملف إلى المنطقة الموثوقة.

كيفية إنشاء نطاق الفحص في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **المهام**.

3. حدد مهمة الفحص وانقر نقرًا مزدوجًا لفتح خصائص المهمة.
إذا لزم الأمر، أنشئ مهمة فحص البرامج الضارة.

4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.

5. في القسم **نطاق الفحص**، انقر فوق **الإعدادات**.

6. في النافذة التي تفتح، حدد الكائنات التي تريد إضافتها إلى نطاق الفحص أو استثنائها منه.

7. إذا كنت تريد إضافة كائن جديد لنطاق الفحص:

   a. انقر على **إضافة**.

   b. في الحقل **الكائن**، أدخل المسار إلى المجلد أو الملف.
   استخدم الأقنعة:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.
- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.
- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

يمكنك استخدام الأقنعة في أي مكان في مسار الملف أو المجلد. على سبيل المثال، إذا كنت تريد أن يتضمن نطاق الفحص مجلد Downloads لجميع حسابات المستخدمين على الكمبيوتر، فأدخل القناع `C:\Users\*\Downloads\`.

يمكنك استثناء كائن من عمليات الفحص دون حذفه من قائمة الكائنات في نطاق الفحص. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

8. احفظ تغييراتك.

كيفية إنشاء نطاق الفحص في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.

نافذة خصائص المهمة. إذا لزم الأمر، أنشئ مهمة فحص البرامج الضارة.

3. حدد علامة التبويب **Application settings**.

4. في القسم **Scan scope**، حدد الكائنات التي تريد إضافتها إلى نطاق الفحص أو استثنائها منه.

5. إذا كنت تريد إضافة كائن جديد لنطاق الفحص:

a. انقر فوق الزر **إضافة**.

b. في الحقل **Path**، أدخل المسار إلى المجلد أو الملف.

استخدم الأقنعة:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

يمكنك استخدام الأقنعة في أي مكان في مسار الملف أو المجلد. على سبيل المثال، إذا كنت تريد أن يتضمن نطاق الفحص مجلد Downloads لجميع حسابات المستخدمين على الكمبيوتر، فأدخل القناع `C:\Users\*\Downloads\`.

يمكنك استثناء كائن من عمليات الفحص دون حذفه من قائمة الكائنات في نطاق الفحص. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.

6. احفظ تغييراتك.

كيفية تحرير نطاق فحص في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. يفتح هذا قائمة المهام؛ وحدد مهمة فحص مخصص وانقر فوق **تحديد**.

يمكنك أيضًا تحرير نطاق الفحص لمهام أخرى. وينصحك خبراء Kaspersky بعدم تغيير نطاق الفحص لمهام فحص كامل وفحص المناطق الحرجة.

3. في النافذة التي تفتح، حدد الكائنات التي تريد إضافتها إلى نطاق الفحص.

4. احفظ تغييراتك.

إذا لم يتم عرض مهمة الفحص، فيعني هذا أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

إجراء فحص مجدول

يستغرق فحص الكمبيوتر بالكامل بعض الوقت والموارد من الكمبيوتر. ويجب عليك اختيار الوقت الأمثل لإجراء فحص للكمبيوتر لتجنب التأثير سلبًا على أداء البرامج الأخرى. ويتيح لك Kaspersky Endpoint Security تكوين جدولة عادية لفحص الكمبيوتر. ويعد هذا مناسبًا إذا كانت مؤسستك لديها جدول عمل. ويمكنك تكوين فحص للكمبيوتر لتشغيله ليلاً أو في عطلات نهاية الأسبوع. إذا استحال تشغيل مهمة الفحص لأي سبب (على سبيل المثال: عدم تشغيل الكمبيوتر في ذلك الوقت)، يمكنك تكوين المهمة التي تم تخطيها لتبدأ تلقائيًا في أقرب وقت ممكن.

وإذا ثبت أن تكوين جدولة فحص مثالي أمر مستحيل، يتيح لك Kaspersky Endpoint Security إجراء فحص للكمبيوتر عند استيفاء الشروط الخاصة التالية:

- بعد تحديث قاعدة البيانات.

  يُجري Kaspersky Endpoint Security فحص الكمبيوتر باستخدام قواعد بيانات التوقيع المحدثة.

- بعد بدء تشغيل التطبيق.

  يُجري Kaspersky Endpoint Security فحصًا للكمبيوتر عند انقضاء فترة زمنية محددة بعد بدء تشغيل التطبيق. عند بدء تشغيل نظام التشغيل، يتم تشغيل العديد من العمليات، لذلك من المفيد تأجيل تشغيل مهمة الفحص بدلاً من تشغيلها فور بدء تشغيل Kaspersky Endpoint Security.

- التشغيل عن بُعد عبر الشبكة المحلية.

  يُجري Kaspersky Endpoint Security فحصًا للكمبيوتر وفقًا للجدولة حتى في حالة إيقاف تشغيل الكمبيوتر. ولفعل ذلك، يستخدم التطبيق ميزة التشغيل عن بُعد عبر الشبكة المحلية في نظام التشغيل. وتتيح ميزة التشغيل عن بُعد عبر الشبكة المحلية تشغيل الكمبيوتر عن بُعد بواسطة إرسال إشارة خاصة عبر الشبكة المحلية. ولاستخدام هذه الميزة، يجب تمكين التشغيل عن بُعد عبر الشبكة المحلية في إعدادات BIOS.

  ويمكنك تكوين تشغيل الفحص باستخدام التشغيل عن بُعد عبر الشبكة المحلية فقط لمهمة فحص البرامج الضارة في Kaspersky Security Center. ولا يمكنك تمكين التشغيل عن بُعد عبر الشبكة المحلية لفحص الكمبيوتر في واجهة التطبيق.

- عندما يكون الكمبيوتر في وضع الخمول.

  يُجري Kaspersky Endpoint Security فحصًا للكمبيوتر وفقًا للجدولة عندما تكون شاشة التوقف نشطة أو تكون الشاشة مقفلة. وإذا ألغى المستخدم قفل الكمبيوتر، يوقف Kaspersky Endpoint Security الفحص مؤقتًا. ويعني هذا أن التطبيق قد يستغرق عدة أيام لإكمال فحص الكمبيوتر بالكامل.

كيفية تكوين جدولة الفحص في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **المهام**.
3. حدد مهمة الفحص وانقر نقرًا مزدوجًا لفتح خصائص المهمة.

   إذا لزم الأمر، أنشئ مهمة فحص البرامج الضارة.
4. من نافذة خصائص الكمبيوتر، حدد القسم **جدولة**.
5. تكوين جدول مهمة الفحص.
6. بناءً على التكرار الذي تم تحديده، كوّن الإعدادات المتقدمة التي تحدد جدول تشغيل المهمة (انظر الجدول أدناه).
7. احفظ تغييراتك.

كيفية تكوين جدولة الفحص في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.

نافذة خصائص المهمة.

3. حدد علامة التبويب **Schedule**.

4. تكوين جدول مهمة الفحص.

5. بناءً على التكرار الذي تم تحديده، كوّني الإعدادات المتقدمة التي تحدد جدول تشغيل المهمة (انظر الجدول أدناه).

6. احفظ تغييراتك.

كيفية تكوين جدولة الفحص في واجهة التطبيق

يمكنك تكوين جدولة الفحص فقط إذا لم يتم تطبيق سياسة على الكمبيوتر. ولأجهزة الكمبيوتر الخاضعة للسياسة، يمكنك تكوين جدولة مهمة فحص البرامج الضارة في Kaspersky Security Center.

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. في قائمة المهام، حدد مهمة الفحص وانقر فوق ⚙.

يمكنك تكوين جدولة لتشغيل فحص كامل أو فحص المناطق الحرجة أو التحقق من السلامة. ويمكنك فقط تشغيل فحص مخصص يدويًا.

3. انقر على **جدولة الفحص**.

4. في النافذة التي تفتح، كوّن جدول تشغيل مهمة الفحص.

5. بناءً على التكرار الذي تم تحديده، كوّني الإعدادات المتقدمة التي تحدد جدول تشغيل المهمة (انظر الجدول أدناه).

6. احفظ تغييراتك.

إعدادات جدولة الفحص

المعلمة	الوصف
جدولة الفحص	**يدويًا**. وضع التشغيل الذي يمكنك فيه بدء الفحص يدويًا في الوقت الذي يناسبك. **حسب الجدولة**. في وضع تشغيل مهمة الفحص هذه، يبدأ التطبيق تشغيل مهمة الفحص حسب الجدول الذي قمت بإنشائه. في حالة تحديد وضع تشغيل مهمة الفحص هذه، يمكنك أيضًا بدء تشغيل مهمة الفحص يدويًا.
تأجيل التشغيل بعد بدء التطبيق لمدة N دقيقة	تأجيل بدء مهمة الفحص بعد بدء تشغيل التطبيق. عند بدء تشغيل نظام التشغيل، يتم تشغيل العديد من العمليات، لذلك من المفيد تأجيل تشغيل مهمة الفحص بدلاً من تشغيلها فور بدء تشغيل Kaspersky Endpoint Security.
تشغيل المهام التي تم تخطيها	في حالة تحديد خانة الاختيار، يبدأ Kaspersky Endpoint Security في تشغيل مهمة الفحص التي تم تخطيها بمجرد أن يكون هذا الأمر ممكنًا. يمكن تخطي مهمة الفحص، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء مهمة الفحص المجدولة. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل مهام الفحص التي تم تخطيها. كبديل، سيقوم بتشغيل مهمة الفحص التالية بما يتوافق مع الجدول الحالي.
التشغيل فقط عندما يكون	تأجيل بدء مهمة الفحص عندما تكون موارد الكمبيوتر مشغولة. يبدأ Kaspersky Endpoint Security مهمة الفحص إذا كان الكمبيوتر مقفلاً أو إذا كانت شاشة التوقف قيد التشغيل. إذا قاطعت تنفيذ المهمة، على سبيل المثال بواسطة إلغاء تأمين الكمبيوتر،

الكمبيوتر خاملاً	يجري Kaspersky Endpoint Security تشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقفت عندها.
استخدم التأخير العشوائي لبدء المهام تلقائيًا (متوفر فقط في Kaspersky Security Center (Console	في حالة تحديد خانة الاختيار، لن يتم تشغيل المهمة بدقة وفقًا للجدولة، لكن بشكل عشوائي خلال فترة زمنية معينة، أي يتم توزيع أوقات بدء المهمة. وتساعد أوقات البدء العشوائية في تجنب وصول عدد كبير من أجهزة الكمبيوتر إلى خادم الإدارة في الوقت نفسه عند تشغيل المهمة في الموعد المحدد. يتم حساب نطاق أوقات البدء العشوائية تلقائيًا عند إنشاء المهمة، اعتمادًا على عدد أجهزة الكمبيوتر التي تم تعيين المهمة لها. وبعد ذلك، يتم تشغيل المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، عندما يتم تعديل إعدادات المهمة أو تشغيل المهمة يدويًا، يتغير وقت البدء المحسوب. في حالة إلغاء تحديد خانة الاختيار، يتم تشغيل المهمة بالضبط في الوقت المجدول.
أوقف المهمة إذا كانت تعمل لمدة أطول من N (دقيقة) (متوفر فقط في Kaspersky Security Center (Console	تقييد وقت تنفيذ المهمة – بعد مقدار الوقت المحدد، يوقف Kaspersky Endpoint Security المهمة. ولا تُوضع علامة على المهمة كمكتملة. وفي المرة القادمة التي يُشغل فيها Kaspersky Endpoint Security المهمة، سيتم تشغيلها من البداية وفي الموعد المحدد وفق الجدولة. لتقليل وقت تنفيذ المهمة، يمكنك، على سبيل المثال، تكوين نطاق الفحص أو تحسين الفحص.
تفعيل الجهاز قبل بدء المهمة عبر Wake On LAN (بالدقائق) (متوفر فقط في Kaspersky Security Center (Console	في حالة تحديد خانة الاختيار، سيتم منح نظام تشغيل الكمبيوتر مهلة زمنية محددة لإكمال بدء التشغيل قبل تشغيل المهمة. المهلة الافتراضية 5 دقائق. حدد خانة الاختيار إذا كنت تريد تشغيل المهمة على كل أجهزة الكمبيوتر بما في ذلك أجهزة الكمبيوتر التي تم إيقاف تشغيلها.

إجراء فحص كمستخدم مختلف

بشكل افتراضي، يتم تشغيل مهمة الفحص باسم المستخدم الذي سجلتَ باستخدام حقوقه في نظام التشغيل. وقد يشمل نطاق الحماية محركات أقراص الشبكة أو كائنات أخرى تتطلب حقوقًا خاصة للوصول. يمكنك تحديد مستخدم يمتلك الحقوق المطلوبة في إعدادات التطبيق وتشغيل مهمة الفحص تحت حساب هذا المستخدم.

يمكنك إجراء عمليات الفحص التالية كمستخدم مختلف:

- فحص المناطق الحرجة.
- فحص كامل.
- فحص مخصص.
- الفحص من قائمة السياق.

لا يمكنك تكوين حقوق المستخدم لتشغيل فحص محركات الأقراص القابلة للإزالة أو فحص في الخلفية أو التحقق من السلامة.

كيفية تشغيل فحص كمستخدم مختلف في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في مجلد **الأجهزة المدارة** الخاص بشجرة وحدة تحكم الإدارة، افتح المجلد الذي يحمل اسم مجموعة الإدارة التي تنتمي إليها أجهزة الكمبيوتر العميلة ذات الصلة.

3. في مساحة العمل، حدد علامة التبويب **المهام**.

4. حدد مهمة الفحص وانقر نقرًا مزدوجًا لفتح خصائص المهمة.

5. من نافذة خصائص المهمة، حدد القسم **الحساب**.

6. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل مهمة فحص.

7. احفظ تغييراتك.

كيفية تشغيل فحص كمستخدم مختلف في Web Console أو Cloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Tasks** ← **Devices**.
تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.
نافذة خصائص المهمة.

3. حدد علامة التبويب **Settings**.

4. في القسم **Account** انقر على **Settings**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل مهمة فحص.

6. احفظ تغييراتك.

كيفية تشغيل فحص كمستخدم مختلف في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. في قائمة المهام، حدد مهمة الفحص وانقر فوق ⚙.

3. في خصائص المهمة، حدد **إعدادات متقدمة** ← **تشغيل الفحص باسم**.

4. في النافذة التي تفتح، أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل مهمة فحص.

5. احفظ تغييراتك.

إذا لم يتم عرض مهمة الفحص، فيعني هذا أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

تحسين الفحص

يمكنك تحسين فحص الملفات: تقليل وقت الفحص وزيادة سرعة تشغيل أمان نقطة النهاية من Kaspersky. يمكن تحقيق ذلك عن طريق فحص الملفات الجديدة والملفات التي تم تعديلها فقط منذ إجراء الفحص السابق. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة. ويمكنك أيضًا تعيين حد لفحص ملف واحد. عند انتهاء الفاصل الزمني المحدد، سيقوم Kaspersky Endpoint Security باستثناء الملف من الفحص الحالي (فيما عدا الأرشيف والكائنات التي تتكون من عدة ملفات).

يعتبر زرع الفيروسات والبرامج الضارة في الملفات المركّبة، مثل ملفات الأرشيف أو قواعد البيانات من الأساليب الشائعة لإخفاء الفيروسات والبرمجيات الضارة الأخرى. ولاكتشاف الفيروسات والبرمجيات الضارة الأخرى المختبئة بهذه الطريقة، يجب فك حزمة الملف المركب، وهو الأمر الذي قد يؤدي إلى إبطاء عملية الفحص. يمكنك تقييد أنواع الملفات المركبة المطلوب فحصها، وبالتالي زيادة سرعة عملية الفحص.

يمكنك أيضًا تمكين استخدام تقنيات iChecker وiSwift. إن تقنيتي iChecker and iSwift يعملان على زيادة سرعة عملية فحص الملفات عن طريق استثناء الملفات التي لم يتم تعديلها منذ إجراء آخر فحص.

كيفية تحسين الفحص في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **المهام**.

3. حدد مهمة الفحص وانقر نقرًا مزدوجًا لفتح خصائص المهمة.

إذا لزم الأمر، أنشئ مهمة فحص البرامج الضارة.

4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.

5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة إعدادات مهمة الفحص.

6. في القسم **تحسين الفحص**، كوّن إعدادات الفحص:

- **فحص الملفات الجديدة والتي تم تغييرها فقط**. يفحص فقط الملفات الجديدة والملفات التي تم تعديلها منذ آخر مرة لفحصها. هذا يساعد على تقليل فترة الفحص. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.

  يمكنك أيضًا تكوين فحص الملفات الجديدة حسب النوع. على سبيل المثال، يمكنك فحص جميع حزم التوزيع وفحص الأرشيفات الجديدة وملفات تنسيق Office فقط.

- **تخطي الملفات التي تم فحصها لأكثر من N ثانية**. ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.

- **عدم تشغيل مهام فحص متعددة في الوقت نفسه**. يتم تأجيل بدء مهام الفحص إذا كان الفحص قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص الجديدة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، لنفترض أن التطبيق بدأ مهمة فحص كامل وفقًا للجدولة. إذا حاول المستخدم بدء فحص سريع من واجهة التطبيق، سوف يُدرج Kaspersky Endpoint Security مهمة الفحص السريع هذه في قائمة الانتظار ثم يبدأ هذه المهمة تلقائيًا بعد انتهاء مهمة الفحص الكامل.

7. انقر على **إضافي**.

يفتح هذا نافذة إعدادات فحص الملفات المركبة.

8. في القسم **حد الحجم**، حدد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم**. ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.

يفحص Kaspersky Endpoint Security الملفات كبيرة الحجم التي يتم استخراجها من الأرشيفات، بغض النظر عن تحديد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم** أم لا.

9. انقر على **موافق**.

10. حدد علامة التبويب **إضافي**.

11. في القسم **تقنيات الفحص**، حدد خانات الاختيار المجاورة لأسماء التقنيات التي ترغب في استخدامها أثناء الفحص:

- **تقنية iSwift**. تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.

- **تقنية iChecker**. تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).

12. احفظ تغييراتك.

كيفية تحسين الفحص في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.

نافذة خصائص المهمة. إذا لزم الأمر، أنشئ مهمة فحص البرامج الضارة.

3. حدد علامة التبويب **Application settings**.

4. في القسم **Action on threat detection**، حدد خانة الاختيار **Scan only new and modified files**. يفحص فقط الملفات الجديدة والملفات التي تم تعديلها منذ آخر مرة لفحصها. هذا يساعد على تقليل فترة الفحص. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.

يمكنك أيضًا تكوين فحص الملفات الجديدة حسب النوع. على سبيل المثال، يمكنك فحص جميع حزم التوزيع وفحص الأرشيفات الجديدة وملفات تنسيق Office فقط.

5. في القسم **Scan optimization**، حدد خانة الاختيار **Do not unpack large compound files**. ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.

يفحص Kaspersky Endpoint Security الملفات كبيرة الحجم التي يتم استخراجها من الأرشيفات، بغض النظر عن تحديد خانة الاختيار **Do not unpack large compound files** أم لا.

6. حدد خانة الاختيار **Do not run multiple scan tasks at the same time**. يتم تأجيل بدء مهام الفحص إذا كان الفحص قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص الجديدة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، لنفترض أن التطبيق بدأ مهمة فحص كامل وفقًا للجدولة. إذا حاول المستخدم بدء فحص سريع من واجهة التطبيق، سوف يُدرج Kaspersky Endpoint Security مهمة الفحص السريع هذه في قائمة الانتظار ثم يبدأ هذه المهمة تلقائيًا بعد انتهاء مهمة الفحص الكامل.

7. في القسم **Advanced settings**، حدد خانة الاختيار **Skip files that are scanned for longer than N ثانية**. ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.

8. احفظ تغييراتك.

كيفية تحسين الفحص في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **المهام**.

2. في قائمة المهام، حدد مهمة الفحص وانقر فوق ⚙.

3. انقر على **إعدادات متقدمة**.

4. في القسم **تحسين الفحص**، كوّن إعدادات الفحص:

- **فحص الملفات الجديدة والتي تم تغييرها فقط**. يفحص فقط الملفات الجديدة والملفات التي تم تعديلها منذ آخر مرة لفحصها. هذا يساعد على تقليل فترة الفحص. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.

  يمكنك أيضًا تكوين فحص الملفات الجديدة حسب النوع. على سبيل المثال، يمكنك فحص جميع حزم التوزيع وفحص الأرشيفات الجديدة وملفات تنسيق Office فقط.

- **تخطي الملفات إذا استغرق فحصها أكثر من N من الثواني**. ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.

- **عدم تشغيل مهام فحص متعددة في الوقت نفسه**. يتم تأجيل بدء مهام الفحص إذا كان الفحص قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص الجديدة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، لنفترض أن التطبيق بدأ مهمة فحص كامل وفقًا للجدولة. إذا حاول المستخدم بدء فحص سريع من واجهة التطبيق، سوف يُدرج Kaspersky Endpoint Security مهمة الفحص السريع هذه في قائمة الانتظار ثم يبدأ هذه المهمة تلقائيًا بعد انتهاء مهمة الفحص الكامل.

5. في القسم **حد الحجم**، حدد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم**. ويحدد هذا حد الوقت لفحص كائن واحد. وبعد مدة زمنية معينة، يتوقف التطبيق عن فحص الملف. هذا يساعد على تقليل فترة الفحص.

يفحص Kaspersky Endpoint Security الملفات كبيرة الحجم التي يتم استخراجها من الأرشيفات، بغض النظر عن تحديد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم** أم لا.

6. في القسم **تقنيات الفحص**، حدد خانات الاختيار المجاورة لأسماء التقنيات التي ترغب في استخدامها أثناء الفحص:

- **تقنية iSwift**. تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.

- **تقنية iChecker**. تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).

7. احفظ تغييراتك.

إذا لم يتم عرض مهمة الفحص، فيعني هذا أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق

يضمن تحديث قواعد بيانات Kaspersky Endpoint Security والوحدات النمطية للتطبيق الخاصة به توفير أحدث حماية متوفرة على الكمبيوتر الخاص بك. تظهر بصفة يومية فيروسات جديدة وأنواع أخرى من البرمجيات الضارة على مستوى العالم. وتحتوي قواعد بيانات Kaspersky Endpoint Security على معلومات حول التهديدات وطرق تحييدها. ولاكتشاف التهديدات بسرعة، يجب أن تهتم بتحديث قواعد البيانات والوحدات النمطية للتطبيق بانتظام.

تحتاج التحديثات المنتظمة ترخيص ساريًا. في حالة عدم وجود ترخيص موجود، سيكون بإمكانك إجراء تحديث لمرة واحدة فقط.

وتعتبر خوادم تحديث Kaspersky هي المصدر الرئيسي لتحديث Kaspersky Endpoint Security.

يجب توصيل جهاز الكمبيوتر الخاص بك إلى الإنترنت لتتمكن من تنزيل حزمة التحديثات من خوادم تحديث Kaspersky بنجاح. وافتراضيًا، يتم تحديد إعدادات توصيل الإنترنت تلقائيًا. إذا كنت تستخدم خادمًا وكيلاً، فأنت بحاجة إلى تكوين إعدادات الخادم الوكيل.

يتم تنزيل التحديثات عبر بروتوكول HTTPS. قد يتم تنزيلهم أيضًا عبر بروتوكول HTTP عند استحالة تنزيل التحديثات عبر بروتوكول HTTPS.

أثناء تنفيذ التحديث، يتم تنزيل الكائنات التالية وتثبيتها على جهاز الكمبيوتر الخاص بك:

- قواعد بيانات Kaspersky Endpoint Security. يتم توفير حماية الكمبيوتر باستخدام قواعد البيانات التي تحتوي على توقيعات الفيروسات والتهديدات الأخرى ومعلومات حول طرق إبطالها. كما تقوم مكونات الحماية باستخدام هذه المعلومات عند البحث عن الملفات المصابة الموجودة على الكمبيوتر الخاص بك وتحييدها. يتم تحديث قواعد البيانات باستمرار وتزويدها بسجلات التهديدات الجديدة وطرق مواجهتها. لذا، نوصي بتحديث قواعد البيانات بانتظام.

  وبالإضافة إلى قواعد بيانات Kaspersky Endpoint Security، يتم تحديث برامج تشغيل الشبكة التي تقوم بتمكين مكونات التطبيق لاعتراض حركة مرور الاتصال.

- الوحدات النمطية للتطبيق. بالإضافة إلى قواعد بيانات برنامج Kaspersky Endpoint Security، يمكنك أيضًا تحديث الوحدات النمطية للتطبيق. ويؤدي تحديث الوحدات النمطية للتطبيق إلى إصلاح نقاط الضعف الموجودة في برنامج Kaspersky Endpoint Security، مع إضافة وظائف جديدة أو تحسين الوظائف الموجودة بالفعل.

خلال التحديث، تتم مقارنة قواعد البيانات والوحدات النمطية للتطبيق الموجودة على جهاز الكمبيوتر الخاص بك مع الإصدار الحديث الموجود على مصدر التحديث. في حالة وجود اختلاف بين قواعد البيانات والوحدات النمطية للتطبيق الموجودة لديك حاليًا على الكمبيوتر عن الإصدارات الحديثة الموجودة على مصدر التحديث، يتم تثبيت الجزء المفقود من التحديثات على جهاز الكمبيوتر الخاص بك.

يمكن تحديث ملفات تعليمات السياق جنبًا إلى جنب مع تحديثات الوحدة النمطية للتطبيق.

إذا كانت قواعد البيانات قديمة، فقد تكون حزمة التحديثات كبيرة، وهو ما قد يتسبب في زيادة حركة الإنترنت (بما يصل إلى عشرات الميجابايت).

يتم عرض معلومات حول الحالة الحالية لقواعد بيانات Kaspersky Endpoint Security في نافذة التطبيق الرئيسية أو تلميح الأدوات الذي تراه عند تحريك المؤشر فوق أيقونة التطبيق في منطقة الإخطارات.

يتم تسجيل المعلومات الخاصة بنتائج التحديث وجميع الأحداث التي تقع أثناء تنفيذ مهمة التحديث في تقرير Kaspersky Endpoint Security.

سيناريوهات تحديثات وحدات التطبيق وقواعد البيانات

يضمن تحديث قواعد بيانات Kaspersky Endpoint Security والوحدات النمطية للتطبيق الخاصة به توفير أحدث حماية متوفرة على الكمبيوتر الخاص بك. تظهر بصفة يومية فيروسات جديدة وأنواع أخرى من البرمجيات الضارة على مستوى العالم. وتحتوي قواعد بيانات Kaspersky Endpoint Security على معلومات حول التهديدات وطرق تحييدها. ولاكتشاف التهديدات بسرعة، يجب أن تهتم بتحديث قواعد البيانات والوحدات النمطية للتطبيق بانتظام.

تم تحديث الكائنات التالية على أجهزة الكمبيوتر الخاصة بالمستخدمين:

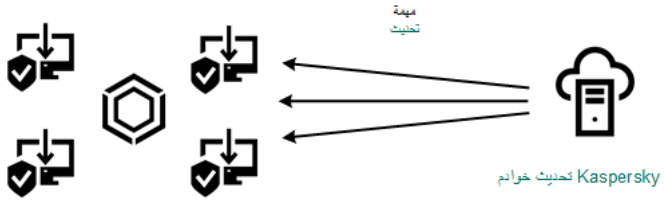
- قواعد بيانات مكافحة الفيروسات. تتضمن قواعد بيانات مكافحة الفيروسات قواعد بيانات لتوقيعات البرمجيات الضارة، ووصفًا للهجمات على الشبكة، وقواعد بيانات لعناوين الويب الضارة والاحتيالية، وقواعد بيانات الشعارات، وقواعد بيانات اكتشاف البريد غير المرغوب فيه، وبيانات أخرى.

- الوحدات النمطية للتطبيق. تهدف تحديثات الوحدة النمطية إلى إزالة الثغرات الأمنية في التطبيق وتحسين أساليب حماية الكمبيوتر. قد تقوم تحديثات الوحدة النمطية بتغيير سلوك مكونات التطبيق وإضافة إمكانات جديدة.

يدعم برنامج Kaspersky Endpoint Security السيناريوهات التالية لتحديث قواعد البيانات والوحدات النمطية للتطبيق:

- التحديث من خوادم Kaspersky.

تقع خوادم التحديث الخاصة بـ Kaspersky في العديد من البلدان في جميع أنحاء العالم. هذا يضمن موثوقية مرتفعة للتحديثات. إذا تعذر إجراء تحديث من خادم واحد ينتقل Kaspersky Endpoint Security إلى الخادم التالي.



التحديث من خوادم Kaspersky

- التحديث المركزي.

يعمل التحديث المركزي على تقليل عدد حركة المرور الخارجية للإنترنت الإنترنت ويوفر إمكانية المراقبة المناسبة للتحديث.

يتكون التحديث المركزي من الخطوات التالية:

1. قم بتنزيل حزمة التحديث إلى المستودع ضمن شبكة المؤسسة.

تم تنزيل حزمة التحديث للمستودع عن طريق مهمة خادم الإدارة المُسمى تنزيل تحديثات لمستودع خادم الإدارة.

2. قم بتنزيل حزمة التحديث إلى مجلد مشترك (اختياري).

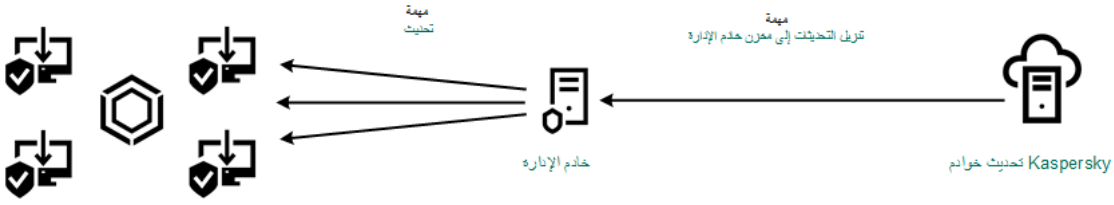
يمكنك تنزيل حزمة التحديث إلى مجلد مشترك باستخدام الطرق التالية:

- استخدام مهمة تحديث الخاصة ببرنامج Kaspersky Endpoint Security. المهمة مخصصة لأحد أجهزة الكمبيوتر الموجود في شبكة الشركة المحلية.

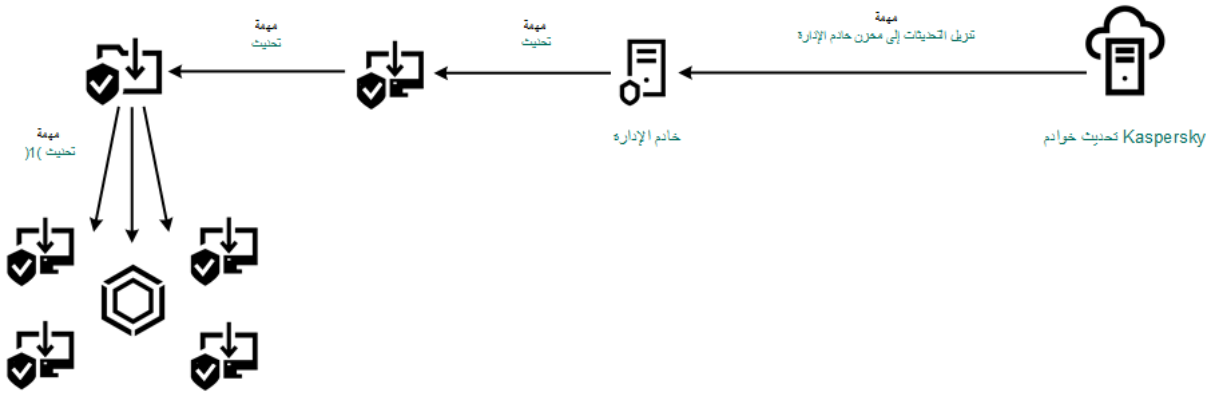
- باستخدام الأداة المساعدة Kaspersky Update Utility. للحصول على معلومات تفصيلية حول استخدام Kaspersky Update Utility، يُرجى الرجوع إلى قاعدة معارف Kaspersky.

3. قم بتوزيع حزمة التحديث على أجهزة الكمبيوتر العميلة.

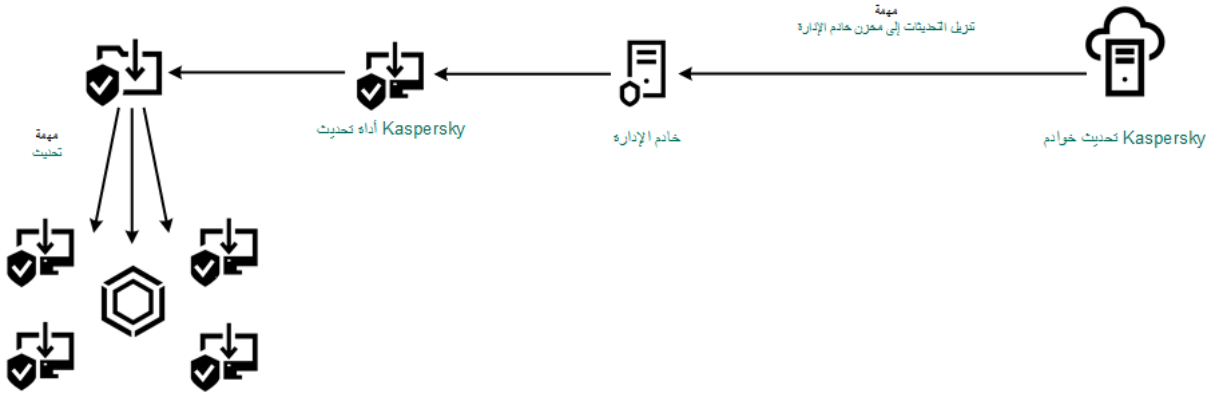
يتم توزيع حزمة التحديث على أجهزة الكمبيوتر العميلة بواسطة مهمة تحديث الخاصة ببرنامج Kaspersky Endpoint Security. يمكنك إنشاء عدد غير محدود من مهام التحديث لكل مجموعة إدارة.



التحديث من مستودع الخادم



التحديث من مجلد مشترك



التحديث باستخدام برنامج Kaspersky Update Utility

بالنسبة إلى Web Console، تتضمن القائمة الافتراضية لمصادر التحديث خادم إدارة Kaspersky Security Center وخوادم التحديث الخاصة بـ Kaspersky. بالنسبة لوحدة التحكم Kaspersky Security Center Cloud Console، تشتمل القائمة الافتراضية لمصادر التحديث على نقاط التوزيع وخوادم تحديث Kaspersky. وللمزيد من التفاصيل حول نقاط التوزيع، يُرجى الرجوع إلى تعليمات Kaspersky Security Center Cloud Console. يمكنك إضافة مصادر تحديث إلى القائمة. ويمكنك تحديد خوادم HTTP/FTP ومجلدات مشتركة كمصادر تحديث. إذا تعذر إجراء تحديث من مصدر تحديث واحد، ينتقل Kaspersky Endpoint Security إلى المصدر التالي.

يتم تنزيل التحديثات من خوادم تحديث Kaspersky أو من خوادم FTP أو HTTP الأخرى عبر بروتوكولات الشبكة القياسية. إذا كان الاتصال بالخادم الوكيل مطلوبًا للوصول إلى مصدر التحديث، فحدد إعدادات الخادم الوكيل في إعدادات سياسة برنامج Kaspersky Endpoint Security.

التحديث من مستودع الخادم

للحفاظ على حركة الإنترنت، يمكنك تكوين تحديثات قواعد البيانات ووحدات التطبيق على أجهزة كمبيوتر الشبكة المحلية للمؤسسة من مستودع الخادم. لهذا الغرض يجب أن يقوم Kaspersky Security Center بتنزيل حزمة تحديث إلى المستودع (FTP أو خادم HTTP أو الشبكة أو المجلد المحلي) من خوادم تحديث Kaspersky. ستتمكن أجهزة الكمبيوتر الأخرى المحلية للمؤسسة LAN من استلام حزمة التحديث من مستودع الخادم.

تكوين تحديثات قواعد البيانات ووحدات التطبيق من مستودع الخادم يتكون من الخطوات التالية:

1. قم بتكوين تنزيل حزمة التحديث على مستودع خادم الإدارة (مهمة تنزيل التحديثات على مستودع خادم الإدارة).

يتم إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة تلقائيًا بواسطة معالج البدء السريع لخادم الإدارة، ولا يمكن أن تتضمن هذه المهمة سوى مثيل واحد. وبشكل افتراضي، ينسخ Kaspersky Security Center حزمة التحديث إلى المجلد `\\<server name>\KLSHARE\Updates`. وللمزيد من المعلومات عن تنزيل التحديثات إلى مستودع خادم الإدارة، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

2. قم بتكوين تحديثات قاعدة البيانات ووحدة التطبيق من مخزن الخادم المحدد إلى أجهزة الكمبيوتر المتبقية على شبكة LAN الخاصة بالمنظمة (مهمة تحديث).

كيفية تكوين تحديث Kaspersky Endpoint Security من مخزن الخادم المحدد في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

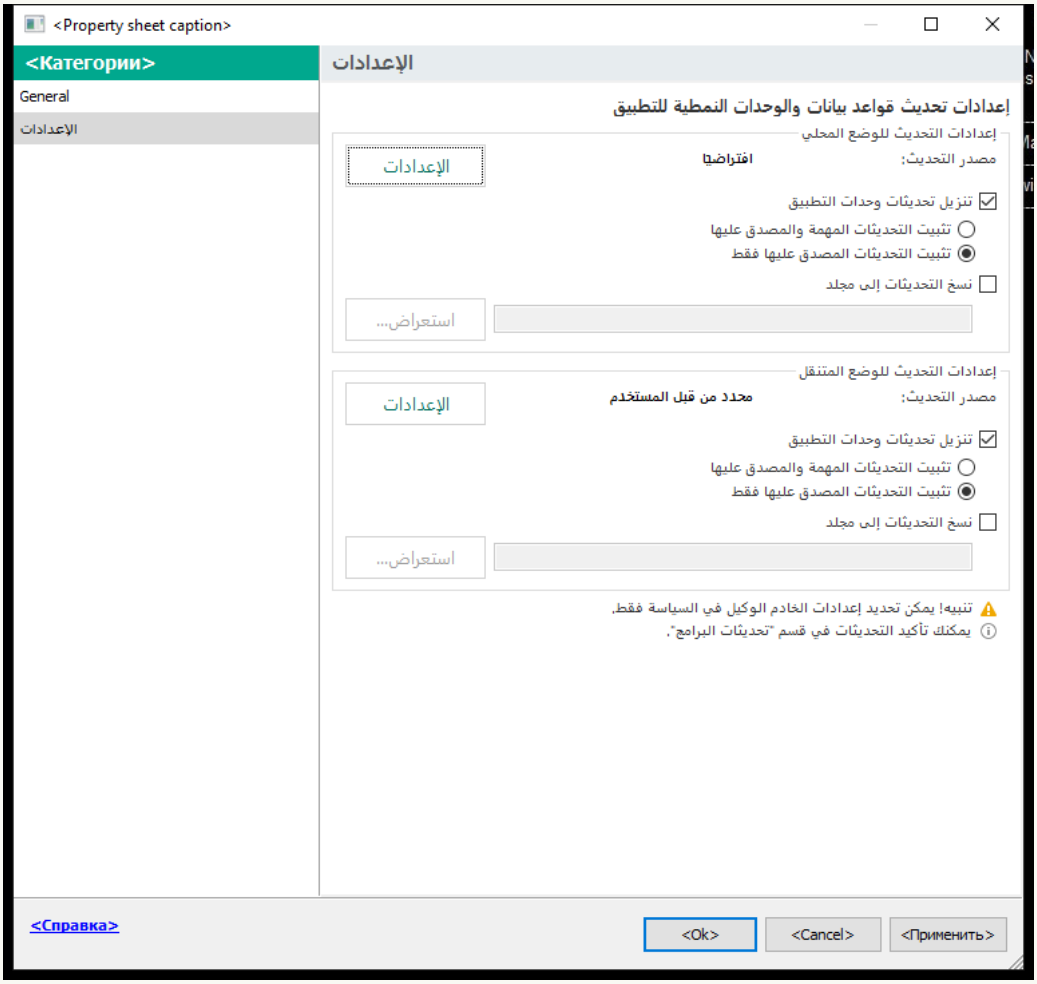
في شجرة وحدة التحكم، حدد **المهام**.

2. انقر فوق المهمة **تحديث** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة تحديث تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. من نافذة خصائص المهام، حدد القسم **الإعدادات**.



إعدادات مهمة تحديث

4. في القسم **إعدادات التحديث للوضع المحلي**، انقر على الزر **الإعدادات**.

5. في قائمة مصادر التحديث، تأكد من تمكين التحديث من مصدر **Kaspersky Security Center**. بالإضافة إلى ذلك، يجب أن يكون لمصدر **Kaspersky Security Center** الأولوية القصوى.

6. إذا لزم الأمر، أضف مصادر التحديث:

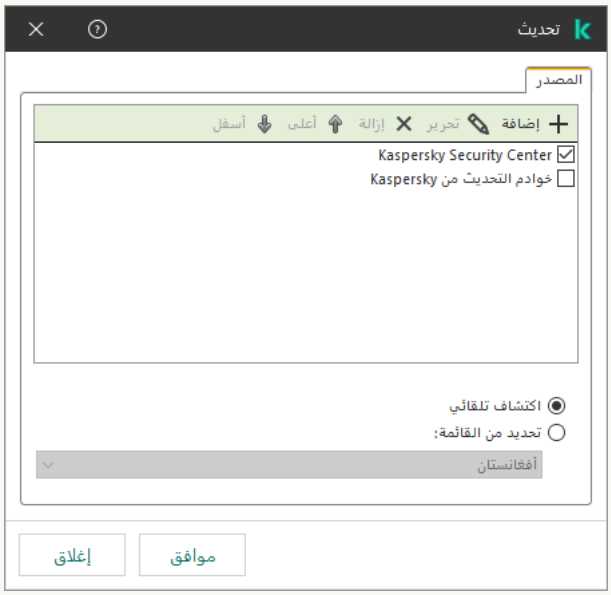
a. في قائمة مصادر التحديث انقر فوق الزر **إضافة**.

b. في الحقل **"المصدر"**، حدد عنوان خادم FTP- أو HTTP، أو مجلد الشبكة، أو المجلد المحلي الذي سيقوم Kaspersky Security Center بنسخ حزمة التحديث التي تم استلامها من خوادم Kaspersky فيه.

يجب أن يطابق عنوان مصدر التحديث العنوان الذي حددته في الحقل **مجلد تخزين التحديثات** عندما قمت بتكوين تنزيل التحديثات إلى مخزن الخادم (مهمة تنزيل التحديثات إلى مستودع خادم الإدارة).

c. انقر فوق **موافق**.

يمكنك استثناء مصدر التحديث دون إزالته من قائمة مصادر التحديث. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.



مصادر التحديث

7. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

في حالة تعذر إجراء تحديث من مصدر التحديث الأول، فإن برنامج Kaspersky Endpoint Security ينتقل تلقائيًا إلى المصدر التالي.

8. في نافذة خصائص المهمة، حدد القسم **جدولة** وكوّن وضع تشغيل المهمة.

9. بشكل افتراضي، يقوم Kaspersky Endpoint Security بتشغيل المهمة في الوضع اليدوي.

10. احفظ تغييراتك.

كيفية تكوين تحديث Kaspersky Endpoint Security من مخزن الخادم المحدد في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق المهمة **Update** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة Update تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة Update، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. حدد علامة التبويب **Local mode** ← **Application settings**.

4. في قائمة مصادر التحديث، تأكد من تمكين التحديث من مصدر **Kaspersky Security Center**. بالإضافة إلى ذلك، يجب أن يكون لمصدر **Kaspersky Security Center** الأولوية القصوى.

5. إذا لزم الأمر، أضف مصادر التحديث:

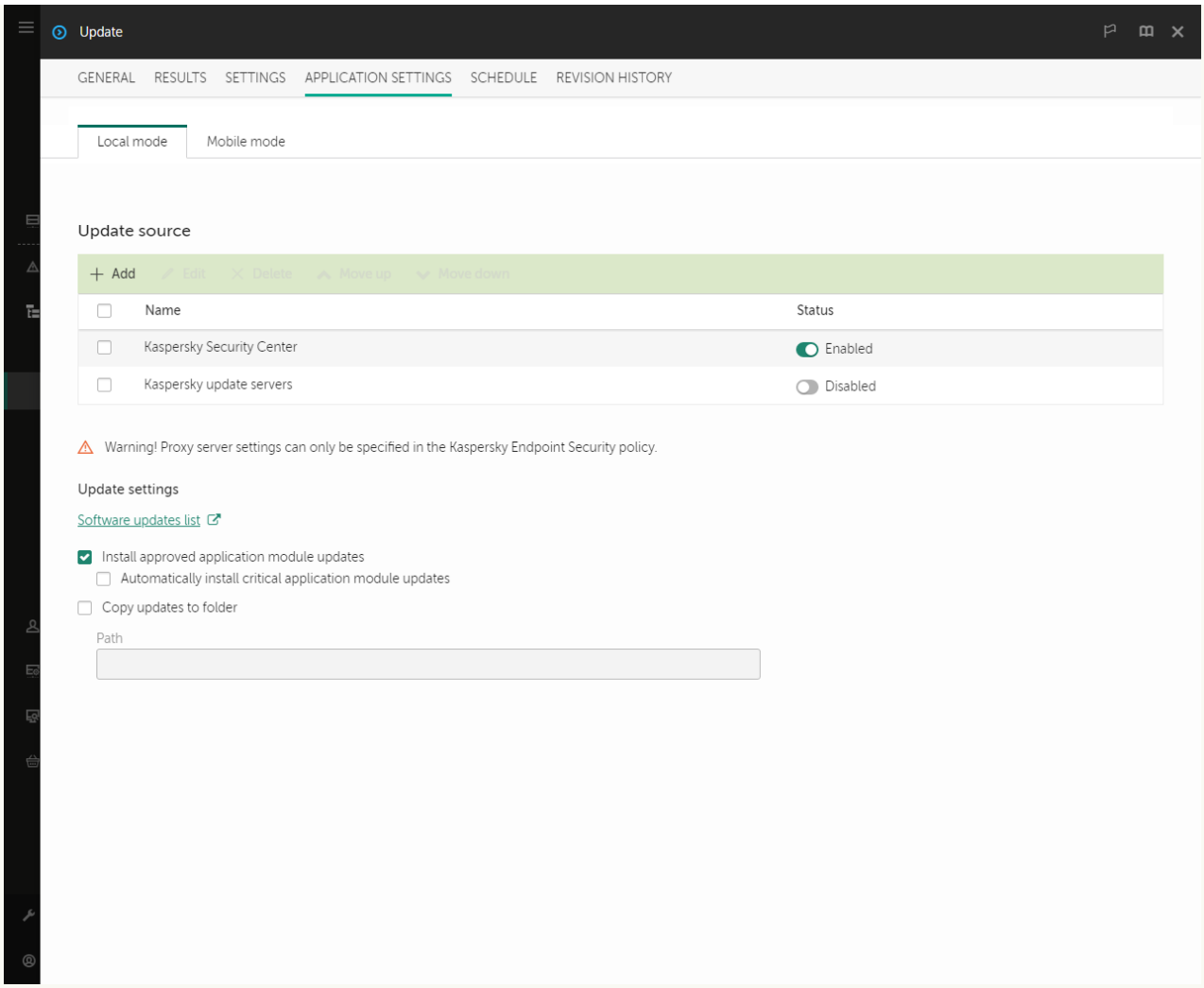
a. في قائمة مصادر التحديث انقر فوق الزر **Add**.

b. في الحقل **Source**، حدد عنوان خادم FTP- أو HTTP، أو مجلد الشبكة، أو المجلد المحلي الذي سيقوم Kaspersky Security Center بنسخ حزمة التحديث التي تم استلامها من خوادم Kaspersky فيه.

يجب أن يطابق عنوان مصدر التحديث العنوان الذي حددته في الحقل **Folder for storing updates** عندما قمت بتكوين تنزيل التحديثات إلى مخزن الخادم (مهمة تنزيل التحديثات إلى مستودع خادم الإدارة).

c. انقر على **OK**.

يمكنك استثناء مصدر التحديث دون إزالته من قائمة مصادر التحديث. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.



مصادر التحديث

6. قم بتكوين أولويات مصادر التحديث باستخدام الزر **Up** و**Down**.

في حالة تعذر إجراء تحديث من مصدر التحديث الأول، فإن برنامج Kaspersky Endpoint Security ينتقل تلقائيًا إلى المصدر التالي.

7. في نافذة خصائص المهمة، حدد القسم **Schedule** وكوّن وضع تشغيل المهمة.

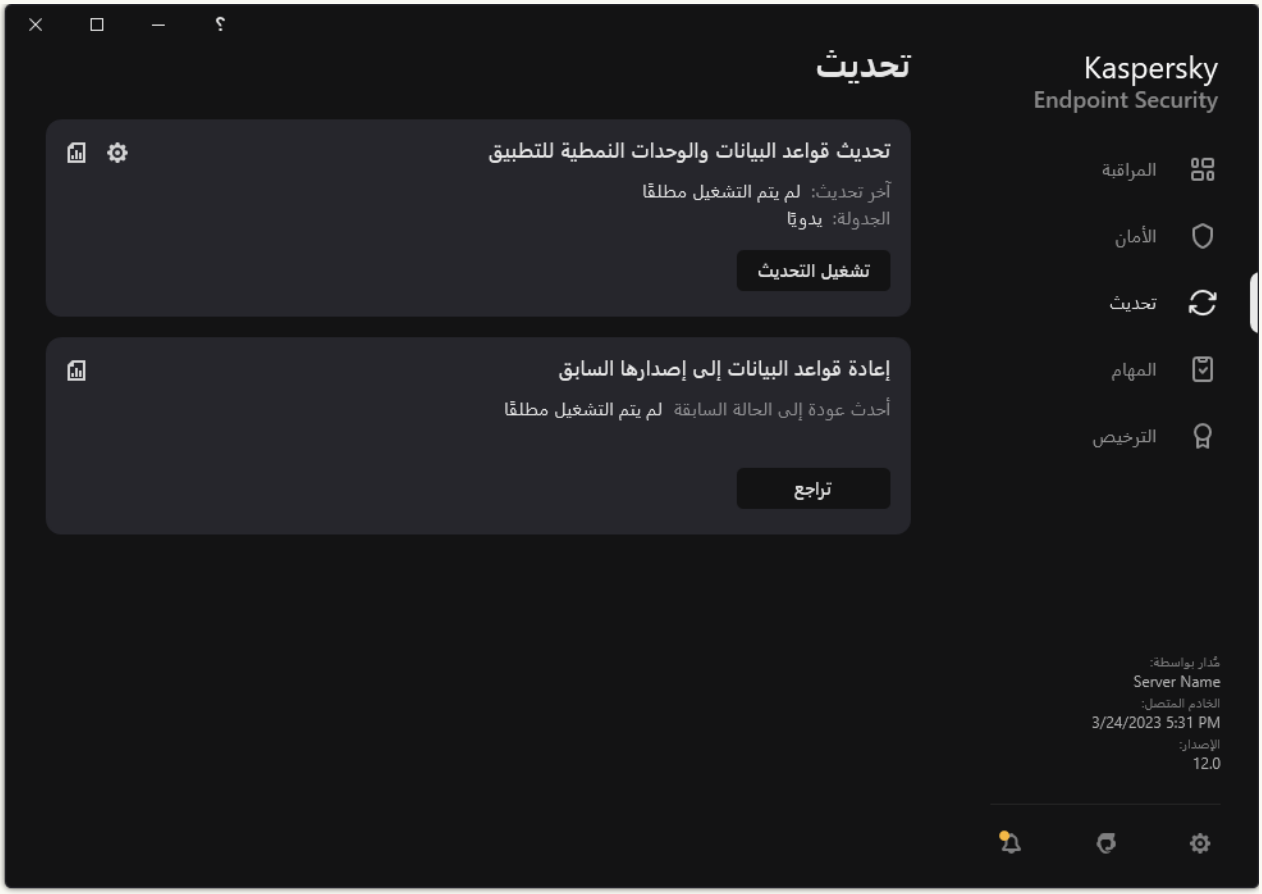
8. بشكل افتراضي، يقوم Kaspersky Endpoint Security بتشغيل المهمة في الوضع اليدوي.

9. احفظ تغييراتك.

كيفية تكوين تحديث Kaspersky Endpoint Security من مخزن الخادم المحدد في واجهة التطبيق

لا يمكنك تكوين المهمة الجماعية تحديث في واجهة التطبيق. وتتاح فقط مهمة تحديث محلية، تحديث قواعد البيانات والوحدات النمطية للتطبيق للمستخدم. إذا لم يتم عرض مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، فهذا يعني أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.



مهام التحديث المحلية

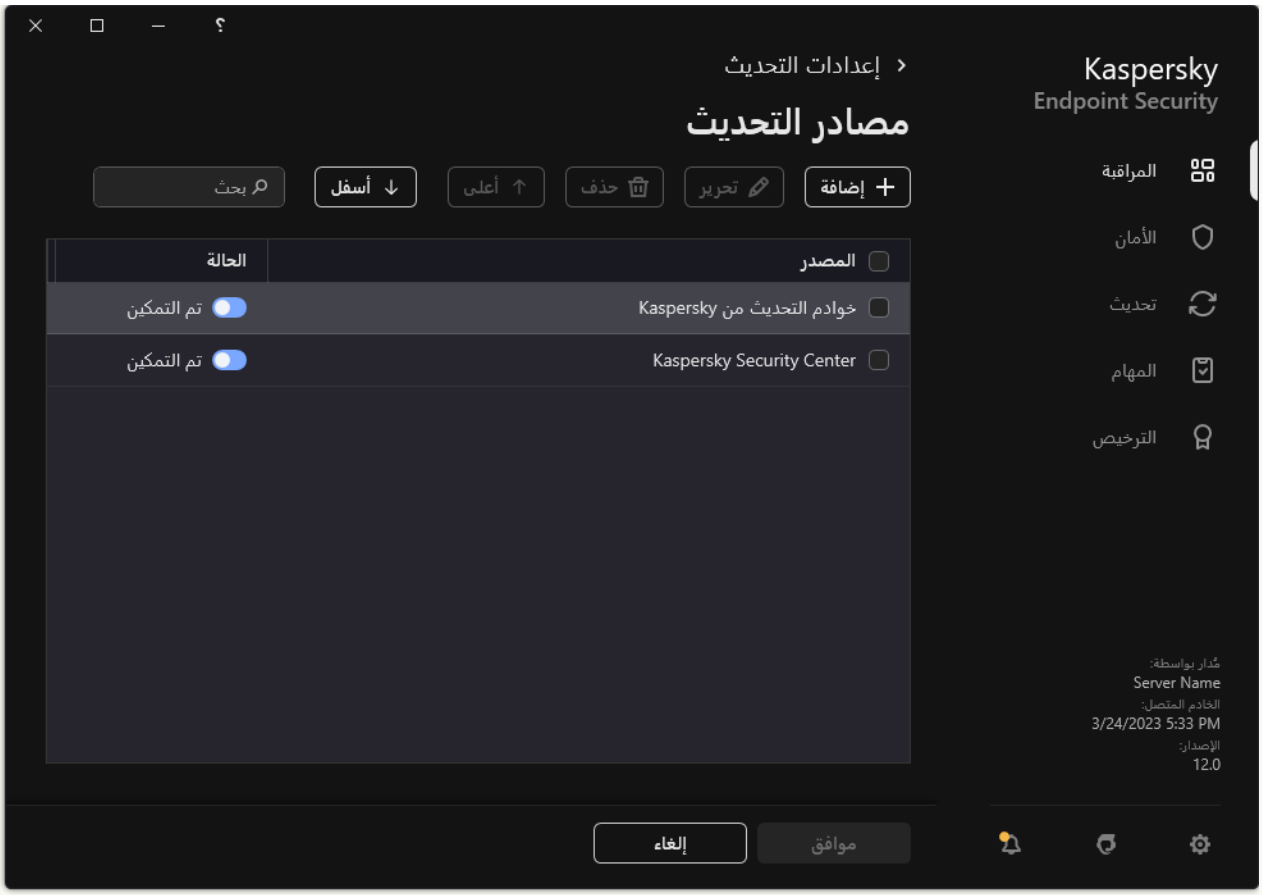
2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق ⚙.
نافذة خصائص المهمة.

3. في نافذة خصائص المهمة، انقر على **تحديد مصادر التحديث**.

4. في قائمة مصادر التحديث، تأكد من تمكين التحديث من مصدر **Kaspersky Security Center**. بالإضافة إلى ذلك، يجب أن يكون لمصدر **Kaspersky Security Center** الأولوية القصوى.

5. إذا لزم الأمر، أضف مصادر التحديث:

a. في قائمة مصادر التحديث انقر فوق الزر **إضافة**.



مصادر التحديث

a. حدد عنوان خادم FTP- أو HTTP، أو مجلد الشبكة، أو المجلد المحلي الذي سيقوم Kaspersky Security Center بنسخ حزمة التحديث التي تم استلامها من خوادم التحديث من Kaspersky فيه.

يجب أن يطابق عنوان مصدر التحديث العنوان الذي حددته في الحقل **مجلد تخزين التحديثات** عندما قمت بتكوين تنزيل التحديثات إلى مخزن الخادم (مهمة تنزيل التحديثات إلى مستودع خادم الإدارة).

b. انقر على **تحديد**.

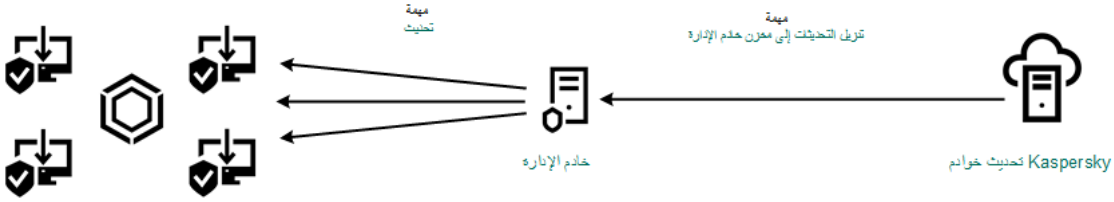
يمكنك استثناء مصدر التحديث دون إزالته من قائمة مصادر التحديث. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.

6. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

في حالة تعذر إجراء تحديث من مصدر التحديث الأول، فإن برنامج Kaspersky Endpoint Security ينتقل تلقائيًا إلى المصدر التالي.

في حالة إدارة جهاز كمبيوتر بواسطة Kaspersky Security Center، فلن يمكن تكوين وضع التشغيل لمهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق. ويمكنك فقط تشغيل الفحص يدويًا.

7. احفظ تغييراتك.



التحديث من مستودع الخادم

التحديث من مجلد مشترك

للحفاظ على حركة الإنترنت، يمكنك تكوين تحديثات قواعد البيانات ووحدات التطبيق على أجهزة كمبيوتر الشبكة المحلية للمؤسسة من مجلد مشترك. لذلك، يتلقى أحد أجهزة الكمبيوتر المتصل بالشبكة المحلية LAN حزمة تحديث حديثة من خادم Kaspersky Security Center أو من خوادم تحديث Kaspersky، ثم ينسخ حزمة التحديث التي تم الحصول عليها إلى مجلد مشترك. ستتمكن أجهزة الكمبيوتر الأخرى الموجودة على الشبكة المحلية للمؤسسة LAN من تلقي حزمة التحديث من هذا الملف المشترك.

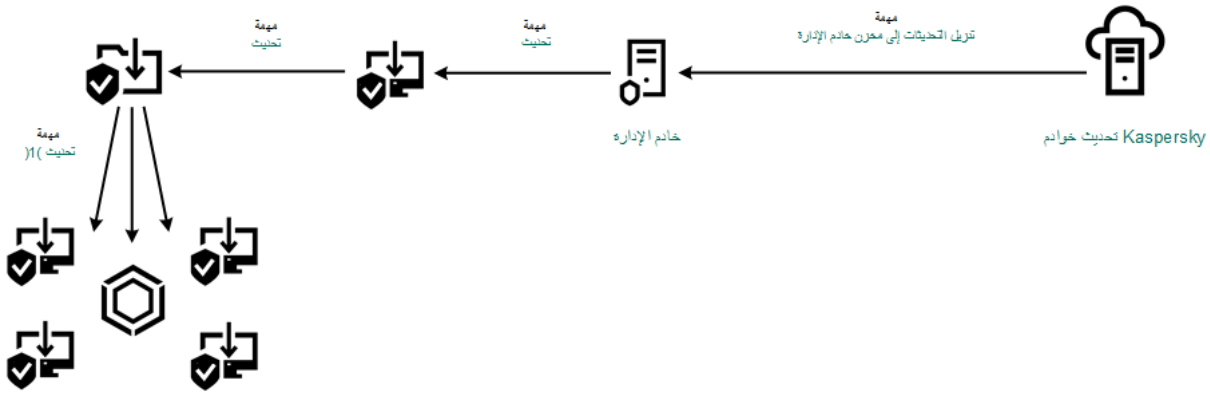
يتكون تحديث قاعدة بيانات التطبيق والوحدة النمطية ذات المجلد المشترك من الخطوات التالية:

1. تكوين قاعدة البيانات والوحدة النمطية للتطبيق من مستودع الخادم.

2. تمكين نسخ حزمة تحديث إلى مجلد مشترك على أحد أجهزة الكمبيوتر الموجودة على شبكة المنطقة المحلية (LAN) للمؤسسة (انظر التعليمات أدناه).

3. قم بتكوين تحديثات قاعدة البيانات والوحدة النمطية للتطبيق من المجلد المشترك المحدد إلى أجهزة الكمبيوتر المتبقية على شبكة المنطقة المحلية (LAN) للمؤسسة (انظر التعليمات أدناه).

يجب أن يتطابق إصدار وترجمة تطبيق Kaspersky Endpoint Security الذي ينسخ حزمة التحديث إلى مجلد مشترك مع إصدار وترجمة التطبيق الذي يقوم بتحديث قواعد البيانات من المجلد المشترك. وإذا لم تتطابق إصدارات أو ترجمات التطبيقات، فقد ينتهي تحديث قاعدة البيانات بخطأ.



التحديث من مجلد مشترك

لتمكين نسخ حزمة التحديث إلى المجلد المشترك:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

يجب تعيين مهمة التحديثلجهاز كمبيوتر واحد سيعمل كمصدر للتحديثات.

2. انقر فوق المهمة **Update** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة Update تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة Update، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. حدد علامة التبويب **Local mode** ← **Application settings**.

4. لتكوين مصادر التحديث.

يمكن أن تكون مصادر التحديثات هي خوادم تحديثات Kaspersky، أو خادم الإدارة Kaspersky Security Center، أو خوادم FTP- أو HTTP الأخرى، أو المجلدات المحلية، أو مجلدات الشبكة.

5. حدد خانة الاختيار **Copy updates to folder**.

6. في الحقل **Path**، أدخل مسار UNC للمجلد المشترك (مثل `\\Server\Share\Update distribution`).

إذا تُرك الحقل فارغًا، سينسخ Kaspersky Endpoint Security حزمة التحديث إلى المجلد `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

7. احفظ تغييراتك.

تكوين تحديثات من مجلد مشترك:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type**، حدد **Update**.

c. في الحقل **Task name**، أدخل وصفًا موجزًا على سبيل المثال التحديث من مجلد مشترك.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

يجب تعيين مهمة تحديث على أجهزة الكمبيوتر الخاصة بالشبكة المحلية (LAN) الخاصة بالمؤسسة، باستثناء الكمبيوتر الذي يعمل كمصدر للتحديث.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد وانتقل إلى الخطوة التالية.

5. أغلق المعالج.

سيتم عرض مهمة جديدة في جدول المهام.

6. انقر فوق المهمة التي تم انشاؤها حديثًا تحديث.

نافذة خصائص المهمة.

7. انتقل إلى القسم **Application settings**.

8. حدد علامة التبويب **Local mode**.

9. في القسم **Update source** انقر على **إضافة**.

10. في الحقل **Source**، أدخل المسار المؤدي إلى المجلد المشترك.

يجب أن يطابق عنوان المصدر العنوان الذي حددته في الحقل **Path** عند قيامك بتكوين نسخ حزمة التحديث إلى المجلد المشترك (راجع الإرشادات أعلاه).

11. انقر على **OK**.

12. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

13. احفظ تغييراتك.

التحديث باستخدام برنامج Kaspersky Update Utility

للحفاظ على حركة مرور الإنترنت، يمكنك تكوين تحديثات قواعد البيانات ووحدات التطبيق على أجهزة كمبيوتر الشبكة المحلية (LAN) الخاصة بالمؤسسة من مجلد مشترك باستخدام Kaspersky Update Utility. لذلك، يتلقى أحد أجهزة الكمبيوتر المتصل بالشبكة المحلية (LAN) الخاصة بالمؤسسة حزم تحديث حديثة من خادم الإدارة Kaspersky Security Center أو من خوادم تحديث Kaspersky ثم ينسخ حزم التحديث التي تم استلامها على مجلد مشترك باستخدام الأداة. ستتمكن أجهزة الكمبيوتر الأخرى الموجودة على الشبكة المحلية للمؤسسة LAN من تلقي حزمة التحديث من هذا الملف المشترك.

يتكون تحديث قاعدة بيانات التطبيق والوحدة النمطية ذات المجلد المشترك من الخطوات التالية:

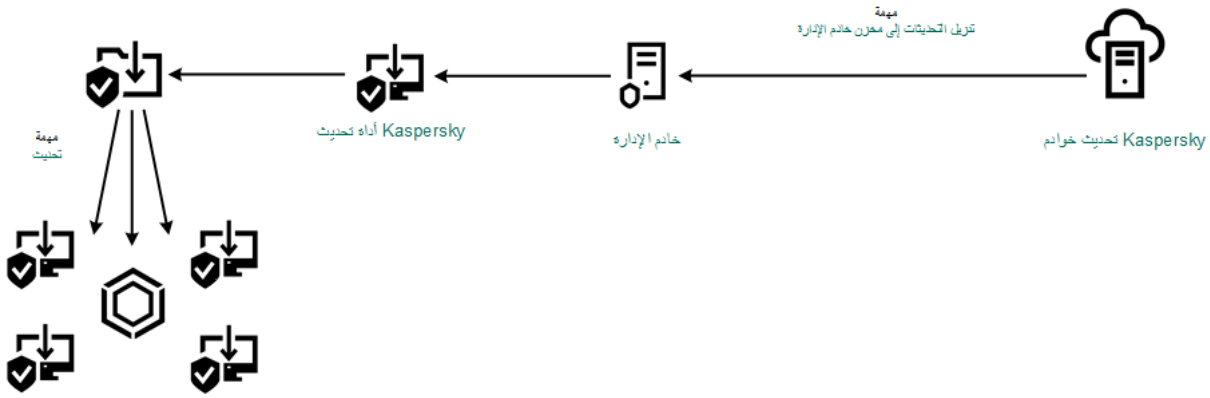
1. تكوين قاعدة البيانات والوحدة النمطية للتطبيق من مستودع الخادم.

2. قم بتثبيت أداة تحديث Kaspersky على أحد أجهزة كمبيوتر الشبكة المحلية (LAN) الخاصة بالمؤسسة.

3. قم بتكوين نسخ حزمة التحديث إلى المجلد المشترك الموجود في إعدادات أداة تحديث Kaspersky.

4. قم بتكوين تحديثات قاعدة البيانات والتطبيق من المجلد المشترك المحدد إلى أجهزة الكمبيوتر الباقية على الشبكة المحلية الخاصة بالمؤسسة .

يجب أن يتطابق إصدار وترجمة تطبيق Kaspersky Endpoint Security الذي ينسخ حزمة التحديث إلى مجلد مشترك مع إصدار وترجمة التطبيق الذي يقوم بتحديث قواعد البيانات من المجلد المشترك. وإذا لم تتطابق إصدارات أو ترجمات التطبيقات، فقد ينتهي تحديث قاعدة البيانات بخطأ.



التحديث باستخدام برنامج Kaspersky Update Utility

يُمكنك تنزيل حزمة التوزيع الخاصة بأداة تحديث Kaspersky من موقع ويب الدعم الفني في Kaspersky. بعد تثبيت الأداة، حدد مصدر التحديث (على سبيل المثال، مستودع خادم الإدارة) والمجلد المشترك الذي ستقوم أداة تحديث Kaspersky بنسخ حزم التحديث إليه. للحصول على معلومات تفصيلية حول استخدام Kaspersky Update Utility، يُرجى الرجوع إلى قاعدة معارف Kaspersky.

تكوين تحديثات من مجلد مشترك:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق المهمة **Update** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة Update تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة Update، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. حدد علامة التبويب **Application settings ← Local mode**.

4. في قائمة مصادر التحديث انقر فوق الزر **إضافة**.

5. في الحقل **Source**، أدخل مسار UNC للمجلد المشترك (مثل `\\Server\Share\Update distribution`).

يجب أن يتطابق عنوان المصدر مع العنوان الذي تمت الإشارة إليه في إعدادات أداة تحديث Kaspersky.

6. انقر على **OK**.

7. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

8. احفظ تغييراتك.

التحديث أثناء الوضع المتنقل

الوضع المتنقل هو وضع تشغيل برنامج Kaspersky Endpoint Security، عندما يترك الكمبيوتر شبكة مؤسسة محيطة (جهاز كمبيوتر غير متصل). للمزيد من التفاصيل عن العمل مع أجهزة الكمبيوتر غير المتصلة بالإنترنت والمستخدمين خارج المكتب، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

يتعذر على جهاز الكمبيوتر غير المتصل خارج شبكة المؤسسة الاتصال بخادم الإدارة لتحديث قواعد البيانات والوحدات النمطية للتطبيق. يتم بشكلٍ افتراضي استخدام خوادم التحديث الخاصة بـ Kaspersky فقط كمصدر للتحديثات لتحديث قواعد البيانات والوحدات النمطية للتطبيق في الوضع المتنقل. يتم تحديد استخدام خادم وكيل للاتصال بالإنترنت من خلال سياسة الوجود خارج المكتب. يجب إنشاء سياسة الوجود خارج المكتب بشكل منفصل. عندما يتم تحويل برنامج Kaspersky Endpoint Security إلى الوضع المتنقل يتم تحديث المهام كل ساعتين.

لتكوين إعدادات التحديث للوضع المتنقل:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Tasks**.

تفتح قائمة المهام.

2. انقر فوق المهمة **Update** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة Update تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة Update، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. حدد علامة التبويب **Application settings ← Mobile mode**.

4. لتكوين مصادر التحديث. يمكن أن تكون مصادر التحديثات هي خوادم التحديث الخاصة بـ Kaspersky، أو خوادم FTP- وHTTP الأخرى، أو المجلدات المحلية، أو مجلدات الشبكة.

5. احفظ تغييراتك.

ونتيجة لذلك، سيتم تحديث قواعد البيانات والوحدات النمطية للتطبيق على أجهزة المستخدم عند التبديل إلى الوضع المتنقل.

بدء مهمة تحديث وإيقافها

بغض النظر عن وضع تشغيل مهام التحديث المحددة، يمكنك بدء مهمة تحديث Kaspersky Endpoint Security أو إيقافها في أي وقت.

لبدء مهمة تحديث أو إيقافها:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.

2. في الإطار **تحديث قواعد البيانات والوحدات النمطية للتطبيق**، انقر فوق الزر **تحديث** إذا كنت تريد بدء مهمة التحديث.

سيبدأ Kaspersky Endpoint Security في تحديث الوحدات النمطية للتطبيق وقواعد البيانات. وسيعرض التطبيق تقدم المهمة وحجم الملفات التي يتم تنزيلها ومصدر التحديث. يمكنك إيقاف المهمة في أي وقت بالنقر فوق الزر **إيقاف التحديث**.

لبدء أو إيقاف مهمة التحديث عند عرض واجهة التطبيق المبسطة:

1. انقر بزر الماوس الأيمن لإظهار القائمة السياقية الخاصة بأيقونة التطبيق في منطقة إعلام شريط المهام.

2. في القائمة المنسدلة **المهام** في قائمة السياق، نفذ أحد ما يلي:

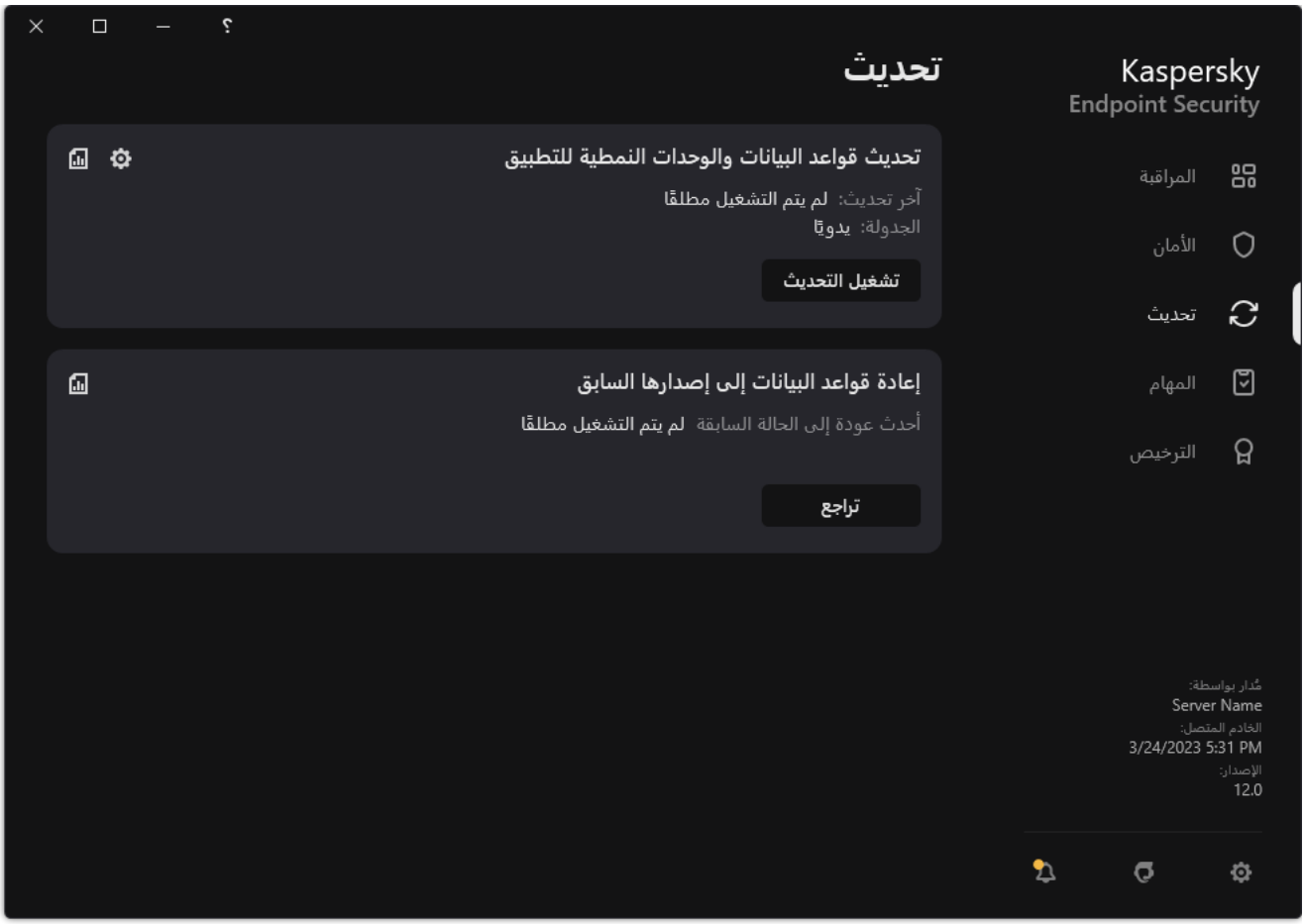
- حدد مهمة تحديث ليست قيد التشغيل لبدء تشغيلها
- حدد مهمة تحديث قيد التشغيل لإيقافها
- حدد مهمة تحديث متوقفة مؤقتًا لاستئنافها أو إعادة بدء تشغيلها

بدء مهمة تحديث تحت حقوق حساب مستخدم مختلف

في الوضع الافتراضي، يتم بدء مهمة تحديث برنامج Kaspersky Endpoint Security نيابة عن المستخدم الذي قمت باستخدام حسابه لتسجيل الدخول في نظام التشغيل. على الرغم من ذلك، قد يتم تحديث Kaspersky Endpoint Security من مصدر تحديث يتعذّر على المستخدم الوصول إليه لوجود نقص في الحقوق المطلوبة (على سبيل المثال، من مجلد مشترك يحتوي على حزمة تحديث) أو مصدر تحديث لم يتم تكوين مصادقة الخادم الوكيل له. في إعدادات التطبيق، يمكنك تحديد مستخدم يمتلك هذه الحقوق وتقوم ببدء مهمة تحديث برنامج Kaspersky Endpoint Security تحت حساب ذلك المستخدم.

لبدء مهمة تحديث في حساب مستخدم مختلف:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.



مهام التحديث المحلية

2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق ⚙.
نافذة خصائص المهمة.

3. انقر على **تشغيل تحديث قاعدة البيانات مع حقوق المستخدم**.

4. في النافذة التي تفتح، حدد **مستخدم آخر**.

5. أدخل بيانات اعتماد حساب مستخدم يمتلك الأذونات اللازمة للوصول إلى مصدر التحديث.

6. احفظ تغييراتك.

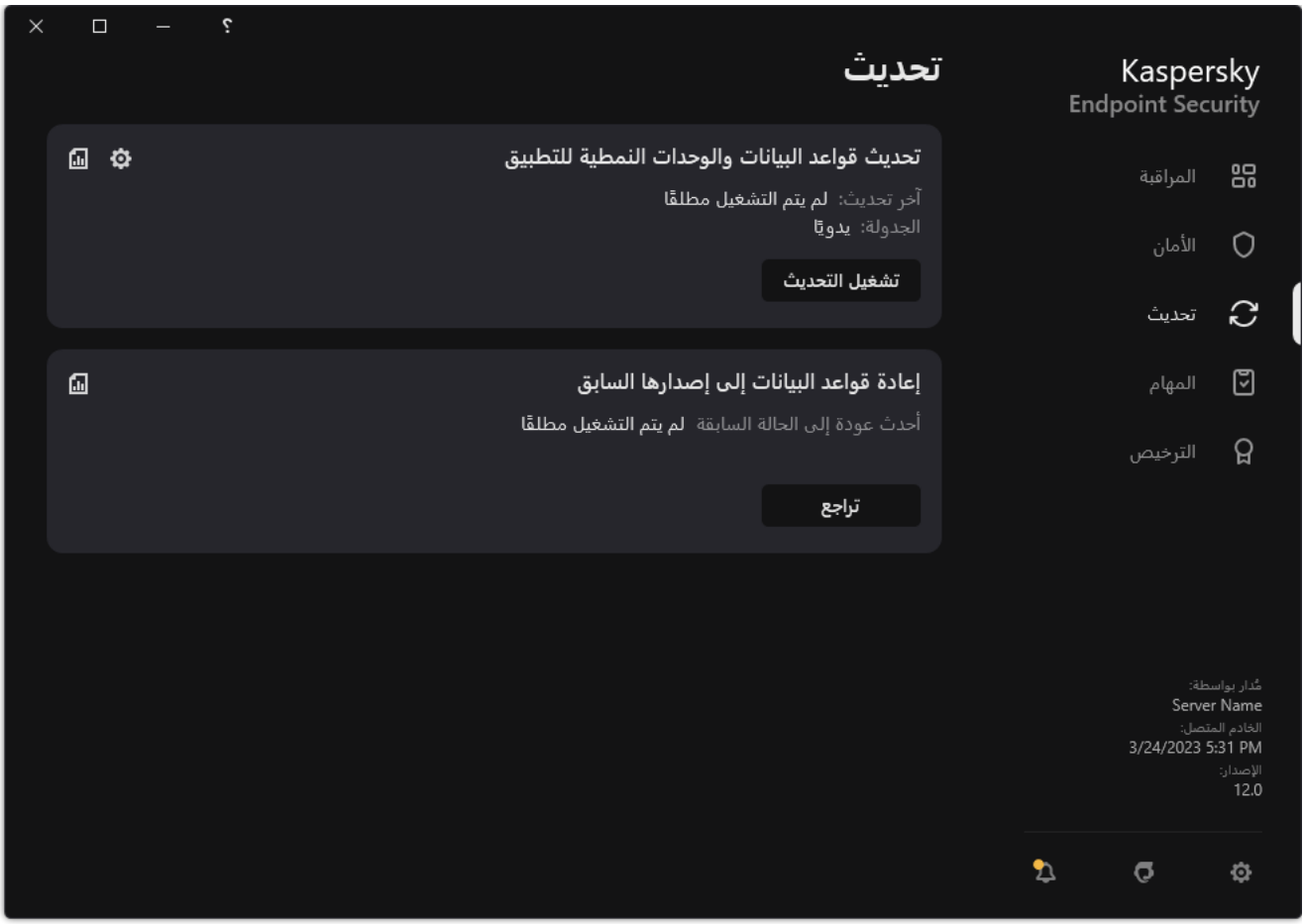
تحديد وضع تشغيل مهام التحديث

إذا تعذر تشغيل مهمة التحديث لأي سبب (على سبيل المثال: عدم تشغيل الكمبيوتر في ذلك الوقت)، يمكنك تكوين المهمة التي تم تخطيها لتبدأ تلقائيًا في أقرب وقت ممكن.

يمكنك تأجيل بدء مهمة التحديث بعد بدء تشغيل التطبيق إذا قمت بتحديد وضع تشغيل مهمة التحديث **حسب الجدولة**، وإذا كان وقت بدء Kaspersky Endpoint Security متطابقًا مع جدولة بدء مهمة التحديث. ولا يمكن تشغيل مهمة التحديث إلا بعد انقضاء الفترة الزمنية المحددة بعد بدء تشغيل Kaspersky Endpoint Security.

لتحديد وضع التشغيل لمهمة التحديث:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.



مهام التحديث المحلية

2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق ⚙.

نافذة خصائص المهمة.

3. انقر على **وضع التشغيل**.

4. في النافذة التي تفتح، حدد وضع تشغيل مهمة التحديث:

- إذا كنت تريد أن يقوم Kaspersky Endpoint Security بتشغيل مهمة التحديث حسب توفّر حزمة التحديث في مصدر التحديث، فحدد **تلقائيًا**. يكرر Kaspersky Endpoint Security عملية التحقق من وجود حزم تحديثات لمرات أكثر في أوقات انتشار الفيروسات، ولمرات أقل في الأوقات الأخرى.
- إذا كنت تريد بدء مهمة التحديث يدويًا، فحدد **يدويًا**.
- إذا كنت تريد تكوين جدولة لتشغيل مهمة التحديث، فحدد خيارات أخرى. تكوين الإعدادات المتقدمة لبدء مهمة التحديث:
  - في الحقل **تأجيل التشغيل بعد بدء التطبيق لمدة N دقيقة**، أدخل الفاصل الزمني الذي تريد من خلاله تأجيل بدء مهمة التحديث بعد بدء تشغيل Kaspersky Endpoint Security.
  - حدد **تشغيل الفحص المجدول في اليوم التالي في حالة إيقاف تشغيل الكمبيوتر** إذا كنت تريد أن يقوم Kaspersky Endpoint Security بتشغيل مهام التحديث الفائتة في أول فرصة.

5. احفظ تغييراتك.

إضافة مصدر تحديث

مصدر التحديث عبارة عن مورد يحتوي على تحديثات لقواعد البيانات ووحدات تطبيق برنامج Kaspersky Endpoint Security.

تتضمن مصادر التحديث خادم Kaspersky Security Center وخوادم تحديث Kaspersky والشبكة أو المجلدات المحلية.

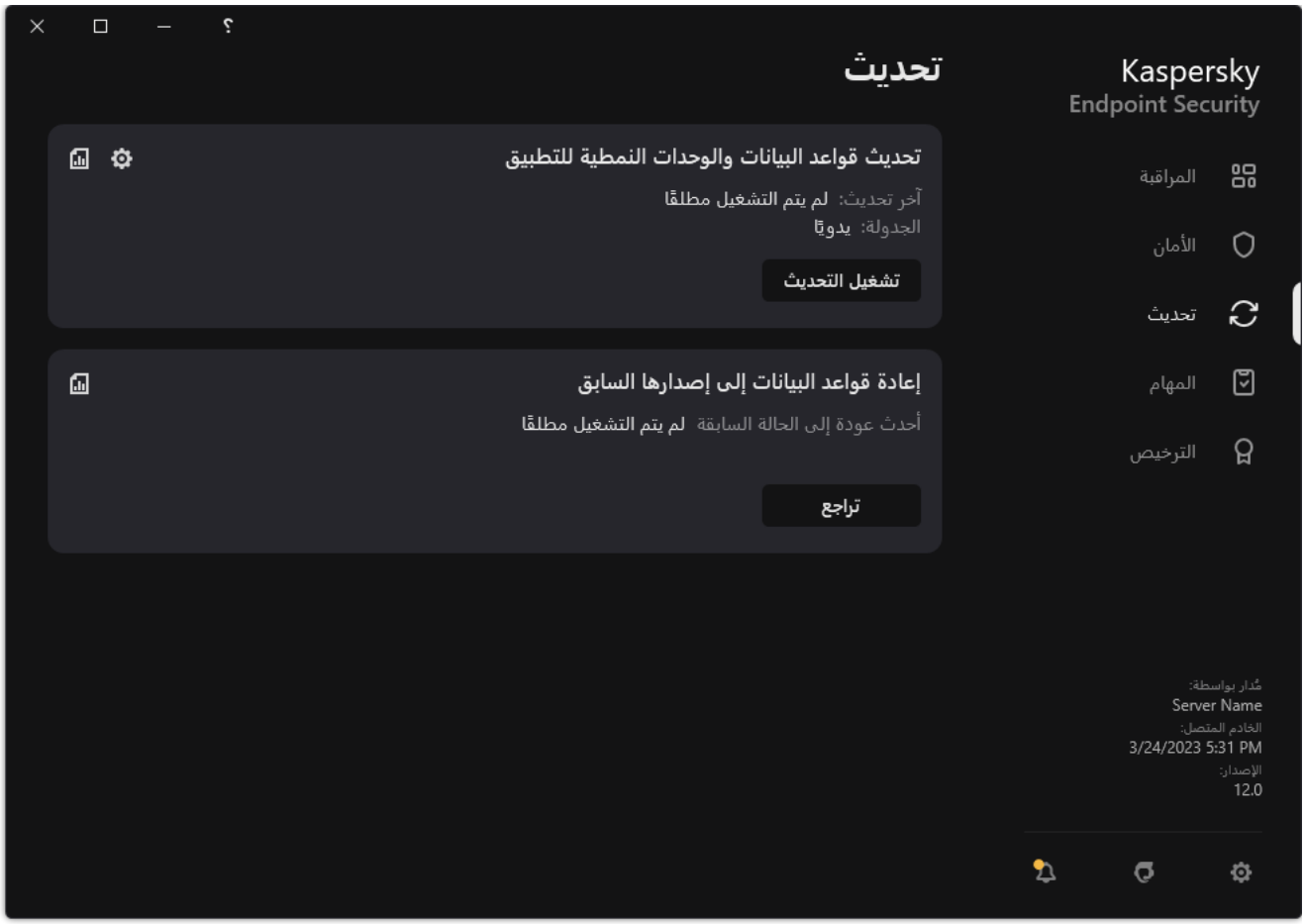
تتضمن القائمة الافتراضية لمصادر التحديث خوادم تحديث Kaspersky Security Center وKaspersky. يمكنك إضافة مصادر تحديث إلى القائمة. ويمكنك تحديد خوادم HTTP/FTP ومجلدات مشتركة كمصادر تحديث.

لا يدعم Kaspersky Endpoint Security التحديثات من خوادم HTTPS ما لم تكن خوادم تحديث من Kaspersky.

إذا تم تحديد موارد متعددة كمصادر للتحديث، يحاول برنامج Kaspersky Endpoint Security الاتصال بتلك الموارد واحدًا تلو الآخر، ابتداءً بأعلى القائمة، ويجري مهمة تحديث من خلال الحصول حزمة التحديثات من المصدر المتاح أولاً.

لإضافة مصدر تحديث:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.

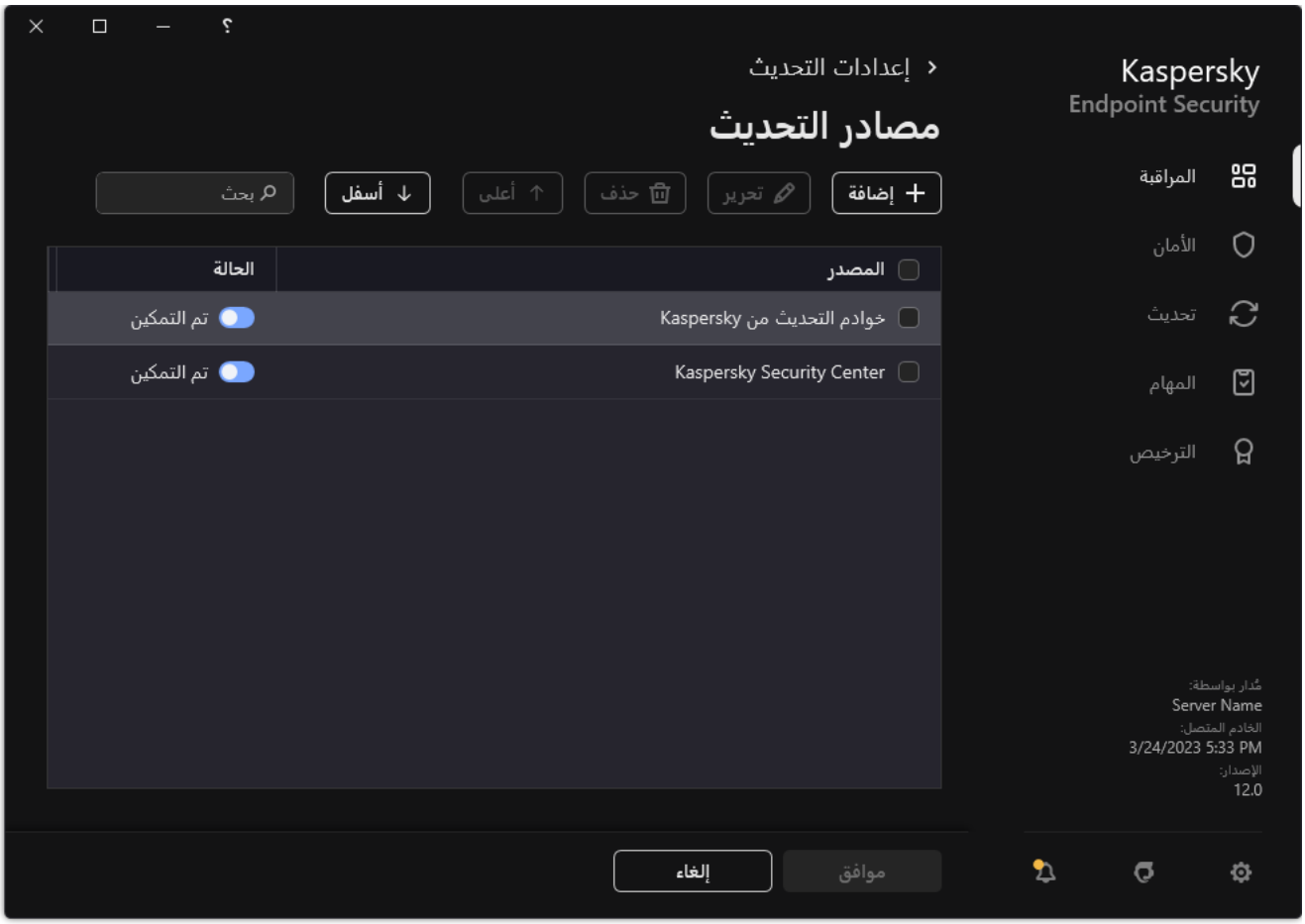


مهام التحديث المحلية

2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق ⚙.
نافذة خصائص المهمة.

3. انقر فوق الزر **تحديد مصادر التحديث**.

4. في النافذة التي ستفتح، انقر فوق الزر **إضافة**.



مصادر التحديث

5. في النافذة التي ستفتح، حدد عنوان خادم FTP أو HTTP أو مجلد الشبكة أو المجلد المحلي الذي يحتوي على حزمة التحديث.

يتم استخدام تنسيق المسار التالي لمصدر التحديث:

- بالنسبة لخادم FTP أو HTTP، أدخل عنوان الويب أو عنوان IP الخاص به.

  على سبيل المثال `http://dnl-01.geo.kaspersky.com/` او `93.191.13.103`.

  بالنسبة لخادم FTP، يمكنك تحديد إعدادات المصادقة من خلال العنوان الموجود في التنسيق التالي: `ftp://<user name>:<password>@<node>:<port>`.

- عند استخدام مجلد الشبكة، أدخل مسار UNC.

  على سبيل المثال `\\ Server\Share\Update distribution`.

- بالنسبة للمجلد المحلي، أدخل المسار الكامل إلى ذلك المجلد.

  على سبيل المثال: `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Update distribution\`.

6. انقر فوق الزر **تحديد**.

7. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

8. احفظ تغييراتك.

تكوين تحديثات من مجلد مشترك

للحفاظ على حركة الإنترنت، يمكنك تكوين تحديثات قواعد البيانات ووحدات التطبيق على أجهزة كمبيوتر الشبكة المحلية للمؤسسة من مجلد مشترك. لذلك، يتلقى أحد أجهزة الكمبيوتر المتصل بالشبكة المحلية LAN حزمة تحديث حديثة من خادم Kaspersky Security Center أو من خوادم تحديث Kaspersky، ثم ينسخ حزمة التحديث التي تم الحصول عليها إلى مجلد مشترك. ستتمكن أجهزة الكمبيوتر الأخرى الموجودة على الشبكة المحلية للمؤسسة LAN من تلقي حزمة التحديث من هذا الملف المشترك.

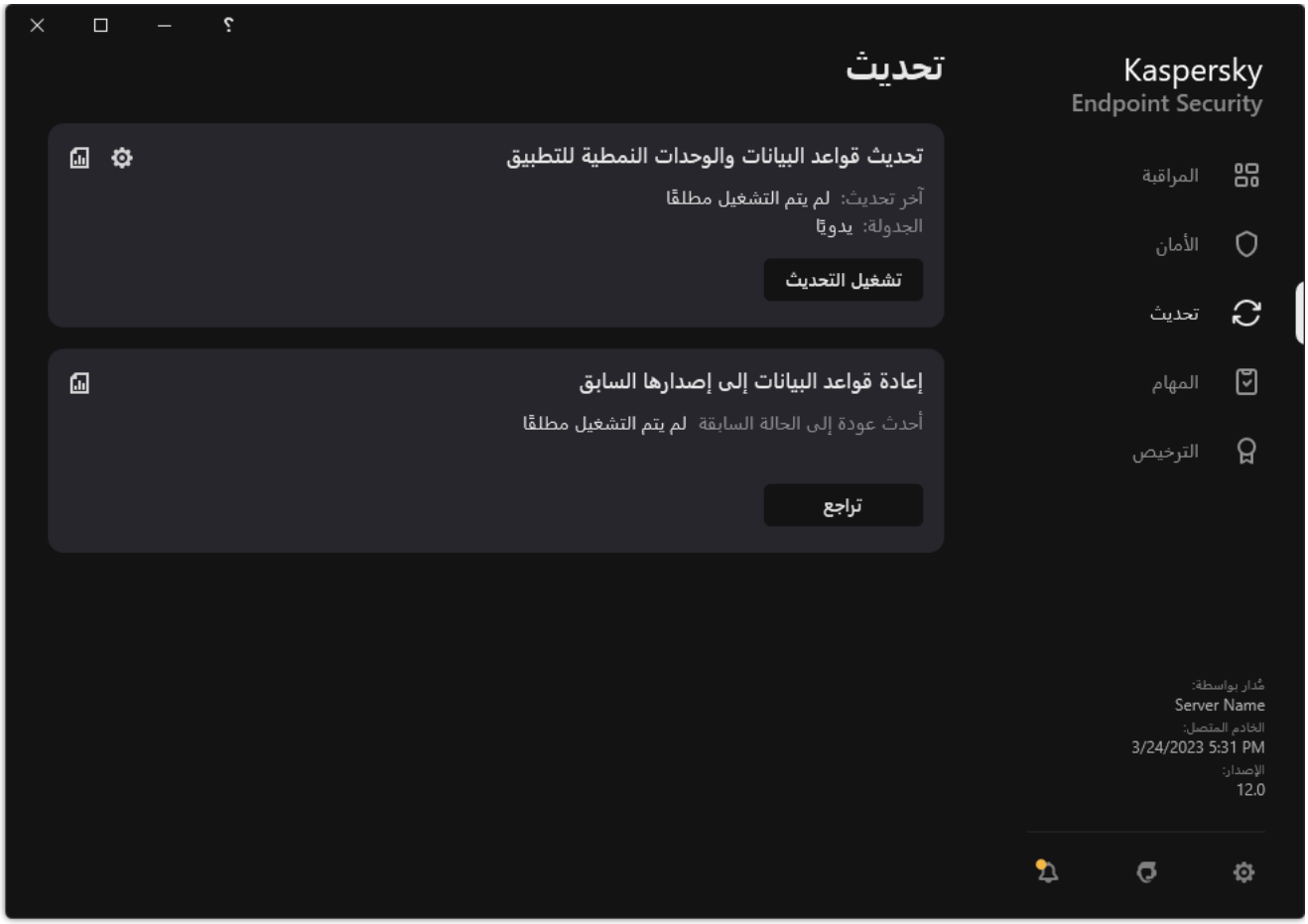
يتكون تحديث قاعدة بيانات التطبيق والوحدة النمطية ذات المجلد المشترك من الخطوات التالية:

1. تمكين نسخ حزمة التحديث إلى أحد المجلدات المشتركة في أحد أجهزة الكمبيوتر في الشبكة المحلية.

2. قم بتكوين تحديثات قاعدة البيانات والتطبيق من المجلد المشترك المحدد إلى أجهزة الكمبيوتر الباقية على الشبكة المحلية الخاصة بالمؤسسة .

لتمكين نسخ حزمة التحديث إلى المجلد المشترك:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.



مهام التحديث المحلية

2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق ⚙.
نافذة خصائص المهمة.

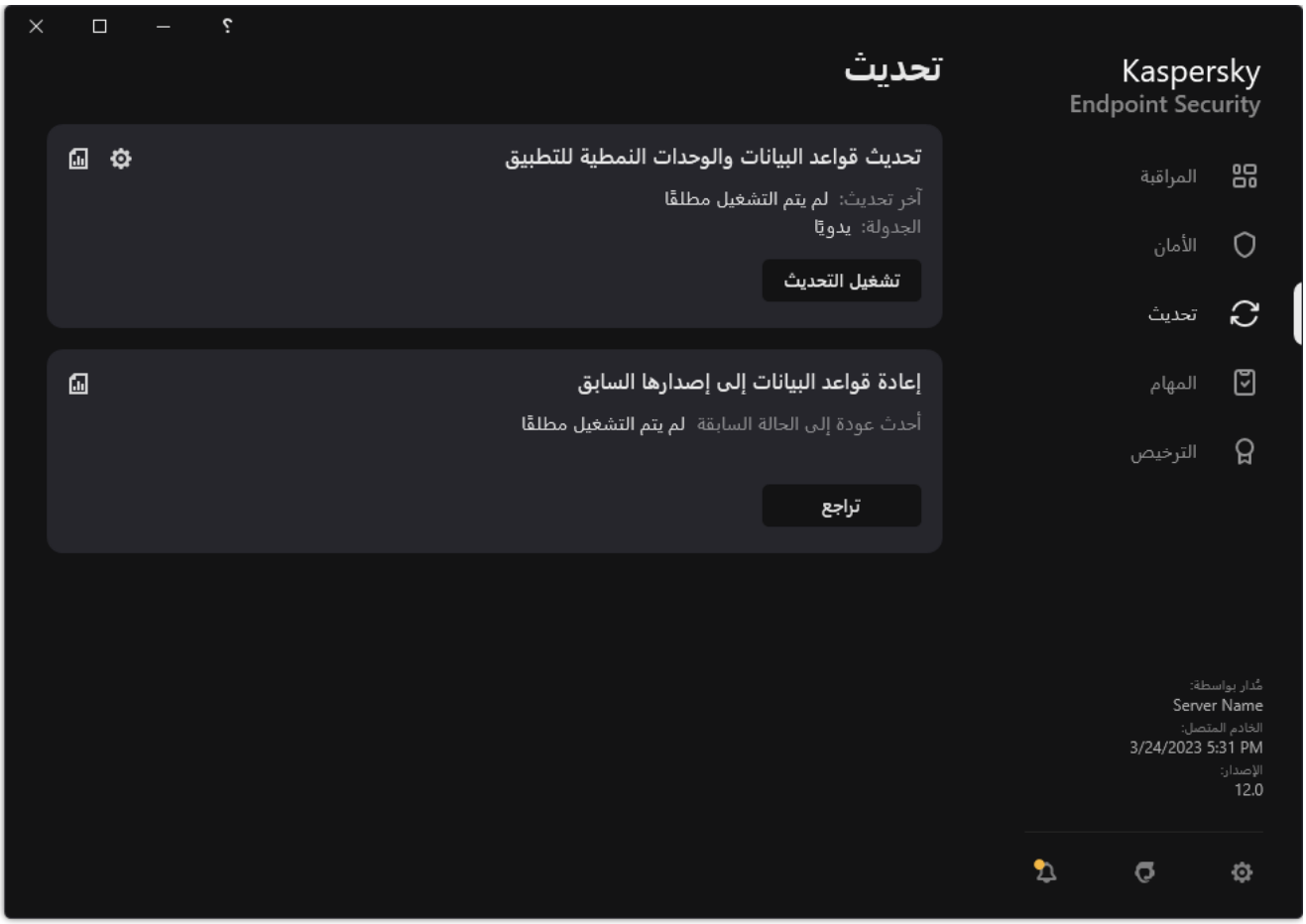
3. في القسم **توزيع التحديثات**، حدد خانة الاختيار **نسخ التحديثات إلى مجلد**.

4. أدخل مسار UNC للمجلد المشترك (مثل `\\Server\Share\Update distribution`).

5. احفظ تغييراتك.

تكوين تحديثات من مجلد مشترك:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.



مهام التحديث المحلية

2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق ⚙.

3. نافذة خصائص المهمة.

4. انقر على **تحديد مصادر التحديث**.

5. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

6. في النافذة التي تفتح، أدخل المسار المؤدي إلى المجلد المشترك.

يجب أن يطابق عنوان المصدر العنوان الذي حددته عند قيامك بتكوين نسخ حزمة التحديث إلى المجلد المشترك (راجع الإرشادات أعلاه).

7. انقر على **تحديد**.

8. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

9. احفظ تغييراتك.

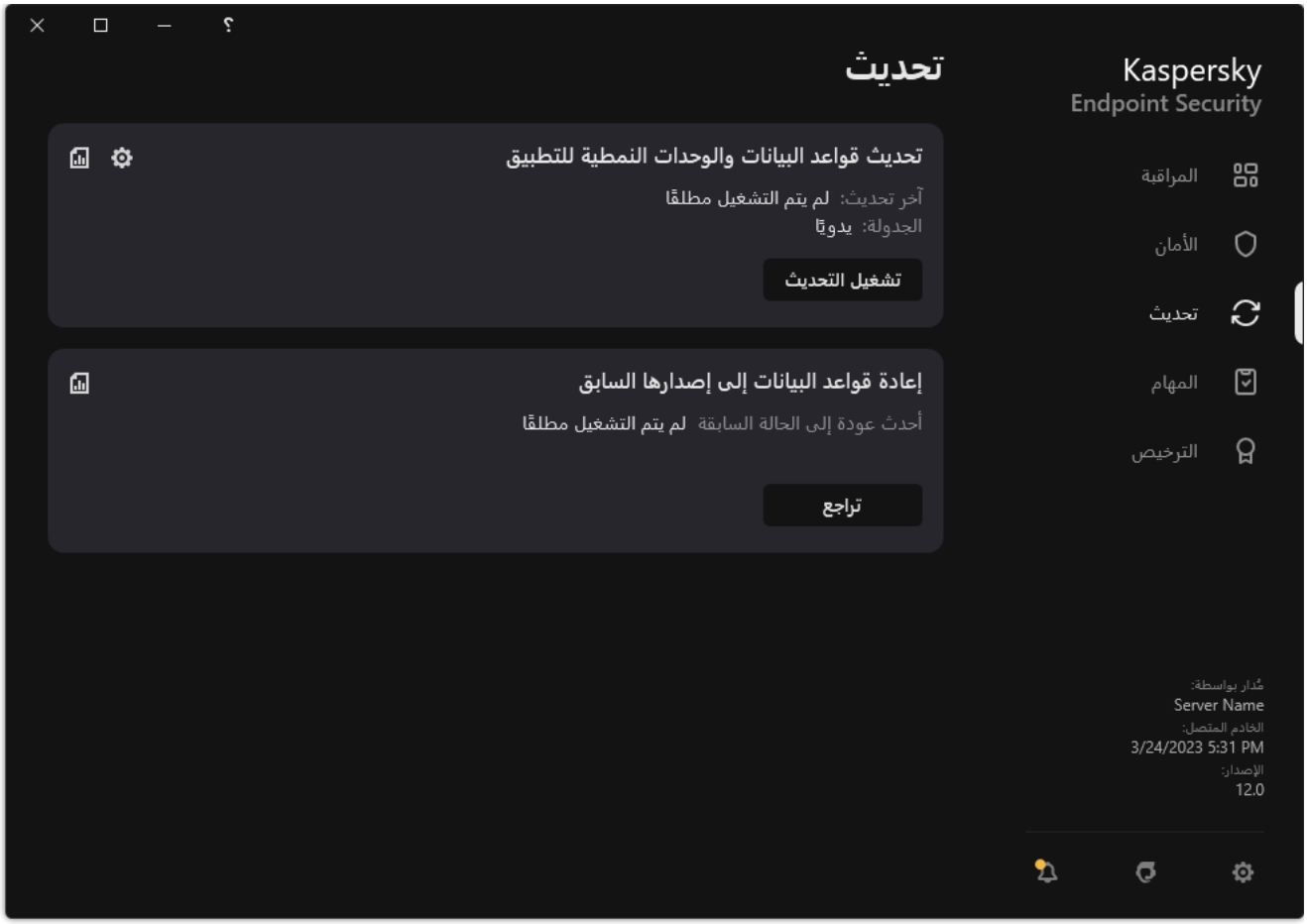
تحديث الوحدات النمطية للتطبيق

تعمل تحديثات الوحدة النمطية للتطبيق على إصلاح الأخطاء وتحسين الأداء وإضافة ميزات جديدة. وعندما يتوفر تحديث جديد للوحدة النمطية للتطبيق، فأنت بحاجة إلى تأكيد تثبيت التحديث. ويمكنك تأكيد تثبيت تحديث الوحدة النمطية للتطبيق إما في واجهة التطبيق أو في Kaspersky Security Center. كلما توفر تحديث، يعرض التطبيق إشعارًا في النافذة الرئيسية لتطبيق Kaspersky Endpoint Security: . إذا اقتضت تحديثات الوحدة النمطية للتطبيق مراجعة وقبول شروط اتفاقية ترخيص المستخدم النهائي، يقوم التطبيق بتثبيت التحديثات عقب قبول شروط اتفاقية ترخيص المستخدم النهائي. وللحصول على تفاصيل حول تتبع تحديثات الوحدة النمطية للتطبيق وتأكيد التحديث في Kaspersky Security Center، يرجى الرجوع إلى تعليمات Kaspersky Security Center.

بعد تثبيت تحديث التطبيق، قد تتم مطالبتك بإعادة تشغيل جهاز الكمبيوتر الخاص بك.

لتكوين تحديثات الوحدة النمطية للتطبيق:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.



مهام التحديث المحلية

2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق .

نافذة خصائص المهمة.

3. في القسم **تنزيل وتثبيت تحديثات وحدات التطبيق**، حدد خانة الاختيار **تنزيل تحديثات وحدات التطبيق**.

4. حدد تحديثات وحدات التطبيق التي تريد تثبيتها.

- **تثبيت التحديثات المهمة والمصدق عليها**. إذا تم تحديد هذا الخيار، وعند توافر تحديثات الوحدة النمطية للتطبيق يقوم Kaspersky Endpoint Security بتثبيت التحديثات الهامة تلقائيًا وجميع تحديثات الوحدة النمطية للتطبيق الأخرى فقط بعد أن تتم الموافقة على تثبيتهم محليًا بواسطة واجهة التطبيق أو على جانب Kaspersky Security Center.

- **تثبيت التحديثات المصدق عليها فقط**. إذا تم تحديد هذا الخيار، عند توافر تحديثات الوحدة النمطية للتطبيق يقومKaspersky Endpoint Security بتثبيتهم فقط بعد أن يتم الموافقة على تثبيتهم محليًا عبر واجهة التطبيق أو على جانب Kaspersky Security Center. ويتم تحديد هذا الخيار بشكل افتراضي.

5. احفظ تغييراتك.

استخدام الخادم الوكيل للتحديثات

قد تكون مطالبًا بتحديد إعدادات الخادم الوكيل لتنزيل تحديثات قواعد البيانات والتطبيقات من مصدر التحديث. إذا كانت هناك مصادر متعددة للتحديث، فسيتم تطبيق إعدادات الخادم الوكيل على جميع المصادر. إذا لم يكن خادم الوكيل مطلوبًا لبعض مصادر التحديث، فيمكنك تعطيل استخدام خادم وكيل في خصائص السياسة. Kaspersky Endpoint Security سوف يستخدم خادم وكيل للوصول إلى شبكة Kaspersky Security Network وخوادم التفعيل.

لتكوين اتصال لتحديث المصادر من خلال خادم الوكيل:

1. في النافذة الرئيسية لمكون Web Console، انقر فوق ⚙.
   سيتم فتح نافذة خصائص خادم الإدارة.

2. انتقل إلى القسم **Configuring Internet access**.

3. حدد خانة الاختيار **Use proxy server**.

4. تكوين إعدادات اتصال الخادم الوكيل وعنوان الخادم الوكيل والمنفذ وإعدادات المصادقة (اسم المستخدم وكلمة المرور).

5. احفظ تغييراتك.

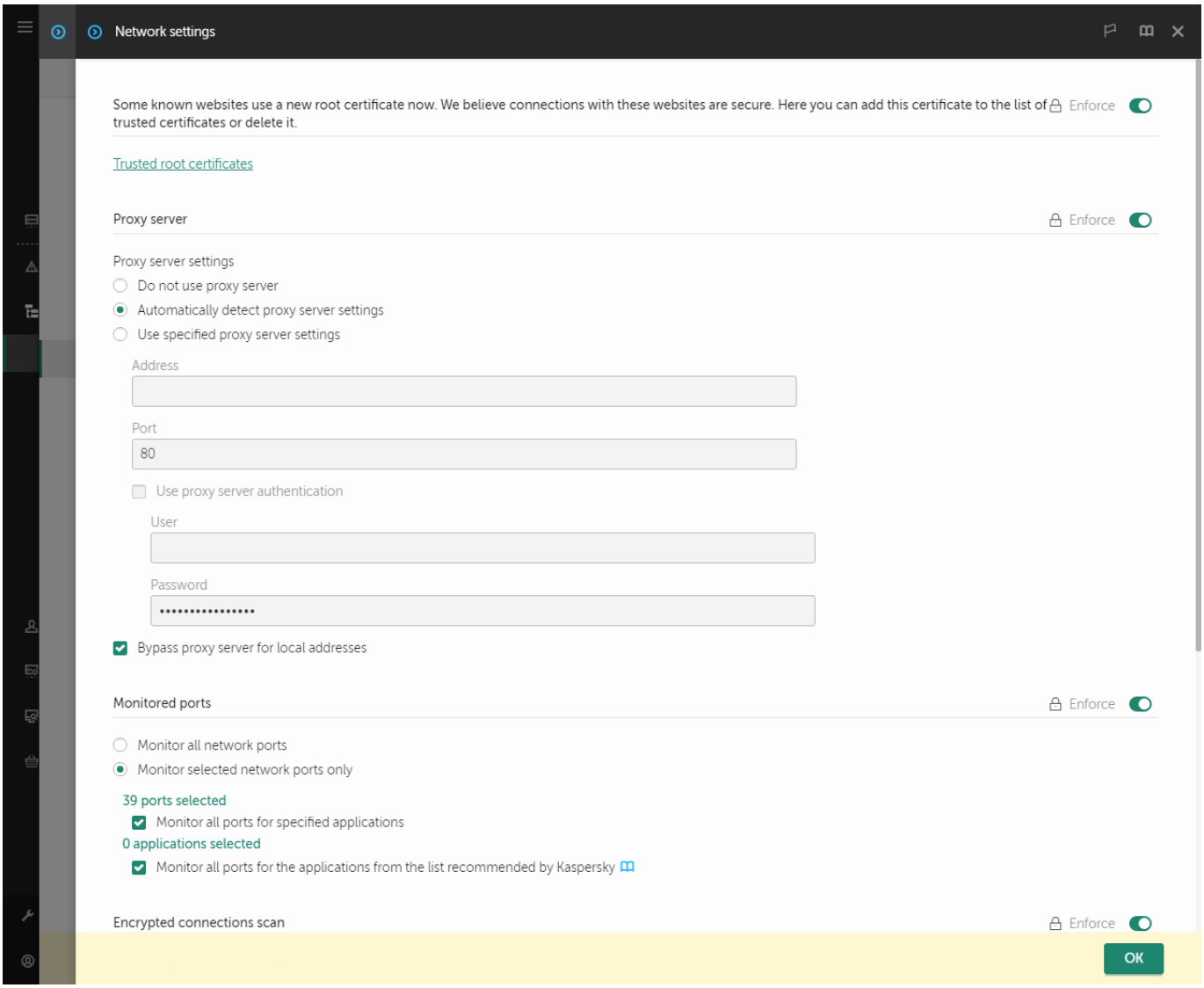
لتعطيل استخدام خادم وكيل لمجموعة إدارة محددة:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **الإعدادات العامة** ← **إعدادات الشبكة**.



إعدادات شبكة Kaspersky Endpoint Security for Windows.

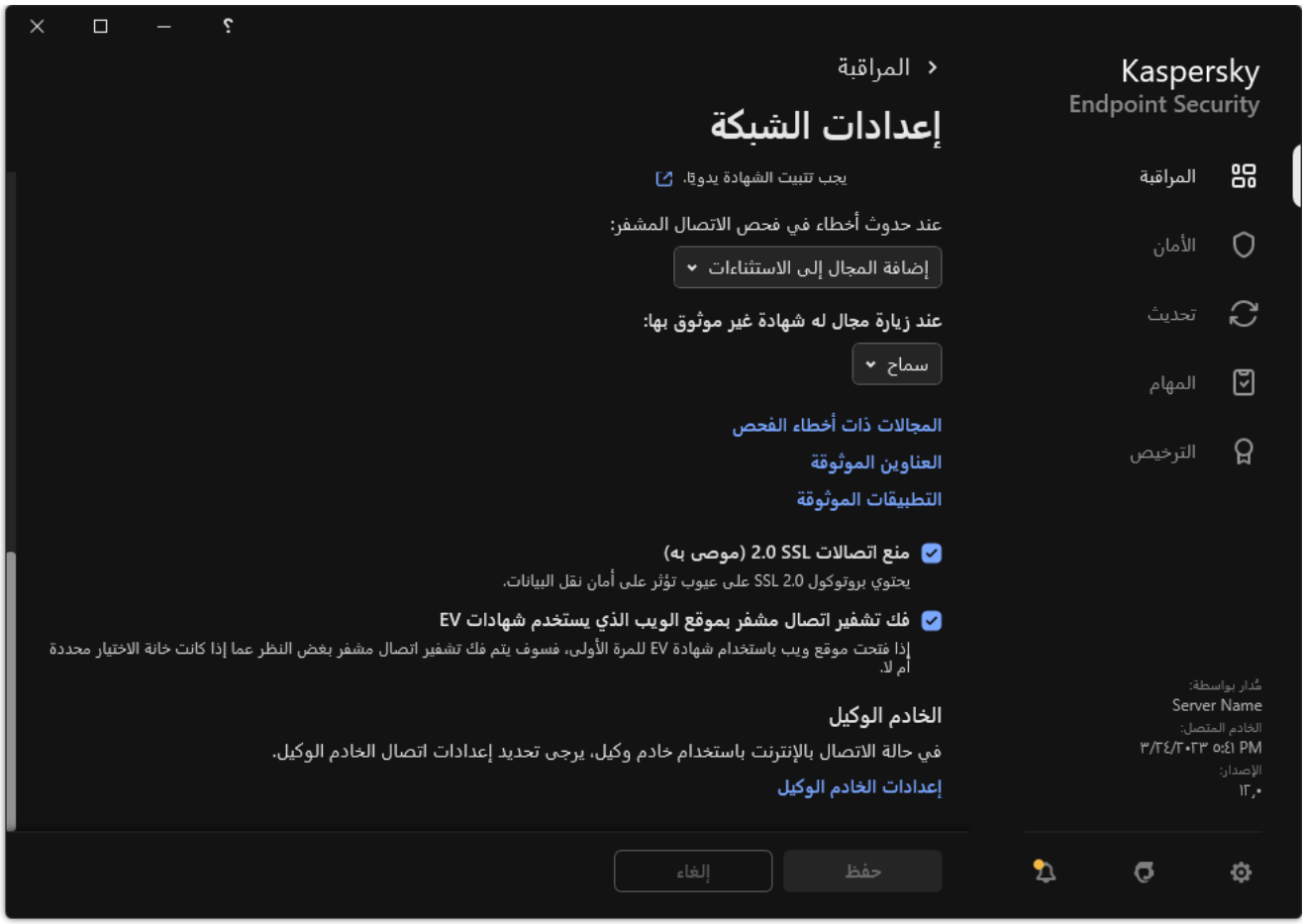
5. في القسم **Proxy server settings**، حدد **Bypass proxy server for local addresses**.

6. احفظ تغييراتك.

لتكوين إعدادات الخادم الوكيل في واجهة التطبيق:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.



إعدادات شبكة التطبيق

3. في القسم **الخادم الوكيل**، انقر على الرابط **إعدادات الخادم الوكيل**.

إعدادات اتصال الخادم الوكيل

4. في النافذة التي تفتح، حدد أحد الخيارات التالية لتحديد عنوان الخادم الوكيل:

- **اكتشاف إعدادات الخادم الوكيل تلقائيًا**.

  ويتم تحديد هذا الخيار بشكل افتراضي. يستخدم Kaspersky Endpoint Security إعدادات الخادم الوكيل المحددة في إعدادات نظام التشغيل.

- **استخدام إعدادات محددة للخادم الوكيل**.

  إذا حددت هذا الخيار، فقم بتكوين الإعدادات للاتصال بالخادم الوكيل: عنوان الخادم الوكيل والمنفذ.

5. إذا كنت تريد تمكين المصادقة على الخادم الوكيل، فحدد خانة الاختيار **استخدام مصادقة الخادم الوكيل** وقدم بيانات اعتماد حساب المستخدم الخاص بك.

6. إذا كنت تريد تعطيل استخدام الخادم الوكيل عند تحديث قواعد البيانات والوحدات النمطية للتطبيق من مجلد مشترك، حدد خانة الاختيار **تجاوز الخادم الوكيل للعناوين المحلية**.

7. احفظ تغييراتك.

نتيجة لذلك، سيستخدم Kaspersky Endpoint Security الخادم الوكيل لتنزيل الوحدة النمطية للتطبيق وتحديثات قاعدة البيانات. سيستخدم Kaspersky Endpoint Security أيضًا الخادم الوكيل للوصول إلى خوادم KSN وخوادم التفعيل من Kaspersky. إذا كانت المصادقة مطلوبة على الخادم الوكيل، لكن لم يتم تقديم بيانات اعتماد حساب المستخدم أو كانت غير صحيحة، فسيطالبك Kaspersky Endpoint Security بإدخال اسم المستخدم وكلمة المرور.

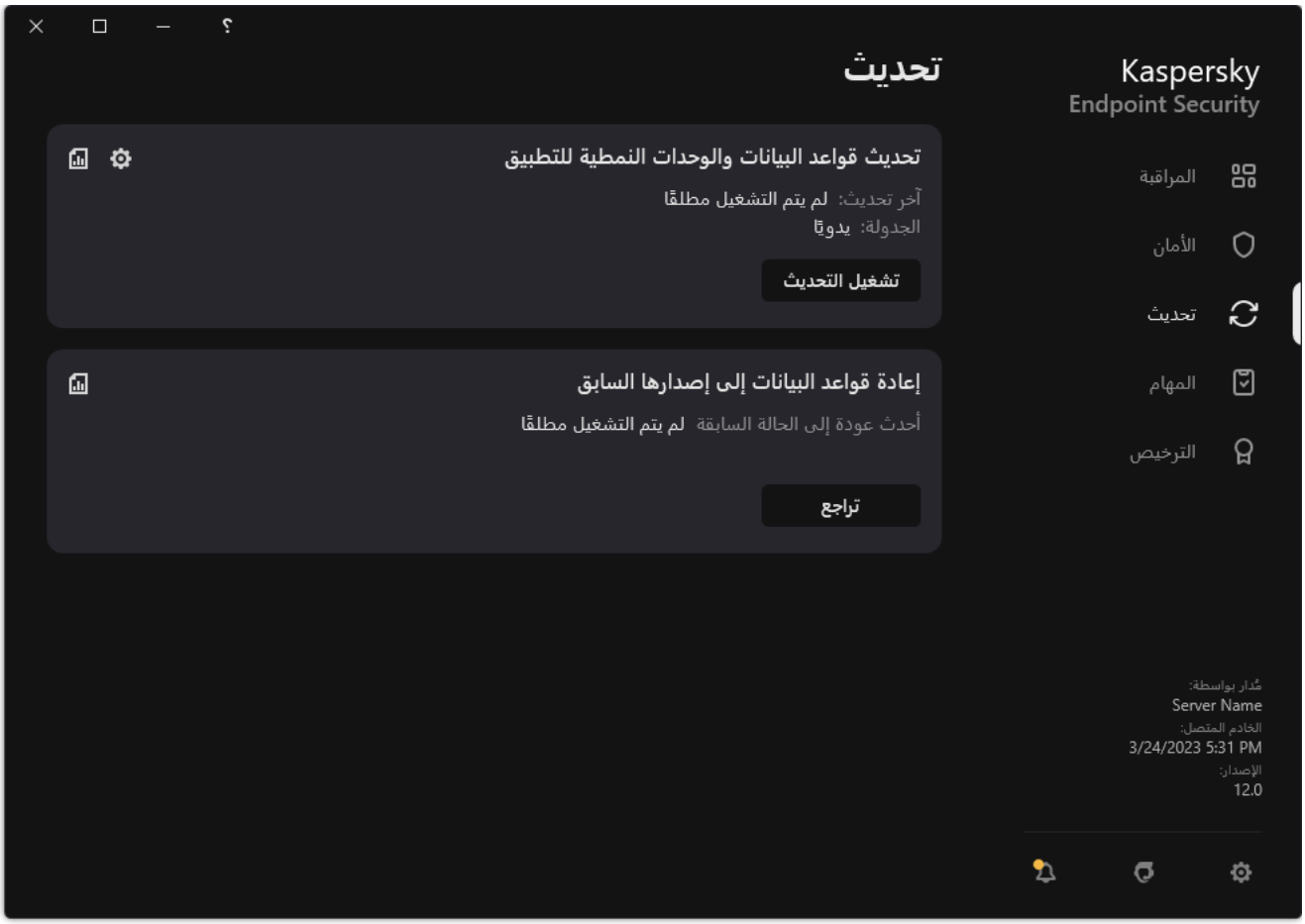
استرجاع آخر تحديث

بعد تحديث قواعد البيانات والوحدات النمطية للتطبيق النمطية للمرة الأولى، تتوفر وظيفة الرجوع إلى الإصدارات السابقة من قواعد البيانات ووحدات التطبيق النمطية.

في كل مرة يبدأ فيها المستخدم عملية التحديث، يُنشئ برنامج Kaspersky Endpoint Security نسخة احتياطية من وحدات التطبيق النمطية وقواعد البيانات الحالية. ويتيح لك هذا الرجوع إلى الإصدارات السابقة من قواعد البيانات ووحدات التطبيق النمطية عند الضرورة. ويُعد التراجع عن آخر تحديث أمرًا مفيدًا عندما يحتوي إصدار جديد من قاعدة البيانات على توقيع غير صالح يؤدي ببرنامج Kaspersky Endpoint Security إلى منع تطبيق آمن، على سبيل المثال.

للتراجع عن آخر تحديث:

1. في نافذة التطبيق الرئيسية، انتقل إلى القسم **تحديث**.



مهام التحديث المحلية

2. في الإطار **إعادة قواعد البيانات إلى إصدارها السابق**، انقر فوق الزر **تراجع**.

سيبدأ Kaspersky Endpoint Security في التراجع إلى آخر تحديث لقاعدة البيانات. وسيعرض التطبيق تقدم التراجع وحجم الملفات التي يتم تنزيلها ومصدر التحديث. يمكنك إيقاف المهمة في أي وقت بالنقر فوق الزر **إيقاف التحديث**.

لبدء أو إيقاف مهمة تراجع عند عرض واجهة التطبيق المبسطة:

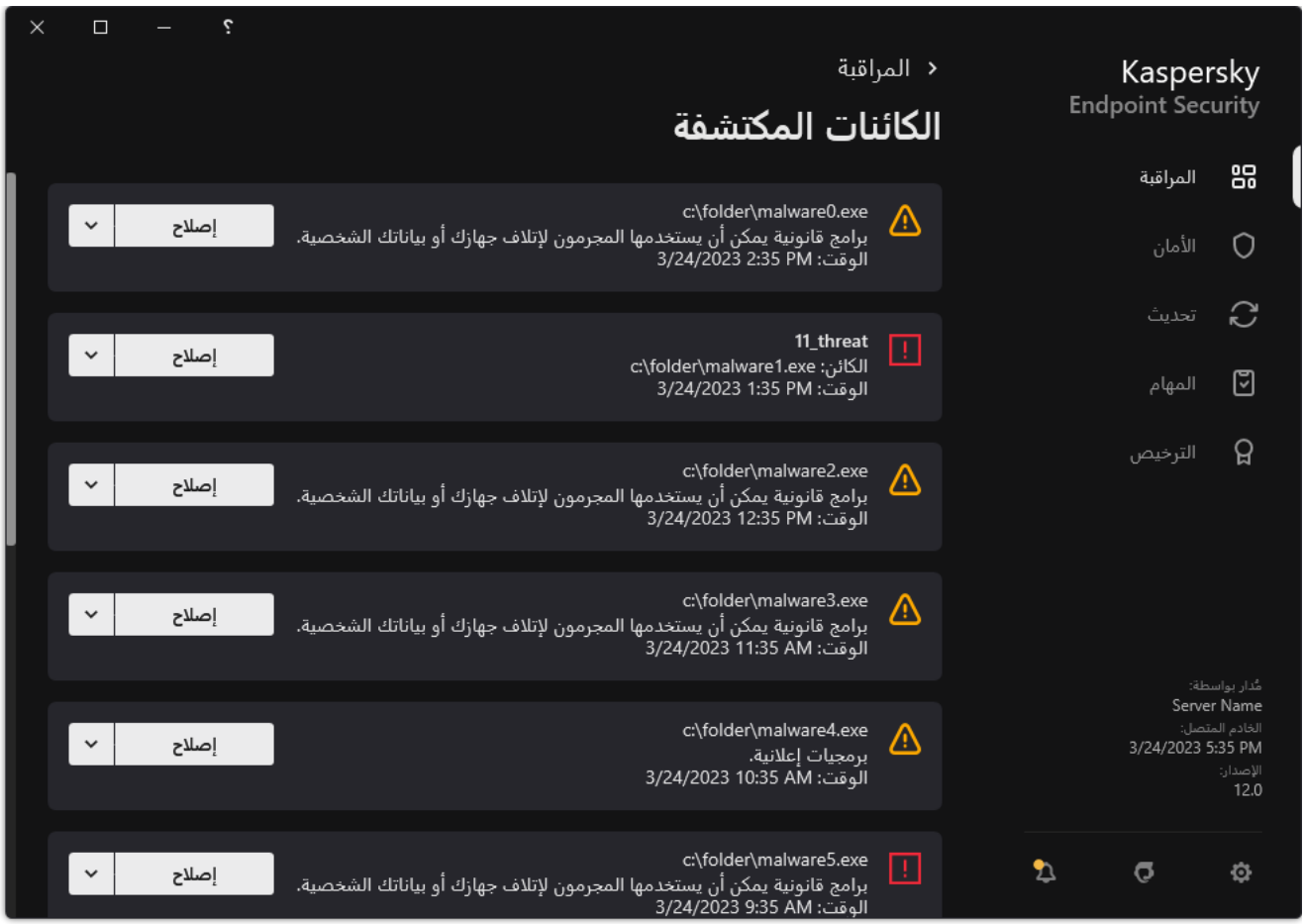
1. انقر بزر الماوس الأيمن لإظهار القائمة السياقية الخاصة بأيقونة التطبيق في منطقة إعلام شريط المهام.

2. في القائمة المنسدلة **المهام** في قائمة السياق، نفذ أحد ما يلي:

- حدد مهمة تراجع ليست قيد التشغيل لبدء تشغيلها.
- حدد مهمة تراجع قيد التشغيل لإيقافها.
- حدد مهمة تراجع متوقفة مؤقتًا لاستئنافها أو إعادة بدء تشغيلها.

التعامل مع التهديدات النشطة

يقوم Kaspersky Endpoint Security بتسجيل معلومات حول الملفات التي لم يتم علاجها لبعض الأسباب. ويتم تسجيل هذه المعلومات في نموذج أحداث في قائمة التهديدات النشطة (انظر الشكل أدناه). وللتعامل مع التهديدات النشطة، يستخدم Kaspersky Endpoint Security تقنية التنظيف المتقدم. ويعمل التنظيف المتقدم بشكل مختلف لمحطات العمل والخوادم. ويمكنك تكوين التنظيف المتقدم في إعدادات مهمة فحص البرامج الضارة وفي إعدادات التطبيق.



قائمة بالتهديدات النشطة

تنظيف التهديدات النشطة على محطات العمل

للتعامل مع التهديدات النشطة على محطات العمل، قم بتمكين تقنية التنظيف المتقدم في إعدادات التطبيق. بعد ذلك، قم بتكوين تجربة المستخدم في ملف خصائص مهمة فحص البرامج الضارة. توجد خانة اختيار **تشغيل التنظيف المتقدم على الفور** في خصائص المهمة. وفي حالة تعيين العلامة، سوف ينفذ Kaspersky Endpoint Security عملية التنظيف دون إخطار المستخدم. وعند اكتمال التنظيف، سيتم إعادة تشغيل الكمبيوتر. وإذا لم يتم تعيين العلامة، سيعرض Kaspersky Endpoint Security إخطارًا حول التهديدات النشطة (انظر الشكل أدناه). ولا يمكنك إغلاق هذا الإخطار دون معالجة الملف.

يتم تنفيذ التنظيف المتقدم أثناء مهمة فحص فيروسات على جهاز كمبيوتر فقط في حالة تمكين ميزة التنظيف المتقدم في خصائص السياسة المطبقة على هذا الكمبيوتر.

الإخطار حول التهديد النشط

تنظيف التهديدات النشطة على الخوادم

للتعامل مع التهديدات النشطة على الخوادم، يتعين عليك تنفيذ ما يلي:

- تمكين تقنية التنظيف المتقدم في إعدادات التطبيق؛
- تمكين التنظيف المتقدم الفوري في خصائص مهمة فحص البرامج الضارة.

في حالة تثبيت Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام Windows for Servers، فلن يعرض Kaspersky Endpoint Security الإخطار. ولذلك، لا يستطيع المستخدم تحديد إجراء لتنظيف تهديد نشط. ولتنظيف تهديد، تحتاج إلى enable Advanced Disinfection technology في إعدادات التطبيق وenable immediate Advanced Disinfection في إعدادات مهمة فحص البرامج الضارة. بعد ذلك يتعين عليك بدء مهمة فحص البرامج الضارة.

تمكين أو تعطيل تقنية التنظيف المتقدمة

إذا لم يتمكن Kaspersky Endpoint Security من إيقاف تنفيذ جزء من البرامج الضارة، فيمكنك استخدام تقنية التنظيف المتقدم. وبشكل افتراضي، يتم تعطيل التنظيف المتقدم لأن هذه التقنية تستخدم قدرًا كبيرًا من موارد الحوسبة. لذلك، يمكنك تمكين التنظيف المتقدم فقط عند التعامل مع التهديدات النشطة.

ويعمل التنظيف المتقدم بشكل مختلف لمحطات العمل والخوادم. ولاستخدام التقنية على الخوادم، يجب تمكين التنظيف الفوري المتقدم في خصائص مهمة فحص البرامج الضارة. وهذا الشرط الأساسي ليس ضروريًا لاستخدام التقنية على محطات العمل.

كيفية تمكين أو تعطيل تقنية التنظيف المتقدمة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.

5. في القسم **وضع التشغيل**، حدد أو امسح خانة الاختيار **تمكين تقنية التنظيف المتقدم** لتمكين تقنية التنظيف المتقدم أو تعطيلها.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل تقنية التنظيف المتقدمة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. حدد **Application Settings** ← **General settings**.

5. في القسم **Operating mode**، حدد أو امسح خانة الاختيار **Enable Advanced Disinfection technology** لتمكين تقنية التنظيف المتقدم أو تعطيلها.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل تقنية التنظيف المتقدمة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.

إعدادات Kaspersky Endpoint Security for Windows

3. في القسم **وضع التشغيل**، حدد أو امسح خانة الاختيار **استخدام تقنية التنظيف المتقدم (تتطلب موارد كمبيوتر كبيرة)** لتمكين تقنية التنظيف المتقدم أو تعطيلها.

4. احفظ تغييراتك.

نتيجة لذلك، لا يستطيع المستخدم استخدام معظم ميزات نظام التشغيل أثناء تنفيذ التنظيف الفعال. وعند اكتمال التنظيف، تتم إعادة تشغيل الكمبيوتر.

معالجة التهديدات النشطة

يعتبر الملف المصاب تمت معالجته إذا نظف Kaspersky Endpoint Security الملف أو أزال التهديد كجزء من فحص الكمبيوتر للبحث عن الفيروسات والبرامج الضارة الأخرى.

ينقل Kaspersky Endpoint Security الملف إلى قائمة التهديدات النشطة إذا فشل Kaspersky Endpoint Security لأي سبب في تنفيذ إجراء على هذا الملف وفقًا للإعدادات التطبيق المحددة أثناء فحص الكمبيوتر للبحث عن الفيروسات والتهديدات الأخرى.

يكون هذا الوضع ممكنًا في الحالات التالية:

- الملف الممسوح إلكترونيًا غير متاح (كأن يكون موجود على محرك أقراص شبكة أو محرك أقراص قابل للإزالة بدون امتيازات كتابة).
- في إعدادات مهمة فحص البرامج الضارة ، يتم تعيين الإجراء المطلوب اتخاذه عند اكتشاف تهديد على **إخطار**. وبعد ذلك، عندما يتم عرض إخطار الملف المصاب على الشاشة، حدد المستخدم **تخطي**.

في حالة وجود أي تهديدات لم تتم معالجتها، يُغير Kaspersky Endpoint Security الأيقونة إلى . في نافذة التطبيق الرئيسية ، يتم عرض إخطار التهديد (انظر الشكل أدناه). وفي وحدة تحكم Kaspersky Security Center، يتم تغيير حالة الكمبيوتر إلى حرج – .

كيفية معالجة تهديد في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى المجلد **خادم الإدارة** ← **إضافي** ← **المستودعات** ← **التثبيت عن بُعد**.
تفتح قائمة التهديدات النشطة.
2. حدد الكائن الذي تريد معالجته.
3. اختر الطريقة التي تريد التعامل بها مع التهديد:
   - **تنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات.
   - **حذف**.

كيفية معالجة تهديد في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Active threats** ← **Repositories** ← **Operations**.
تفتح قائمة التهديدات النشطة.
2. حدد الكائن الذي تريد معالجته.
3. اختر الطريقة التي تريد التعامل بها مع التهديد:
   - **Disinfect**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات.
   - **Delete**.

كيفية معالجة تهديد في واجهة التطبيق

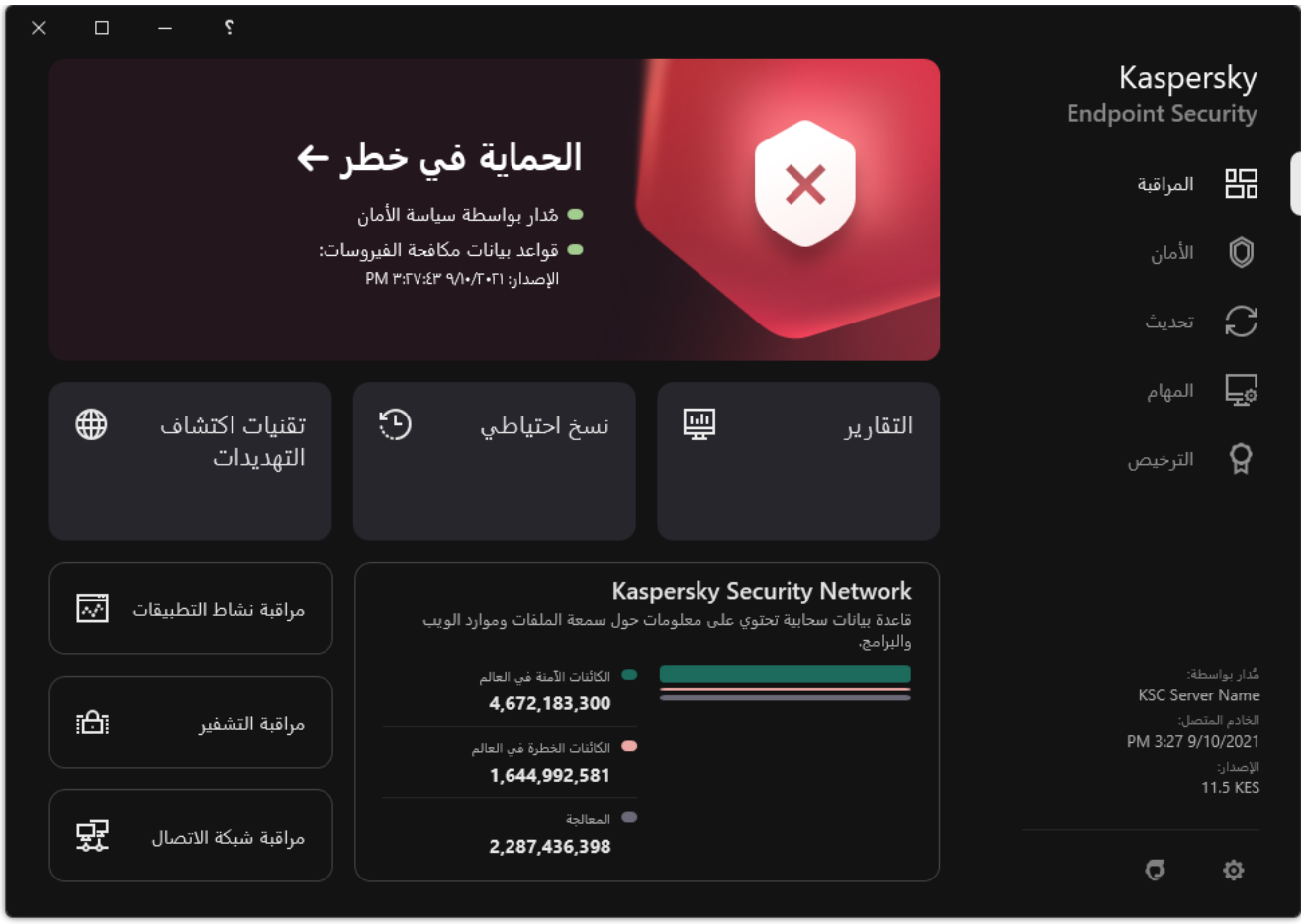
1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **الحماية في خطر**.

تفتح قائمة التهديدات النشطة.

2. حدد الكائن الذي تريد معالجته.

3. اختر الطريقة التي تريد التعامل بها مع التهديد:

- **إصلاح**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات.
- **إضافة إلى الاستثناءات**. في حالة تحديد هذا الإجراء، يقترح Kaspersky Endpoint Security إضافة الملف إلى قائمة استثناءات الفحص. ويتم تكوين إعدادات الاستثناء تلقائيًا. وفي حالة عدم توفر إضافة استثناء، فهذا يعني أن المسؤول قد قام بتعطيل إضافة الاستثناءات في إعدادات السياسة.
- **تجاهل**. في حالة تحديد هذا الخيار، يحذف Kaspersky Endpoint Security الإدخال من قائمة التهديدات النشطة. وفي حالة عدم وجود تهديدات نشطة متبقية في القائمة، فسيتم تغيير حالة الكمبيوتر إلى موافق. وفي حالة اكتشاف الكائن مرة أخرى، سيضيف Kaspersky Endpoint Security إدخالاً جديدًا إلى قائمة التهديدات النشطة.
- **فتح مجلد الاحتواء**. في حالة تحديد هذا الخيار، يفتح Kaspersky Endpoint Security المجلد الذي يحتوي على الكائن في مدير الملفات. ويمكنك بعد ذلك حذف الكائن يدويًا أو نقله إلى مجلد ليس ضمن نطاق الحماية.
- **معرفة المزيد**. في حالة تحديد هذا الخيار، يفتح Kaspersky Endpoint Security موقع ويب موسوعة الفيروسات من Kaspersky.



نافذة التطبيق الرئيسية عند اكتشاف تهديد

الحماية من تهديدات الملفات

يتيح لك مكون الحماية من تهديدات الملفات منع إصابة نظام الملفات في جهاز الكمبيوتر. بشكل افتراضي، يوجد مكون الحماية من تهديدات الملفات بشكل دائم في ذاكرة الوصول العشوائي للكمبيوتر. يقوم المكون بفحص الملفات على كافة محركات الأقراص للكمبيوتر وكذلك على محركات الأقراص المتصلة. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

يقوم المكون بفحص الملفات التي تم الوصول إليها بواسطة المستخدم أو التطبيق. إذا تم الكشف عن ملف ضار، يقوم Kaspersky Endpoint Security بحظر عمل الملف. يقوم التطبيق بعد ذلك بتطهير أو حذف الملف الضار، وذلك اعتمادًا على إعدادات مكون الحماية من تهديدات الملفات.

عند محاولة الوصول إلى ملف تم حفظ محتوياته في خدمة التخزين عبر الإنترنت OneDrive، يقوم Kaspersky Endpoint Security بتنزيل وفحص محتويات الملف.

تمكين وتعطيل الحماية من تهديدات الملفات

بشكل افتراضي، يتم تكوين مكون الحماية من تهديدات الملفات وتشغيله في الوضع الموصى به من خبراء Kaspersky. للحماية من تهديدات الملفات، يستطيع Kaspersky Endpoint Security تطبيق مجموعات مختلفة من الإعدادات. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان: **مرتفع**، **مستحسن**، **منخفض**. وتُعد إعدادات مستوى الأمان **مستحسن** الإعدادات المُثلى التي يوصي بها خبراء Kaspersky (انظر الجدول أدناه). يمكنك تحديد أحد مستويات الأمان المعدة مسبقًا أو تكوين إعدادات مستوى الأمان يدويًا. في حالة تغيير إعدادات مستوى الأمان، يمكنك دائمًا العودة إلى إعدادات مستوى الأمان الموصى بها.

لتمكين أو تعطيل مكون الحماية من تهديدات الملفات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.
3. استخدم مفتاح تبديل **الحماية من تهديدات الملفات** لتمكين المكون أو تعطيله.
4. في حالة قيامك بتمكين المكون، نفذ أحد الإجراءات التالية في القسم **مستوى الأمان**:

- إذا كنت تريد استخدام أحد مستويات الأمان المعدة مسبقًا، فقم بتحديده باستخدام شريط التمرير:

- **مرتفع**. عندما يتم تحديد مستوى أمان الملف هذا، يتحكم مكون الحماية من تهديدات الملفات بأقصى صرامة في كل الملفات التي يتم فتحها وحفظها وبدء تشغيلها. ويفحص مكون الحماية من تهديدات الملفات كل أنواع الملفات على كل محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة من الكمبيوتر. يقوم أيضًا بفحص الأرشيفات وحزم التثبيت وكائنات OLE المضمنة.
- **مستحسن**. يوصي خبراء Kaspersky Lab بمستوى أمان الملف هذا. ويفحص مكون الحماية من تهديدات الملفات فقط تنسيقات الملفات المحددة على جميع محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة على الكمبيوتر وكائنات OLE المضمنة. لا يفحص مكون الحماية من تهديدات الملفات الأرشيفات وحزم التثبيت. يتم توفير قيم الإعدادات لمستوى الأمان المستحسن في الجدول أدناه.
- **منخفض**. تضمن إعدادات مستوى أمان الملف هذه الوصول لسعة الفحص القصوى. ولا يفحص مكون الحماية من تهديدات الملفات إلا الملفات ذات الامتدادات المحددة على كل محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة من الكمبيوتر. ولا يقوم مكون الحماية من تهديدات الملفات بفحص الملفات المركبة.

- إذا كنت ترغب في تكوين مستوى أمان مخصص، فانقر فوق الزر **إعدادات متقدمة** وحدد إعدادات المكون الخاص بك.

يمكنك استعادة قيم مستويات الأمان المعينة مسبقًا بالنقر فوق الزر **استعادة مستوى الأمان الموصى به**.

5. احفظ تغييراتك.

إعدادات الحماية من تهديدات الملفات الموصى بها من خبراء Kaspersky (مستوى الأمان المستحسن)

المعلمة	القيمة	الوصف
أنواع الملفات	**الملفات التي تم فحصها حسب التنسيق**	إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. قبل فحص أحد الملفات بحثًا عن التعليمات البرمجية الضارة، يتم تحليل العنوان الداخلي للملف لتحديد تنسيق الملف (على سبيل المثال، .txt أو .doc أو .exe). ويبحث الفحص أيضًا عن الملفات بملحقات ملف معينة.
التحليل المساعد على الاكتشاف	**فحص خفيف**	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف. عند فحص الملفات للبحث عن تعليمات برمجية ضارة، ينفذ المحلل المساعد على الاكتشاف الإرشادات الواردة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
فحص الملفات الجديدة والتي تم تغييرها فقط	**تشغيل**	يفحص فقط الملفات الجديدة والملفات التي تم تعديلها منذ آخر مرة لفحصها. هذا يساعد على تقليل فترة الفحص. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.
استخدام تقنية iSwift	**تشغيل**	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.
استخدام تقنية iChecker	**تشغيل**	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).
فحص الملفات بتنسيقات Microsoft Office	**تشغيل**	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
وضع الفحص	**الوضع الذكي**	في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائن بناءً على تحليل الإجراءات المتخذة على الكائن. على سبيل المثال، عند العمل على مستند Microsoft Office، يفحص Kaspersky Endpoint Security الملف عند فتحه لأول مرة وإغلاقه لآخر مرة. أما العمليات التي تجرى أثناء فتح الملف والتي يتم فيها استبدال الملف فلا تتسبب في فحصه.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**تنظيف؛ حذف إذا فشل التنظيف**	في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات.

الإيقاف التلقائي المؤقت للحماية من تهديدات الملفات

يمكنك تكوين الحماية من تهديدات الملفات لإيقافها مؤقتًا تلقائيًا في وقت محدد أو عند العمل باستخدام برامج معينة.

ينبغي إيقاف الحماية من تهديدات الملفات مؤقتًا فقط كحل أخير عندما تتعارض مع بعض التطبيقات. في حالة ظهور أي تعارض أثناء تشغيل أحد المكونات، يُنصح بالاتصال بالدعم الفني من Kaspersky. سوف يساعدك خبراء الدعم على إعداد مكون الحماية من تهديدات الملفات لتعمل في وقت واحد مع التطبيقات الأخرى على جهاز الكمبيوتر الخاص بك.

لتكوين الإيقاف المؤقت التلقائي للحماية من تهديدات الملفات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الملفات**.
3. انقر على **إعدادات متقدمة**.
4. في القسم **إيقاف الحماية من تهديد الملفات مؤقتًا**، انقر على الرابط **إيقاف الحماية من تهديد الملفات مؤقتًا**.
5. في النافذة التي تفتح، كوّن الإعدادات لإيقاف الحماية من تهديدات الملفات مؤقتًا:
   a. كوّن جدولاً لإيقاف الحماية من تهديدات الملفات مؤقتًا بشكل تلقائي.
   b. أنشئ قائمة بالتطبيقات التي يجب أن يتسبب تشغيلها في إيقاف الحماية من تهديدات الملفات لأنشطتها مؤقتًا.
6. احفظ تغييراتك.

تغيير الإجراءات التي تتخذها الملفات المصابة بواسطة مكون الحماية من تهديدات الملفات

بشكل افتراضي، يحاول مكون الحماية من تهديدات الملفات تلقائيًا تنظيف كل الملفات المصابة المكتشفة. وإذا فشل التنظيف، يحذف مكون الحماية من تهديدات الملفات هذه الملفات.

لتغيير الإجراءات التي تتخذها الملفات المصابة بواسطة مكون الحماية من تهديدات الملفات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الملفات**.
3. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد الخيار المناسب:

- **تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات.
- **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا تعذر التنظيف، يضيف Kaspersky Endpoint Security معلومات حول الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة.
- **منع**. في حالة تحديد هذا الخيار، فإن مكون الحماية من تهديدات الملفات يمنع تلقائيًا كل الملفات المصابة دون محاولة تنظيفها.

قبل محاولة تنظيف ملف مصاب أو حذفه، ينشئ التطبيق نسخة احتياطية من الملف في حال احتجت إلى استعادة الملف أو إذا كان من الممكن تنظيفه في المستقبل.

4. احفظ تغييراتك.

تشكيل نطاق الحماية لمكون الحماية من تهديدات الملفات

يشير نطاق الحماية إلى الكائنات التي يقوم المكون بفحصها عند تمكينه. تتمتع نطاقات الحماية للمكونات المختلفة بخصائص مختلفة. يعتبر موقع الملفات التي سيتم فحصها ونوعها خصائص لنطاق الحماية لمكون الحماية من تهديدات الملفات. ويفحص مكون الحماية من تهديدات الملفات بشكل افتراضي الملفات المحتمل قابليتها للإصابة فقط التي تعمل من محركات الأقراص الثابتة محركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة.

عند تحديد نوع الملفات المراد فحصها، تذكر ما يلي:

1. يوجد احتمالية ضعيفة لدخول رمز خبيث إلى ملفات صيغ معينة وتفعيلها التابع (مثل صيغة TXT). وفي الوقت نفسه، توجد صيغ ملفات تحتوي على رموز تنفيذية (مثل exe. وdll.) أو يمكن أن تحتوي عليها. يمكن للرمز التنفيذ أن يوجد كذلك على جميع الصيغ غير المستهدف استخدامها في هذا الغرض (مثل صيغة DOC). وتكون نسبة خطر اختراق الرموز الضارة وتفعيلها في مثل هذه الملفات عالية.

2. يمكن لأي دخيل إرسال فيروس أو تطبيق خبيث آخر إلى جهازك في ملف تنفيذي تمت إعادة تسميته بملحق txt. إذا اخترت فحص الملفات حسب الامتداد، فيتخطى التطبيق هذا الملف أثناء الفحص. وفي حالة تحديد فحص الملفات حسب التنسيق، يحلل Kaspersky Endpoint Security رأس الملف بغض النظر عن ملحقه. إذا أظهر هذا التحليل أن الملف له تنسيق الملف التنفيذي (على سبيل المثال، EXE)، فإن التطبيق يقوم بفحصه.

لإنشاء نطاق الحماية:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الملفات**.

3. انقر على **إعدادات متقدمة**.

4. في القسم **أنواع الملفات**، حدد نوع الملفات التي ترغب في فحصها بواسطة مكون الحماية من تهديدات الملفات:

- **كل الملفات**. إذا تم تمكين هذا الإعداد، فإن Kaspersky Endpoint Security يفحص كل الملفات دون استثناء (كل التنسيقات والامتدادات).
- **الملفات التي تم فحصها حسب التنسيق**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. قبل فحص أحد الملفات بحثًا عن التعليمات البرمجية الضارة، يتم تحليل العنوان الداخلي للملف لتحديد تنسيق الملف (على سبيل المثال، .txt أو .doc أو .exe). ويبحث الفحص أيضًا عن الملفات بملحقات ملف معينة.
- **الملفات التي تم فحصها حسب الامتداد**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. ويتم تحديد تنسيق الملف عندئذٍ استنادًا إلى امتداد الملف.

5. انقر على رابط **تحرير نطاق الحماية**.

6. في النافذة التي تفتح، حدد الكائنات التي تريد إضافتها إلى نطاق الحماية أو استثنائها منه.

لا يمكنك إزالة أو تحرير الكائنات المضمنة في نطاق الحماية الافتراضي.

7. إذا كنت تريد إضافة كائن جديد إلى نطاق الحماية:

a. انقر على **إضافة**.

تفتح شجرة المجلد.

b. حدد كائنًا لإضافته إلى نطاق الحماية.

يمكنك استثناء كائن من عمليات الفحص دون حذفه من قائمة الكائنات في نطاق الفحص. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

8. احفظ تغييراتك.

استخدام طرق الفحص

يستخدم Kaspersky Endpoint Security أسلوب فحص يسمى التعلم الآلي وتحليل التوقيع. أثناء تحليل التوقيع، يطابق Kaspersky Endpoint Security الكائن الذي تم اكتشافه مع السجلات في قواعد بياناته. بناءً على توصيات خبراء Kaspersky، يتم تمكين التعلّم الآلي وتحليل التوقيع دائمًا.

لزيادة كفاءة الحماية، يمكنك استخدام التحليل المساعد على الاكتشاف. عند فحص الملفات للبحث عن تعليمات برمجية ضارة، ينفذ المحلل المساعد على الاكتشاف الإرشادات الواردة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.

لتكوين استخدام التحليل المساعد على الاكتشاف في تشغيل مكون الحماية من تهديدات الملفات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.
3. انقر على **إعدادات متقدمة**.
4. إذا كنت تريد أن يستخدم التطبيق التحليل المساعد على الاكتشاف من تهديدات الملفات، فحدد خانة الاختيار **التحليل المساعد على الاكتشاف** في القسم **طرق الفحص**. بعدها استخدم شريط التمرير لضبط مستوى التحليل المساعد على الاكتشاف: **فحص خفيف** أو **فحص متوسط** أو **فحص عميق**.
5. احفظ تغييراتك.

استخدام تقنيات الفحص في تشغيل مكون الحماية من تهديدات الملفات

لتكوين استخدام تقنيات الفحص في تشغيل مكون الحماية من تهديدات الملفات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.
3. انقر على **إعدادات متقدمة**.
4. في كتلة **تقنيات الفحص**، حدد خانات الاختيار المجاورة لأسماء التقنيات التي ترغب في استخدامها للحماية من تهديدات الملفات:
   - **استخدام تقنية iSwift**. تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.
   - **استخدام تقنية iChecker**. تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).
5. احفظ تغييراتك.

تحسين فحص الملفات

يمكنك تحسين فحص الملفات الذي يتم تنفيذه بواسطة مكون الحماية من تهديدات الملفات، مما يؤدي إلى تقليل الوقت المستغرق في الفحص وزيادة سرعة تشغيل برنامج Kaspersky Endpoint Security. يمكن تحقيق ذلك عن طريق فحص الملفات الجديدة والملفات التي تم تعديلها فقط منذ إجراء الفحص السابق. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.

يمكنك أيضًا تمكين استخدام تقنيتي iChecker و iSwift، اللتين تعملان على زيادة سرعة عملية فحص الملفات عن طريق استثناء الملفات التي لم يتم تعديلها منذ إجراء آخر عملية فحص.

لتحسين فحص الملفات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.
3. انقر على **إعدادات متقدمة**.
4. في القسم **التحسين**، حدد خانة الاختيار **فحص الملفات الجديدة والتي تم تغييرها فقط**.
5. احفظ تغييراتك.

فحص الملفات المركبة

يعتبر زرع الفيروسات والبرامج الضارة في الملفات المركّبة، مثل ملفات الأرشيف أو قواعد البيانات من الأساليب الشائعة لإخفاء الفيروسات والبرمجيات الضارة الأخرى. ولاكتشاف الفيروسات والبرمجيات الضارة الأخرى المختبئة بهذه الطريقة، يجب فك حزمة الملف المركب، وهو الأمر الذي قد يؤدي إلى إبطاء عملية الفحص. يمكنك تقييد أنواع الملفات المركبة المطلوب فحصها، وبالتالي زيادة سرعة عملية الفحص.

وتعتمد الطريقة التي يتم بها معالجة ملف مركب مصاب (التطهير أو الحذف) على نوع الملف.

يتولى مكون الحماية من تهديدات الملفات تنظيف الملفات المركبة بتنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE ويحذف الملفات بجميع التنسيقات الأخرى (باستثناء قواعد بيانات البريد).

لتكوين فحص الملفات المركبة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.
3. انقر على **إعدادات متقدمة**.
4. في القسم **فحص الملفات المركبة**، حدد أنواع الملفات المركبة التي تريد فحصها: ملفات الأرشيف، أو حِزم التثبيت، أو الملفات بتنسيقات office.
5. في حالة تعطيل فحص الملفات الجديدة والمعدلة فقط، كوّن الإعدادات لفحص كل نوع من أنواع الملفات المركبة: فحص جميع الملفات من هذا النوع أو الملفات الجديدة فقط.

   في حالة تمكين فحص الملفات الجديدة والمعدلة فقط، فإن Kaspersky Endpoint Security يفحص فقط الملفات الجديدة والمعدلة لجميع أنواع الملفات المركبة.
6. تكوين الإعدادات المتقدمة لفحص الملفات المركبة.

- **عدم فك ضغط الملفات المركبة كبيرة الحجم**.

  في حالة تحديد هذا المربع، لا يقوم Kaspersky Endpoint Security بفحص الملفات المركبة إذا كان حجمها يتجاوز القيمة المحددة.

  في حالة إلغاء تحديد خانة الاختيار هذه، يقوم Kaspersky Endpoint Security بفحص الملفات المركبة بجميع الأحجام.

يفحص Kaspersky Endpoint Security الملفات كبيرة الحجم التي يتم استخراجها من الأرشيفات، بغض النظر عن تحديد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم** أم لا.

- **فك حزمة الملفات المركبة في الخلفية**.

في حالة تحديد خانة الاختيار، فإن Kaspersky Endpoint Security سيوفر الوصول إلى ملفات مركبة أكبر من القيمة المحددة قبل أن يتم فحص هذه الملفات. في هذه الحالة، فإن Kaspersky Endpoint Security يفك حزمة الملفات المركبة ويفحصها في الخلفية.

Kaspersky Endpoint Security لا يوفر الوصول إلى الملفات المركبة الأصفر من هذه القيمة إلا بعد فك حزمة هذه الملفات وفحصها.

في حالة عدم تحديد صندوق الاختيار، فإن Kaspersky Endpoint Security لا يوفر الوصول إلى الملفات المركبة إلا بعد فك الحزمة الملفات وفحصها، أيًا كان حجمها.

7. احفظ تغييراتك.

تغيير وضع الفحص

يشير القسم وضع الفحص إلى الشرط الذي يقوم بتشغيل فحص الملف بواسطة مكون الحماية من تهديدات الملفات. بشكل افتراضي، يقوم برنامج Kaspersky Endpoint Security بفحص الملفات في الوضع الذكي. في وضع فحص الملفات هذا، يقرر مكون الحماية من تهديدات الملفات ما إذا كان فحص الملفات سيتم أم لا بعد عمليات التحليل التي يتم تنفيذها على الملف بواسطة المستخدم أو بواسطة التطبيق بالنيابة عن المستخدم (من خلال الحساب الذي تم استخدامه لتسجيل الدخول أو حساب مستخدم مختلف) أو بواسطة نظام التشغيل. على سبيل المثال، عند العمل بمستند Microsoft Office Word، يقوم برنامج Kaspersky Endpoint Security بفحص الملف عند فتحه لأول مرة وإغلاقه لآخر مرة. أما العمليات التي تجرى أثناء فتح الملف والتي يتم فيها استبدال الملف فلا تتسبب في فحصه.

لتغيير وضع فحص الملف:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الملفات**.

3. انقر على **إعدادات متقدمة**.

4. في القسم **وضع الفحص**، حدد الوضع المطلوب:

- **الوضع الذكي**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائن بناءً على تحليل الإجراءات المتخذة على الكائن. على سبيل المثال، عند العمل على مستند Microsoft Office، يفحص Kaspersky Endpoint Security الملف عند فتحه لأول مرة وإغلاقه لآخر مرة. أما العمليات التي تجرى أثناء فتح الملف والتي يتم فيها استبدال الملف فلا تتسبب في فحصه.
- **عند الوصول والتعديل**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائنات عند وجود محاولة لفتحها أو تعديلها.
- **عند الوصول**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائنات عند محاولة فتحها فقط.
- **عند التنفيذ**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائنات عند محاولة تشغيلها فقط.

5. احفظ تغييراتك.

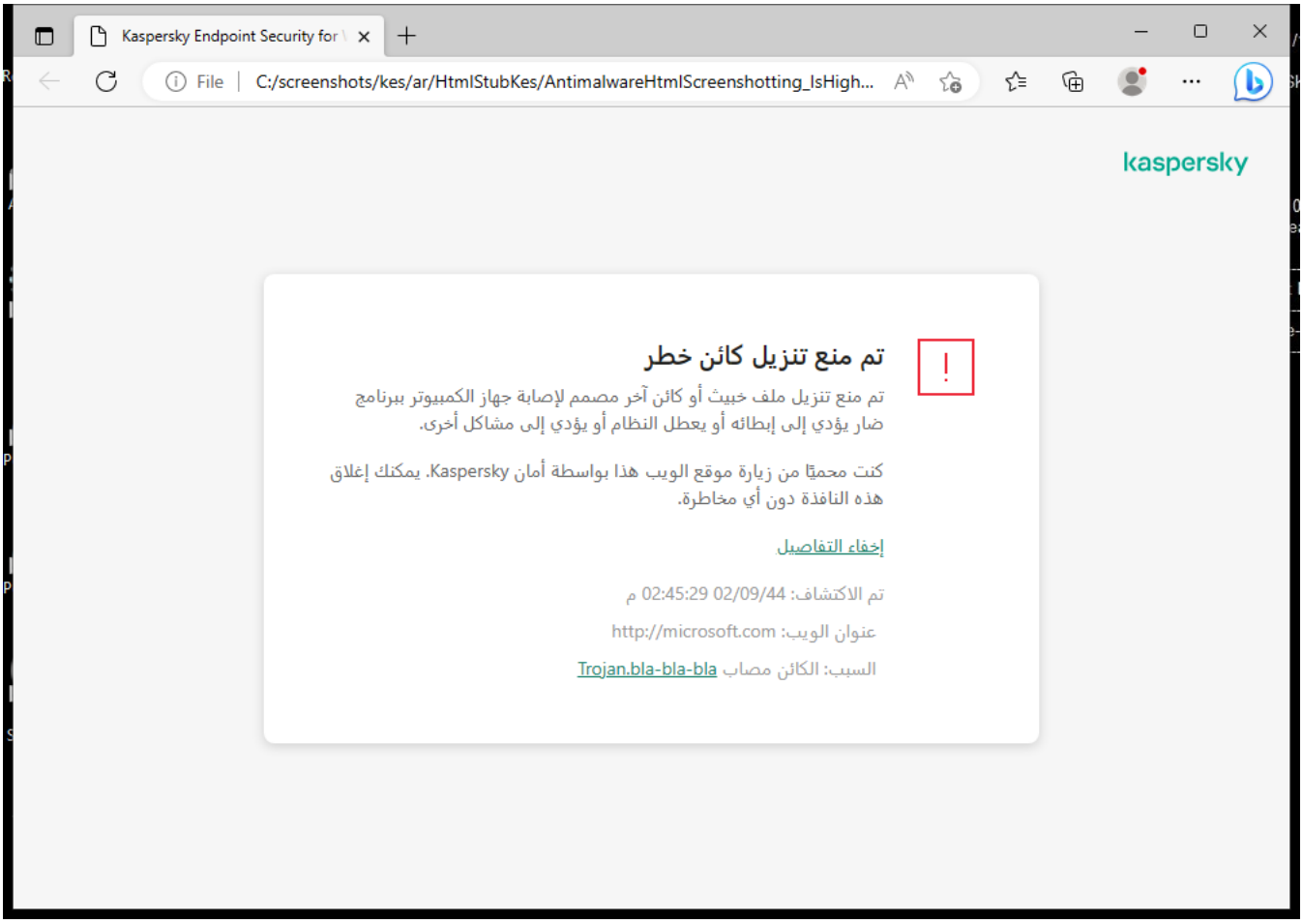
الحماية من تهديدات الويب

يمنع مكون الحماية من تهديدات الويب تنزيلات الملفات الضارة عبر الإنترنت، ويحظر أيضًا مواقع الويب الضارة والاحتيالية. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

يفحص برنامج Kaspersky Endpoint Security حركة مرور HTTP، وHTTPS، وFTP. إن Kaspersky Endpoint Security يفحص عناوين URL وعناوين IP. يمكنك تحديد المنافذ التي يراقبها Kaspersky Endpoint Security، أو تحديد كل المنافذ.

لمراقبة حركة مرور HTTPS، تحتاج إلى تمكين عمليات فحص الاتصالات المشفرة.

عندما يحاول مستخدم فتح موقع إلكتروني ضار أو احتيالي، فإن Kaspersky Endpoint Security سوف يحجب الوصول إلى ذلك الموقع ويعرض تحذيرًا (راجع الشكل أدناه).



رسالة رفض الوصول الخاص بموقع الويب

تمكين وتعطيل الحماية من تهديدات الويب

بشكل افتراضي، يتم تكوين مكون الحماية من تهديدات الويب وتشغيله في الوضع الموصى به من خبراء Kaspersky. للحماية من تهديدات الويب، فإن التطبيق باستطاعته تطبيق مجموعات مختلفة من الإعدادات. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان: **مرتفع**، **مستحسن**، **منخفض**. وتُعد إعدادات مستوى أمان حركة الويب **مستحسن** الإعدادات المُثلى التي يوصي بها خبراء Kaspersky (انظر الجدول أدناه). يمكنك تحديد أحد مستويات الأمان المثبتة مسبقًا لحركة المرور على الويب التي تم استلامها أو إرسالها عبر بروتوكولي HTTP وFTP، أو تكوين مستوى أمان حركة ويب مخصص. إذا غيرت إعدادات مستوى أمان حركة المرور على الويب، فيمكنك دائمًا العودة إلى إعدادات مستوى أمان حركة المرور على الويب الموصى بها.

يمكنك تحديد أو تكوين مستوى الأمان فقط في وحدة تحكم الإدارة (MMC) أو الواجهة المحلية للتطبيق. ولا يمكنك تحديد أو تكوين مستوى الأمان في Web Console أو Cloud Console.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات الويب في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

5. استخدم خانة الاختيار **الحماية من تهديدات الويب** لتمكين المكون أو تعطيله.

6. في حالة قيامك بتمكين المكون، نفذ أحد الإجراءات التالية في القسم **مستوى الأمان**:

- إذا كنت تريد استخدام أحد مستويات الأمان المعدة مسبقًا، فقم بتحديده باستخدام شريط التمرير:

- **مرتفع**. مستوى الأمان الذي ينفذ مكون الحماية من تهديدات الويب من خلاله الحد الأقصى من الفحص لحركة المرور على الويب التي يتلقاها الكمبيوتر عبر بروتوكولات HTTP وFTP. ينفذ مكون الحماية من تهديدات الويب فحصًا مفصلاً لجميع كائنات حركة المرور على الويب باستخدام المجموعة الكاملة من قواعد بيانات التطبيق وينفذ أعمق تحليل مساعد على الاكتشاف ممكن.

- **مستحسن**. مستوى الأمان الذي يوفر التوازن المثالي بين أداء Kaspersky Endpoint Security وأمان حركة المرور على الويب. وينفذ مكون الحماية من تهديدات الويب التحليل المساعد على الاكتشاف وفقًا لمستوى فحص متوسط. ويوصي الخبراء في Kaspersky بهذا المستوى من أمان حركة المرور على الويب. يتم توفير قيم الإعدادات لمستوى الأمان المستحسن في الجدول أدناه.

- **منخفض**. تضمن إعدادات هذا المستوى من أمان حركة الويب أقصى سرعة فحص لحركة الويب. وينفذ مكون الحماية من تهديدات الويب التحليل المساعد على الاكتشاف وفقًا لمستوى فحص خفيف.

- إذا كنت ترغب في تكوين مستوى أمان مخصص، فانقر فوق الزر **الإعدادات** وحدد إعدادات المكون الخاص بك.

  يمكنك استعادة قيم مستويات الأمان المعينة مسبقًا بالنقر فوق الزر **افتراضيًا**.

7. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد الإجراء الذي سينفذه برنامج Kaspersky Endpoint Security على كائنات حركة المرور على الويب الضارة:

- **منع**. إذا تم تحديد هذا الاختيار واكتشاف كائن مصاب في حركة المرور على الويب، يمنع مكون الحماية من تهديدات الويب الوصول إلى الكائن ويعرض رسالةً في المستعرض.

- **إعلام**. إذا تم تحديد هذا الخيار وتم اكتشاف كائن مصاب في حركة المرور على الويب، فإن Kaspersky Endpoint Security يسمح بتنزيل هذا الكائن إلى الكمبيوتر ولكنه يضيف معلومات حول الكائن المصاب إلى قائمة التهديدات النشطة.

8. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات الويب في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Essential Threat Protection** ← **Web Threat Protection**.

5. استخدم مفتاح تبديل **Web Threat Protection** لتمكين المكون أو تعطيله.

6. في القسم **Action on threat detection**، حدد الإجراء الذي سينفذه برنامج Kaspersky Endpoint Security على كائنات حركة المرور على الويب الضارة:

- **Block**. إذا تم تحديد هذا الاختيار واكتشاف كائن مصاب في حركة المرور على الويب، يمنع مكون الحماية من تهديدات الويب الوصول إلى الكائن ويعرض رسالةً في المستعرض.
- **Inform**. إذا تم تحديد هذا الخيار وتم اكتشاف كائن مصاب في حركة المرور على الويب، فإن Kaspersky Endpoint Security يسمح بتنزيل هذا الكائن إلى الكمبيوتر ولكنه يضيف معلومات حول الكائن المصاب إلى قائمة التهديدات النشطة.

7. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات الويب

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الويب**.

3. استخدم مفتاح تبديل **الحماية من تهديدات الويب** لتمكين المكون أو تعطيله.

4. في حالة قيامك بتمكين المكون، نفذ أحد الإجراءات التالية في القسم **مستوى الأمان**:

- إذا كنت تريد استخدام أحد مستويات الأمان المعدة مسبقًا، فقم بتحديده باستخدام شريط التمرير:

- **مرتفع**. مستوى الأمان الذي ينفذ مكون الحماية من تهديدات الويب من خلاله الحد الأقصى من الفحص لحركة المرور على الويب التي يتلقاها الكمبيوتر عبر بروتوكولات HTTP وFTP. ينفذ مكون الحماية من تهديدات الويب فحصًا مفصلاً لجميع كائنات حركة المرور على الويب باستخدام المجموعة الكاملة من قواعد بيانات التطبيق وينفذ أعمق تحليل مساعد على الاكتشاف ممكن.

- **مستحسن**. مستوى الأمان الذي يوفر التوازن المثالي بين أداء Kaspersky Endpoint Security وأمان حركة المرور على الويب. وينفذ مكون الحماية من تهديدات الويب التحليل المساعد على الاكتشاف وفقًا لمستوى فحص متوسط. ويوصي الخبراء في Kaspersky بهذا المستوى من أمان حركة المرور على الويب. يتم توفير قيم الإعدادات لمستوى الأمان المستحسن في الجدول أدناه.

- **منخفض**. تضمن إعدادات هذا المستوى من أمان حركة الويب أقصى سرعة فحص لحركة الويب. وينفذ مكون الحماية من تهديدات الويب التحليل المساعد على الاكتشاف وفقًا لمستوى فحص خفيف.

- إذا كنت ترغب في تكوين مستوى أمان مخصص، فانقر فوق الزر **إعدادات متقدمة** وحدد إعدادات المكون الخاص بك.

يمكنك استعادة قيم مستويات الأمان المعينة مسبقًا بالنقر فوق الزر **استعادة مستوى الأمان الموصى به**.

5. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد الإجراء الذي سينفذه برنامج Kaspersky Endpoint Security على كائنات حركة المرور على الويب الضارة:

- **منع**. إذا تم تحديد هذ الاختيار واكتشاف كائن مصاب في حركة المرور على الويب، يمنع مكون الحماية من تهديدات الويب الوصول إلى الكائن ويعرض رسالةً في المستعرض.

- **إعلام**. إذا تم تحديد هذا الخيار وتم اكتشاف كائن مصاب في حركة المرور على الويب، فإن Kaspersky Endpoint Security يسمح بتنزيل هذا الكائن إلى الكمبيوتر ولكنه يضيف معلومات حول الكائن المصاب إلى قائمة التهديدات النشطة.

6. احفظ تغييراتك.

إعدادات الحماية من تهديدات الويب التي يوصي بها خبراء Kaspersky (مستوى الأمان المستحسن)

المعلمة	القيمة	الوصف
التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الخبيثة	**تشغيل**	يسمح لك فحص الروابط لتحديد ما إذا كانت مدرجة في قاعدة بيانات عناوين الويب الضارة بتتبع مواقع الويب التي تم إضافتها إلى قائمة الرفض. يتم الاحتفاظ بقاعدة بيانات عناوين الويب الضارة بواسطة Kaspersky وتضمينها في حزمة تثبيت التطبيق وإكمال تحديثات قاعدة بيانات Kaspersky Endpoint Security.
التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الاحتيالية	**تشغيل**	تتضمن قاعدة بيانات مواقع الويب الاحتيالية عناوين الويب الخاصة بمواقع الويب المعروف حاليًا أنها تُستخدم في بدء الهجمات الاحتيالية. وتستكمل Kaspersky قاعدة بيانات الروابط الاحتيالية هذه بالعناوين التي يتم الحصول عليها من المنظمة الدولية المعروفة باسم "مجموعة عمل مكافحة الاحتيال". يتم تضمين قاعدة بيانات العناوين الاحتيالية في حزمة تثبيت التطبيق وإكمال تحديثات قاعدة بيانات Kaspersky Endpoint Security.
استخدام التحليل المساعد على الاكتشاف (الحماية من	**فحص متوسط**	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف.

تهديدات الويب)		عند فحص حركة الويب للبحث عن الفيروسات والتطبيقات الأخرى التي تشكل تهديدًا، ينفذ المحلل المساعد على الاكتشاف التعليمات المدرجة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
استخدام التحليل المساعد على الاكتشاف (مكافحة الاحتيال)	**تشغيل**	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**منع**	إذا تم تحديد هذ الاختيار واكتشاف كائن مصاب في حركة المرور على الويب، يمنع مكون الحماية من تهديدات الويب الوصول إلى الكائن ويعرض رسالةً في المستعرض.

تكوين طرق اكتشاف عناوين الويب الخبيثة

تكتشف الحماية من تهديدات الويب عناوين الويب الخبيثة باستخدام قواعد بيانات مكافحة الفيروسات، والخدمة السحابية لشبكة Kaspersky Security Network، والتحليل المساعد على الاكتشاف.

يمكنك تحديد طرق اكتشاف عناوين الويب الخبيثة فقط في وحدة تحكم الإدارة (MMC) أو الواجهة المحلية للتطبيق. لا يمكنك تحديد طرق اكتشاف عناوين الويب الخبيثة في Web Console أو Cloud Console. ويكون الخيار الافتراضي التحقق من عناوين الويب بمقارنتها بقاعدة البيانات الخاصة بالعناوين الخبيثة من خلال التحليل المساعد على الاكتشاف (فحص متوسط).

الفحص باستخدام قاعدة بيانات العناوين الخبيثة

يسمح لك فحص الروابط لتحديد ما إذا كانت مدرجة في قاعدة بيانات عناوين الويب الضارة بتتبع مواقع الويب التي تم إضافتها إلى قائمة الرفض. يتم الاحتفاظ بقاعدة بيانات عناوين الويب الضارة بواسطة Kaspersky وتضمينها في حزمة تثبيت التطبيق وإكمال تحديثات قاعدة بيانات Kaspersky Endpoint Security.

يفحص Kaspersky Endpoint كل الروابط لتحديد ما إذا كانت مدرجة في قواعد بيانات عناوين الويب الضارة. لا تؤثر إعدادات فحص الاتصال الآمن الخاصة بالتطبيق على وظيفة فحص الرابط. بمعنى آخر، في حالة تعطيل عمليات فحص الاتصالات المشفرة، يتحقق Kaspersky Endpoint Security من الروابط مقابل قواعد بيانات عناوين الويب الخبيثة حتى إذا تم نقل حركة مرور شبكة الاتصال عبر اتصال مشفر.

كيفية تمكين أو تعطيل التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الخبيثة باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، في القسم **طرق الفحص**، حدد أو امسح خانة الاختيار **التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الخبيثة** لتمكين أو تعطيل التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الخبيثة.

7. احفظ تغييراتك.

كيفية تمكين أو تعطيل التحقق من العناوين مقابل قاعدة بيانات العناوين الخبيثة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

3. انقر على **إعدادات متقدمة**.

4. في القسم **طرق الفحص**، حدد أو امسح خانة الاختيار **التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الخبيثة** لتمكين أو تعطيل التحقق من العناوين مقابل قاعدة بيانات عناوين الويب الخبيثة.

5. احفظ تغييراتك.

التحليل المساعد على الاكتشاف

أثناء استخدام التحليل المساعد على الاكتشاف، يحلل برنامج Kaspersky Endpoint Security نشاط التطبيقات في نظام التشغيل. يستطيع التحليل المساعد على الاكتشاف أن يكتشف التهديدات ولذلك لا توجد حاليًا أية سجلات في قواعد بيانات برنامج Kaspersky Endpoint Security.

عند فحص حركة الويب للبحث عن الفيروسات والتطبيقات الأخرى التي تشكل تهديدًا، ينفذ المحلل المساعد على الاكتشاف التعليمات المدرجة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.

كيفية تمكين أو تعطيل استخدام التحليل المساعد على الاكتشاف في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

6. في القسم **طرق الفحص**، حدد خانة الاختيار **استخدام التحليل المساعد على الاكتشاف** إذا كنت تريد أن يستخدم التطبيق التحليل المساعد على الاكتشاف عند فحص حركة الويب للبحث عن الفيروسات والبرامج الضارة الأخرى.

7. استخدم شريط التمرير لضبط مستوى التحليل المساعد على الاكتشاف: **فحص خفيف** أو **فحص متوسط** أو **فحص عميق**.

   عند فحص حركة الويب للبحث عن الفيروسات والتطبيقات الأخرى التي تشكل تهديدًا، ينفذ المحلل المساعد على الاكتشاف التعليمات المدرجة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.

8. احفظ تغييراتك.

كيفية تمكين أو تعطيل استخدام التحليل المساعد على الاكتشاف في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

3. انقر على **إعدادات متقدمة**.

4. في القسم **طرق الفحص**، حدد خانة الاختيار **استخدام التحليل المساعد على الاكتشاف** إذا كنت تريد أن يستخدم التطبيق التحليل المساعد على الاكتشاف عند فحص حركة الويب للبحث عن الفيروسات والبرامج الضارة الأخرى.

   عند فحص حركة الويب للبحث عن الفيروسات والتطبيقات الأخرى التي تشكل تهديدًا، ينفذ المحلل المساعد على الاكتشاف التعليمات المدرجة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.

5. احفظ تغييراتك.

مكافحة الاحتيال

تتحقق الحماية من تهديدات الويب من الروابط لمعرفة ما إذا كانت تنتمي إلى عناوين ويب خاصة بالاحتيال. ويساعد هذا على منع هجمات الاحتيال. ويمكن إخفاء الهجوم الاحتيالي، على سبيل المثال، في شكل رسالة بريد إلكتروني من المفترض أن تكون من البنك الخاص بك مع ارتباط لموقعه الرسمي على الويب. وبالنقر على الارتباط، فإنك تنتقل إلى نسخة مماثلة تمامًا لموقع البنك وبإمكانك حتى رؤية عنوان الويب الحقيقي في المتصفح، على الرغم من أنك في موقع مزور. ومن هذا المنطلق يتم تعقب جميع أنشطتك على الموقع ويمكن استخدامها لسرقة أموالك.

نظرًا لأن ارتباطات مواقع الويب الاحتيالية قد يتم استلامها ليس فقط في رسالة بريد إلكتروني ولكن أيضًا من مصادر أخرى مثل برامج المراسلة، فإن مكون الحماية من تهديدات الويب يراقب محاولات الوصول إلى موقع ويب احتيالي على مستوى فحص حركة المرور على الويب ويمنع الوصول إلى مواقع الويب هذه. يتم إدراج قوائم عناوين مواقع الويب الاحتيالية مع مجموعة توزيع برنامج Kaspersky Endpoint Security.

يمكنك تكوين مكافحة الاحتيال فقط في وحدة تحكم الإدارة (MMC) أو الواجهة المحلية للتطبيق. ولا يمكنك تكوين مكافحة الاحتيال في Web Console أو Cloud Console. وافتراضيًا، يتم تمكين مكافحة الاحتيال باستخدام التحليل المساعد على الاكتشاف.

كيفية تمكين أو تعطيل مكافحة الاحتيال في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.
5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.
6. في النافذة التي تفتح، في القسم **إعدادات مكافحة الاحتيال**، حدد أو امسح خانة الاختيار **التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الاحتيالية** لتمكين أو تعطيل مكافحة الاحتيال.

   تتضمن قاعدة بيانات مواقع الويب الاحتيالية عناوين الويب الخاصة بمواقع الويب المعروف حاليًا أنها تُستخدم في بدء الهجمات الاحتيالية. وتستكمل Kaspersky قاعدة بيانات الروابط الاحتيالية هذه بالعناوين التي يتم الحصول عليها من المنظمة الدولية المعروفة باسم "مجموعة عمل مكافحة الاحتيال". يتم تضمين قاعدة بيانات العناوين الاحتيالية في حزمة تثبيت التطبيق وإكمال تحديثات قاعدة بيانات Kaspersky Endpoint Security.
7. حدد خانة الاختيار **استخدام التحليل المساعد على الاكتشاف** إذا كنت تريد أن يستخدم التطبيق التحليل المساعد على الاكتشاف عند فحص حركة صفحة الويب للبحث عن الروابط الاحتيالية.

   أثناء استخدام التحليل المساعد على الاكتشاف، يحلل برنامج Kaspersky Endpoint Security نشاط التطبيقات في نظام التشغيل. يستطيع التحليل المساعد على الاكتشاف أن يكتشف التهديدات ولذلك لا توجد حاليًا أية سجلات في قواعد بيانات برنامج Kaspersky Endpoint Security.

   لفحص الروابط، بالإضافة إلى قاعدة بيانات مكافحة الفيروسات والتحليل المساعد على الاكتشاف، يمكنك استخدام قواعد بيانات السمعة من Kaspersky Security Network.
8. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكافحة الاحتيال في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الويب**.

3. انقر على **إعدادات متقدمة**.

4. إذا كنت تريد أن يفحص مكون الحماية من تهديدات الويب الروابط مقابل قواعد بيانات عناوين الويب الاحتيالية، فحدد خانة الاختيار **التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الاحتيالية** في القسم **مكافحة الاحتيال**. تتضمن قاعدة بيانات مواقع الويب الاحتيالية عناوين الويب الخاصة بمواقع الويب المعروف حاليًا أنها تُستخدم في بدء الهجمات الاحتيالية. وتستكمل Kaspersky قاعدة بيانات الروابط الاحتيالية هذه بالعناوين التي يتم الحصول عليها من المنظمة الدولية المعروفة باسم "مجموعة عمل مكافحة الاحتيال". يتم تضمين قاعدة بيانات العناوين الاحتيالية في حزمة تثبيت التطبيق وإكمال تحديثات قاعدة بيانات Kaspersky Endpoint Security.

5. حدد خانة الاختيار **استخدام التحليل المساعد على الاكتشاف** إذا كنت تريد أن يستخدم التطبيق التحليل المساعد على الاكتشاف عند فحص حركة صفحة الويب للبحث عن الروابط الاحتيالية.

   أثناء استخدام التحليل المساعد على الاكتشاف، يحلل برنامج Kaspersky Endpoint Security نشاط التطبيقات في نظام التشغيل. يستطيع التحليل المساعد على الاكتشاف أن يكتشف التهديدات ولذلك لا توجد حاليًا أية سجلات في قواعد بيانات برنامج Kaspersky Endpoint Security.

   لفحص الروابط، بالإضافة إلى قاعدة بيانات مكافحة الفيروسات والتحليل المساعد على الاكتشاف، يمكنك استخدام قواعد بيانات السمعة من Kaspersky Security Network.

6. احفظ تغييراتك.

إنشاء قائمة عناوين الويب الموثوقة

بالإضافة إلى مواقع الويب الخبيثة والاحتيالية، من الممكن أن تمنع الحماية من تهديدات الويب مواقع الويب الأخرى. على سبيل المثال، تمنع الحماية من تهديدات الويب حركة مرور HTTP التي لا تلبي معايير RFC. يمكنك إنشاء قائمة بعناوين URL التي تثق في محتواها. لا يحلل مكون الحماية من تهديدات الويب المعلومات من عناوين الويب الموثوقة للتحقق منها للبحث عن الفيروسات أو غيرها من التهديدات. قد يكون هذا الخيار مفيدًا، على سبيل المثال، عندما يقوم مكون الحماية من تهديدات الويب باعتراض تنزيل ملف من موقع ويب معروف.

قد يكون عنوان URL هو عنوان صفحة ويب محددة أو عنوان موقع ويب.

كيفية إضافة عنوان ويب موثوق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، حدد القسم **عناوين الويب الموثوقة**.

7. حدد خانة الاختيار **عدم فحص حركة المرور على الويب من عناوين الويب الموثوقة**.

في حالة تحديد خانة الاختيار هذه، لا يفحص مكون الحماية من تهديدات الويب محتوى صفحات الويب أو مواقع الويب التي تم تضمين عناوينها في قائمة عناوين الويب الموثوقة. يمكنك إضافة كلاً من العنوان المحدد وقناع عنوان صفحة الويب / موقع الويب إلى قائمة عناوين الويب الموثوقة.

8. إنشاء قائمة بعناوين المواقع الموثوقة/صفحات الويب التي تثق في محتوياتها.

يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع.

يمكنك أيضًا استيراد قائمة بعناوين الويب الموثوقة من ملف XML.

9. احفظ تغييراتك.

كيفية إضافة عنوان ويب موثوق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Essential Threat Protection** ← **Web Threat Protection**.

5. في القسم **Trusted web addresses**، حدد خانة الاختيار **Do not scan web traffic from trusted web addresses**.

في حالة تحديد خانة الاختيار هذه، لا يفحص مكون الحماية من تهديدات الويب محتوى صفحات الويب أو مواقع الويب التي تم تضمين عناوينها في قائمة عناوين الويب الموثوقة. يمكنك إضافة كلاً من العنوان المحدد وقناع عنوان صفحة الويب / موقع الويب إلى قائمة عناوين الويب الموثوقة.

6. إنشاء قائمة بعناوين المواقع الموثوقة/صفحات الويب التي تثق في محتوياتها.

يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع.

يمكنك أيضًا استيراد قائمة بعناوين الويب الموثوقة من ملف XML.

7. احفظ تغييراتك.

كيفية إضافة عنوان ويب موثوق في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الويب**.

3. انقر على **إعدادات متقدمة**.

4. حدد خانة الاختيار **عدم فحص حركة الويب من عناوين المواقع الموثوقة**.

   في حالة تحديد خانة الاختيار هذه، لا يفحص مكون الحماية من تهديدات الويب محتوى صفحات الويب أو مواقع الويب التي تم تضمين عناوينها في قائمة عناوين الويب الموثوقة. يمكنك إضافة كلاً من العنوان المحدد وقناع عنوان صفحة الويب / موقع الويب إلى قائمة عناوين الويب الموثوقة.

5. إنشاء قائمة بعناوين المواقع الموثوقة/صفحات الويب التي تثق في محتوياتها.

   يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع.

   يمكنك أيضًا استيراد قائمة بعناوين الويب الموثوقة من ملف XML.

6. احفظ تغييراتك.

نتيجة لذلك، لا تفحص الحماية من تهديدات الويب حركة مرور عناوين الويب الموثوقة. ويستطيع المستخدم دائمًا فتح موقع ويب موثوق وتنزيل ملف من هذا موقع الويب هذا. وإذا لم تتمكن من الوصول إلى موقع الويب، فتحقق من إعدادات مكونات فحص الاتصالات المشفرة والتحكم في الويب ومراقبة منافذ شبكة الاتصال. وإذا اكتشف Kaspersky Endpoint Security أن ملفًا تم تنزيله من موقع ويب موثوق به خبيث، فيمكنك إضافة هذا الملف إلى الاستثناءات.

يمكنك أيضا إنشاء قائمة عامة باستثناءات الاتصالات المشفرة. وفي هذه الحالة، لا يفحص Kaspersky Endpoint Security حركة مرور HTTPS لعناوين الويب الموثوقة عندما يؤدي مكونات الحماية من تهديدات الويب والحماية من تهديدات البريد والتحكم في الويب عملها.

تصدير واستيراد قائمة عناوين الويب الموثوقة

يمكنك تصدير قائمة عناوين الويب الموثوقة إلى ملف XML. ثم يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من عناوين الويب من النوع نفسه. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة عناوين الويب الموثوقة أو لترحيل القائمة إلى خادم مختلف.

كيفية تصدير واستيراد قائمة بعناوين الويب الموثوقة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، حدد القسم **عناوين الويب الموثوقة**.

7. لتصدير قائمة عناوين الويب الموثوقة:

   a. حدد عناوين الويب الموثوقة التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.
   إذا لم تحدد أي عنوان ويب موثوق، فسيقوم Kaspersky Endpoint Security بتصدير كل عناوين الويب.

   b. انقر على رابط **تصدير**.

   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة عناوين الويب الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   d. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير قائمة عناوين الويب الموثوقة بالكامل إلى ملف XML.

8. لاستيراد قائمة العناوين الموثوقة:

   a. انقر على رابط **استيراد**.
   في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة العناوين الموثوقة منه.

   b. افتح الملف.
   إذا كان جهاز الكمبيوتر يحتوي على قائمة عناوين موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

9. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة عناوين الويب الموثوقة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Essential Threat Protection** ← **Web Threat Protection**.

5. لتصدير قائمة الاستثناءات في القسم **Trusted web addresses**:

a. حدد عناوين الويب الموثوقة التي تريد تصديرها.

b. انقر على رابط **Export**.

c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة عناوين الويب الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة عناوين الويب الموثوقة بالكامل إلى ملف XML.

6. لاستيراد قائمة الاستثناءات في القسم **Trusted web addresses**:

a. انقر على رابط **Import**.
في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة العناوين الموثوقة منه.

b. افتح الملف.
إذا كان جهاز الكمبيوتر يحتوي على قائمة عناوين موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

الحماية من تهديدات البريد

يفحص مكون الحماية من تهديدات البريد مرفقات رسائل البريد الإلكتروني الصادرة والواردة للحماية من الفيروسات والتهديدات الأخرى. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

تستطيع الحماية من تهديدات البريد فحص كل من الرسائل الواردة والصادرة. ويدعم التطبيق بروتوكولات POP3 وSMTP وIMAP وNNTP في عملاء البريد التاليين:

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail

لا تدعم الحماية من تهديدات البريد البروتوكولات وعملاء البريد الآخرين.

قد لا تتمكن الحماية من تهديدات البريد دائمًا من الحصول على الوصول إلى الرسائل على مستوى البروتوكول (على سبيل المثال، عند استخدام حل Microsoft Exchange). ولهذا السبب، تتضمن الحماية من تهديدات البريد ملحقًا لبرنامج Microsoft Office Outlook. ويسمح الملحق بفحص الرسائل على مستوى عميل البريد. يدعم ملحق الحماية من تهديدات البريد العمليات باستخدام Outlook 2010 و2013 و2016 و2019.

لا يقوم مكون الحماية من تهديدات البريد بفحص الرسائل إذا كان عميل البريد مفتوحًا في مستعرض.

عند اكتشاف ملف ضار في مرفق، يضيف Kaspersky Endpoint Security معلومات عن الإجراء المتخذ إلى موضوع الرسالة، على سبيل المثال: [تمت معالجة الرسالة] <موضوع الرسالة>.

تمكين وتعطيل الحماية من تهديدات البريد

بشكل افتراضي، يتم تكوين مكون الحماية من تهديدات البريد وتشغيله في الوضع الموصى به من خبراء Kaspersky. وللحماية من تهديدات البريد، يطبق Kaspersky Endpoint Security مجموعات مختلفة من الإعدادات. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان: **مرتفع**، **مستحسن**، **منخفض**. وتُعد إعدادات مستوى أمان البريد **مستحسن** الإعدادات المُثلى التي يوصي بها خبراء Kaspersky (انظر الجدول أدناه). يمكنك تحديد أحد مستويات أمان البريد الإلكتروني المثبتة مسبقًا أو تكوين مستوى مخصص لأمان البريد الإلكتروني. في حالة تغيير إعدادات مستوى أمان البريد الإلكتروني، يمكنك دائمًا العودة إلى إعدادات مستوى أمان البريد الإلكتروني المستحسَنة.

لتمكين أو تعطيل مكون الحماية من تهديدات البريد:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.
3. استخدم مفتاح تبديل **الحماية من تهديدات البريد** لتمكين المكون أو تعطيله.
4. في حالة قيامك بتمكين المكون، نفذ أحد الإجراءات التالية في القسم **مستوى الأمان**:

- إذا كنت تريد استخدام أحد مستويات الأمان المعدة مسبقًا، فقم بتحديده باستخدام شريط التمرير:

- **مرتفع**. عند تحديد مستوى أمان البريد الإلكتروني هذا، يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني بشكل أكثر شمولاً. يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني الواردة والصادرة ويقوم بإجراء تحليل مساعد على الاكتشاف عميق. ويُوصى بمستوى أمان البريد "مرتفع" للبيئات عالية المخاطر. ومن الأمثلة على هذه البيئات، الاتصال بخدمة بريد إلكتروني مجانية من شبكة اتصال منزلية ليست محمية بواسطة حماية البريد الإلكتروني المركزية.

- **مستحسن**. مستوى أمان البريد الإلكتروني الذي يوفر التوازن الأمثل بين أداء Kaspersky Endpoint Security وأمان البريد الإلكتروني. يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني الواردة والصادرة ويقوم بإجراء تحليل مساعد على الاكتشاف متوسط المستوى. يوصى بمستوى أمان حركة البريد هذا بواسطة مختصي Kaspersky. يتم توفير قيم الإعدادات لمستوى الأمان المستحسن في الجدول أدناه.

- **منخفض**. عندما يتم تحديد مستوى أمان البريد الإلكتروني هذا، يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني الواردة فقط، وينفذ تحليلاً مساعدًا على الاكتشاف خفيفًا، ولا يفحص الأرشيفات الملحقة برسائل البريد الإلكتروني. في مستوى أمان البريد هذا، يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني بأقصى سرعة ويستخدم الحد الأدنى من موارد نظام التشغيل. ويُوصى باستخدام مستوى أمان البريد "منخفض" في بيئة محمية جيدًا. وقد يكون أحد الأمثلة على هذه البيئة شبكة المنطقة المحلية (LAN) للمؤسسة مع أمان مركزي للبريد الإلكتروني.

- إذا كنت ترغب في تكوين مستوى أمان مخصص، فانقر فوق الزر **إعدادات متقدمة** وحدد إعدادات المكون الخاص بك.

يمكنك استعادة قيم مستويات الأمان المعينة مسبقًا بالنقر فوق الزر **استعادة مستوى الأمان الموصى به**.

5. احفظ تغييراتك.

إعدادات الحماية من تهديدات البريد التي أوصى بها خبراء Kaspersky (مستوى الأمان المستحسن)

المعلمة	القيمة	الوصف
نطاق الحماية	**الرسائل الواردة والصادرة**	يتضمن نطاق الحماية الكائنات التي يتحقق منها المكون عند تشغيله: الرسائل الواردة والصادرة أو الرسائل الواردة فقط. لحماية أجهزة الكمبيوتر الخاصة بك، ما عليك سوى فحص الرسائل الواردة. ويمكنك تشغيل الفحص للبحث عن الرسائل الصادرة لمنع إرسال الملفات المصابة في الأرشيفات. ويمكنك أيضًا تشغيل فحص الرسائل الصادرة إذا كنت تريد منع إرسال ملفات ذات تنسيقات محددة، مثل ملفات الصوت والفيديو، على سبيل المثال.

توصيل ملحق Microsoft Outlook	**تشغيل**	إذا تم تحديد خانة الخيار يتم تمكين فحص رسائل البريد الإلكتروني التي يتم بثها عبر البروتوكولات POP3 وSMTP وNNTP وIMAP على جانب الملحق المدمج في Microsoft Outlook. في حالة فحص البريد باستخدام ملحق برنامج Microsoft Outlook، فمن المستحسن استخدام وضع Exchange المُخَزَّن مؤقتًا. للمزيد من المعلومات التفصيلية حول وضع التبادل المخزن مؤقتًا والتوصيات حول استخدامه، يُرجى الرجوع إلى قاعدة معارف Microsoft.
فحص الأرشيفات المرفقة	**تشغيل**	فحص تنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE وتنسيقات الأرشيفات الأخرى. يفحص التطبيق الأرشيفات ليس فقط حسب الملحق، لكن أيضًا حسب التنسيق. عند التحقق من الأرشيفات، ينفذ التطبيق عملية تفريغ متكررة. ويسمح هذا باكتشاف التهديدات داخل أرشيفات متعددة المستويات (أرشيف داخل أرشيف).
فحص الملفات المرفقة بتنسيقات Microsoft Office	**تشغيل**	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
عامل تصفية المرفقات	**إعادة تسمية المرفقات من الأنواع المحددة**	في حالة تحديد هذا الخيار، يستبدل مكون الحماية من تهديدات البريد آخر حرف في الملفات المرفقة من الأنواع المحددة برمز تسطير أسفل السطر (على سبيل المثال، _). وبالتالي، لفتح الملف، يجب على المستخدم إعادة تسميته.
التحليل المساعد على الاكتشاف	**فحص متوسط**	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف. عند فحص الملفات للبحث عن تعليمات برمجية ضارة، ينفذ المحلل المساعد على الاكتشاف الإرشادات الواردة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**تنظيف؛ حذف إذا فشل التنظيف**	عند اكتشاف كائن مصاب في رسالة واردة أو صادرة، يحاول Kaspersky Endpoint Security تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف Kaspersky Endpoint Security الكائن المصاب. ويضيف Kaspersky Endpoint Security معلومات عن الإجراء المتخذ إلى موضوع الرسالة، على سبيل المثال: [تمت معالجة الرسالة] <موضوع الرسالة>.

تغيير الإجراء الذي تود اتخاذه بشأن رسائل البريد الإلكتروني المصابة

بشكل افتراضي، يحاول مكون الحماية من تهديدات البريد تلقائيًا تنظيف كل الرسائل المصابة المكتشفة. وإذا فشل التنظيف، يحذف مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني المصابة.

لتغيير الإجراء المتخذ للتعامل مع رسائل البريد الإلكتروني المصابة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.
3. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد الإجراء الذي سينفذه برنامج Kaspersky Endpoint Security عند اكتشاف رسالة مصابة:

- **تنظيف؛ حذف إذا فشل التنظيف**. عند اكتشاف كائن مصاب في رسالة واردة أو صادرة، يحاول Kaspersky Endpoint Security تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف Kaspersky Endpoint Security الكائن المصاب. ويضيف Kaspersky Endpoint Security معلومات عن الإجراء المتخذ إلى موضوع الرسالة، على سبيل المثال: [تمت معالجة الرسالة] <موضوع الرسالة>.

- **تنظيف؛ منع إذا فشل التنظيف**. عند اكتشاف كائن مصاب في رسالة واردة، يحاول Kaspersky Endpoint Security تنظيف الكائن المحدد. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يضيف Kaspersky Endpoint Security تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. عندما يتم اكتشاف كائن مصاب في رسالة صادرة، يحاول Kaspersky Endpoint Security تنظيف الكائن الذي تم اكتشافه. إذا تعذّر تنظيف الكائن، يقوم Kaspersky Endpoint Security بحظر إرسال الرسالة ويظهر عميل البريد خطأ.

- **منع**. في حالة اكتشاف كائن مصاب في رسالة واردة، يضيف Kaspersky Endpoint Security تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. إذا تم اكتشاف كائن مصاب في رسالة صادرة، يقوم Kaspersky Endpoint Security بحظر إرسال الرسالة، ويظهر عميل البريد خطأ.

4. احفظ تغييراتك.

تشكيل نطاق الحماية لمكون الحماية من تهديدات البريد

يشير نطاق الحماية إلى الكائنات التي يتم فحصها بواسطة المكون عندما يكون فعالاً. تتمتع نطاقات الحماية للمكونات المختلفة بخصائص مختلفة. تشتمل خصائص نطاق الحماية الخاص بمكون الحماية من تهديدات البريد على إعدادات لدمج الحماية من تهديدات البريد في عملاء البريد وأنواع رسائل البريد الإلكتروني وبروتوكولات البريد الإلكتروني التي يتم فحص حركتها بواسطة مكون الحماية من تهديدات البريد. وافتراضيًا، يفحص Kaspersky Endpoint Security رسائل البريد الإلكتروني الواردة والصادرة وحركة البروتوكولات POP3 وSMTP وNNTP وIMAP، وهو مُدمج في عميل البريد Microsoft Office Outlook.

لتشكيل نطاق الحماية لمكون الحماية من تهديدات البريد:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات البريد**.

3. انقر على **إعدادات متقدمة**.

4. في القسم **نطاق الحماية**، حدد الرسائل التي تريد فحصها:

- **الرسائل الواردة والصادرة**.

- **الرسائل الواردة فقط**.

لحماية أجهزة الكمبيوتر الخاصة بك، ما عليك سوى فحص الرسائل الواردة. ويمكنك تشغيل الفحص للبحث عن الرسائل الصادرة لمنع إرسال الملفات المصابة في الأرشيفات. ويمكنك أيضًا تشغيل فحص الرسائل الصادرة إذا كنت تريد منع إرسال ملفات ذات تنسيقات محددة، مثل ملفات الصوت والفيديو، على سبيل المثال.

إذا اخترت فحص الرسائل الواردة فقط، فيوصى بإجراء فحص لمرة واحدة لكل الرسائل الصادرة، نظرًا لأن هناك احتمال وجود فيروسات متنقلة خاصة بالبريد الإلكتروني على الكمبيوتر الخاص بك التي تنتشر عبر البريد الإلكتروني. يساعدك هذا على تجنب المشكلات التي تنتج عن الإرسال غير المراقب لأعداد كبيرة من رسائل البريد الإلكتروني المصابة من الكمبيوتر الخاص بك.

5. في القسم **الاتصال** قم بإجراء التالي:

- إذا كنت تريد أن يفحص مكون الحماية من تهديدات البريد الرسائل المنقولة عبر بروتوكولات POP3 وSMTP وNNTP وIMAP قبل وصولها إلى الكمبيوتر الخاص بالمستخدم، فحدد خانة الاختيار **فحص حركة POP3 وSMTP وNNTP وIMAP**.

  إذا كنت لا تريد أن يفحص مكون الحماية من تهديدات البريد الرسائل المنقولة عبر بروتوكولات POP3 وSMTP وNNTP وIMAP قبل وصولها إلى الكمبيوتر الخاص بالمستخدم، فامسح خانة الاختيار **فحص حركة POP3 وSMTP وNNTP وIMAP**. في هذه الحالة، يتم فحص الرسائل بواسطة ملحق الحماية من تهديدات البريد المضمن في عميل بريد Microsoft Office Outlook بعد استلامها على كمبيوتر المستخدم في حالة تحديد خانة الاختيار **توصيل ملحق Microsoft Outlook**.

إذا كنت تستخدم عميل بريد بخلاف Microsoft Office Outlook، فلا يفحص مكون الحماية من تهديدات البريد الرسائل التي يتم إرسالها عبر بروتوكولات POP3 وSMTP وNNTP وIMAP عند مسح خانة الاختيار **فحص حركة POP3 وSMTP وNNTP وIMAP**.

- إذا كنت تريد توفير إمكانية الوصول إلى إعدادات مكون الحماية من تهديدات البريد من Microsoft Office Outlook وتمكين فحص الرسائل التي تم نقلها عبر بروتوكولات POP3 وSMTP وNNTP وIMAP وMAPI بعد وصولها إلى الكمبيوتر الذي يستخدم الملحق المدمج في Microsoft Office Outlook، فقم بتحديد خانة الاختيار **توصيل ملحق Microsoft Outlook**.

  إذا كنت تريد منع الوصول إلى إعدادات مكون الحماية من تهديدات البريد من Microsoft Office Outlook وتعطيل فحص الرسائل التي تم نقلها عبر بروتوكولات POP3 وSMTP وNNTP وIMAP وMAPI بعد وصولها على الكمبيوتر الذي يستخدم الملحق المدمج في Microsoft Office Outlook، فقم بإلغاء تحديد خانة الاختيار **توصيل ملحق Microsoft Outlook**.

يتم دمج ملحق الحماية من تهديدات البريد في عميل البريد Microsoft Office Outlook خلال تثبيت Kaspersky Endpoint Security.

6. احفظ تغييراتك.

فحص الملفات المركبة المرفقة برسائل البريد الإلكتروني

يمكنك تمكين أو تعطيل فحص مرفقات الرسائل، وتقييد الحد الأقصى لحجم مرفقات الرسائل التي يتم فحصها، وتقييد الحد الأقصى لمدة فحص مرفقات الرسالة.

لتكوين فحص الملفات المركبة المرفقة برسائل البريد الإلكتروني:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.
3. انقر على **إعدادات متقدمة**.
4. في القسم **فحص الملفات المركبة**، كوّن إعدادات الفحص:

- **فحص الملفات المرفقة بتنسيقات Microsoft Office**. يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
- **فحص الأرشيفات المرفقة**. فحص تنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE وتنسيقات الأرشيفات الأخرى. يفحص التطبيق الأرشيفات ليس فقط حسب الملحق، لكن أيضًا حسب التنسيق. عند التحقق من الأرشيفات، ينفذ التطبيق عملية تفريغ متكررة. ويسمح هذا باكتشاف التهديدات داخل أرشيفات متعددة المستويات (أرشيف داخل أرشيف).

إذا اكتشف Kaspersky Endpoint Security أثناء الفحص كلمة مرور لأرشيف في نص الرسالة، فسيتم استخدام كلمة المرور هذه لفحص محتوى الأرشيف للبحث عن التطبيقات الضارة. وفي هذه الحالة، لا يتم حفظ كلمة المرور. ويتم فك الأرشيف أثناء الفحص. وفي حالة حدوث خطأ في التطبيق أثناء عملية الفك، يمكنك يدويًا حذف الملفات غير المضغوطة المحفوظة في المسار التالي: %systemroot%\temp. تتضمن الملفات بادئة PR.

- **عدم فحص الأرشيفات الأكبر من N ميجابايت**. في حالة تحديد خانة الاختيار هذه، فإن مكون الحماية من تهديدات البريد يستثني الأرشيفات المرفقة برسائل البريد الإلكتروني من الفحص إذا تجاوز حجمها القيمة المحددة. في حالة إلغاء تحديد خانة الاختيار، يفحص مكون الحماية من تهديدات البريد الأرشيفات المرفقة بالبريد الإلكتروني أيًا كان حجمها.
- **تقييد الوقت للتحقق من الأرشيفات إلى N ثانية**. في حالة تحديد خانة الاختيار، فإن الوقت المخصص لفحص الأرشيفات المرفقة في رسائل البريد الإلكتروني يكون مقصورًا على المدة المحددة.

5. احفظ تغييراتك.

تصفية مرفقات رسائل البريد الإلكتروني

لا يتم تطبيق وظيفة تصفية المرفقات على رسائل البريد الإلكتروني الصادرة.

يمكن توزيع التطبيقات الضارة في شكل مرفقات في رسائل البريد الإلكتروني. يمكنك تكوين التصفية بناءً على نوع مرفقات الرسالة لكي يتم إعادة تسمية الملفات من نوع محدد تلقائيًا أو حذفها. عن طريق إعادة تسمية مرفق من نوع معين، يمكن لـ Kaspersky Endpoint Security حماية جهاز الكمبيوتر الخاص بك ضد التنفيذ التلقائي لتطبيق ضار.

لتكوين تصفية المرفقات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.
3. انقر على **إعدادات متقدمة**.
4. في القسم **عامل تصفية المرفقات**، نفذ أحد الإجراءات التالية:
   - **تعطيل التصفية**. في حالة تحديد هذا الخيار، لا يقوم مكون الحماية من تهديدات البريد بتصفية الملفات المرفقة مع رسائل البريد الإلكتروني.
   - **إعادة تسمية المرفقات من الأنواع المحددة**. في حالة تحديد هذا الخيار، يستبدل مكون الحماية من تهديدات البريد آخر حرف في الملفات المرفقة من الأنواع المحددة برمز تسطير أسفل السطر (على سبيل المثال، _). وبالتالي، لفتح الملف، يجب على المستخدم إعادة تسميته.
   - **حذف المرفقات من الأنواع المحددة**. في حالة تحديد هذا الخيار، يقوم مكون الحماية من تهديدات البريد بحذف الملفات المرفقة من الأنواع المحددة من رسائل البريد الإلكتروني.
5. إذا قمت بتحديد الخيار **إعادة تسمية المرفقات من الأنواع المحددة** أو الخيار **حذف المرفقات من الأنواع المحددة** خلال الخطوة السابقة، فحدد خانات الاختيار المقابلة لأنواع الملفات ذات الصلة.
6. احفظ تغييراتك.

تصدير واستيراد ملحقات لتصفية المرفقات

يمكنك تصدير قائمة ملحقات عامل تصفية المرفقات إلى ملف XML. يمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة الملحقات أو لترحيل القائمة إلى خادم مختلف.

كيفية تصدير واستيراد قائمة ملحقات عامل تصفية المرفقات في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.

5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، حدد علامة التبويب **عامل تصفية المرفقات**.

7. لتصدير قائمة الملحقات:

   a. حدد الملحقات التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

   b. انقر فوق الرابط **تصدير**.

   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الملحقات إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   d. احفظ الملف.

   يقوم Kaspersky Endpoint Security بتصدير قائمة الملحقات بالكامل إلى ملف XML.

8. لاستيراد قائمة الملحقات:

   a. انقر على رابط **Import**.

   b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الملحقات منه.

   c. افتح الملف.

   إذا كان جهاز الكمبيوتر يحتوي على بالفعل على قائمة ملحقات، فإن Kaspersky Endpoint Security سوف يطلب منك حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

9. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة بملحقات عوامل تصفية المرفقات في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.

5. لتصدير قائمة الملحقات في القسم **Attachment filter**:

a. حدد الملحقات التي تريد تصديرها.

b. انقر على رابط **Export**.

c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الملحقات إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة الملحقات بالكامل إلى ملف XML.

6. لاستيراد قائمة الملحقات في القسم **Attachment filter**:

a. انقر على رابط **Import**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الملحقات منه.

c. افتح الملف.
إذا كان جهاز الكمبيوتر يحتوي على بالفعل على قائمة ملحقات، فإن Kaspersky Endpoint Security سوف يطلب منك حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

فحص رسائل البريد الإلكتروني في Microsoft Office Outlook

أثناء تثبيت Kaspersky Endpoint Security، يتم دمج ملحق الحماية من تهديدات البريد في Microsoft Office Outlook (المشار إليه هنا فيما بعد باسم Outlook). ويتيح لك فتح إعدادات الحماية من تهديدات البريد من داخل Outlook، وتحديد الوقت الذي يتم فيه فحص رسائل البريد الإلكتروني للبحث عن الفيروسات والتهديدات الأخرى. ويستطيع ملحق الحماية من تهديدات البريد لبرنامج Outlook فحص الرسائل الواردة والصادرة التي يتم نقلها عبر بروتوكولات POP3 وSMTP وNNTP وIMAP وMAPI. Kaspersky Endpoint Security يدعم كذلك العمل مع عملاء البريد الإلكتروني الآخرين (بما في ذلك Microsoft Outlook Express® وWindows Mail وMozilla™ Thunderbird™).

يدعم ملحق الحماية من تهديدات البريد العمليات باستخدام Outlook 2010 و2013 و2016 و2019.

عند استخدام عميل بريد Mozilla Thunderbird، لا يفحص مكون الحماية من تهديدات البريد الرسائل المرسَلة عبر بروتوكول IMAP للبحث عن الفيروسات والتهديدات الأخرى، في حالة استخدام عوامل التصفية لنقل الرسائل من مجلد صندوق الوارد.

في برنامج Outlook، يتم أولاً فحص رسائل البريد الإلكتروني الواردة بواسطة GIFT (في حالة تحديد خانة الاختيار فحص حركة POP3 و SMTP و NNTP و IMAP في واجهة Kaspersky Endpoint Security)، ثم بواسطة ملحق الحماية من تهديدات البريد لبرنامج Outlook. في حالة اكتشاف مكون الحماية من تهديدات البريد كائنًا ضارًا في رسالة، فإنه يخطرك بهذا الحدث.

يمكن تكوين إعدادات مكون الحماية من تهديدات البريد مباشرة في Outlook في حالة تحديد خانة الاختيار ملحق Microsoft Outlook متصل في واجهة Kaspersky Endpoint Security (انظر الشكل أدناه).

إعدادات مكون الحماية من تهديدات البريد في Outlook

ويتم فحص رسائل البريد الإلكتروني الصادرة أولاً بواسطة ملحق الحماية من تهديدات البريد لبرنامج Outlook، ثم بواسطة مكون الحماية من تهديدات البريد.

في حالة فحص البريد باستخدام ملحق الحماية من تهديدات البريد لبرنامج Outlook، فمن المستحسن استخدام وضع Exchange المُخَزَّن مؤقتًا. للمزيد من المعلومات التفصيلية حول وضع التبادل المخزن مؤقتًا والتوصيات حول استخدامه، يُرجى الرجوع إلى قاعدة معارف Microsoft.

لتكوين وضع التشغيل لملحق الحماية من تهديدات البريد لبرنامج Outlook:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.
5. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.
6. في القسم **الاتصال**، انقر على الزر **الإعدادات**.
7. في النافذة **حماية البريد الإلكتروني**، نفذ ما يلي:
   - حدد خانة الاختيار **الفحص عند الاستلام** إذا كنت تريد أن يقوم ملحق الحماية من تهديدات البريد لبرنامج Outlook بفحص الرسائل الواردة بمجرد وصولها إلى علبة الوارد.
   - حدد خانة الاختيار **الفحص عند القراءة** إذا كنت تريد أن يقوم ملحق الحماية من تهديدات البريد لبرنامج Outlook بفحص الرسائل الواردة عندما يفتحها المستخدم.
   - حدد خانة الاختيار **الفحص عند الإرسال** إذا كنت تريد أن يقوم ملحق الحماية من تهديدات البريد لبرنامج Outlook بفحص الرسائل الصادرة بمجرد إرسالها.
8. احفظ تغييراتك.

الحماية من تهديدات الشبكة

يفحص مكون الحماية من تهديدات الشبكة حركة نقل البيانات الواردة في الشبكة لاكتشاف أي نشاط يعتبر نموذجًا لهجمات على الشبكة. عندما يكتشف Kaspersky Endpoint Security محاولة هجوم على الشبكة على كمبيوتر المستخدم، فإنه يحظر اتصال الشبكة مع الكمبيوتر المهاجم. تتوفر أوصاف لأنواع هجمات الشبكة المعروفة حاليًا وطرق إبطالها في قواعد بيانات Kaspersky Endpoint Security. يتم تحديث قائمة هجمات الشبكة التي يكتشفها مكون الحماية من تهديدات الشبكة أثناء تحديثات قاعدة البيانات والوحدة النمطية للتطبيق.

تمكين وتعطيل الحماية من تهديدات الشبكة

بشكل افتراضي، يتم تمكين الحماية من تهديدات الشبكة وتشغيلها في الوضع الأمثل. ويمكنك تعطيل الحماية من تهديدات الشبكة إذا لزم الأمر.

لتمكين أو تعطيل الحماية من تهديدات الشبكة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الشبكة**.
3. استخدم مفتاح تبديل **الحماية من تهديدات الشبكة** لتمكين المكون أو تعطيله.
4. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين الحماية من تهديدات الشبكة، يفحص Kaspersky Endpoint Security حركة شبكة الاتصال الواردة للبحث عن النشاط النموذجي لهجمات شبكة الاتصال. عندما يكتشف Kaspersky Endpoint Security محاولة هجوم على الشبكة على كمبيوتر المستخدم، فإنه يحظر اتصال الشبكة مع الكمبيوتر المهاجم.

منع الكمبيوتر المهاجم

لمنع الكمبيوتر المهاجم:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الشبكة**.
3. حدد خانة الاختيار **حظر الأجهزة التي تنفذ الهجوم لمدة N دقيقة**.

في حالة تحديد خانة الاختيار، يضيف مكون الحماية من تهديدات الشبكة الكمبيوتر المهاجم إلى قائمة المنع. وهذا يعني أن مكون الحماية من تهديدات الشبكة يمنع اتصال الشبكة بالكمبيوتر المهاجم بعد أول محاولة لهجوم الشبكة لمدة محددة من الوقت. ويؤدي هذا المنع إلى وجود حماية تلقائية لكمبيوتر المستخدم ضد هجمات الشبكة المستقبلية المحتملة من نفس العنوان. الحد الأدنى للوقت الذي يجب أن يقضيه الكمبيوتر المهاجم في قائمة الحظر هو دقيقة واحدة. ويبلغ الحد الأقصى للوقت 999 دقيقة.

يمكنك عرض قائمة المنع في النافذة أداة مراقبة شبكة الاتصال.

يمسح Kaspersky Endpoint Security قائمة المنع عند إعادة تشغيل التطبيق وعندما تتغير إعدادات الحماية من تهديدات الشبكة.

4. قم بتعيين مدة حظر مختلفة لجهاز كمبيوتر مهاجم في الحقل الموجود على يسار خانة الاختيار **حظر الأجهزة التي تنفذ الهجوم لمدة N دقيقة**.
5. احفظ تغييراتك.

نتيجة لذلك، عندما يكتشف Kaspersky Endpoint Security محاولة هجوم شبكة اتصال تم إطلاقه على كمبيوتر المستخدم، فسوف يمنع كل الاتصالات بالكمبيوتر المهاجم.

تكوين عناوين الاستثناءات من المنع

من الممكن أن يتعرف Kaspersky Endpoint Security على هجوم شبكة اتصال ويمنع اتصال شبكة غير آمن يرسل عددًا كبيرًا من الحزم (على سبيل المثال، من كاميرات المراقبة). للعمل مع الأجهزة الموثوقة، يمكنك إضافة عناوين IP لهذه الأجهزة إلى قائمة الاستثناءات.

لتكوين عناوين الاستثناءات من المنع:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.
3. انقر على رابط **إدارة الاستثناءات**.
4. في النافذة التي تفتح، انقر فوق الزر **إضافة**.
5. أدخل عنوان IP للكمبيوتر الذي يجب عدم منع هجمات الشبكة منه.
6. احفظ تغييراتك.

نتيجة لذلك، لا يتتبع Kaspersky Endpoint Security النشاط من الأجهزة المدرجة في قائمة الاستثناءات.

تصدير واستيراد قائمة الاستثناءات من المنع

يمكنك تصدير قائمة الاستثناءات إلى ملف XML. وبعد ذلك يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من العناوين من النوع نفسه. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة الاستثناءات أو لترحيل القائمة إلى خادم مختلف.

كيفية تصدير واستيراد قائمة الاستثناءات في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.

5. في القسم **إعدادات الحماية من تهديدات الشبكة**، انقر على الزر **الاستثناءات**.

6. لتصدير قائمة القواعد:

   a. حدد الاستثناءات التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.
   إذا لم تحدد أي استثناء، فسيقوم Kaspersky Endpoint Security بتصدير كل الاستثناءات.

   b. انقر على رابط **تصدير**.

   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   d. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

7. لاستيراد قائمة الاستثناءات:

   a. انقر على **استيراد**.

   b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

   c. افتح الملف.
   إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة الاستثناءات في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Essential Threat Protection** ← **Network Threat Protection**.

5. في القسم **Network Threat Protection settings**، انقر على الرابط **Exclusions and types of detected objects**.
تفتح قائمة الاستثناءات.

6. لتصدير قائمة القواعد:

a. حدد الاستثناءات التي تريد تصديرها.

b. انقر على **Export**.

c. أكد أنك تريد تصدير الاستثناءات المحددة فقط، أو تصدير قائمة الاستثناءات بأكملها.

d. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

e. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

7. لاستيراد قائمة الاستثناءات:

a. انقر على **Import**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

c. افتح الملف.
إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. احفظ تغييراتك.

تكوين الحماية ضد هجمات شبكة الاتصال حسب النوع

يتيح لك Kaspersky Endpoint Security إدارة الحماية ضد الأنواع التالية من هجمات شبكة الاتصال:

- إغراق الشبكة هو هجوم على موارد شبكة الاتصال لمؤسسة ما (مثل خوادم الويب). يتكون هذا الهجوم من إرسال عدد كبير من الطلبات لزيادة الحمل على النطاق الترددي لموارد شبكة الاتصال. وعند حدوث ذلك، يتعذر على المستخدمين الوصول إلى موارد شبكة الاتصال الخاصة بالمؤسسة.

- يتكون هجوم فحص المنفذ من فحص منافذ UDP ومنافذ TCP وخدمات الشبكة على الكمبيوتر. ويسمح هذا الهجوم للمهاجم بتحديد درجة الثغرات الأمنية للكمبيوتر قبل تنفيذ أنواع أكثر خطورة من هجمات شبكة الاتصال. ويتيح فحص المنفذ أيضًا للمهاجم التعرف على نظام التشغيل على الكمبيوتر وتحديد هجمات شبكة الاتصال المناسبة لنظام التشغيل هذا.

- يتألف هجوم انتحال عنوان MAC من تغيير عنوان MAC الخاص بجهاز شبكة (بطاقة الشبكة). ونتيجة لذلك، يمكن للمهاجم إعادة توجيه البيانات المرسلة إلى جهاز إلى جهاز آخر والوصول إلى هذه البيانات. يتيح لك Kaspersky Endpoint Security حظر هجمات انتحال عنوان MAC وتلقي إشعارات

حول الهجمات.

يمكنك تعطيل اكتشاف هذه الأنواع من الهجمات في حالة إجراء بعض التطبيقات المسموح بها عمليات نموذجية لهذه الأنواع من الهجمات. وسوف يساعد هذا في تجنب الإنذارات الكاذبة.

بشكل افتراضي ، لا يراقب Kaspersky Endpoint Security هجمات إغراق الشبكة وفحص المنفذ وانتحال عنوان MAC.

لتكوين الحماية ضد هجمات شبكة الاتصال حسب النوع:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← الحماية من تهديدات الشبكة**.
3. استخدم مفتاح التبديل **التعامل مع فحص المنافذ وإغراق الشبكة كهجمات** لتمكين أو تعطيل اكتشاف هذه الهجمات.

في حالة تمكين هذه الوظيفة، يراقب Kaspersky Endpoint Security حركة مرور الشبكة لفحص المنافذ وإغراق الشبكة. وفي حالة اكتشاف هذا السلوك، يخطر التطبيق المستخدم ويرسل الحدث المقابل إلى Kaspersky Security Center. ويوفر التطبيق معلومات عن الكمبيوتر الذي يقدم الطلبات. وهذه المعلومات ضرورية للرد في الوقت المناسب. ومع ذلك، لا يحظر Kaspersky Endpoint Security الكمبيوتر الذي يقدم الطلبات لأن حركة المرور هذه قد تكون حدثًا عاديًا على شبكة الشركة.

4. استخدم مفتاح التبديل **الحماية ضد انتحال عنوان MAC**.
5. في القسم **عند اكتشاف هجوم انتحال عنوان MAC**، حدد أحد الخيارات التالية:
   - **إعلام**.
   - **منع**.
6. احفظ تغييراتك.

جدار الحماية

يقوم جدار الحماية بحظر الاتصالات غير المصرح بها للكمبيوتر أثناء العمل على الإنترنت أو الشبكة المحلية. يتحكم جدار الحماية كذلك في نشاط الشبكة للتطبيقات على الكمبيوتر. يسمح لك هذا بحماية الشبكة المحلية الخاصة بشركتك من سرقة الهوية والهجمات الأخرى. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك قواعد الشبكة المحددة مسبقًا.

يتم استخدام وكيل الشبكة للتفاعل مع Kaspersky Security Center. ينشئ جدار الحماية تلقائيًا قواعد الشبكة المطلوبة لكي يعمل التطبيق ووكيل الشبكة. ونتيجة لذلك، يفتح جدار الحماية عدة منافذ على الكمبيوتر. وتعتمد المنافذ المفتوحة على دور الكمبيوتر (على سبيل المثال، نقطة توزيع). ولمعرفة المزيد حول المنافذ التي سيتم فتحها على الكمبيوتر، يرجى الرجوع إلى تعليمات Kaspersky Security Center .

قواعد الشبكة

يمكنك تكوين قواعد الشبكة على المستويات التالية:

- قواعد حزمة الشبكة. تفرض قواعد حزمة الشبكة قيودًا على حزمة الشبكة، بغض النظر عن التطبيق. وتُقيد هذه القواعد من حركة مرور الشبكة الصادرة والواردة من خلال منافذ معينة لبروتوكول البيانات المحدد. قام Kaspersky Endpoint Security بتعريف قواعد حزم الشبكة مسبقًا مع الأذونات التي أوصى بها خبراء Kaspersky.
- قواعد الشبكة للتطبيق. تفرض قواعد الشبكة للتطبيق قيودًا على نشاط الشبكة الخاص بتطبيق معين. لا يعتبر العامل بمثابة خصائص لحزمة الشبكة فقط، لكنه أيضًا تطبيقًا معينًا يقوم بمخاطبة حزمة الشبكة هذه أو أنه أصدر هذه الحزمة.

يتم توفير الوصول المحكوم للتطبيقات إلى موارد نظام التشغيل والعمليات والبيانات الشخصية من خلال مكون منع اختراق المضيف باستخدام حقوق التطبيق.

أثناء بدء التشغيل الأول للتطبيق، يقوم جدار الحماية بتنفيذ الإجراءات التالية:

1. يتحقق من أمان التطبيق باستخدام قواعد بيانات مكافحة الفيروسات التي تم تنزيلها.

2. سيتحقق من درجة أمان التطبيق في شبكة Kaspersky Security Network.

   ننصحك بالمشاركة في شبكة Kaspersky Security Network لمساعدة جدار الحماية على العمل بفعالية أكثر.

3. يضع التطبيق في إحدى مجموعات الثقة: موثوق، مقيد بشكل منخفض، مقيد بشكل عالٍ، غير موثوق.

   تحدد مجموعة ثقة الحقوق التي يشير إليها Kaspersky Endpoint Security عند التحكم في نشاط التطبيق. يضع Kaspersky Endpoint Security تطبيقًا في مجموعة ثقة بناءً على مستوى الخطر الذي قد يشكله هذا التطبيق على الكمبيوتر.

يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة لمكونات جدار الحماية ومنع اختراق المضيف. لا يمكنك تغيير مجموعة الثقة فقط لجدار الحماية أو منع اختراق المضيف.

إذا رفضت المشاركة في KSN أو لم تكن هناك شبكة، يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة اعتمادًا على إعدادات مكون منع اختراق المضيف. بعد استلام سمعة التطبيق من KSN، يمكن تغيير مجموعة الثقة تلقائيًا.

4. هذا يحظر نشاط الشبكة للتطبيق، اعتمادًا على مجموعة الثقة. على سبيل المثال: لا يُسمح للتطبيقات الموجودة في مجموعة الثقة مقيد بشكل عالٍ باستخدام أي اتصالات شبكة.

في المرة التالية التي يعمل فيها التطبيق، يتحقق Kaspersky Endpoint Security من سلامة التطبيق. في حالة عدم تغير التطبيق، يستخدم المكون قواعد الشبكة الحالية عليه. في حالة تعديل التطبيق، فإن Kaspersky Endpoint Security يحلل التطبيق كما لو كان يجرى تشغيله لأول مرة.

أولويات قاعدة الشبكة

لكل قاعدة أولوية. كلما كانت القاعدة تحتل مرتبة أعلى في القائمة، فإنها تكون ذات أولوية أعلى. إذا تمت إضافة نشاط شبكة إلى عدة قواعد، ينظم جدار الحماية نشاط الشبكة وفقًا للقاعدة ذات أعلى أولوية.

قواعد حزمة الشبكة لها أولوية أعلى من قواعد الشبكة الخاصة بالتطبيقات. إذا تم تحديد كل من قواعد حزمة الشبكة وقواعد الشبكة الخاصة بالتطبيقات لنفس نوع نشاط الشبكة، فسيتم معالجة نشاط هذه الشبكة وفقًا لقواعد حزمة الشبكة.

تعمل قواعد الشبكة للتطبيقات بطريقة معينة. وتتضمن قاعدة الشبكة للتطبيقات قواعد الوصول بناءً على حالة الشبكة: الشبكة العامة والشبكة المحلية والشبكة الموثوقة. على سبيل المثال: التطبيقات في مجموعة الثقة مقيد بشكل عالٍ غير مسموح لها بأي نشاط على الشبكة في الشبكات بجميع الحالات، وذلك في الوضع الافتراضي. إذا كانت قاعدة شبكة محددة لتطبيق معين (تطبيق أصلي) فإن العمليات الفرعية للتطبيقات الأخرى سوف تسير وفق قاعدة الشبكة للتطبيق الأصلي. في حالة عدم وجود قاعدة شبكة للتطبيق، فإن العمليات الفرعية سوف تسري وفق قاعدة وصول الشبكة لمجموعة ثقة التطبيق.

على سبيل المثال: لقد منعت أي نشاط على الشبكة في جميع الشبكات بجميع الحالات لجميع التطبيقات باستثناء المستعرض س. بالتالي إذا بدأت تثبيت المستعرض ص (عملية فرعية) من المستعرض س (التطبيق الأصل)، فإن مثبت المستعرض ص سيتمكن من الوصول للشبكة وتنزيل الملفات الضرورية. بعد التثبيت لن يقدر المستعرض ص على الاتصال بأي شبكة، وذلك وفق إعدادات جدار الحماية. لمنع نشاط الشبكة لمثبت المستعرض ص كعملية فرعية، يجب أن تضيف قاعدة شبكة لمثبت المستعرض ص.

حالات اتصال الشبكة

يسمح لك جدار الحماية بالتحكم في نشاط الشبكة اعتمادًا على حالة اتصال الشبكة. يتلقى Kaspersky Endpoint Security حالة اتصال الشبكة من نظام تشغيل الكمبيوتر. يقوم المستخدم بتعيين حالة اتصال الشبكة في نظام التشغيل عند إعداد الاتصال. يمكنك تغيير حالة اتصال الشبكة في إعدادات Kaspersky Endpoint Security. سيراقب جدار الحماية نشاط الشبكة اعتمادًا على حالة الشبكة في إعدادات Kaspersky Endpoint Security وليس في نظام التشغيل.

يمكن أن يشتمل اتصال الشبكة على أنواع الحالة التالية:

- **الشبكة العامة**. الشبكة غير محمية بتطبيقات مكافحة الفيروسات أو جدران الحماية أو المرشحات (مثل Wi-Fi في مقهى). عندما يقوم المستخدم بتشغيل كمبيوتر متصل بشبكة كهذه، فإن جدار الحماية يحجب الوصول إلى الملفات والطابعات على هذا الكمبيوتر. ويتعذر أيضًا على المستخدمين الخارجين الوصول إلى البيانات من خلال مجلدات المشاركة والوصول عن بُعد إلى سطح مكتب هذا الكمبيوتر. يقوم جدار الحماية بتصفية نشاط الشبكة لكل تطبيق حسب قواعد الشبكة التي تم تعيينها له.

  ويقوم جدار الحماية بتعيين حالة الشبكة العامة إلى الإنترنت بشكل افتراضي. لا يمكنك تغيير حالة الإنترنت.

- **الشبكة المحلية**. شبكة للمستخدمين الذين لديهم وصول مقيد إلى الملفات والطابعات على هذا الكمبيوتر (مثل الشبكة المحلية للشركات أو الشبكة المنزلية).

- **الشبكة الموثوقة**. شبكة آمنة لا يتعرض فيها الكمبيوتر للهجمات أو محاولات الوصول للبيانات غير المسموح بها. ويسمح جدار الحماية بأي نشاط للشبكة ضمن الشبكات التي تتمتع بهذه الحالة.

تمكين أو تعطيل جدار الحماية

افتراضيًا يتم تمكين جدار الحماية والوظائف في الوضع الأمثل.

لتمكين أو تعطيل جدار الحماية:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.
3. استخدم مفتاح تبديل **جدار الحماية** لتمكين المكون أو تعطيله.
4. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين جدار الحماية، فإن Kaspersky Endpoint Security يتحكم في نشاط الشبكة ويمنع اتصالات الشبكة غير المصرح بها بجهاز الكمبيوتر الخاص بك، بالإضافة إلى حظر نشاط الشبكة غير المصرح به للتطبيقات على جهاز الكمبيوتر الخاص بك. ويتم التحكم أيضًا في نشاط الشبكة بواسطة مكون الحماية من تهديدات الشبكة. يفحص مكون الحماية من تهديدات الشبكة حركة نقل البيانات الواردة في الشبكة لاكتشاف أي نشاط يعتبر نموذجًا لهجمات على الشبكة.

يسجل Kaspersky Endpoint Security أحداث هجوم الشبكة في تقاريره بصرف النظر عن إعدادات جدار الحماية. وحتى إذا كان جدار الحماية يحظر اتصال الشبكة باستخدام القواعد وبالتالي يمنع هجوم الشبكة، فإن مكون الحماية من تهديدات الشبكة يسجل أحداث هجوم الشبكة. وهو مطلوب لتوليد معلومات إحصائية حول هجمات الشبكة على أجهزة الكمبيوتر في مؤسستك.

تغيير حالة اتصال الشبكة

ويقوم جدار الحماية بتعيين حالة الشبكة العامة إلى الإنترنت بشكل افتراضي. لا يمكنك تغيير حالة الإنترنت.

لتغيير حالة اتصال الشبكة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **الشبكات المتاحة**.

4. حدد اتصال الشبكة الذي ترغب في تغيير حالته.

5. في العمود **نوع شبكة الاتصال**، حدد حالة اتصال الشبكة:

- **الشبكة العامة**. الشبكة غير محمية بتطبيقات مكافحة الفيروسات أو جدران الحماية أو المرشحات (مثل Wi-Fi في مقهى). عندما يقوم المستخدم بتشغيل كمبيوتر متصل بشبكة كهذه، فإن جدار الحماية يحجب الوصول إلى الملفات والطابعات على هذا الكمبيوتر. ويتعذر أيضًا على المستخدمين الخارجين الوصول إلى البيانات من خلال مجلدات المشاركة والوصول عن بُعد إلى سطح مكتب هذا الكمبيوتر. يقوم جدار الحماية بتصفية نشاط الشبكة لكل تطبيق حسب قواعد الشبكة التي تم تعيينها له.
- **الشبكة المحلية**. شبكة للمستخدمين الذين لديهم وصول مقيد إلى الملفات والطابعات على هذا الكمبيوتر (مثل الشبكة المحلية للشركات أو الشبكة المنزلية).
- **الشبكة الموثوقة**. شبكة آمنة لا يتعرض فيها الكمبيوتر للهجمات أو محاولات الوصول للبيانات غير المسموح بها. ويسمح جدار الحماية بأي نشاط للشبكة ضمن الشبكات التي تتمتع بهذه الحالة.

6. احفظ تغييراتك.

إدارة قواعد حزم الشبكة

يمكنك تنفيذ الإجراءات التالية عند إدارة قواعد حزمة الشبكة:

- إنشاء قاعدة حزمة شبكة جديدة.

  يمكنك إنشاء قاعدة حزمة شبكة جديدة عن طريق إنشاء مجموعة من الحالات والإجراءات المطبقة على تدفقات البيانات وحزمة الشبكة.

- تمكين أو تعطيل قاعدة حزمة شبكة.

  لكل قواعد حزم الشبكة التي تم إنشاؤها افتراضيًا بواسطة جدار الحماية حالة تم التمكين. عندما يتم تمكين قاعدة حزمة الشبكة، يُفعل جدار الحماية هذا الدور.

  يمكنك تعطيل أي قاعدة حزمة الشبكة تم تحديدها في قائمة قواعد حزم الشبكة. عندما يتم تعطيل قاعدة حزمة الشبكة، لا يطبق جدار الحماية هذا الدور بشكل مؤقت.

تتم إضافة قاعدة حزمة الشبكة مخصصة وجديدة إلى قائمة قواعد حزم الشبكة افتراضيًا بالحالة تم التمكين.

- تحرير إعدادات قاعدة حزمة الشبكة موجودة.

  بعد إنشاء قاعدة حزمة الشبكة جديدة، يمكنك دائمًا الرجوع لتحرير هذه الإعدادات وتعديلها حسب الحاجة.

- تغيير إجراء جدار الحماية لقاعدة حزمة الشبكة.

  من قائمة قواعد حزم الشبكة، يمكنك تعديل الإجراء الذي يتخذه جدار الحماية في اكتشاف نشاط شبكة تطابق قاعدة حزمة الشبكة محددة.

- تغيير أولوية قاعدة حزمة الشبكة.

  يمكنك رفع أو خفض الأولوية لقاعدة حزمة الشبكة تم تحديدها في القائمة.

- إزالة قائمة حزمة الشبكة.

  يمكنك إزالة قاعدة حزمة الشبكة لإيقاف جدار الحماية عن تطبيق هذا الدور في اكتشاف نشاط شبكة ولإيقاف هذا الدور من العرض في قائمة قواعد حزم الشبكة بالحالة تم التعطيل.

إنشاء قاعدة حزمة الشبكة

يمكنك إنشاء قاعدة حزمة شبكة بالطرق التالية:

- استخدام أداة مراقبة شبكة الاتصال.

مراقبة شبكة الاتصال عبارة عن أداة تستخدم لعرض معلومات حول نشاط الشبكة الخاصة بكمبيوتر المستخدم في الوقت الحقيقي. وهذا مناسب لأنك لست بحاجة إلى تكوين جميع إعدادات القاعدة. وسيتم إدراج بعض إعدادات جدار الحماية تلقائيًا من بيانات مراقبة شبكة الاتصال. وتتوفر مراقبة شبكة الاتصال فقط في واجهة التطبيق.

- تكوين إعدادات جدار الحماية.

يتيح لك هذا ضبط إعدادات جدار الحماية. ويمكنك إنشاء قواعد لأي نشاط للشبكة، حتى إذا لم يكن هناك نشاط للشبكة في الوقت الحالي.

عند إنشاء قواعد حزم الشبكة، تذكر أن لها الأولوية عن قواعد تطبيقات الشبكة.

كيفية استخدام أداة مراقبة شبكة الاتصال لإنشاء قاعدة حزمة شبكة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **مراقبة شبكة الاتصال**.
2. حدد علامة التبويب **نشاط الشبكة**.

تعرض علامة التبويب **نشاط الشبكة** كل اتصالات الشبكة الحالية النشطة بالكمبيوتر. ويتم عرض كل من اتصالي الشبكة الواردة والصادرة.

3. في قائمة سياق اتصال الشبكة، حدد **تكوين قاعدة حزمة الشبكة**.

يفتح هذا خصائص قاعدة الشبكة.

4. قم بتعيين الحالة على **فعال** لقاعدة الحزمة.
5. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.
6. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).

يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **قالب قاعدة الشبكة**. تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.

سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

7. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.
8. انقر على **حفظ**.

ستتم إضافة قاعدة الشبكة الجديدة إلى القائمة.

9. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.
10. احفظ تغييراتك.

كيفية استخدام إعدادات جدار الحماية لإنشاء قاعدة حزمة شبكة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **قواعد الحزمة**.

يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

4. انقر على **إضافة**.

يفتح هذا خصائص قاعدة الشبكة.

5. قم بتعيين الحالة على **فعال** لقاعدة الحزمة.

6. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.

7. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).

يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **قالب قاعدة الشبكة**. تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.

سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

8. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.

9. انقر على **حفظ**.

ستتم إضافة قاعدة الشبكة الجديدة إلى القائمة.

10. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

11. احفظ تغييراتك.

كيفية إنشاء قاعدة حزمة شبكة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

5. في القسم **إعدادات جدار الحماية**، انقر على الزر **الإعدادات**.
يفتح هذا قائمة قواعد حزم الشبكة وقائمة قواعد الشبكة للتطبيق.

6. حدد علامة التبويب **قواعد حزمة الشبكة**.
يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

7. انقر على **إضافة**.
يفتح هذا خصائص قاعدة الحزمة.

8. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.

9. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).
يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الزر . تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.
سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

10. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.

11. حفظ قاعدة الشبكة الجديدة

12. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

13. احفظ تغييراتك.

سيتحكم جدار الحماية في حزم الشبكة وفقًا للقاعدة. ويمكنك تعطيل قاعدة حزمة من عملية جدار الحماية دون حذفها من القائمة. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

كيفية إنشاء قاعدة حزمة شبكة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. حدد **Firewall** ← **Essential Threat Protection**.

5. في القسم **Firewall Settings**، انقر على الرابط **Network packet rules**.
يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

6. انقر على **Add**.
يفتح هذا خصائص قاعدة الحزمة.

7. أدخل اسم خدمة الشبكة يدويًا في الحقل **Name**.

8. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).
يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **Select template**. تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.
سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

9. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **Log events**.

10. احفظ قاعدة الشبكة.
ستتم إضافة قاعدة الشبكة الجديدة إلى القائمة.

11. استخدم الزرين **Up** / **Down** لتعيين أولوية قاعدة الشبكة.

12. احفظ تغييراتك.

سيتحكم جدار الحماية في حزم الشبكة وفقًا للقاعدة. ويمكنك تعطيل قاعدة حزمة من عملية جدار الحماية دون حذفها من القائمة. استخدم زر التبديل في العمود **Status** لتمكين قاعدة الحزمة أو تعطيلها.

إعدادات قاعدة حزم الشبكة

المعلمة	الوصف
الإجراء	**سماح**. **منع**. **حسب قواعد التطبيق**. في حالة تحديد هذا الخيار، يطبق جدار الحماية قواعد شبكة الاتصال للتطبيق على اتصال الشبكة.
البروتوكول	مراقبة نشاط الشبكة عبر البروتوكول المحدد: TCP وUDP وICMP وICMPv6 وIGMP وGRE. في حالة تحديد ICMP أو ICMPv6 كبروتوكول، يمكنك تحديد نوع حزمة ICMP ورمزها. في حالة تحديد TCP أو UDP كنوع البروتوكول، يمكنك تحديد أرقام المنافذ المحددة بفاصلة لأجهزة الكمبيوتر المحلية والبعيدة التي سيتم مراقبة الاتصال بينها.
الاتجاه	**الوارد (حزمة)**. يطبق جدار الحماية قاعدة الشبكة على جميع حزم الشبكة الواردة. **الوارد**. يطبق جدار الحماية قاعدة الشبكة على كل حزمة شبكة الاتصال المرسلة عبر اتصال بدأه كمبيوتر بعيد. **الوارد / الصادر**. يطبق جدار الحماية قاعدة الشبكة على كل من حزم الشبكة الواردة والصادرة، بغض النظر عما إذا كان كمبيوتر المستخدم أو كمبيوتر بعيد قد بدأ اتصال الشبكة. **الصادر (حزمة)**. يطبق جدار الحماية قاعدة الشبكة على كل حزم الشبكة الصادرة. **الصادر**. يطبق جدار الحماية قاعدة الشبكة على حزمة شبكة الاتصال المرسلة عبر اتصال بدأه كمبيوتر المستخدم.

محوّلات الشبكة	محولات الشبكة التي يمكنها إرسال و/أو استقبال حزم الشبكة. تحديد إعدادات محولات الشبكة يجعل من الممكن التفريق بين حزم الشبكة التي يتم إرسالها من محولات الشبكة أو التي يمكن استلامها من محولات الشبكة ذات عناوين IP متطابقة.
مدة البقاء (TTL)	تقييد التحكم في حزم شبكة الاتصال بناءً على مدة بقائها (TTL).
العنوان البعيد	عناوين الشبكة لأجهزة الكمبيوتر البعيدة التي يمكنها إرسال و استقبال حزم شبكة الاتصال. يطبق جدار الحماية قاعدة الشبكة على النطاق المحدد لعناوين الشبكة البعيدة. ويمكنك تضمين كل عناوين IP في قاعدة شبكة، أو إنشاء قائمة منفصلة بعناوين IP، أو تحديد نطاق من عناوين IP، أو تحديد شبكة فرعية (الشبكات الموثوقة وشبكات الاتصال المحلية وشبكات الاتصال العامة). ويمكنك أيضًا تحديد اسم DNS لجهاز كمبيوتر بدلاً من عنوان IP الخاص به. ويجب عليك استخدام أسماء DNS فقط لأجهزة كمبيوتر الشبكة المحلية (LAN) أو الخدمات الداخلية. ويجب التعامل مع التفاعل مع الخدمات السحابية (مثل Microsoft Azure) وموارد الإنترنت الأخرى بواسطة مكون التحكم في الويب. يدعم Kaspersky Endpoint Security أسماء DNS بدءًا من الإصدار 11.7.0. إذا حددت اسم DNS للإصدار 11.6.0 أو أقدم، فقد يطبق Kaspersky Endpoint Security القاعدة ذات الصلة على جميع العناوين.
العنوان المحلي	عناوين الشبكة لأجهزة الكمبيوتر التي يمكنها إرسال واستقبال حزم شبكة الاتصال. يطبق جدار الحماية قاعدة شبكة على النطاق المحدد لعناوين الشبكة المحلية. ويمكنك تضمين كل عناوين IP في قاعدة شبكة أو إنشاء قائمة منفصلة بعناوين IP، أو تحديد نطاق من عناوين IP. يدعم Kaspersky Endpoint Security أسماء DNS بدءًا من الإصدار 11.7.0. إذا حددت اسم DNS للإصدار 11.6.0 أو أقدم، فقد يطبق Kaspersky Endpoint Security القاعدة ذات الصلة على جميع العناوين. أحيانًا لا يمكن الحصول على العنوان المحلي للتطبيقات. وإذا كانت هذه هي الحالة، فسيتم تجاهل هذه المعلمة.

تمكين أو تعطيل قاعدة حزمة الشبكة

لتمكين أو تعطيل قاعدة حزمة شبكة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.
3. انقر على **قواعد الحزمة**.
   يؤدي ذلك إلى فتح قائمة بقواعد حزم الشبكة الافتراضية التي تم تعيينها بواسطة جدار الحماية.
4. حدد قاعدة حزمة الشبكة اللازمة في القائمة.
5. استخدم زر التبديل في عمود **الحالة** لتمكين القاعدة أو تعطيلها.
6. احفظ تغييراتك.

تغيير إجراء جدار الحماية لقاعدة حزمة الشبكة

لتغيير إجراء جدار الحماية الذي تم تطبيقه على قاعدة حزمة الشبكة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **قواعد الحزمة**.
يؤدي ذلك إلى فتح قائمة بقواعد حزم الشبكة الافتراضية التي تم تعيينها بواسطة جدار الحماية.

4. حددها في قائمة قواعد حزمة الشبكة وانقر فوق الزر **تحرير**.

5. في القائمة المنسدلة **الإجراء**، حدد الإجراء الذي يقوم جدار الحماية بتنفيذه لحماية هذا النوع من نشاط الشبكة:

- **سماح**.
- **منع**.
- **حسب قواعد التطبيق**. في حالة تحديد هذا الخيار، يطبق جدار الحماية قواعد شبكة الاتصال للتطبيق على اتصال الشبكة.

6. احفظ تغييراتك.

تغيير أولوية قاعدة حزمة الشبكة

يتم تحديد أولوية قاعدة حزمة الشبكة وفقًا لموقعها في قائمة قواعد حزم الشبكة. تتمتع قاعدة حزمة الشبكة الأعلى في قائمة قواعد حزم الشبكة بأعلى أولوية.

تتم إضافة كل قاعدة حزمة الشبكة يدويًا إلى نهاية قائمة قواعد حزم الشبكة ومن ثّم يكون لها الأولوية الأدنى.

يُنفذ جدار الحماية القواعد بالترتيب التي تظهر عليه في قائمة قواعد حزم الشبكة، وذلك بالترتيب من أعلى إلى أسفل. وفقًا لكل قاعدة حزمة شبكة اتصال تمت معالجتها والتي تنطبق على اتصال شبكة معينة، إما أن يتيح جدار الحماية أو يمنع وصول الشبكة إلى العنوان والمنفذ اللذين تم تحديدهما في إعدادات اتصال هذه الشبكة.

لتغيير أولوية قاعدة حزمة الشبكة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **قواعد الحزمة**.
يؤدي ذلك إلى فتح قائمة بقواعد حزم الشبكة الافتراضية التي تم تعيينها بواسطة جدار الحماية.

4. في القائمة، حدد قاعدة حزمة الشبكة التي ترغب في تغيير أولويتها.

5. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

6. احفظ تغييراتك.

تصدير واستيراد قواعد حزمة الشبكة

يمكنك تصدير قائمة قواعد حزمة الشبكة إلى ملف XML. ثم يمكنك تعديل الملف، على سبيل المثال، إضافة عدد كبير من القواعد من النوع نفسه. يمكنك استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة قواعد حزمة الشبكة أو لترحيل القائمة إلى خادم مختلف.

كيفية تصدير واستيراد قائمة قواعد حزمة الشبكة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

5. في القسم **إعدادات جدار الحماية**، انقر على الزر **الإعدادات**.
يفتح هذا قائمة قواعد حزم الشبكة وقائمة قواعد الشبكة للتطبيق.

6. حدد علامة التبويب **قواعد حزمة الشبكة**.

7. لتصدير قائمة قواعد حزمة الشبكة:

a. حدد القواعد التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.
إذا لم تحدد أي قاعدة، فسيقوم Kaspersky Endpoint Security بتصدير كل القواعد.

b. انقر على رابط **تصدير**.

c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة القواعد إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد بالكامل إلى ملف XML.

8. لاستيراد قائمة بقواعد حزمة الشبكة:

a. انقر على رابط **استيراد**.
في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

b. افتح الملف.
إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

9. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد حزمة الشبكة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. حدد **Firewall ← Essential Threat Protection**.

5. في القسم **Firewall Settings**، انقر على الرابط **Network packet rules**.

6. لتصدير قائمة قواعد حزمة الشبكة:

a. حدد القواعد التي تريد تصديرها.

b. انقر على **Export**.

c. أكد أنك تريد تصدير القواعد المحددة فقط، أو تصدير القائمة بأكملها.

d. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف XML في مجلد التنزيلات الافتراضي.

7. لاستيراد قائمة بقواعد حزمة الشبكة:

a. انقر على رابط **Import**.
في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

b. افتح الملف.
إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. احفظ تغييراتك.

تحديد قواعد حزم الشبكة في XML

يسمح جدار الحماية بتصدير قواعد حزم الشبكة بتنسيق XML. ثم يمكنك تعديل الملف، على سبيل المثال، إضافة عدد كبير من القواعد من النوع نفسه.

يحتوي ملف XML على قسمين رئيسيين: `Rules` و`Resources`. ويسرد قسم `Rules` قواعد حزمة الشبكة. وتحتوي هذه العقدة على قواعد تم تكوينها افتراضيًا (قواعد محددة مسبقًا) بالإضافة إلى القواعد التي أضافها المستخدم (قواعد مخصصة).

علامات قاعدة حزمة الشبكة

```
<"key name="0000>
<tDWORD name="RuleId">100</tDWORD>
<tDWORD name="RuleState">1</tDWORD>
<tDWORD name="RuleTypeId">4</tDWORD>
<tQWORD name="AppIdEx">0</tQWORD>
<tDWORD name="ResIdEx">812</tDWORD>
<tDWORD name="ResIdEx2">0</tDWORD>
```

```
<tDWORD name="AccessFlag">2</tDWORD>
<key/>
```

إعدادات قاعدة حزمة الشبكة بتنسيق XML

المعلمة	الوصف	القيمة
`key> name="0000">`	أولوية القاعدة. كلما قلت القيمة، زادت الأولوية.	عدد صحيح يجب أن تتكون قيمة الأولوية من 4 أرقام. ويجب ترتيب العقد في ملف XML حسب قيمة الأولوية، بدءًا من `0000`.
`RuleId`	معرف القاعدة.	**القواعد المحددة مسبقًا** `100` – **طلبات لخادم DNS عبر TCP**. `101` – **طلبات لخادم DNS عبر UDP**. `102` – **إرسال رسائل بريد إلكتروني**. `110` – **أي نشاط للشبكة** (شبكات موثوقة). `125` – **أي نشاط للشبكة** (شبكات محلية). `130` – **نشاط شبكة سطح المكتب البعيد**. `131` – **اتصالات TCP عبر المنافذ المحلية**. `132` – **اتصالات UDP عبر المنافذ المحلية**. `133` – **تدفق TCP الوارد**. `134` – **تدفق UDP الوارد**. `137` – **الاستجابات الواردة لوجهات ICMP التي يتعذر الوصول إليها**. `138` – **الحزم الواردة لرد طلب ارتداد ICMP**. `140` – **الاستجابات الواردة لتجاوز وقت ICMP**. `142` – **تدفق ICMP الوارد**. `266` – **الحزم الواردة لطلب ارتداد ICMPv6**.
`RuleState`	حالة القاعدة.	`0` – تم تعطيل القاعدة المحددة مسبقًا `1` – تم تمكين القاعدة المحددة مسبقًا `2` – تم تعطيل القاعدة المخصصة `3` – تم تمكين القاعدة المخصصة
`RuleTypeId`	نوع معرّف القاعدة.	`4` – قاعدة حزمة الشبكة.
`AppIdEx`	معرّف التطبيق الذي تنتمي إليه قاعدة حزمة الشبكة.	إذا كانت القاعدة لا تنتمي إلى أي تطبيق، فإن القيمة تكون `0`.
`ResIdEx`	المعرف الرئيسي للمورد الذي يتضمن إعدادات القاعدة. يمكنك استخدام هذا المعرف لتحديد موقع قسم يتضمن إعدادات القاعدة في العقدة `Resources`.	عدد صحيح

ResIdEx2	نوع معرّف الشبكة.	0 – **أي عنوان**. 50 – **شبكات موثوقة**. 51 – **شبكات محلية**. 52 – **الشبكات العامة**. <معرف الشبكة> - **عناوين من القائمة** (يتم تحديد العناوين يدويًا).
AccessFlag	قيمة معلمة **الإجراء**.	0 – **سماح**. 2 – **حسب قواعد التطبيق**. 3 – **منع**. 4 – **سماح** و**أحداث السجل**. 6 – **حسب قواعد التطبيق** و**أحداث السجل**. 7 – **منع** و**أحداث السجل**.
<key/>		

تحتوي عقدة `Resources` على إعدادات قاعدة حزمة الشبكة. ويتم سرد إعدادات قاعدة حزمة الشبكة المخصصة في القسم `<"key name="0004>`.

علامات قاعدة حزمة الشبكة المخصصة

```
                                                                    <"key name="0026>
                                                                <"key name="Data>
                                                    <key name="RemotePorts"> </key>
                                                    <key name="LocalPorts"> </key>
                                                    <"key name="AdapterBindings>
                                                    <"key name="0000>
                                            <"key name="IpAddresses>
                                    <"key name="0000>
                                    <"key name="IP>
                            <"key name="V6>
                             tQWORD>
                                                                    <name="Hi">0</tQWORD
                             tQWORD>
                                                                    <name="Lo">0</tQWORD
                             tDWORD>
                                                                  <name="Zone">0</tDWORD
                     tSTRING>
                                                                        </"name="ZoneStr
                                  <key/>
                                    tBYTE>
                                                                  <name="Version">4</tBYTE
                                    tDWORD>
                                                                <name="V4">16909060</tDWORD
<tBYTE name="Mask">32</tBYTE>
                                          <key/>
                <key name="AddressIP"> </key>
                </"tSTRING name="Address>
                                                    <key/>
                                                            <key/>
                                    <"key name="MacAddresses>
                                    <"key name="0000>
                <tDWORD name="Type">0</tDWORD>
                                              tQWORD>
                                                    <name="AddressData0">1108152157446</tQWORD
<tQWORD name="AddressData1">0</tQWORD>
                                                    <key/>
                                                            <key/>
```

```
<tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                <tDWORD name="InterfaceType">3</tDWORD>
                                                <key/>
                                                    <key/>
                        <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                                    <tBYTE name="Proto">2</tBYTE>
                            <tBYTE name="Direction">2</tBYTE>
                                    <tBYTE name="IcmpType">0</tBYTE>
                                    <tBYTE name="IcmpCode">0</tBYTE>
                                    <tDWORD name="Flags">1</tDWORD>
                                    <tBYTE name="TTL">255</tBYTE>
                                                            <key/>
                                        <key name="Childs"> </key>
                                    <tDWORD name="Id">1073747214</tDWORD>
                                    <tDWORD name="ParentID">7</tDWORD>
                                        <tDWORD name="Flags">38</tDWORD>
                                    <tSTRING name="Name">TEST1</tSTRING>
                                                                <key/>
```

إعدادات قاعدة حزمة الشبكة المخصصة

المعلمة	الوصف	القيمة
key> <"name="Data	معرف قسم المعلمة.	عدد صحيح
RemotePorts	قيمة معلمة **المنافذ البعيدة**.	قائمة نطاقات المنافذ البعيدة.
LocalPorts	قيمة معلمة **المنافذ المحلية**.	قائمة نطاقات المنافذ المحلية.
AdapterBindings	قيمة معلمة **محوّلات الشبكة**.	IpAddresses – قيمة معلمة **عناوين IP**. MacAddresses – قيمة معلمة **عناوين MAC**. AdapterName – اسم محول الشبكة. InterfaceType – قيمة معلمة **نوع الواجهة**: • 0 – **أخرى**. • 1 – **LoopBack**. • 2 – **الشبكة السلكية (الإيثرنت)**. • 3 – **شبكة لاسلكية (Wi-Fi)**. • 4 – **النفق**. • 5 – **اتصال PPP**. • 6 – **اتصال PPPoE**. • 7 – **اتصال VPN**. • 8 – **اتصال مودم**.
unique	المعرف الداخلي للبنية.	عدد صحيح يوصى بترك هذه المعلمة دون تغيير.

`Proto`	قيمة معلمة **البروتوكول**.	`0` – تم التعطيل. `1` – ICMP. `2` – IGMP. `6` – TCP. `17` – UDP. `47` – GRE. `58` – ICMPv6.
`Direction`	قيمة معلمة **الاتجاه**.	1 – **الوارد (حزمة)**. 2 – **الصادر (حزمة)**. 3 – **الوارد / الصادر**. 4 – **الوارد**. 5 – **الصادر**.
`IcmpType`	قيمة معلمة **نوع ICMP**.	بروتوكول ICMP 0 – **رد الارتداد** (ICMP) أو تم التعطيل. 3 – **وجهة يتعذر الوصول إليها** (ICMP). 4 – **كبح المصدر**. 5 – **إعادة توجيه**. 6 – **عنوان المضيف البديل**. 8 – **طلب الارتداد**. 9 – **إعلانات الموجه**. 10 – **اتصال الموجه**. 11 – **تجاوز الوقت**. 12 – **مشكلة المعلمة**. 13 – **الطابع الزمني**. 14 – **رد الطابع الزمني**. 15 – **طلب المعلومات**. 16 – **رد المعلومات**. 17 – **طلب قناع العنوان**. 18 – **رد قناع العنوان**. 30 – **مسار التتبع**. 31 – **خطأ تحويل مخطط البيانات**. 32 – **إعادة توجيه المضيف المتنقل**. 33 – IPv6 Where-Are-You. 34 – IPv6 I-Am-Here. 35 – **طلب التسجيل المتنقل**. 36 – **رد التسجيل المتنقل**. 37 – **طلب اسم المجال**. 38 – **رد اسم المجال**. 40 – Photuris.

پروتوکول ICMPv6

1 – وجهة يتعذر الوصول إليها.

2 – الحزمة كبيرة للغاية.

3 – تجاوز الوقت.

4 – مشكلة المعلمة.

128 – طلب الارتداد.

129 – رد الارتداد.

130 – استعلام موزع رسائل الإرسال المتعدد.

131 – تقرير موزع رسائل الإرسال المتعدد.

132 – اكتمل موزع رسائل الإرسال المتعدد.

133 – اتصال الموجه.

134 – إعلانات الموجه.

135 – اتصال الجوار.

136 – إعلانات الجوار.

137 – إعادة توجيه الرسالة.

138 – إعادة ترقيم الموجه.

139 – الاستعلام عن معلومات عقدة ICMP.

141 – رسالة اتصال اكتشاف الجوار العكسي.

142 – رسالة إعلان اكتشاف الجوار العكسي.

143 – تقرير موزع رسائل الإرسال المتعدد الإصدار 2.

144 – رسالة طلب اكتشاف عنوان العامل الرئيسي.

145 – رسالة الرد على اكتشاف عنوان العامل الرئيسي.

146 – اتصال البادئة المتنقلة.

147 – إعلان البادئة المتنقلة.

148 – رسالة الاتصال بمسار الشهادة.

149 – رسالة إعلان مسار الشهادة.

151 – إعلان موجه الإرسال المتعدد.

		152 – **اتصال موجه الإرسال المتعدد**. 153 – **إنهاء موجه الإرسال المتعدد**.
IcmpCode	قيمة معلمة **رمز ICMP**.	0 – **الكود 0** أو تم التعطيل. 1 – **الكود 1**. 2 – **الكود 2**.
Flags	مؤشر سمة البنية.	عدد صحيح يوصى بترك هذه المعلمة دون تغيير.
TTL	قيمة معلمة **مدة البقاء (TTL)**.	القيمة بالثواني. وفي حالة التعطيل، تكون القيمة 0.
<key/>		
Id	المعرّف الرئيسي للمورد (انظر العقدة القواعد).	عدد صحيح
ParentID	معرّف المجموعة الرئيسية.	عدد صحيح يوصى بترك هذه المعلمة دون تغيير.
Flags	حالة القاعدة.	6 – تم تعطيل القاعدة. 38 – تم تمكين القاعدة.
Name	اسم قاعدة حزمة الشبكة.	السلسلة

إدارة قواعد الشبكة للتطبيق

بشكل افتراضي، يقوم Kaspersky Endpoint Security بتجميع جميع التطبيقات المثبتة على الكمبيوتر من خلال اسم بائع البرامج الذي يقوم هذا البرنامج بمراقبة الملف أو نشاط الشبكة الخاصة به. يتم تصنيف مجموعات التطبيقات في مجموعات ثقة. ترث جميع التطبيقات ومجموعات التطبيق الخصائص من المجموعة الأصل الخاصة بها: قواعد حزمة الشبكة وقواعد شبكة التطبيق وأولوية التنفيذ.

مثل مكون منع اختراق المضيف، يطبق مكون جدار الحماية بشكل افتراضي قواعد الشبكة لمجموعة تطبيق عند تصفية نشاط الشبكة لكل التطبيقات داخل المجموعة. تحدد قواعد شبكة مجموعة التطبيقات حقوق التطبيقات داخل المجموعة للوصول إلى مختلف اتصالات الشبكة.

وحسب إعداد التهيئة المبدئية، يقوم جدار الحماية بإنشاء مجموعة قواعد شبكة لكل مجموعة تطبيقات يكتشفها البرنامج Kaspersky Endpoint Security في الكمبيوتر. يمكنك تغيير إجراء جدار الحماية الذي تم تطبيقه على قواعد شبكة مجموعة التطبيقات التي تم إنشاؤها بشكل افتراضي. لا يمكنك تحرير أولوية قواعد شبكة مجموعة التطبيقات التي تم إنشاؤها بشكل افتراضي أو إزالتها أو تعطيلها أو تغييرها.

يمكنك أيضًا إنشاء قاعدة شبكة لتطبيق فردي. وسيكون لهذه القاعدة أولوية أكبر من قاعدة الشبكة الخاصة بالمجموعة التي ينتمي إليها التطبيق.

إنشاء قاعدة شبكة للتطبيق

بشكل افتراضي، يتم التحكم في نشاط التطبيقات بواسطة قواعد الشبكة المحددة لمجموعة الثقة التي عيّن لها Kaspersky Endpoint Security التطبيق عندما بدأت العمل لأول مرة. عند الضرورة، يمكنك إنشاء قواعد الشبكة لمجموعة ثقة بالكامل أو لتطبيق فردي أو لمجموعة من التطبيقات الموجودة ضمن مجموعة ثقة.

تكون لقواعد الشبكة المحددة يدويًا أولوية أعلى من قواعد الشبكة التي تم تحديدها لمجموعة ثقة. بمعنى آخر، إذا كانت قواعد التطبيق المحددة يدويًا تختلف عن قواعد التطبيق المحددة لمجموعة ثقة، يتحكم جدار الحماية في نشاط التطبيق وفقًا للقواعد المحددة يدويًا للتطبيقات.

بشكل افتراضي، ينشئ جدار الحماية قواعد الشبكة التالية لكل تطبيق:

- أي نشاط للشبكة في الشبكات الموثوقة.
- أي نشاط للشبكة في شبكات الاتصال المحلية.
- أي نشاط للشبكة في الشبكات العامة.

يتحكم Kaspersky Endpoint Security في نشاط الشبكة للتطبيقات وفقًا لقواعد الشبكة المحددة مسبقًا على النحو التالي:

- موثوق ومقيد بشكل منخفض: يُسمح بجميع أنشطة الشبكة.
- مقيد بشكل عالٍ وغير موثوق: يتم منع كل أنشطة الشبكة.

لا يمكن تحرير أو حذف قواعد التطبيق المحددة مسبقًا.

يمكنك إنشاء قاعدة شبكة لتطبيق بالطرق التالية:

- استخدام أداة مراقبة شبكة الاتصال.

  مراقبة شبكة الاتصال عبارة عن أداة تستخدم لعرض معلومات حول نشاط الشبكة الخاصة بكمبيوتر المستخدم في الوقت الحقيقي. وهذا مناسب لأنك لست بحاجة إلى تكوين جميع إعدادات القاعدة. وسيتم إدراج بعض إعدادات جدار الحماية تلقائيًا من بيانات مراقبة شبكة الاتصال. وتتوفر مراقبة شبكة الاتصال فقط في واجهة التطبيق.

- تكوين إعدادات جدار الحماية.

  يتيح لك هذا ضبط إعدادات جدار الحماية. ويمكنك إنشاء قواعد لأي نشاط للشبكة، حتى إذا لم يكن هناك نشاط للشبكة في الوقت الحالي.

عند إنشاء قواعد شبكة للتطبيقات، تذكر أن قواعد حزم الشبكة لها الأولوية على قواعد الشبكة للتطبيق.

كيفية استخدام أداة مراقبة شبكة الاتصال لإنشاء قاعدة شبكة لتطبيق في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **مراقبة شبكة الاتصال**.

2. حدد **نشاط الشبكة** أو علامة التبويب **المنافذ المفتوحة**.

تعرض علامة التبويب **نشاط الشبكة** كل اتصالات الشبكة الحالية النشطة بالكمبيوتر. ويتم عرض كل من اتصالي الشبكة الواردة والصادرة.

تدرج علامة التبويب **المنافذ المفتوحة** كل منافذ الشبكة المفتوحة بالكمبيوتر.

3. في قائمة سياق اتصال الشبكة، حدد **إنشاء قاعدة شبكة للتطبيق**.

تفتح نافذة قواعد التطبيق والخصائص.

4. حدد علامة التبويب **قواعد شبكة الاتصال**.

يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

5. انقر على **إضافة**.

يفتح هذا خصائص قاعدة الشبكة.

6. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.

7. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).

يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **قالب قاعدة الشبكة**. تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.

سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

8. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.

9. انقر على **حفظ**.

ستتم إضافة قاعدة الشبكة الجديدة إلى القائمة.

10. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

11. احفظ تغييراتك.

كيفية استخدام إعدادات جدار الحماية لإنشاء قاعدة شبكة لتطبيق في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **قواعد التطبيقات**.
يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

4. في قائمة التطبيقات، حدد التطبيق أو مجموعة التطبيقات التي ترغب في إنشاء قاعدة الشبكة لها.

5. انقر بزر الماوس الأيمن لفتح قائمة السياق وحدد **تفاصيل وقواعد**.
تفتح نافذة قواعد التطبيق والخصائص.

6. حدد علامة التبويب **قواعد شبكة الاتصال**.

7. انقر على **إضافة**.
يفتح هذا خصائص قاعدة الشبكة.

8. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.

9. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).
يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **قالب قاعدة الشبكة**. تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.
سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

10. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.

11. انقر على **حفظ**.
ستتم إضافة قاعدة الشبكة الجديدة إلى القائمة.

12. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

13. احفظ تغييراتك.

كيفية إنشاء قاعدة شبكة للتطبيق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية ← جدار الحماية**.

5. في القسم **إعدادات جدار الحماية**، انقر على الزر **الإعدادات**.

يفتح هذا قائمة قواعد حزم الشبكة وقائمة قواعد الشبكة للتطبيق.

6. حدد علامة التبويب **قواعد شبكة الاتصال للتطبيق**.

7. انقر على **إضافة**.

8. في النافذة التي تفتح، أدخل معايير للبحث عن التطبيق الذي ترغب في إنشاء قاعدة شبكة له.

يمكنك إدخال اسم التطبيق أو اسم البائع. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع.

9. انقر فوق الزر **تحديث**.

سيبحث Kaspersky Endpoint Security عن التطبيق في القائمة الموحدة للتطبيقات المثبتة على أجهزة الكمبيوتر المدارة. سيعرض Kaspersky Endpoint Security قائمة بالتطبيقات التي تلبي معايير البحث الخاصة بك.

10. حدد التطبيق المطلوب.

11. في القائمة المنسدلة **إضافة التطبيق المحدد إلى مجموعة الثقة**، حدد **المجموعات الافتراضية** وانقر فوق **موافق**.

ستتم إضافة التطبيق إلى المجموعة الافتراضية.

12. حدد التطبيق ذي الصلة، ثم حدد **حقوق التطبيق** من قائمة السياق الخاصة بالتطبيق.

تفتح نافذة قواعد التطبيق والخصائص.

13. حدد علامة التبويب **قواعد شبكة الاتصال**.

يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

14. انقر على **إضافة**.

يفتح هذا خصائص قاعدة الشبكة.

15. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.

16. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).

يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الزر . تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.

سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

17. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.

18. حفظ قاعدة الشبكة الجديدة

19. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

20. احفظ تغييراتك.

كيفية إنشاء قاعدة شبكة لتطبيق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. حدد **Firewall** ← **Essential Threat Protection**.

5. في القسم **Firewall Settings**، انقر على الرابط **Application network rules**.
يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **Application rights**.
سترى قائمة تتضمن مجموعات الثقة على الجانب الأيمن من النافذة وخصائصها على الجانب الأيسر.

7. انقر على **Add**.
يؤدي هذا إلى تشغيل المعالج لإضافة تطبيق إلى مجموعة ثقة.

8. حدد مجموعة الثقة ذات الصلة للتطبيق.

9. حدد نوع **Application**. انتقل إلى الخطوة التالية.
إذا كنت تريد إنشاء قاعدة شبكة لتطبيقات متعددة، فحدد نوع **Group** ثم حدد اسمًا لمجموعة التطبيق.

10. في قائمة التطبيقات المفتوحة، حدد التطبيقات التي ترغب في إنشاء قاعدة شبكة لها.
استخدم عامل تصفية. يمكنك إدخال اسم التطبيق أو اسم البائع. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع.

11. أغلق المعالج.
ستتم إضافة التطبيق إلى مجموعة الثقة.

12. في الجزء الأيمن من النافذة، حدد التطبيق ذي الصلة.

13. في الجزء الأيسر من النافذة، حدد **Network rules** من القائمة المنسدلة.
يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

14. انقر على **Add**.
يفتح هذا خصائص قاعدة التطبيق.

15. أدخل اسم خدمة الشبكة يدويًا في الحقل **Name**.

16. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).
يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **Select template**. تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.
سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

17. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **Log events**.

18. احفظ قاعدة الشبكة.
ستتم إضافة قاعدة الشبكة الجديدة إلى القائمة.

19. استخدم الزرين **Up** / **Down** لتعيين أولوية قاعدة الشبكة.

20. احفظ تغييراتك.

إعدادات قاعدة الشبكة للتطبيق

المعلمة	الوصف
الإجراء	**سماح**. **منع**.
البروتوكول	مراقبة نشاط الشبكة عبر البروتوكول المحدد: TCP وUDP وICMP وICMPv6 وIGMP وGRE. في حالة تحديد ICMP أو ICMPv6 كبروتوكول، يمكنك تحديد نوع حزمة ICMP ورمزها. في حالة تحديد TCP أو UDP كنوع البروتوكول، يمكنك تحديد أرقام المنافذ المحددة بفاصلة لأجهزة الكمبيوتر المحلية والبعيدة التي سيتم مراقبة الاتصال بينها.
الاتجاه	**الوارد**. **الوارد / الصادر**. **الصادر**.
العنوان البعيد	عناوين الشبكة لأجهزة الكمبيوتر البعيدة التي يمكنها إرسال و استقبال حزم شبكة الاتصال. يطبق جدار الحماية قاعدة الشبكة على النطاق المحدد لعناوين الشبكة البعيدة. ويمكنك تضمين كل عناوين IP في قاعدة شبكة، أو إنشاء قائمة منفصلة بعناوين IP، أو تحديد نطاق من عناوين IP، أو تحديد شبكة فرعية (الشبكات الموثوقة وشبكات الاتصال المحلية وشبكات الاتصال العامة). ويمكنك أيضًا تحديد اسم DNS لجهاز كمبيوتر بدلاً من عنوان IP الخاص به. ويجب عليك استخدام أسماء DNS فقط لأجهزة كمبيوتر الشبكة المحلية (LAN) أو الخدمات الداخلية. ويجب التعامل مع التفاعل مع الخدمات السحابية (مثل Microsoft Azure) وموارد الإنترنت الأخرى بواسطة مكون التحكم في الويب. يدعم Kaspersky Endpoint Security أسماء DNS بدءًا من الإصدار 11.7.0. إذا حددت اسم DNS للإصدار 11.6.0 أو أقدم، فقد يطبق Kaspersky Endpoint Security القاعدة ذات الصلة على جميع العناوين.
العنوان المحلي	عناوين الشبكة لأجهزة الكمبيوتر التي يمكنها إرسال واستقبال حزم شبكة الاتصال. يطبق جدار الحماية قاعدة شبكة على النطاق المحدد لعناوين الشبكة المحلية. ويمكنك تضمين كل عناوين IP في قاعدة شبكة أو إنشاء قائمة منفصلة بعناوين IP، أو تحديد نطاق من عناوين IP. يدعم Kaspersky Endpoint Security أسماء DNS بدءًا من الإصدار 11.7.0. إذا حددت اسم DNS للإصدار 11.6.0 أو أقدم، فقد يطبق Kaspersky Endpoint Security القاعدة ذات الصلة على جميع العناوين. أحيانًا لا يمكن الحصول على العنوان المحلي للتطبيقات. وإذا كانت هذه هي الحالة، فسيتم تجاهل هذه المعلمة.

تمكين وتعطيل قعدة شبكة التطبيق

لتمكين أو تعطيل قاعدة الشبكة الخاصة بالتطبيق:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.
3. انقر على **قواعد التطبيقات**.
   يفتح هذا قائمة قواعد التطبيق.
4. في قائمة التطبيقات، حدد التطبيق أو مجموعة التطبيقات التي ترغب في إنشاء قاعدة الشبكة لها أو تحريرها.

5. انقر بزر الماوس الأيمن لفتح قائمة السياق وحدد **تفاصيل وقواعد**.
تفتح نافذة قواعد التطبيق والخصائص.

6. حدد علامة التبويب **قواعد شبكة الاتصال**.

7. في قائمة قواعد الشبكة الخاصة بمجموعة تطبيقات، حدد قاعدة الشبكة المعنية.
تفتح نافذة خصائص قاعدة الشبكة.

8. قم بتعيين الحالة **فعال** أو **غير فعال** لقاعدة الشبكة.
لا يمكنك تعطيل قاعدة شبكة الاتصال الخاصة بمجموعة التطبيقات التي تم إنشاؤها باستخدام جدار الحماية بشكل افتراضي.

9. احفظ تغييراتك.

تغيير إجراء جدار الحماية الخاص بقاعدة شبكة اتصال لتطبيق

يمكنك تغيير إجراء "جدار الحماية" المطبق على كل قواعد الشبكة الخاصة بأحد التطبيقات أو بمجموعة تطبيقات تم إنشاؤها بشكل افتراضي، وتغيير إجراء "جدار الحماية" الخاص بقاعدة شبكة مخصصة فردية لتطبيق أو مجموعة تطبيقات.

لتغيير إجراء جدار الحماية لكل قواعد الشبكة لأحد التطبيقات أو مجموعة تطبيقات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **قواعد التطبيقات**.
يفتح هذا قائمة قواعد التطبيق.

4. إذا كنت تريد تغيير إجراء جدار الحماية المطبق على كل قواعد الشبكة التي تم إنشاؤها بشكل افتراضي، حدد التطبيق أو مجموعة التطبيقات في القائمة. يتم ترك قواعد الشبكة للتطبيق التي تم إنشاؤها يدويًا بلا تغيير.

5. انقر بزر الماوس الأيمن لفتح قائمة السياق، وحدد **قواعد شبكة الاتصال**، ثم حدد الإجراء الذي تريد تعيينه:

- **توريث**.
- **سماح**.
- **منع**.

6. احفظ تغييراتك.

لتغيير استجابة "جدار الحماية" لإحدى قواعد الشبكة لأحد التطبيقات أو لمجموعة تطبيقات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **قواعد التطبيقات**.
يفتح هذا قائمة قواعد التطبيق.

4. في القائمة، حدد التطبيق أو مجموعة التطبيقات التي تريد لأجلها تغيير الإجراء قاعدة شبكة واحدة.

5. انقر بزر الماوس الأيمن لفتح قائمة السياق وحدد **تفاصيل وقواعد**.

تفتح نافذة قواعد التطبيق والخصائص.

6. حدد علامة التبويب **قواعد شبكة الاتصال**.

7. حدد قاعدة الشبكة التي تريد لأجلها تغيير إجراء جدار الحماية.

8. في العمود **الإذن**، انقر بزر الماوس الأيمن لعرض القائمة السياقية وتحديد الإجراء الذي ترغب في تعيينه:

- **توريث**.
- **سماح**.
- **رفض**.
- **أحداث السجل**.

9. احفظ تغييراتك.

تغيير أولوية قاعدة شبكة تطبيق

يتم تحديد أولوية قاعدة الشبكة حسب موقعها في قائمة قواعد الشبكة. يقوم جدار الحماية بتنفيذ هذه القواعد بالترتيب التي تظهر به في قائمة قواعد الشبكة بدءًا من أعلى إلى أسفل. ووفقًا لكل قاعدة شبكة تنطبق على اتصال شبكة محددة تمت معالجتها، يقوم جدار الحماية إما بالسماح بوصول الشبكة أو منع وصولها إلى العنوان والمنفذ المحدد في إعدادات اتصال الشبكة هذا.

يكون لقواعد الشبكة التي تم إنشاؤها يدويًا أولوية أعلى من قواعد الشبكة الافتراضية.

لا يمكنك تغيير أولوية قواعد شبكة مجموعة التطبيقات التي تم إنشاؤها بشكل افتراضي.

لتغيير أولوية قاعدة الشبكة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

3. انقر على **قواعد التطبيقات**.
يفتح هذا قائمة قواعد التطبيق.

4. في قائمة التطبيقات، حدد التطبيق أو مجموعة التطبيقات التي ترغب لأجلها في تغيير أولوية قاعدة شبكة.

5. انقر بزر الماوس الأيمن لفتح قائمة السياق وحدد **تفاصيل وقواعد**.
تفتح نافذة قواعد التطبيق والخصائص.

6. حدد علامة التبويب **قواعد شبكة الاتصال**.

7. حدد قاعدة الشبكة التي تريد تغيير أولويتها.

8. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

9. احفظ تغييراتك.

مراقبة شبكة الاتصال

مراقبة شبكة الاتصال عبارة عن أداة تستخدم لعرض معلومات حول نشاط الشبكة الخاصة بكمبيوتر المستخدم في الوقت الحقيقي.

لبدء مراقبة شبكة الاتصال:

في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **مراقبة شبكة الاتصال**.

تفتح النافذة مراقبة شبكة الاتصال. يتم عرض معلومات حول نشاط الشبكة لهذا الكمبيوتر على أربعة علامات تبويب في هذه النافذة:

- تعرض علامة التبويب **نشاط الشبكة** كل اتصالات الشبكة الحالية النشطة بالكمبيوتر. ويتم عرض كل من اتصالي الشبكة الواردة والصادرة. يمكنك في علامة التبويب هذه أيضًا إنشاء قواعد حزم الشبكة لعملية جدار الحماية.
- تدرج علامة التبويب **المنافذ المفتوحة** كل منافذ الشبكة المفتوحة بالكمبيوتر. وفي علامة التبويب هذه، يمكنك أيضًا إنشاء قواعد حزم الشبكة وقواعد التطبيق لعملية جدار الحماية.
- تعرض علامة التبويب **حركة شبكة الاتصال** مقدار الحركة الواردة والصادرة بين كمبيوتر المستخدم وأجهزة الكمبيوتر في الشبكة التي يتصل بها المستخدم في الوقت الحالي.
- تسرد علامة التبويب **أجهزة الكمبيوتر المحظورة** عناوين بروتوكول الإنترنت لأجهزة الكمبيوتر البعيدة التي تم حظر نشاط الشبكة الخاص بها بواسطة مكون الحماية من تهديدات الشبكة بعد اكتشاف محاولات تنفيذ هجمات عبر الشبكة من عناوين بروتوكول الإنترنت (IP) هذه.

منع هجمات BadUSB

تقوم بعض الفيروسات بتعديل البرامج الثابتة لأجهزة USB، بهدف خداع نظام التشغيل ليكتشف جهاز USB على أنه لوحة مفاتيح. نتيجة لذلك، قد ينفذ الفيروس أوامر من حساب المستخدم الخاص بك لتنزيل البرامج الضارة، على سبيل المثال.

يمنع المكون "منع هجمات BadUSB" أجهزة USB المصابة من محاكاة لوحة المفاتيح للاتصال بالكمبيوتر.

عند توصيل جهاز USB بالكمبيوتر وتم التعرف عليه كلوحة مفاتيح بواسطة نظام التشغيل، يطلب التطبيق من المستخدم إدخال رمز رقمي يتم إنشاؤه بواسطة التطبيق من لوحة المفاتيح هذه أو باستخدام لوحة المفاتيح على الشاشة إذا كانت متاحة (انظر الشكل أدناه). يُعرف هذا الإجراء باسم مصادقة لوحة المفاتيح.

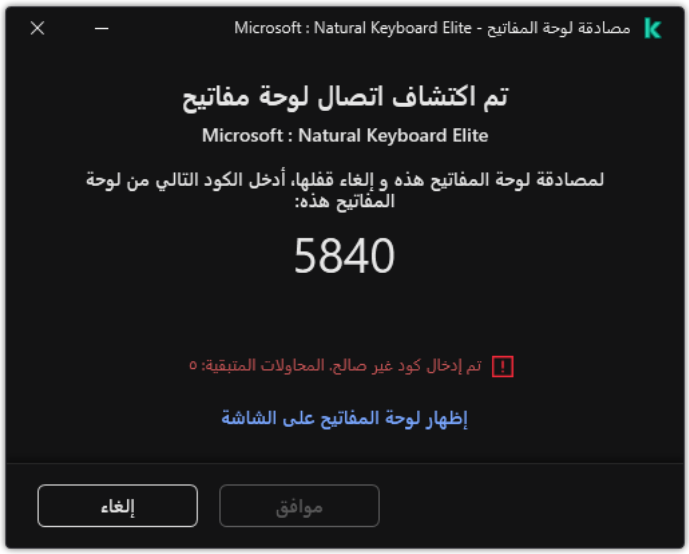
إذا تم إدخال الرمز بشكل صحيح، فيقوم التطبيق بحفظ معلمات التعريف – VID/PID للوحة المفاتيح ورقم المنفذ الذي تم توصيلها به – في قائمة لوحات المفاتيح المصرح لها. لا يلزم تكرار مصادقة لوحة المفاتيح عند إعادة توصيل لوحة المفاتيح أو بعد إعادة تشغيل نظام التشغيل.

عندما يتم توصيل لوحة المفاتيح المصرح لها بمنفذ مختلف في الكمبيوتر، يقوم التطبيق بإظهار مطالبة بالحصول على تصريح للوحة المفاتيح هذه مرة أخرى.

إذا تم إدخال الرمز الرقمي بطريقة غير صحيحة، فيقوم التطبيق بإنشاء رمز جديد. يمكنك تكوين عدد محاولات إدخال الرمز العددي. وفي حالة إدخال الرمز العددي بشكل غير صحيح عدة مرات أو إغلاق نافذة مصادقة لوحة المفاتيح (انظر الشكل أدناه)، فإن التطبيق يحظر الإدخال من لوحة المفاتيح هذه. وعند انقضاء وقت منع جهاز USB أو إعادة تشغيل نظام التشغيل، يطالب التطبيق المستخدم بإجراء مصادقة للوحة المفاتيح مرة أخرى.

يتيح التطبيق استخدام لوحة مفاتيح مصرح لها، ويمنع لوحة المفاتيح التي لم يتم التصريح لها.

لا يتم تثبيت مكون الوقاية من هجمات USB الخبيثة بشكل افتراضي. إذا كنت بحاجة إلى مكون الوقاية من هجمات USB الخبيثة، يمكنك إضافة المكون في خصائص حزمة التثبيت قبل تثبيت التطبيق أو تغيير مكونات التطبيق المتاحة بعد تثبيت التطبيق.



مصادقة لوحة المفاتيح

تمكين "منع هجمات BadUSB" أو تعطيلها

تعتبر أجهزة USB التي تم التعرف عليها بواسطة نظام التشغيل على أنها لوحات مفاتيح وتم توصيلها بالكمبيوتر قبل تثبيت مكون منع هجمات BadUSB مُصرح لها بعد تثبيت المكون.

لتمكين أو تعطيل منع هجمات BadUSB:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← منع هجمات BadUSB**.
3. استخدم مفتاح تبديل **منع هجمات BadUSB** لتمكين المكون أو تعطيله.
4. في القسم **مصادقة لوحة مفاتيح USB عند الاتصال**، اضبط إعدادات الأمان لإدخال رمز التفويض:

- **الحد الأقصى لعدد محاولات مصادقة جهاز USB**. حظر جهاز USB تلقائيًا في حالة إدخال رمز المصادقة بشكل غير صحيح لعدد المرات المحدد. القيم الصالحة من 1 إلى 10. على سبيل المثال، إذا سمحت بخمس محاولات لإدخال رمز المصادقة، فسيتم حظر جهاز USB بعد المحاولة الفاشلة الخامسة. ويعرض Kaspersky Endpoint Security مدة الحظر لجهاز USB. وبعد انقضاء هذا الوقت، يكون لديك 5 محاولات لإدخال رمز المصادقة.
- **المهلة عند الوصول إلى الحد الأقصى لعدد المحاولات**. مدة حظر جهاز USB بعد العدد المحدد من المحاولات الفاشلة لإدخال رمز المصادقة. القيم الصالحة من 1 إلى 180 (دقيقة).

5. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين منع هجوم BadUSB، فإن Kaspersky Endpoint Security يتطلب مصادقة لجهاز USB موصل تم التعرف عليه كلوحة مفاتيح بواسطة نظام التشغيل. يتعذر على المستخدم استخدام لوحة مفاتيح غير مصرح لها إلى أن يتم التصريح لها.

استخدام لوحة المفاتيح على الشاشة للمصادقة على أجهزة USB

ينبغي استخدام لوحة المفاتيح على الشاشة فقط للحصول على تصريح لأجهزة USB التي لا تدعم إدخال أحرف عشوائية (على سبيل المثال، ماسحات الباركود). من غير المستحسن استخدام لوحة المفاتيح على الشاشة للحصول على تصريح لأجهزة USB غير المعروفة.

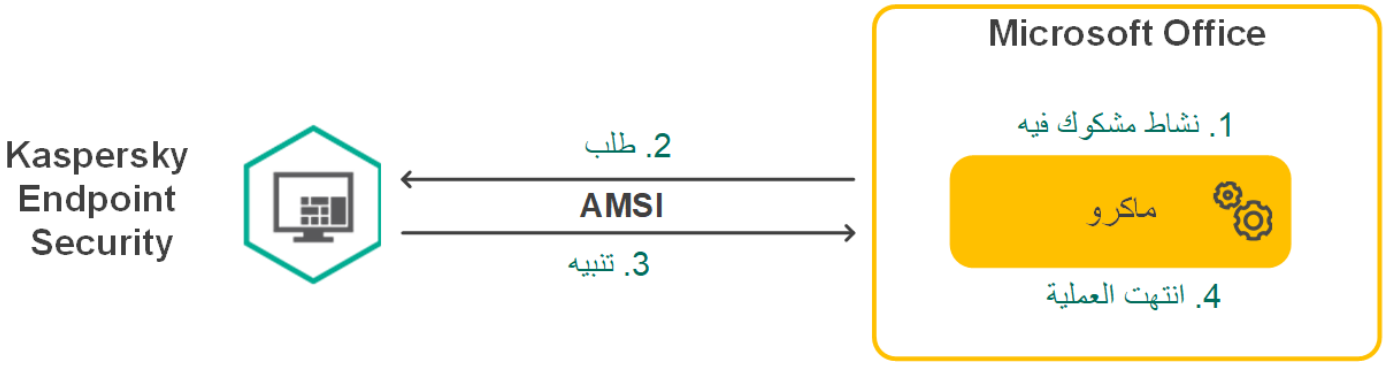
للسماح أو تعطيل استخدام لوحة المفاتيح على الشاشة للحصول على تصريح:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← منع هجمات BadUSB**.
3. استخدم خانة الاختيار **منع استخدام لوحة المفاتيح على الشاشة لمصادقة أجهزة USB** لمنع استخدام لوحة المفاتيح على الشاشة أو السماح باستخدامها للمصادقة.
4. احفظ تغييراتك.

حماية AMSI

يكون مكون حماية AMSI مخصصًا لدعم واجهة فحص البرمجيات الضارة من Microsoft. تتيح واجهة فحص البرمجيات الضارة (AMSI) للتطبيقات الخارجية التي تتمتع بدعم AMSI إرسال الكائنات (على سبيل المثال، البرامج النصية PowerShell) إلى برنامج Kaspersky Endpoint Security لإجراء عملية فحص إضافية واستقبال نتائج الفحص لهذه الكائنات. قد تتضمن التطبيقات الخارجية، على سبيل المثال، تطبيقات Microsoft Office (انظر الشكل أدناه). ولمعرفة التفاصيل حول AMSI، يُرجى الرجوع إلى وثائق Microsoft.

لا يستطيع مكون حماية AMSI سوى اكتشاف التهديدات وإخطار تطبيق خارجي بالتهديد المكتشف. لا يتيح التطبيق الخارجي بعد استلام الإخطار بوجود تهديد تنفيذ إجراءات مشكوك فيها (على سبيل المثال، عمليات الإنهاء).



مثال عملية AMSI

قد يرفض مكون حماية AMSI طلبًا من تطبيق خارجي، على سبيل المثال، إذا تجاوز هذا التطبيق الحد الأقصى لعدد الطلبات في خلال فترة زمنية محددة. يرسل Kaspersky Endpoint Security معلومات بشأن طلب مرفوض من تطبيق تابع لجهة خارجية إلى خادم الإدارة. لا يرفض مكون حماية AMSI الطلبات الواردة من تطبيقات الطرف الثالث التي يتم تمكين التكامل المستمر مع مكون حماية AMSI لأجلها.

تتوفر وظائف مكون حماية AMSI لأنظمة التشغيل التالية المخصصة لمحطات العمل والخوادم:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise؛
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise؛
- Windows Server 2016 Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2019 Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (بما في ذلك Core Mode).

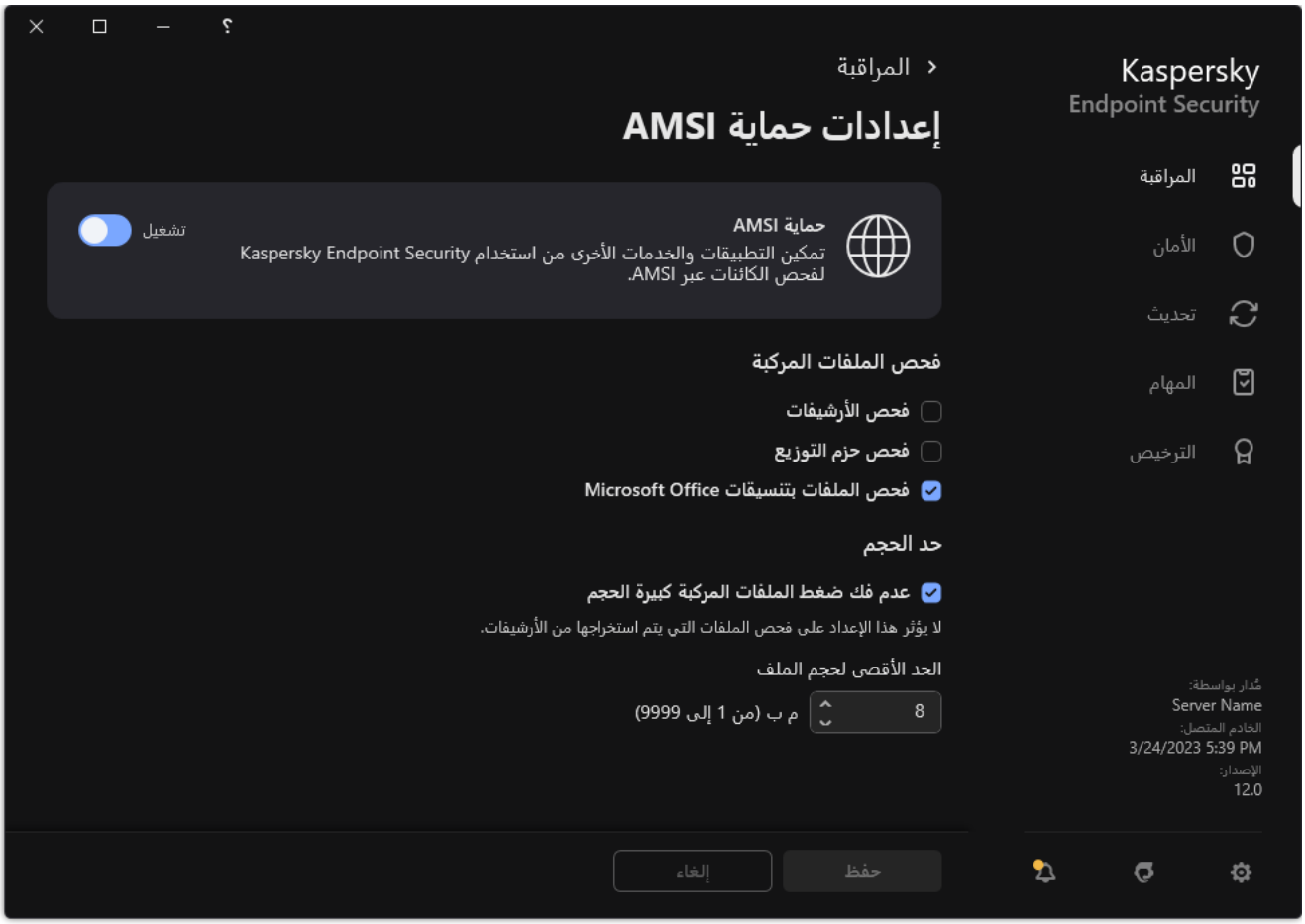
تمكين حماية AMSI وتعطيلها

يتم تمكين حماية AMSI افتراضيًا.

لتمكين حماية AMSI وتعطيلها:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **حماية AMSI**.



إعدادات حماية AMSI

3. استخدم مفتاح تبديل **حماية AMSI** لتمكين المكون أو تعطيله.

4. احفظ تغييراتك.

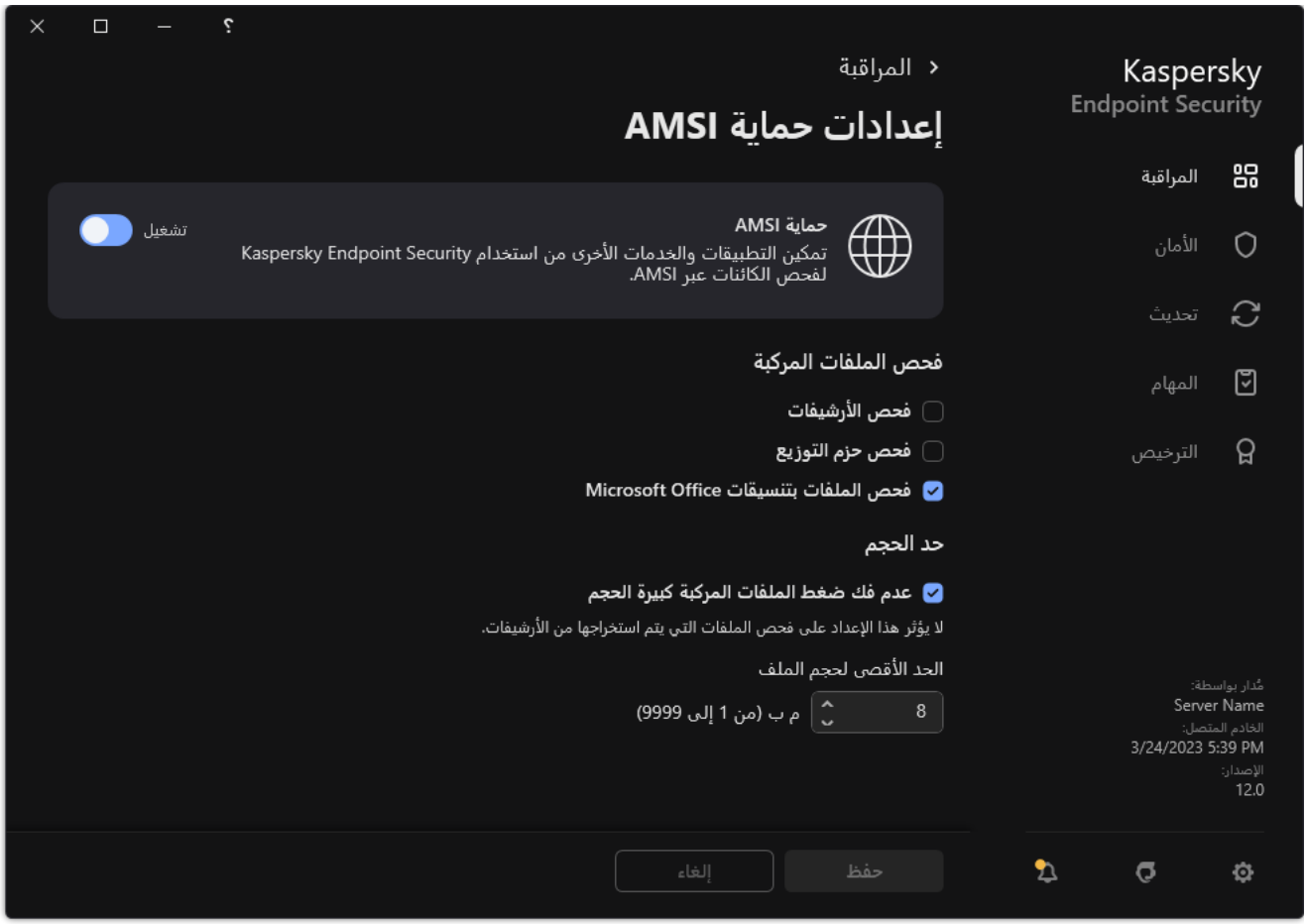
استخدام حماية AMSI لفحص الملفات المركبة

يعتبر تضمين الفيروسات والبرمجيات الضارة الأخرى في الملفات المركّبة، مثل ملفات الأرشيف من الأساليب الشائعة لإخفائها. ولاكتشاف الفيروسات والبرمجيات الضارة الأخرى المختبئة بهذه الطريقة، يجب فك حزمة الملف المركب، وهو الأمر الذي قد يؤدي إلى إبطاء عملية الفحص. يمكنك تقييد أنواع الملفات المركبة المراد فحصها، مما يؤدي إلى زيادة سرعة عميلة الفحص.

لتكوين حماية AMSI لفحص الملفات المركبة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية ← حماية AMSI**.



إعدادات حماية AMSI

3. في القسم **فحص الملفات المركبة**، حدد أنواع الملفات المركبة التي تريد فحصها: ملفات الأرشيف، أو حِزم التثبيت، أو الملفات بتنسيقات office.

4. في القسم **حد الحجم**، نفذ أحد الإجراءات التالية:

- لمنع مكون حماية AMSI من فك حزمة الملفات المركبة كبيرة الحجم، حدد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم** وحدد القيمة المطلوبة في الحقل **الحد الأقصى لحجم الملف**. لن يفك مكون الحماية AMSI حزمة الملفات المركبة التي يزيد حجمها عن الحجم المحدد.
- للسماح لمكون حماية AMSI بفك حزمة الملفات المركبة كبيرة الحجم، قم بمسح خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم**.

يفحص مكون حماية AMSI الملفات الكبيرة التي يتم استخراجها من الأرشيفات، بغض النظر عن تحديد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم** أم لا.

5. احفظ تغييراتك.

منع الاستغلال

مكون منع الاستغلال يكتشف رمز البرنامج الذي يستفيد من الثغرات الأمنية الموجودة على جهاز الكمبيوتر لاستغلال امتيازات المسؤول أو لتنفيذ أنشطة ضارة. على سبيل المثال، يمكن أن يستخدم المستغلون هجوم تجاوز سعة المخزن المؤقت للقيام بذلك، يُرسل المستغل كمية كبيرة من البيانات إلى تطبيق معرض للاختراق. عند معالجة هذه البيانات، ينفذ التطبيق المعرض للاختراق تعليمات برمجية ضارة. كنتيجة لهذا الهجوم، يمكن أن يبدأ المستغل عملية تثبيت مُصرح بها للبرمجيات الضارة. عند اكتشاف محاولة لتشغيل الملف التنفيذي من تطبيق قابل للاختراق والتي لم يتم تنفيذها من قِبل المستخدم، يحظر برنامج Kaspersky Endpoint Security تشغيل هذا الملف ويقوم بإخطار المستخدم.

تمكين وتعطيل منع الاستغلال

بشكل افتراضي، يتم تمكين منع الاستغلال ويعمل في الوضع الموصى به من قبل Kaspersky. يمكنك تعطيل منع الاستغلال، إذا لزم الأمر.

لتمكين أو تعطيل منع الاستغلال:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع الاستغلال**.
3. استخدم مفتاح تبديل **منع الاستغلال** لتمكين المكون أو تعطيله.
4. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين منع الاستغلال، سيقوم Kaspersky Endpoint Security بمراقبة الملفات القابلة للتنفيذ التي يتم تشغيلها بواسطة التطبيقات العرضة للخطر. إذا اكتشف Kaspersky Endpoint Security تشغيل ملف قابل للتنفيذ من تطبيق عرضة للاختراق بواسطة شيء آخر غير المستخدم، فسينفذ Kaspersky Endpoint Security الإجراء المحدد (على سبيل المثال، سيمنع العملية).

تحديد إجراء لاتخاذه عند اكتشاف استغلال

بشكل افتراضي، عند اكتشاف استغلال، يمنع Kaspersky Endpoint Security العمليات التي يحاول الاستغلال تنفيذها.

لاختيار إجراء لاتخاذه عند اكتشاف استغلال:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع الاستغلال**.
3. حدد الإجراء المناسب من القسم **عند اكتشاف استغلال**:
   - **منع التشغيل**. في حالة تحديد هذا العنصر، عند اكتشاف استغلال، يمنع Kaspersky Endpoint Security عمليات هذا الاستغلال ويدون إدخال سجل بالمعلومات حول هذا الاستغلال.
   - **إخطار**. في حالة تحديد هذا العنصر، عندما يكتشف Kaspersky Endpoint Security استغلالاً فإنه يسجل إدخالاً يحتوي على معلومات حول الاستغلال ويضيف معلومات حول هذا الاستغلال إلى قائمة التهديدات النشطة.
4. احفظ تغييراتك.

حماية ذاكرة عمليات النظام

بشكل افتراضي، يتم تمكين حماية ذاكرة عملية النظام.

لتمكين أو تعطيل حماية ذاكرة عملية النظام:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع الاستغلال**.

3. استخدم مفتاح التبديل **تمكين حماية ذاكرة عملية النظام** لتمكين هذه الميزة أو تعطيلها.

4. احفظ تغييراتك.

نتيجة لذلك، سيمنع Kaspersky Endpoint Security العمليات الخارجية التي تحاول الوصول إلى عمليات النظام.

اكتشاف السلوك

يتلقى مكون اكتشاف السلوك بيانات حول إجراءات التطبيقات على جهاز الكمبيوتر الخاص بك ويقدم هذه المعلومات إلى مكونات الحماية الأخرى لتحسين أدائها. يستخدم مكون اكتشاف السلوك توقيعات تدفق السلوك (BSS) للتطبيقات. إذا كان نشاط تطبيق متطابقًا مع توقيع تدفق سلوك، ينفذ Kaspersky Endpoint Security إجراء الاستجابة المحدد. ويوفر الأداء الوظيفي لبرنامج Kaspersky Endpoint Security المستند إلى توقيعات تدفق السلوك دفاعًا وقائيًا للكمبيوتر.

تمكين وتعطيل اكتشاف السلوك

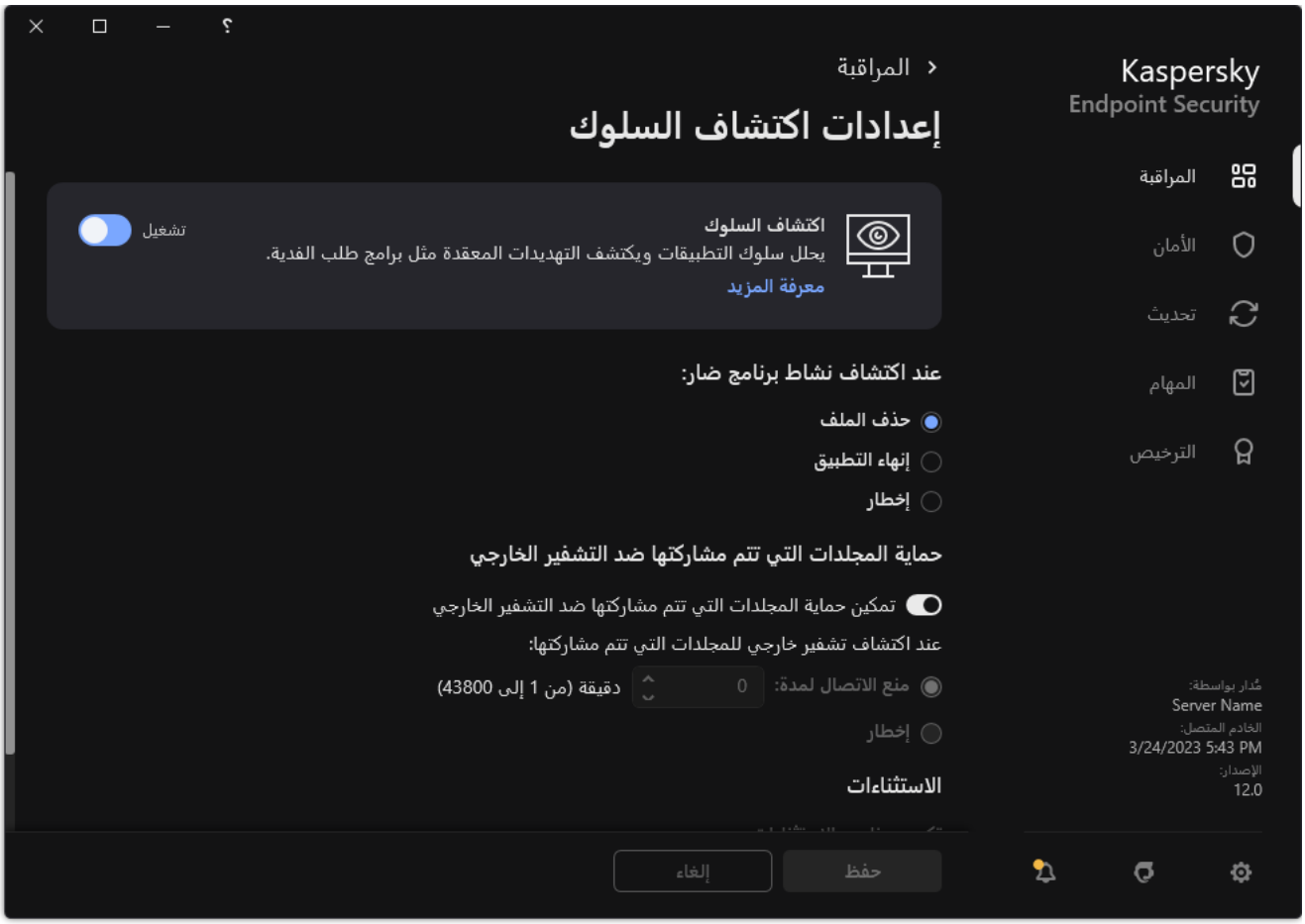
بشكل افتراضي، يتم تمكين اكتشاف السلوك ويعمل في الوضع الموصى به من قبل Kaspersky. يمكنك تعطيل اكتشاف السلوك، إذا لزم الأمر.

من غير المستحسن تعطيل اكتشاف السلوك إلا إذا كان ذلك ضروريًا تمامًا لأن فعل ذلك سوف يقلل من فعالية مكونات الحماية. وقد تطلب مكونات الحماية جمع البيانات بواسطة مكون اكتشاف السلوك لاكتشاف التهديدات.

لتمكين أو تعطيل اكتشاف السلوك:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **اكتشاف السلوك**.



إعدادات اكتشاف السلوك

3. استخدم مفتاح تبديل **اكتشاف السلوك** لتمكين المكون أو تعطيله.

4. احفظ تغييراتك.

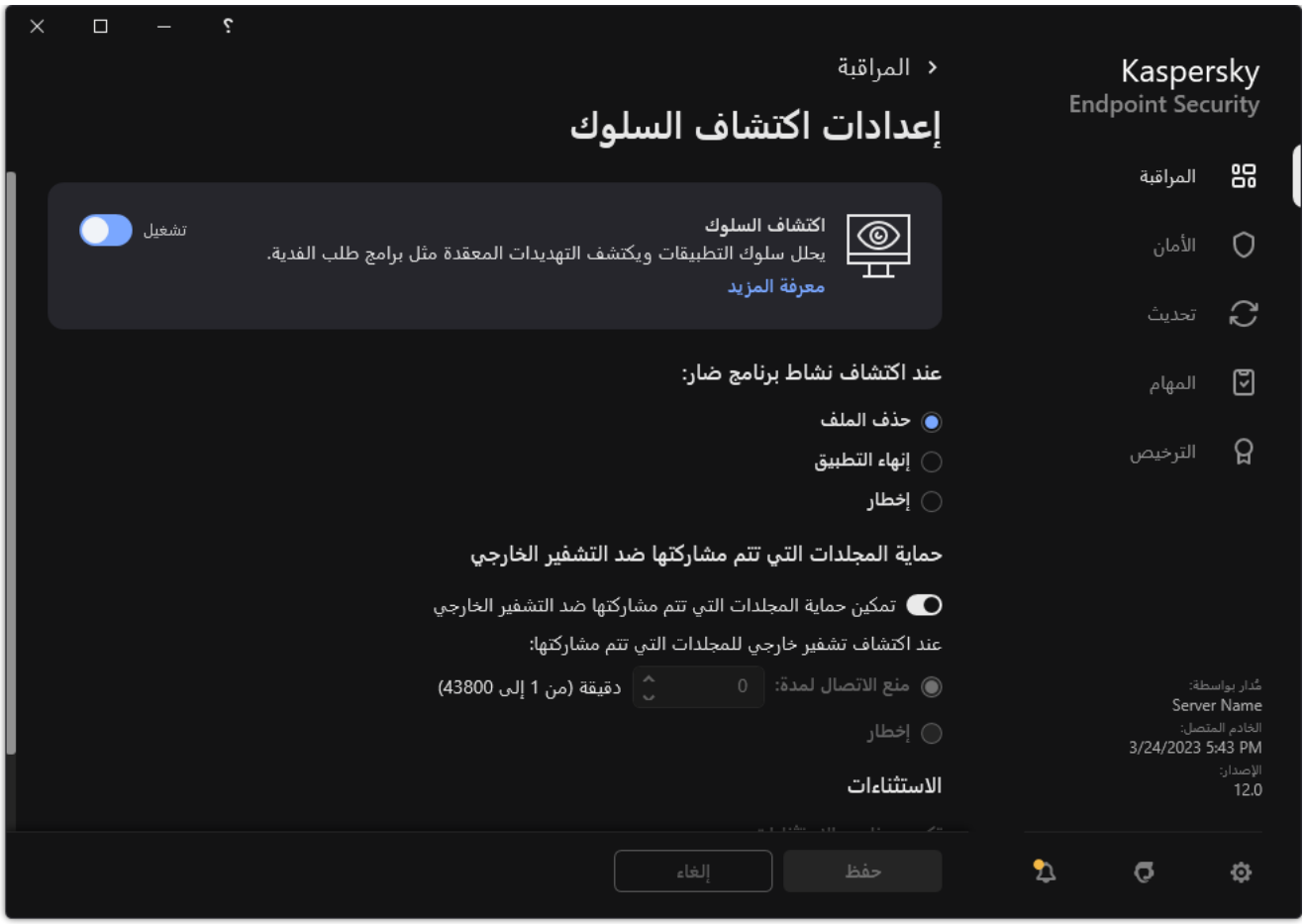
نتيجة لذلك، في حالة تمكين اكتشاف السلوك، سيستخدم Kaspersky Endpoint Security توقيعات بث السلوك لتحليل نشاط التطبيقات في نظام التشغيل.

تحديد الإجراء الذي سيتم اتخاذه عند اكتشاف نشاط برمجيات ضارة

لاختيار ما يجب فعله إذا كان تطبيق ما مشتركًا في نشاط ضار، نفّذ الخطوات التالية:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **اكتشاف السلوك**.



إعدادات اكتشاف السلوك

3. حدد الإجراء المناسب من القسم **عند اكتشاف نشاط برنامج ضار**:

- **حذف الملف**. في حالة تحديد هذا العنصر، عند اكتشاف نشاط ضار، يحذف Kaspersky Endpoint Security الملف التنفيذي للتطبيق الضار وينشئ نسخة احتياطية من الملف في النسخ الاحتياطي.
- **إنهاء التطبيق**. في حالة تحديد هذا العنصر، يقوم برنامج Kaspersky Endpoint Security بإنهاء هذا التطبيق في حالة اكتشاف وجود أي نشاط خبيث.
- **إخطار**. في حالة تحديد هذا العنصر واكتشاف نشاط برمجيات ضارة لأحد التطبيقات، يضيف Kaspersky Endpoint Security معلومات حول نشاط البرمجيات الضارة للتطبيق إلى قائمة التهديدات النشطة.

4. احفظ تغييراتك.

حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي

يراقب المكون العمليات التي يتم تنفيذها فقط مع هذه الملفات المخزنة على أجهزة تخزين كبيرة السعة بنظام ملف NTFS وغير المشفرة بنظام EFS.

توفر حماية المجلدات المشتركة ضد التشفير الخارجي تحليل الأنشطة في المجلدات المشتركة. إذا توافق هذا النشاط مع توقيع تدفق السلوك المشابه للتشفير الخارجي، فإن Kaspersky Endpoint Security يقوم باتخاذ الإجراء المحدد.

بشكل افتراضي، يتم تعطيل حماية المجلدات المشتركة ضد التشفير الخارجي.

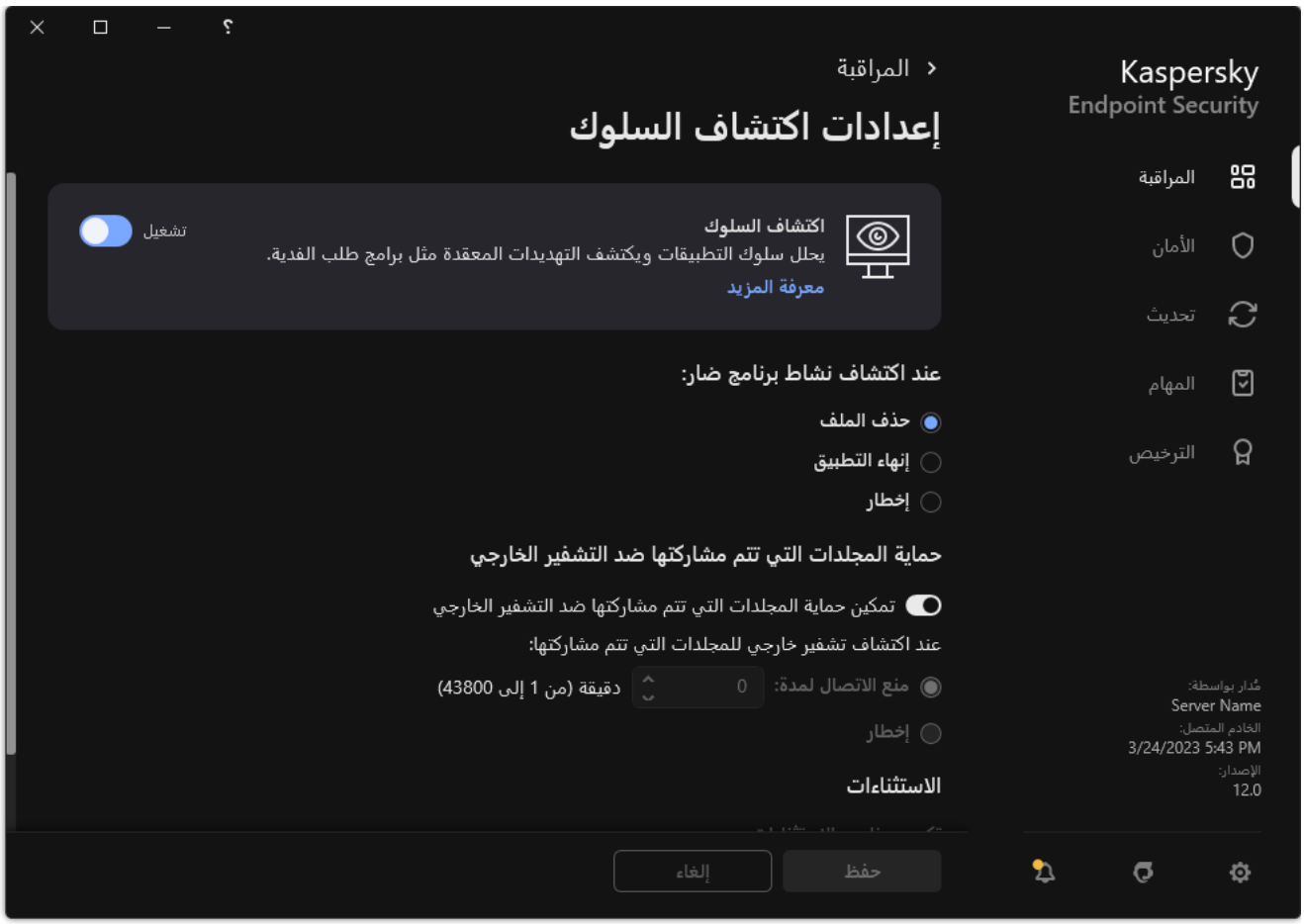
بعد تثبيت Kaspersky Endpoint Security، سوف تكون حماية المجلدات المشتركة ضد التشفير الخارجي محدودة حتى تتم إعادة تشغيل الكمبيوتر.

تمكين وتعطيل حماية المجلدات المشتركة ضد التشفير الخارجي

بعد تثبيت Kaspersky Endpoint Security، سوف تكون حماية المجلدات المشتركة ضد التشفير الخارجي محدودة حتى تتم إعادة تشغيل الكمبيوتر.

لتمكين أو تعطيل حماية المجلدات المشتركة ضد التشفير الخارجي:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **اكتشاف السلوك**.



إعدادات اكتشاف السلوك

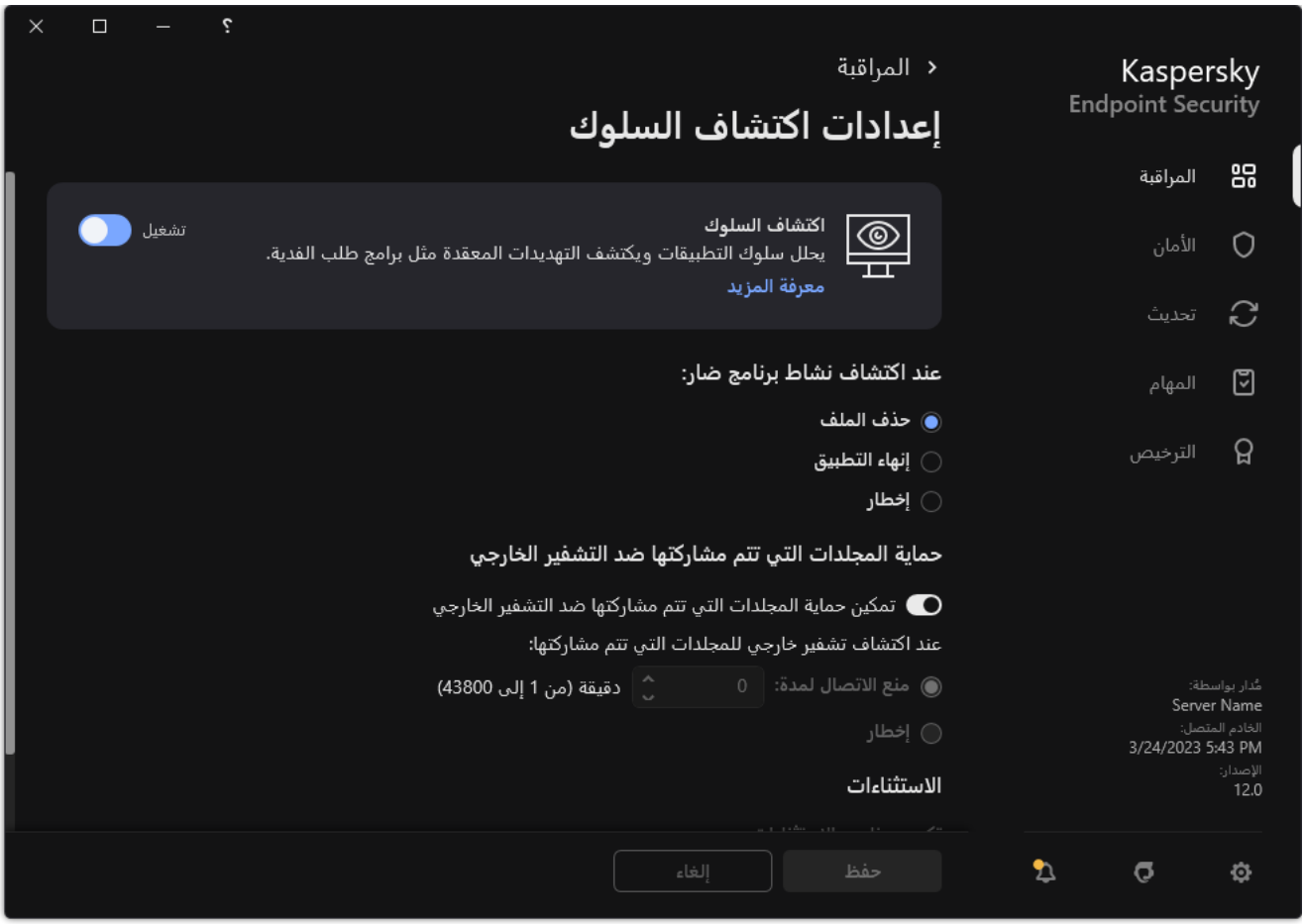
3. استخدم مفتاح التبديل **تمكين حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي** لتمكين الكشف عن النشاط المعتاد للتشفير الخارجي أو تعطيله.
4. احفظ تغييراتك.

تحديد الإجراء الذي يمكن اتخاذه عند اكتشاف تشفير خارجي للمجلدات التي تتم مشاركتها

لتحديد الإجراء الذي يمكن اتخاذه عند اكتشاف تشفير خارجي للمجلدات التي تتم مشاركتها:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **اكتشاف السلوك**.



إعدادات اكتشاف السلوك

3. حدد الإجراء المناسب من القسم **حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي**:

- **منع الاتصال لمدة N دقيقة (من 1 إلى 43800)**. في حالة تحديد هذا الخيار واكتشف برنامج Kaspersky Endpoint Security محاولة لتعديل الملفات الموجودة في المجلدات المشتركة، فإنه ينفذ الإجراءات التالية:
  - يحظر الوصول إلى تعديل الملف للجلسة التي بدأت النشاط الضار (سيكون الملف للقراءة فقط).
  - يقوم بإنشاء النسخ الاحتياطي من الملفات التي يتم تعديلها.
  - يُضيف إدخال إلى تقارير واجهة التطبيق المحلية.
  - يُرسل معلومات حول النشاط الضار الذي تم اكتشافه إلى Kaspersky Security Center.

  وأيضًا، في حال تمكين مكون محرك المعالجة، يتم استرداد الملفات المعدّلة من النسخ الاحتياطية.
- **إخطار**. في حالة تحديد هذا الخيار واكتشف برنامج Kaspersky Endpoint Security محاولة لتعديل الملفات الموجودة في المجلدات المشتركة، فإنه ينفذ الإجراءات التالية:
  - يُضيف إدخال إلى تقارير واجهة التطبيق المحلية.
  - يضيف إدخالاً إلى قائمة التهديدات النشطة.
  - يُرسل معلومات حول النشاط الضار الذي تم اكتشافه إلى Kaspersky Security Center.

4. احفظ تغييراتك.

إنشاء استثناء لحماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي

من الممكن أن يؤدي استبعاد مجلد إلى تقليل مقدار الإيجابيات الخاطئة إذا كانت مؤسستك تستخدم تشفير البيانات عند تبادل الملفات باستخدام المجلدات المشتركة. على سبيل المثال، من الممكن أن يثير اكتشاف السلوك إيجابيات خاطئة عندما يعمل المستخدم مع ملفات بامتداد ENC في مجلد مشترك. ويطابق هذا النشاط نمطًا سلوكيًا نموذجيًا للتشفير الخارجي. وإذا قمت بتشفير الملفات في مجلد مشترك لحماية البيانات، فأضف هذا المجلد إلى الاستثناءات.

كيفية إنشاء استثناء لحماية المجلدات المشتركة باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات**.

5. في القسم **استثناءات من الفحص والتطبيقات الموثوقة**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، حدد القسم **استثناءات الفحص**.

يفتح هذا نافذة تحتوي على قائمة استثناءات.

7. حدد خانة الاختيار **دمج القيم عند التوريث** إذا كنت ترغب في إنشاء قائمة موحدة بالاستثناءات لجميع أجهزة الكمبيوتر في الشركة. سيتم دمج قوائم الاستثناءات في السياسات الأصلية والفرعية. سيتم دمج القوائم بشرط أن تكون قيم الدمج مفعلة عند التوريث. ويتم عرض الاستثناءات من السياسة الأصلية في السياسات الفرعية في عرض قراءة فقط. لا يمكن تغيير الاستثناءات أو حذفها من السياسة الرئيسية.

8. حدد خانة الاختيار **السماح باستخدام الاستثناءات المحلية** إذا كنت تريد تمكين المستخدم لإنشاء قائمة استثناءات محلية. وبهذه الطريقة، يستطيع المستخدم إنشاء قائمة الاستثناءات المحلية الخاصة به بالإضافة إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر.

في حالة تحديد خانة الاختيار، يستطيع المستخدم الوصول فقط إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة.

9. انقر على **إضافة**.

10. في القسم **الخصائص**، حدد خانة الاختيار **الملف أو المجلد**.

11. انقر فوق الرابط **تحديد ملف أو مجلد** في القسم **وصف الاستثناء من الفحص (انقر فوق العناصر التي تحتها خط لتحريرها)** لفتح النافذة **اسم الملف أو المجلد**.

12. انقر فوق **استعراض** وحدد المجلد المشترك.

يمكنك أيضًا إدخال المسار يدويًا. يدعم Kaspersky Endpoint Security حرفي * و ? عند إدخال قناع:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

يمكنك استخدام الأقنعة في بداية مسار الملف أو في منتصفه أو في نهايته. على سبيل المثال، إذا كنت تريد إضافة مجلد لجميع المستخدمين إلى الاستثناءات، أدخل القناع `C:\Users\*\Folder\`.

13. إذا لزم الأمر، في الحقل **تعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

14. انقر فوق الرابط **any** في القسم **وصف الاستثناء من الفحص (انقر فوق العناصر التي تحتها خط لتحريرها)** لتفعيل الرابط **select components**.

15. انقر فوق الرابط **تحديد المكونات** لفتح النافذة **مكونات الحماية**.

16. حدد خانة الاختيار الموجودة بجوار المكون **اكتشاف السلوك**.

17. احفظ تغييراتك.

كيفية إنشاء استثناء لحماية المجلدات المشتركة باستخدام Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings ← Exclusions and types of detected objects**.

5. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Scan exclusions**.

6. حدد خانة الاختيار **Merge values when inheriting** إذا كنت ترغب في إنشاء قائمة موحدة بالاستثناءات لجميع أجهزة الكمبيوتر في الشركة. سيتم دمج قوائم الاستثناءات في السياسات الأصلية والفرعية. سيتم دمج القوائم بشرط أن تكون قيم الدمج مفعلة عند التوريث. ويتم عرض الاستثناءات من السياسة الأصلية في السياسات الفرعية في عرض قراءة فقط. لا يمكن تغيير الاستثناءات أو حذفها من السياسة الرئيسية.

7. حدد خانة الاختيار **Allow use of local exclusions** إذا كنت تريد تمكين المستخدم لإنشاء قائمة استثناءات محلية. وبهذه الطريقة، يستطيع المستخدم إنشاء قائمة الاستثناءات المحلية الخاصة به بالإضافة إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر.

في حالة تحديد خانة الاختيار، يستطيع المستخدم الوصول فقط إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة.

8. انقر على **Add**.

9. حدد كيف تريد إضافة الاستثناء **File or folder**.

10. انقر فوق **استعراض** وحدد المجلد المشترك.

يمكنك أيضًا إدخال المسار يدويًا. يدعم Kaspersky Endpoint Security حرفي * و ? عند إدخال قناع:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

يمكنك استخدام الأقنعة في بداية مسار الملف أو في منتصفه أو في نهايته. على سبيل المثال، إذا كنت تريد إضافة مجلد لجميع المستخدمين إلى الاستثناءات، أدخل القناع `C:\Users\*\Folder\`.

11. في القسم **مكونات الحماية**، حدد المكون **اكتشاف السلوك**.

12. إذا لزم الأمر، في الحقل **التعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

13. حدد الحالة **فعال** للاستثناء.

يمكنك استخدام مفتاح التبديل إيقاف استثناء في أي وقت.

14. احفظ تغييراتك.

كيفية إنشاء استثناء لحماية المجلدات المشتركة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة ← الاستثناءات وأنواع الكائنات المكتشفة**.

3. في القسم **الاستثناءات**، انقر على الرابط **إدارة الاستثناءات**.

4. انقر على **إضافة**.

5. انقر فوق **استعراض** وحدد المجلد المشترك.

يمكنك أيضًا إدخال المسار يدويًا. يدعم Kaspersky Endpoint Security حرفي * و ? عند إدخال قناع:

- حرف * (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي \ و / (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان * محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي \ و / (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف ? (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي \ و / (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

يمكنك استخدام الأقنعة في بداية مسار الملف أو في منتصفه أو في نهايته. على سبيل المثال، إذا كنت تريد إضافة مجلد لجميع المستخدمين إلى الاستثناءات، أدخل القناع `C:\Users\*\Folder\`.

6. في القسم **مكونات الحماية**، حدد المكون **اكتشاف السلوك**.

7. إذا لزم الأمر، في الحقل **التعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

8. حدد الحالة **فعال** للاستثناء.

يمكنك استخدام مفتاح التبديل إيقاف استثناء في أي وقت.

9. احفظ تغييراتك.

تكوين عناوين الاستثناءات من حماية المجلدات المشتركة ضد التشفير الخارجي

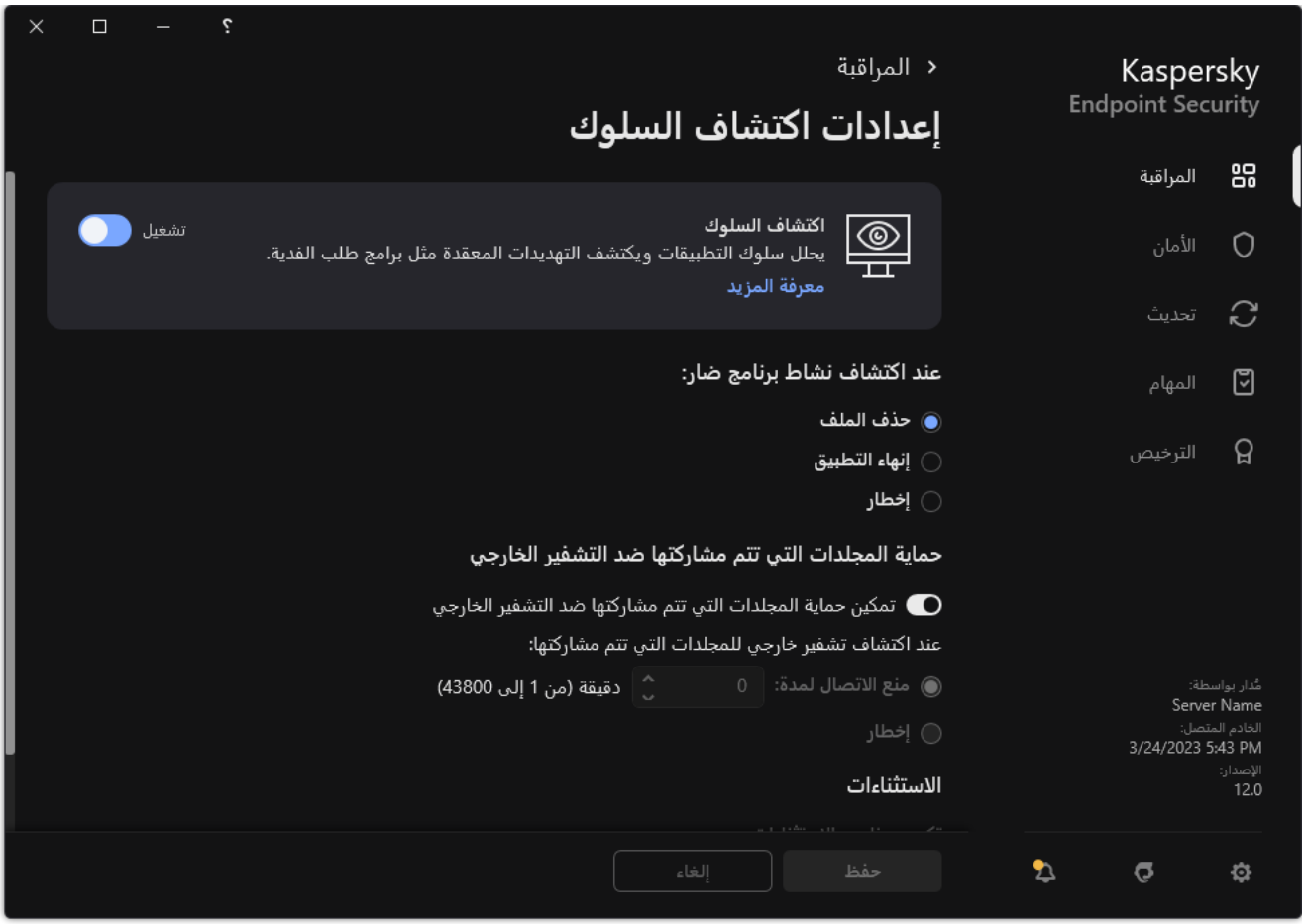
يجب تمكين خدمة تسجيل الدخول للتدقيق لتمكين استثناءات العناوين من حماية للمجلدات المشتركة ضد التشفير الخارجي. وبشكل افتراضي، يتم تعطيل خدمة تسجيل الدخول للتدقيق (للحصول على معلومات مفصلة حول تمكين خدمة تسجيل الدخول للتدقيق، يرجى زيارة موقع ويب Microsoft).

لا تعمل وظيفة استثناء العناوين من حماية المجلد المشترك على كمبيوتر بعيد في حالة تشغيل الكمبيوتر البعيد قبل بدء تشغيل Kaspersky Endpoint Security. يمكنك إعادة تشغيل هذا الكمبيوتر البعيد بعد بدء تشغيل Kaspersky Endpoint Security لضمان عمل وظيفة استثناء العناوين من حماية المجلد المشترك على هذا الكمبيوتر البعيد.

لاستثناء أجهزة الكمبيوتر البعيدة التي تنفذ التشفير الخارجي للمجلدات المشتركة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **اكتشاف السلوك**.



إعدادات اكتشاف السلوك

3. في القسم **الاستثناءات**، انقر على الرابط **تكوين عناوين الاستثناءات**.

4. إذا كنت تريد إضافة عنوان IP أو اسم كمبيوتر إلى قائمة الاستثناءات، انقر فوق الزر **إضافة**.

5. أدخل عنوان IP أو اسم الكمبيوتر الذي يجب عدم التعامل مع محاولات التشفير الخارجي منه.

6. احفظ تغييراتك.

تصدير واستيراد قائمة استثناءات من حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي

يمكنك تصدير قائمة الاستثناءات إلى ملف XML. وبعد ذلك يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من العناوين من النوع نفسه. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة الاستثناءات أو لترحيل القائمة إلى خادم مختلف.

كيفية تصدير واستيراد قائمة الاستثناءات في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **اكتشاف السلوك**.

5. في القسم **حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي**، انقر على الزر **الاستثناءات**.

6. لتصدير قائمة القواعد:

   a. حدد الاستثناءات التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.
   إذا لم تحدد أي استثناء، فسيقوم Kaspersky Endpoint Security بتصدير كل الاستثناءات.

   b. انقر على رابط **تصدير**.

   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   d. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

7. لاستيراد قائمة الاستثناءات:

   a. انقر على **استيراد**.

   b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

   c. افتح الملف.
   إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة الاستثناءات في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Behavior Detection**.

5. لتصدير قائمة الاستثناءات في القسم **Exclusions**:

a. حدد الاستثناءات التي تريد تصديرها.

b. انقر على **Export**.

c. أكد أنك تريد تصدير الاستثناءات المحددة فقط، أو تصدير قائمة الاستثناءات بأكملها.

d. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

e. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

6. لاستيراد قائمة الاستثناءات في القسم **Exclusions**:

a. انقر على **Import**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

c. افتح الملف.
إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

منع اختراق المضيف

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل. لا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم.

يمنع مكون منع اختراق المضيف التطبيقات من تنفيذ الإجراءات التي قد تكون خطرة على نظام التشغيل ويضمن التحكم في الوصول إلى موارد نظام التشغيل والبيانات الشخصية. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network.

يتحكم المكون في تشغيل التطبيقات باستخدام حقوق التطبيقات . حقوق التطبيقات تتضمن معلمات الوصول التالية:

- الوصول إلى موارد نظام التشغيل (على سبيل المثال، خيارات بدء التشغيل التلقائي ومفاتيح التسجيل)
- الوصول إلى البيانات الشخصية (مثل الملفات والتطبيقات)

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة جدار الحماية باستخدام قواعد الشبكة.

أثناء بدء التشغيل الأول للتطبيق، يقوم مكون منع اختراق المضيف بتنفيذ الإجراءات التالية:

1. يتحقق من أمان التطبيق باستخدام قواعد بيانات مكافحة الفيروسات التي تم تنزيلها.

2. سيتحقق من درجة أمان التطبيق في شبكة Kaspersky Security Network.

ننصحك بالمشاركة في شبكة Kaspersky Security Network لمساعدة مكون منع اختراق المضيف على العمل على نحو أكثر فعالية.

3. يضع التطبيق في إحدى مجموعات الثقة: موثوق، مقيد بشكل منخفض، مقيد بشكل عالٍ، غير موثوق.

تحدد مجموعة ثقة الحقوق التي يشير إليها Kaspersky Endpoint Security عند التحكم في نشاط التطبيق. يضع Kaspersky Endpoint Security تطبيقًا في مجموعة ثقة بناءً على مستوى الخطر الذي قد يشكله هذا التطبيق على الكمبيوتر.

يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة لمكونات جدار الحماية ومنع اختراق المضيف. لا يمكنك تغيير مجموعة الثقة فقط لجدار الحماية أو منع اختراق المضيف.

إذا رفضت المشاركة في KSN أو لم تكن هناك شبكة، يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة اعتمادًا على إعدادات مكون منع اختراق المضيف. بعد استلام سمعة التطبيق من KSN، يمكن تغيير مجموعة الثقة تلقائيًا.

4. يحظر إجراءات التطبيق بناءً على مجموعة الثقة. على سبيل المثال: يتم رفض وصول التطبيقات من مجموعة الثقة مقيد بشكل عالٍ إلى وحدات نظام التشغيل.

في المرة التالية التي يعمل فيها التطبيق، يتحقق Kaspersky Endpoint Security من سلامة التطبيق. في حالة عدم تغير التطبيق، يستخدم المكون حقوق التطبيق الحالية عليه. في حالة تعديل التطبيق، فإن Kaspersky Endpoint Security يحلل التطبيق كما لو كان يجرى تشغيله لأول مرة.

تمكين وتعطيل منع اختراق المضيف

بشكل افتراضي، يتم تكوين مكون منع اختراق المضيف وتشغيله في الوضع الموصى به من خبراء Kaspersky.

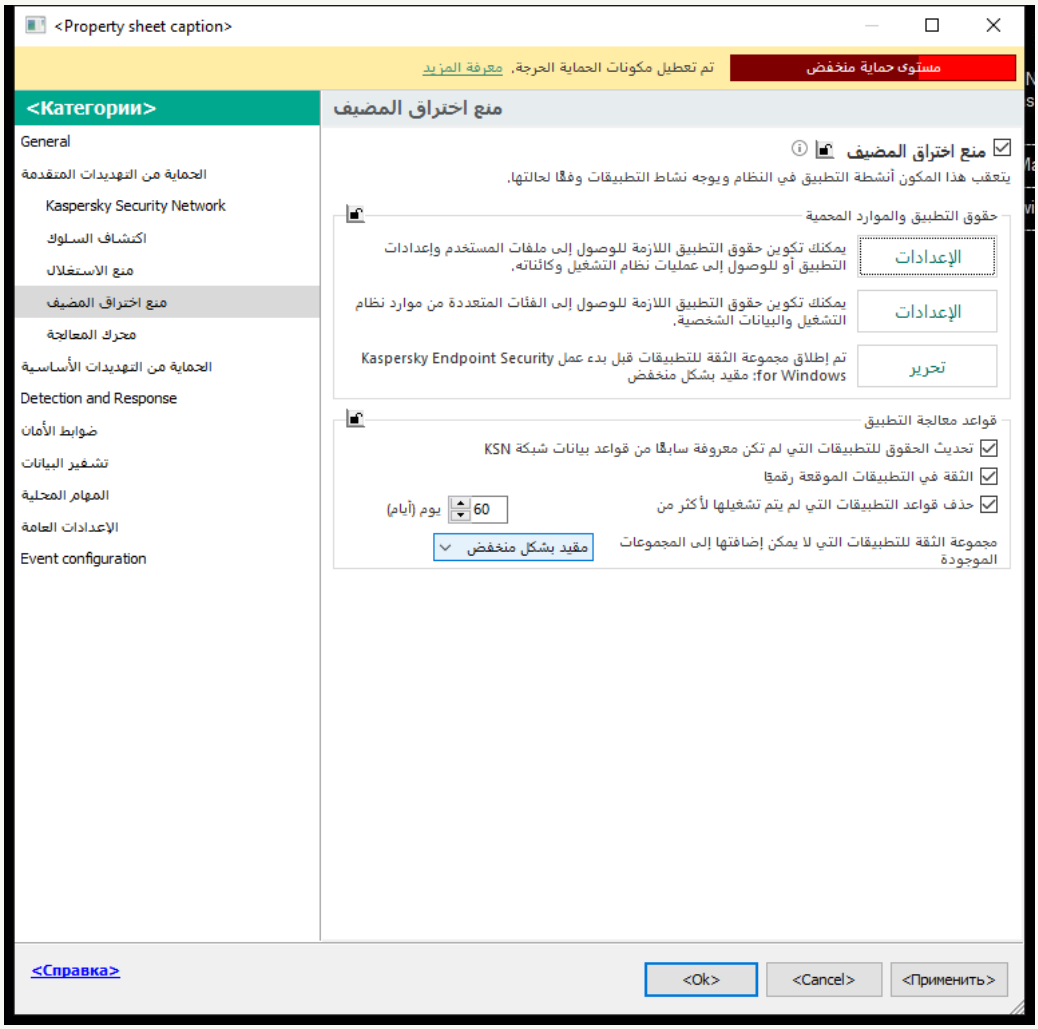
كيفية تمكين أو تعطيل مكون منع اختراق المضيف في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **منع اختراق المضيف**.



إعدادات منع الاختراق

5. استخدم خانة الاختيار **منع اختراق المضيف** لتمكين المكون أو تعطيله.

6. احفظ تغييراتك.

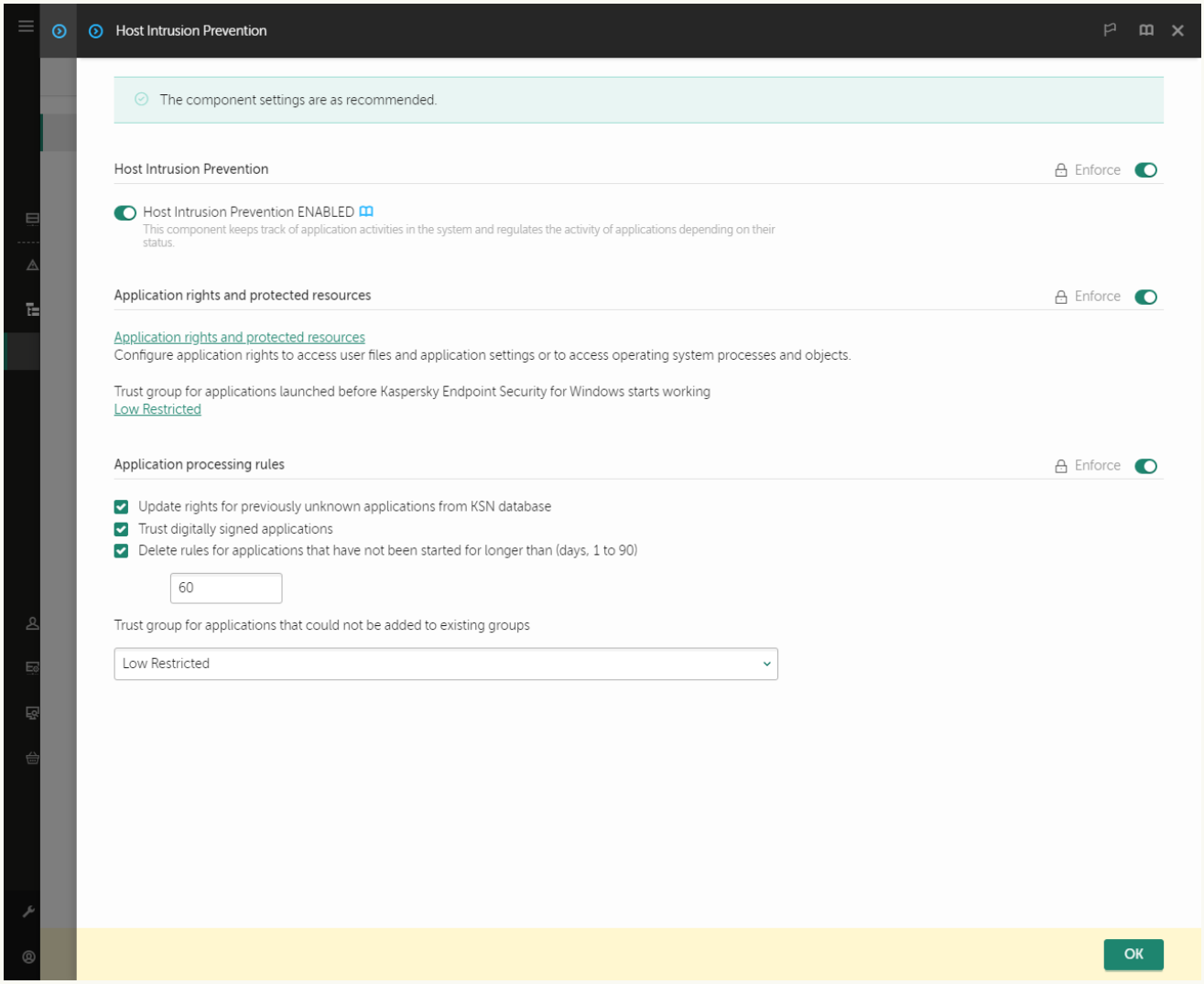
[كيفية تمكين أو تعطيل مكون منع اختراق المضيف في Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. استخدم مفتاح تبديل **منع اختراق المضيف** لتمكين المكون أو تعطيله.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون منع اختراق المضيف في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.

3. استخدم مفتاح تبديل **منع اختراق المضيف** لتمكين المكون أو تعطيله.

4. احفظ تغييراتك.

في حالة تمكين مكون منع اختراق المضيف، سيضع Kaspersky Endpoint Security تطبيقًا في مجموعة ثقة بناءً على مستوى الخطر الذي قد يشكله هذا التطبيق على الكمبيوتر. سوف يحظر Kaspersky Endpoint Security بعد ذلك إجراءات التطبيق بناءً على مجموعة الثقة.

إدارة المجموعات الموثوقة للتطبيق

عند بدء أي تطبيق لأول مرة، يفحص مكون منع اختراق المضيف أمان التطبيق ويضع التطبيق في مجموعات الثقة.

في المرحلة الأولى من فحص التطبيق، يبحث Kaspersky Endpoint Security عن إدخال متوافق في قاعدة البيانات الداخلية للتطبيقات المعروفة وفي نفس الوقت يرسل طلبًا إلى قاعدة بيانات Kaspersky Security Network (في حالة توفر الاتصال بالإنترنت). بناءً على نتيجة البحث في قاعدة البيانات الداخلية وقاعدة بيانات Kaspersky Security Network، يتم وضع التطبيق داخل مجموعة ثقة. في كل مرة يتم بدء تشغيل التطبيق فيها لاحقًا، يُرسل Kaspersky Endpoint Security استعلامًا جديدًا إلى قاعدة بيانات KSN ويضع التطبيق في مجموعة ثقة مختلفة إذا تغيرت سمعة التطبيق في قاعدة بيانات KSN.

يمكنك تحديد مجموعة ثقة يجب أن يعين Kaspersky Endpoint Security لها كل التطبيقات غير المعروفة بشكل تلقائي. يتم نقل التطبيقات التي تم بدؤها قبل Kaspersky Endpoint Security تلقائيًا إلى مجموعة الثقة المحددة في إعدادات مكون منع اختراق المضيف.

بالنسبة للتطبيقات التي بدأ تشغيلها قبل Kaspersky Endpoint Security، يتم التحكم في نشاط الشبكة فقط. يتم التحكم وفقًا لقواعد الشبكة المحددة في إعدادات جدار الحماية.

تغيير مجموعة الثقة لتطبيق

عند بدء أي تطبيق لأول مرة، يفحص مكون منع اختراق المضيف أمان التطبيق ويضع التطبيق في مجموعات الثقة.

لا يوصي المتخصصون في Kaspersky بنقل التطبيقات من المجموعة الموثوقة التلقائية إلى مجموعة موثوقة أخرى. بدلاً من ذلك تستطيعتعديل الحقوق للطلبات الفردية إذا لزم الأمر.

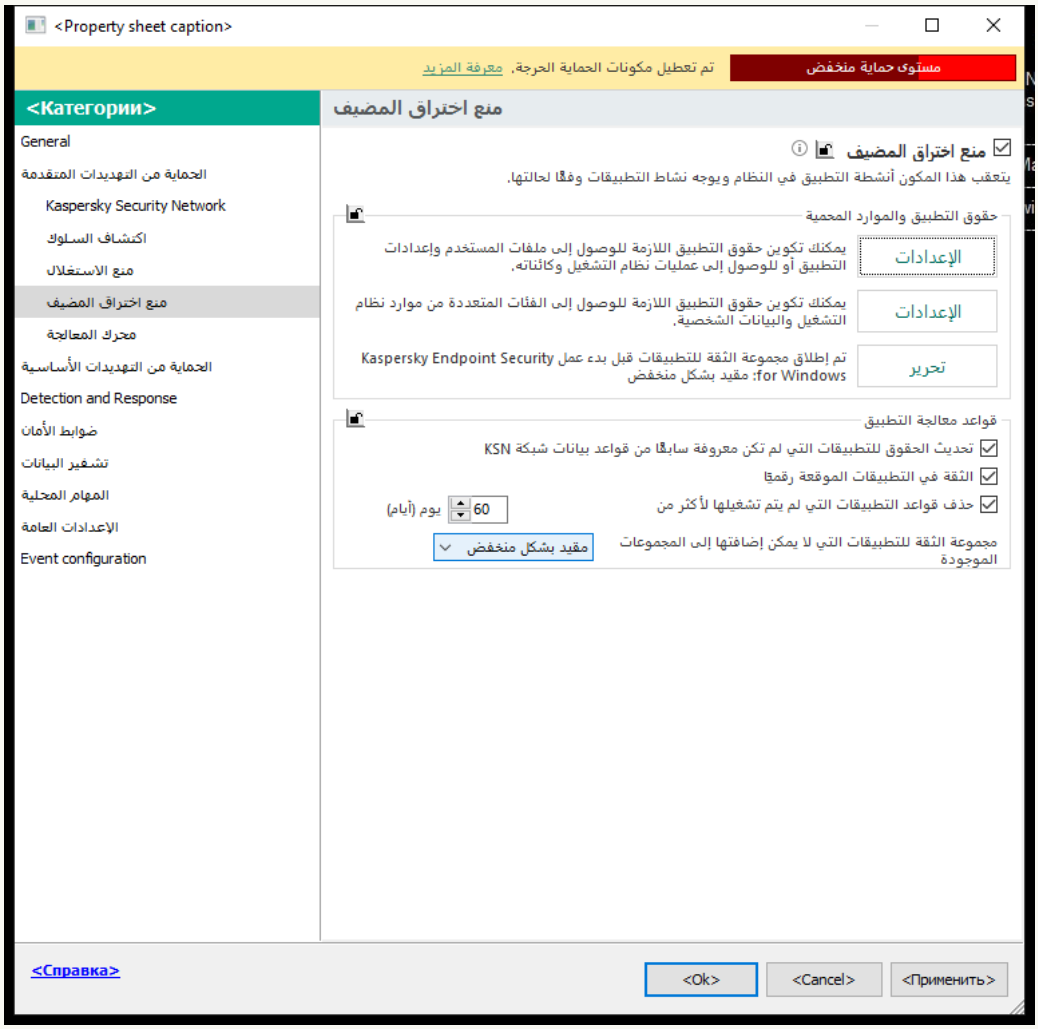
كيفية تغيير مجموعة الثقة لتطبيق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

5. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **حقوق التطبيق**.

7. انقر على **إضافة**.

8. في النافذة التي تفتح، أدخل المعايير للبحث عن التطبيق الذي تريد تغيير مجموعة الثقة الخاصة به.

يمكنك إدخال اسم التطبيق أو اسم البائع. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

9. انقر على **تحديث**.

سيبحث Kaspersky Endpoint Security عن التطبيق في القائمة الموحدة للتطبيقات المثبتة على أجهزة الكمبيوتر المدارة. سيعرض Kaspersky Endpoint Security قائمة بالتطبيقات التي تلبي معايير البحث الخاصة بك.

10. حدد التطبيق المطلوب.

11. في القائمة المنسدلة **إضافة التطبيق المحدد إلى مجموعة الثقة**، حدد مجموعة الثقة اللازمة للتطبيق.

12. احفظ تغييراتك.

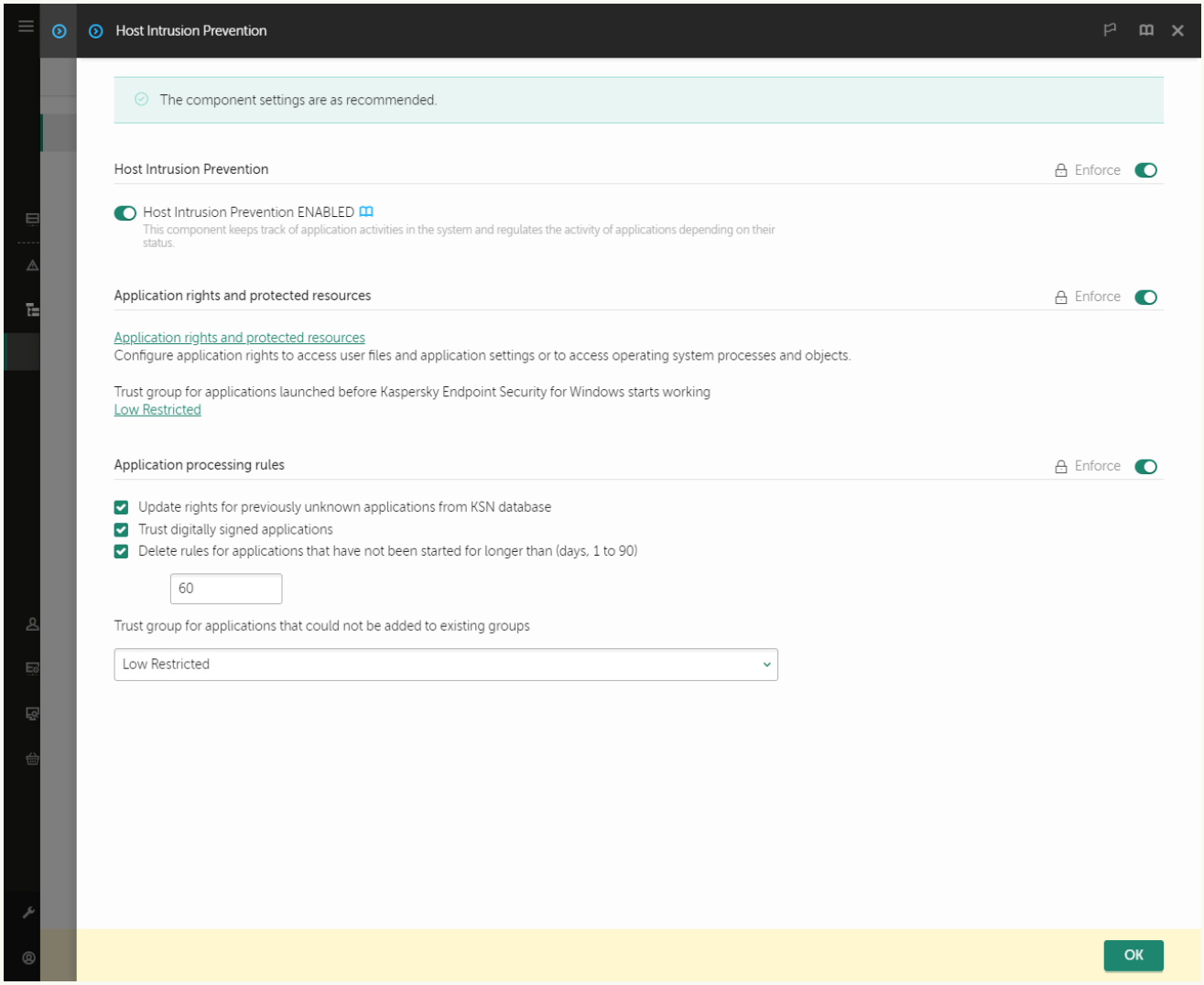
كيفية تغيير مجموعة الثقة لتطبيق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. في القسم **Application rights and protected resources**، انقر على الرابط **Application rights and protected resources**.
يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **Application rights**.
سترى قائمة تتضمن مجموعات الثقة على الجانب الأيمن من النافذة وخصائصها على الجانب الأيسر.

7. انقر على **Add**.
يؤدي هذا إلى تشغيل المعالج لإضافة تطبيق إلى مجموعة ثقة.

8. حدد مجموعة الثقة ذات الصلة للتطبيق.

9. حدد نوع **Application**. انتقل إلى الخطوة التالية.

إذا كنت تريد تغيير مجموعة الثقة لتطبيقات متعددة، فحدد نوع **Group** وحدد اسمًا لمجموعة التطبيقات.

10. في قائمة التطبيقات المفتوحة، حدد التطبيقات التي تريد تغيير مجموعة الثقة الخاصة بها.

استخدم عامل تصفية. يمكنك إدخال اسم التطبيق أو اسم البائع. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

11. أغلق المعالج.

ستتم إضافة التطبيق إلى مجموعة الثقة.

12. احفظ تغييراتك.

كيفية تغيير مجموعة الثقة لتطبيق في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **منع اختراق المضيف**.
3. انقر على **إدارة التطبيقات**.

يفتح هذا قائمة التطبيقات المثبتة.

4. حدد التطبيق المطلوب.
5. في قائمة السياق الخاصة بالتطبيق، انقر فوق **القيود** ← **<مجموعة الثقة>**.
6. احفظ تغييراتك.

نتيجة لذلك، سيتم وضع التطبيق في مجموعة الثقة الأخرى. سوف يحظر Kaspersky Endpoint Security بعد ذلك إجراءات التطبيق بناءً على مجموعة الثقة. سيتم تعيين حالة (محدد بواسطة المستخدم) للتطبيق. في حالة تغيير سمعة التطبيق في Kaspersky Security Network، سيترك مكون منع اختراق المضيف مجموعة الثقة الخاصة بهذا التطبيق دون تغيير.

تكوين حقوق مجموعة الثقة

يتم إنشاء حقوق التطبيق المثلى لمجموعات ثقة مختلفة بشكل افتراضي. وترث إعدادات حقوق مجموعات التطبيق الموجودة في مجموعة الثقة قيمًا من إعدادات حقوق هذه المجموعة.

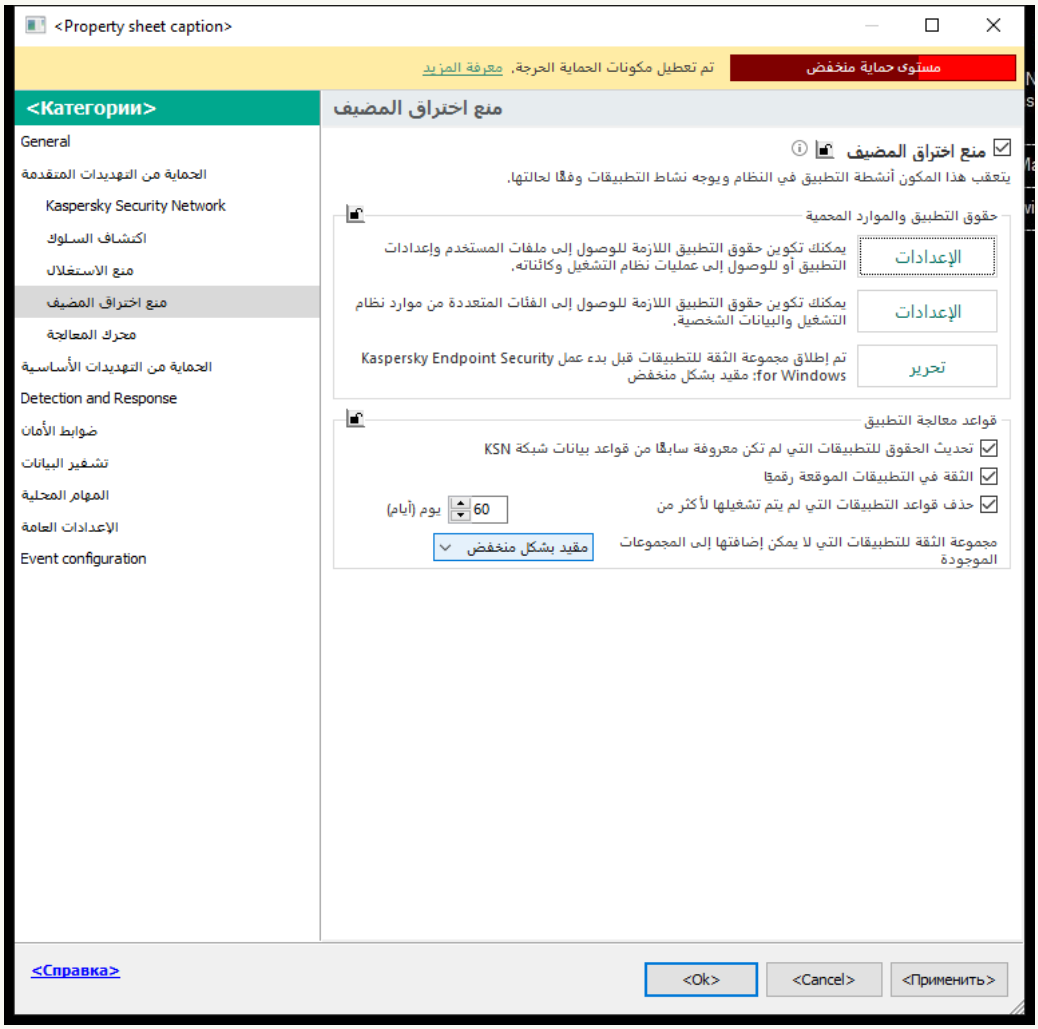
كيفية تغيير حقوق مجموعة الثقة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

5. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **حقوق التطبيق**.

7. حدد المجموعة الموثوقة اللازمة.

8. في قائمة السياق الخاصة بمجموعة الثقة، حدد **حقوق المجموعات**.

يفتح هذا خصائص مجموعة الثقة.

9. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد علامة التبويب **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد علامة التبويب **الحقوق**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة جدار الحماية باستخدام قواعد الشبكة.

10. للمورد ذي الصلة، في عمود الإجراء المتوافق، انقر بزر الماوس الأيمن لفتح قائمة السياق وتحديد الخيار اللازم: **توريث** أو **سماح** (✓) أو **منع** (⊘).

11. إذا كنت تريد مراقبة استخدام موارد الكمبيوتر، حدد **أحداث السجل** (✓ / ⊘).

سوف يسجل Kaspersky Endpoint Security معلومات حول تشغيل مكون منع اختراق المضيف. وتحتوي التقارير على معلومات حول العمليات باستخدام موارد الكمبيوتر التي ينفذها التطبيق (مسموح بها أو ممنوعة). وتحتوي التقارير أيضًا على معلومات حول التطبيقات التي تستخدم كل مورد.

12. احفظ تغييراتك.

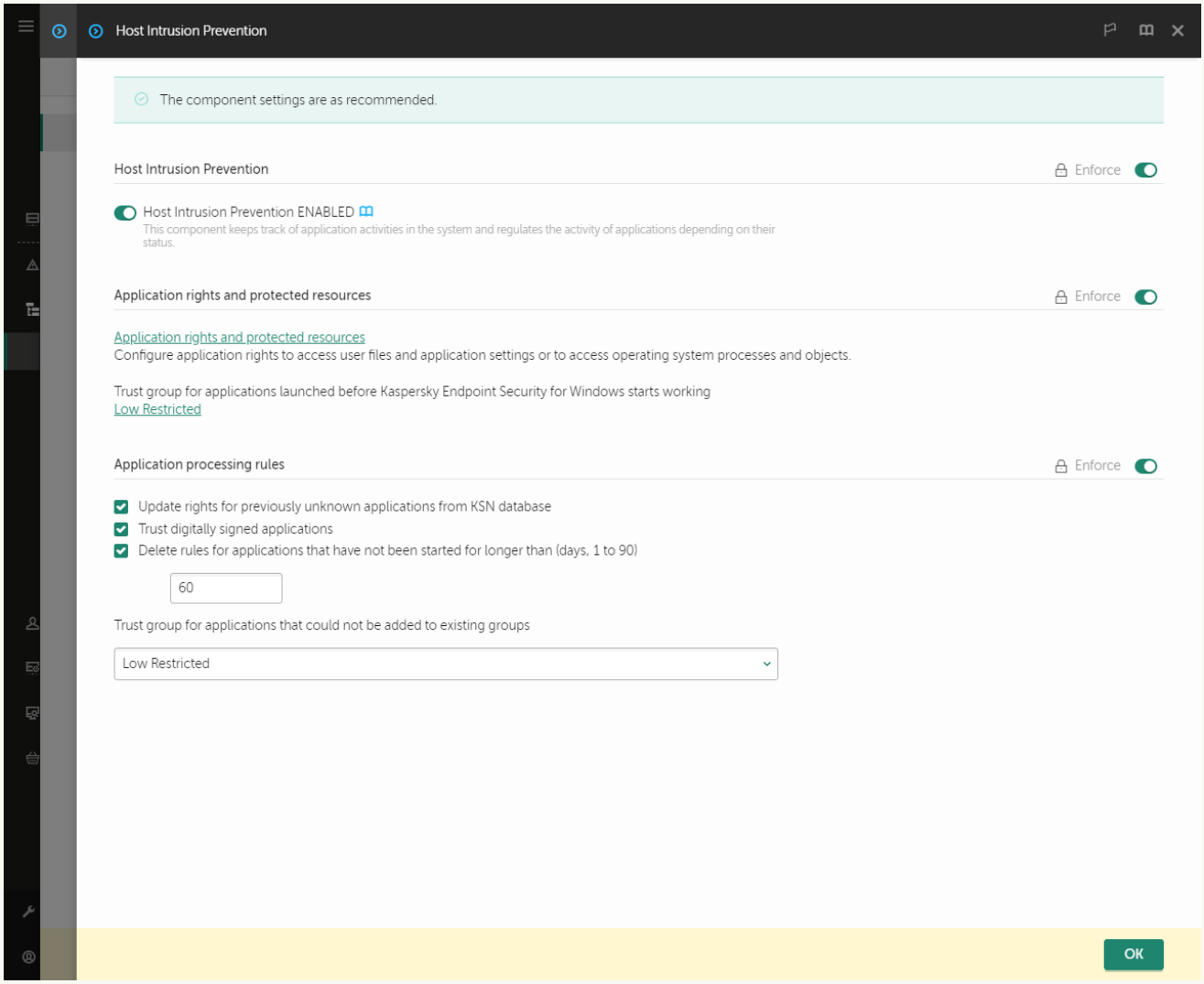
كيفية تغيير حقوق مجموعة الثقة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. في القسم **Application rights and protected resources**، انقر على الرابط **Application rights and protected resources**.
يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **Application rights**.
سترى قائمة تتضمن مجموعات الثقة على الجانب الأيمن من النافذة وخصائصها على الجانب الأيسر.

7. في الجزء الأيمن من النافذة، حدد مجموعة الثقة ذات الصلة.

8. في الجزء الأيسر من النافذة، في القائمة المنسدلة، نفذ أحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد **Files and system registry**.

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد **Rights**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة جدار الحماية باستخدام قواعد الشبكة.

9. للمورد ذي الصلة، في عمود الإجراء المتوافق، حدد الخيار اللازم: **Inherit** أو **Allow** (✓) أو **Block** (✗).

10. إذا كنت تريد مراقبة استخدام موارد الكمبيوتر، حدد **Log events** (✓ / ✗).

سوف يسجل Kaspersky Endpoint Security معلومات حول تشغيل مكون منع اختراق المضيف. وتحتوي التقارير على معلومات حول العمليات باستخدام موارد الكمبيوتر التي ينفذها التطبيق (مسموح بها أو ممنوعة). وتحتوي التقارير أيضًا على معلومات حول التطبيقات التي تستخدم كل مورد.

11. احفظ تغييراتك.

كيفية تغيير حقوق مجموعة الثقة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **منع اختراق المضيف**.

3. انقر على **إدارة التطبيقات**.

يفتح هذا قائمة التطبيقات المثبتة.

4. حدد المجموعة الموثوقة اللازمة.

5. في قائمة السياق الخاصة بمجموعة الثقة، حدد **تفاصيل وقواعد**.

يفتح هذا خصائص مجموعة الثقة.

6. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد علامة التبويب **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد علامة التبويب **الحقوق**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة جدار الحماية باستخدام قواعد الشبكة.

7. للمورد ذي الصلة، في عمود الإجراء المتوافق، انقر بزر الماوس الأيمن لفتح قائمة السياق وتحديد الخيار اللازم: **توريث** أو **سماح** (✓) أو **رفض** (!).

8. إذا كنت تريد مراقبة استخدام موارد الكمبيوتر، فحدد **أحداث السجل** (📊).

سوف يسجل Kaspersky Endpoint Security معلومات حول تشغيل مكون منع اختراق المضيف. وتحتوي التقارير على معلومات حول العمليات باستخدام موارد الكمبيوتر التي ينفذها التطبيق (مسموح بها أو ممنوعة). وتحتوي التقارير أيضًا على معلومات حول التطبيقات التي تستخدم كل مورد.

9. احفظ تغييراتك.

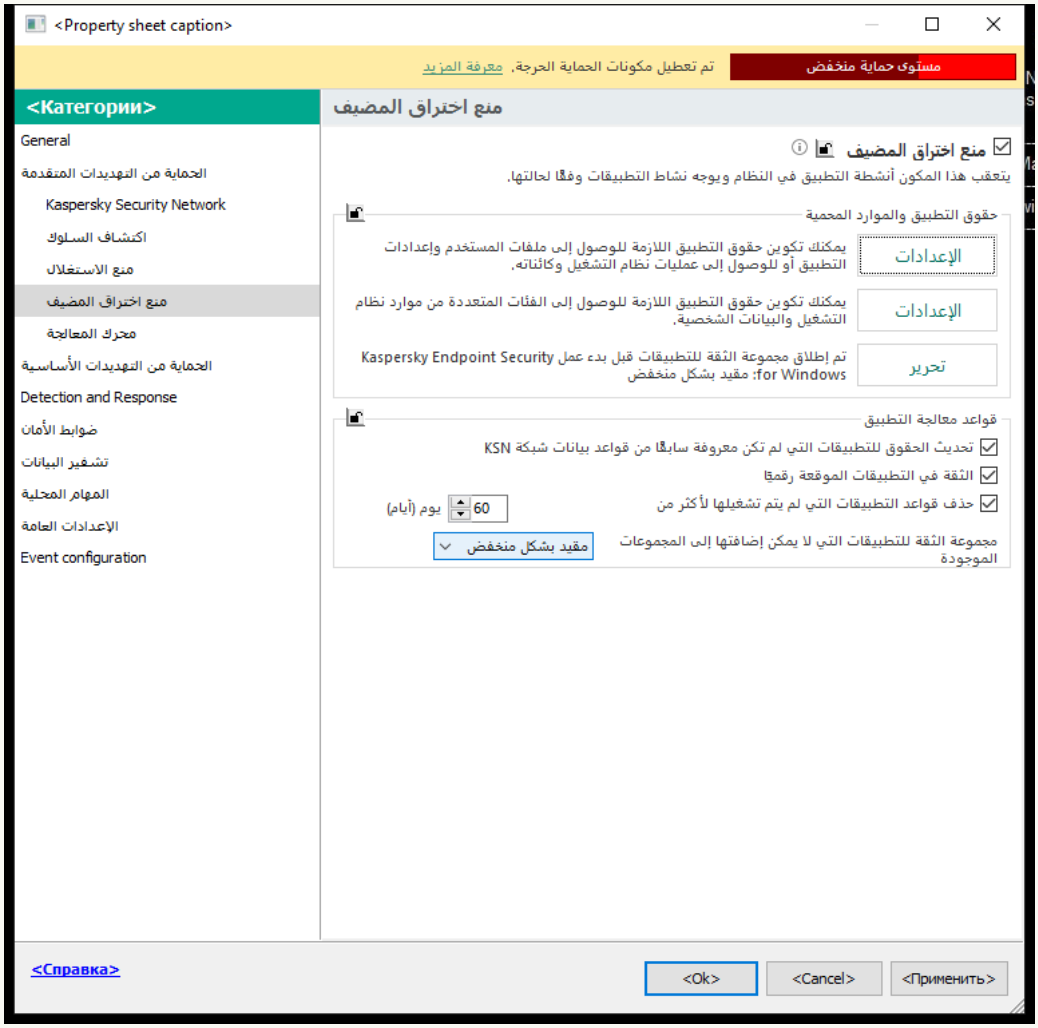
سيتم تغيير حقوق مجموعة الثقة. سوف يحظر Kaspersky Endpoint Security بعد ذلك إجراءات التطبيق بناءً على مجموعة الثقة. سيتم تعيين الحالة (إعدادات مخصصة) إلى مجموعة الثقة.

تحديد مجموعة ثقة للتطبيقات التي تم بدؤها قبل Kaspersky Endpoint Security

بالنسبة للتطبيقات التي بدأ تشغيلها قبل Kaspersky Endpoint Security، يتم التحكم في نشاط الشبكة فقط. يتم تنفيذ التحكم وفقًا لقواعد الشبكة المحددة في إعدادات جدار الحماية. لتحديد أي من قواعد الشبكة يجب تطبيقها لمراقبة نشاط الشبكة لمثل هذه التطبيقات، يجب تحديد مجموعة ثقة.

كيفية تحديد مجموعة ثقة للتطبيقات التي بدأت قبل Kaspersky Endpoint Security في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **منع اختراق المضيف**.

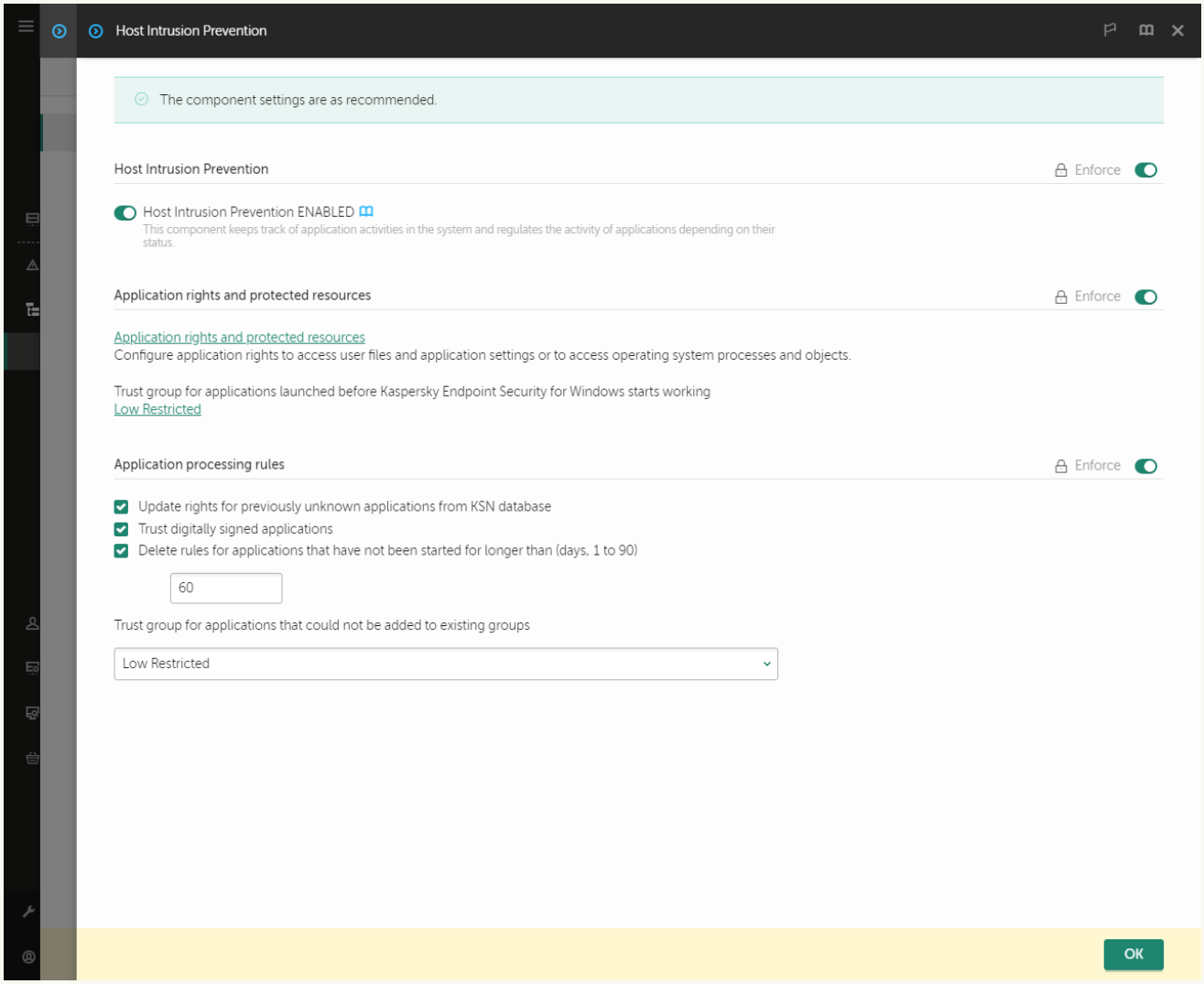


إعدادات منع الاختراق

5. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **تحرير**.
6. لضبط **تم إطلاق مجموعة الثقة للتطبيقات قبل بدء عمل Kaspersky Endpoint Security for Windows**، حدد مجموعة الثقة المناسبة.
7. احفظ تغييراتك.

كيفية تحديد مجموعة ثقة للتطبيقات التي بدأت قبل Kaspersky Endpoint Security في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Advanced Threat Protection ← Host Intrusion Prevention**.



إعدادات منع الاختراق

5. لضبط **تم إطلاق مجموعة الثقة للتطبيقات قبل بدء عمل Kaspersky Endpoint Security for Windows**، حدد مجموعة الثقة المناسبة.
6. احفظ تغييراتك.

كيفية تحديد مجموعة ثقة للتطبيقات التي بدأت قبل Kaspersky Endpoint Security في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.

3. في القسم **تم إطلاق مجموعة الثقة للتطبيقات قبل بدء عمل Kaspersky Endpoint Security for Windows**، حدد مجموعة الثقة المناسبة.

4. احفظ تغييراتك.

نتيجة لذلك، سيتم وضع تطبيق تم بدء تشغيله قبل Kaspersky Endpoint Security في مجموعة الثقة الأخرى. سوف يحظر Kaspersky Endpoint Security بعد ذلك إجراءات التطبيق بناءً على مجموعة الثقة.

تحديد مجموعة ثقة للتطبيقات غير المعروفة

أثناء بدء التشغيل الأول لأحد التطبيقات، يحدد مكون منع اختراق المضيف مجموعة الثقة للتطبيق. وإذا لم يكن لديك وصول للإنترنت أو إذا لم يكن لدى Kaspersky Security Network أي معلومات حول هذا التطبيق، فسوف يضع Kaspersky Endpoint Security التطبيق في المجموعة مقيد بشكل منخفض افتراضيًا. وعند اكتشاف معلومات حول تطبيق غير معروف سابقًا في شبكة KSN، سوف يقوم Kaspersky Endpoint Security بتحديث حقوق هذا التطبيق. وتستطيع بعد ذلك تحرير حقوق التطبيق يدويًا.

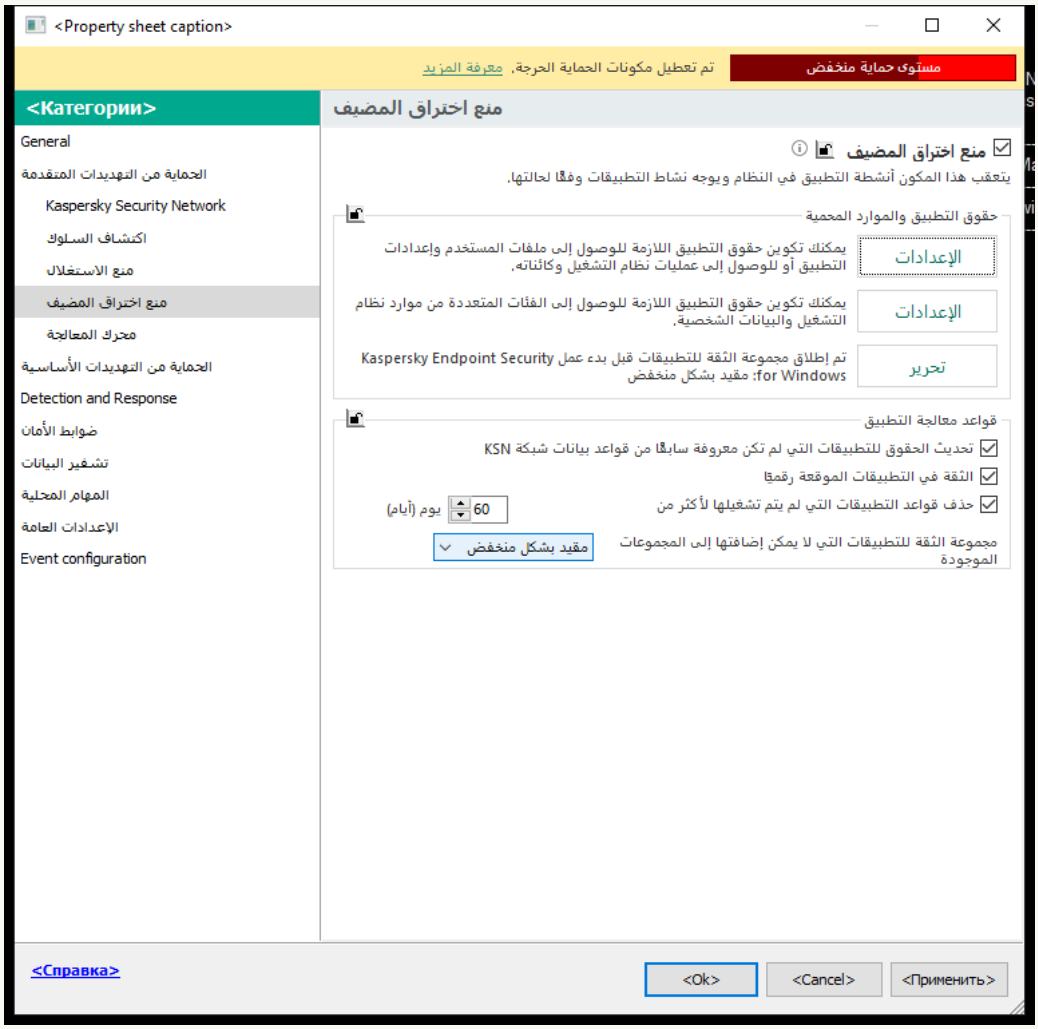
كيفية تحديد مجموعة ثقة للتطبيقات غير المعروفة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

5. في القسم **قواعد معالجة التطبيق**، استخدم القائمة المنسدلة **مجموعة الثقة للتطبيقات التي لا يمكن إضافتها إلى المجموعات الموجودة** لتحديد مجموعة الثقة اللازمة.

في حالة تمكين المشاركة في شبكة Kaspersky Security Network، يُرسل Kaspersky Endpoint Security طلبًا إلى شبكة KSN حول سمعة أحد التطبيقات في كل مرة يبدأ تشغيل التطبيق فيها. وبناءً على الرد المستلم، قد يتم نقل التطبيق إلى مجموعة ثقة مختلفة عن المحددة في إعدادات مكون منع اختراق المضيف.

6. استخدم خانة الاختيار **تحديث الحقوق للتطبيقات التي لم تكن معروفة سابقًا من قواعد بيانات شبكة KSN** لتكوين التحديث التلقائي لحقوق التطبيقات غير المعروفة.

7. احفظ تغييراتك.

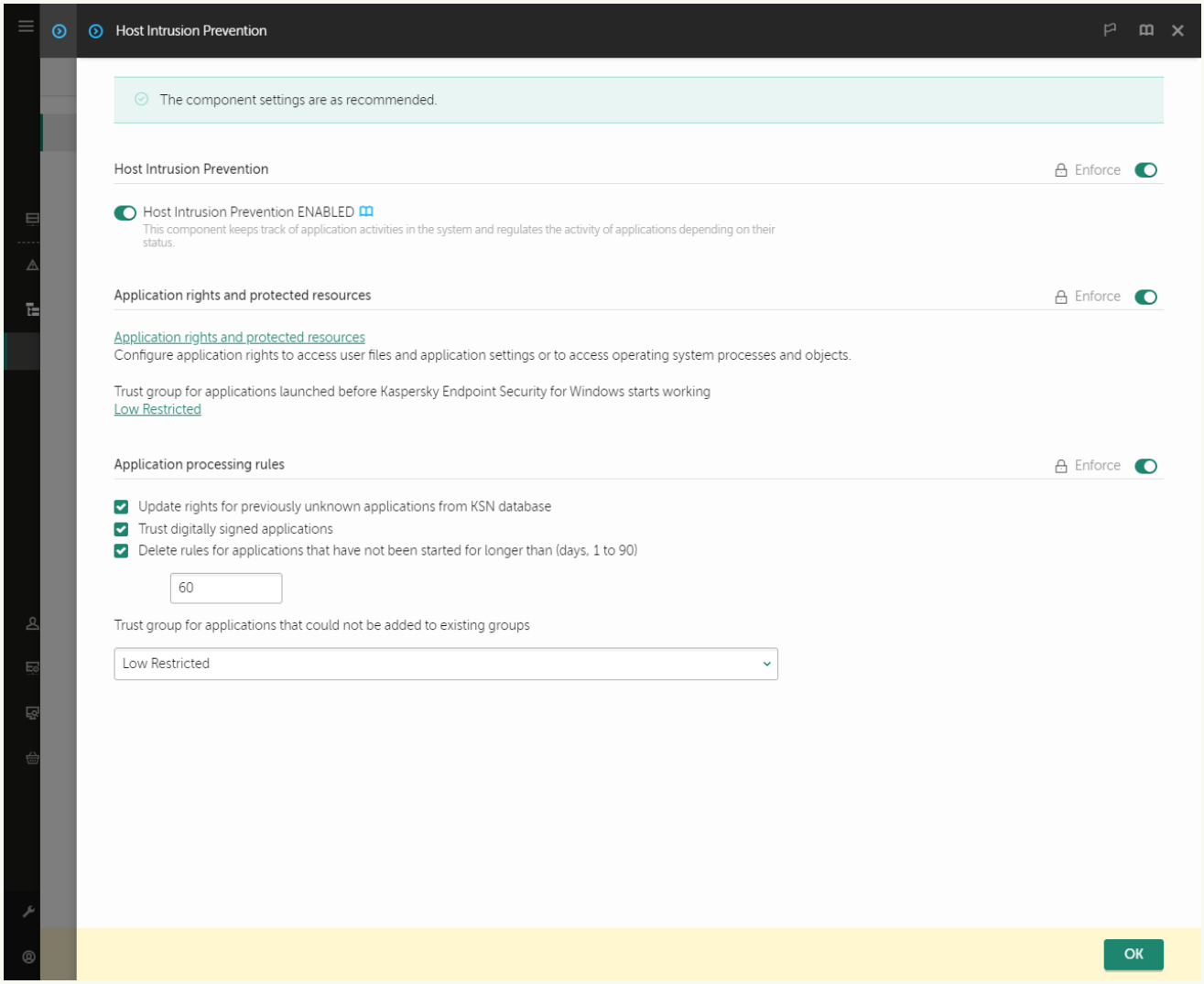
كيفية تحديد مجموعة ثقة للتطبيقات غير المعروفة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. في القسم **قواعد معالجة التطبيق**، استخدم القائمة المنسدلة **مجموعة الثقة للتطبيقات التي لا يمكن إضافتها إلى المجموعات الموجودة** لتحديد مجموعة الثقة اللازمة.

في حالة تمكين المشاركة في شبكة Kaspersky Security Network، يُرسل Kaspersky Endpoint Security طلبًا إلى شبكة KSN حول سمعة أحد التطبيقات في كل مرة يبدأ تشغيل التطبيق فيها. وبناءً على الرد المستلم، قد يتم نقل التطبيق إلى مجموعة ثقة مختلفة عن المحددة في إعدادات مكون منع اختراق المضيف.

6. استخدم خانة الاختيار **تحديث الحقوق للتطبيقات التي لم تكن معروفة سابقًا من قواعد بيانات شبكة KSN** لتكوين التحديث التلقائي لحقوق التطبيقات غير المعروفة.

7. احفظ تغييراتك.

كيفية تحديد مجموعة ثقة للتطبيقات غير المعروفة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.

3. في القسم **قواعد معالجة التطبيق**، حدد مجموعة الثقة المناسبة.

في حالة تمكين المشاركة في شبكة Kaspersky Security Network، يُرسل Kaspersky Endpoint Security طلبًا إلى شبكة KSN حول سمعة أحد التطبيقات في كل مرة يبدأ تشغيل التطبيق فيها. وبناءً على الرد المستلم، قد يتم نقل التطبيق إلى مجموعة ثقة مختلفة عن المحددة في إعدادات مكون منع اختراق المضيف.

4. استخدم خانة الاختيار **تحديث القواعد للتطبيقات التي لم تكن معروفة سابقًا من Kaspersky Security Network** لتكوين التحديث التلقائي لحقوق التطبيقات غير المعروفة.

5. احفظ تغييراتك.

تحديد مجموعة ثقة للتطبيقات الموقعة رقمياً

يضع Kaspersky Endpoint Security دائمًا التطبيقات الموقعة بواسطة شهادات Microsoft أو شهادات Kaspersky في المجموعة موثوق.

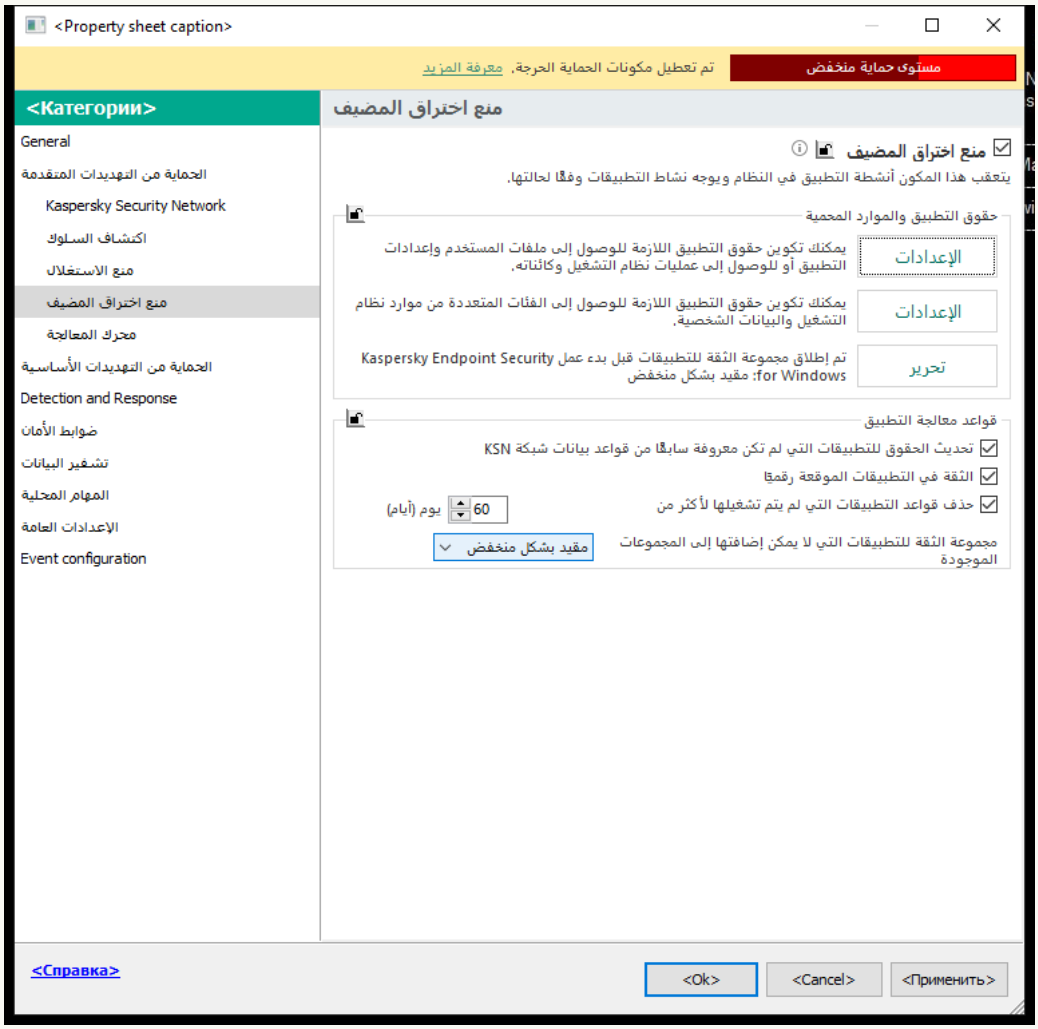
كيفية تحديد مجموعة ثقة للتطبيقات الموقعة رقمياً في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

5. في القسم **قواعد معالجة التطبيق**، استخدم خانة الاختيار **الثقة في التطبيقات الموقعة رقميًا** لتمكين التعيين التلقائي أو تعطيله للمجموعة الموثوقة للتطبيقات التي تحتوي على التوقيع الرقمي للبائعين الموثوقين.

البائعون الموثوقون هم بائعو البرامج الذين يتم تضمينهم في المجموعة الموثوقة بواسطة Kaspersky. ويمكنك أيضًا إضافة شهادة البائع إلى مخزن شهادات النظام الموثوق يدويًا.

في حالة إلغاء تحديد خانة الاختيار هذه، فإن مكون منع اختراق المضيف لا يعتبر التطبيقات الموقعة رقميًا موثوقة، ويستخدم المعلمات الأخرى لتحديد مجموعة الثقة الخاصة بها.

6. احفظ تغييراتك.

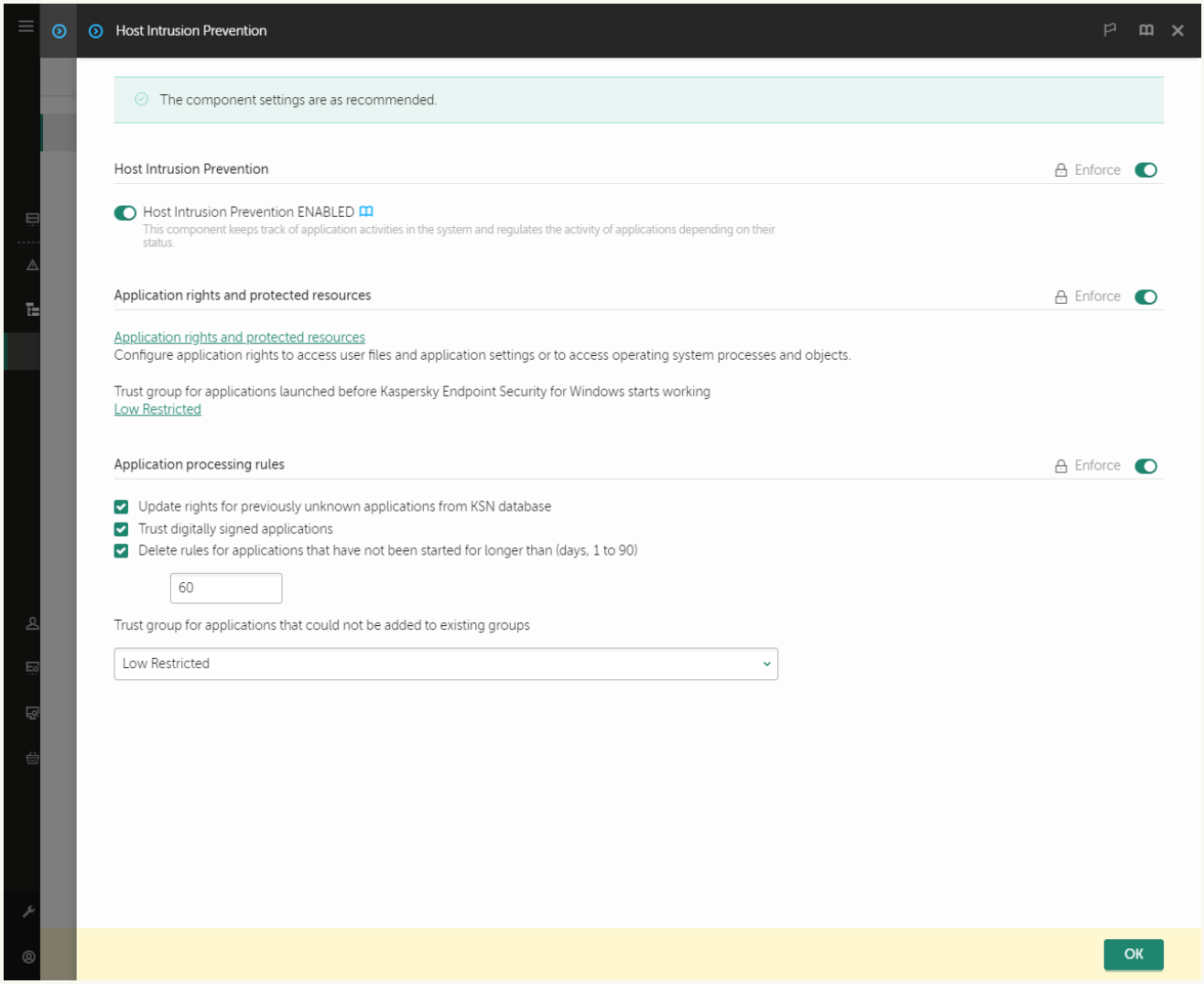
كيفية تحديد مجموعة ثقة للتطبيقات الموقعة رقميًا في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. في القسم **قواعد معالجة التطبيق**، استخدم خانة الاختيار **الثقة في التطبيقات الموقعة رقميًا** لتمكين التعيين التلقائي أو تعطيله للمجموعة الموثوقة للتطبيقات التي تحتوي على التوقيع الرقمي للبائعين الموثوقين.

البائعون الموثوقون هم بائعو البرامج الذين يتم تضمينهم في المجموعة الموثوقة بواسطة Kaspersky. ويمكنك أيضًا إضافة شهادة البائع إلى مخزن شهادات النظام الموثوق يدويًا.

في حالة إلغاء تحديد خانة الاختيار هذه، فإن مكون منع اختراق المضيف لا يعتبر التطبيقات الموقعة رقميًا موثوقة، ويستخدم المعلمات الأخرى لتحديد مجموعة الثقة الخاصة بها.

6. احفظ تغييراتك.

كيفية تحديد مجموعة ثقة للتطبيقات الموقعة رقميًا في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.

3. في القسم **قواعد معالجة التطبيق**، استخدم خانة الاختيار **الثقة في التطبيقات الموقعة رقميًا** لتمكين التعيين التلقائي أو تعطيله للمجموعة الموثوقة للتطبيقات التي تحتوي على التوقيع الرقمي للبائعين الموثوقين.

   البائعون الموثوقون هم بائعو البرامج الذين يتم تضمينهم في المجموعة الموثوقة بواسطة Kaspersky. ويمكنك أيضًا إضافة شهادة البائع إلى مخزن شهادات النظام الموثوق يدويًا.

   في حالة إلغاء تحديد خانة الاختيار هذه، فإن مكون منع اختراق المضيف لا يعتبر التطبيقات الموقعة رقميًا موثوقة، ويستخدم المعلمات الأخرى لتحديد مجموعة الثقة الخاصة بها.

4. احفظ تغييراتك.

إدارة حقوق التطبيق

بشكل افتراضي، يتم التحكم في نشاط التطبيق استنادًا إلى حقوق التطبيق المحددة إلى مجموعة الثقة المحددة التي عينها Kaspersky Endpoint Security للتطبيق عند بدء تشغيله لأول مرة. وعند الضرورة، يمكنك تحرير قواعد التحكم في امتيازات التطبيق لمجموعة الثقة بأكملها، لتطبيق فردي أو لمجموعة من التطبيقات الموجودة ضمن مجموعة ثقة.

تمتلك حقوق التطبيق المحددة يدويًا أولوية أعلى من حقوق التطبيق التي تم تحديدها لمجموعة ثقة. بمعنى آخر، إذا كانت حقوق التطبيق المحددة يدويًا تختلف عن حقوق التطبيق المحددة لمجموعة ثقة، يتحكم مكون منع اختراق المضيف في نشاط التطبيق وفقًا لحقوق التطبيق المحددة يدويًا.

يتم توريث القواعد التي تنشؤها للتطبيقات بواسطة التطبيقات الفرعية. على سبيل المثال، إذا رفضت كل أنشطة الشبكة لبرنامج cmd.exe، فسيتم رفض كل أنشطة الشبكة أيضًا لبرنامج notepad.exe إذا بدأ تشغيله باستخدام cmd.exe. عندما لا يكون تطبيق تابعًا للتطبيق الذي يتم تشغيله منه، لا يتم وراثة القواعد.

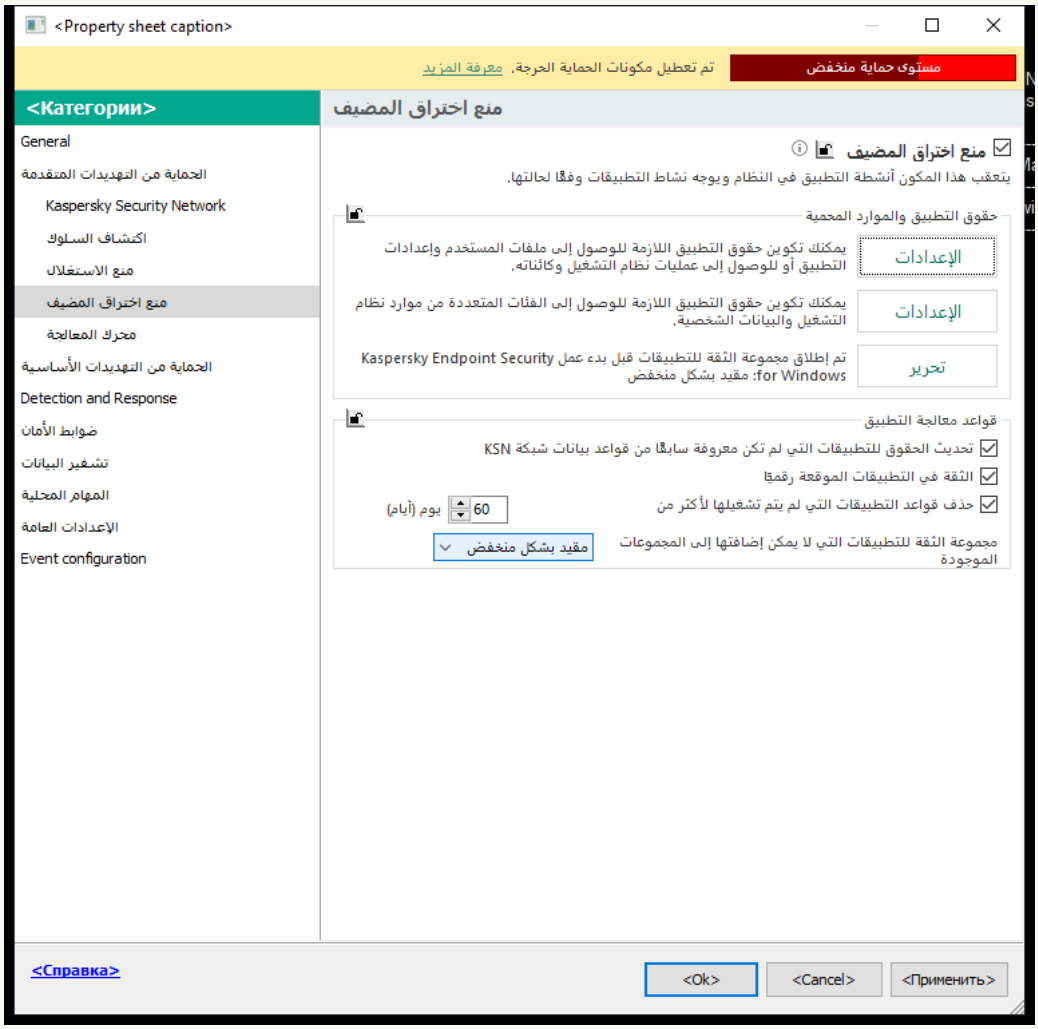
كيفية تغيير حقوق التطبيق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

5. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **حقوق التطبيق**.

7. انقر على **إضافة**.

8. في النافذة التي تفتح، أدخل المعايير للبحث عن التطبيق الذي تريد تغيير حقوقه.

يمكنك إدخال اسم التطبيق أو اسم البائع. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

9. انقر فوق الزر **تحديث**.

سيبحث Kaspersky Endpoint Security عن التطبيق في القائمة الموحدة للتطبيقات المثبتة على أجهزة الكمبيوتر المدارة. سيعرض Kaspersky Endpoint Security قائمة بالتطبيقات التي تلبي معايير البحث الخاصة بك.

10. حدد التطبيق المطلوب.

11. في القائمة المنسدلة **إضافة التطبيق المحدد إلى مجموعة الثقة**، حدد **المجموعات الافتراضية** وانقر فوق **موافق**.

ستتم إضافة التطبيق إلى المجموعة الافتراضية.

12. حدد التطبيق ذي الصلة، ثم حدد **حقوق التطبيق** من قائمة السياق الخاصة بالتطبيق.

تفتح هذه الخطوة خصائص التطبيق.

13. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد علامة التبويب **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد علامة التبويب **الحقوق**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة جدار الحماية باستخدام قواعد الشبكة.

14. للمورد ذي الصلة، في عمود الإجراء المتوافق، انقر بزر الماوس الأيمن لفتح قائمة السياق وتحديد الخيار اللازم: **توريث** أو **سماح** (✓) أو **منع** (⊘).

15. إذا كنت تريد مراقبة استخدام موارد الكمبيوتر، حدد **أحداث السجل** (✓ / ⊘).

سوف يسجل Kaspersky Endpoint Security معلومات حول تشغيل مكون منع اختراق المضيف. وتحتوي التقارير على معلومات حول العمليات باستخدام موارد الكمبيوتر التي ينفذها التطبيق (مسموح بها أو ممنوعة). وتحتوي التقارير أيضًا على معلومات حول التطبيقات التي تستخدم كل مورد.

16. احفظ تغييراتك.

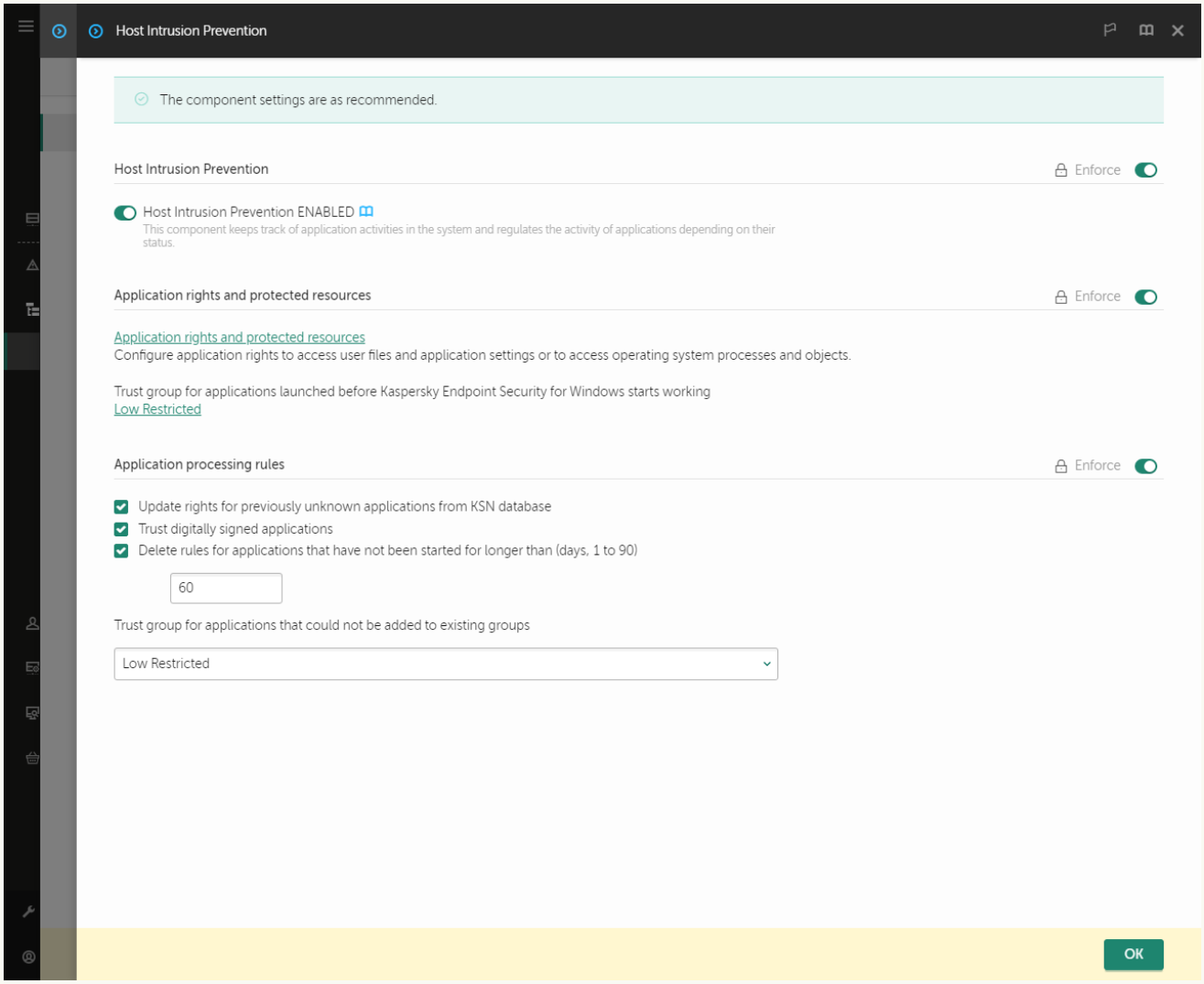
كيفية تغيير حقوق التطبيق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. في القسم **Application rights and protected resources**، انقر على الرابط **Application rights and protected resources**.
يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **Application rights**.
سترى قائمة تتضمن مجموعات الثقة على الجانب الأيمن من النافذة وخصائصها على الجانب الأيسر.

7. انقر على **Add**.
يؤدي هذا إلى تشغيل المعالج لإضافة تطبيق إلى مجموعة ثقة.

8. حدد مجموعة الثقة ذات الصلة للتطبيق.

9. حدد نوع **Application**. انتقل إلى الخطوة التالية.

إذا كنت تريد تغيير مجموعة الثقة لتطبيقات متعددة، فحدد نوع **Group** وحدد اسمًا لمجموعة التطبيقات.

10. في قائمة التطبيقات المفتوحة، حدد التطبيقات التي تريد تغيير حقوق التطبيق الخاصة بها.

استخدم عامل تصفية. يمكنك إدخال اسم التطبيق أو اسم البائع. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

11. أغلق المعالج.

ستتم إضافة التطبيق إلى مجموعة الثقة.

12. في الجزء الأيمن من النافذة، حدد التطبيق ذي الصلة.

13. في الجزء الأيسر من النافذة، في القائمة المنسدلة، نفذ أحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد **Files and system registry**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد **Rights**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة جدار الحماية باستخدام قواعد الشبكة.

14. للمورد ذي الصلة، في عمود الإجراء المتوافق، حدد الخيار اللازم: **Inherit** أو **Allow** (✓) أو **Block** (✗).

15. إذا كنت تريد مراقبة استخدام موارد الكمبيوتر، حدد **Log events** (✓ / ✗).

سوف يسجل Kaspersky Endpoint Security معلومات حول تشغيل مكون منع اختراق المضيف. وتحتوي التقارير على معلومات حول العمليات باستخدام موارد الكمبيوتر التي ينفذها التطبيق (مسموح بها أو ممنوعة). وتحتوي التقارير أيضًا على معلومات حول التطبيقات التي تستخدم كل مورد.

16. احفظ تغييراتك.

كيفية تغيير حقوق التطبيق في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **منع اختراق المضيف**.

3. انقر على **إدارة التطبيقات**.

يفتح هذا قائمة التطبيقات المثبتة.

4. حدد التطبيق المطلوب.

5. في قائمة السياق الخاصة بالتطبيق، حدد **تفاصيل وقواعد**.

تفتح هذه الخطوة خصائص التطبيق.

6. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد علامة التبويب **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد علامة التبويب **الحقوق**.

7. للمورد ذي الصلة، في عمود الإجراء المتوافق، انقر بزر الماوس الأيمن لفتح قائمة السياق وتحديد الخيار اللازم: **توريث** أو **سماح** (✓) أو **رفض** (!).

8. إذا كنت تريد مراقبة استخدام موارد الكمبيوتر، فحدد **أحداث السجل** (📊).

سوف يسجل Kaspersky Endpoint Security معلومات حول تشغيل مكون منع اختراق المضيف. وتحتوي التقارير على معلومات حول العمليات باستخدام موارد الكمبيوتر التي ينفذها التطبيق (مسموح بها أو ممنوعة). وتحتوي التقارير أيضًا على معلومات حول التطبيقات التي تستخدم كل مورد.

9. حدد علامة التبويب **الاستثناءات** وكوّن الإعدادات المتقدمة للتطبيق (انظر الجدول أدناه).

10. احفظ تغييراتك.

الإعدادات المتقدمة للتطبيق

المعلمة	الوصف
عدم فحص الملفات قبل الفتح	يتم استثناء كل الملفات المفتوحة بواسطة التطبيق من عمليات الفحص بواسطة Kaspersky Endpoint Security. على سبيل المثال، إذا كنت تستخدم تطبيقات لنسخ الملفات احتياطيًا، فتساعد هذه الميزة في تقليل استهلاك الموارد بواسطة Kaspersky Endpoint Security.
عدم مراقبة نشاط التطبيق	لن يراقب Kaspersky Endpoint Security نشاط الملف والشبكة الخاص بالتطبيق في نظام التشغيل. تتم مراقبة نشاط التطبيق من خلال المكونات التالية: اكتشاف السلوك ومنع الاستغلال ومنع اختراق المضيف ومحرك المعالجة وجدار الحماية.
عدم وراثة القيود من العملية الأصلية (للتطبيق)	لن يتم تطبيق القيود التي تم تكوينها للعملية الرئيسية بواسطة Kaspersky Endpoint Security على عملية فرعية. تبدأ العملية الأصلية بواسطة تطبيق تم تكوين حقوق التطبيق (منع اختراق المضيف) وقواعد الشبكة للتطبيق (جدار الحماية) له.
عدم مراقبة نشاط التطبيق التابع	لن يراقب Kaspersky Endpoint Security نشاط الملف ونشاط الشبكة للتطبيقات التي يتم بدء تشغيلها بواسطة التطبيق.
السماح بالتفاعل مع واجهة Kaspersky Endpoint Security for Windows	يمنع الدفاع الذاتي في Kaspersky Endpoint Security جميع محاولات إدارة خدمات التطبيقات من كمبيوتر بعيد. في حالة تحديد خانة الاختيار، يتم السماح بتطبيق الوصول عن بعد عن طريق إدارة إعدادات Kaspersky Endpoint Security من خلال واجهة Kaspersky Endpoint Security.
عدم فحص حركة مرور البيانات المشفرة / عدم فحص كل حركة البيانات	سيتم استثناء حركة شبكة الاتصال التي بدأها التطبيق من عمليات الفحص بواسطة Kaspersky Endpoint Security. يمكنك استثناء كل حركة المرور أو حركة المرور المشفرة فقط من عمليات الفحص. يمكنك أيضًا استثناء عناوين IP فردية وأرقام المنافذ من عمليات الفحص.

حماية موارد نظام التشغيل والبيانات الشخصية

يدير مكون منع اختراق المضيف حقوق التطبيقات لاتخاذ إجراءات حول مختلف فئات موارد نظام التشغيل والبيانات الشخصية. أنشأ مختصو Kaspersky فئات معدة مسبقًا من الموارد المحمية. على سبيل المثال، تتضمن فئة نظام التشغيل فئة فرعية باسم إعدادات بدء التشغيل تسرد جميع مفاتيح التسجيل المرتبطة بالتشغيل التلقائي للتطبيقات. لا يمكنك تحرير أو حذف الفئات المعدة مسبقًا من الموارد المحمية أو الموارد المحمية التي تتضمنها هذه الفئات.

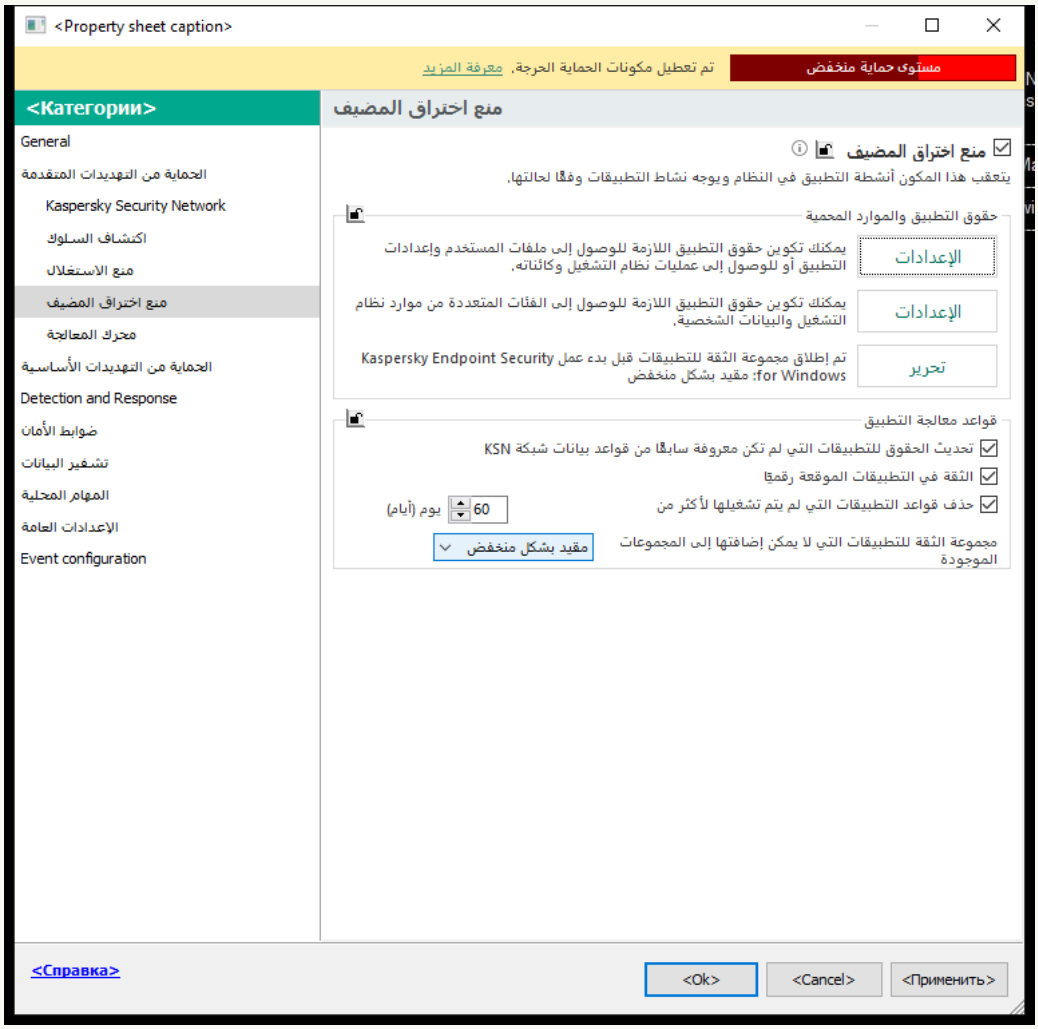
كيفية إضافة مورد محمي في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

5. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **الموارد المحمية**.

سترى قائمة بالموارد المحمية في الجزء الأيمن من النافذة والحقوق المقابلة للوصول إلى هذه الموارد حسب مجموعة الثقة المحددة.

7. حدد فئة الموارد المحمية التي تريد إضافة مورد محمي جديد إليها.

إذا كنت ترغب في إضافة فئة فرعية، فانقر فوق **إضافة ← الفئة**.

8. انقر على الزر **إضافة**. في القائمة المنسدلة، حدد نوع المورد الذي تريد إضافته: **الملف أو المجلد** أو **مفتاح التسجيل**.

9. في النافذة التي تفتح، حدد ملفًا أو مجلدًا أو مفتاح تسجيل.

يمكنك عرض حقوق التطبيقات للوصول إلى الموارد المضافة. ولفعل ذلك، حدد موردًا مضافًا في الجزء الأيمن من النافذة وسيعرض Kaspersky Endpoint Security حقوق الوصول لكل مجموعة ثقة. ويمكنك أيضًا تعطيل تحكم نشاط التطبيق في الموارد باستخدام خانة الاختيار الموجودة بجوار مورد جديد.

10. احفظ تغييراتك.

[كيفية إضافة مورد محمي في Web Console وCloud Console]

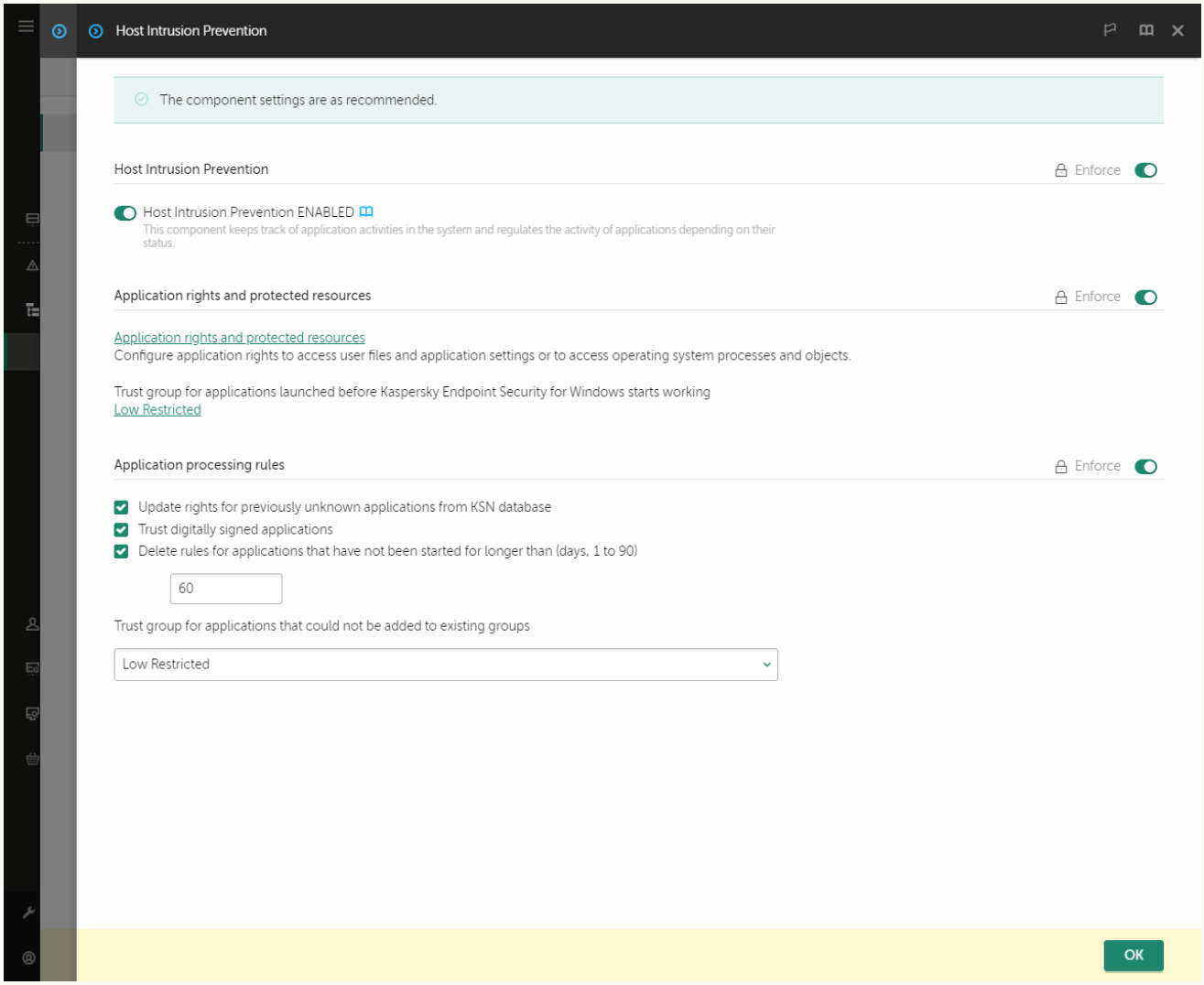
1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. في القسم **Application rights and protected resources**، انقر على الرابط **Application rights and protected resources**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. حدد علامة التبويب **Protected resources**.

سترى قائمة بالموارد المحمية في الجزء الأيمن من النافذة والحقوق المقابلة للوصول إلى هذه الموارد حسب مجموعة الثقة المحددة.

7. انقر على **Add**.

يبدأ معالج المورد الجديد.

8. انقر فوق الرابط **Group name** لتحديد فئة الموارد المحمية التي تريد إضافة مورد محمي جديد إليها.

إذا كنت تريد إضافة فئة فرعية، فحدد الخيار **Category of protected resources**.

9. حدد نوع المورد الذي تريد إضافته: **File or folder** أو **Registry key**.

10. حدد ملفًا أو مجلدًا أو مفتاح تسجيل.

11. أغلق المعالج.

يمكنك عرض حقوق التطبيقات للوصول إلى الموارد المضافة. ولفعل ذلك، حدد موردًا مضافًا في الجزء الأيمن من النافذة وسيعرض Kaspersky Endpoint Security حقوق الوصول لكل مجموعة ثقة. يمكنك أيضًا استخدام خانة الاختيار في العمود **Status** لتعطيل تحكم نشاط التطبيقات في الموارد.

12. احفظ تغييراتك.

كيفية إضافة مورد محمي في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **منع اختراق المضيف**.

3. انقر على **إدارة الموارد**.

تفتح قائمة الموارد المحمية.

4. حدد فئة الموارد المحمية التي تريد إضافة مورد محمي جديد إليها.

إذا كنت ترغب في إضافة فئة فرعية، فانقر فوق **إضافة** ← **الفئة**.

5. انقر على الزر **إضافة**. في القائمة المنسدلة، حدد نوع المورد الذي تريد إضافته: **الملف أو المجلد** أو **مفتاح التسجيل**.

6. في النافذة التي تفتح، حدد ملفًا أو مجلدًا أو مفتاح تسجيل.

يمكنك عرض حقوق التطبيقات للوصول إلى الموارد المضافة. ولفعل ذلك، حدد موردًا مضافًا في الجزء الأيمن من النافذة وسيعرض Kaspersky Endpoint Security قائمة بالتطبيقات وحقوق الوصول لكل تطبيق. يمكنك أيضًا تعطيل تحكم نشاط التطبيقات في الموارد باستخدام الزر **تمكين التحكم** في العمود **الحالة**.

7. احفظ تغييراتك.

سيتحكم Kaspersky Endpoint Security في الوصول إلى موارد نظام التشغيل المضافة والبيانات الشخصية. ويتحكم Kaspersky Endpoint Security في وصول التطبيق إلى الموارد بناءً على مجموعة الثقة المعينة للتطبيق. ويمكنك تغيير مجموعة الثقة لتطبيق.

حذف معلومات حول التطبيقات غير المستخدمة

Kaspersky Endpoint Security يستخدم حقوق التطبيق للتحكم في أنشطة التطبيقات. حقوق التطبيق يحددها مجموعة الثقة التابعة لها. يضع Kaspersky Endpoint Security تطبيقًا في مجموعة الثقة عند بدء تشغيل التطبيق لأول مرة. يمكنك تغيير مجموعة الثقة لتطبيق يدويًا. يمكنك كذلك تكوين حقوق تطبيق معين يدويًا. يقوم Kaspersky Endpoint Security بتخزين المعلومات التالية عن أي تطبيق: مجموعة ثقة التطبيق وحقوق التطبيق.

يقوم Kaspersky Endpoint Security تلقائيًا بحذف المعلومات عن التطبيقات غير المستخدمة بهدف المحافظة على موارد الكمبيوتر. يقوم Kaspersky Endpoint Security بحذف معلومات التطبيق وفق القواعد التالية:

- إذا كانت مجموعة الثقة والحقوق لتطبيق محددة بشكل تلقائي، سيقوم Kaspersky Endpoint Security تلقائيًا بحذف معلومات هذا التطبيق بعد 30 يومًا. إذا لم يمكن من الممكن تغيير مدة التخزين لمعلومات التطبيق أو إلغاء الحذف.
- إذا كنت تقوم يدويًا بوضع تطبيق في مجموعة ثقة أو تقوم بتكوين حقوق الوصول إليه، فإن Kaspersky Endpoint Security يحذف معلومات ذلك التطبيق بعد مرور 60 يومًا (مدة التخزين الافتراضية). يمكنك تغيير مدة التخزين لمعلومات تطبيق أو إلغاء الحذف التلقائي (راجع التعليمات أدناه).

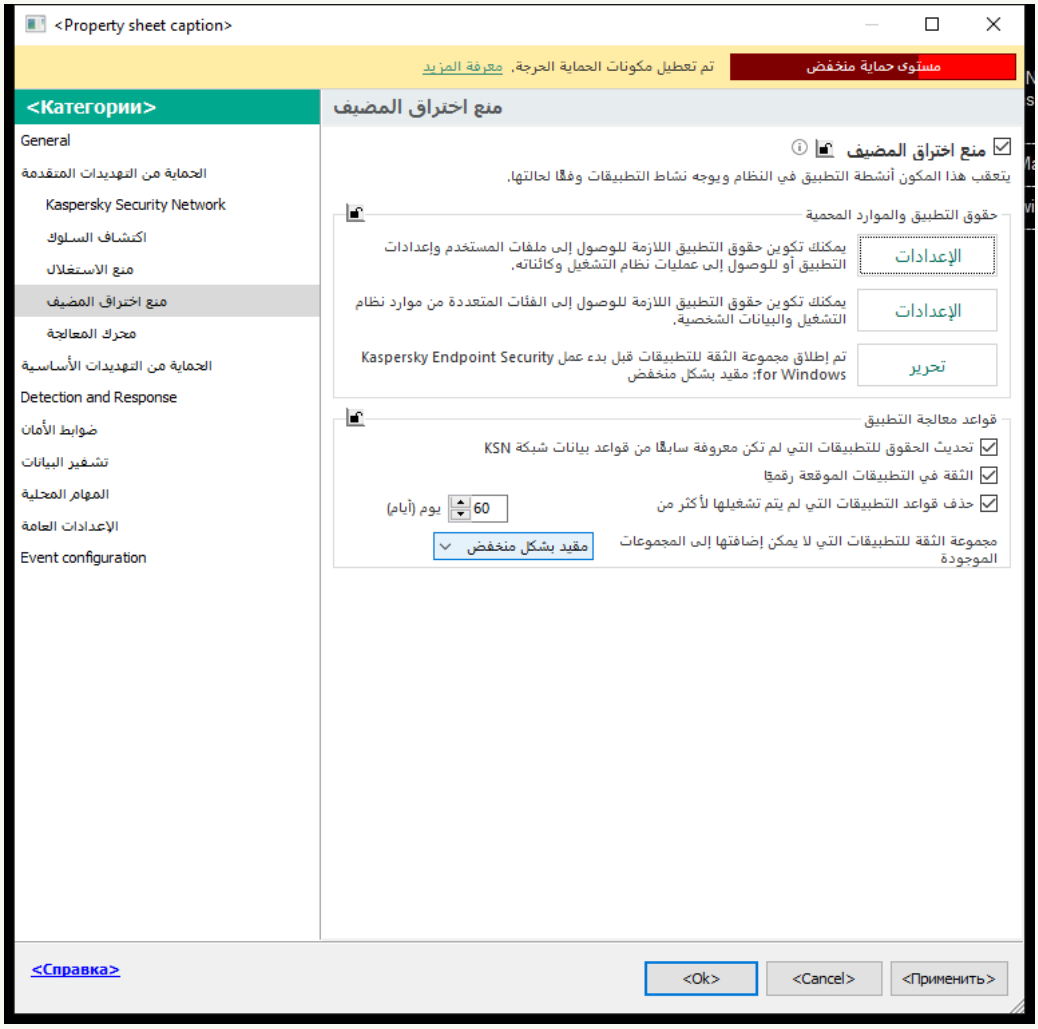
عندما تبدأ تطبيقًا قد تم حذف معلوماته، فإن Kaspersky Endpoint Security يحلل التطبيق كأنه يبدأ لأول مرة.

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

5. في القسم **قواعد معالجة التطبيق**، نفذ أحد الإجراءات التالية:

- إذا كنت ترغب في تكوين الحذف التلقائي، حدد خانة الاختيار **حذف قواعد التطبيقات التي لم يتم تشغيلها لأكثر من N يوم (أيام)** وأدخل عدد الأيام.

  سيقوم Kaspersky Endpoint Security بحذف معلومات التطبيقات التي قمت يدويًا بوضعها في مجموعة ثقة أو قد كونت حقوق الوصول إليها بعد مرور عدد الأيام المحددة. المعلومات المتوفرة عن التطبيقات التي قد حددت مجموعة ثقتها وحقوق التطبيق لها سوف يحذفها Kaspersky Endpoint Security أيضًا بعد مرور 30 يومًا.

- إذا كنت ترغب في إيقاف تشغيل الحذف التلقائي، فقم بإلغاء تحديد خانة الاختيار **حذف قواعد التطبيقات التي لم يتم تشغيلها لأكثر من N يوم (أيام)**.

  سيقوم Kaspersky Endpoint Security باستعادة معلومات التطبيقات التي قمت يدويًا بوضعها في مجموعة ثقة أو قد كونت حقوق الوصول إليها إلى الأبد دون أي قيود على مدة التخزين. لن يحذف Kaspersky Endpoint Security إلا معلومات التطبيقات التي قد تم تحديد حذف مجموعة ثقتها وحقوقها تلقائيًا بعد مرور 30 يومًا.

6. احفظ تغييراتك.

كيفية تكوين الحذف التلقائي للمعلومات حول التطبيقات غير المستخدمة في Web Console وCloud Console

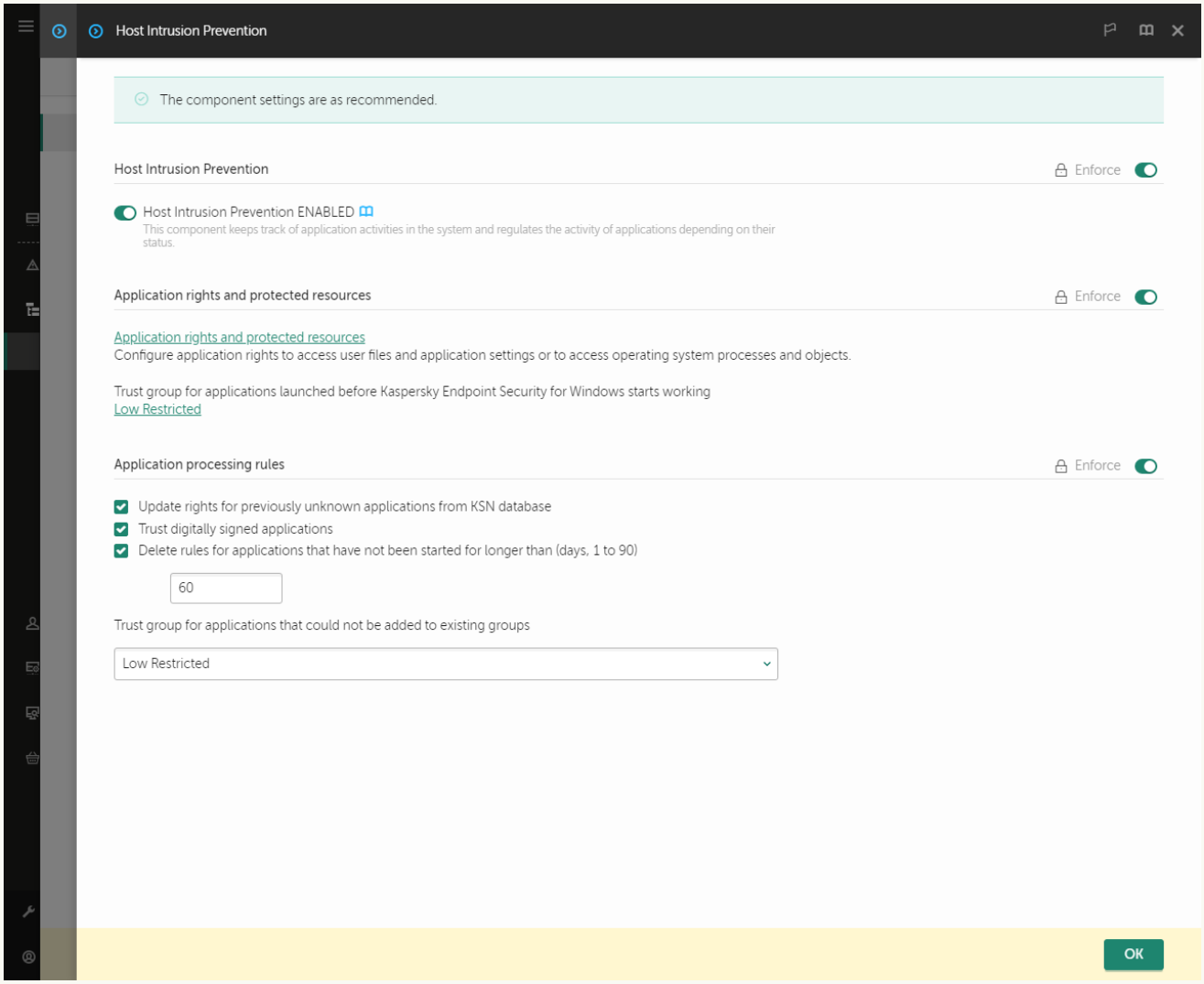
1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Host Intrusion Prevention**.



إعدادات منع الاختراق

5. في القسم **قواعد معالجة التطبيق**، نفذ أحد الإجراءات التالية:

- إذا كنت ترغب في تكوين الحذف التلقائي، حدد خانة الاختيار **حذف قواعد التطبيقات التي لم يتم تشغيلها لأكثر من N يوم (أيام)** وأدخل عدد الأيام.

  سيقوم Kaspersky Endpoint Security بحذف معلومات التطبيقات التي قمت يدويًا بوضعها في مجموعة ثقة أو قد كونت حقوق الوصول إليها بعد مرور عدد الأيام المحددة. المعلومات المتوفرة عن التطبيقات التي قد حددت مجموعة ثقتها وحقوق التطبيق لها سوف يحذفها Kaspersky Endpoint Security أيضًا بعد مرور 30 يومًا.

- إذا كنت ترغب في إيقاف تشغيل الحذف التلقائي، فقم بإلغاء تحديد خانة الاختيار **حذف قواعد التطبيقات التي لم يتم تشغيلها لأكثر من N يوم (أيام)**.

  سيقوم Kaspersky Endpoint Security باستعادة معلومات التطبيقات التي قمت يدويًا بوضعها في مجموعة ثقة أو قد كونت حقوق الوصول إليها إلى الأبد دون أي قيود على مدة التخزين. لن يحذف Kaspersky Endpoint Security إلا معلومات التطبيقات التي قد تم تحديد حذف مجموعة ثقتها وحقوقها تلقائيًا بعد مرور 30 يومًا.

6. احفظ تغييراتك.

كيفية تكوين الحذف التلقائي للمعلومات حول التطبيقات غير المستخدمة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.
3. في القسم **قواعد معالجة التطبيق**، نفذ أحد الإجراءات التالية:
   - إذا كنت ترغب في تكوين الحذف التلقائي، حدد خانة الاختيار **حذف قواعد التطبيقات التي لم يتم تشغيلها لأكثر من N يوم (أيام)** وأدخل عدد الأيام.
     سيقوم Kaspersky Endpoint Security بحذف معلومات التطبيقات التي قمت يدويًا بوضعها في مجموعة ثقة أو قد كونت حقوق الوصول إليها بعد مرور عدد الأيام المحددة. المعلومات المتوفرة عن التطبيقات التي قد حددت مجموعة ثقتها وحقوق التطبيق لها سوف يحذفها Kaspersky Endpoint Security أيضًا بعد مرور 30 يومًا.
   - إذا كنت ترغب في إيقاف تشغيل الحذف التلقائي، فقم بإلغاء تحديد خانة الاختيار **حذف قواعد التطبيقات التي لم يتم تشغيلها لأكثر من N يوم (أيام)**.
     سيقوم Kaspersky Endpoint Security باستعادة معلومات التطبيقات التي قمت يدويًا بوضعها في مجموعة ثقة أو قد كونت حقوق الوصول إليها إلى الأبد دون أي قيود على مدة التخزين. لن يحذف Kaspersky Endpoint Security إلا معلومات التطبيقات التي قد تم تحديد حذف مجموعة ثقتها وحقوقها تلقائيًا بعد مرور 30 يومًا.
4. احفظ تغييراتك.

مراقبة منع اختراق المضيف

يمكنك تلقي تقارير حول تشغيل مكون منع اختراق المضيف. وتحتوي التقارير على معلومات حول العمليات باستخدام موارد الكمبيوتر التي ينفذها التطبيق (مسموح بها أو ممنوعة). وتحتوي التقارير أيضًا على معلومات حول التطبيقات التي تستخدم كل مورد.

لمراقبة عمليات منع اختراق المضيف، تحتاج إلى تمكين كتابة التقارير. على سبيل المثال، يمكنك تمكين إعادة توجيه التقارير لتطبيقات فردية في إعدادات مكون منع اختراق المضيف.

عند تكوين مراقبة منع اختراق المضيف، ضع في الاعتبار الحمل المحتمل للشبكة عند إعادة توجيه الأحداث إلى Kaspersky Security Center. يمكنك أيضًا تمكين حفظ التقارير فقط في السجل المحلي لتطبيق Kaspersky Endpoint Security.

حماية الوصول إلى الصوت والفيديو

يستطيع مجرمو الإنترنت استخدام برامج خاصة لمحاولة الوصول إلى الأجهزة التي تسجل الصوت والفيديو (مثل الميكروفونات أو كاميرات الويب). ويتحكم Kaspersky Endpoint Security عندما تتلقى التطبيقات بثًا صوتيًا أو بث فيديو، ويحمي البيانات من الاعتراض غير المصرح به.

افتراضيًا، يتحكم Kaspersky Endpoint Security في وصول التطبيقات إلى بث الصوت والفيديو على النحو التالي:

- يُسمح للتطبيقات في فئة موثوق ومقيد بشكل منخفض باستقبال بث الصوت والفيديو من الأجهزة بشكل افتراضي.
- لا يُسمح للتطبيقات في فئة مقيد بشكل عالٍ وغير موثوق باستقبال بث الصوت وبث الفيديو من الأجهزة بشكل افتراضي.

يمكنك السماح للتطبيقات باستقبال الصوت والفيديو يدويًا.

ميزات خاصة لحماية بث الصوت

تتضمن حماية بث الصوت السمات الخاصة التالية:

- يجب تمكين مكون منع اختراق المضيف لكي تعمل هذه الوظيفة.
- إذا بدأ التطبيق في استقبال تدفق الصوت قبل بدء مكون منع اختراق المضيف، فسيسمح Kaspersky Endpoint Security للتطبيق باستقبال تدفق الصوت دون إظهار أية إخطارات.
- إذا قمت بنقل تطبيق إلى مجموعة غير موثوق أو مجموعة مقيد بشكل عالٍ بعد بدء التطبيق في استقبال تدفق الصوت، فيسمح Kaspersky Endpoint Security للتطبيق باستقبال تدفق الصوت ولا يقوم بإظهار أية إخطارات.
- بعد تغيير إعدادات وصول التطبيق إلى أجهزة تسجيل الصوت (على سبيل المثال، في حالة منع التطبيق من استقبال بث الصوت)، فيجب إعادة تشغيل هذا التطبيق لإيقافه من استقبال بث الصوت.
- لا يعتمد التحكم في الوصول إلى تدفق الصوت من أجهزة تسجيل الصوت على إعدادات وصول التطبيق إلى كاميرا الويب.
- يحمي Kaspersky Endpoint Security الوصول إلى أجهزة الميكروفون المدمجة وأجهزة الميكروفون الخارجية فقط. لا يتم دعم أجهزة تدفق الصوت الأخرى.
- لا يضمن Kaspersky Endpoint Security حماية تدفق الصوت من أجهزة مثل كاميرات DSLR وكاميرات الفيديو المحمولة وكاميرات العمل.
- عندما تقوم بتشغيل تسجيل الصوت والفيديو أو تطبيقات التشغيل للمرة الأولى منذ تثبيت Kaspersky Endpoint Security، فقد يتم مقاطعة تشغيل أو تسجيل الصوت والفيديو. ويعد ذلك ضروريًا لتمكين وظائف التحكم في الوصول إلى أجهزة تسجيل الصوت بواسطة التطبيقات. ويتم إعادة تشغيل خدمة النظام التي تتحكم في أجهزة الصوت عند تشغيل Kaspersky Endpoint Security للمرة الأولى.

ميزات خاصة لحماية الوصول إلى كاميرا الويب للتطبيق

لوظائف حماية الوصول إلى كاميرا الويب الاعتبارات والقيود الخاصة التالية:

- يتحكم التطبيق في الفيديو والصور الثابتة المستمدة من معالجة بيانات كاميرا الويب.
- يتحكم التطبيق في تدفق الصوت إذا كان جزءً من تدفق الفيديو الذي يتم استلامه من كاميرا الويب.
- يتحكم التطبيق فقط في كاميرات الويب المتصلة عبر USB أو IEEE1394 والمعروضة كأجهزة تصوير في Windows Device Manager.
- يدعم Kaspersky Endpoint Security كاميرات الويب التالية:
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800

- Microsoft LifeCam Cinema

لا تضمن Kaspersky دعم كاميرات الويب غير المحددة في هذه القائمة.

محرك المعالجة

يتيح محرك المعالجة لبرنامج Kaspersky Endpoint Security التراجع عن الإجراءات التي تم تنفيذها باستخدام برمجيات ضارة في نظام التشغيل.

عند التراجع عن نشاط ضار في نظام التشغيل، يتعامل Kaspersky Endpoint Security مع الأنواع التالية من أنشطة البرمجيات الضارة:

- **نشاط الملف**

  يقوم Kaspersky Endpoint Security بالإجراءات التالية:

  - يحذف الملفات القابلة للتنفيذ التي تم إنشاؤها من قبل برمجيات ضارة (في جميع الوسائط ما عدا محركات الشبكات).
  - يحذف الملفات القابلة للتنفيذ التي تم إنشاؤها بواسطة البرامج التي تسللت بواسطة البرمجيات الضارة.
  - يستعيد الملفات التي تم تعديلها أو حذفها بواسطة البرمجيات الضارة.

  لدى ميزة استرداد الملف عدد من القيود.

- **نشاط التسجيل**

  يقوم Kaspersky Endpoint Security بالإجراءات التالية:

  - يحذف مفاتيح التسجيل التي تم إنشاؤها بواسطة البرمجيات الضارة.
  - لا يستعيد مفاتيح التسجيل التي تم تعديلها أو حذفها بواسطة البرمجيات الضارة.

- **نشاط النظام**

  يقوم Kaspersky Endpoint Security بالإجراءات التالية:

  - ينهي العمليات التي تم بدؤها بواسطة البرمجيات الضارة.
  - ينهي العمليات التي اخترقها تطبيق ضار.
  - لا يستأنف العمليات التي تم وقفها باستخدام برمجيات ضارة.

- **نشاط الشبكة**

  يقوم Kaspersky Endpoint Security بالإجراءات التالية:

  - يحظر نشاط شبكة البرمجيات الضارة.
  - يحظر نشاط شبكة العمليات التي تسللت بواسطة البرمجيات الضارة.

يمكن بدء التراجع عن إجراءات البرامج الضارة بواسطة مكون الحماية من تهديدات الملفات أو اكتشاف السلوك أو أثناء فحص البرامج الضارة.

يؤثر التراجع عن عمليات البرمجيات الضارة على مجموعة محددة من البيانات. التراجع لا يوجد له تأثيرات سلبية على نظام التشغيل أو على سلامة بيانات جهاز الكمبيوتر.

كيفية تمكين أو تعطيل مكون محرك المعالجة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **محرك المعالجة**.

5. استخدم خانة الاختيار **محرك المعالجة** لتمكين المكون أو تعطيله.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون محرك المعالجة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Remediation Engine**.

5. استخدم مفتاح تبديل **محرك المعالجة** لتمكين المكون أو تعطيله.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون محرك المعالجة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **محرك المعالجة**.

3. استخدم مفتاح تبديل **محرك المعالجة** لتمكين المكون أو تعطيله.

4. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين محرك المعالجة، فسوف يلغي Kaspersky Endpoint Security الإجراءات التي اتخذتها التطبيقات الخبيثة في نظام التشغيل.

Kaspersky Security Network

لحماية الكمبيوتر الخاص بك بشكل أكثر فاعلية، يستخدم برنامج Kaspersky Endpoint Security بيانات تم تلقيها من المستخدمين من جميع أنحاء العالم. تم تصميم Kaspersky Security Network للحصول على هذه البيانات.

تعتبر شبكة Kaspersky Security Network (KSN) بنية تحتية من الخدمات السحابية التي توفر الوصول إلى قاعدة معارف Kaspersky على الإنترنت والتي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج. ويعد استخدام البيانات من Kaspersky Security Network ضمانًا لسرعة وقت استجابات Kaspersky Endpoint Security عند مواجهة تهديدات جديدة، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية ويقلل من خطر وقوع الحالات الإيجابية الزائفة. إذا كنت تشارك في شبكة Kaspersky Security Network، فإن خدمات شبكة KSN تقوم بتزويد برنامج Kaspersky Endpoint Security بمعلومات حول فئة وسمعة الملفات التي تم فحصها، بالإضافة إلى معلومات حول سمعة عناوين الويب التي تم فحصها.

استخدام شبكة Kaspersky Security Network اختياري. يطلب منك التطبيق استخدام KSN أثناء التكوين الأولي للتطبيق. يمكن للمستخدمين بدء المشاركة في KSN وعدم المتابعة في أي وقت.

للحصول على مزيد من المعلومات التفصيلية حول إرسال معلومات إحصائية إلى Kaspersky والتي يتم إنشاؤها أثناء المشاركة في شبكة KSN، وكذلك حول تخزين تلك المعلومات وتدميرها، الرجاء الرجوع إلى بيان Kaspersky Security Network وموقع ويب Kaspersky. يتم تضمين الملف ksn_<language ID>.txt مع نص بيان Kaspersky Security Network في حزمة توزيع التطبيق.

البنية التحتية لقواعد بيانات السمعة من Kaspersky

يدعم Kaspersky Endpoint Security حلول البنية التحتية التالية للعمل مع قواعد بيانات السمعة من Kaspersky:

- Kaspersky Security Network هي المنتج الذي يتم استخدامه من قِبل أغلب تطبيقات Kaspersky. يتسلم المشتركين في شبكة KSN معلومات من Kaspersky ويرسلوا معلومات إلى Kaspersky حول الكائنات التي تم اكتشافها على جهاز كمبيوتر المستخدم ليتم تحليلها بشكل إضافي من قِبل محللي Kaspersky وليتم إدراجها في قواعد بيانات الإحصائية والخاصة بالسمعة.
- Kaspersky Private Security Network عبارة عن حل يتيح لمستخدمي أجهزة الكمبيوتر التي تستضيف Kaspersky Endpoint Security أو غيره من تطبيقات Kaspersky الحصول على حق الوصول إلى قواعد بيانات السمعة من Kaspersky، وإلى البيانات الإحصائية الأخرى دون إرسال بيانات إلى Kaspersky من أجهزة الكمبيوتر الخاصة بهم. وصُممت شبكة KPSN لعملاء الشركات الذين لا يستطيعون المشاركة في شبكة Kaspersky Security Network لأي من الأسباب التالية:
  - محطات العمل المحلية غير متصلة بالإنترنت.
  - يُعتبر نقل أي بيانات خارج البلد أو خارج الشبكة المحلية (LAN) الخاصة بالشركة ممنوعًا بواسطة القانون أو مُقيدًا بواسطة سياسات الأمن الخاصة بالشركة.

افتراضيًا، يستخدم Kaspersky Security Center شبكة KSN. ويمكنك تكوين استخدام شبكة KPSN في وحدة تحكم الإدارة (MMC) في Kaspersky Security Center Web Console وفي سطر الأوامر. ولا يمكن تكوين استخدام شبكة KPSN في Kaspersky Security Center Cloud Console.

للمزيد من التفاصيل عن شبكة KPSN، يُرجى الرجوع إلى الوثائق الموجودة على شبكة Kaspersky Private Security Network.

تمكين وتعطيل استخدام Kaspersky Security Network

لتمكين أو تعطيل استخدام Kaspersky Security Network:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **Kaspersky Security Network**.
3. استخدم مفتاح تبديل **Kaspersky Security Network** لتمكين المكون أو تعطيله.

إذا قمت بتمكين استخدام KSN، فسيعرض Kaspersky Endpoint Security بيان Kaspersky Security Network. يُرجى قراءة شروط استخدام بيان Kaspersky Security Network (KSN) وقبولها إذا كنت توافق عليها.

بشكل افتراضي، Kaspersky Endpoint Security يستخدم وضع KSN الموسع. إن وضع KSN الموسع هو وضع يقوم فيه Kaspersky Endpoint Security بإرسال بيانات إضافية إلى Kaspersky.

4. عند الحاجة، قم بتغيير خانة الاختيار **تمكين وضع KSN الموسع** إلى إيقاف التشغيل.

5. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين استخدام KSN، يستخدم Kaspersky Endpoint Security معلومات حول سمعة الملفات وموارد الويب والتطبيقات المستلمة من Kaspersky Security Network.

قيود Kaspersky Private Security Network

Kaspersky Private Security Network عبارة عن حل يتيح لمستخدمي أجهزة الكمبيوتر التي تستضيف Kaspersky Endpoint Security أو غيره من تطبيقات Kaspersky الحصول على حق الوصول إلى قواعد بيانات السمعة من Kaspersky، وإلى البيانات الإحصائية الأخرى دون إرسال بيانات إلى Kaspersky من أجهزة الكمبيوتر الخاصة بهم. تتيح لك Kaspersky Private Security Network استخدام قاعدة بيانات السمعة المحلية لديك للتحقق من سمعة الكائنات (الملفات أو عناوين الويب). وتتمتع سمعة كائن مضاف إلى قاعدة بيانات السمعة المحلية بأولوية أعلى من هذا المضاف إلى KSN/KPSN. على سبيل المثال، تخيل أن تطبيق Kaspersky Endpoint Security يفحص جهاز كمبيوتر ويطلب سمعة ملف في KSN/KPSN. وإذا كان الملف يتمتع بسمعة غير موثوق في قاعدة بيانات السمعة المحلية لكنه يتمتع بسمعة موثوق في KSN/KPSN، فسيقوم Kaspersky Endpoint Security باكتشاف الملف على أنه غير موثوق وسيتخذ الإجراء المحدد للتهديدات المكتشفة.

مع ذلك، في بعض الحالات، قد لا يطلب Kaspersky Endpoint Security سمعة كائن في KSN/KPSN. وإذا كانت هذه هي الحالة، فلن يتلقى Kaspersky Endpoint Security بيانات من قاعدة بيانات السمعة المحلية على KPSN. قد لا يطلب Kaspersky Endpoint Security سمعة كائن في KSN/KPSN للأسباب التالية:

- تستخدم تطبيقات Kaspersky قواعد بيانات السمعة غير المتصلة بالإنترنت. تم تصميم قواعد بيانات السمعة غير المتصلة بالإنترنت لتحسين الموارد أثناء تشغيل تطبيقات Kaspersky ولحماية الكائنات بالغة الأهمية على الكمبيوتر. ويتم إنشاء قواعد بيانات السمعة غير المتصلة بالإنترنت بواسطة خبراء Kaspersky استنادًا إلى بيانات من Kaspersky Security Network. وتقوم تطبيقات Kaspersky بتحديث قواعد بيانات السمعة غير المتصلة بالإنترنت باستخدام قواعد بيانات مكافحة الفيروسات الخاصة بالتطبيق المحدد. وإذا كانت قواعد بيانات السمعة غير المتصلة بالإنترنت تحتوي على معلومات حول كائن يجري فحصه، فلن يطلب التطبيق سمعة هذا الكائن من KSN/KPSN.

- يتم تكوين استثناءات الفحص (المنطقة الموثوقة) في إعدادات التطبيق. وإذا كانت هذه هي الحالة، فإن التطبيق لا يأخذ في الاعتبار سمعة الكائن في قاعدة بيانات السمعة المحلية.

- يستخدم التطبيق تقنيات تحسين الفحص، مثل iSwift أو iChecker، أو يخزن طلبات السمعة مؤقتًا في KSN / KPSN. وإذا كانت هذه هي الحالة، فقد لا يطلب التطبيق سمعة الكائنات التي تم فحصها مسبقًا.

- لتحسين عبء عمله، يفحص التطبيق الملفات بتنسيق وحجم معينين. ويحدد خبراء Kaspersky قائمة التنسيقات ذات الصلة وحدود الحجم. يتم تحديث هذه القائمة بقواعد بيانات برنامج مكافحة الفيروسات الخاصة بالتطبيق. ويمكنك أيضًا تكوين إعدادات تحسين الفحص في واجهة التطبيق، على سبيل المثال، لمكون الحماية من تهديدات الملفات.

تمكين وتعطيل وضع السحابة لمكونات الحماية

الوضع السحابي تُشير إلى وضع تشغيل التطبيق الذي يستخدم فيه برنامج Kaspersky Endpoint Security إصدارًا خفيفًا من قواعد بيانات مكافحة الفيروسات. تدعم Kaspersky Security Network تشغيل التطبيق عند استخدام إصدار خفيف من قواعد بيانات مكافحة الفيروسات. يُتيح لك الإصدار الخفيف من قواعد بيانات مكافحة الفيروسات استخدام نصف ذاكرة الوصول العشوائي الموجودة بجهاز الكمبيوتر تقريبًا والتي يمكن استخدامها مع قواعد البيانات المعتادة بطريقة أخرى. إذا لم تشارك في Kaspersky Security Network أو إذا تم تعطيل الوضع السحابي، يقوم برنامج Kaspersky Endpoint Security بتنزيل الإصدار الكامل من قواعد بيانات مكافحة الفيروسات من خوادم Kaspersky.

عند استخدام Kaspersky Private Security Network، تتوافر وظيفة وضع السحابة بداية من Kaspersky Private Security Network الإصدار 3.0.

لتمكين أو تعطيل وضع السحابة لمكونات الحماية:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **Kaspersky Security Network**.

3. استخدم مفتاح تبديل **تمكين وضع السحابة** لتمكين المكون أو تعطيله.

4. احفظ تغييراتك.

نتيجة لذلك، يقوم Kaspersky Endpoint Security بتنزيل إصدار خفيف أو إصدار كامل من قواعد بيانات مكافحة الفيروسات أثناء التحديث التالي.

إذا لم يتوفر الإصدار الخفيف من قواعد بيانات مكافحة الفيروسات للاستخدام، فإن Kaspersky Endpoint Security يتحول تلقائيًا إلى الإصدار المميز من قواعد بيانات مكافحة الفيروسات.

إعدادات وكيل KSN

يمكن لأجهزة الكمبيوتر المدارة بواسطة خادم إدارة Kaspersky Security Center التفاعل مع شبكة KSN عبر خدمة وكيل KSN.

توفر خدمة وكيل KSN الإمكانيات التالية:

- يستطيع كمبيوتر المستخدم الاستعلام بسرعة من KSN وتقديم المعلومات إليها، حتى بدون الوصول المباشر إلى الإنترنت.
- تقوم خدمة الوكيل لشبكة KSN بتخزين البيانات المعالجة بشكل مؤقت، مما يؤدي إلى تخفيض التحميل على قناة اتصال الشبكة الخارجية والإسراع بعملية استلام المعلومات التي طلبها جهاز كمبيوتر المستخدم.

افتراضيًا، بعد تمكين KSN وقبول بيان KSN، يستخدم التطبيق خادمًا وكيلاً للاتصال بشبكة Kaspersky Security Network. ويكون الخادم الوكيل الذي يستخدمه التطبيق هو خادم إدارة Kaspersky Security Center عبر منفذ TCP 13111. لذلك، إذا لم يكن وكيل KSN متاحًا، فأنت بحاجة إلى التحقق مما يلي:

- خدمة ksnproxy قيد التشغيل على خادم الإدارة.
- لا يحظر جدار الحماية الموجود على الكمبيوتر المنفذ 13111.

يمكنك تكوين استخدام وكيل KSN على النحو التالي: تمكين أو تعطيل وكيل KSN، وتكوين المنفذ للاتصال. ولفعل ذلك، تحتاج إلى فتح خصائص خادم الإدارة. وللحصول على التفاصيل عن تكوين وكيل KSN، يُرجى الرجوع إلى تعليمات Kaspersky Security Center. ويمكنك أيضًا تمكين أو تعطيل وكيل KSN لأجهزة الكمبيوتر الفردية في سياسة Kaspersky Endpoint Security.

كيفية تمكين أو تعطيل وكيل KSN في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **Kaspersky Security Network**.

5. في القسم **إعدادات وكيل KSN**، استخدم خانة الاختيار **استخدام وكيل شبكة KSN** لتمكين أو تعطيل وكيل KSN.

6. وإذا لزم الأمر، حدد خانة الاختيار **استخدام خوادم شبكة KSN عندما يكون وكيل شبكة KSN غير متاح**.

   إذا تم تحديد خانة الاختيار، سيقوم برنامج Kaspersky Endpoint Security باستخدام خوادم شبكة KSN عند عدم توافر خدمة الوكيل لشبكة KSN. قد يتم وضع خوادم KSN على جانب Kaspersky وعلى جانب أطراف خارجية (عند استخدام Kaspersky Private Security Network).

7. احفظ تغييراتك.

كيفية تمكين أو تعطيل وكيل KSN في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Advanced Threat Protection** ← **Kaspersky Security Network**.

5. استخدم خانة الاختيار **Use KSN Proxy** لتمكين أو تعطيل وكيل KSN.

6. وإذا لزم الأمر، حدد خانة الاختيار **Use KSN servers when KSN Proxy is not available**.

   إذا تم تحديد خانة الاختيار، سيقوم برنامج Kaspersky Endpoint Security باستخدام خوادم شبكة KSN عند عدم توافر خدمة الوكيل لشبكة KSN. قد يتم وضع خوادم KSN على جانب Kaspersky وعلى جانب أطراف خارجية (عند استخدام Kaspersky Private Security Network).

7. احفظ تغييراتك.

يتطابق عنوان وكيل KSN مع عنوان خادم الإدارة. وعندما يتم تغيير اسم مجال خادم الإدارة، فأنت بحاجة إلى تحديث عنوان وكيل KSN يدويًا.

لتكوين عنوان وكيل KSN:

1. في وحدة تحكم الإدارة، انتقل إلى المجلد **خادم الإدارة** ← **إضافي** ← **التثبيت عن بُعد** ← **حزم التثبيت**.

2. في قائمة السياق الخاصة بالمجلد **حزم التثبيت**، حدد **خصائص**.

3. في علامة التبويب **عام** في النافذة المفتوحة، حدد العنوان الجديد لخادم وكيل KSN.

4. احفظ تغييراتك.

التحقق من سمعة أحد الملفات في شبكة Kaspersky Security Network

إذا كنت تشك في أمان ملف، يمكنك التأكد من سمعته باستخدام Kaspersky Security Network.

يمكنك التحقق من سمعة ملف إذا كنت قد وافقت على شروط بيان Kaspersky Security Network.

للتحقق من سمعة ملف في شبكة Kaspersky Security Network:

افتح قائمة السياق للملف وحدد خيار **فحص السمعة في KSN** (اطلع على الشكل أدناه).

قائمة سياق الملف

سيعرض Kaspersky Endpoint Security سمعة الملف:

موثوق (Kaspersky Security Network). أكد معظم مستخدمي Kaspersky Security Network أن الملف موثوق.

برامج قانونية يمكن أن يستخدمها المجرمون لإتلاف جهازك أو بياناتك الشخصية. رغم أنها لا تحتوي على أي وظائف ضارة، إلا أنه المتسللين يستطيعون استغلال هذه التطبيقات. وللحصول على تفاصيل عن البرامج الشرعية التي يمكن أن يستخدمها المجرمون لإلحاق الضرر بالكمبيوتر أو البيانات الشخصية للمستخدم، يرجى الرجوع إلى موقع ويب موسوعة تكنولوجيا معلومات Kaspersky . يمكنك إضافة هذه التطبيقات إلى القائمة الموثوقة.

غير موثوق به (Kaspersky Security Network). فيروس أو تطبيق آخر يمثل تهديدًا.

غير معروف (Kaspersky Security Network). لا تتضمن Kaspersky Security Network أي معلومات عن الملف. ويمكنك فحص ملف باستخدام قواعد بيانات مكافحة الفيروسات (الخيار **فحص للبحث عن الفيروسات** في قائمة السياق).

Kaspersky Endpoint Security يعرض حل KSN الذي تم استخدامه في تحديد سمعة الملف: Kaspersky Security Network أو Kaspersky Private Security Network.

Kaspersky Endpoint Security يعرض كذلك معلومات إضافية عن الملف (راجع الشكل أدناه).

سمعة ملف في Kaspersky Security Network

فحص الاتصالات المشفرة

بعد التثبيت، يضيف Kaspersky Endpoint Security شهادة Kaspersky إلى محزن النظام للحصول على شهادات موثوقة (مخزن شهادات Windows). يستخدم Kaspersky Endpoint Security هذه الشهادة لفحص الاتصالات المشفرة. Kaspersky Endpoint Security يشمل كذلك استخدام تخزين النظام للشهادات الموثوقة في Firefox وThunderbird لفحص المرور على هذه التطبيقات.

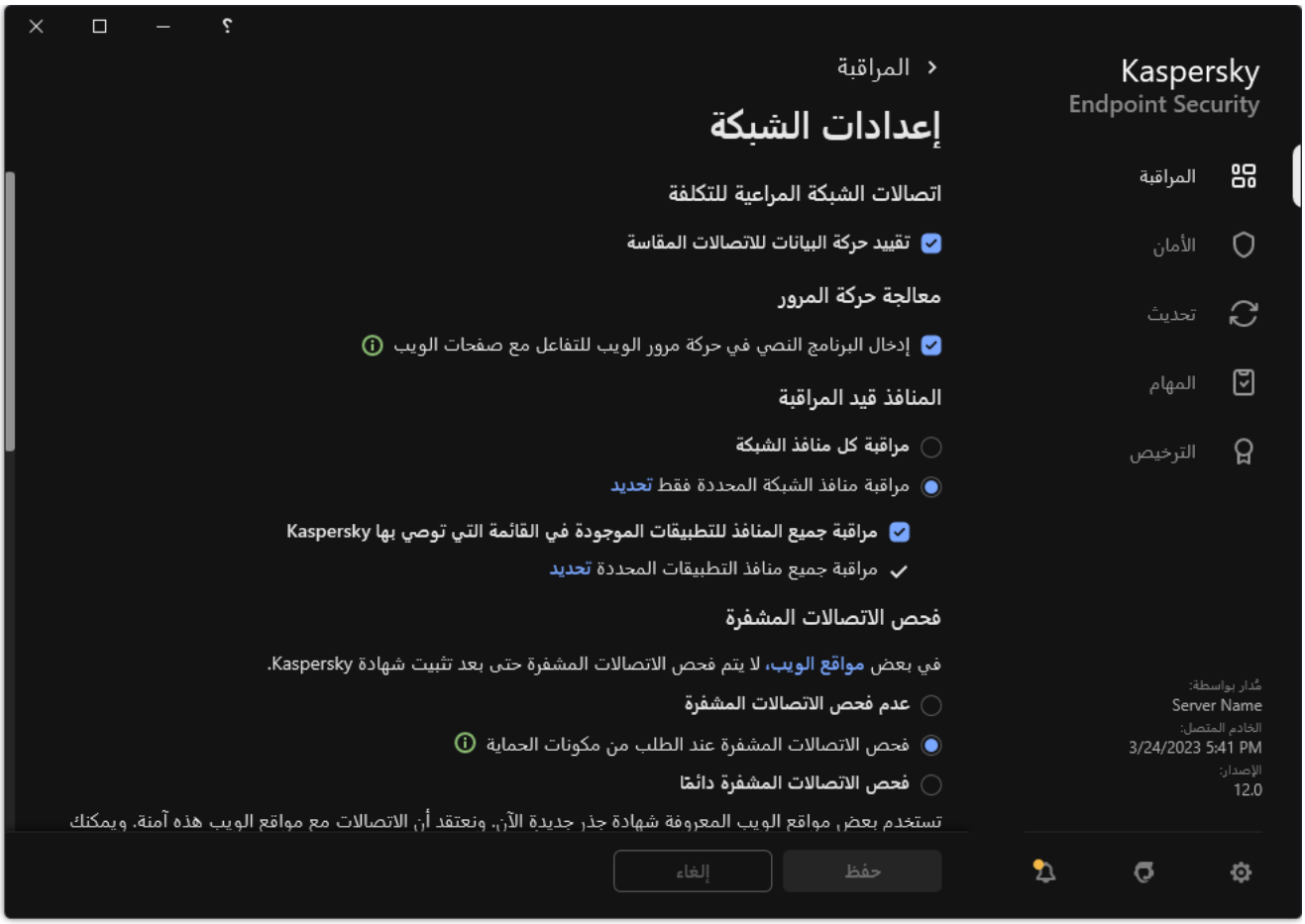
يمكن لمكونات Web Control، والحماية من تهديدات البريد، والحماية من تهديدات الويب فك تشفير وفحص حركة الشبكة المرسلة عبر الاتصالات المشفرة باستخدام البروتوكولات التالية:

- SSL 3.0.
- TLS 1.0، TLS 1.1، TLS 1.2، TLS 1.3.

تمكين فحص الاتصالات المشفرة

لتمكين فحص الاتصالات المشفرة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.



إعدادات فحص الاتصالات المشفرة

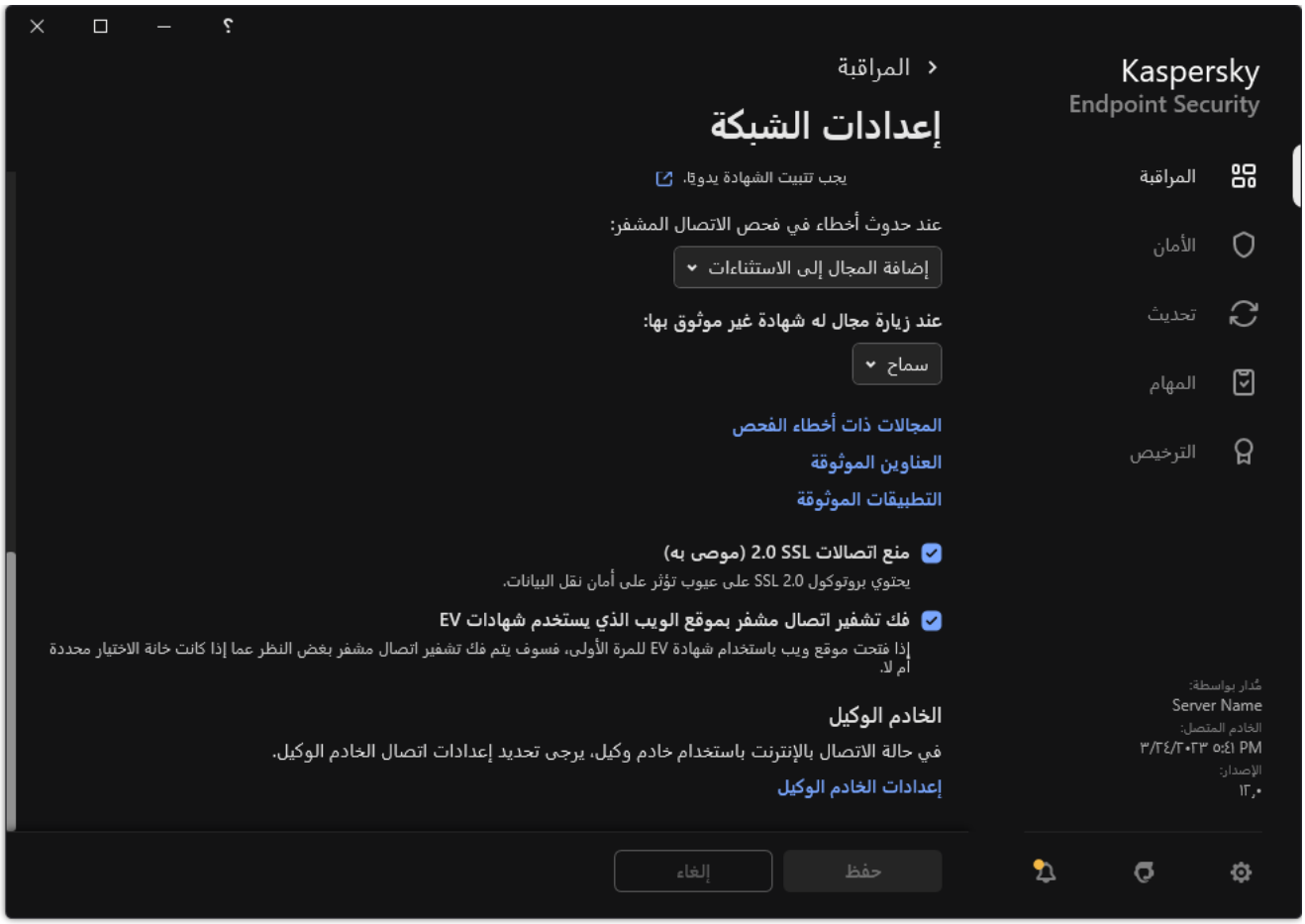
3. في القسم **فحص الاتصالات المشفرة**، حدد وضع فحص الاتصال المشفر:

- **عدم فحص الاتصالات المشفرة**. لن يتمكن Kaspersky Endpoint Security من الوصول إلى محتويات مواقع الويب التي تبدأ بالحروف `https://`.
- **فحص الاتصالات المشفرة عند الطلب من مكونات الحماية**. سوف يفحص Kaspersky Endpoint Security الحركة المشفرة فقط عند طلبها بواسطة مكونات الحماية من تهديدات الويب والحماية من تهديدات البريد والتحكم في الويب.
- **فحص الاتصالات المشفرة دائمًا**. سوف يفحص Kaspersky Endpoint Security حركة شبكة الاتصالات المشفرة حتى إذا تم تعطيل مكونات الحماية.

لا يفحص Kaspersky Endpoint Security الاتصالات المشفرة التي تم إنشاؤها بواسطة تطبيقات موثوقة تم تعطيل فحص حركة مرورها. لا يفحص Kaspersky Endpoint Security الاتصالات المشفرة من قائمة مواقع الويب الموثوقة المحددة مسبقًا. يتم إنشاء القائمة المحددة مسبقًا لمواقع الويب الموثوقة بواسطة خبراء Kaspersky. يتم تحديث هذه القائمة بقواعد بيانات برنامج مكافحة الفيروسات الخاصة بالتطبيق. ويمكنك عرض القائمة المحددة مسبقًا لمواقع الويب الموثوقة فقط في واجهة Kaspersky Endpoint Security. ولا يمكنك عرض القائمة في وحدة تحكم Kaspersky Security Center.

4. يمكنك عند الضرورة إضافة الاستثناءات من الفحص: العناوين والتطبيقات الموثوقة.

5. يمكنك تكوين الإعدادات لفحص الاتصالات المشفرة (انظر الجدول أدناه).



الإعدادات الإضافية لفحص الاتصالات المشفرة

6. احفظ تغييراتك.

إعدادات فحص الاتصالات المشفرة

المعلمة	الوصف
شهادات الجذر الموثوق بها	قائمة شهادات الجذر الموثوق بها. يتيح لك Kaspersky Endpoint Security تثبيت شهادات الجذر الموثوق بها على أجهزة كمبيوتر المستخدم إذا احتجت، على سبيل المثال، إلى نشر مركز شهادات جديد. ويتيح لك التطبيق إضافة شهادة إلى متجر شهادات Kaspersky Endpoint Security خاص. وفي هذه الحالة، تعتبر الشهادة موثوقة فقط لتطبيق Kaspersky Endpoint Security. بمعنى آخر، يستطيع المستخدم الوصول إلى موقع ويب باستخدام الشهادة الجديدة في المستعرض. وإذا حاول تطبيق آخر الوصول إلى موقع الويب، فيمكنك الحصول على خطأ في الاتصال بسبب مشكلة في الشهادة. ولإضافتها إلى مخزن شهادات النظام، يمكنك استخدام سياسات مجموعة Active Directory.
عند زيارة مجال له شهادة غير موثوق بها	• **سماح**. عند زيارة مجال ذو شهادة غير موثوقة، يسمح برنامج Kaspersky Endpoint Security باتصال الشبكة. عند فتح مجال ذو شهادة غير موثوقة في مستعرض، يعرض Kaspersky Endpoint Security صفحة HTML يظهر بها تحذيرًا وسببًا يفسر عدم التوصية بزيارة ذلك المجال. بإمكان المستخدم النقر على الرابط من صفحة HTML التحذيرية للحصول على إمكانية الوصول إلى مورد الويب المطلوب. إذا أنشأ تطبيق أو خدمة تابعة لجهة خارجية اتصالاً بمجال بشهادة غير موثوقة، فإن Kaspersky Endpoint Security ينشئ شهادته الخاصة لفحص حركة المرور. وتكون الشهادة الجديدة غير موثوق. ويعد ذلك ضروريًا لتحذير تطبيق الجهة الخارجية بشأن الاتصال غير الموثوق به لأنه لا يمكن عرض صفحة HTML في هذه الحالة ويمكن إنشاء الاتصال في وضع الخلفية. • **منع الاتصال**. عند زيارة مجال ذو شهادة غير موثوقة، يمنع برنامج Kaspersky Endpoint Security اتصال الشبكة. عند فتح مجال ذو شهادة غير موثوقة في مستعرض، يعرض Kaspersky Endpoint Security صفحة HTML يظهر بها سببًا يفسر منع زيارة ذلك المجال.
عند حدوث أخطاء في	• **منع الاتصال**. إذا تم تحديد هذا العنصر، فعند ظهور خطأ في فحص الاتصالات المشفرة، يقوم Kaspersky Endpoint Security بحظر اتصال الشبكة.

فحص الاتصال المشفر	• **إضافة المجال إلى الاستثناءات**. إذا تم تحديد هذا العنصر، فعند ظهور خطأ في فحص الاتصال المشفر، يضيف Kaspersky Endpoint Security المجال الذي نتج عنه الخطأ إلى قائمة المجالات ذات أخطاء الفحص ولا يقوم بمراقبة نسبة استخدام شبكة الاتصال المشفرة عند زيارة هذا المجال. يمكنك عرض قائمة بمجالات أخطاء فحص الاتصالات المشفرة فقط في الواجهة المحلية الخاصة بالتطبيق. لمسح محتويات القائمة، تحتاج إلى تحديد **منع الاتصال**. ينشئ Kaspersky Endpoint Security أيضًا حدثًا لخطأ فحص الاتصال المشفر.
منع اتصالات SSL 2.0 (موصى به)	في حالة تحديد خانة الاختيار، لن يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 2.0. في حالة إلغاء تحديد خانة الاختيار، لا يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 2.0 ولا يراقب حركة شبكة الاتصال التي تم إرسالها عبر هذه الاتصالات.
فك تشفير اتصال مشفر بموقع الويب الذي يستخدم شهادات EV	تؤكد شهادات EV (شهادات التحقق الموسَّع) مصادقة مواقع الويب وتُحسّن تأمين الاتصال. تستخدم المستعرضات رمز قفل في شريط العناوين للإشارة إلى أن موقع الويب لديه شهادة EV. قد تقوم المستعرضات أيضًا بتلوين شريط العناوين باللون الأخضر كليًا أو جزئيًا. في حالة تحديد خانة الاختيار، يفك التطبيق تشفير الاتصالات المشفرة ويراقبها مع مواقع الويب التي تستخدم شهادة EV. في حالة إلغاء تحديد خانة الاختيار، لن يمتلك للتطبيق حق الوصول إلى المحتويات الخاصة بحركة مرور HTTPS. لهذا السبب، يراقب التطبيق حركة مرور HTTPS فقط بناءً على عنوان موقع الويب، على سبيل المثال، `https://bing.com`. إذا فتحت موقع ويب باستخدام شهادة EV للمرة الأولى، فسوف يتم فك تشفير الاتصال المُشفر بغض النظر عما إذا كانت خانة الاختيار مُحددة أم لا.

تثبيت شهادات الجذر الموثوق بها.

يتيح لك Kaspersky Endpoint Security تثبيت شهادات الجذر الموثوق بها على أجهزة كمبيوتر المستخدم إذا احتجت، على سبيل المثال، إلى نشر مركز شهادات جديد. ويتيح لك التطبيق إضافة شهادة إلى متجر شهادات Kaspersky Endpoint Security خاص. وفي هذه الحالة، تعتبر الشهادة موثوقة فقط لتطبيق Kaspersky Endpoint Security. بمعنى آخر، يستطيع المستخدم الوصول إلى موقع ويب باستخدام الشهادة الجديدة في المستعرض. وإذا حاول تطبيق آخر الوصول إلى موقع الويب، فيمكنك الحصول على خطأ في الاتصال بسبب مشكلة في الشهادة. ولإضافتها إلى مخزن شهادات النظام، يمكنك استخدام سياسات مجموعة Active Directory.

كيفية تثبيت شهادات الجذر الموثوق بها في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.
5. في القسم **شهادات الجذر الموثوق بها**، انقر فوق **إضافة**.
6. يفتح هذا نافذة؛ وفي تلك النافذة، حدد شهادة جذر موثوقًا بها.
   يدعم Kaspersky Endpoint Security الشهادات بملحقات PEM وDER وCRT.
7. احفظ تغييراتك.

كيفية تثبيت شهادات الجذر الموثوق بها في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General settings** ← **Network Settings**.
5. انقر على رابط **Trusted root certificates**.
6. يفتح هذا نافذة؛ وفي تلك النافذة، انقر فوق **Add** وحدد شهادة جذر موثوقًا بها.
يدعم Kaspersky Endpoint Security الشهادات بملحقات PEM وDER وCRT.
7. احفظ تغييراتك.

كيفية تثبيت شهادات الجذر الموثوق بها في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.
3. في القسم **فحص الاتصالات المشفرة**، انقر على الزر **إظهار الشهادات**.
4. يفتح هذا نافذة؛ وفي تلك النافذة، انقر فوق **إضافة** وحدد شهادة جذر موثوقًا بها.
يدعم Kaspersky Endpoint Security الشهادات بملحقات PEM وDER وCRT.
5. احفظ تغييراتك.

نتيجة لذلك، عند فحص حركة المرور، بالإضافة إلى مخزن شهادات النظام، يستخدم Kaspersky Endpoint Security مخزن الشهادات الخاص به.

فحص الاتصالات المشفرة التي تتضمن شهادة غير موثوقة

بعد التثبيت، يضيف Kaspersky Endpoint Security شهادة Kaspersky إلى محزن النظام للحصول على شهادات موثوقة (مخزن شهادات Windows). يستخدم Kaspersky Endpoint Security هذه الشهادة لفحص الاتصالات المشفرة. وعند زيارة مجال له شهادة غير موثوق بها، يمكنك السماح أو وصول المستخدم إلى هذا المجال أو رفض وصوله (راجع التعليمات أدناه).

إذا سمحت للمستخدم بزيارة المجالات ذات الشهادات غير الموثوقة، فسينفذ Kaspersky Endpoint Security الإجراءات التالية:

- عند زيارة مجال له شهادة غير موثوق بها في المستعرض، يستخدم Kaspersky Endpoint Security شهادة Kaspersky لفحص حركة المرور. ويعرض Kaspersky Endpoint Security صفحة HTML مع تحذير ومعلومات حول سبب عدم التوصية بزيارة المجال ذي الصلة (انظر الشكل أدناه). بإمكان المستخدم النقر على الرابط من صفحة HTML التحذيرية للحصول على إمكانية الوصول إلى مورد الويب المطلوب. بعد اتباع هذا الرابط، وفي خلال الساعة التالية، لن يعرض Kaspersky Endpoint Security تحذيرات بشأن شهادة غير موثوقة عند زيارة موارد أخرى في نفس هذا المجال. زينشئ Kaspersky Endpoint Security أيضًا حدثًا حول إنشاء اتصال مشفر بشهادة غير موثوق بها.
- إذا أنشأ تطبيق أو خدمة تابعة لجهة خارجية اتصالاً بمجال بشهادة غير موثوقة، فإن Kaspersky Endpoint Security ينشئ شهادته الخاصة لفحص حركة المرور. وتكون الشهادة الجديدة غير موثوقة. ويعد ذلك ضروريًا لتحذير تطبيق الجهة الخارجية بشأن الاتصال غير الموثوق به لأنه لا يمكن عرض

صفحة HTML في هذه الحالة ويمكن إنشاء الاتصال في وضع الخلفية. لذلك، إذا كان لدى تطبيق جهة خارجية أدوات مضمنة للتحقق من الشهادة، فقد يتم إنهاء الاتصال. وفي هذه الحالة، يجب عليك الاتصال بمالك المجال وإعداد اتصال موثوق. وإذا كان إعداد اتصال موثوق مستحيلاً، يمكنك إضافة تطبيق الجهة الخارجية هذا إلى قائمة التطبيقات الموثوقة. زينشئ Kaspersky Endpoint Security أيضًا حدثًا حول إنشاء اتصال مشفر بشهادة غير موثوق بها.

كيفية تكوين فحص الاتصالات المشفرة بشهادة غير موثوقة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.
5. في القسم **فحص الاتصالات المشفرة**، انقر على الزر **إعدادات متقدمة**.
6. في النافذة التي تفتح، حدد وضع تشغيل التطبيق عند زيارة مجال له شهادة غير موثوق بها: **سماح** أو **منع الاتصال**.
7. احفظ تغييراتك.

كيفية تكوين فحص الاتصالات المشفرة بشهادة غير موثوقة في Cloud Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General settings** ← **Network Settings**.
5. في القسم **Encrypted connections scan** ، حدد وضع تشغيل التطبيق عند زيارة مجال له شهادة غير موثوق بها: **Allow** أو **Block connection**.
6. احفظ تغييراتك.

كيفية تكوين فحص الاتصالات المشفرة بشهادة غير موثوقة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.
3. في القسم **فحص الاتصالات المشفرة**، حدد وضع تشغيل التطبيق عند زيارة مجال له شهادة غير موثوق بها: **Allow** أو **Block connection**.
4. احفظ تغييراتك.

تحذير عند زيارة مجال له شهادة غير موثوق بها

فحص الاتصالات المشفرة في Firefox وThunderbird

بعد التثبيت، يضيف Kaspersky Endpoint Security شهادة Kaspersky إلى محزن النظام للحصول على شهادات موثوقة (مخزن شهادات Windows). وبشكل افتراضي، يستخدم Firefox وThunderbird مخزن شهادات Mozilla الخاص بهما بدلاً من مخزن شهادات Windows. وفي حالة نشر Kaspersky Security Center في مؤسستك وتم تطبيق سياسة على جهاز كمبيوتر، فإن Kaspersky Endpoint Security يقوم تلقائيًا بتمكين استخدام مخزن شهادات Windows في Firefox وThunderbird لفحص حركة مرور هذه التطبيقات. وإذا لم يتم تطبيق سياسة ما على الكمبيوتر، فيمكنك اختيار تخزين الشهادة الذي ستستخدمه تطبيقات Mozilla. وإذا حددت مخزن شهادات Mozilla، فأضف شهادة Kaspersky يدويًا إليه. وسيساعد هذا في تجنب الأخطاء عند العمل مع حركة مرور HTTPS.

لفحص حركة المرور في مستعرض Mozilla Firefox وعميل البريد Thunderbird، يجب عليك تمكين فحص الاتصالات المشفرة. وفي حالة تعطيل فحص الاتصالات المشفرة، لا يفحص التطبيق حركة المرور في مستعرض Mozilla Firefox وعميل البريد Thunderbird.

قبل إضافة شهادة إلى مخزن Mozilla، قم بتصدير شهادة Kaspersky من لوحة تحكم Windows (خصائص المستعرض). للحصول على تفاصيل عن تصدير شهادة Kaspersky، يُرجى الرجوع إلى قاعدة معارف الدعم الفني. للحصول على التفاصيل حول إضافة شهادة إلى المخزن، يرجى زيارة موقع ويب الدعم الفني من Mozilla.

يمكنك اختيار مخزن الشهادات فقط في الواجهة المحلية للتطبيق.

لاختيار مخزن شهادات لفحص الاتصالات المشفرة في Firefox وThunderbird:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.
3. في القسم **Mozilla Firefox وThunderbird**، حدد خانة الاختيار **استخدام مخزن الشهادات المحدد لفحص الاتصالات المشفرة في تطبيقات Mozilla**.

4. تحديد مخزن شهادات:

- **استخدام مخزن شهادات Windows (مستحسن)**. تتم إضافة شهادة جذر Kaspersky إلى هذا المخزن أثناء تثبيت Kaspersky Endpoint Security.
- **استخدام مخزن شهادات Mozilla**. يستخدم Mozilla Firefox وThunderbird مخازن الشهادات الخاصة بهما. في حالة تحديد مخزن شهادات Mozilla، ستحتاج إلى إضافة شهادة جذر Kaspersky يدويًا إلى هذا المخزن من خلال خصائص المستعرض.

5. احفظ تغييراتك.

استثناء الاتصالات المشفرة من الفحص

معظم موارد الويب تستخدم اتصالات مشفرة. يوصيك خبراء Kaspersky بتفعيل فحص الاتصالات المشفرة. وفي حالة تداخل فحص الاتصالات المشفرة مع نشاط مرتبط بالعمل، يمكنك إضافة موقع إلكتروني إلى الاستثناءات المشار إليها باسم العناوين الموثوقة. وفي هذه الحالة، لا يفحص Kaspersky Endpoint Security حركة مرور HTTPS لعناوين الويب الموثوقة عندما يؤدي مكونات الحماية من تهديدات الويب والحماية من تهديدات البريد والتحكم في الويب عملها.

في حال وجود تطبيق موثوق يستخدم اتصال مشفر، يمكنك تعطيل فحص الاتصالات المشفرة للتطبيق. على سبيل المثال: يمكنك تعطيل فحص الاتصالات المشفرة لتطبيقات التخزين السحابي التي تستخدم المصادقة ثنائية العوامل لشهادتها الخاصة.

كيفية استثناء عنوان ويب من عمليات فحص الاتصال المشفر في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.

5. في القسم **فحص الاتصالات المشفرة**، انقر على الزر **العناوين الموثوقة**.

6. انقر على **إضافة**.

7. أدخل اسم مجال أو عنوان IP إذا لم ترغب في أن يقوم Kaspersky Endpoint Security بفحص الاتصالات المشفرة التي تم إنشاؤها عند زيارة هذا المجال.

يدعم Kaspersky Endpoint Security حرف `*` لإدخال قناع في اسم المجال.

لا يدعم Kaspersky Endpoint Security رموز `*` لعناوين IP. ويمكنك تحديد نطاق من عناوين IP باستخدام القناع الشبكة الفرعية (على سبيل المثال، 198.51.100.0/24).

أمثلة:

- `domain.com` - يتضمن السجل العناوين التالية: `https://domain.com` و`https://www.domain.com` و`https://domain.com/page123`. ولا يتضمن السجل المجالات الفرعية (على سبيل المثال، `subdomain.domain.com`).
- `subdomain.domain.com` - يتضمن السجل العناوين التالية: `https://subdomain.domain.com` و`https://subdomain.domain.com/page123`. السجل حصري لمجال `domain.com`.
- `*.domain.com` - يتضمن السجل العناوين التالية: `https://movies.domain.com` و`https://images.domain.com/page123`. السجل حصري لمجال `domain.com`.

8. احفظ تغييراتك.

[كيفية استثناء عنوان ويب من عمليات فحص الاتصال المشفر في Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Network Settings**.

5. في القسم **Encrypted connections scan**، انقر على الزر **Trusted addresses**.

6. انقر على **Add**.

7. أدخل اسم مجال أو عنوان IP إذا لم ترغب في أن يقوم Kaspersky Endpoint Security بفحص الاتصالات المشفرة التي تم إنشاؤها عند زيارة هذا المجال.
يدعم Kaspersky Endpoint Security حرف `*` لإدخال قناع في اسم المجال.

> لا يدعم Kaspersky Endpoint Security رموز `*` لعناوين IP. ويمكنك تحديد نطاق من عناوين IP باستخدام القناع الشبكة الفرعية (على سبيل المثال، 198.51.100.0/24).

أمثلة:

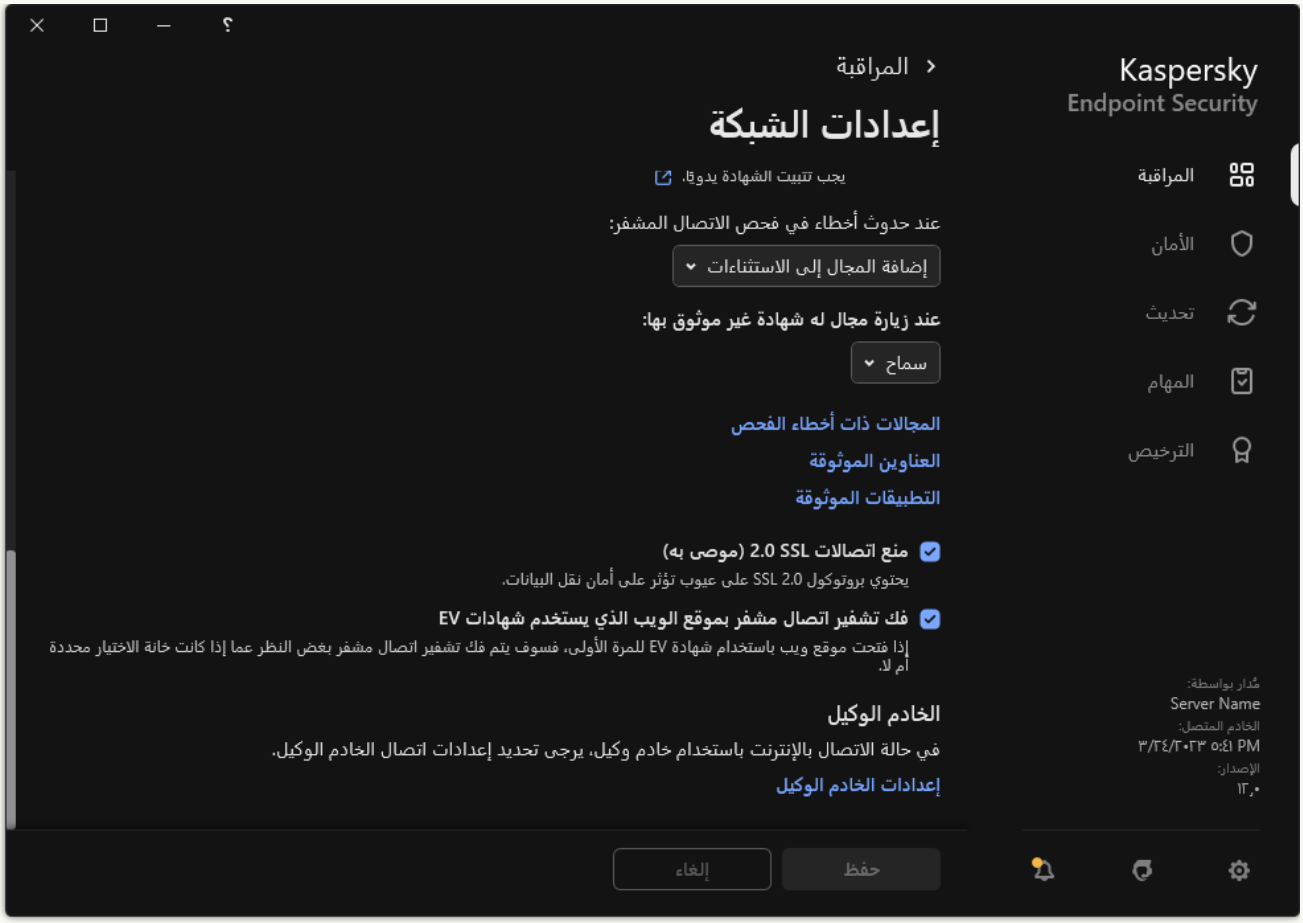
- `domain.com` - يتضمن السجل العناوين التالية: `https://domain.com` و`https://www.domain.com` و`https://domain.com/page123`. ولا يتضمن السجل المجالات الفرعية (على سبيل المثال، `subdomain.domain.com`).
- `subdomain.domain.com` - يتضمن السجل العناوين التالية: `https://subdomain.domain.com` و`https://subdomain.domain.com/page123`. السجل حصري لمجال `domain.com`.
- `*.domain.com` - يتضمن السجل العناوين التالية: `https://movies.domain.com` و`https://images.domain.com/page123`. السجل حصري لمجال `domain.com`.

8. احفظ تغييراتك.

كيفية استثناء عنوان ويب من عمليات فحص الاتصال المشفر في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.



إعدادات شبكة التطبيق

3. في القسم **فحص الاتصالات المشفرة**، انقر على الزر **العناوين الموثوقة**.

4. انقر على **إضافة**.

5. أدخل اسم مجال أو عنوان IP إذا لم ترغب في أن يقوم Kaspersky Endpoint Security بفحص الاتصالات المشفرة التي تم إنشاؤها عند زيارة هذا المجال.

يدعم Kaspersky Endpoint Security حرف `*` لإدخال قناع في اسم المجال.

لا يدعم Kaspersky Endpoint Security رموز `*` لعناوين IP. ويمكنك تحديد نطاق من عناوين IP باستخدام القناع الشبكة الفرعية (على سبيل المثال، 198.51.100.0/24).

أمثلة:

- `domain.com` - يتضمن السجل العناوين التالية: `https://domain.com` و`https://www.domain.com` و`https://domain.com/page123`. ولا يتضمن السجل المجالات الفرعية (على سبيل المثال، `subdomain.domain.com`).
- `subdomain.domain.com` - يتضمن السجل العناوين التالية: `https://subdomain.domain.com` و`https://subdomain.domain.com/page123`. السجل حصري لمجال `domain.com`.
- `*.domain.com` - يتضمن السجل العناوين التالية: `https://movies.domain.com` و`https://images.domain.com/page123`. السجل حصري لمجال `domain.com`.

6. احفظ تغييراتك.

الوضع الافتراضي أن Kaspersky Endpoint Security لا يفحص الاتصالات المشفرة عند حدوث أخطاء، ويضيف الموقع إلى قائمة خاصة من المجالات ذات أخطاء الفحص. يقوم Kaspersky Endpoint Security بتشكيل قائمة منفصلة لكل مستخدم ولا يرسل البيانات إلى Kaspersky Endpoint Security. يمكنك تفعيل حجب الاتصال عند حدوث خطأ في الفحص. يمكنك عرض قائمة بمجالات أخطاء فحص الاتصالات المشفرة فقط في الواجهة المحلية الخاصة بالتطبيق.

لعرض قائمة المجالات ذات أخطاء الفحص:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.

3. في القسم **فحص الاتصالات المشفرة**، انقر على الزر **المجالات ذات أخطاء الفحص**.

سوف تفتح قائمة بالمجالات ذات أخطاء الفحص. لإعادة تعيين هذه القائمة، قم بتفعيل حجب الاتصال عند حدوث أخطاء في الفحص في السياسة وطبق السياسة ثم أعد ضبط المعامل إلى قيمته الأولية وطبق السياسة مرة أخرى.

لقد أنشأ متخصصو Kaspersky قائمة من الاستثناءات العامة — المواقع الموثوقة التي لا يفحصها Kaspersky Endpoint Security بغض النظر عن إعدادات التطبيق.

لعرض الاستثناءات العامة من فحص حركة المرور المشفرة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.

3. في القسم **فحص الاتصالات المشفرة**، انقر على الرابط مواقع الويب الموثوقة.

يفتح هذا قائمة بمواقع الويب التي جمعها خبراء Kaspersky. لا يفحص Kaspersky Endpoint Security الاتصالات المحمية لمواقع الويب المدرجة في القائمة. قد يتم تحديث القائمة عندما يتم تحديث قواعد البيانات والوحدات النمطية لتطبيق Kaspersky Endpoint Security.

مسح البيانات

يُتيح لك برنامج Kaspersky Endpoint Security استخدام مهمة لحذف البيانات عن بُعد من كمبيوتر المستخدم.

يقوم برنامج Kaspersky Endpoint Security بحذف البيانات على النحو التالي:

- في الوضع الصامت؛
- على محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة؛
- لجميع حسابات المستخدمين على الكمبيوتر.

يقوم برنامج Kaspersky Endpoint Security بمهمة مسح البيانات بغض النظر عن نوع الترخيص الذي يتم استخدامه، حتى بعد انتهاء صلاحية الترخيص.

أوضاع مسح البيانات

تُمكنك هذه المهمة من حذف البيانات في الأوضاع التالية:

- حذف البيانات بشكل فوري.

في هذا الوضع، على سبيل المثال، يُمكنك حذف البيانات القديمة لتفريغ مساحة على القرص.

- حذف البيانات المؤجل.

يختص هذا الوضع، على سبيل المثال، بحماية البيانات الموجودة على الكمبيوتر المحمول في حال فقدانه أو سرقته. يُمكنك تكوين حذف البيانات التلقائي إذا كان الكمبيوتر المحمول موجود خارج حدود شبكة الشركة ولم تتم مزامنته مع Kaspersky Security Center منذ وقت طويل.

لا يمكن تعيين جدول زمني لحذف البيانات في خصائص المهمة. يمكنك فقط حذف البيانات مباشرةً بعد بدء المهمة يدويًا، أو تكوين حذف البيانات المؤجل إذا لم يوجد اتصال بـKaspersky Security Center.

قيود

يخضع مسح البيانات إلى القيود التالية:

- لا يمكن إلا لمدير Kaspersky Security Center إدارة مهمة مسح البيانات. لا يمكنك تكوين أو بدء مهمة في الواجهة المحلية لـ Kaspersky Endpoint Security.
- في نظام الملفات NTFS، يحذف Kaspersky Endpoint Security أسماء تدفقات البيانات الرئيسية فقط. ولا يمكن حذف أسماء تدفقات البيانات البديلة.
- عندما تحذف ملف الرابط الرمزي، يحذف Kaspersky Endpoint Security أيضًا الملفات التي تم تحديد مساراتها في الرابط الرمزي.

إنشاء مهمة مسح بيانات

لمسح البيانات الموجودة على كمبيوتر المستخدم:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.
تفتح قائمة المهام.
2. انقر على الزر **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.
   b. في القائمة المنسدلة **Task type** حدد **Wipe data**.
   c. في الحقل **Task name** ، أدخل وصفًا موجزًا، على سبيل المثال، مسح البيانات (مكافحة السرقة).
   d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.

إذا تمت إضافة أجهزة كمبيوتر جديدة إلى مجموعة الإدارة خلال نطاق المهمة، يتم تشغيل مهمة حذف البيانات بشكل فوري على أجهزة الكمبيوتر الجديدة فقط إذا اكتملت المهمة خلال 5 دقائق من إضافة أجهزة الكمبيوتر الجديدة.

5. أغلق المعالج.

سيتم عرض مهمة جديدة في قائمة المهام.

6. انقر فوق المهمة **Wipe data** في برنامج Kaspersky Endpoint Security.
نافذة خصائص المهمة.

7. حدد علامة التبويب **Application settings**.

8. حدد طريقة حذف البيانات:

- **Delete by means of the operating system**. يستخدم برنامج Kaspersky Endpoint Security موارد نظام التشغيل لحذف الملفات دون إرسالهم إلى سلة المحذوفات.
- **Delete completely, no recovery possible**. يستبدل برنامج Kaspersky Endpoint Security الملفات باستخدام بيانات عشوائية. من المستحيل عمليا استعادة البيانات بعد حذفها.

9. إذا أردت تأجيل حذف البيانات، حدد خانة الاختيار **Automatically wipe data when there is no connection to Kaspersky Security Center for more than N days**. حدد عدد الأيام.

سيتم تنفيذ مهمة حذف البيانات المؤجلة في كل مرة لا يتواجد اتصال بـ Kaspersky Security Center للمدة الزمنية المُحددة.

عند تكوين مهمة حذف البيانات المؤجلة، ضع في اعتبارك أن الموظفين قد يقوموا بإيقاف تشغيل أجهزة الكمبيوتر الخاصة بهم قبل ذهابهم في عطلة. في هذه الحالة، قد تمتد المدة التي يكون بها الاتصال غير موجود وسيتم حذف البيانات. ضع في اعتبارك أيضًا جدول الأعمال الخاص بالمستخدمين غير المتصلين. للمزيد من التفاصيل عن العمل مع أجهزة الكمبيوتر غير المتصلة بالإنترنت والمستخدمين خارج المكتب، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

في حالة إلغاء تحديد خانة الاختيار، سيتم تنفيذ المهمة على الفور بعد إجراء مزامنة مع Kaspersky Security Center.

10. إنشاء قائمة بالكائنات التي ستقوم بحذفها:

- **المجلدات**. يحذف برنامج Kaspersky Endpoint Security جميع الملفات الموجودة في المجلدات، والمجلدات الفرعية. لا يدعم Kaspersky Endpoint Security استخدام الأقنعة ومتغيرات البيئة لإدخال مسار المجلد.
- **الملفات حسب الملحق**. يقوم برنامج Kaspersky Endpoint Security بالبحث عن ملفات باستخدام الامتدادات المحددة على جميع محركات أقراص الكمبيوتر، بما في ذلك محركات الأقراص القابلة للإزالة. استخدم الأحرف "؛" أو "،" لتحديد امتدادات متعددة.
- **النطاق المحدد مسبقًا**. Kaspersky Endpoint Security سوف يحذف ملفات من المناطق التالية:
  - **Documents**. الملفات في مجلد المستندات القياسي لنظام التشغيل والمجلدات الفرعية به.
  - **Cookies**. الملفات التي يقوم المستعرض فيها بحفظ البيانات التي يجمعها من المواقع التي يزورها المستخدم (مثل بيانات مصادقة المستخدم).
  - **Desktop**. الملفات في مجلد سطح المكتب القياسي لنظام التشغيل والمجلدات الفرعية به.
  - **Temporary Internet Explorer files**. الملفات المؤقتة المتعلقة بعمل مستعرض Internet Explorer، مثل نسخ صفحات الويب والصور وملفات الوسائط.
  - **Temporary files**. الملفات المؤقتة المتعلقة بعمل التطبيقات المثبتة على الكمبيوتر. على سبيل المثال: تطبيقات Microsoft Office تنشئ ملفات مؤقتة تحتوي على نسخ احتياطية من المستندات.
  - **Outlook files**. الملفات المتعلقة بعمل عميل بريد Outlook: ملفات البيانات (PST)، وملفات بيانات عدم الاتصال (OST)، وملفات دفتر العناوين غير المتصل (OAB)، وملفات دفتر العناوين الشخصي (PAB).
  - **User profile**. مجموعة من الملفات والمجلدات التي تقوم بتخزين إعدادات نظام التشغيل الخاصة بحساب المستخدم المحلي.

يمكنك إنشاء قائمة بالكائنات التي ستقوم بحذفها في كل علامة تبويب. سيقوم Kaspersky Endpoint Security بإنشاء قائمة موحدة وسيحذف ملفات من القائمة عند إكمال مهمة.

لا يمكنك حذف الملفات المطلوبة لتشغيل Kaspersky Endpoint Security.

11. احفظ تغييراتك.

12. حدد خانة الاختيار المجاورة للمهمة.

13. انقر على الزر **Run**.

كنتيجة لذلك، سيتم حذف البيانات الموجودة على أجهزة كمبيوتر المستخدمين وذلك وفقًا للوضع المُحدد: بشكل فوري أو في حالة عدم وجود اتصال. إذا لم يتمكن برنامج Kaspersky Endpoint Security من حذف ملف ما، مثلًا عندما يستخدم المستخدم ملفًا في الوقت الحالي، لن يحاول التطبيق حذفه مرة أخرى. لإكمال حذف البيانات، قم بتشغيل المهمة مرة أخرى.

التحكم في الويب

يقوم المكون التحكم في الويب بإدارة وصول المستخدمين إلى موارد الويب. هذا يساعد على تقليل حركة المرور والاستخدام غير المناسب لوقت العمل. عندما يحاول مستخدم فتح موقع إلكتروني محجوب من التحكم في الويب، فإن Kaspersky Endpoint Security سوف يحجب الوصول إلى ذلك الموقع أو يعرض تحذيرًا (راجع الشكل أدناه).

يراقب برنامج Kaspersky Endpoint Security حركة مرور HTTP، وHTTPS فقط.

لمراقبة حركة مرور HTTPS، تحتاج إلى تمكين عمليات فحص الاتصالات المشفرة.

طرق لإدارة الوصول إلى مواقع الويب

يُتيح لك المكون التحكم في الويب تكوين الوصول إلى مواقع الويب باستخدام الطرق التالية:

- **فئة موقع الويب**. يتم تصنيف مواقع الويب وفقًا لخدمة سحابة Kaspersky Security Network، والتحليل الموجه، وقاعدة بيانات المواقع المعروفة (المُضمنة في قواعد بيانات التطبيق). على سبيل المثال، يمكنك تقييد وصول المستخدم إلى فئة الشبكات الاجتماعية أو إلى فئات أخرى.
- **نوع البيانات**. يمكنك تقييد وصول المستخدمين إلى البيانات الموجودة على موقع الويب، وإخفاء الصور الرسومية، على سبيل المثال. يحدد برنامج Kaspersky Endpoint Security نوع البيانات بناءً على تنسيق الملف وليس بناءً على ملحقاته.

لا يفحص برنامج Kaspersky Endpoint Security الملفات الموجودة في الأرشيفات. على سبيل المثال، إذا تم وضع ملفات الصور في الأرشيف، فإن برنامج Kaspersky Endpoint Security يحدد نوع البيانات لتكون الأرشيفات وليس الرسومات.

- **العنوان الفردي**. يمكنك إدخال عنوان الويب أو استخدام الأقنعة.

يمكنك في الوقت نفسه استخدام طرق متعددة لتنظيم الوصول إلى مواقع الويب. على سبيل المثال، يمكنك تقييد الوصول إلى نوع البيانات "ملفات Office" وحصره فقط على فئة موقع الويب البريد الإلكتروني على الويب.

قواعد الوصول لموقع الويب

يقوم المكون التحكم في الويب بإدارة وصول المستخدم إلى مواقع الويب باستخدام قواعد الوصول. يمكنك تكوين الإعدادات المتقدمة التالية الخاصة بقاعدة الوصول إلى موقع الويب:

- المستخدمين الذين تنطبق عليهم القاعدة.

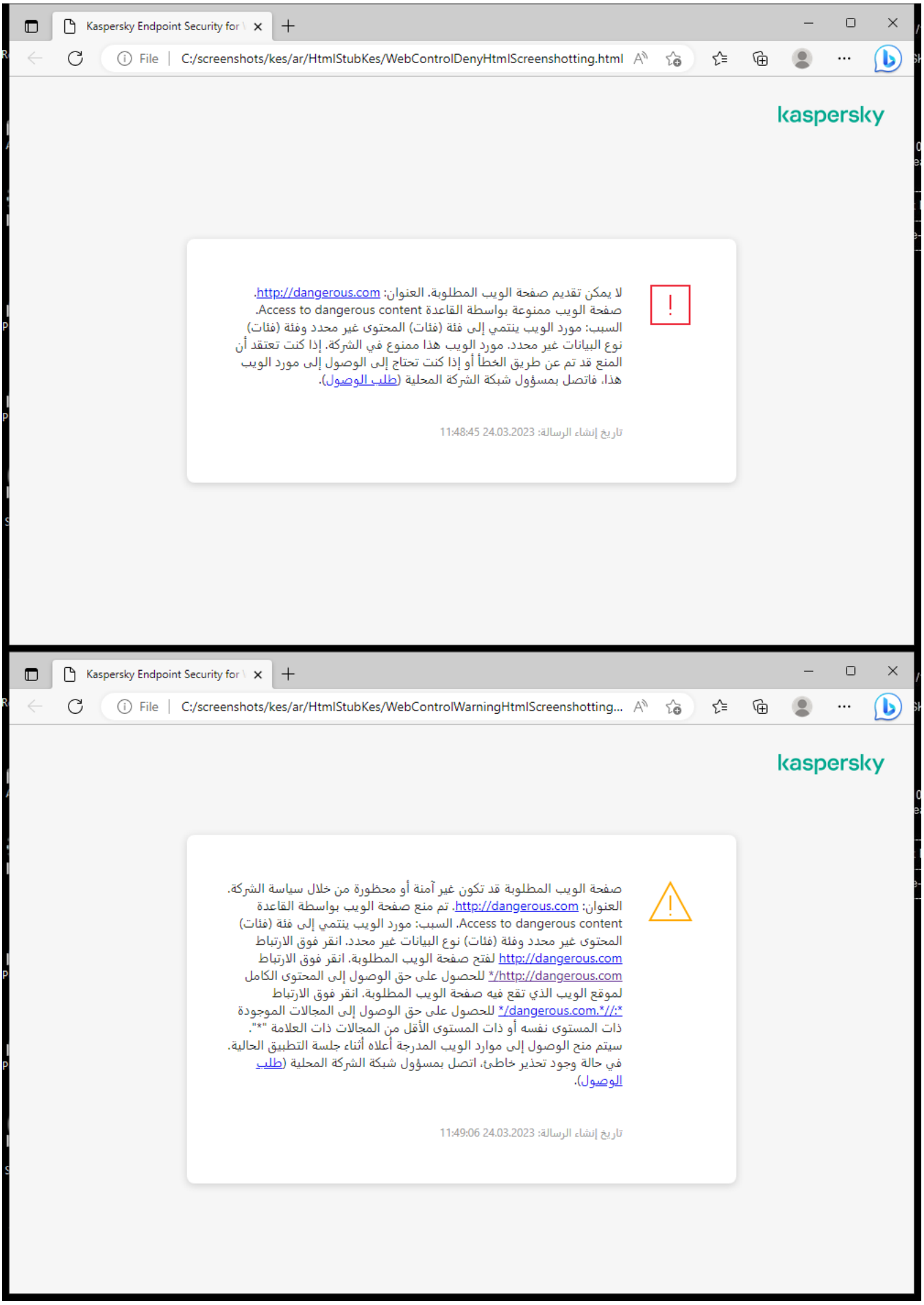
  على سبيل المثال، يمكنك تقييد وصول جميع مستخدمي الشركة إلى الإنترنت من خلال المستعرض باستثناء قسم تكنولوجيا المعلومات.

- جدول القاعدة.

  على سبيل المثال، يمكنك تقييد الوصول إلى الإنترنت من خلال المستعرض خلال ساعات العمل فقط.

أولوية قاعدة الوصول

لكل قاعدة أولوية. كلما كانت القاعدة تحتل مرتبة أعلى في القائمة، فإنها تكون ذات أولوية أعلى. إذا تمت إضافة موقع ويب إلى قواعد متعددة، ينظم المكون التحكم في الويب الوصول إلى موقع الويب بناءً إلى القاعدة ذات أعلى أولوية. على سبيل المثال، قد يحدد برنامج Kaspersky Endpoint Security بوابة شركة لتكون شبكة اجتماعية. لتقييد الوصول إلى الشبكات الاجتماعية وتوفير الوصول إلى بوابة الويب الخاصة بالشركة، قم بإنشاء قاعدتين: قاعدة واحدة لحظر الوصول إلى فئة موقع الويب الشبكات الاجتماعية وقاعدة واحدة للسماح بالوصول إلى بوابة الويب الخاصة بالشركة. يجب أن يكون لقاعدة الوصول لبوابة الويب الخاصة بالشركة أولوية أعلى من قاعدة الوصول إلى الشبكات الاجتماعية.



رسائل التحكم في الويب

تمكين وتعطيل التحكم في الويب

افتراضيًا، يتم تمكين التحكم في الويب.

لتمكين أو تعطيل التحكم في الويب:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.
3. استخدم مفتاح تبديل **التحكم في الويب** لتمكين المكون أو تعطيله.
4. احفظ تغييراتك.

الإجراءات المتبعة مع قواعد الوصول إلى موارد الويب

من غير المستحسن إنشاء أكثر من 1000 قاعدة للوصول إلى موارد الويب لأن هذا قد يتسبب في جعل النظام غير مستقر.

قاعدة الوصول إلى موارد الويب هي مجموعة من عوامل التصفية والإجراءات التي يجريها Kaspersky Endpoint Security عندما يزور المستخدم موارد الويب الموضحة في القاعدة أثناء الفترة الزمنية المشار إليها في جدولة القاعدة. تتيح لك عوامل التصفية التحديد الدقيق لمجموعة من موارد الويب التي يتم التحكم في الوصول إليها عبر مكون التحكم في الويب.

تتوافر عوامل التصفية التالية:

- **التصفية حسب المحتوى**. يصنف التحكم في الويب موارد الويب حسب المحتوى ونوع البيانات. يمكنك التحكم في وصول المستخدم إلى موارد الويب التي تضم محتوى وبيانات تندرج ضمن أنواع محددة بواسطة هذه الفئات. عندما يزور المستخدمون موارد الويب التي تنتمي إلى فئة المحتوى المحدد و/أو فئة نوع البيانات، يتخذ Kaspersky Endpoint Security الإجراء المحدد في القاعدة.
- **التصفية حسب عناوين موارد الويب**. يمكنك التحكم في وصول مستخدم إلى كل عناوين موارد الويب أو إلى عناوين موارد ويب مفردة و/أو مجموعات من عناوين موارد الويب.

  إذا تم تحديد التصفية حسب المحتوى والتصفية حسب عناوين موارد الويب، وكانت عناوين موارد الويب المحددة و/أو مجموعات عناوين موارد الويب تنتمي إلى فئات المحتويات أو فئات أنواع البيانات المحددة، فلا يتحكم Kaspersky Endpoint Security في الوصول إلى كل موارد الويب في فئات المحتويات و/أو فئات أنواع البيانات المحددة. بدلاً من ذلك، يتحكم التطبيق فقط في الوصول إلى عناوين موارد الويب و/أو مجموعات عناوين موارد الويب المحددة.
- **التصفية حسب أسماء المستخدمين ومجموعات المستخدمين**. يمكنك تحديد أسماء المستخدمين و/أو مجموعات المستخدمين الذين يتم التحكم في وصولهم إلى موارد الويب وفقًا للقاعدة.
- **جدولة القاعدة**. يمكنك تحديد جدول القاعدة. يحدد جدول القاعدة الفترة الزمنية التي يقوم خلالها Kaspersky Endpoint Security بمراقبة الوصول إلى موارد الويب الخاضعة للقاعدة.

بعد تثبيت Kaspersky Endpoint Security، لا تكون قائمة قواعد مكون التحكم في الويب فارغة. ويتم ضبط القاعدة الافتراضية مسبقًا. يتم تطبيق هذه القاعدة لأي من موارد الويب التي لا تشملها قواعد أخرى، و تسمح أو تمنع الوصول إلى موارد الويب تلك لجميع المستخدمين.

إضافة قاعدة وصول إلى موارد الويب

لإضافة قاعدة وصول إلى مورد الويب أو تحريرها:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.

3. في القسم **الإعدادات**، انقر على الزر **قواعد الوصول إلى موارد الويب**.

4. في النافذة التي تفتح، انقر فوق الزر **إضافة**.
تفتح النافذة **قاعدة الوصول إلى موارد الويب**.

5. في الحقل **اسم القاعدة** أدخل اسم القاعدة.

6. حدد الحالة **تشغيل** لقاعدة الوصول إلى موارد الويب.
يمكنك استخدام مفتاح التبديل لتعطيل قاعدة الوصول إلى موارد الويب في أي وقت.

7. في القسم **الإجراء**، حدد الخيار المناسب:

- **سماح**. إذا تم تحديد هذه القيمة، فإن Kaspersky Endpoint Security يتيح الوصول إلى موارد الويب التي تطابق معلمات القاعدة.
- **منع**. إذا تم تحديد هذه القيمة، فإن Kaspersky Endpoint Security يمنع الوصول إلى موارد الويب التي تطابق معلمات القاعدة.
- **تحذير**. إذا تم تحديد هذه القيمة، فإن Kaspersky Endpoint Security يقوم بعرض تحذير يفيد بأن مورد الويب غير مرغوب فيه عند محاولة المستخدم الوصول إلى موارد الويب التي تطابق القاعدة. عن طريق استخدام الارتباطات من رسالة التحذير، يمكن للمستخدم التمتع بالوصول إلى مورد الويب المطلوب.

8. في القسم **محتوى عامل التصفية** ، حدد عامل تصفية المحتوى ذي الصلة:

- **حسب فئات المحتوى**. يمكنك التحكم في وصول المستخدم إلى موارد الويب حسب category (على سبيل المثال، فئة الشبكات الاجتماعية).
- **حسب أنواع البيانات**. يمكنك التحكم في وصول المستخدم إلى موارد الويب بناءً على نوع البيانات المحدد لبياناته المنشورة (على سبيل المثال، الرسومات).

لتكوين عامل تصفية للمحتوى:

a. انقر على رابط **الإعدادات**.

b. حدد خانات الاختيار الموجودة بجوار أسماء الفئات المطلوبة للمحتوى و/أو أنواع البيانات.

المقصود بتحديد خانة الاختيار الموجودة بجوار اسم فئة المحتوى و/أو نوع البيانات هو أن برنامج Kaspersky Endpoint Security يقوم بتطبيق القاعدة للتحكم في الوصول إلى موارد الويب التي تنتمي إلى الفئات المحددة للمحتوى و/أو أنواع البيانات.

c. ارجع إلى النافذة لتكوين قاعدة الوصول إلى مورد الويب.

9. في القسم **العناوين**، حدد عامل تصفية عنوان مورد الويب ذي الصلة:

- **على جميع العناوين**. لن يقوم التحكم في الويب بتصفية موارد الويب حسب العنوان.
- **على العناوين الفردية**. سيقوم التحكم في الويب بتصفية عناوين موارد الويب فقط من القائمة. لإنشاء قائمة بعناوين موارد الويب:

a. انقر فوق الزر **إضافة عنوان** أو **إضافة مجموعة من العناوين**.

b. في النافذة التي تفتح، أنشئ قائمة بعناوين موارد الويب. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT.

c. ارجع إلى النافذة لتكوين قاعدة الوصول إلى مورد الويب.

إذا كان فحص الاتصالات المشفرة معطلاً، فبالنسبة لبروتوكول HTTPS، فيمكنك التصفية فقط عن طريق اسم الخادم.

10. في القسم **المستخدمون**، حدد عامل التصفية المناسب للمستخدمين:

- **على جميع المستخدمين**. لن يقوم التحكم في الويب بتصفية موارد الويب لمستخدمين محددين.
- **على مستخدمين أفراد و/أو مجموعات**. سيقوم التحكم في الويب بتصفية موارد الويب لمستخدمين محددين فقط. لإنشاء قائمة بالمستخدمين الذين تريد تطبيق القاعدة عليهم:

a. انقر على **إضافة**.

b. في النافذة التي تفتح، حدد المستخدمين أو مجموعة المستخدمين الذين تريد تطبيق قاعدة الوصول إلى موارد الويب عليهم.

c. ارجع إلى النافذة لتكوين قاعدة الوصول إلى مورد الويب.

11. من القائمة المنسدلة **جدولة القاعدة**، حدد اسم الجدولة المطلوبة أو أنشئ جدولة جديدة تعتمد على جدولة القاعدة المحددة. للقيام بذلك:

a. انقر على **تحرير أو إضافة جديد**.

b. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

c. في النافذة التي تفتح، أدخل اسم جدولة القاعدة.

d. قم بتكوين جدول الوصول إلى مورد الويب للمستخدمين.

e. ارجع إلى النافذة لتكوين قاعدة الوصول إلى مورد الويب.

12. احفظ تغييراتك.

تعيين أولويات لقواعد الوصول إلى موارد الويب

لكل قاعدة أولوية. كلما كانت القاعدة تحتل مرتبة أعلى في القائمة، فإنها تكون ذات أولوية أعلى. إذا تمت إضافة موقع ويب إلى قواعد متعددة، ينظم المكون التحكم في الويب الوصول إلى موقع الويب بناءً إلى القاعدة ذات أعلى أولوية. على سبيل المثال، قد يحدد برنامج Kaspersky Endpoint Security بوابة شركة لتكون شبكة اجتماعية. لتقييد الوصول إلى الشبكات الاجتماعية وتوفير الوصول إلى بوابة الويب الخاصة بالشركة، قم بإنشاء قاعدتين: قاعدة واحدة لحظر الوصول إلى فئة موقع الويب الشبكات الاجتماعية وقاعدة واحدة للسماح بالوصول إلى بوابة الويب الخاصة بالشركة. يجب أن يكون لقاعدة الوصول لبوابة الويب الخاصة بالشركة أولوية أعلى من قاعدة الوصول إلى الشبكات الاجتماعية.

يمكنك تعيين أولويات لكل قاعدة من قائمة القواعد، وذلك من خلال ترتيب القواعد بترتيب معين.

لتعيين أولوية لقاعدة وصول إلى موارد الويب:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.

3. في القسم **الإعدادات**، انقر على الزر **قواعد الوصول إلى موارد الويب**.

4. في النافذة التي تفتح، حدد القاعدة التي تريد تغيير أولويتها.

5. استخدم الزرين **أعلى** و**أسفل** لنقل القاعدة إلى الموضع المناسب في قائمة قواعد الوصول إلى موارد الويب.

6. احفظ تغييراتك.

تمكين وتعطيل قاعدة الوصول إلى مورد ويب

لتمكين أو تعطيل قاعدة الوصول إلى مورد ويب:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.
3. في القسم **الإعدادات**، انقر على الزر **قواعد الوصول إلى موارد الويب**.
4. في النافذة المفتوحة، حدد القاعدة التي تريد تمكينها أو تعطيلها.
5. في العمود **الحالة**، نفذ ما يلي:
   - إذا كنت ترغب في تمكين استخدام القاعدة، فحدد القيمة **تشغيل**.
   - إذا كنت ترغب في تعطيل استخدام القاعدة، فحدد قيمة **إيقاف التشغيل**.
6. احفظ تغييراتك.

تصدير واستيراد قواعد التحكم في الويب

يمكنك تصدير قائمة قواعد التحكم في الويب إلى ملف XML. وبعد ذلك يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من العناوين من النوع نفسه. ويمكنك استخدام وظيفة التصدير / الاستيراد لإنشاء نسخة احتياطية من قائمة قواعد التحكم في الويب أو لترحيل القائمة إلى خادم مختلف.

كيفية تصدير واستيراد قائمة قواعد التحكم في الويب في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الويب**.

5. لتصدير قائمة قواعد التحكم في الويب:

   a. حدد القواعد التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

   إذا لم تحدد أي قاعدة، فسيقوم Kaspersky Endpoint Security بتصدير كل القواعد.

   b. انقر على رابط **تصدير**.

   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة القواعد إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.

   d. احفظ الملف.

   يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد بالكامل إلى ملف XML.

6. لاستيراد قائمة قواعد التحكم في الويب:

   a. انقر على رابط **استيراد**.

   في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

   b. افتح الملف.

   إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد التحكم في الويب في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Security Controls** ← **Web Control**.

5. لتصدير قائمة القواعد، في القسم **Rule List**:

a. حدد القواعد التي تريد تصديرها.

b. انقر على **Export**.

c. أكد أنك تريد تصدير القواعد المحددة فقط، أو تصدير القائمة بأكملها.

d. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف XML في مجلد التنزيلات الافتراضي.

6. لاستيراد قائمة القواعد، في القسم **Rule List**:

a. انقر على رابط **Import**.
في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

b. افتح الملف.
إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

اختبار قواعد الوصول إلى موارد الويب

يمكنك اختبار قواعد التحكم في الويب للتحقق من تناسقها. ولهذا الغرض، يحتوي مكون التحكم في الويب على وظيفة لتشخيص القواعد.

لاختبار قواعد الوصول إلى موارد الويب:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.

3. في القسم **الإعدادات**، انقر على الرابط **تشخيصات القواعد**.
تفتح النافذة **تشخيصات القواعد**.

4. إذا كنت تريد اختبار القواعد التي يستخدمها Kaspersky Endpoint Security للتحكم في الوصول إلى مورد محدد من موارد الويب، فحدد مربع الاختيار **تحديد عنوان**. أدخل عنوان مورد الويب في الحقل الموجود أدناه.

5. إذا كنت تريد اختبار القواعد التي يستخدمها Kaspersky Endpoint Security للتحكم في الوصول إلى موارد الويب بالنسبة إلى مستخدمين معيّنين و / أو مجموعات معيّنة من المستخدمين، فحدد قائمة بهؤلاء المستخدمين و / أو مجموعات المستخدمين.

6. إذا كنت تريد اختبار القواعد التي يستخدمها Kaspersky Endpoint Security للتحكم في الوصول إلى موارد الويب التي تعرض فئات معيّنة للمحتوى و/أو لأنواع البيانات، فحدد خانة الاختيار **تصفية المحتوى** واختر الخيار المناسب من القائمة المنسدلة (**حسب فئات المحتوى** أو **حسب أنواع البيانات** أو **حسب فئات المحتوى وأنواع البيانات**).

7. إذا كنت تريد اختبار القواعد مع اعتبار الوقت واليوم الذي حدثت فيه محاولة الوصول إلى موارد الويب المحددة في شروط تشخيص القواعد، فحدد مربع الاختيار **تضمين وقت محاولة الوصول**. ثم حدد بعد ذلك اليوم والوقت.

8. انقر على **فحص**.

بعد اكتمال الاختبار، تظهر رسالة تتضمن معلومات عن الإجراء الذي اتخذه Kaspersky Endpoint Security وفقًا لأول قاعدة تم تشغيلها عند محاولة الوصول إلى مورد الويب المحدد (سماح أو منع، أو تحذير). إن أول قاعدة يتم تشغيلها هي تلك التي تحتل ترتيبًا في قائمة قواعد التحكم في الويب أعلى من ترتيب بقية العناصر الأخرى التي تتوافق مع شروط التشخيص. يتم عرض الرسالة على يمين الزر **فحص**. ويعرض الجدول التالي بقية القواعد التي تم تشغيلها، مع تحديد الإجراء الذي اتخذه Kaspersky Endpoint Security. وقد تم إدراج القواعد بالترتيب من الأعلى أولويةً للأدنى.

تصدير واستيراد قائمة عناوين موارد الويب

إذا قمت بإنشاء قائمة بعناوين مورد ويب في قاعدة الوصول إلى موارد الويب، فيمكنك تصديرها إلى ملف .txt. ويمكنك بالتالي استيراد القائمة من هذا الملف لتجنب إنشاء قائمة جديدة لعناوين مورد الويب يدويًا عند تكوين قاعدة وصول. قد يكون خيار تصدير واستيراد قائمة عناوين مورد الويب مفيدًا، عند إنشاء قاعدة وصول بمعلمات متشابهة.

لاستيراد أو تصدير قائمة عناوين موارد الويب إلى ملف:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.

3. في القسم **الإعدادات**، انقر على الزر **قواعد الوصول إلى موارد الويب**.

4. حدد القاعدة التي تريد تصدير أو استيراد قائمة عناوين موارد الويب الخاصة بها.

5. لتصدير قائمة عناوين الويب الموثوقة، نفذ ما يلي في القسم **العناوين**:

   a. حدد العناوين التي تريد تصديرها.

   إذا لم تحدد أي عنوان، فسيقوم Kaspersky Endpoint Security بتصدير كل العناوين.

   b. انقر على **تصدير**.

   c. في النافذة التي تفتح، أدخل اسم ملف TXT الذي تريد تصدير قائمة عناوين موارد الويب إليه، وحدد المجلد الذي تريد حفظ هذا الملف فيه.

   d. احفظ الملف.

   يقوم Kaspersky Endpoint Security بتصدير قائمة عناوين موارد الويب إلى ملف TXT.

6. لاستيراد قائمة موارد الويب، نفذ ما يلي في القسم **العناوين**:

   a. انقر على **استيراد**.

   في النافذة التي تفتح، حدد ملف TXT الذي تريد استيراد قائمة موارد الويب منه.

   b. افتح الملف.

   إذا كان جهاز الكمبيوتر يتضمن قائمة أجهزة موثوقة بالفعل، فسوف يطلب منكKaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

مراقبة نشاط إنترنت المستخدم

يُتيح لك برنامج Kaspersky Endpoint Security تسجيل بيانات عن زيارات المستخدم لجميع مواقع الويب، بما في ذلك مواقع الويب المسموح بها. يُمكّنك هذا من الحصول على السجل الكامل لمشاهدات المستعرض. يُرسل برنامج Kaspersky Endpoint Security الأحداث الخاصة بنشاط المستخدم إلى Kaspersky Security Center، وإلى السجل المحلي لبرنامج Kaspersky Endpoint Security، وإلى سجل أحداث Windows. لاستلام أحداث في Kaspersky Security Center، تحتاج إلى تكوين الإعدادات الخاصة بالأحداث في سياسة في وحدة تحكم الإدارة أو في Web Console. يمكنك أيضًا تكوين الإرسال الخاص بأحداث التحكم في الويب عن طريق البريد الإلكتروني وعرض الإخطارات التي تظهر على الشاشة على جهاز كمبيوتر المستخدم.

المستعرضات التي تدعم وظيفة المراقبة: Microsoft Edge وMicrosoft Internet Explorer وGoogle Chrome وYandex Browser وMozilla Firefox. ولا تعمل مراقبة نشاط المستخدم في المستعرضات الأخرى.

يقوم برنامج Kaspersky Endpoint Security بإنشاء أحداث نشاط إنترنت المستخدم التالية:

- حظر موقع الويب (أحداث حرجة حالة).
- زيارة لموقع غير مرغوبة (حالة التحذيرات).
- قم بزيارة موقع ويب مسموح به (رسائل معلوماتية حالة).

قبل تمكين مراقبة نشاط الإنترنت للمستخدم، يجب عليك تنفيذ ما يلي:

- أدخل برنامجًا نصيًا للتفاعل لصفحة الويب في حركة المرور على الويب (راجع الإرشادات أدناه). يتيح البرنامج النصي تسجيل أحداث التحكم في الويب.
- لمراقبة حركة مرور HTTPS، تحتاج إلى تمكين عمليات فحص الاتصالات المشفرة.

لإدخال برنامج نصي لتفاعل صفحة الويب في حركة المرور على الويب:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر .
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.

إعدادات شبكة التطبيق

3. في القسم **معالجة حركة المرور**، حدد خانة الاختيار **إدخال البرنامج النصي في حركة مرور الويب للتفاعل مع صفحات الويب**.

4. احفظ تغييراتك.

نتيجة لذلك، سيقوم Kaspersky Endpoint Security بإدخال برنامج نصي لتفاعل صفحة الويب في حركة المرور على الويب. يتيح هذا البرنامج النصي تسجيل أحداث التحكم في الويب لسجل أحداث التطبيق، وسجل أحداث نظام التشغيل، و[التقارير](#).

لتمكين تسجيل الأحداث الخاصة بالتحكم في الويب على كمبيوتر المستخدم:

1. في [نافذة التطبيق الرئيسية](#)، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة ← الواجهة**.

3. في القسم **الإخطارات**، انقر على الزر **إعدادات الإخطار**.

4. في النافذة التي تفتح، حدد القسم **التحكم في الويب**.

هذا يفتح الجدول الخاص بأحداث التحكم في الويب وطرق عرض الإخطارات.

5. تكوين طريقة عرض الإخطارات لكل حدث: **حفظ في تقرير محلي** أو **حفظ في سجل أحداث Windows**.

لتسجيل أحداث الزيارة الخاصة بموقع الويب المسموح به، تحتاج أيضًا إلى تكوين التحكم في الويب (راجع الإرشادات الموجودة أدناه).

في جدول الأحداث، يمكنك أيضًا تمكين الإخطارات التي تظهر على الشاشة وإخطارات البريد الإلكتروني. لإرسال الإخطارات عن طريق البريد الإلكتروني، تحتاج إلى تكوين إعدادات خادم SMTP. وللمزيد من التفاصيل حول إرسال الإخطارات عن طريق البريد الإلكتروني، يُرجى الرجوع إلى [تعليمات Kaspersky Security Center](#).

6. احفظ تغييراتك.

كنتيجة لذلك، سيبدأ برنامج Kaspersky Endpoint Security بتسجيل أحداث نشاط إنترنت المستخدم.

التحكم في الويب ترسل أحداث النشاط إلى Kaspersky Security Center كما يلي:

- إذا كنت تستخدم Kaspersky Security Center، فإن التحكم في الويب ترسل الأحداث لجميع الكائنات التي تكون صفحة الويب. لهذا السبب، قد يتم إنشاء أحداثًا متعددة عند حظر صفحة ويب واحدة. على سبيل المثال، عند حظر صفحة الويب http://www.example.com، قد يقوم برنامج Kaspersky Endpoint Security بترحيل الأحداث للكائنات التالية: http://www.example.com، و http://www.example.com/icon.ico، و http://www.example.com/file.js، إلخ.

- إذا كنت تستخدم Kaspersky Security Center Cloud Console، فإن التحكم في الويب تقوم بتجميع الأحداث وترسل فقط البروتوكول والنطاق للموقع الإلكتروني. على سبيل المثال: إذا كان مستخدم يزور صفحات ويب غير مرغوبة http://www.example.com/main أو http://www.example.com/contact أو http://www.example.com/gallery، فإن Kaspersky Endpoint Security لن يرسل إلا حدث واحد بكائن http://www.example.com.

لتمكين تسجيل الأحداث لزيارة مواقع الويب المسموح بها:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.
3. في القسم **إضافي**، انقر على الزر **إعدادات متقدمة**.
4. في النافذة التي تفتح، حدد خانة الاختيار **تسجيل فتح الصفحات المسموح بها**.
5. احفظ تغييراتك.

كنتيجة لذلك، ستتمكن من عرض السجل الكامل للمستعرض.

تحرير قوالب رسائل التحكم في الويب

حسب نوع الإجراء المحدد في خصائص قواعد التحكم في الويب، يعرض Kaspersky Endpoint Security أحد أنواع الرسائل التالية عندما يحاول المستخدمون الوصول إلى موارد الإنترنت (يحجب التطبيق صفحة HTML ويعرض بدلاً منها رسالةً توضّح استجابة خادم HTTP):

- رسالة تحذير. تحذر هذه الرسالة المستخدم من أن زيارة موارد الويب غير موصى بها و / أو تمثل انتهاكًا لسياسة أمن الشركة. يعرض Kaspersky Endpoint Security رسالة تحذير في حالة تحديد الخيار **تحذير** في إعدادات القاعدة التي تصِف مورد الويب هذا.

  إذا اعتقد المستخدم أن التحذير خطأ، يمكن للمستخدم النقر فوق الرابط الموجود في التحذير لإرسال رسالة مُعَدّة مسبقًا إلى مسؤول الشبكة المحلية للشركة.

- رسالة إبلاغ بمنع مورد الويب. يعرض Kaspersky Endpoint Security رسالة تفيد بأن مورد الويب ممنوع في حالة تحديد الخيار **منع** في إعدادات القاعدة التي تصِف مورد الويب هذا.

  إذا اعتقد المستخدم أنه قد تم منع مورد الويب عن طريق الخطأ، يمكن للمستخدم النقر فوق الرابط في رسالة إخطار منع مورد الويب لإرسال الرسالة التي تم إنشاؤها مسبقًا إلى مسؤول الشبكة المحلية للشركة.

تتوفر قوالب خاصة لرسائل التحذير، والرسائل التي تبلّغ بأن مورد الويب ممنوع، ورسالة يتم إرسالها إلى مسؤول الشبكة المحلية. ويمكنك تعديل محتوى هذه الرسائل.

لتغيير قالب رسائل التحكم في الويب:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.
3. في القسم **القوالب**، كوّن القوالب لرسائل التحكم في الويب:

- **تحذير**. يتكون حقل الإدخال من قالب للرسالة التي يتم عرضها إذا تم تشغيل قاعدة للتحذير بشأن محاولات وصول إلى مورد ويب غير مرغوب فيه.

- **رسالة حول المنع**. يحتوي حقل الإدخال على قالب الرسالة التي تظهر في حالة تشغيل قاعدة تمنع الوصول إلى أحد موارد الويب.

- **رسالة إلى المسؤول**. قالب الرسالة المقرر إرسالها إلى مسؤول الشبكة المحلية إذا كان المستخدم يعتقد أن المنع تم عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع الوصول لصفحة الويب إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.

4. احفظ تغييراتك.

تحرير أقنعة عناوين مصادر الويب

قد يكون استخدام قناع عنوان مورد ويب (يشار إليه أيضًا "بقناع العنوان") مفيدًا إذا كنت بحاجة لإدخال العديد من عناوين موارد الويب المتشابهة عند إنشاء قاعدة وصول إلى مورد ويب. إذا تم إنشاء القناع بشكل جيد، فإن قناع عنوان واحد يمكنه استبدال عدد كبير من عناوين مورد الويب.

عند إنشاء قناع عنوان، اتبع هذه القواعد:

1. يستبدل الرمز `*` أي تسلسل يحتوي على رمز صفر أو أكثر.

   على سبيل المثال، إذا قمت بإدخال قناع العنوان `*abc`، فسيتم تطبيق قاعدة الوصول على كل موارد الويب التي تحتوي على `abc`. مثال: `http://www.example.com/page_0-9abcdef.html`.

2. يتيح لك تسلسل أحرف `.*` (المعروفة باسم قناع نطاق) تحديد كل نطاقات عنوان ما. يمثل قناع النطاق `.*` أي اسم نطاق أو اسم نطاق فرعي أو سطر فارغ.

   مثال: يمثل قناع `*.example.com` العناوين التالية:

   - `http://pictures.example.com`. يمثل قناع النطاق `pictures.*.`.
   - `http://user.pictures.example.com`. يمثل قناع النطاق `pictures.*.` و`user.`.
   - `http://example.com`. يُفسر قناع النطاق `.*` على أنه سطر فارغ.

3. يتم تفسير تسلسل الرمز `www.` في بداية قناع العنوان باعتباره تسلسل `.*`.

   مثال: تتم معاملة قناع العنوان `www.example.com` يترجم إلى `*.example.com`. يغطي هذا القناع العنوانين `www2.example.com` و`www.pictures.example.com`.

4. إذا لم يكن قناع العنوان يبدأ بالرمز `*`، فإن محتوى قناع العنوان يعتبر مكافئًا لنفس المحتوى الذي يشتمل على رمز البادئة `.*`.

5. إذا كان قناع العنوان ينتهي برمز غير `/` أو `*`، فإن محتوى قناع العنوان سيكون مكافئًا لنفس المحتوى الذي يشتمل على اللاحقة `*/`.

   مثال: قناع العنوان `http://www.example.com` يغطي عناوين مثل `http://www.example.com/abc`، حيث تعبر `a` و`b` و`c` عن أي رمز.

6. إذا كان قناع العنوان ينتهي برمز `/`، فإن محتوى قناع العنوان يعتبر مكافئًا لنفس المحتوى الذي يشتمل على رمز اللاحقة `.*/`.

7. يتم تفسير تسلسل الرمز `*/` في نهاية قناع العنوان باعتباره `*/` أو سلسلة فارغة.

8. يتم التحقق من عناوين مورد الويب في مقابل قناع عنوان معين مع وضع في الاعتبار البروتوكول المستخدم (http أو https):

   - إذا كان قناع العنوان لا يحتوي على بروتوكول شبكة، فإن قناع العنوان هذا يغطي عناوين مزودة بأي بروتوكول شبكة.

     مثال: يغطي قناع العنوان `example.com` العنوانين `http://example.com` و`https://example.com`.

   - إذا كان قناع العنوان يحتوي على بروتوكول شبكة، فإن قناع العنوان هذا سيغطي فقط العناوين التي تستخدم نفس بروتوكول الشبكة المحددة في قناع العنوان.

مثال: قناع العنوان `http://*.example.com` يغطي العنوان `http://www.example.com` ولكنه لا يغطي `https://www.example.com`.

9. تتم معاملة قناع العنوان الموجود داخل علامات اقتباس مزدوجة بدون اعتبار أي استبدالات إضافية، باستثناء الرمز `*` إذا كان مضمنًا بشكل أولي في قناع العنوان. لا تنطبق القواعد 5 و7 على أقنعة العناوين المحاطة بين علامتي اقتباس مزدوجة (راجع الأمثلة من 14 إلى 18 في الجدول أدناه).

10. ولا يتم اعتبار اسم المستخدم وكلمة المرور ومنفذ الاتصال وحالة الحرف خلال المقارنة مع قناع العنوان الخاص بمورد الويب.

أمثلة حول كيفية استخدام قواعد إنشاء أقنعة عنوان

الرقم.	قناع العنوان	عنوان مورد الويب للتحقق	هل يغطي قناع العنوان	التعليق
1	*.example.com	http://www.123example.com	لا	راجع القاعدة 1.
2	*.example.com	http://www.123.example.com	نعم	راجع القاعدة 2.
3	*example.com	http://www.123example.com	نعم	راجع القاعدة 1.
4	*example.com	http://www.123.example.com	نعم	راجع القاعدة 1.
5	http://www.*.example.com	http://www.123example.com	لا	راجع القاعدة 1.
6	www.example.com	http://www.example.com	نعم	راجع القواعد 3 و2 و1.
7	www.example.com	https://www.example.com	نعم	راجع القواعد 3 و2 و1.
8	http://www.*.example.com	http://123.example.com	نعم	راجع القواعد 3 و4 و1.
9	www.example.com	http://www.example.com/abc	نعم	راجع القواعد 3 و5 و1.
10	example.com	http://www.example.com	نعم	راجع القاعدتين 3 و1.
11	http://example.com/	http://example.com/abc	نعم	راجع القاعدة 6.
12	http://example.com/*	http://example.com	نعم	راجع القاعدة 7.
13	http://example.com	https://example.com	لا	راجع القاعدة 8.
14	"example.com"	http://www.example.com	لا	راجع القاعدة 9.
15	"http://www.example.com"	http://www.example.com/abc	لا	راجع القاعدة 9.
16	"*.example.com"	http://www.example.com	نعم	راجع القاعدتين 1 و9.
17	"http://www.example.com/*"	http://www.example.com/abc	نعم	راجع القاعدتين 1 و9.
18	"www.example.com"	http://www.example.com; https://www.example.com	نعم	راجع القاعدتين 9 و8.
19	www.example.com/abc/123	http://www.example.com/abc	لا	يحتوي قناع المعلومات على المزيد من المعلومات عن عنوان مورد الويب.

التحكم في الجهاز

يعمل التحكم في الجهاز على إدارة إمكانية وصول المستخدم إلى الأجهزة المثبت عليها أو المتصلة بجهاز الكمبيوتر (على سبيل المثال، الأقراص الصلبة أو الكاميرات أو وحدات شبكة Wi-Fi). يتيح لك هذا حماية جهاز الكمبيوتر من الإصابة بالفيروسات عند اتصال مثل هذه الأجهزة به بالإضافة إلى الوقاية من فقدان البيانات أو تسريبها.

مستويات الوصول إلى الجهاز

يعمل التحكم في الجهاز على التحكم في إمكانية الوصول عند المستويات التالية:

- **نوع الجهاز**. على سبيل المثال، آلات الطباعة ومحركات الأقراص القابلة للإزالة ومحركات الأقراص المضغوطة / أقراص DVD.

  يمكنك تكوين إمكانية الوصول إلى الجهاز على النحو التالي:

  - سماح – .
  - منع – .
  - حسب القواعد (الطابعات والأجهزة المحمولة فقط) – .
  - يعتمد على ناقل الاتصال (باستثناء Wi-Fi) – .
  - حظر مع استثناءات (Wi-Fi فقط) – .

- **ناقل الاتصال**. ناقل الاتصال عبارة عن واجهة تستخدم لتوصيل الأجهزة بجهاز الكمبيوتر (على سبيل المثال، أجهزة USB أو FireWire). ولذلك، يمكنك تقييد اتصال جميع الأجهزة، على سبيل المثال، ما يزيد عن USB.

  يمكنك تكوين إمكانية الوصول إلى الجهاز على النحو التالي:

  - سماح – .
  - منع – .

- **الأجهزة الموثوقة**. الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

  يمكنك إضافة الأجهزة الموثوقة وفقًا للبيانات التالية:

  - **الأجهزة حسب المُعرِّف**. كل جهاز له معرف فريد (معرف الأجهزة أو HWID). يمكنك عرض المُعرّف في خصائص الجهاز من خلال استخدام أدوات نظام التشغيل. مثال على معرف الجهاز: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. إضافة الأجهزة حسب المُعرّف عملية ملائمة إذا كنت ترغب في إضافة مجموعة أجهزة محددة.

  - **الأجهزة حسب الموديل**. كل جهاز له معرف بائع (VID) ومعرف منتج (PID). يمكنك عرض المُعرّفات في خصائص الجهاز من خلال استخدام أدوات نظام التشغيل. قالب إدخال معرف البائع ومعرف المنتج: `VID_1234&PID_5678`. إضافة أجهزة حسب الموديل طريقة ملائمة إذا كنت تستخدم أجهزة ذات موديل معين في مؤسستك. بهذه الطريقة، يمكنك إضافة جميع الأجهزة من هذا الموديل.

  - **الأجهزة حسب قناع المُعرّف**. إذا كنت تستخدم عدة أجهزة ذات معرفات متشابهة، يمكنك إضافة الأجهزة إلى القائمة الموثوقة باستخدام الأقنعة. الحرف `*` يستبدل أي مجموعة من الرموز. لا يدعم برنامج Kaspersky Endpoint Security الحرف `?` عند إدخال قناع. على سبيل المثال: `WDC_C*`.

  - **الأجهزة حسب قناع الطراز**. إذا كنت تستخدم عدة أجهزة لها معرفات البائعين ومعرفات المنتجين نفسها (مثل أجهزة من الشركة المصنعة ذاتها)، عندها يمكنك إضافة أجهزة إلى القائمة الموثوقة باستخدام الأقنعة. الحرف `*` يستبدل أي مجموعة من الرموز. لا يدعم برنامج Kaspersky Endpoint Security الحرف `?` عند إدخال قناع. على سبيل المثال، `VID_05AC & PID_ *`.

يقوم التحكم في الجهاز بتنظيم وصول المستخدم إلى الأجهزة باستخدام قواعد الوصول. وكذلك يتيح لك التحكم في الجهاز القيام بحفظ أحداث اتصال الجهاز/انقطاع اتصاله. لحفظ الأحداث، تحتاج إلى تكوين تسجيل الأحداث في السياسة.

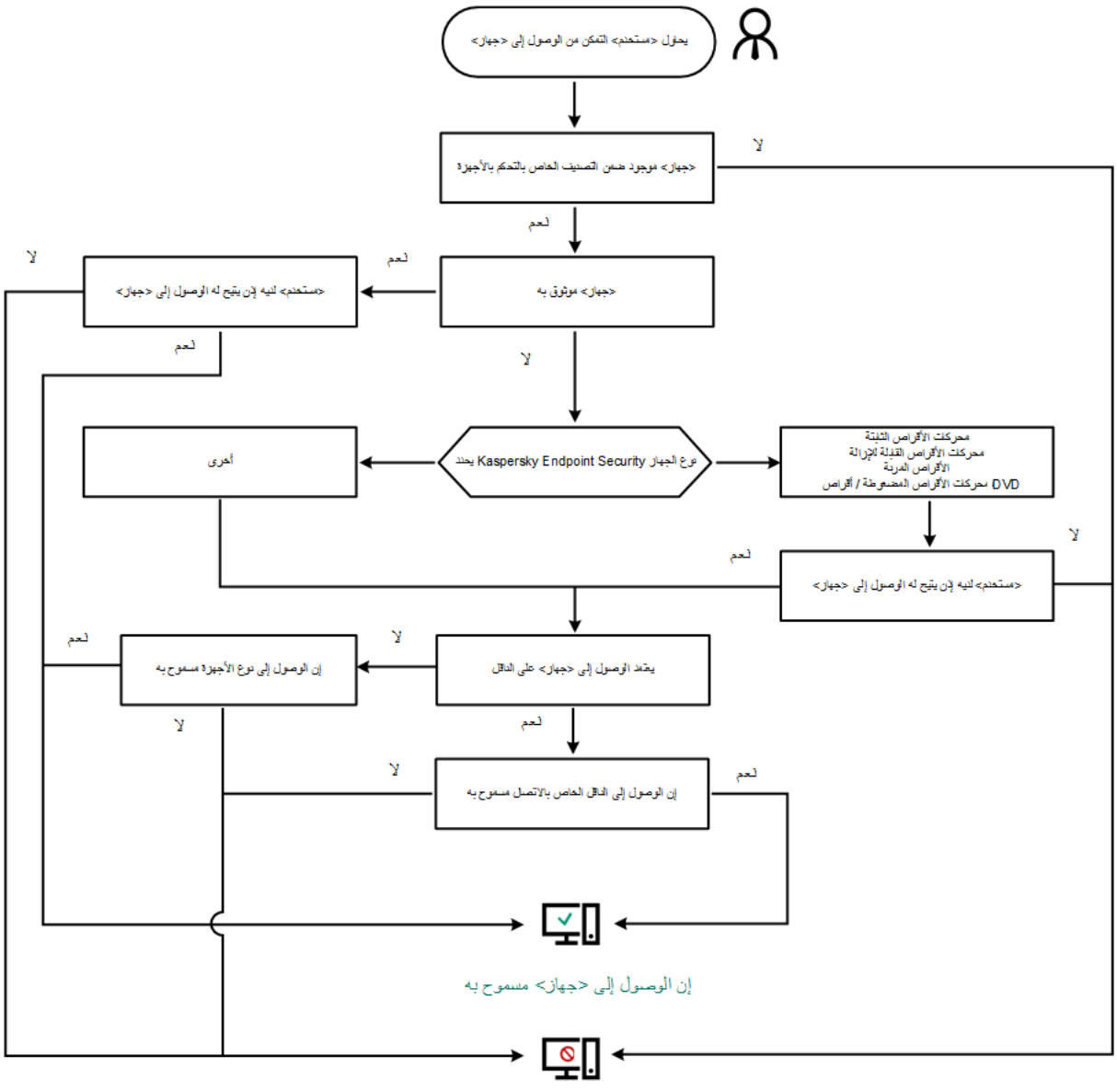
إذا كان يعتمد الوصول إلى جهاز ما على ناقل الاتصال (الحالة)، لا يقوم برنامج Kaspersky Endpoint Security بحفظ أحداث اتصال الجهاز/انقطاع اتصاله. لتمكين برنامج Kaspersky Endpoint Security من حفظ أحداث اتصال الجهاز/انقطاع اتصاله، قم بالسماح بالوصول إلى نوع الجهاز المتطابق (الحالة) أو قم بإضافة الجهاز إلى القائمة الموثوقة.

عند حظر جهاز متصل بجهاز كومبيوتر بواسطة التحكم في الجهاز، فإن برنامج Kaspersky Endpoint Security سيقوم بحظر الوصول وإظهار إخطار (انظر الشكل أدناه).

إخطار التحكم في الجهاز

خوارزمية تشغيل التحكم في الجهاز

يتخذ برنامج Kaspersky Endpoint Security قرارًا بشأن السماح بالوصول إلى الجهاز بعد أن يقوم المستخدم بتوصيل هذا الجهاز بجهاز الكمبيوتر (انظر الشكل أدناه).



خوارزمية تشغيل التحكم في الجهاز

إذا كان الجهاز متصلًا وكان الوصول مسموحًا به، يمكنك تحرير قاعدة الوصول وحظر الوصول. في هذه الحالة، في المرة التالية التي يحاول فيها شخص ما الوصول إلى الجهاز (على سبيل المثال عرض شجرة المجلدات، أو تنفيذ عمليات القراءة أو الكتابة)، سيقوم برنامج Kaspersky Endpoint Security بحظر الوصول. يتم منع أي جهاز لا يحتوي على ملف نظام، ولكن في المرة التالية التي يتم فيها توصيل الجهاز.

إذا كان يجب على مستخدم جهاز كمبيوتر مثبت عليه Kaspersky Endpoint Security طلب الوصول إلى جهاز يعتقد المستخدم أنه تم منعه عن طريق الخطأ، فأرسل للمستخدم تعليمات طلب الوصول.

تمكين وتعطيل التحكم في الجهاز

افتراضيًا، يتم تمكين التحكم في الجهاز.

لتمكين أو تعطيل التحكم في الجهاز:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.
3. استخدم مفتاح تبديل **التحكم في الجهاز** لتمكين المكون أو تعطيله.
4. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين التحكم في الجهاز، ينقل التطبيق معلومات حول الأجهزة المتصلة إلى Kaspersky Security Center. يمكنك عرض قائمة الأجهزة المتصلة في Kaspersky Security Center في المجلد **خيارات متقدمة** ← **التخزين** ← **الأجهزة**.

حول قواعد الوصول

تضم قواعد الوصول مجموعة من الإعدادات التي تحدد المستخدمين الذين يستطيعون الوصول إلى الأجهزة المثبتة أو المتصلة بالجهاز. لا يمكنك إضافة جهاز يوجد خارج تصنيف التحكم في الجهاز. يتم السماح بالوصول إلى كل الأجهزة لجميع المستخدمين.

قواعد الوصول إلى الجهاز

تختلف مجموعة إعدادات قاعدة الوصول وفقًا لنوع الجهاز (انظر الجدول أدناه).

إعدادات قاعدة الوصول

الأجهزة	التحكم في الوصول	جداول الوصول إلى الجهاز	تعيين المستخدمين و/أو مجموعة المستخدمين	الأولوية	قراءة/كتابة التصريح
محركات الأقراص الثابتة	✓	✓	✓	✓	✓
محركات الأقراص القابلة للإزالة (بما في ذلك محركات أقراص USB المحمولة)	✓	✓	✓	✓	✓
الأقراص المرنة	✓	✓	✓	✓	✓
محركات أقراص CD/DVD	✓	✓	✓	✓	✓
أجهزة محمولة (MTP)	✓	✓	✓	✓	✓
الطابعات المحلية	✓	–	✓	✓	–
طابعات الشبكة	✓	–	✓	✓	–

أجهزة المودم	✓	–	–	–	–
أجهزة شرائط	✓	–	–	–	–
أجهزة متعددة الوظائف	✓	–	–	–	–
أجهزة قراءة البطاقات الذكية	✓	–	–	–	–
أجهزة Windows CE USB ActiveSync	✓	–	–	–	–
محولات الشبكات الخارجية	✓	–	–	–	–
تقنية Bluetooth	✓	–	–	–	–
الكاميرات والماسحات الضوئية	✓	–	–	–	–

قواعد الوصول لشبكات Wi-Fi

تحدد قاعدة الوصول لشبكة Wi-Fi ما إذا كان يسمح باستخدام شبكات Wi-Fi (الحالة ✓) أم يحظر استخدامها (الحالة ⊘). يمكنك إضافة شبكة Wi-Fi موثوقة (الحالة ⬇) إلى القاعدة. يسمح باستخدام شبكة Wi-Fi موثوقة دون قيود. بشكل افتراضي، تسمح قاعدة الوصول لشبكة Wi-Fi بالوصول إلى أي شبكة Wi-Fi.

قواعد الوصول إلى ناقل الاتصال

تحدد قواعد وصول ناقل الاتصال ما إذا كان يسمح الاتصال بالجهاز مسموح (الحالة ✓) أم محظور (الحالة ⊘). القواعد التي تسمح للنواقل التي تم إنشاؤها بشكل افتراضي لجميع نواقل الاتصال الموجودة في تصنيف مكون التحكم في الجهاز.

لا يمكن قفل لوحة المفاتيح والماوس باستخدام التحكم في الجهاز. وإذا منعت الوصول إلى ناقل اتصال USB، سيستمر المستخدم في العمل باستخدام لوحة المفاتيح والماوس المتصلين عبر USB. تم تصميم مكون منع هجمات BadUSB لمنع أجهزة USB المصابة التي تحاكي لوحات المفاتيح من الاتصال بالكمبيوتر.

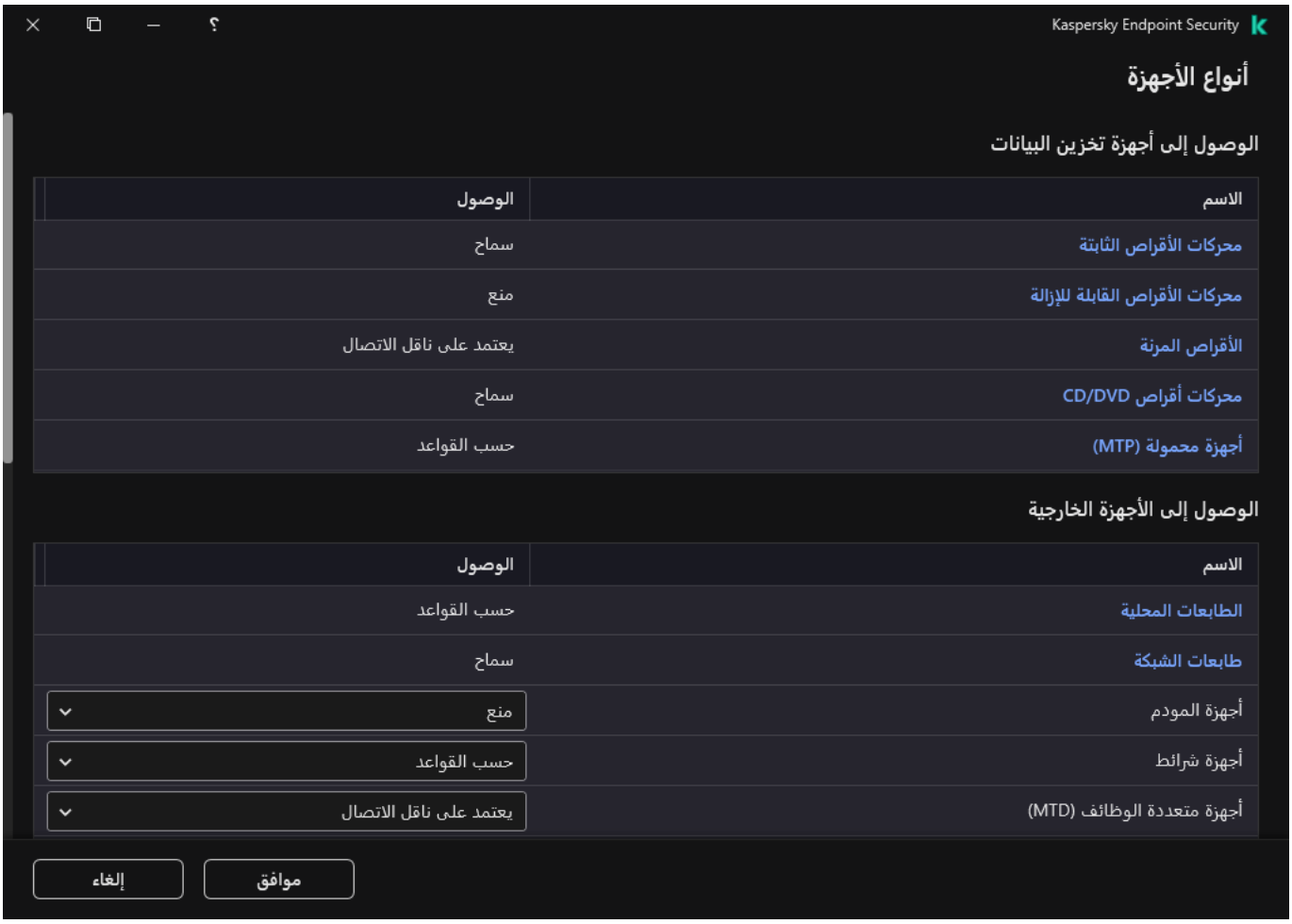
تحرير قاعدة الوصول للجهاز

قواعد الوصول إلى الجهاز عبارة عن مجموعة من الإعدادات التي تحدد كيفية وصول المستخدمين إلى الأجهزة المثبتة أو المتصلة بالكمبيوتر. وتتضمن هذه الإعدادات الوصول إلى جهاز معين وجدول وصول وأذونات القراءة أو الكتابة.

لتحرير قاعدة الوصول إلى الأجهزة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.
3. في القسم **إعدادات الوصول**، انقر على الزر **الأجهزة وشبكات Wi-Fi**.

تعرض النافذة المفتوحة قواعد الوصول لجميع الأجهزة المدرجة في تصنيف مكون التحكم في الجهاز.



أنواع الأجهزة في مكون التحكم في الجهاز

4. في القسم **الوصول إلى أجهزة تخزين البيانات**، حدد قاعدة الوصول التي تريد تحريرها. يحتوي المنع على الأجهزة التي تتضمن نظام ملفات يمكنك تكوين إعدادات وصول إضافية له. تمنح قاعدة الوصول إلى الأجهزة – افتراضيًا – جميع المستخدمين وصولاً كاملاً إلى أنواع الأجهزة المحددة في أي وقت.

a. في العمود **الوصول**، حدد خيار الوصول إلى الجهاز المناسب:

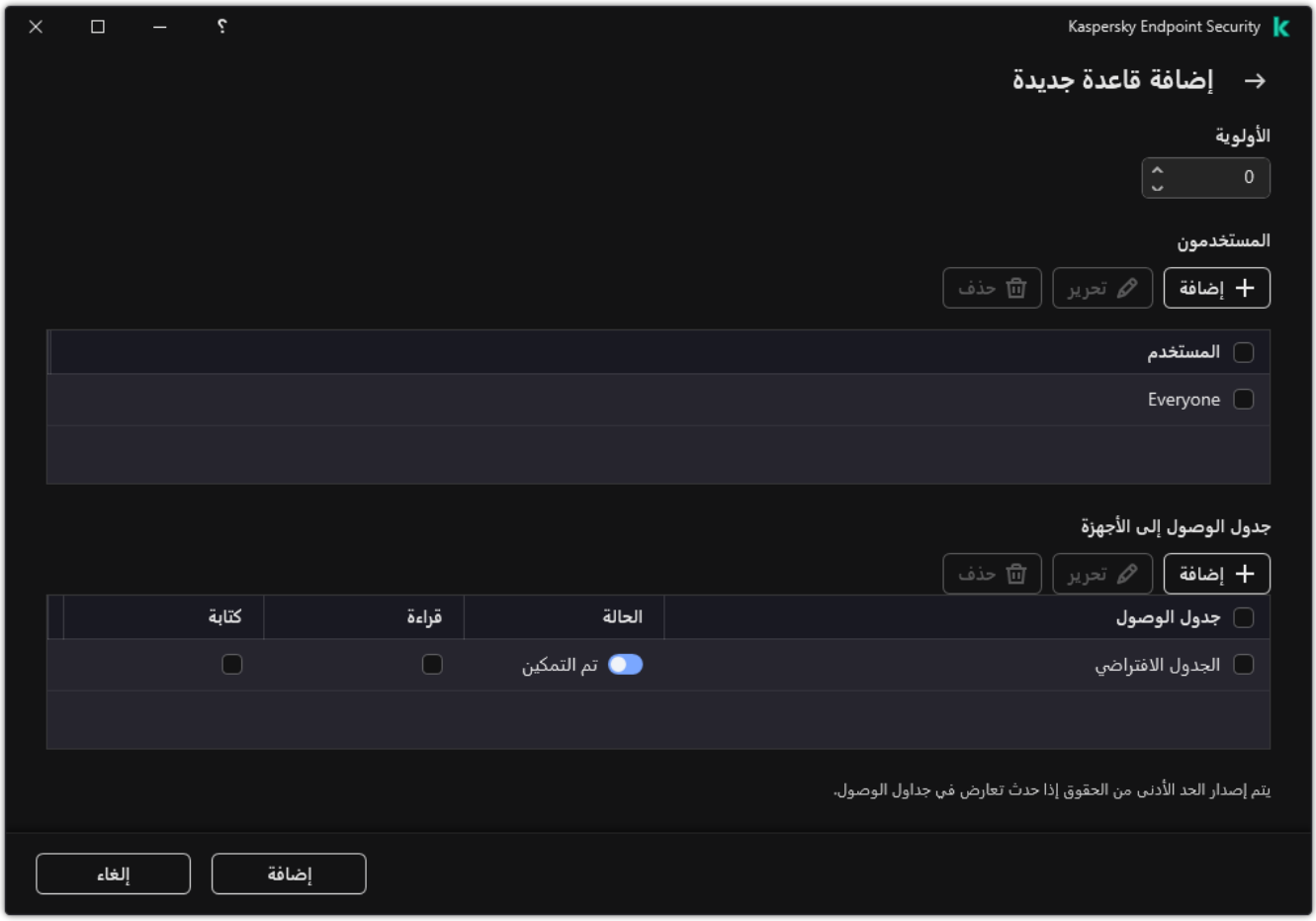
- **سماح**.
- **منع**.
- **يعتمد على ناقل الاتصال**.

  لمنع الوصول إلى جهاز أو السماح به، كوّن الوصول إلى ناقل الاتصال.
- **حسب القواعد**.

  يتيح لك هذا الخيار تكوين حقوق المستخدم والأذونات ولجدول الوصول إلى الجهاز.

b. في القسم **حقوق المستخدمين**، انقر على الزر **إضافة**.

يفتح هذا نافذة لإضافة قاعدة وصول جديدة للجهاز.



إعدادات قاعد التحكم في الجهاز

a. قم بتعيين أولوية للقاعدة. تتضمن القاعدة السمات التالية: حساب المستخدم والجدول والأذونات (القراءة/الكتابة) والأولوية.

تتضمن القاعدة أولوية محددة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. يسمح Kaspersky Endpoint Security بتعيين الأولوية من 0 إلى 10.000. كلما ارتفعت القيمة، زادت الأولوية. بمعنى آخر، يكون الإدخال بقيمة 0 بالأولوية الأدنى.

على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 1 لمجموعة المسؤولين وقم بتعيين أولوية من 0 لمجموعة "الجميع".

تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. بمعنى آخر، في حالة إضافة مستخدم إلى مجموعات متعددة وكانت أولوية جميع القواعد متشابهة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز استنادًا إلى أي قاعدة منع موجودة.

b. حدد الحالة **تم التمكين** لقاعدة الوصول إلى الجهاز.

c. كوّن أذونات الوصول إلى أجهزة المستخدمين: القراءة و/أو الكتابة.

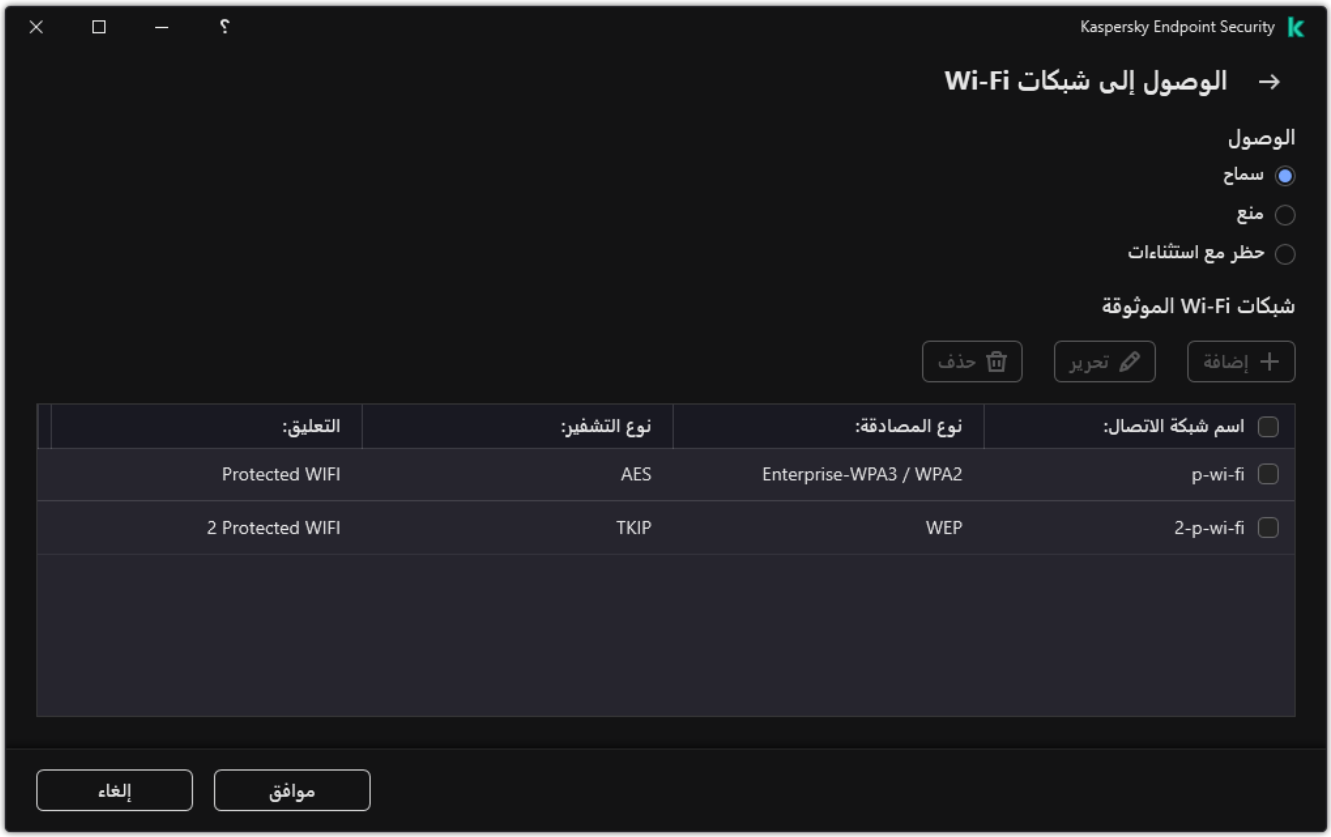
d. حدد المستخدمين أو مجموعة المستخدمين الذين تريد تطبيق قاعدة الوصول للجهاز عليهم.

e. كوّن جدولاً للوصول إلى الجهاز للمستخدمين.

f. انقر على **إضافة**.

5. في القسم **الوصول إلى الأجهزة الخارجية**، حدد القاعدة وكوّن الوصول: **سماح** أو **منع** أو **يعتمد على ناقل الاتصال**. إذا لزم الأمر، كوّن الوصول إلى ناقل الاتصال.

6. في القسم **الوصول إلى شبكات Wi-Fi**، انقر فوق الرابط **Wi-Fi** وكوّن الوصول: **سماح** أو **منع** أو **حظر مع استثناءات**. إذا لزم الأمر، أضف شبكات Wi-Fi إلى القائمة الموثوقة.



إعدادات الوصول إلى Wi-Fi

7. احفظ تغييراتك.

تحرير قاعدة الوصول إلى ناقل الاتصال

لتحرير قاعدة الوصول إلى ناقل الاتصال:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.
3. في القسم **إعدادات الوصول**، انقر على الزر **ناقلات الاتصال**.
تعرض النافذة المفتوحة قواعد الوصول لجميع ناقلات الاتصال المضمنة في تصنيف مكون التحكم في الجهاز.
4. حدد قاعدة الوصول التي تريد تحريرها.
5. في العمود **الوصول**، حدد ما إذا كنت تريد السماح بالوصول إلى ناقل الاتصال أم لا: **سماح** أو **منع**.

إذا غيرت الوصول إلى ناقل الاتصال **المنفذ التسلسلي** (COM) أو **المنفذ المتوازي** (LPT)، يجب إعادة تشغيل الكمبيوتر لتفعيل قاعدة الوصول.

6. احفظ تغييراتك.

إدارة الوصول إلى الأجهزة المحمولة

يتيح لك Kaspersky Endpoint Security التحكم في الوصول إلى البيانات على الأجهزة المحمولة التي تعمل بنظامي Android وiOS. وتنتمي الأجهزة المحمولة إلى فئة الأجهزة المحمولة (MTP). لذلك، لتكوين الوصول إلى البيانات على الأجهزة المحمولة، تحتاج إلى تحرير إعدادات الوصول للأجهزة المحمولة (MTP).

عند اتصال جهاز محمول بالكمبيوتر، يقوم نظام التشغيل بتحديد نوع الجهاز. إذا تم تثبيت الوضع Android Debug Bridge (ADB) أو iTunes أو ما يعادلها من التطبيقات على الكمبيوتر، يقوم نظام التشغيل بتحديد الأجهزة المحمولة كأجهزة ADB أو iTunes. في جميع الحالات الأخرى، قد يحدد نظام التشغيل نوع الجهاز المحمول كجهاز متنقل (MTP) لنقل الملفات أو جهاز PTP (الكاميرا) لنقل الصور أو جهاز آخر. ويعتمد نوع الجهاز على طراز الجهاز المحمول ووضع اتصال USB المحدد. ويتيح لك Kaspersky Endpoint Security تكوين أذونات الوصول الفردية للبيانات الموجودة على الأجهزة المحمولة في تطبيقات ADB أو iTunes أو برنامج إدارة الملفات. وفي جميع الحالات الأخرى، يسمح التحكم في الجهاز بالوصول إلى الأجهزة المحمولة وفقًا لقواعد الوصول إلى الأجهزة المحمولة (MTP).

الوصول إلى الأجهزة المحمولة

تنتمي الأجهزة المحمولة إلى فئة الأجهزة المحمولة (MTP)، وبالتالي فإن الإعدادات الخاصة بها واحدة. يمكنك تحديد أحد الأوضاع التالية للوصول إلى الأجهزة المحمولة:

- **سماح**. يتيح تطبيق Kaspersky Endpoint Security الوصول الكامل إلى الأجهزة المحمولة. ويمكنك فتح الملفات أو إنشائها أو تعديلها أو نسخها أو حذفها على الأجهزة المحمولة باستخدام مدير الملفات أو تطبيقي ADB وiTunes. ويمكنك أيضًا شحن بطارية الجهاز عن طريق توصيل الجهاز المحمول بمنفذ USB بالكمبيوتر.
- **منع**. يقيد تطبيق Kaspersky Endpoint Security الوصول إلى الأجهزة المحمولة في مدير الملفات وتطبيقي ADB وiTunes. ويسمح التطبيق بالوصول فقط إلى الأجهزة المحمولة الموثوقة. ويمكنك أيضًا شحن بطارية الجهاز عن طريق توصيل الجهاز المحمول بمنفذ USB بالكمبيوتر.
- **يعتمد على ناقل الاتصال**. يسمح تطبيق Kaspersky Endpoint Security بالاتصال بالأجهزة المحمولة وفقًا لحالة توصيل USB (**سماح** أو **منع**).
- **حسب القواعد**. يقيد تطبيق Kaspersky Endpoint Security الوصول إلى الأجهزة المحمولة وفقًا للقواعد. وفي القواعد، يمكنك تكوين حقوق الوصول (القراءة / الكتابة)، وتحديد المستخدمين أو مجموعة من المستخدمين الذين يمكنهم الوصول إلى الأجهزة المحمولة (MTP)، وتكوين جدول وصول للأجهزة المحمولة. ويمكنك أيضًا تقييد الوصول إلى الأجهزة من خلال تطبيقي ADB وiTunes.

تكوين قواعد الوصول إلى الجهاز المحمول

يتم تكوين قواعد الوصول للأجهزة المحمولة (MTP) وأجهزة ADB وأجهزة iTunes بشكل مختلف. وبالنسبة للأجهزة المحمولة (MTP) وأجهزة ADB، يمكنك تكوين القواعد للمستخدمين الفرديين أو مجموعات المستخدمين وإنشاء جدول زمني لتطبيق القواعد. وبالنسبة لأجهزة iTunes، لا يمكنك فعل ذلك. ويمكنك فقط السماح بالوصول إلى البيانات أو رفضه من خلال تطبيق iTunes لجميع المستخدمين.

كيفية تكوين قواعد الوصول إلى الجهاز المحمول في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.

5. تحت **إعدادات التحكم في الجهاز**، حدد علامة التبويب **أنواع الأجهزة**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. في قائمة السياق لنوع الجهاز **أجهزة محمولة (MTP)**، قم بتكوين وضع الوصول إلى الجهاز المحمول: **سماح** أو **منع** أو **يعتمد على ناقل الاتصال**.

7. لتكوين قواعد الوصول إلى الأجهزة المحمولة، انقر نقرًا مزدوجًا لفتح قائمة القواعد.

8. تكوين قاعدة الوصول إلى الجهاز المحمول:

a. في القسم **قواعد الوصول**، انقر على الزر **إضافة**.

يفتح هذا نافذة لإضافة قاعدة وصول جديدة للجهاز المحمول.

b. في الحقل **الأولوية**، قم بتعيين أولوية كتابة القاعدة. تتضمن القاعدة السمات التالية: حساب المستخدم والجدول والأذونات (القراءة / الكتابة / الوصول إلى ADB) والأولوية.

تتضمن القاعدة أولوية محددة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. يسمح Kaspersky Endpoint Security بتعيين الأولوية من 0 إلى 10.000. كلما ارتفعت القيمة، زادت الأولوية. بمعنى آخر، يكون الإدخال بقيمة 0 بالأولوية الأدنى.

على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 1 لمجموعة المسؤولين وقم بتعيين أولوية من 0 لمجموعة "الجميع".

تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. بمعنى آخر، في حالة إضافة مستخدم إلى مجموعات متعددة وكانت أولوية جميع القواعد متشابهة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز استنادًا إلى أي قاعدة منع موجودة.

c. تحت **القاعدة للمستخدمين والمجموعات**، حدد المستخدمين أو مجموعات المستخدمين.

d. انقر على **موافق**.

9. تحت **جداول قاعدة الوصول المحددة**، كوّن جدولاً للوصول إلى الجهاز المحمول للمستخدمين.

لا يمكن تكوين جدول وصول منفصل لأجهزة ADB. ويمكنك تكوين جدول وصول مشترك لأجهزة ADB والأجهزة المحمولة (MTP).

10. كوّن أذونات وصول المستخدمين إلى الأجهزة المحمولة في برنامج إدارة الملفات (**قراءة / كتابة**).

11. كوّن الوصول إلى البيانات على جهاز محمول من خلال تطبيق ADB باستخدام خانة الاختيار **الوصول عبر ADB**.

في حالة إلغاء تحديد خانة الاختيار، عند توصيل الجهاز المحمول، يتم منع تطبيق ADB من اكتشاف الجهاز.

12. تحت **الوصول عبر iTunes**، كوّن الوصول إلى البيانات الموجودة على الجهاز المحمول من خلال تطبيق iTunes.

يطبق Kaspersky Endpoint Security الإعدادات الخاصة بالوصول إلى الجهاز المحمول من خلال تطبيق iTunes لجميع المستخدمين. ولا يمكن تكوين جدول وصول منفصل لأجهزة iTunes.

13. احفظ تغييراتك.

كيفية تكوين قواعد الوصول إلى الجهاز المحمول في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Device Control** ← **Security Controls**.

5. في القسم **Device Control Settings**، انقر على الرابط **Access rules for devices and Wi-Fi networks**.
يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. حدد نوع الجهاز **Portable devices (MTP)**.
يفتح هذا حقوق الوصول إلى الأجهزة المحمولة (MTP).

7. تحت **Configuring device access rules**، قم بتكوين وضع الوصول إلى الأجهزة المحمولة: **Allow** أو **Block** أو **Depends on connection bus** أو **By rules**.

8. إذا حددت الوضع **By rules**، يجب عليك إضافة قواعد الوصول للأجهزة. ولفعل ذلك، تحت **Users**، انقر على الزر **Add** وكوّن قاعدة الوصول إلى الجهاز المحمول:

   a. في الحقل **Rule of access to devices**، قم بتعيين أولوية كتابة القاعدة. تتضمن القاعدة السمات التالية: حساب المستخدم والجدول والأذونات (القراءة / الكتابة / الوصول إلى ADB) والأولوية.

   تتضمن القاعدة أولوية محددة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. يسمح Kaspersky Endpoint Security بتعيين الأولوية من 0 إلى 10.000. كلما ارتفعت القيمة، زادت الأولوية. بمعنى آخر، يكون الإدخال بقيمة 0 بالأولوية الأدنى.

   على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 1 لمجموعة المسؤولين وقم بتعيين أولوية من 0 لمجموعة "الجميع".

   تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. بمعنى آخر، في حالة إضافة مستخدم إلى مجموعات متعددة وكانت أولوية جميع القواعد متشابهة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز استنادًا إلى أي قاعدة منع موجودة.

   b. تحت **Users**، حدد المستخدمين أو مجموعات المستخدمين للوصول إلى الأجهزة المحمولة.

   c. تحت **Schedule for access to devices**، كوّن جدولاً للوصول إلى الجهاز المحمول للمستخدمين.

> لا يمكن تكوين جدول وصول منفصل لأجهزة ADB. ويمكنك تكوين جدول وصول مشترك لأجهزة ADB والأجهزة المحمولة (MTP).

   d. كوّن أذونات وصول المستخدمين إلى الأجهزة المحمولة في برنامج إدارة الملفات (**Read / Write**).

   e. كوّن الوصول إلى البيانات على جهاز محمول من خلال تطبيق ADB باستخدام خانة الاختيار **Access via ADB**.
   في حالة إلغاء تحديد خانة الاختيار، عند توصيل الجهاز المحمول، يتم منع تطبيق ADB من اكتشاف الجهاز.

   f. تحت **Access via iTunes**، كوّن الوصول إلى البيانات الموجودة على الجهاز المحمول من خلال تطبيق iTunes.

> يطبق Kaspersky Endpoint Security الإعدادات الخاصة بالوصول إلى الجهاز المحمول من خلال تطبيق iTunes لجميع المستخدمين. ولا يمكن تكوين جدول وصول منفصل لأجهزة iTunes.

9. احفظ تغييراتك.

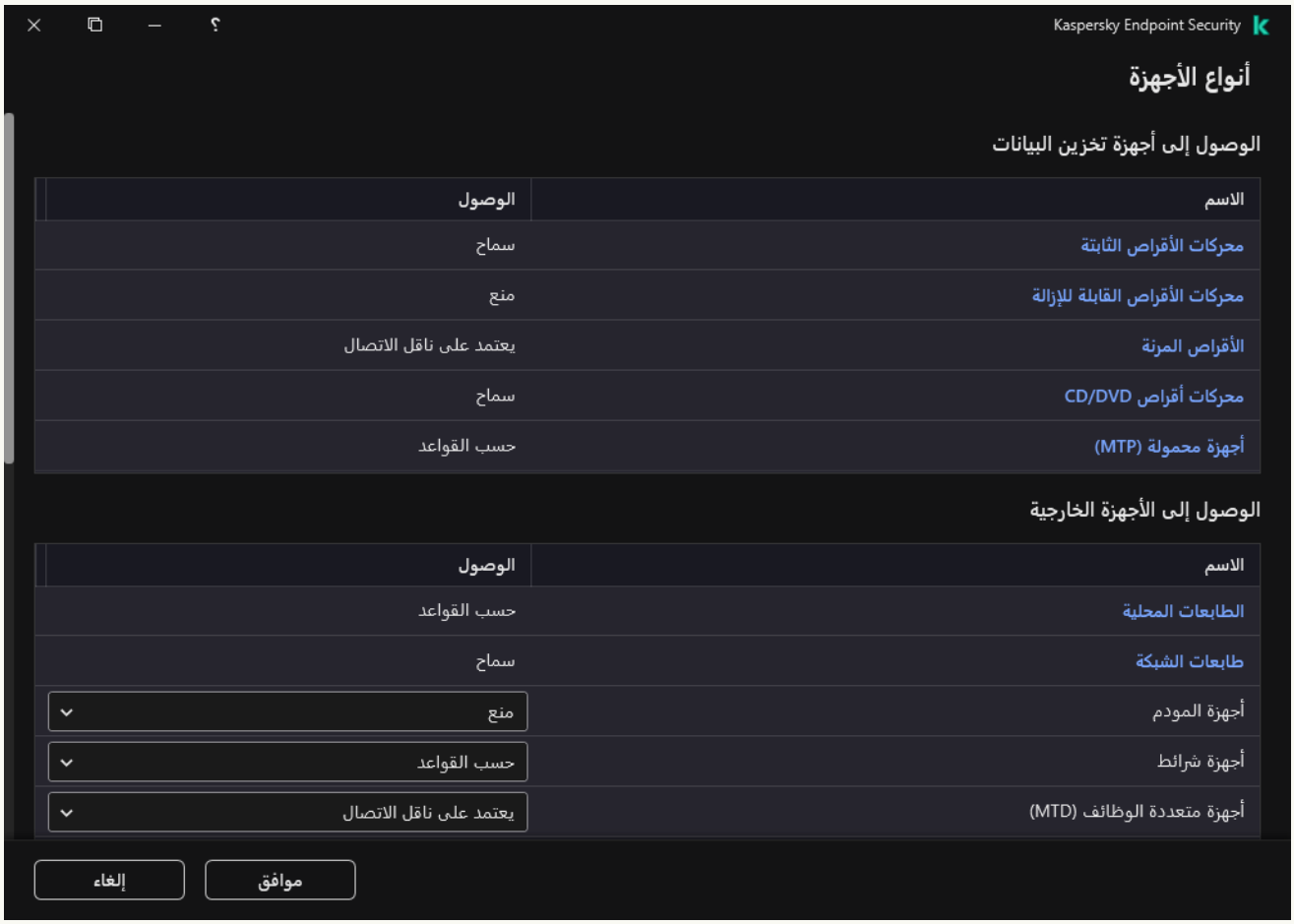
[كيفية تكوين قواعد الوصول إلى الجهاز المحمول في واجهة التطبيق](#)

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **إعدادات الوصول**، انقر على الزر **الأجهزة وشبكات Wi-Fi**.

تعرض النافذة المفتوحة قواعد الوصول لجميع الأجهزة المدرجة في تصنيف مكون التحكم في الجهاز.



أنواع الأجهزة في مكون التحكم في الجهاز

4. في القسم **الوصول إلى أجهزة تخزين البيانات**، انقر على الرابط **أجهزة محمولة (MTP)**.

يفتح هذا نافذة تحتوي على قواعد الوصول للأجهزة المحمولة (MTP).

5. تحت **الوصول**، قم بتكوين وضع الوصول إلى الأجهزة المحمولة: **سماح** أو **منع** أو **يعتمد على ناقل الاتصال** أو **حسب القواعد**.

6. إذا حددت الوضع **حسب القواعد**، يجب عليك إضافة قواعد الوصول للأجهزة.

a. في القسم **حقوق المستخدمين**، انقر على الزر **إضافة**.

يفتح هذا نافذة لإضافة قاعدة وصول جديدة للجهاز المحمول.

b. في الحقل **الأولوية**، قم بتعيين أولوية كتابة القاعدة. تتضمن القاعدة السمات التالية: حساب المستخدم والجدول والأذونات (القراءة / الكتابة / الوصول إلى ADB) والأولوية.

تتضمن القاعدة أولوية محددة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. يسمح Kaspersky Endpoint Security بتعيين الأولوية من 0 إلى 10.000. كلما ارتفعت القيمة، زادت الأولوية. بمعنى آخر، يكون الإدخال بقيمة 0 بالأولوية الأدنى.

على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 1 لمجموعة المسؤولين وقم بتعيين أولوية من 0 لمجموعة "الجميع".

تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. بمعنى آخر، في حالة إضافة مستخدم إلى مجموعات متعددة وكانت أولوية جميع القواعد متشابهة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز استنادًا إلى أي قاعدة منع موجودة.

c. تحت **الحالة**، قم بتشغيل قاعدة الوصول إلى الجهاز المحمول.

d. تحت **قواعد الوصول**، كوّن أذونات الوصول إلى الجهاز المحمول للمستخدمين.

- كوّن أذونات وصول المستخدمين إلى الأجهزة المحمولة في برنامج إدارة الملفات (**قراءة / كتابة**).
- كوّن الوصول إلى البيانات على جهاز محمول من خلال تطبيق ADB باستخدام خانة الاختيار **الوصول عبر ADB**.
  في حالة إلغاء تحديد خانة الاختيار، عند توصيل الجهاز المحمول، يتم منع تطبيق ADB من اكتشاف الجهاز.

e. تحت **المستخدمون**، حدد المستخدمين أو مجموعات المستخدمين للوصول إلى الأجهزة المحمولة.

f. تحت **جدول الوصول إلى الأجهزة**، كوّن جدول وصول للجهاز للمستخدمين.

لا يمكن تكوين جدول وصول منفصل لأجهزة ADB. ويمكنك تكوين جدول وصول مشترك لأجهزة ADB والأجهزة المحمولة (MTP).

g. تحت **الوصول عبر iTunes**، كوّن الوصول إلى البيانات الموجودة على الجهاز المحمول من خلال تطبيق iTunes.

يطبق Kaspersky Endpoint Security الإعدادات الخاصة بالوصول إلى الجهاز المحمول من خلال تطبيق iTunes لجميع المستخدمين. ولا يمكن تكوين جدول وصول منفصل لأجهزة iTunes.

7. احفظ تغييراتك.

نتيجة لذلك، يتم تقييد وصول المستخدم إلى الأجهزة المحمولة وفقًا للقواعد. إذا كان لديك وصول محظور إلى الأجهزة المحمولة في تطبيقي ADB وiTunes عند توصيل جهاز محمول، يتم منع تطبيقي ADB وiTunes من اكتشاف الجهاز المحمول.

الأجهزة المحمولة الموثوقة

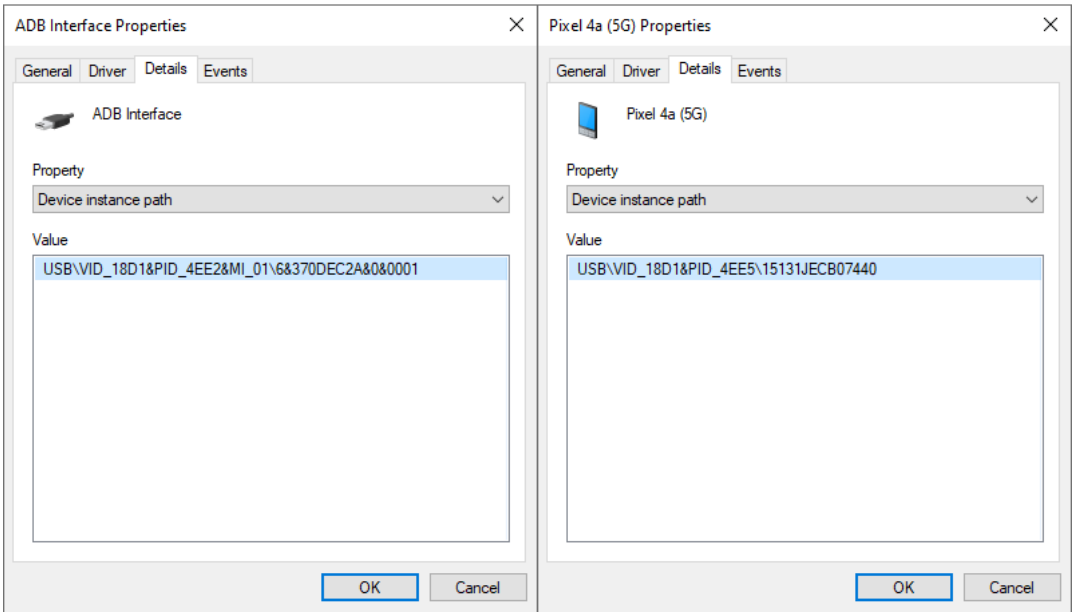
الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

يشبه إجراء إضافة جهاز محمول موثوق تمامًا إضافة الأنواع الأخرى من الأجهزة الموثوقة. ويمكنك إضافة جهاز محمول حسب المعرف أو طراز الجهاز.

لإضافة جهاز محمول موثوق بواسطة المعرف، ستحتاج إلى معرف فريد (معرف الجهاز – HWID). ويمكنك العثور على المعرف في خصائص الجهاز باستخدام أدوات نظام التشغيل (انظر الشكل أدناه). وتتيح لك أداة إدارة الأجهزة فعل ذلك. وتختلف معرفات الأجهزة المحمولة (MTP) وأجهزة ADB وiTunes حتى للجهاز المحمول نفسه. قد يبدو معرّف الجهاز المحمول (MTP) كما يلي: `15131JECB07440`. وقد يبدو معرف جهاز ADB كما يلي: `370DEC2A&0&C000&6`. إضافة الأجهزة حسب المُعرِّف عملية ملائمة إذا كنت ترغب في إضافة مجموعة أجهزة محددة. ويمكنك أيضًا استخدام الأقنعة.

إذا قمت بتثبيت تطبيقات ADB أو iTunes بعد توصيل جهاز بالكمبيوتر، فقد يتم إعادة تعيين المعرف الفريد للجهاز. يعني هذا أن Kaspersky Endpoint Security سوف يتعرف على هذا الجهاز كأنه جهاز جديد. إذا كان الجهاز موثوقًا، أضف الجهاز إلى القائمة الموثوقة مرة أخرى.

لإضافة جهاز محمول موثوق حسب موديل الجهاز، ستحتاج إلى معرف البائع (VID) ومعرف المنتج (PID). ويمكنك العثور على المعرفات في خصائص الجهاز باستخدام أدوات نظام التشغيل (انظر الشكل أدناه). قالب إدخال معرف البائع ومعرف المنتج: `VID_18D1&PID_4EE5`. إضافة أجهزة حسب الموديل طريقة ملائمة إذا كنت تستخدم أجهزة ذات موديل معين في مؤسستك. بهذه الطريقة، يمكنك إضافة جميع الأجهزة من هذا الموديل.



معرف الجهاز في إدارة الأجهزة

التحكم في الطباعة

يمكنك استخدام التحكم في الطباعة لتكوين وصول المستخدم إلى الطابعات المحلية وطابعات الشبكة.

التحكم في الطابعة المحلية

يتيح Kaspersky Endpoint Security تكوين الوصول إلى الطابعات المحلية على مستويين: جارٍ التوصيل والطباعة.

يتحكم Kaspersky Endpoint Security في اتصال الطابعة المحلية عبر النواقل التالية: USB والمنفذ التسلسلي (COM)، المنفذ المتوازي (LPT).

يتحكم تطبيق Kaspersky Endpoint Security في اتصال الطابعات المحلية بمنافذ COM وLPT على مستوى الناقل فقط. أي لمنع اتصال الطابعات بمنافذ COM وLPT، يجب حظر اتصال كل أنواع الأجهزة بنواقل COM وLPT. وبالنسبة للطابعات المتصلة بمنفذ USB، يمارس التطبيق التحكم على مستويين: نوع الجهاز (الطابعات المحلية) وناقل الاتصال (USB). لذلك يمكنك السماح لجميع أنواع الأجهزة باستثناء الطابعات المحلية بالاتصال بمنفذ USB.

تستطيع تحديد أحد أوضاع الوصول إلى الطابعات المحلية التالية عبر USB:

- **سماح**. يمنح Kaspersky Endpoint Security وصولاً كاملاً إلى الطابعات المحلية لجميع المستخدمين. ويستطيع المستخدمون توصيل الطابعات وطباعة المستندات باستخدام الوسائل التي يوفرها نظام التشغيل.
- **منع**. يحظر Kaspersky Endpoint Security اتصال الطابعات المحلية. ويسمح التطبيق باتصال الطابعات الموثوقة فقط.
- **يعتمد على ناقل الاتصال**. يسمح Kaspersky Endpoint Security بالاتصال بالطابعات المحلية حسب حالة اتصال ناقل USB (**سماح** أو **منع**).
- **حسب القواعد**. للتحكم في الطباعة، يجب عليك إضافة قواعد الطباعة. وفي القواعد، يمكنك تحديد المستخدمين أو مجموعة من المستخدمين الذين تريد السماح لهم أو حتى منعهم من الوصول إلى طباعة المستندات على الطابعات المحلية.

التحكم في طابعة الشبكة

يتيح Kaspersky Endpoint Security تكوين الوصول إلى الطباعة على طابعات الشبكة. وتستطيع تحديد أحد أوضاع الوصول التالية على طابعات الشبكة:

- **السماح وعدم التسجيل**. لا يتحكم Kaspersky Endpoint Security في الطباعة على طابعات الشبكة. ويتيح التطبيق الوصول إلى الطباعة على طابعات الشبكة لجميع المستخدمين ولا يحفظ معلومات الطباعة في سجل الأحداث.
- **سماح**. يمنح Kaspersky Endpoint Security الوصول إلى الطباعة على طابعات الشبكة لجميع المستخدمين.
- **منع**. يقيد Kaspersky Endpoint Security الوصول إلى طابعات الشبكة لجميع المستخدمين. ويسمح التطبيق بالوصول فقط إلى الطابعات الموثوقة.
- **حسب القواعد**. يمنح Kaspersky Endpoint Security إمكانية الوصول إلى الطباعة وفقًا لقواعد الطباعة. وفي القواعد، يمكنك تحديد المستخدمين أو مجموعة من المستخدمين الذين سيتم السماح لهم أو حتى منعهم من طباعة المستندات على طابعة الشبكة.

إضافة قواعد الطباعة للطابعات

كيفية إضافة قواعد مخصصة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.

5. تحت **إعدادات التحكم في الجهاز**، حدد علامة التبويب **أنواع الأجهزة**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. في قائمة السياق لأنواع أجهزة **الطابعات المحلية** و**طابعات الشبكة**، كوّن وضع الوصول للطابعات ذات الصلة: **سماح** و**منع** أو **السماح وعدم التسجيل** (لطابعات الشبكة فقط) أو **يعتمد على ناقل الاتصال** (للطابعات المحلية فقط).

7. لتكوين قواعد الطباعة على الطابعات المحلية وطابعات الشبكة، انقر نقرًا مزدوجًا فوق قوائم القواعد لفتحها.

8. يختار **حسب القواعد** كوضع وصول للطابعة.

9. حدد المستخدمين أو مجموعة المستخدمين الذين تريد تطبيق قاعدة الطباعة عليهم.

a. انقر على **إضافة**.

يفتح هذا نافذة لإضافة قاعدة طباعة جديدة.

b. قم بتعيين أولوية إدخال القاعدة. يتضمن إدخال القاعدة السمات التالية: حساب المستخدم والإجراء (سماح/منع) والأولوية.

تتضمن القاعدة أولوية محددة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. يسمح Kaspersky Endpoint Security بتعيين الأولوية من 0 إلى 10.000. كلما ارتفعت القيمة، زادت الأولوية. بمعنى آخر، يكون الإدخال بقيمة 0 بالأولوية الأدنى.

على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 1 لمجموعة المسؤولين وقم بتعيين أولوية من 0 لمجموعة "الجميع".

تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. بمعنى آخر، في حالة إضافة مستخدم إلى مجموعات متعددة وكانت أولوية جميع القواعد متشابهة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز استنادًا إلى أي قاعدة منع موجودة.

c. تحت **الإجراء**، كوّن وصول المستخدم إلى الطباعة على الطابعة.

d. تحت **المستخدمون والمجموعات**، حدد المستخدمين أو مجموعات المستخدمين للوصول إلى الطباعة.

e. انقر على **موافق**.

10. احفظ تغييراتك.

[كيفية إضافة قواعد طباعة في Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Security Controls** ← **Device Control**.

5. في القسم **Device Control Settings**، انقر على الرابط **Access rules for devices and Wi-Fi networks**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. حدد نوع الجهاز **Local printers** أو **Network printers**.

يفتح هذا قواعد وصول الطابعة.

7. كوّن وضع الوصول للطابعات ذات الصلة: **Allow** و**Block** و**السماح وعدم التسجيل** (لطابعات الشبكة فقط) أو **Depends on connection bus** (للطابعات المحلية فقط) أو **By rules**.

8. إذا حددت وضع **By rules**، يجب إضافة قواعد الطباعة للطابعات المحلية أو طابعات الشبكة. ولفعل ذلك، انقر فوق الزر **Add** في جدول قواعد الطباعة.

يفتح هذا إعدادات قاعدة الطباعة الجديدة.

9. قم بتعيين أولوية إدخال القاعدة. يتضمن إدخال القاعدة السمات التالية: حساب المستخدم والإجراء (سماح/منع) والأولوية.

تتضمن القاعدة أولوية محددة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. يسمح Kaspersky Endpoint Security بتعيين الأولوية من 0 إلى 10.000. كلما ارتفعت القيمة، زادت الأولوية. بمعنى آخر، يكون الإدخال بقيمة 0 بالأولوية الأدنى.

على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 1 لمجموعة المسؤولين وقم بتعيين أولوية من 0 لمجموعة "الجميع".

تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. بمعنى آخر، في حالة إضافة مستخدم إلى مجموعات متعددة وكانت أولوية جميع القواعد متشابهة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز استنادًا إلى أي قاعدة منع موجودة.

10. تحت **Action**، كوّن وصول المستخدم إلى الطباعة على الطابعة.

11. تحت **Users and groups**، حدد المستخدمين أو مجموعات المستخدمين للوصول إلى الطباعة.

12. احفظ تغييراتك.

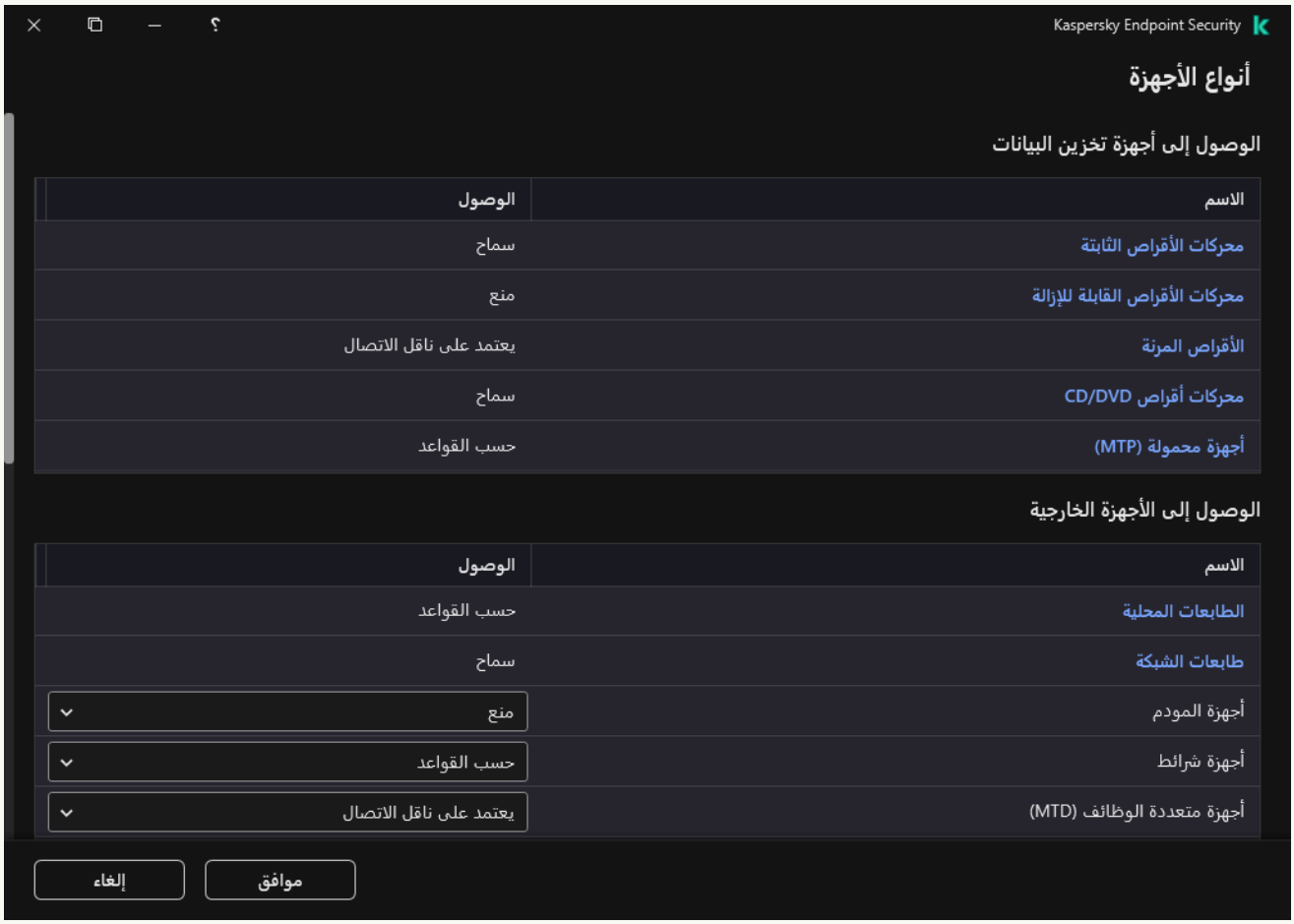
كيفية إضافة قواعد طباعة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **إعدادات الوصول**، انقر على الزر **الأجهزة وشبكات Wi-Fi**.

تعرض النافذة المفتوحة قواعد الوصول لجميع الأجهزة المدرجة في تصنيف مكون التحكم في الجهاز.



أنواع الأجهزة في مكون التحكم في الجهاز

4. تحت **الوصول إلى الأجهزة الخارجية**، انقر على **الطابعات المحلية** أو **طابعات الشبكة**.

يفتح هذا نافذة بقواعد وصول الطابعة.

5. تحت **الوصول إلى الطابعات المحلية** أو **الوصول إلى طابعات الشبكة** كوّن وضع الوصول للطابعات: **سماح** و**منع** و**السماح وعدم التسجيل** (لطابعات الشبكة فقط) أو **يعتمد على ناقل الاتصال** (للطابعات المحلية فقط) أو **حسب القواعد**.

6. إذا حددت الوضع **حسب القواعد**، يجب إضافة قواعد الطباعة للطابعات. حدد المستخدمين أو مجموعة المستخدمين الذين تريد تطبيق قاعدة الطباعة عليهم.

a. انقر على **إضافة**.

يفتح هذا نافذة لإضافة قاعدة طباعة جديدة.

b. قم بتعيين أولوية إدخال القاعدة. ويتضمن إدخال القاعدة السمات التالية: حساب المستخدم والأذونات (سماح/منع) والأولوية.

تتضمن القاعدة أولوية محددة. وفي حالة إضافة مستخدم إلى مجموعات متعددة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز بناءً على القاعدة ذات الأولوية الأعلى. يسمح Kaspersky Endpoint Security بتعيين الأولوية من 0 إلى 10.000. كلما ارتفعت القيمة، زادت الأولوية. بمعنى آخر، يكون الإدخال بقيمة 0 بالأولوية الأدنى.

على سبيل المثال، يمكنك منح أذونات القراءة فقط لمجموعة "الجميع" ومنح أذونات القراءة/الكتابة لمجموعة المسؤولين. ولفعل ذلك، قم بتعيين أولوية من 1 لمجموعة المسؤولين وقم بتعيين أولوية من 0 لمجموعة "الجميع".

تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. بمعنى آخر، في حالة إضافة مستخدم إلى مجموعات متعددة وكانت أولوية جميع القواعد متشابهة، ينظم Kaspersky Endpoint Security الوصول إلى الجهاز استنادًا إلى أي قاعدة منع موجودة.

c. تحت **الإجراء**، كوّن أذونات المستخدم للوصول إلى الطباعة.

d. تحت **المستخدمون والمجموعات**، حدد المستخدمين أو مجموعات المستخدمين للوصول إلى الطباعة.

7. احفظ تغييراتك.

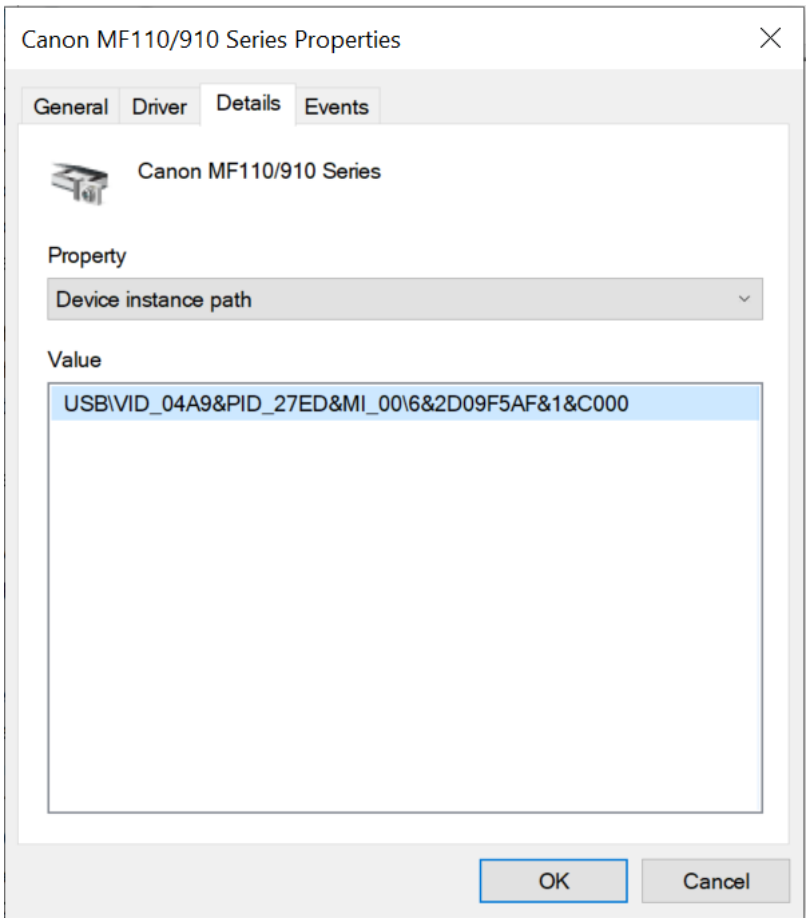
الطابعات الموثوقة

الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

يشبه إجراء إضافة طابعات موثوقة تمامًا إضافة الأنواع الأخرى من الأجهزة الموثوقة. ويمكنك إضافة طابعات محلية حسب المعرف أو موديل الجهاز. ويمكنك فقط إضافة طابعات الشبكة من خلال معرف الجهاز.

لإضافة طابعة محلية موثوقة بواسطة المعرف، ستحتاج إلى معرف فريد (معرف الجهاز – HWID). ويمكنك العثور على المعرف في خصائص الجهاز باستخدام أدوات نظام التشغيل (انظر الشكل أدناه). وتتيح لك أداة إدارة الأجهزة فعل ذلك. وقد يبدو معرف الطابعة المحلية كما يلي: `2D09F5AF&1&C000&6`. إضافة الأجهزة حسب المُعرّف عملية ملائمة إذا كنت ترغب في إضافة مجموعة أجهزة محددة. ويمكنك أيضًا استخدام الأقنعة.

لإضافة طابعة محلية موثوقة حسب موديل الجهاز، ستحتاج إلى معرف البائع (VID) ومعرف المنتج (PID). ويمكنك العثور على المعرفات في خصائص الجهاز باستخدام أدوات نظام التشغيل (انظر الشكل أدناه). قالب إدخال معرف البائع ومعرف المنتج: `VID_04A9&PID_27FD`. إضافة أجهزة حسب الموديل طريقة ملائمة إذا كنت تستخدم أجهزة ذات موديل معين في مؤسستك. بهذه الطريقة، يمكنك إضافة جميع الأجهزة من هذا الموديل.



معرف الجهاز في إدارة الأجهزة

لإضافة طابعة شبكة موثوقة، ستحتاج إلى معرف الجهاز الخاص بها. وبالنسبة لطابعات الشبكة، يمكن أن يكون معرف الجهاز هو اسم الشبكة الخاص بالطابعة (اسم الطابعة المشتركة) أو عنوان IP الخاص بالطابعة أو عنوان URL الخاص بالطابعة.

التحكم في اتصالات Wi-Fi

يسمح التحكم في الجهاز بإدارة اتصال Wi-Fi للكمبيوتر (الكمبيوتر المحمول). وقد تكون شبكات Wi-Fi العامة غير آمنة، وقد يؤدي استخدام هذه الشبكات إلى فقدان البيانات. ويتيح لك التحكم في الجهاز حظر المستخدم من الاتصال بشبكة Wi-Fi أو السماح بالاتصال فقط بالشبكات الموثوقة. على سبيل المثال، يمكنك السماح بالاتصال فقط بشبكة Wi-Fi الخاصة بالشركة التي تكون آمنة بدرجة كافية. سيقوم مكون التحكم في الجهاز بمنع الوصول إلى شبكات Wi-Fi باستثناء الشبكات المحددة في القائمة الموثوقة.

كيفية تقييد اتصالات Wi-Fi في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.

5. تحت **إعدادات التحكم في الجهاز**، حدد علامة التبويب **أنواع الأجهزة**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. في قائمة السياق لنوع جهاز **Wi-Fi**، حدد إجراء التحكم في الجهاز الذي يتم اتخاذه عند الاتصال بشبكة Wi-Fi: **سماح** (✓) أو **منع** (⊘) أو **حظر مع استثناءات** (📋).

7. إذا حددت الخيار **حظر مع استثناءات**، أنشئ قائمة بشبكات Wi-Fi الموثوقة:

a. انقر نقرًا مزدوجًا لفتح قائمة شبكات Wi-Fi الموثوقة.

b. في القسم **شبكات Wi-Fi الموثوقة**، انقر على الزر **إضافة**.

c. يفتح هذا نافذة، وفي تلك النافذة، قم بتهيئة شبكة Wi-Fi الموثوقة (انظر الشكل أدناه):

- **اسم شبكة الاتصال**. الاسم أو SSID (معرف مجموعة الخدمات) لشبكة Wi-Fi.
- **نوع المصادقة**. نوع المصادقة المستخدم عند الاتصال بشبكة Wi-Fi.
- **نوع التشفير**. نوع التشفير المستخدم لحماية حركة مرور Wi-Fi.
- **تعليق**. المزيد من المعلومات عن شبكة Wi-Fi المضافة.

يمكنك عرض إعدادات شبكة Wi-Fi الموثوقة في إعدادات جهاز التوجيه.

يتم اعتبار شبكة Wi-Fi موثوقة إذا تطابقت إعداداتها مع كل الإعدادات المحددة في القاعدة.

8. احفظ تغييراتك.

إعدادات شبكة Wi-Fi الموثوقة

[كيفية تقييد اتصالات Wi-Fi في Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Device Control** ← **Security Controls**.

5. في القسم **Device Control Settings**، انقر على الرابط **Access rules for devices and Wi-Fi networks**.
يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. في القسم **Access to Wi-Fi networks**، انقر على الرابط **Wi-Fi**.

7. ضمن **Access to Wi-Fi networks**، اختر إجراء التحكم في الجهاز الذي تم اتخاذه عند الاتصال بشبكة Wi-Fi: **Allow** أو **Block** أو **Block with exceptions**.

8. إذا حددت الخيار **Block with exceptions**، أنشئ قائمة بشبكات Wi-Fi الموثوقة:

   a. انقر نقرًا مزدوجًا لفتح قائمة شبكات Wi-Fi الموثوقة.

   b. في القسم **Trusted Wi-Fi networks**، انقر على الزر **Add**.

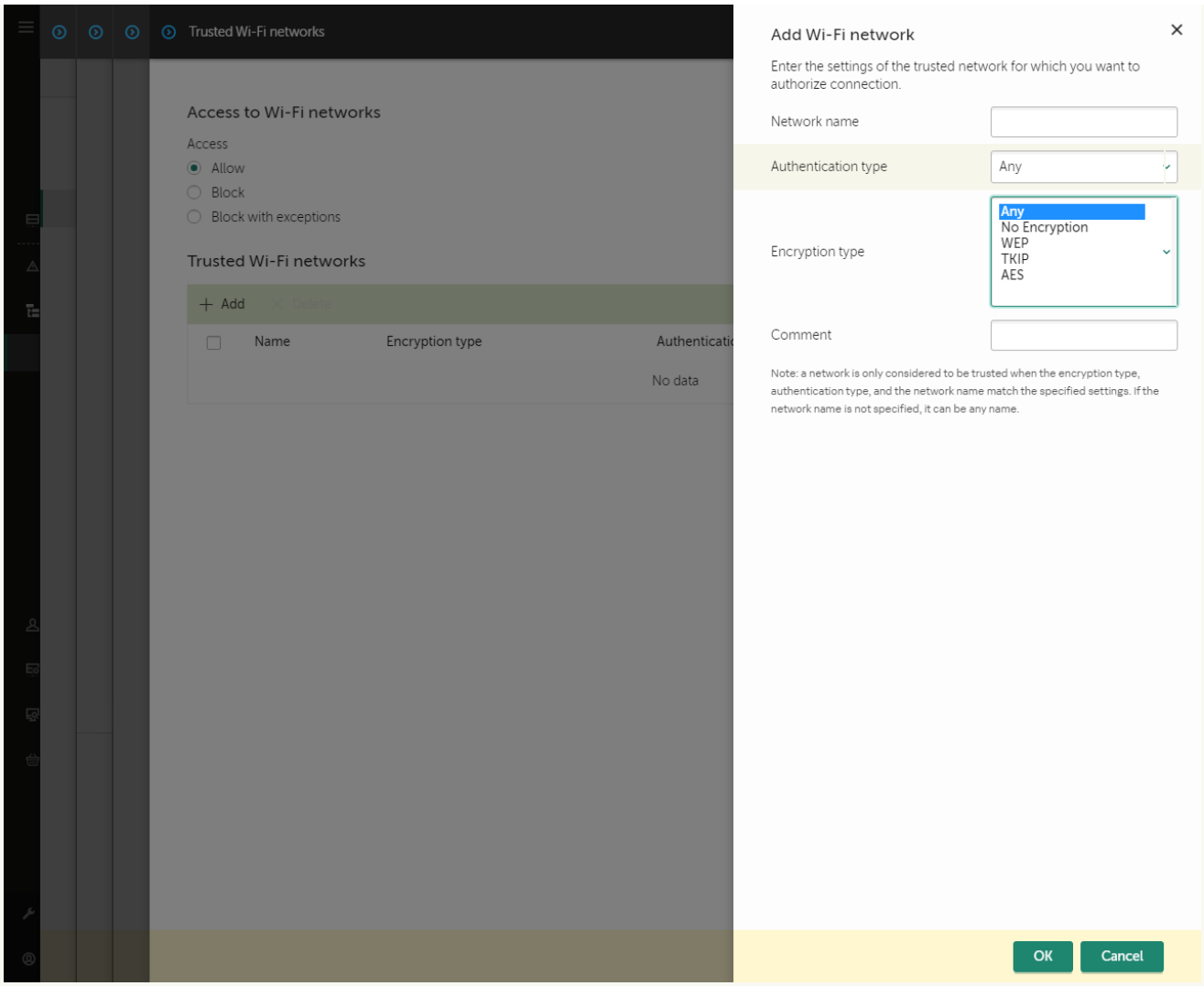
   c. يفتح هذا نافذة، وفي تلك النافذة، قم بتهيئة شبكة Wi-Fi الموثوقة (انظر الشكل أدناه):

   - **Network name**. الاسم أو SSID (معرف مجموعة الخدمات) لشبكة Wi-Fi.
   - **Authentication type**. نوع المصادقة المستخدم عند الاتصال بشبكة Wi-Fi.
   - **Encryption type**. نوع التشفير المستخدم لحماية حركة مرور Wi-Fi.
   - **Comment**. المزيد من المعلومات عن شبكة Wi-Fi المضافة.

   يمكنك عرض إعدادات شبكة Wi-Fi الموثوقة في إعدادات جهاز التوجيه.

   يتم اعتبار شبكة Wi-Fi موثوقة إذا تطابقت إعداداتها مع كل الإعدادات المحددة في القاعدة.

9. احفظ تغييراتك.



إعدادات شبكة Wi-Fi الموثوقة

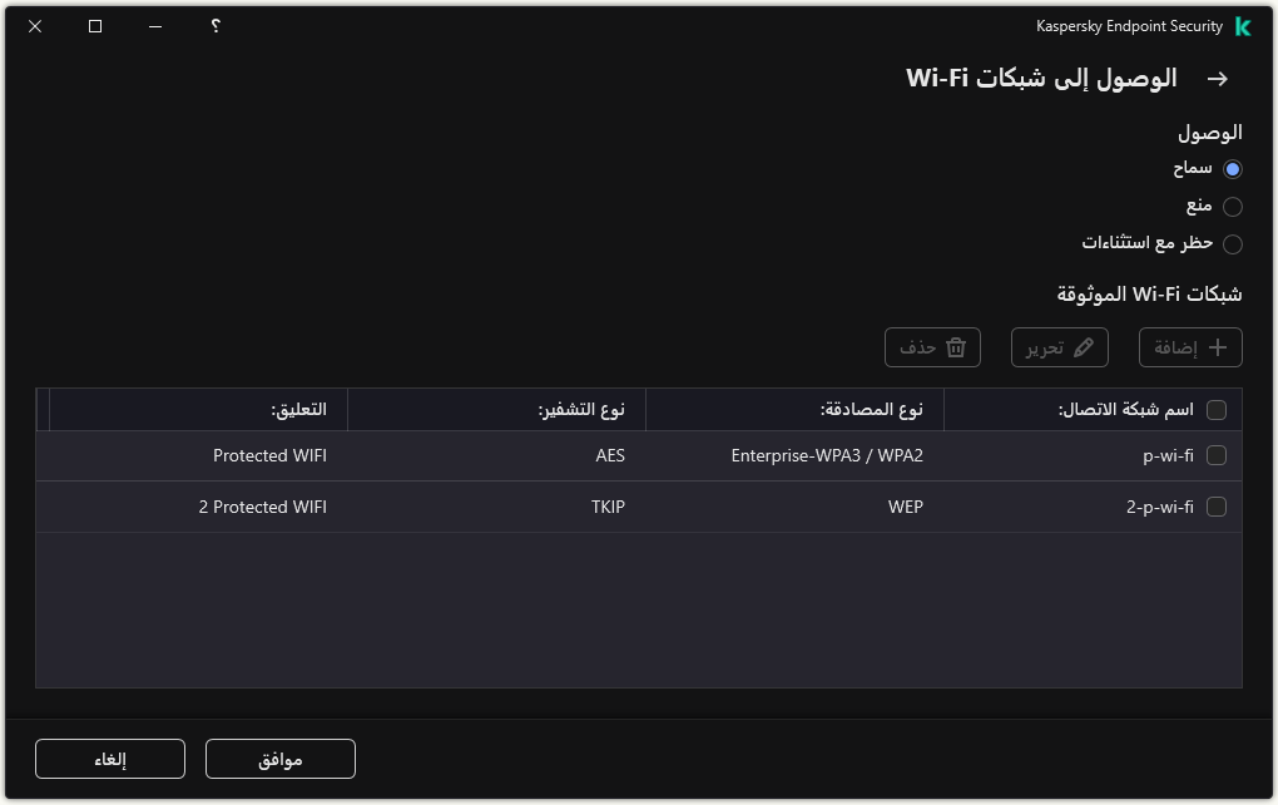
[كيفية تقييد اتصالات Wi-Fi في واجهة التطبيق]

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **إعدادات الوصول**، انقر على الزر **الأجهزة وشبكات Wi-Fi**.
تعرض النافذة المفتوحة قواعد الوصول لجميع الأجهزة المدرجة في تصنيف مكون التحكم في الجهاز.

4. في القسم **الوصول إلى شبكات Wi-Fi**، انقر على الرابط **Wi-Fi**.
تعرض النافذة المفتوحة قواعد الوصول إلى شبكة Wi-Fi.



إعدادات الوصول إلى Wi-Fi

5. ضمن **الوصول**، اختر إجراء التحكم في الجهاز الذي تم اتخاذه عند الاتصال بشبكة Wi-Fi: **سماح** أو **منع** أو **حظر مع استثناءات**.

6. إذا حددت الخيار **حظر مع استثناءات**، أنشئ قائمة بشبكات Wi-Fi الموثوقة:

a. في القسم **شبكات Wi-Fi الموثوقة**، انقر على الزر **إضافة**.

b. يفتح هذا نافذة، وفي تلك النافذة، قم بتهيئة شبكة Wi-Fi الموثوقة (انظر الشكل أدناه):

- **اسم شبكة الاتصال**. الاسم أو SSID (معرف مجموعة الخدمات) لشبكة Wi-Fi.
- **نوع المصادقة**. نوع المصادقة المستخدم عند الاتصال بشبكة Wi-Fi.
- **نوع التشفير**. نوع التشفير المستخدم لحماية حركة مرور Wi-Fi.
- **التعليق**. المزيد من المعلومات عن شبكة Wi-Fi المضافة.

يمكنك عرض إعدادات شبكة Wi-Fi الموثوقة في إعدادات جهاز التوجيه.

يتم اعتبار شبكة Wi-Fi موثوقة إذا تطابقت إعداداتها مع كل الإعدادات المحددة في القاعدة.

7. احفظ تغييراتك.

إعدادات شبكة Wi-Fi الموثوقة

نتيجة لذلك، عندما يحاول المستخدم الاتصال بشبكة Wi-Fi غير مدرجة كموثوقة، يحظر التطبيق الاتصال ويعرض إخطارًا (انظر الشكل أدناه).

إخطار التحكم في الجهاز

مراقبة استخدام محركات الأقراص القابلة للإزالة

تتضمن مراقبة استخدام محركات الأقراص القابلة للإزالة:

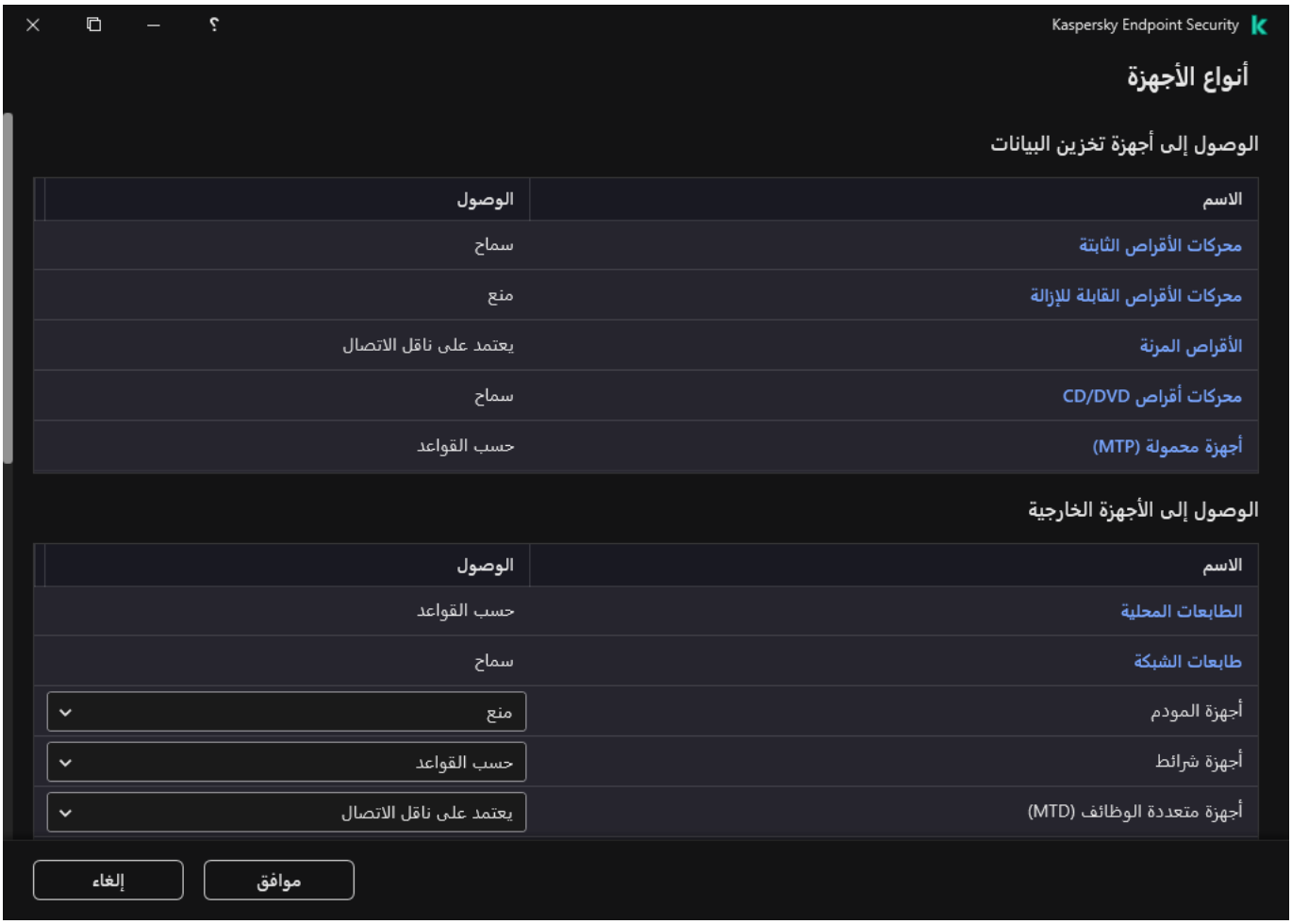
- مراقبة العمليات على الملفات الموجودة على محركات الأقراص القابلة للإزالة.
- مراقبة الاتصال وقطع الاتصال لمحركات الأقراص القابلة للإزالة الموثوقة.

يسمح Kaspersky Endpoint Security بمراقبة الاتصال وقطع الاتصال لجميع الأجهزة الموثوقة وليس فقط محركات الأقراص القابلة للإزالة. ويمكنك تشغيل تسجيل الأحداث في إعدادات الإخطار لمكون التحكم في الجهاز. لدى الأحداث مستوى الخطورة معلوماتي.

لتمكين مراقبة استخدام محرك الأقراص القابل للإزالة:

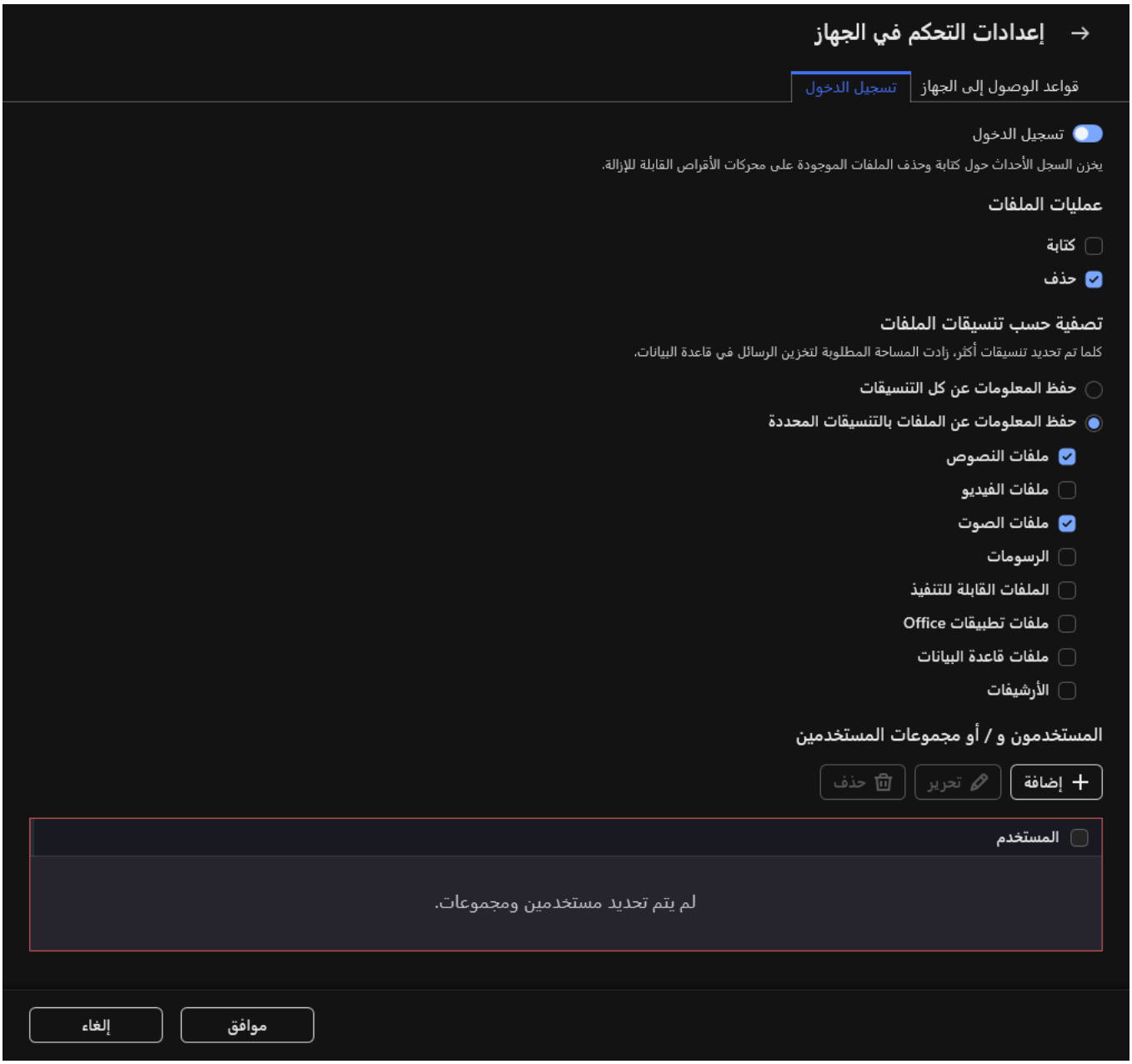
1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.
3. في القسم **إعدادات الوصول**، انقر على الزر **الأجهزة وشبكات Wi-Fi**.

تعرض النافذة المفتوحة قواعد الوصول لجميع الأجهزة المدرجة في تصنيف مكون التحكم في الجهاز.



أنواع الأجهزة في مكون التحكم في الجهاز

4. في القسم **الوصول إلى أجهزة تخزين البيانات**، حدد **محركات الأقراص القابلة للإزالة**.
5. في النافذة التي تفتح، حدد القسم **تسجيل الدخول**.



إعدادات مراقبة استخدام محرك الأقراص القابل للإزالة

6. قم بتشغيل مفتاح **تسجيل الدخول**.

7. في القسم **عمليات الملفات**، حدد العمليات التي تريد مراقبتها: **كتابة**، **حذف**.

8. في القسم **تصفية حسب تنسيقات الملفات**، حدد تنسيقات الملفات التي يجب تسجيل العمليات المرتبطة بها عن طريق التحكم في الجهاز.

9. حدد المستخدمين أو مجموعة المستخدمين الذين تريد مراقبة استخدامهم لمحركات الأقراص القابلة للإزالة.

10. احفظ تغييراتك.

نتيجة لذلك، عندما يكتب المستخدمون إلى الملفات الموجودة على محركات الأقراص القابلة للإزالة أو يحذفون الملفات من محركات الأقراص القابلة للإزالة، سيحفظ Kaspersky Endpoint Security المعلومات حول هذه العمليات في سجل الأحداث ويرسل الأحداث إلى Kaspersky Security Center. يمكنك عرض الأحداث المرتبطة بالملفات على محركات الأقراص القابلة للإزالة في وحدة تحكم إدارة Kaspersky Security Center في عقدة مساحة عمل **خادم الإدارة** من علامة التبويب **الأحداث**. بالنسبة للأحداث المُراد عرضها في سجل الأحداث المحلي لتطبيق Kaspersky Endpoint Security، يجب تحديد خانة الاختيار **تم تنفيذ عملية الملف** في notifications settings لمكون التحكم في الجهاز.

تغيير مدة التخزين المؤقت

يسجل مكون التحكم في الجهاز الأحداث المتعلقة بالأجهزة التي يتم مراقبتها، مثل توصيل الجهاز وفصله وقراءة ملف من الجهاز وكتابة ملف إلى الجهاز والأحداث الأخرى. ثم يسمح التحكم في الجهاز بالإجراء أو يحظره وفقًا لإعدادات Kaspersky Endpoint Security.

يحفظ التحكم في الجهاز معلومات حول الأحداث لفترة زمنية محددة تسمى فترة التخزين المؤقت. وفي حالة تخزين معلومات حول حدث ما مؤقتًا وتكرر هذا الحدث، فلا داعي لإخطار Kaspersky Endpoint Security به أو لإظهار مطالبة أخرى لمنح الوصول إلى الإجراء المقابل، مثل توصيل جهاز. ويجعل هذا العمل مع الجهاز أكثر سهولة.

يعتبر الحدث مكررًا إذا تطابقت جميع إعدادات الحدث التالية مع السجل الموجود في ذاكرة التخزين المؤقت:

- معرّف الجهاز
- يحاول SID لحساب المستخدم الوصول
- فئة الجهاز
- الإجراء الذي تم اتخاذه مع الجهاز
- إذن التطبيق لهذا الإجراء: مسموح به أو مرفوض
- المسار إلى العملية المستخدمة لاتخاذ الإجراء
- الملف الذي يتم الوصول إليه

قبل تغيير فترة التخزين المؤقت، قم بتعطيل الدفاع الذاتي في Kaspersky Endpoint Security. بعد تغيير فترة التخزين المؤقت، يرجى تمكين الدفاع الذاتي.

لتغيير فترة التخزين المؤقت:

1. افتح محرر التسجيل على الكمبيوتر.
2. في محرر التسجيل، انتقل إلى القسم التالي:
   - لأنظمة تشغيل 64 بت:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - لأنظمة تشغيل 32 بت: `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. افتح `DeviceControlEventsCachePeriod` لتحريره.
4. حدد عدد الدقائق التي يجب أن يحفظ فيها التحكم في الجهاز معلومات حول حدث ما قبل حذف هذه المعلومات.

الإجراءات المصاحبة للأجهزة الموثوقة

الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

للعمل مع الأجهزة الموثوقة، يمكنك منح الوصول إلى مستخدم على حدة أو مجموعة مستخدمين أو إلى جميع المستخدمين في المؤسسة.

على سبيل المثال: إذا كانت مؤسستك لا تسمح لمستخدم محركات الأقراص القابلة للإزالة لكن يمكن للمسؤولين استخدام محركات الأقراص القابلة للإزالة في عملهم، يمكنك إتاحة محركات الأقراص القابلة للإزالة لمجموعة محددة من المسؤولين. لفعل ذلك، أضف محركات الأقراص القابلة للإزالة إلى قائمة "موثوق" وقم بتحديد أذونات وصول المستخدمين.

لا يوصى بإضافة أكثر من 1000 جهاز موثوق، حيث يمكن أن يتسبب ذلك في عدم استقرار النظام.

Kaspersky Endpoint Security يتيح لك إضافة جهاز إلى قائمة "الموثوق" بالطرق التالية:

- إذا كان Kaspersky Security Center غير مطبق في مؤسستك، يمكنك توصيل الجهاز بجهاز الكمبيوتر ثم إضافته إلى قائمة "موثوق" في إعدادات التطبيق. لتوزيع قائمة الأجهزة الموثوقة على جميع أجهزة الكمبيوتر في مؤسستك، يمكنك تفعيل دمج قوائم الأجهزة الموثوقة في سياسة استخدام إجراء تصدير/استيراد.
- إذا كان Kaspersky Security Center مطبقًا في مؤسستك، يمكنك اكتشاف جميع الأجهزة المتصلة عن بعد وكذلك إنشاء قائمة بالأجهزة الموثوقة في السياسة. ستكون قائمة الأجهزة الموثوقة متوفرة على جميع أجهزة الكمبيوتر المطبق السياسة فيها.

يسمح Kaspersky Endpoint Security بالتحكم في استخدام الأجهزة الموثوقة (الاتصال وقطع الاتصال). ويمكنك تشغيل تسجيل الأحداث في إعدادات الإخطار لمكون التحكم في الجهاز. لدى الأحداث مستوى الخطورة معلوماتي.

إضافة جهاز إلى القائمة الموثوقة من واجهة التطبيق

عندما تتم إضافة جهاز لقائمة الأجهزة الموثوقة، يتم منح حق الوصول للجهاز، بشكل افتراضي، لجميع المستخدمين (مجموعة المستخدمين "الكل").

لإضافة جهاز إلى القائمة الموثوقة من واجهة التطبيق:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.
3. في القسم **إعدادات الوصول**، انقر على الزر **الأجهزة الموثوقة**.
   يفتح هذا قائمة الأجهزة الموثوقة.
4. انقر على **تحديد**.
   يفتح هذا قائمة الأجهزة المتصلة. تعتمد قائمة الأجهزة على القيمة المحددة في القائمة المنسدلة **عرض الأجهزة المتصلة**.
5. في قائمة الأجهزة، حدد الجهاز الذي تريد إضافته إلى القائمة الموثوقة.
6. في الحقل **التعليق**، يمكنك تقديم أي معلومات ذات صلة بالجهاز الموثوق به.
7. حدد المستخدمين أو مجموعة المستخدمين الذين تريد السماح لهم بالوصول إلى الأجهزة الموثوقة.
8. احفظ تغييراتك.

إضافة جهاز إلى القائمة الموثوقة من Kaspersky Security Center

Kaspersky Security Center يستقبل معلومات عن الأجهزة إذا كان Kaspersky Endpoint Security مثبتًا على أجهزة الكمبيوتر وكان التحكم في الجهاز مفعلاً. من غير الممكن إضافة جهاز إلى القائمة الموثوقة ما لم تكن المعلومات عن الجهاز متوفرة في Kaspersky Security Center.

يمكنك إضافة جهاز إلى القائمة الموثوقة وفق البيانات التالية:

- **الأجهزة حسب المُعرِّف**. كل جهاز له معرف فريد (معرف الأجهزة أو HWID). يمكنك عرض المُعرّف في خصائص الجهاز من خلال استخدام أدوات نظام التشغيل. مثال على معرف الجهاز: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. إضافة الأجهزة حسب المُعرِّف عملية ملائمة إذا كنت ترغب في إضافة مجموعة أجهزة محددة.

- **الأجهزة حسب الموديل**. كل جهاز له معرف بائع (VID) ومعرف منتج (PID). يمكنك عرض المُعرّفات في خصائص الجهاز من خلال استخدام أدوات نظام التشغيل. قالب إدخال معرف البائع ومعرف المنتج: `VID_1234&PID_5678`. إضافة أجهزة حسب الموديل طريقة ملائمة إذا كنت تستخدم أجهزة ذات موديل معين في مؤسستك. بهذه الطريقة، يمكنك إضافة جميع الأجهزة من هذا الموديل.

- **الأجهزة حسب قناع المُعرّف**. إذا كنت تستخدم عدة أجهزة ذات معرفات متشابهة، يمكنك إضافة الأجهزة إلى القائمة الموثوقة باستخدام الأقنعة. الحرف `*` يستبدل أي مجموعة من الرموز. لا يدعم برنامج Kaspersky Endpoint Security الحرف `?` عند إدخال قناع. على سبيل المثال: `*WDC_C`.

- **الأجهزة حسب قناع الطراز**. إذا كنت تستخدم عدة أجهزة لها معرفات البائعين ومعرفات المنتجين نفسها (مثل أجهزة من الشركة المصنعة ذاتها)، عندها يمكنك إضافة أجهزة إلى القائمة الموثوقة باستخدام الأقنعة. الحرف `*` يستبدل أي مجموعة من الرموز. لا يدعم برنامج Kaspersky Endpoint Security الحرف `?` عند إدخال قناع. على سبيل المثال، `VID_05AC & PID_ *`.

لإضافة أجهزة إلى قائمة الأجهزة الموثوقة:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.

5. في الجزء الأيسر من النافذة، حدد علامة التبويب **الأجهزة الموثوقة**.

6. حدد خانة الاختيار **دمج القيم عند التوريث** إذا كنت ترغب في إنشاء قائمة موحدة من الأجهزة الموثوقة لجميع أجهزة الكمبيوتر في الشركة.

   سيتم دمج قوائم الأجهزة الموثوقة في السياسات الأصلية والفرعية. سيتم دمج القوائم بشرط أن تكون قيم الدمج مفعلة عند التوريث. الأجهزة الموثوقة من السياسة الأصلية ستصبح معروضة في السياسات الفرعية في عرض القراءة فقط. تغيير الأجهزة الموثوقة أو حذفها من السياسة الرئيسية أمر غير ممكن.

7. انقر فوق زر **إضافة** واختر طريقة لإضافة جهاز إلى القائمة الموثوقة.

8. لتصفية الأجهزة، حدد نوع جهاز من القائمة المنسدلة **نوع الجهاز** (مثل **محركات الأقراص القابلة للإزالة**).

9. في حقل **الاسم / الطراز**، أدخل معرف الجهاز أو (معرف البائع ومعرف المنتج) للموديل أو القناع، حسب طريقة الإضافة المحددة.

   إضافة أجهزة عن طريق أقنعة الطراز (معرف البائع ومعرف المنتج) يجري كما يلي: إذا أدخلت قناع موديل لا يطابق أي موديل، فإن Kaspersky Endpoint Security سيتحقق من إن كان معرف الجهاز (HWID) يطابق القناع. لا يتحقق Kaspersky Endpoint Security إلا من جزء معرف الجهاز الذي يحدد الشركة المصنعة ونوع الجهاز (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`). إذا كان قناع الموديل يطابق هذا الجزء من معرف الجهاز، فإن الأجهزة التي تطابق القناع سوف تضاف إلى قائمة الأجهزة الموثوقة على الكمبيوتر. وفي الوقت نفسه، فإن قائمة الأجهزة في Kaspersky Security Center تبقى خالية عندما تنقر على زر **تحديث**. لعرض قائمة الأجهزة بشكل صحيح، يمكنك إضافة أجهزة عن طريق قناع معرف الجهاز.

10. لتصفية الأجهزة، في حقل **اسم الكمبيوتر** أدخل اسم الكمبيوتر أو قناعًا لاسم الكمبيوتر الذي يتصل الجهاز به.

    الحرف `*` يستبدل أي مجموعة من الرموز. الحرف `؟` يستبدل أي حرف مفرد.

11. انقر فوق الزر **تحديث**.

    تعرض الطاولة قائمة بالأجهزة التي تطابق معايير التصفية المحددة.

12. حدد مربعات الاختيار المجاورة لأسماء الأجهزة التي ترغب في إضافتها إلى قائمة الأجهزة الموثوقة.

13. في حقل **تعليق**، أدخل وصفًا لسبب إضافة الأجهزة إلى القائمة الموثوقة.

14. انقر فوق الزر **Select** على يمين الحقل **السماح للمستخدمين و / أو مجموعات المستخدمين**.

15. حدد مستخدم أو مجموعة في Active Directory وقم بتأكيد اختيارك.
الوصول إلى الأجهزة الموثوقة متاح لمجموعة "الكل" بشكل افتراضي.

16. احفظ تغييراتك.

عندما يكون الجهاز متصلاً، يتحقق Kaspersky Endpoint Security من قائمة الأجهزة الموثوقة لمستخدم معتمد. إذا كان الجهاز موثوقًا، فإن Kaspersky Endpoint Security يسمح بالوصول إلى الجهاز بكل الأذونات حتى إذا تم رفض الوصول إلى نوع الجهاز أو ناقل الاتصال. إذا كان الجهاز غير موثوقٍ وكان الوصول مرفوضًا، يمكنك طلب الوصول إلى الجهاز المُقفل.

تصدير واستيراد قائمة بالأجهزة الموثوقة

لتوزيع قائمة الأجهزة الموثوقة على جميع أجهزة الكمبيوتر في مؤسستك، يمكنك استخدام إجراء تصدير/استيراد.

على سبيل المثال: إذا كنت تحتاج إلى توزيع قائمة بمحركات الأقراص القابلة للإزالة الموثوقة، ستحتاج إلى فعل التالي:

1. توصيل محركات الأقراص القابلة للإزالة بشكل متتالٍ.

2. في إعدادات Kaspersky Endpoint Security، أضف محركات الأقراص القابلة للإزالة إلى القائمة الموثوقة. قم بتكوين أذونات وصول المستخدم، إذا كان ذلك ضروريًا. على سبيل المثال، اسمح للمسؤولين فقط بالوصول إلى محركات الأقراص القابلة للإزالة.

3. قد بتصدير قائمة بالأجهزة الموثوقة في إعدادات Kaspersky Endpoint Security (انظر التعليمات أدناه).

4. قم بتوزيع ملف قائمة الأجهزة الموثوقة إلى أجهزة كمبيوتر أخرى في مؤسستك. مثال: ضع الملف في مجلد مشترك.

5. قد باستيراد قائمة بالأجهزة الموثوقة في إعدادات Kaspersky Endpoint Security على أجهزة الكمبيوتر في المؤسسة (انظر التعليمات أدناه).

لاستيراد قائمة الأجهزة الموثوقة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **إعدادات الوصول**، انقر على الزر **الأجهزة الموثوقة**.
يفتح هذا قائمة الأجهزة الموثوقة.

4. لتصدير قائمة بالأجهزة الموثوقة:

a. حدد الأجهزة الموثوقة التي تريد تصديرها.

b. انقر على **تصدير**.

c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الأجهزة الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير كامل قائمة الأجهزة الموثوقة إلى ملف XML.

5. لاستيراد قائمة بالأجهزة الموثوقة:

a. في القائمة المنسدلة **استيراد**، حدد الإجراء المناسب: **استيراد وإضافة إلى الموجود** أو **استيراد واستبدال الموجود**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الأجهزة الموثوقة منه.

c. افتح الملف.

إذا كان جهاز الكمبيوتر به قائمة أجهزة موثوقة بالفعل، فإن Kaspersky Endpoint Security سوف يطلب منك حذف القائمة الحالية أو إضافة مدخلات جديدة إليها من ملف XML.

6. احفظ تغييراتك.

عندما يكون الجهاز متصلاً، يتحقق Kaspersky Endpoint Security من قائمة الأجهزة الموثوقة لمستخدم معتمد. إذا كان الجهاز موثوقًا، فإن Kaspersky Endpoint Security يسمح بالوصول إلى الجهاز بكل الأذونات حتى إذا تم رفض الوصول إلى نوع الجهاز أو ناقل الاتصال.

الوصول إلى جهاز ممنوع

عند تكوين التحكم في الجهاز، يمكنك عن طريق الخطأ حظر الوصول إلى جهاز ضروري للعمل.

إذا لم يتم نشر Kaspersky Security Center في المؤسسة التي تكون تابع إليها، يمكنك توفير الوصول إلى جهاز في إعدادات برنامج Kaspersky Endpoint Security. على سبيل المثال، يمكنك إضافة الجهاز إلى القائمة الموثوقة أو أن تقوم مؤقتًا بتعطيل التحكم في الجهاز.

إذا تم نشر Kaspersky Security Center في المؤسسة التي تكون تابع إليها وتم تطبيق سياسة على أجهزة الكمبيوتر، يمكنك توفير الوصول إلى جهاز في وحدة تحكم الإدارة.

وضع الاتصال بالإنترنت لمنح صلاحية الوصول

يمكنك منح صلاحية الوصول إلى جهاز محظور بوضع الاتصال بالإنترنت إذا تم نشر Kaspersky Security Center في المؤسسة وتم تطبيق سياسة على الكمبيوتر. يجب أن يكون لدى الكمبيوتر القدرة على تأسيس اتصال مع خادم الإدارة.

منح صلاحية الوصول في وضع الاتصال بالإنترنت يتضمن الخطوات التالية:

1. يرسل المستخدم رسالة إلى المسؤول تحتوي على طلب وصول.

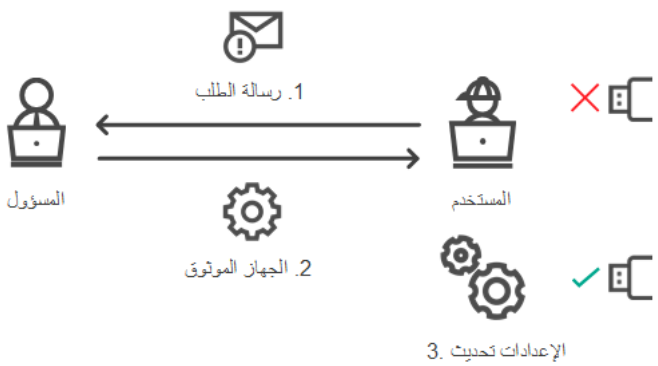
2. يتلقى المسؤول رسالة بالطلب في وحدة تحكم Kaspersky Security Center.

تحتوي وحدة تحكم Kaspersky Security Center على طلبات المستخدم كتحديد لحدث معين مسبقًا لسهولة تتبع الرسائل من المستخدمين.

3. يضف المسؤول الجهاز إلى القائمة الموثوقة.

يمكنك إضافة جهاز موثوق في سياسة ما لمجموعة الإدارة أو في إعدادات التطبيق المحلية لجهاز كمبيوتر فردي.

4. يقوم المسؤول بتحديث إعدادات برنامج Kaspersky Endpoint Security الموجود على جهاز كمبيوتر المستخدم.



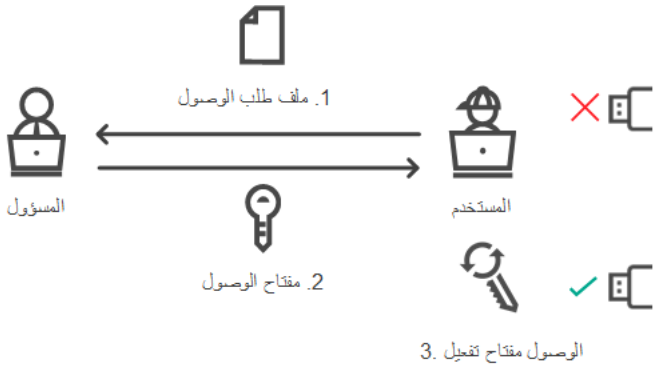
والوضع غير متصل بالإنترنت لمنح صلاحية الوصول

يمكنك منح حق الوصول إلى جهاز محظور عندما يكون بالوضع غير متصل بالإنترنت إذا تم نشر Kaspersky Security Center في المؤسسة وتم تطبيق سياسة على الكمبيوتر. في إعدادات السياسة، في قسم **التحكم في الجهاز**، يجب أن يتم تحديد خانة الاختيار **السماح بطلب للوصول المؤقت**.

إذا كنت تحتاج إلى منح صلاحية وصول مؤقت إلى جهاز محظور ولكن لا يمكنك إضافة الجهاز إلى القائمة الموثوقة، يمكنك منح صلاحية الوصول إلى الجهاز بالوضع غير متصل بالإنترنت. وبهذه الطريقة، يمكنك منح صلاحية الوصول إلى جهاز محظور حتى إذا لم يكن جهاز الكمبيوتر لديه حق الوصول إلى الشبكة أو إذا كان جهاز الكمبيوتر خارج شبكة الشركة.

منح صلاحية الوصول في الوضع غير متصل بالإنترنت يتضمن الخطوات التالية:

1. يقوم المستخدم بإنشاء ملف طلب الوصول ويرسله إلى المسؤول.
2. يقوم المسؤول بإنشاء مفتاح وصول من ملف طلب الوصول ويرسله إلى المستخدم.
3. يقوم المستخدم بتفعيل مفتاح الوصول.



رسم تخطيطي لمنح صلاحية وصول إلى جهاز بالوضع غير متصل بالإنترنت

وضع الاتصال بالإنترنت لمنح صلاحية الوصول

يمكنك منح صلاحية الوصول إلى جهاز محظور بوضع الاتصال بالإنترنت إذا تم نشر Kaspersky Security Center في المؤسسة وتم تطبيق سياسة على الكمبيوتر. يجب أن يكون لدى الكمبيوتر القدرة على تأسيس اتصال مع خادم الإدارة.

يطلب المستخدم الوصول إلى جهاز محظور على النحو التالي:

1. توصيل الجهاز بجهاز الكمبيوتر.

   سيعرض برنامج Kaspersky Endpoint Security إخطارًا ليشير أن الوصول إلى الجهاز محظور (انظر الشكل أدناه).

2. انقر على رابط **طلب الوصول**.

   يفتح هذا نافذة تحتوي على رسالة للمسؤول. تحتوي هذه الرسالة على معلومات حول الجهاز المحظور.

3. انقر على **إرسال**.

إخطار التحكم في الجهاز

بعد ذلك، سيتلقى المسؤول حدث رسالة منع الوصول للجهاز إلى المسؤول في وحدة تحكم Kaspersky Security Center. ويحتوي الحدث على اسم المستخدم واسم الكمبيوتر ومعلومات عن الجهاز الذي يحاول المستخدم الوصول إليه وبيانات أخرى. ويمكنك تكوين طريقة إخطار المسؤول بمثل هذه الأحداث، وعلى سبيل المثال، اختيار إخطار البريد الإلكتروني. تحتوي وحدة تحكم Kaspersky Security Center على طلبات المستخدم كتحديد لحدث معين مسبقًا لسهولة تتبع الرسائل من المستخدمين.

لمنح حق الوصول تحتاج إلى إضافة جهاز إلى القائمة الموثوقة. بعد تحديث إعدادات Kaspersky Endpoint Security على الكمبيوتر، سيحصل المستخدم على حق الوصول إلى الجهاز.

والوضع غير متصل بالإنترنت لمنح صلاحية الوصول

يمكنك منح حق الوصول إلى جهاز محظور عندما يكون بالوضع غير متصل بالإنترنت إذا تم نشر Kaspersky Security Center في المؤسسة وتم تطبيق سياسة على الكمبيوتر. في إعدادات السياسة، في قسم **التحكم في الجهاز**، يجب أن يتم تحديد خانة الاختيار **السماح بطلب للوصول المؤقت**.

يطلب المستخدم الوصول إلى جهاز محظور على النحو التالي:

1. توصيل الجهاز بجهاز الكمبيوتر.
سيعرض برنامج Kaspersky Endpoint Security إخطارًا ليشير أن الوصول إلى الجهاز محظور (انظر الشكل أدناه).

2. انقر على رابط **طلب وصول مؤقت**.
يفتح هذا نافذة تحتوي على قائمة بالأجهزة المتصلة.

3. في قائمة الأجهزة المتصلة، حدد الجهاز الذي تود الحصول على صلاحية الوصول إليه.

4. انقر على **إنشاء ملف طلب الوصول**.

5. في الحقل **مدة صلاحية الوصول**، حدد الفترة الزمنية التي ترغب خلالها في الوصول إلى الجهاز.

6. احفظ الملف في ذاكرة جهاز الكمبيوتر.

كنتيجة لذلك، سيتم تنزيل ملف طلب الوصول مع ملحق *.akey في ذاكرة جهاز الكمبيوتر. استخدم أي طريقة متاحة لإرسال ملف طلب الوصول إلى الجهاز إلى مسؤول الشبكة المحلية الخاصة بالشركة.

إخطار التحكم في الجهاز

كيف يستطيع المسؤول إنشاء مفتاح وصول للجهاز الممنوع في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في المجلد **الأجهزة المدارة** الخاص بشجرة وحدة تحكم الإدارة، افتح المجلد الذي يحمل اسم مجموعة الإدارة التي ينتمي إليها جهاز الكمبيوتر العميل المناسب.
3. في مساحة العمل، حدد علامة تبويب **الأجهزة**.
4. في قائمة أجهزة الكمبيوتر العميلة، حدد جهاز الكمبيوتر الذي يجب أن يحصل على حق وصول مؤقت إلى جهاز ممنوع.
5. في قائمة السياق الخاصة بالكمبيوتر، حدد العنصر **منح إمكانية الوصول في وضع عدم الاتصال**.
6. في النافذة التي تفتح، حدد القسم **التحكم في الجهاز**.
7. انقر فوق الزر **استعراض** وقم بتنزيل ملف طلب الوصول الذي تم استلامه من المستخدم.
   سترى معلومات حول الجهاز المحظور الذي طلب المستخدم الوصول إليه.
8. إذا لزم الأمر، قم بتغيير قيمة الإعداد **مدة صلاحية الوصول**.
   في الوضع الافتراضي، يأخذ إعداد **مدة صلاحية الوصول** القيمة التي أشار إليها المستخدم عند إنشاء ملف طلب الوصول.
9. حدد قيمة إعداد **تفعيل بحلول**.
   يحدد هذا الإعداد الفترة الزمنية التي يمكن للمستخدم أن يقوم خلالها بتفعيل الوصول إلى الجهاز المحظور باستخدام مفتاح الوصول الذي تم توفيره.
10. احفظ ملف مفتاح الوصول في ذاكرة جهاز الكمبيوتر.

كيف يستطيع المسؤول إنشاء مفتاح وصول للجهاز الممنوع في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Managed devices**.

2. في قائمة أجهزة الكمبيوتر العميلة، حدد جهاز الكمبيوتر الذي يجب أن يحصل على حق وصول مؤقت إلى جهاز ممنوع.

3. انقر فوق زر علامة الحذف () أعلى قائمة أجهزة الكمبيوتر، ثم انقر فوق الزر **Grant access to the device in offline mode**.

4. في النافذة التي تفتح، حدد القسم **Device Control**.

5. انقر فوق الزر **Browse** وقم بتنزيل ملف طلب الوصول الذي تم استلامه من المستخدم.
سترى معلومات حول الجهاز المحظور الذي طلب المستخدم الوصول إليه.

6. إذا لزم الأمر، قم بتغيير قيمة الإعداد **Access duration (hours)**.
في الوضع الافتراضي، يأخذ إعداد **Access duration (hours)** القيمة التي أشار إليها المستخدم عند إنشاء ملف طلب الوصول.

7. حدد الفترة الزمنية التي يمكن خلالها تفعيل مفتاح الوصول على الجهاز.
يحدد هذا الإعداد الفترة الزمنية التي يمكن للمستخدم أن يقوم خلالها بتفعيل الوصول إلى الجهاز المحظور باستخدام مفتاح الوصول الذي تم توفيره.

8. احفظ ملف مفتاح الوصول في ذاكرة جهاز الكمبيوتر.

كنتيجة لذلك، سيتم تنزيل مفتاح الوصول الخاص بالجهاز المحظور في ذاكرة جهاز الكمبيوتر. يحتوي ملف مفتاح الوصول على ملحق *.acode. استخدم أي طريقة متاحة لإرسال مفتاح الوصول الخاص بالجهاز المحظور إلى المستخدم.

يقوم المستخدم بتفعيل مفتاح الوصول على النحو التالي:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان ← التحكم في الجهاز**.

3. في القسم **طلب الوصول**، انقر على الزر **طلب الوصول إلى الجهاز**.

4. في النافذة التي تفتح، انقر فوق الزر **تفعيل مفتاح الوصول**.

5. في النافذة التي تفتح، حدد الملف باستخدام مفتاح الوصول الخاص بالجهاز الذي تم استلامه من مسؤول الشبكة المحلية الخاصة بالشركة.
يؤدي ذلك إلى فتح نافذة تحتوي على معلومات حول إتاحة الوصول.

6. انقر على **موافق**.

كنتيجة لذلك، يقوم المستخدم باستلام حق الوصول إلى الجهاز للفترة الزمنية التي يحددها المسؤول. يقوم المستخدم باستلام مجموعة كاملة من حقوق الوصول إلى الجهاز (للقراءة والكتابة). عندما تنتهي صلاحية المفتاح، سيكون الوصول إلى الجهاز محظورًا. إذا كان المستخدم يطلب مفتاح دائم للوصول إلى الجهاز، قم بإضافة الجهاز إلى القائمة الموثوقة.

تحرير قوالب رسائل التحكم في الجهاز

بمجرد محاولة المستخدم الوصول إلى أحد الأجهزة المحظورة، يعرض برنامج Kaspersky Endpoint Security رسالة تفيد بأنه يُحظر الوصول إلى الجهاز أو يُحظر التشغيل باستخدام محتويات الجهاز. إذا كان المستخدم يعتقد أن الجهاز تم منعه عن طريق الخطأ، أو أنه تم منع عملية باستخدام محتويات الجهاز عن طريق الخطأ، فبإمكان المستخدم إرسال رسالة إلى مسؤول شبكة الشركة المحلية عن طريق النقر فوق الرابط الموجود في الرسالة التي تم عرضها حول الإجراء الممنوع.

تتوفر قوالب للرسائل التي تدور حول الوصول المحظور للأجهزة أو عمليات التشغيل المحظورة باستخدام محتويات الجهاز، وكذلك للرسائل التي يتم إرسالها إلى المسؤول. ويمكنك تعديل قوالب الرسالة.

لتحرير القوالب لرسائل التحكم في الجهاز:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **قوالب الرسائل**، كوّن القوالب لرسائل التحكم في الجهاز:

- **رسالة حول المنع**. قالب الرسالة الذي يظهر عندما يحاول المستخدم الوصول إلى جهاز محظور. تظهر هذه الرسالة أيضًا عندما يحاول المستخدم تنفيذ عملية على محتويات الجهاز الذي تم حظره لهذا المستخدم.

- **رسالة إلى المسؤول**. قالب الرسالة الذي يتم إرساله إلى مسؤول الشبكة المحلية (LAN) عندما يعتقد المستخدم أنه قد تم حظر وصوله إلى الجهاز أو منعه من إجراء عملية باستخدام محتوى الجهاز عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع الوصول للجهاز إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.

4. احفظ تغييراتك.

منع تعدد الاتصال

تمنع مكافحة اتصالات الجسر إنشاء جسور شبكة عن طريق منع التأسيس المتزامن لاتصالات الشبكة المتعددة لجهاز الكمبيوتر. يتيح لك ذلك حماية شبكة الشركة من الهجمات عبر شبكات غير محمية وغير مُصرح بها.

تنظم مكافحة اتصالات الجسر إنشاء اتصالات الشبكة عن طريق استخدام قواعد الاتصال.

يتم إنشاء قواعد الاتصال للأنواع التالية سابقة التحديد من الأجهزة:

- محوّلات الشبكة؛
- محولات Wi-Fi؛
- أجهزة المودم.

في حالة تمكين قاعدة اتصال، ينفذ Kaspersky Endpoint Security التالي:

- يمنع الاتصال النشط عند إنشاء اتصال جديد، في حالة تحديد نوع الجهاز في القاعدة المستخدمة لكلا الاتصالين؛
- يمنع الاتصالات التي يتم إنشاؤها باستخدام أنواع الأجهزة التي يتم استخدام قواعد منخفضة الأولوية لها.

تمكين منع تعدد الاتصال

يتم تعطيل مكافحة اتصالات الجسر بشكل افتراضي.

تمكين منع تعدد الاتصال:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **إعدادات الوصول**، انقر على الزر **منع تعدد الاتصال**.

4. استخدم مفتاح التبديل **تمكين منع تعدد الاتصال** لتمكين هذه الميزة أو تعطيلها.

5. احفظ تغييراتك.

بعد تمكين مكافحة اتصالات الجسر، يمنع Kaspersky Endpoint Security بالفعل الاتصالات التي تم إنشاؤها وفقًا لقواعد الاتصال.

تغيير حالة قاعدة اتصال

لتغيير حالة قاعدة اتصال:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **إعدادات الوصول**، انقر على الزر **منع تعدد الاتصال**.

4. في القسم **قواعد الأجهزة**، حدد القاعدة التي تريد تغيير حالتها.

5. استخدم مفاتيح التبديل في العمود **التحكم** لتمكين القاعدة أو تعطيلها.

6. احفظ تغييراتك.

تغيير أولوية قاعدة اتصال

لتغيير أولوية قاعدة اتصال:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الجهاز**.

3. في القسم **إعدادات الوصول**، انقر على الزر **منع تعدد الاتصال**.

4. في المجموعة **قواعد الأجهزة**، حدد القاعدة التي تريد تغيير أولويتها.

5. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الاتصال.

كلما كانت القاعدة تحتل رتبة أعلى في جدول القواعد، أصبحت تتمتع بدرجة أعلى من الأولوية. تمنع مكافحة اتصالات الجسر كل الاتصالات باستثناء اتصال واحد يتم إنشاؤه باستخدام نوع الجهاز الذي يتم استخدام قاعدة الأولوية العليا له.

6. احفظ تغييراتك.

مراقبة عيوب التكيف

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل. لا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم.

يراقب مكون مراقبة عيوب التكيف ويمنع الإجراءات التي لا تعتبر معتادة لأجهزة الكمبيوتر الموجودة في شبكة الشركة. يستخدم نظام مراقبة عيوب التكيف مجموعة من القواعد لتتبع السلوك غير النموذجي (على سبيل المثال، قاعدة بدء تشغيل Windows PowerShell من خلال تطبيق Office). تم إنشاء القواعد من قِبل متخصصي Kaspersky استنادًا إلى سيناريوهات نموذجية للنشاط الضار. تستطيع تكوين كيفية قيام نظام مراقبة عيوب التكيف بمعالجة كل قاعدة، وعلى سبيل المثال، يسمح بتنفيذ نصوص PowerShell التي تقوم بالتشغيل التلقائي لبعض مهام سير العمل. يقوم Kaspersky Endpoint Security بتحديث مجموعة القواعد إلى جانب قواعد بيانات التطبيق. يجب تأكيد إجراء تحديثات لمجموعات القواعد يدويًا.

إعدادات مراقبة عيوب التكيف

يتضمن تكوين نظام مراقبة عيوب التكيف الخطوات التالية:

1. تدريب نظام مراقبة عيوب التكيف.

بعد تمكين نظام مراقبة عيوب التكيف، تعمل قواعده في وضع التدريب. خلال التدريب، يقوم نظام مراقبة عيوب التكيف بمراقبة تشغيل القاعدة وإرسال أحداث التشغيل إلى Kaspersky Security Center. لكل قاعدة المدة الزمنية الخاصة بها لوضع التدريب. يتم تعيين المدة الزمنية لوضع التدريب من جانب خبراء Kaspersky. عادةً، يكون وضع التدريب نشط لمدة أسبوعين.

في حال عدم تشغيل قاعدة ما أبدًا خلال التدريب، سيعتبر نظام مراقبة عيوب التكيف الإجراءات المرتبطة بهذه القاعدة غير نموذجية. سيقوم Kaspersky Endpoint Security بحظر جميع الإجراءات المرتبطة بهذه القاعدة.

في حالة تشغيل قاعدة ما خلال التدريب، سيسجل Kaspersky Endpoint Security أحداث في تقرير تشغيل القاعدة ومستودع **تشغيل القواعد في حالة التدريب الذكي**.

2. تحليل تقرير تشغيل القاعدة.

يحلل المسؤول تقرير تشغيل القاعدة أو محتويات مستودع **تشغيل القواعد في حالة التدريب الذكي**. يمكن أن يحدد المسؤول سلوك مراقبة عيوب التكيف عند تشغيل القاعدة: إما الحظر أو السماح. يمكن أن يستمر المسؤول أيضًا في مراقبة كيفية عمل القاعدة وتمديد المدة الزمنية لوضع التدريب. إذا لم يتخذ المسؤول أي إجراء، سيستمر التطبيق أيضًا في العمل بوضع التدريب. تم إعادة تشغيل فترة وضع التدريب.

يتم تكوين مراقبة عيوب التكيف في الوقت الحقيقي. يتم تكوين مراقبة عيوب التكيف عبر القنوات التالية:

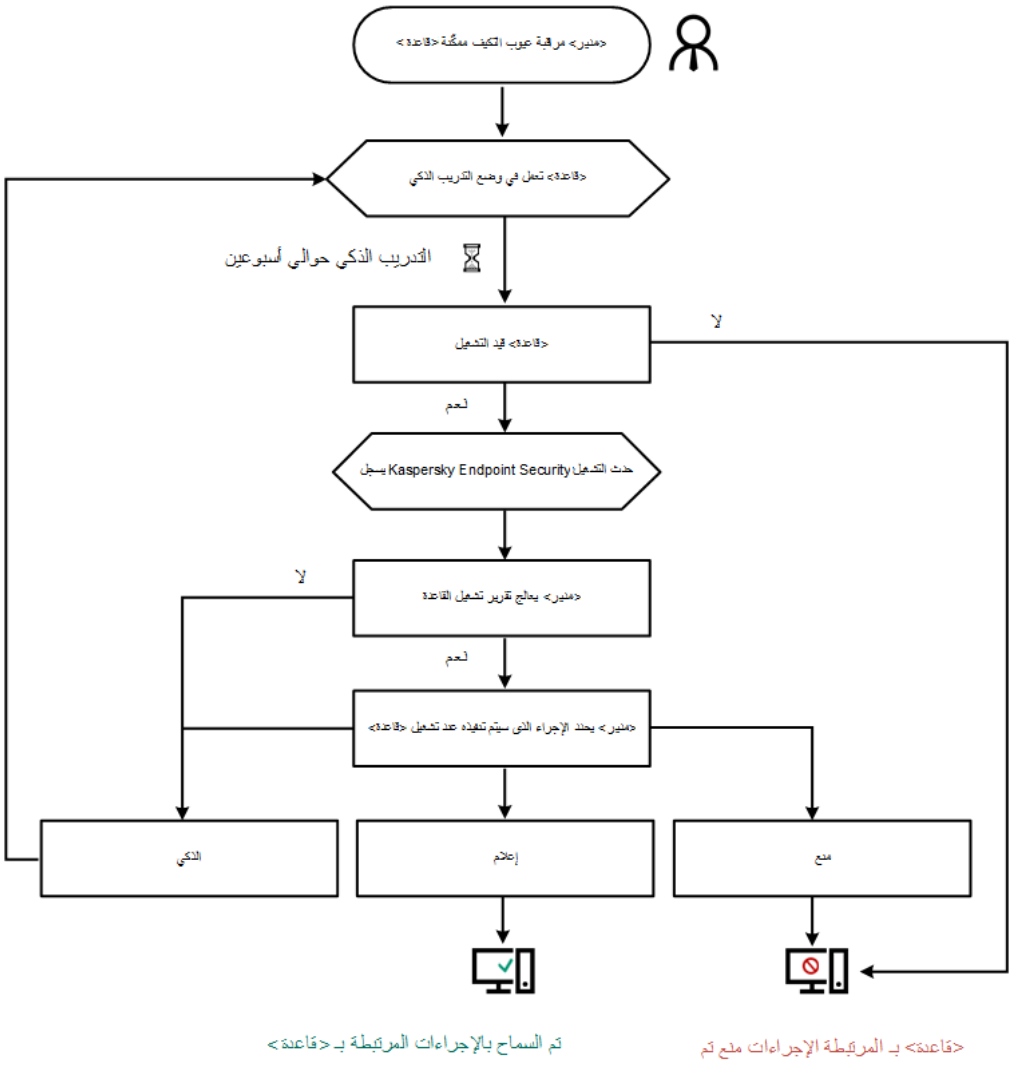
- يتم بدء تشغيل مراقبة عيوب التكيف تلقائيًا لحظر الإجراءات المرتبطة بالقواعد التي لم يتم تشغيلها أبدًا في وضع التدريب.
- يضيف Kaspersky Endpoint Security قواعد جديدة أو يحذف قواعد قديمة.
- يكون المسؤول عملية مراقبة عيوب التكيف بعد مراجعة تقرير تشغيل القاعدة ومحتويات مستودع **تشغيل القواعد في حالة التدريب الذكي**. ويُوصى بالتحقق من تقرير تشغيل القاعدة ومحتويات مستودع **تشغيل القواعد في حالة التدريب الذكي**.

عندما يحاول تطبيق ضار تنفيذ إجراء ما، سيحظر Kaspersky Endpoint Security الإجراء ويعرض إخطارًا (انظر الشكل أدناه).

إخطار مراقبة عيوب التكيف

خوارزمية تشغيل مراقبة عيوب التكيف

يقرر Kaspersky Endpoint Security ما إذا كان يجب السماح بإجراء مرتبط بقاعدة أو حظره استنادًا على الخوارزمية التالية (انظر الشكل أدناه).



خوارزمية تشغيل مراقبة عيوب التكيف

تمكين وتعطيل مراقبة عيوب التكيف

يتم تمكين مراقبة عيوب التكيف بصورة افتراضية.

لتمكين أو تعطيل مراقبة عيوب التكيف:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة عيوب التكيف**.
3. استخدم مفتاح تبديل **مراقبة عيوب التكيف** لتمكين المكون أو تعطيله.
4. احفظ تغييراتك.

نتيجة لذلك، ستتحول مراقبة عيوب التكيف إلى وضع التدريب. وأثناء التدريب، تراقب مراقبة عيوب التكيف بدء تشغيل القاعدة. وعند اكتمال التدريب، تبدأ مراقبة عيوب التكيف في حظر الإجراءات غير المعتادة لأجهزة الكمبيوتر في شبكة الشركة.

إذا بدأت مؤسستك في استخدام بعض الأدوات الجديدة، وحظرت مراقبة عيوب التكيف إجراءات تلك الأدوات، يمكنك إعادة تعيين نتائج وضع التدريب وتكرار التدريب. ولفعل ذلك، تحتاج إلى تغيير الإجراء الذي يتم تنفيذه عند تشغيل القاعدة (على سبيل المثال، ضبطه على **إخطار**). وبعد ذلك تحتاج إلى إعادة تمكين وضع التدريب (ضبط قيمة **الذكي**).

تمكين وتعطيل قاعدة مراقبة عيوب التكيف

لتمكين أو تعطيل قاعدة مراقبة عيوب التكيف:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة عيوب التكيف**.
3. في القسم **القواعد**، انقر على الزر **تحرير القواعد**.
   تفتح قائمة قاعدة مراقبة عيوب التكيف.
4. في الجدول، حدد مجموعة قواعد (على سبيل المثال، نشاط تطبيقات Office) وقم بتوسيع المجموعة.
5. حدد القاعدة (على سبيل المثال، بدء تشغيل Windows PowerShell من خلال تطبيق Office).
6. استخدم مفتاح التبديل في العمود **الحالة** لتمكين أو تعطيل قاعدة مراقبة عيوب التكيف.
7. احفظ تغييراتك.

تعديل الإجراء المتخذ عند إطلاق قاعدة مراقبة عيوب التكيف

لتعديل الإجراء المتخذ عند بدء تنفيذ قاعدة مراقبة عيوب التكيف:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة عيوب التكيف**.
3. في القسم **القواعد**، انقر على الزر **تحرير القواعد**.
   تفتح قائمة قاعدة مراقبة عيوب التكيف.
4. حدد قاعدة في الجدول.
5. انقر على **تحرير**.
   تفتح نافذة خصائص قاعدة التحكم غير الطبيعي التكيفي.
6. في القسم **الإجراء**، حدد أحد الخيارات التالية:

- **الذكي**. في حالة تحديد هذا الخيار، فإن قاعدة مراقبة عيوب التكيف تعمل في حالة التدريب الذكي لفترة زمنية يحددها خبراء Kaspersky. وفي هذا الوضع، عند تشغيل قاعدة مراقبة عيوب التكيف، يسمح Kaspersky Endpoint Security بإجراء النشاط الذي تشمله القاعدة ويسجل حالة إدخال في المخزن **تشغيل القواعد في حالة التدريب الذكي** الخاص بخادم إدارة Kaspersky Security Center. عندما تنتهي الفترة الزمنية المحددة للعمل في حالة التدريب الذكي، يمنع Kaspersky Endpoint Security النشاط الذي تشمله قاعدة مراقبة عيوب التكيف ويسجل إدخالاً يتضمن معلومات عن النشاط.

- **منع**. إذا تم تحديد هذا الإجراء، وعندما يتم تشغيل قاعدة مراقبة عيوب التكيف، يمنع Kaspersky Endpoint Security النشاط الذي تشمله القاعدة ويقوم بتسجيل إدخال يحتوي على معلومات بشأن النشاط.
- **إخطار**. إذا تم تحديد هذا الإجراء، وعندما يتم تشغيل قاعدة مراقبة عيوب التكيف، يسمح Kaspersky Endpoint Security بالنشاط الذي تشمله القاعدة ويقوم بتسجيل إدخال يحتوي على معلومات بشأن النشاط.

7. احفظ تغييراتك.

إنشاء استثناء لقاعدة التحكم غير الطبيعي التكيفي

لا يمكنك إنشاء أكثر من 1.000 استثناء لقواعد مراقبة عيوب التكيف. من غير المستحسن إنشاء ما يزيد عن 200 استثناء. لتقليل عدد الاستثناءات المستخدمة، يُوصى باستخدام الأقنعة في إعدادات الاستثناءات.

تتضمن استثناءات قاعدة مراقبة عيوب التكيف وصف لكائنات المصدر والهدف. الكائن المصدر هو الكائن الذي يقوم بإجراء الإجراءات. الكائن الهدف هو الكائن الذي يتم إجراء الإجراءات عليه. على سبيل المثال، لقد قمت بفتح ملف يسمى `file.xlsx`. ونتيجة لهذا، يتم تحميل ملف مكتبة له امتداد DLL في ذاكرة جهاز الكمبيوتر. يتم استخدام هذه المكتبة بواسطة المستعرض (الملف التنفيذي المسمى `browser.exe`). في هذا المثال، يعتبر `file.xlsx` هو الملف المصدر، و Excel هو العملية المصدر و `browser.exe` هو الكائن الهدف وBrowser هو العملية الهدف.

لإنشاء استثناء لقاعدة التحكم غير الطبيعي التكيفي:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة عيوب التكيف**.
3. في القسم **القواعد**، انقر على الزر **تحرير القواعد**.
   تفتح قائمة قاعدة مراقبة عيوب التكيف.
4. حدد قاعدة في الجدول.
5. انقر على **تحرير**.
   تفتح نافذة خصائص قاعدة التحكم غير الطبيعي التكيفي.
6. في القسم **الاستثناءات**، انقر على الزر **إضافة**.
   تفتح نافذة خصائص الاستثناء.
7. حدد المستخدم الذي تريد تكوين استثناء له.

لا تدعم مراقبة عيوب التكيف الاستثناءات لمجموعات المستخدمين. وإذا حددت مجموعة مستخدمين، فلن يطبق Kaspersky Endpoint Security الاستثناء.

8. في الحقل **الوصف** أدخل وصفًا للاستثناء.
9. حدد إعدادات الكائن المصدر أو العملية المصدر التي تم بدؤها بواسطة الكائن:
   - **العملية المصدر**. مسار أو قناع المسار إلى الملف أو المجلد الذي يحتوي على الملفات (على سبيل المثال، `C:\Dir\File.exe` أو `Dir\*.exe`).
   - **تجزئة العملية المصدر**. رمز تجزئة الملف.

- **الكائن المصدر**. مسار أو قناع المسار إلى الملف أو المجلد الذي يحتوي على الملفات (على سبيل المثال، `C:\Dir\File.exe` أو `Dir\*.exe`). على سبيل المثال، مسار الملف `document.docm` الذي يستخدم نص أو ماكرو لبدء العمليات الهدف.

  وكذلك يمكنك القيام بتحديد كائنات أخرى لاستبعادها، مثل عنوان الويب أو ماكرو أو أحد الأوامر في سطر الأوامر أو مسار التسجيل أو غيرها. حدد الكائن وفقًا للقالب التالي: `object://<object>`، حيث يشير `<object>` إلى اسم الكائن، على سبيل المثال، `object://web.site.example.com` أو `object://VBA, object://ipconfig` أو `object://HKEY_USERS`. يمكنك أيضًا استخدام الأقنعة، على سبيل المثال، `object://*C:\Windows\temp\*`.

- **تجزئة الكائن المصدر**. رمز تجزئة الملف.

لا يتم تطبيق قاعدة مراقبة عيوب التكيف على الإجراءات التي يتم إجراؤها بواسطة الكائن أو على العمليات التي يتم بدؤها من قبل الكائن.

10. حدد الإعدادات الخاصة بالكائن الهدف أو العمليات الهدف التي تم بدؤها على الكائن.

- **العملية الهدف**. مسار أو قناع المسار إلى الملف أو المجلد الذي يحتوي على الملفات (على سبيل المثال، `C:\Dir\File.exe` أو `Dir\*.exe`).

- **تجزئة العملية الهدف**. رمز تجزئة الملف.

- **الكائن الهدف**. الأمر لبدء العملية الهدف. حدد الأمر باستخدام النمط التالي `object://<command>`، على سبيل المثال، `object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage txt'"`. يمكنك أيضًا استخدام الأقنعة، على سبيل المثال، `object://*C:\Windows\temp\*`.

- **تجزئة الكائن الهدف**. رمز تجزئة الملف.

لا يتم تطبيق قاعدة مراقبة عيوب التكيف على الإجراءات التي يتم إجراؤها على الكائن أو على العمليات التي يتم بدؤها على الكائن.

11. احفظ تغييراتك.

تصدير واستيراد الاستثناءات لقواعد التحكم غير الطبيعي التكيفي

لتصدير أو استيراد قائمة الاستثناءات للقواعد المحددة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة عيوب التكيف**.

3. في القسم **القواعد**، انقر على الزر **تحرير القواعد**.
   تفتح قائمة قاعدة مراقبة عيوب التكيف.

4. لتصدير قائمة القواعد:

   a. حدد القواعد التي تريد تصدير استثناءاتها.

   b. انقر على **تصدير**.

   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   d. أكد أنك تريد تصدير الاستثناءات المحددة فقط، أو تصدير قائمة الاستثناءات بأكملها.

   e. احفظ الملف.

5. لاستيراد قائمة القواعد:

a. انقر على **استيراد**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

c. افتح الملف.

إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

6. احفظ تغييراتك.

تطبيق التحديثات لقواعد مراقبة عيوب التكيف

قد تتم إضافة قواعد مراقبة عيوب التكيف الجديدة إلى جدول القواعد وقد يتم حذف قواعد مراقبة عيوب التكيف الموجودة بالفعل من جدول القواعد عند تحديث قواعد بيانات مكافحة الفيروسات. يقوم Kaspersky Endpoint Security بالتمييز بين قواعد مراقبة عيوب التكيف المراد حذفها أو إضافتها في حال لم يتم تطبيق تحديث لهذه القواعد.

إلى حين تطبيق التحديث، يعرضKaspersky Endpoint Security مجموعة قواعد مراقبة عيوب التكيف المراد حذفها من خلال التحديث في جدول القواعد ويقوم بتعيين الحالة تم التعطيل لها. من غير الممكن تغيير إعدادات هذه القواعد.

لتطبيق التحديثات لقواعد مراقبة عيوب التكيف:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة عيوب التكيف**.

3. في القسم **القواعد**، انقر على الزر **تحرير القواعد**.

تفتح قائمة قاعدة مراقبة عيوب التكيف.

4. في النافذة التي تفتح، انقر فوق الزر **الموافقة على التحديثات**.

يتوفر الزر **الموافقة على التحديثات** إذا توفر تحديث لقواعد مراقبة عيوب التكيف.

5. احفظ تغييراتك.

تحرير قالب رسالة مراقبة عيوب التكيف

عندما يحاول المستخدم القيام بإجراء ما، ممنوع من جانب قواعد مراقبة عيوب التكيف، يعرض Kaspersky Endpoint Security رسالة تفيد بمنع إجراءات يُحتمل أن تكون ضارة. إذا كان المستخدم يظن بأن الإجراء قد تم منعه عن طريق الخطأ، فيمكن للمستخدم استخدام الرابط الموجود في نص الرسالة لإرسال رسالة إلى مسؤول شبكة الشركة المحلية.

تتوفر قوالب خاصة للرسالة المتعلقة بمنع إجراءات يُحتمل أن تكون ضارة وللرسالة المراد إرسالها إلى المسؤول. ويمكنك تعديل قوالب الرسالة.

لتحرير قالب رسالة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة عيوب التكيف**.

3. في القسم **القوالب**، كوّن القوالب لرسائل التحكم غير الطبيعي التكيفي:

- **رسالة حول المنع**. قالب الرسالة المعروض لمستخدم عند تشغيل قاعدة مراقبة عيوب التكيف والتي تمنع وجود الإجراء غير النموذجي.

- **رسالة إلى المسؤول**. قالب الرسالة التي يمكن أن يرسلها مستخدم إلى المسؤول عن شبكة المؤسسة المحلية إذا كان المستخدم يعتبر عملية المنع حدثت عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع نشاط التطبيق إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.

4. احفظ تغييراتك.

عرض تقارير مراقبة عيوب التكيف

لعرض تقارير مراقبة عيوب التكيف:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **مراقبة عيوب التكيف**.
يتم عرض إعدادات مكون مراقبة عيوب التكيف في الجزء الأيمن من النافذة.

5. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في عرض تقرير حول إعدادات قواعد مراقبة عيوب التكيف، انقر فوق الزر **تقرير عن حالة قواعد مراقبة عيوب التكيف**.

- إذا كنت ترغب في عرض تقرير حول قواعد مراقبة عيوب التكيف التي تم تشغيلها، انقر فوق الزر **تقرير حول قواعد مراقبة عيوب التكيف التي تم تشغيلها**.

6. تبدأ عملية إنشاء التقرير.

يتم عرض التقرير في نافذة جديدة.

التحكم في التطبيقات

يدير التحكم في التطبيقات بدء تشغيل التطبيقات على أجهزة كمبيوتر المستخدمين. يتيح لك هذا تنفيذ سياسة أمان الشركة عند استخدام التطبيقات. التحكم في التطبيقات يقلل أيضًا من خطر إصابة الكمبيوتر بتقييد الوصول إلى التطبيقات.

يتضمن تكوين نظام مراقبة عيوب التكيف الخطوات التالية:

1. إنشاء فئات التطبيقات.
يقوم المسؤول بإنشاء فئات التطبيقات التي يريد المسؤول إدارتها. فئات التطبيقات مخصصة لجميع أجهزة الكمبيوتر في شبكة الشركة، بغض النظر عن مجموعات الإدارة. لإنشاء فئة، يمكنك استخدام المعايير التالية: فئة KL (على سبيل المثال المستعرضات) وتجزئة الملف وبائع التطبيق ومعايير أخرى.

2. إنشاء قواعد التحكم في التطبيق.
يقوم المسؤول بإنشاء قواعد التحكم في التطبيقات في السياسة لمجموعة الإدارة. تتضمن القاعدة فئات التطبيقات وحالة بدء تشغيل التطبيقات من هذه الفئات: محظورة أو مسموح بها.

3. تحديد وضع التحكم في التطبيق.

يختار المسؤول وضع العمل مع التطبيقات غير المدرجة في أي من القواعد (قائمة السماح وقائمة الرفض الخاصة بالتطبيق).

عندما يحاول مستخدم بدء تشغيل تطبيق محظور ، سيحظر Kaspersky Endpoint Security التطبيق من بدء التشغيل وسيعرض إشعارًا (انظر الشكل أدناه).

يتم توفير وضع اختبار للتحقق من تكوين التحكم في التطبيقات. في هذا الوضع، يقوم Kaspersky Endpoint Security بما يلي:

- يسمح ببدء تشغيل التطبيقات، بما في ذلك التطبيقات المحظورة.
- يعرض إشعارًا حول بدء تشغيل تطبيق محظور ويضيف معلومات إلى التقرير على جهاز الكمبيوتر الخاص بالمستخدم.
- يرسل بيانات حول بدء تشغيل التطبيقات المحظورة إلى Kaspersky Security Center.

إشعار التحكم في التطبيقات

أوضاع تشغيل التحكم في التطبيقات

يعمل مكون التحكم في التطبيقات في وضعين:

- **قائمة الرفض**. في هذا الوضع، يتيح التحكم في التطبيقات للمستخدمين بدء تشغيل جميع التطبيقات باستثناء التطبيقات المحظورة في قواعد التحكم في التطبيقات.

  يتم تمكين وضع المنع لإجراءات التحكم في التطبيقات بشكلٍ افتراضي.

- **قائمة السماح**. في هذا الوضع، يمنع التحكم في التطبيقات المستخدمين من بدء أي تطبيقات باستثناء التطبيقات المسموح بها وغير المحظورة في قواعد التحكم في التطبيقات.

  إذا تم تكوين قواعد السماح للتحكم في التطبيقات بالكامل، فسيحظر المكون بدء تشغيل جميع التطبيقات الجديدة التي لم يتم التحقق منها بواسطة مسؤول الشبكة المحلية، وذلك مع السماح بتشغيل نظام التشغيل والتطبيقات الموثوقة التي يعتمد عليها المستخدمون في عملهم.

  يمكنك قراءة التوصيات الخاصة بتكوين قواعد التحكم في التطبيقات في وضع قائمة السماح.

يمكن تكوين التحكم في التطبيقات للعمل في هذه الأوضاع باستخدام واجهة Kaspersky Endpoint Security المحلية واستخدام Kaspersky Security Center.

ومع ذلك، يقدم Kaspersky Security Center أدوات غير متوفرة في واجهة Kaspersky Endpoint Security المحلية، مثل الأدوات اللازمة للمهام التالية:

- إنشاء فئات التطبيقات.

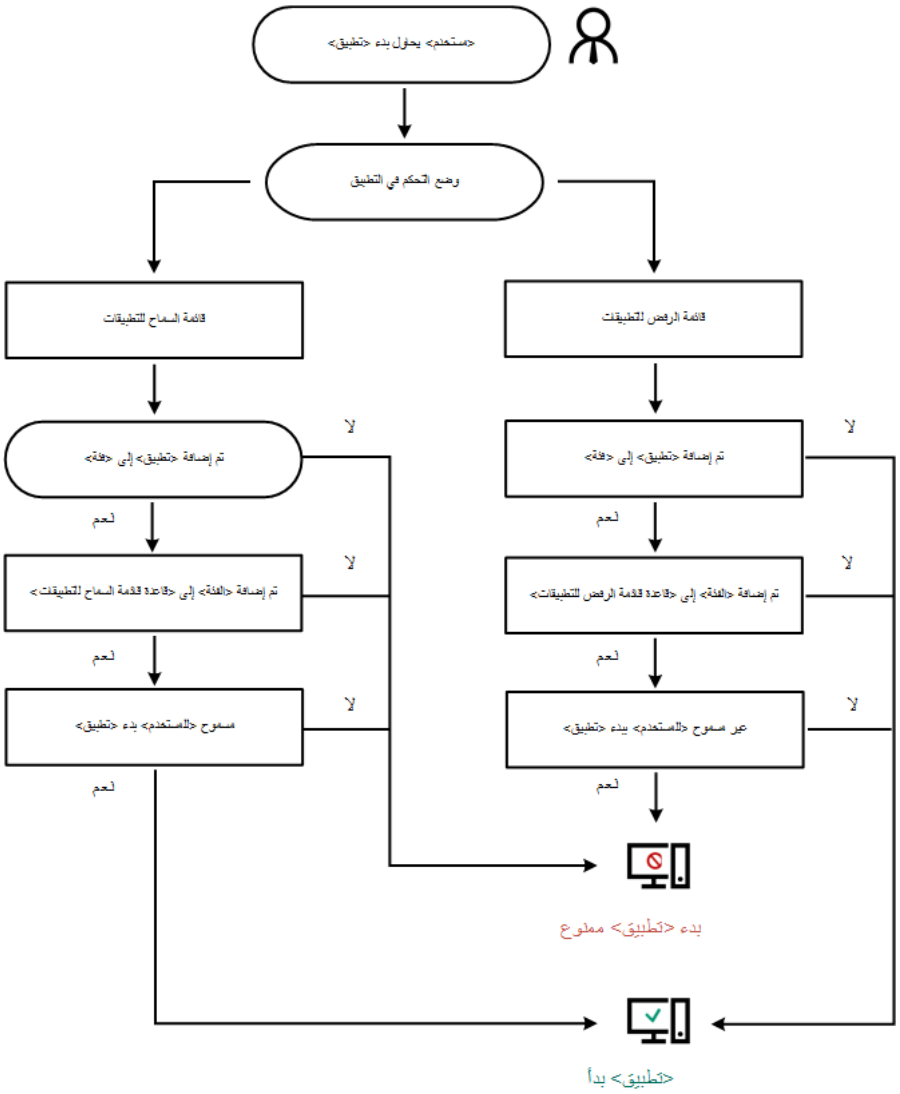
  تستند قواعد التحكم في التطبيقات التي تم إنشاؤها في وحدة تحكم إدارة Kaspersky Security Center إلى فئات التطبيقات المخصصة وليس على شروط التضمين والاستبعاد كما هو الحال في الواجهة المحلية لـ Kaspersky Endpoint Security.

- استلام معلومات حول التطبيقات المثبّتة على أجهزة كمبيوتر الشبكة المحلية للشركة.

ولهذا يوصى باستخدام Kaspersky Security Center لتكوين تشغيل مكون التحكم في التطبيقات.

خوارزمية تشغيل التحكم في التطبيقات

يستخدم Kaspersky Endpoint Security خوارزمية لاتخاذ قرار بشأن تطبيق (انظر الشكل أدناه).



خوارزمية تشغيل التحكم في التطبيقات

قيود وظيفة التحكم في التطبيق

يتم تقييد تشغيل مكون التحكم في التطبيقات في الحالات التالية:

- عندما يتم ترقية إصدار التطبيق، لا يتم دعم استيراد إعدادات مكون التحكم في التطبيق.
- في حالة عدم وجود اتصال بخوادم KSN، يتلقى Kaspersky Endpoint Security معلومات حول سمعة التطبيقات والوحدات النمطية الخاصة بها من قواعد البيانات المحلية فقط.

قد تختلف قائمة التطبيقات التي يعينها Kaspersky Endpoint Security كفئة KL **التطبيقات الأخرى \ التطبيقات، الموثوقة وفقًا للسمعة في شبكة KSN بناءً** على ما إذا كان الاتصال بخوادم KSN متاحًا أم لا.

- في قاعدة بيانات Kaspersky Security Center، يمكن تخزين معلومات حول 150.000 ملف تمت معالجته. وبمجرد تحقق هذا العدد من السجلات، لن تتم معالجة ملفات جديدة. لاستئناف عمليات التخزين، يجب حذف الملفات التي تم تخزينها مسبقًا في قاعدة بيانات Kaspersky Security Center من على الكمبيوتر المثبت عليه Kaspersky Endpoint Security.
- ولا يتحكم المكون في البرامج النصية لبدء التشغيل حتى يتم إرسال البرنامج النصي إلى المفسر عبر سطر الأوامر.

في حالة السماح ببدء تشغيل المفسر بواسطة قواعد التحكم في التطبيق، فلن يقوم المكون بمنع بدء برنامج نصي من هذا المفسر.

في حال منع بدء تشغيل واحد على الأقل من البرامج النصية المحددة في سطر الأوامر الخاص بالمفسر من جانب قواعد التحكم في التطبيق، فإن المكون يقوم بمنع جميع البرامج النصية، المحددة في سطر الأوامر الخاص بالمفسر.

- لا يتحكم المكون في بدء تشغيل البرامج النصية من المفسرين غير المدعومين بوسطة Kaspersky Endpoint Security.

يدعم Kaspersky Endpoint Security المفسرين التاليين:

- Java
- PowerShell

يتم دعم أنواع المفسرين التالية:

- %ComSpec%؛
- %SystemRoot%\\system32\\regedit.exe؛
- %SystemRoot%\\regedit.exe؛
- %SystemRoot%\\system32\\regedt32.exe؛
- %SystemRoot%\\system32\\cscript.exe؛
- %SystemRoot%\\system32\\wscript.exe؛
- %SystemRoot%\\system32\\msiexec.exe؛
- %SystemRoot%\\system32\\mshta.exe؛
- %SystemRoot%\\system32\\rundll32.exe؛
- %SystemRoot%\\system32\\wwahost.exe؛
- %SystemRoot%\\syswow64\\cmd.exe؛
- %SystemRoot%\\syswow64\\regedit.exe؛
- %SystemRoot%\\syswow64\\regedt32.exe؛
- %SystemRoot%\\syswow64\\cscript.exe؛
- %SystemRoot%\\syswow64\\wscript.exe؛
- %SystemRoot%\\syswow64\\msiexec.exe؛
- %SystemRoot%\\syswow64\\mshta.exe؛

- %SystemRoot%\\syswow64\\rundll32.exe؛
- %SystemRoot%\\syswow64\\wwahost.exe.

استلام المعلومات حول التطبيقات المثبَّتة على أجهزة كمبيوتر المستخدمين

لإنشاء القواعد المثلى للتحكم في التطبيق، يوصى أولاً بالحصول على صورة للتطبيقات المستخدمة على أجهزة الكمبيوتر على الشبكة المحلية للشركة. للقيام بذلك، يمكنك الحصول على المعلومات التالية:

- بائعو التطبيقات المستخدمة على الشبكة المحلية بالشركة وإصداراتها وترجمتها.
- عدد مرات تحديث التطبيق.
- سياسات استخدام التطبيق المتبعة في الشركة (قد يكون ذلك سياسات الأمان أو سياسات إدارية).
- مكان تخزين حزم توزيع التطبيق.

تتوافر معلومات حول التطبيقات المستخدمة على أجهزة الكمبيوتر في شبكة المحلية بالشركة في مجلد **سجل التطبيقات** وفي المجلد **الملفات القابلة للتنفيذ**. يوجد مجلد **سجل التطبيقات** ومجلد **الملفات القابلة للتنفيذ** في المجلد **إدارة التطبيق** في شجرة Kaspersky Security Center Administration Console.

يحتوي المجلد **سجل التطبيقات** على قائمة التطبيقات التي اكتشفها عميل الشبكة المثبتة على الكمبيوتر العميل.

يحتوي المجلد **الملفات القابلة للتنفيذ** على قائمة بكل الملفات القابلة للتنفيذ التي تم بدء تشغيلها على أجهزة كمبيوتر عميلة أو تم اكتشافها خلال مهمة مخزون Kaspersky Endpoint Security.

لعرض معلومات عامة حول التطبيق وملفاته التنفيذية، وقائمة بأجهزة الكمبيوتر المثبت عليها تطبيق ما، افتح نافذة خصائص في تطبيق ما تم تحديده في المجلد **سجل التطبيقات** أو في المجلد **الملفات القابلة للتنفيذ**.

لفتح نافذة خصائص التطبيقات في مجلد سجل التطبيقات:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة تحكم الإدارة، حدد مجلد **إضافي** ← **إدارة التطبيق** ← **سجل التطبيقات**.
3. حدد تطبيقًا.
4. في قائمة السياق الخاصة بالتطبيق، حدد **الخصائص**.

لفتح نافذة الخصائص لملف قابل للتنفيذ في المجلد الملفات القابلة للتنفيذ:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة تحكم الإدارة، حدد المجلد **إضافي** ← **إدارة التطبيق** ← **الملفات القابلة للتنفيذ**.
3. حدد ملفًا قابلاً للتنفيذ.
4. في قائمة سياق الملف التنفيذي، حدد **الخصائص**.

تمكين وتعطيل التحكم في التطبيق

يتم تعطيل التحكم في التطبيقات بشكل افتراضي.

تمكين وتعطيل التحكم في التطبيق:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.

3. استخدم مفتاح تبديل **التحكم في التطبيقات** لتمكين المكون أو تعطيله.

4. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين التحكم في التطبيقات، يعيد التطبيق توجيه المعلومات حول تشغيل الملفات القابلة للتنفيذ إلى Kaspersky Security Center. ويمكنك عرض قائمة تشغيل الملفات القابلة للتنفيذ في Kaspersky Security Center في المجلد **الملفات القابلة للتنفيذ**. لتلقي معلومات عن كل الملفات القابلة للتنفيذ بدلاً من الملفات القابلة للتنفيذ قيد التشغيل فقط، قم بتشغيل مهمة المخزون.

تحديد وضع التحكم في التطبيق

لتحديد وضع التحكم في التطبيقات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.

3. في القسم **وضع التحكم في بدء تشغيل التطبيق**، حدد أحد الخيارات التالية:

- **تطبيقات ممنوعة**. في حالة تحديد هذا الخيار، يسمح التحكم في التطبيقات لكل المستخدمين بدء تشغيل أي تطبيقات، إلا في الحالات التي تفي بشروط قواعد منع التحكم في التطبيقات.
- **التطبيقات المسموح بها**. في حالة تحديد هذا الخيار، يمنع التحكم في التطبيقات جميع المستخدمين من بدء تشغيل أي تطبيقات، إلا في الحالات التي تفي بشروط قواعد السماح بالتحكم في التطبيقات.

يتم تحديد القاعدة **صورة ذهبية** والقاعدة **برامج التحديث الموثوقة** مبدئيًا لوضع قائمة السماح. تتوافق قواعد التحكم في التطبيقات هذه مع فئات KL. تتضمن فئة KL "صورة ذهبية" برامج تضمن التشغيل العادي لنظام التشغيل. تتضمن فئة KL "برامج التحديث الموثوقة" برامج تحديث لبائعي البرامج الأكثر شهرة. كما لا يمكنك حذف تلك القواعد. ولا يمكن تحرير إعدادات هذه القواعد. بشكل افتراضي، يتم تمكين القاعدة **صورة ذهبية**، وتعطيل القاعدة **برامج التحديث الموثوقة**. يتم السماح لكل المستخدمين من بدء تشغيل التطبيقات التي تطابق شروط تشغيل تلك القواعد.

ويتم حفظ كل القواعد التي تم إنشاؤها خلال الوضع المحدد بعد تغيير الوضع حتى يمكن استخدام القواعد مرة أخرى. للعودة إلى استخدام هذه القواعد، كل ما عليك فعله هو تحديد الوضع اللازم.

4. في القسم **الإجراء عند بدء تشغيل التطبيقات الممنوعة**، حدد الإجراء الذي سيتم تنفيذه بواسطة المكون عندما يحاول أحد المستخدمين بدء أحد التطبيقات التي تم منعها بواسطة قواعد التحكم في التطبيقات.

5. حدد خانة الاختيار **التحكم في تحميل وحدات DLL** إذا كنت تريد أن يراقب Kaspersky Endpoint Security تحميل وحدات DLL عند بدء التطبيقات بواسطة المستخدمين.

سوف يتم حفظ المعلومات حول الوحدة النمطية والتطبيق الذي قام بتحميل الوحدة النمطية في تقرير.

يراقب Kaspersky Endpoint Security وحدات DLL وبرامج التشغيل التي تم تحميلها منذ تحديد خانة الاختيار. أعد تشغيل الكمبيوتر بعد تحديد خانة الاختيار إذا كنت تريد أن يراقب Kaspersky Endpoint Security جميع وحدات DLL وبرامج التشغيل، بما في ذلك تلك التي تم تحميلها قبل بدء تشغيل Kaspersky Endpoint Security.

عند تمكين التحكم في تحميل وحدات DLL وبرامج التشغيل، تأكد من تمكين إحدى القواعد التالية في إعدادات التحكم في التطبيقات: القاعدة الافتراضية **صورة ذهبية** أو قاعدة أخرى تتضمن فئة KL للشهادات الموثوقة وتضمن تحميل وحدات DLL و برامج التشغيل قبل بدء تشغيل Kaspersky Endpoint Security. وقد يتسبب تمكين التحكم في تحميل وحدات DLL وبرامج التشغيل عند تعطيل قاعدة **صورة ذهبية** في عدم استقرار في نظام التشغيل.

نوصي بتشغيل خاصية حماية كلمة المرور لتكوين إعدادات التطبيق، بحيث يكون من الممكن إيقاف القواعد التي تمنع بدء تشغيل الوحدات النمطية DLL وبرامج التشغيل المهمة، من دون تعديل إعدادات سياسة Kaspersky Security Center.

6. احفظ تغييراتك.

إدارة قواعد التحكم في التطبيق

يتحكم Kaspersky Endpoint Security في بدء تشغيل التطبيقات بواسطة المستخدمين والقواعد. تحدد قاعدة التحكم في التطبيق شروط بدء التشغيل والإجراءات التي يتم تنفيذها بواسطة مكون التحكم في التطبيقات عند بدء تشغيل القاعدة (مما يسمح ببدء تشغيل التطبيق بواسطة المستخدمين أو منعه).

شروط بدء تشغيل القاعدة

يتضمن شرط بدء تشغيل القاعدة الترابط التالي: "نوع الشرط – معيار الشرط – قيمة الشرط". وبناءً على شروط بدء تشغيل القاعدة، يُطبق Kaspersky Endpoint Security (أو لا يطبق) قاعدة على تطبيق.

يتم استخدام الأنواع التالية من الشروط في القواعد:

- شروط التضمين. يطبق Kaspersky Endpoint Security القاعدة إذا توافق التطبيق مع شرط واحد من شروط التضمين على الأقل.
- شروط الاستثناء. لا يطبق Kaspersky Endpoint Security القاعدة على التطبيق إذا توافق التطبيق مع شرط واحد من شروط الاستثناء على الأقل ولا يتوافق مع أي من شروط التضمين.

يتم إنشاء شروط بدء تشغيل التطبيق باستخدام المعايير. يتم استخدام المعايير التالية لإنشاء قواعد في Kaspersky Endpoint Security:

- مسار يقود إلى المجلد الذي يحتوي على الملف التنفيذي للتطبيق أو مسار يقود إلى الملف التنفيذي للتطبيق.
- البيانات الوصفية: اسم الملف التنفيذي الخاص بالتطبيق، إصدار الملف التنفيذي الخاص بالتطبيق، اسم التطبيق، إصدار التطبيق، بائع التطبيق.
- تجزئة الملف التنفيذي الخاص بالتطبيق.
- الشهادة: جهة الإصدار، الموضوع، البصمة.
- تضمين التطبيق في فئة KL.
- مكان الملف التنفيذي الخاص بالتطبيق على محرك القرص القابل للإزالة.

يجب تحديد قيمة المعيار لكل معيار مستخدم في الشرط. إذا تطابقت معلمات التطبيق الجاري بدء تشغيلها مع قيم المعايير المحددة في شرط التضمين، فيتم بدء تشغيل القاعدة. وفي هذه الحالة، ينفذ مكون التحكم في التطبيقات الإجراء المحدد في القاعدة. إذا تطابقت معلمات التطبيق مع قيم المعيار المحددة في شرط الاستثناء، فلا يتحكم مكون التحكم في التطبيقات في بدء تشغيل التطبيق.

إذا كنت قد حددت شهادة كشرط لتشغيل القاعدة، فستحتاج إلى التأكد من إضافة هذه الشهادة إلى وحدة تخزين النظام الموثوقة على الكمبيوتر، وتحقق من إعدادات استخدام وحدة تخزين النظام الموثوقة في التطبيق.

القرارات التي يتم اتخاذها بواسطة مكون التحكم في التطبيقات عند تشغيل قاعدة

عند بدء تشغيل قاعدة، يسمح التحكم في التطبيقات للمستخدمين (أو مجموعات المستخدمين) ببدء التطبيقات أو منع بدء التشغيل وفقًا للقاعدة. يمكنك تحديد مستخدمين فرديين أو مجموعة مستخدمين المسموح لهم أو غير المسموح لهم ببدء تشغيل التطبيقات التي تؤدي لتشغيل قاعدة.

يُطلق على القاعدة التي لا تحدد هؤلاء المستخدمين المسموح لهم ببدء التطبيقات التي تفي بالقاعدة قاعدة منع.

يطلق على القاعدة التي لا تحدد أيًا من المستخدمين غير المسموح لهم ببدء التطبيقات التي تطابق القاعدة قاعدة السماح.

تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. على سبيل المثال، في حالة تعيين قاعدة سماح للتحكم في التطبيق لمجموعة مستخدمين بينما يتم تعيين قاعدة منع للتحكم في التطبيق لمستخدم واحد في مجموعة المستخدمين هذه، فسيتم منع هذا المستخدم من بدء التطبيق.

حالة التشغيل للقاعدة

من الممكن أن تكون قواعد التحكم في التطبيق بواحدة من حالات التشغيل التالية:

- **تم التمكين**. تعني هذه الحالة أن القاعدة مستخدمة عند تشغيل مكون التحكم في التطبيقات.
- **تم التعطيل**. تعني هذه الحالة أن القاعدة يتم تجاهلها عند تشغيل مكون التحكم في التطبيقات.
- **الاختبار**. تشير هذه الحالة إلى أن Kaspersky Endpoint Security يسمح ببدء تشغيل التطبيقات التي تنطبق عليها القواعد ولكنه يسجل معلومات حول بدء تشغيل هذه التطبيقات في التقرير.

إضافة شرط تشغيل لقاعدة التحكم في التطبيقات

لمزيد من الراحة عند إنشاء قواعد التحكم في التطبيقات، يمكنك إنشاء فئات التطبيقات.

يوصى بإنشاء فئة "تطبيقات العمل" التي تغطي مجموعة التطبيقات القياسية التي تستخدم في الشركة. في حالة وجود مجموعات مستخدمين مختلفة تستخدم مجموعات تطبيقات في أعمالها، يمكن إنشاء فئة تطبيق منفصلة لكل مجموعة مستخدمين.

لإنشاء فئة تطبيق في وحدة تحكم الإدارة:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة تحكم الإدارة، حدد **إضافي** ← **إدارة التطبيقات** ← مجلد **فئات التطبيق**.
3. انقر فوق الزر **فئة جديدة** في مساحة العمل.
   يبدأ معالج إنشاء فئة المستخدم.
4. اتبع تعليمات معالج إنشاء فئة المستخدم.

الخطوة 1. تحديد نوع الفئة

يمكنك في هذه الخطوة تحديد أحد أنواع فئات التطبيق التالية:

- **فئة ذات محتوى مضاف يدويًا**. إذا حددت هذا النوع من الفئات، فسوف تتمكن في خطوة "تكوين الشروط لتضمين التطبيقات في فئة" وخطوة "تكوين الشروط لاستثناء التطبيقات من فئة" من تحديد المعايير التي سيتم تضمين الملفات القابلة للتنفيذ بموجبها في الفئة.
- **فئة تتضمن ملفات تنفيذية من الأجهزة المحددة**. إذا حددت هذا النوع من الفئات، فسوف تتمكن في خطوة "الإعدادات" من تحديد كمبيوتر سيتم تضمين الملفات القابلة للتنفيذ الخاصة به في الفئة بشكل آلي.

- **فئة تحتوي على ملفات تنفيذية من مجلد محدد**. إذا حددت هذا النوع من الفئة، فسوف تتمكن في خطوة "مجلد المستودع" من تحديد مجلد سوف يتم تضمين الملفات القابلة للتنفيذ منه في الفئة.

عند إنشاء فئة تتضمن محتويات مضافة تلقائيًا، ينفذ Kaspersky Security Center مخزونًا على الملفات بالتنسيقات التالية: EXE وCOM وDLL وSYS وBAT وPS1 وCMD وVBS وREG وMSI وMSC وCPL وHTML وHTM وDRV وOCX وSCR.

الخطوة 2. إدخال اسم فئة مستخدم

في هذه الخطوة، حدد اسمًا لفئة التطبيق.

الخطوة 3. تكوين الشروط لتضمين التطبيقات في فئة

تتوافر هذه الخطوة إذا حددت نوع الفئة **فئة ذات محتوى مضاف يدويًا**.

في هذه الخطوة، في القائمة المنسدلة **إضافة**، حدد شروط إضافة التطبيقات إلى الفئة:

- **من قائمة الملفات التنفيذية**. إضافة تطبيقات من قائمة الملفات القابلة للتنفيذ على الجهاز العميل إلى الفئة المخصصة.
- **من خصائص الملف**. حدد البيانات التفصيلية للملفات التنفيذية كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **بيانات وصفية من الملفات في المجلد**. حدد مجلدًا على الجهاز العميل يحتوي على الملفات القابلة للتنفيذ. سوف يشير Kaspersky Security Center إلى البيانات الوصفية الخاصة بهذه الملفات كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **المجموعات الاختبارية للملفات في المجلد**. حدد مجلدًا على الجهاز العميل يحتوي على الملفات القابلة للتنفيذ. سوف يشير Kaspersky Security Center إلى تجزئات هذه الملفات كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **شهادات الملفات من المجلد**. حدد مجلدًا على الجهاز العميل يحتوي على الملفات القابلة للتنفيذ الموقعة بهذه الشهادات. سوف يشير Kaspersky Security Center إلى شهادات هذه الملفات كشرط لإضافة التطبيقات إلى الفئة المخصصة.

لا ينصح باستخدام الشروط التي لم يتم تحديد المعلمة **Certificate thumbprint** في خصائصها.

- **البيانات الوصفية لملفات مُثبّت MSI**. حدد حزمة MSI. سوف يشير Kaspersky Security Center إلى بيانات تعريف الملفات القابلة للتنفيذ المجمعة في حزمة MSI هذه كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **المجاميع الاختبارية لـملفات من مُثبّت MSI الخاص بالتطبيق**. حدد حزمة MSI. سوف يشير Kaspersky Security Center إلى تجزئات الملفات القابلة للتنفيذ المجمعة في حزمة MSI هذه كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **من فئة KL**. حدد فئة KL كشرط لإضافة التطبيقات إلى الفئة المخصصة. تعتبر فئة KL عبارة عن قائمة تضم التطبيقات التي لها سمات سمة مشتركة. وتتم إدارة هذه القائمة بواسطة خبراء Kaspersky. على سبيل المثال، تتضمن فئة KL المعروفة باسم "تطبيقات Office" التطبيقات من مجموعة Microsoft Office وAdobe Acrobat وغيرها.

  يمكنك تحديد كل فئات KL لتوليد قائمة موسعة بالتطبيقات الموثوقة.
- **تحديد المسار إلى تطبيق**. حدد مجلدًا على الجهاز العميل. سوف يضيف Kaspersky Security Center الملفات القابلة للتنفيذ من هذا المجلد إلى الفئة المخصصة.
- **تحديد شهادة من المستودع**. حدد الشهادات التي تم استخدامها لتوقيع الملفات القابلة للتنفيذ باعتبارها شرط لإضافة تطبيقات إلى الفئة المخصصة.

لا ينصح باستخدام الشروط التي لم يتم تحديد المعلمة **Certificate thumbprint** في خصائصها.

- **نوع محرك الأقراص**. حدد نوع جهاز التخزين (كل محركات الأقراص الثابتة ومحركات الأقراص القابلة للإزالة، أو محركات الأقراص القابلة للإزالة فقط) كشرط لإضافة التطبيقات إلى الفئة المخصصة.

الخطوة 4. تكوين الشروط لاستثناء التطبيقات من فئة

تتوافر هذه الخطوة إذا حددت نوع الفئة **فئة ذات محتوى مضاف يدويًا**.

يتم استثناء التطبيقات المحددة في هذه الخطوة من الفئة حتى في حالة تحديد هذه التطبيقات في الخطوة "تكوين الشروط لتضمين التطبيقات في فئة".

في هذه الخطوة، في القائمة المنسدلة **إضافة**، حدد شروط استثناء التطبيقات من الفئة:

- **من قائمة الملفات التنفيذية**. إضافة تطبيقات من قائمة الملفات القابلة للتنفيذ على الجهاز العميل إلى الفئة المخصصة.
- **من خصائص الملف**. حدد البيانات التفصيلية للملفات التنفيذية كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **بيانات وصفية من الملفات في المجلد**. حدد مجلدًا على الجهاز العميل يحتوي على الملفات القابلة للتنفيذ. سوف يشير Kaspersky Security Center إلى البيانات الوصفية الخاصة بهذه الملفات كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **المجموعات الاختبارية للملفات في المجلد**. حدد مجلدًا على الجهاز العميل يحتوي على الملفات القابلة للتنفيذ. سوف يشير Kaspersky Security Center إلى تجزئات هذه الملفات كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **شهادات الملفات من المجلد**. حدد مجلدًا على الجهاز العميل يحتوي على الملفات القابلة للتنفيذ الموقعة بهذه الشهادات. سوف يشير Kaspersky Security Center إلى شهادات هذه الملفات كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **البيانات الوصفية لملفات مُثبّت MSI**. حدد حزمة MSI. سوف يشير Kaspersky Security Center إلى بيانات تعريف الملفات القابلة للتنفيذ المجمعة في حزمة MSI هذه كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **المجاميع الاختبارية لـملفات من مُثبّت MSI الخاص بالتطبيق**. حدد حزمة MSI. سوف يشير Kaspersky Security Center إلى تجزئات الملفات القابلة للتنفيذ المجمعة في حزمة MSI هذه كشرط لإضافة التطبيقات إلى الفئة المخصصة.
- **من فئة KL**. حدد فئة KL كشرط لإضافة التطبيقات إلى الفئة المخصصة. تعتبر فئة KL عبارة عن قائمة تضم التطبيقات التي لها سمات سمة مشتركة. وتتم إدارة هذه القائمة بواسطة خبراء Kaspersky. على سبيل المثال، تتضمن فئة KL المعروفة باسم "تطبيقات Office" التطبيقات من مجموعة Microsoft Office وAdobe Acrobat وغيرها.

  يمكنك تحديد كل فئات KL لتوليد قائمة موسعة بالتطبيقات الموثوقة.
- **تحديد المسار إلى تطبيق**. حدد مجلدًا على الجهاز العميل. سوف يضيف Kaspersky Security Center الملفات القابلة للتنفيذ من هذا المجلد إلى الفئة المخصصة.
- **تحديد شهادة من المستودع**. حدد الشهادات التي تم استخدامها لتوقيع الملفات القابلة للتنفيذ باعتبارها شرط لإضافة تطبيقات إلى الفئة المخصصة.
- **نوع محرك الأقراص**. حدد نوع جهاز التخزين (كل محركات الأقراص الثابتة ومحركات الأقراص القابلة للإزالة، أو محركات الأقراص القابلة للإزالة فقط) كشرط لإضافة التطبيقات إلى الفئة المخصصة.

الخطوة 5. الإعدادات

تتوفر هذه الخطوة إذا حددت نوع الفئة **فئة تتضمن ملفات تنفيذية من الأجهزة المحددة**.

في هذه الخطوة، انقر فوق الزر **إضافة** وحدد أجهزة الكمبيوتر التي ستتم إضافة ملفات القابلة للتنفيذ الخاصة بها إلى فئة التطبيق بواسطة Kaspersky Security Center. سوف تضاف كل الملفات القابلة للتنفيذ من أجهزة الكمبيوتر المحددة المعروضة في مجلد **الملفات القابلة للتنفيذ** إلى فئة التطبيق بواسطة Kaspersky Security Center.

في هذه الخطوة، يمكنك تكوين الإعدادات التالية:

- خوارزمية لحساب دالة التجزئة. لتحديد خوارزمية، يجب أن تحدد واحدة على الأقل من خانات الاختيار التالية:
  - **حساب SHA-256 للملفات في هذه الفئة (مدعوم بواسطة Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث)**.
  - **حساب MD5 للملفات في هذه الفئة (مدعوم بواسطة إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- خانة الاختيار **مزامنة البيانات مع مستودع خادم الإدارة**. حدد خانة الاختيار هذه إذا كنت تريد أن يمسح Kaspersky Security Center بصفة دورية فئة التطبيق ويضيفها إلى كل الملفات القابلة للتنفيذ من أجهزة الكمبيوتر المحددة الموجودة في المجلد **الملفات القابلة للتنفيذ**.

  إذا تم مسح خانة الاختيار **مزامنة البيانات مع مستودع خادم الإدارة**، فإن Kaspersky Security Center لن يقوم بإجراء أي تعديلات لفئة التطبيق بعد إنشائها.
- الحقل **مدة الفحص (بالساعات)**. في هذا الحقل، يمكنك تحديد الفترة الزمنية (بالساعات) التي يمسح Kaspersky Security Center بعدها فئة التطبيق ويضيفها إلى كل الملفات القابلة للتنفيذ من أجهزة الكمبيوتر المحددة الموجودة في المجلد **الملفات القابلة للتنفيذ**.

  يتوفر الحقل في حالة تحديد خانة الاختيار **مزامنة البيانات مع مستودع خادم الإدارة**.

الخطوة 6. مجلد المستودع

تتوفر هذه الخطوة إذا حددت نوع الفئة **فئة تحتوي على ملفات تنفيذية من مجلد محدد**.

في هذه الخطوة، دد المجلد الذي سيبحث فيه Kaspersky Security Center عن الملفات القابلة للتنفيذ لإضافة التطبيقات تلقائيًا إلى فئة التطبيق.

في هذه الخطوة، يمكنك تكوين الإعدادات التالية:

- خانة الاختيار **تضمين مكتبات الروابط الديناميكية (.DLL) في هذه الفئة**. حدد خانة الاختيار هذه إذا كنت ترغب في أن تكون مكتبات الربط الديناميكي (ملفات DLL) ضمن فئة التطبيق.

  قد يقلل تضمين ملفات DLL في فئة التطبيق من أداء Kaspersky Security Center.
- خانة الاختيار **تضمين بيانات البرنامج النصي في هذه الفئة**. حدد خانة الاختيار هذه إذا كنت ترغب في أن تكون البرامج النصية ضمن فئة التطبيق.

  قد يقلل تضمين ملفات السيناريوهات في فئة التطبيق من أداء Kaspersky Security Center.
- خوارزمية لحساب دالة التجزئة. لتحديد خوارزمية، يجب أن تحدد واحدة على الأقل من خانات الاختيار التالية:
  - **حساب SHA-256 للملفات في هذه الفئة (مدعوم بواسطة Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث)**.
  - **حساب MD5 للملفات في هذه الفئة (مدعوم بواسطة إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- خانة الاختيار **فرض فحص المجلد للتغييرات**. حدد خانة الاختيار هذه إذا كنت تريد أن يبحث Kaspersky Security Center بشكل دوري عن الملفات القابلة للتنفيذ في المجلد المستخدم للإضافة تلقائيًا إلى فئة التطبيق.

في حالة إلغاء تحديد خانة الاختيار **فرض فحص المجلد للتغييرات**، يبحث Kaspersky Security Center عن الملفات القابلة للتنفيذ في المجلد المستخدم للإضافة تلقائيًا إلى فئة التطبيق فقط في حالة إجراء تغييرات في المجلد أو تمت إضافة ملفات إليه أو حذفها منه.

- الحقل **مدة الفحص (بالساعات)**. في هذا الحقل، يمكنك تحديد الفاصل الزمني (بالساعات) الذي سيبدأ بعده Kaspersky Security Center البحث عن الملفات القابلة للتنفيذ في المجلد المستخدم للإضافة تلقائيًا إلى فئة التطبيق.

  يتوفر هذا الحقل في حالة تحديد خانة الاختيار **فرض فحص المجلد للتغييرات**.

الخطوة 7. إنشاء فئة مخصصة

أغلق المعالج.

لإضافة شرط تفعيل جديد إلى قاعدة التحكم في التطبيق في واجهة التطبيق:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.
3. انقر فوق الزر **تطبيقات ممنوعة** أو **التطبيقات المسموح بها**.

   يفتح هذا قائمة قواعد التحكم في التطبيقات.
4. حدد القاعدة التي تريد تكوين شرط تشغيل لها.

   يتم فتح خصائص قاعدة التحكم في التطبيقات.
5. حدد علامة التبويب **الشروط: N** أو علامة التبويب **الاستثناءات: N** وانقر فوق الزر **إضافة**.
6. حدد شروط التشغيل لقاعدة التحكم في التطبيقات:

- **شروط من خصائص التطبيقات التي تم بدء تشغيلها**. في قائمة التطبيقات قيد التشغيل، يمكنك تحديد التطبيقات التي سيتم تطبيق قاعدة التحكم في التطبيقات عليها. يسرد Kaspersky Endpoint Security أيضًا التطبيقات التي كانت تعمل مسبقًا على الكمبيوتر. تحتاج إلى تحديد المعيار الذي تريد استخدامه لإنشاء شرط تشغيل قاعدة واحد أو عدة شروط: **مسار الملف** أو **الشهادة** أو **فئة KL** أو **البيانات الوصفية** أو **المسار المؤدي للملف أو المجلد**.
- **شروط "فئة KL"**. تعتبر فئة KL عبارة عن قائمة تضم التطبيقات التي لها سمات سمة مشتركة. وتتم إدارة هذه القائمة بواسطة خبراء Kaspersky. على سبيل المثال، تتضمن فئة KL المعروفة باسم "تطبيقات Office" التطبيقات من مجموعة Microsoft Office و®Acrobat ®Adobe وغيرها.
- **شرط مخصص**. يمكنك تحديد ملف التطبيق وتحديد أحد شروط تشغيل القاعدة: **مسار الملف** أو **الشهادة** أو **البيانات الوصفية** أو **المسار المؤدي للملف أو المجلد**.
- **الحالة عن طريق محرك أقراص الملفات (محرك الأقراص القابل للإزالة)**. يتم تطبيق قاعدة التحكم في التطبيقات فقط على الملفات التي يتم تشغيلها على محرك أقراص قابل للإزالة.
- **شروط من خصائص الملفات في المجلد المُحدد**. يتم تطبيق قاعدة التحكم في التطبيقات فقط على الملفات الموجودة داخل المجلد المحدد. يمكنك أيضًا تضمين أو استثناء الملفات من المجلدات الفرعية. تحتاج إلى تحديد المعيار الذي تريد استخدامه لإنشاء شرط تشغيل قاعدة واحد أو عدة شروط: **مسار الملف** أو **الشهادة** أو **فئة KL** أو **البيانات الوصفية** أو **المسار المؤدي للملف أو المجلد**.

7. احفظ تغييراتك.

عند إضافة الشروط، يرجى مراعاة الاعتبارات الخاصة التالية للتحكم في التطبيقات:

- لا يدعم Kaspersky Endpoint Security تجزئة الملف MD5 ولا يتحكم في بدء تشغيل التطبيقات بناءً على تجزئة MD5. يتم استخدام تجزئة SHA256 كشرط لتشغيل القاعدة.
- لا يوصى باستخدام معياري **جهة الإصدار** و**الموضوع** فقط كشروط لإطلاق القاعدة. حيث أن استخدام تلك المعايير غير موثوق به.

- إذا كنت تستخدم رابطًا رمزيًا في الحقل **المسار المؤدي للملف أو المجلد**، فننصحك بحل الرابط الرمزي للتشغيل الصحيح لقاعدة التحكم في التطبيق. للقيام بذلك، انقر فوق الزر **حل الرابط الرمزي**.

إضافة الملفات التنفيذية من مجلد الملفات التنفيذية إلى فئة التطبيق

في المجلد **الملفات القابلة للتنفيذ**، يتم عرض قائمة الملفات القابلة للتنفيذ المكتشفة على أجهزة الكمبيوتر. يقوم برنامج Kaspersky Endpoint Security بإنشاء قائمة بالملفات القابلة للتنفيذ بعد تنفيذ مهمة المخزون.

لإضافة الملفات القابلة للتنفيذ من مجلد الملفات القابلة للتنفيذ إلى فئة التطبيق:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة تحكم الإدارة، حدد مجلد **إضافي** ← **إدارة التطبيق** ← **الملفات القابلة للتنفيذ**.
3. في مساحة العمل، حدد الملفات القابلة للتنفيذ التي تريد إضافتها إلى فئة التطبيق.
4. انقر بزر الماوس الأيمن لفتح قائمة السياق الخاصة بالملفات القابلة للتنفيذ المحددة وحدد **إضافة إلى فئة**.
5. في النافذة التي تفتح، افعل ما يلي:
   - في الجزء العلوية من النافذة، اختر أحد الخيارات التالية:
     - **إضافة إلى فئة تطبيق جديدة**. اختر هذا الخيار إذا كنت تريد إنشاء فئة تطبيق جديدة، وأضف الملفات القابلة للتنفيذ إليه.
     - **إضافة إلى فئة تطبيق حالي**. اختر هذا الخيار إذا كنت تريد تحديد فئة تطبيق موجودة وإضافة الملفات القابلة للتنفيذ إليها.
   - في القسم **نوع القاعدة**، حدد أحد الخيارات التالية:
     - **قواعد الإضافة إلى التضمينات**. حدد هذا الخيار إذا كنت تريد إنشاء شرط يضيف الملفات القابلة للتنفيذ إلى فئة التطبيق.
     - **قواعد الإضافة إلى الاستثناءات**. حدد هذا الخيار إذا كنت تريد إنشاء شرط يستثني الملفات القابلة للتنفيذ إلى فئة التطبيق.
   - في القسم **المعلمة المستخدمة كشرط**، حدد أحد الخيارات التالية:
     - **تفاصيل الشهادة (أو تجزئة SHA-256 للملفات التي لا تحتوي على شهادة)**.
     - **تفاصيل الشهادة (سيتم تخطي الملفات التي لا يوجد لديها شهادة)**.
     - **SHA-256 فقط (سيتم تخطي الملفات التي لا تحتوي على تجزئة)**.
     - **MD5 فقط (الوضع المتوقف، لإصدار Kaspersky Endpoint Security 10 Service Pack 1 فقط)**.
6. احفظ تغييراتك.

إضافة الملفات التنفيذية ذات الصلة بالحدث إلى فئة التطبيق

لإضافة الملفات القابلة للتنفيذ المرتبطة بأحداث التحكم في التطبيق إلى فئة التطبيق:

1. افتح Kaspersky Security Center Administration Console.
2. في العقدة **خادم الإدارة** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **الأحداث**.

3. اختر مجموعة أحداث متعلقة بتشغيل مكون التحكم في التطبيقات (عرض الأحداث الناتجة عن تشغيل مكون التحكم في التطبيقات، عرض الأحداث الناتجة عن عملية اختبار مكون التحكم في التطبيقات) في القائمة المنسدلة **تحديدات الأحداث**.

4. انقر فوق الزر **تشغيل التحديد**.

5. حدد الأحداث التي تريد إضافة ملفاتها التنفيذية المرتبطة إلى فئة التطبيق.

6. انقر بزر الماوس الأيمن لفتح قائمة السياق الخاصة بالأحداث المحددة وحدد **إضافة إلى فئة**.

7. في النافذة التي تفتح، كوّن إعدادات فئة التطبيق:

- في الجزء العلوية من النافذة، اختر أحد الخيارات التالية:
- **إضافة إلى فئة تطبيق جديدة**. اختر هذا الخيار إذا كنت تريد إنشاء فئة تطبيق جديدة، وأضف الملفات القابلة للتنفيذ إليه.
- **إضافة إلى فئة تطبيق حالي**. اختر هذا الخيار إذا كنت تريد تحديد فئة تطبيق موجودة وإضافة الملفات القابلة للتنفيذ إليها.
- في القسم **نوع القاعدة**، حدد أحد الخيارات التالية:
- **قواعد الإضافة إلى التضمينات**. حدد هذا الخيار إذا كنت تريد إنشاء شرط يضيف الملفات القابلة للتنفيذ إلى فئة التطبيق.
- **قواعد الإضافة إلى الاستثناءات**. حدد هذا الخيار إذا كنت تريد إنشاء شرط يستثني الملفات القابلة للتنفيذ إلى فئة التطبيق.
- في القسم **المعلمة المستخدمة كشرط**، حدد أحد الخيارات التالية:
- **تفاصيل الشهادة (أو تجزئات SHA-256 للملفات التي لا تحتوي على شهادة)**.
- **تفاصيل الشهادة (سيتم تخطي الملفات التي لا يوجد لديها شهادة)**.
- **SHA-256 فقط (سيتم تخطي الملفات التي لا تحتوي على تجزئة)**.
- **MD5 فقط (الوضع المتوقف، لإصدار Kaspersky Endpoint Security 10 Service Pack 1 فقط)**.

8. احفظ تغييراتك.

إضافة قاعدة التحكم في التطبيقات

لإضافة قاعدة تحكم في التطبيق باستخدام Kaspersky Security Center:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان ← التحكم في التطبيقات**.
في الجزء الأيسر من النافذة، يتم عرض إعدادات مكون التحكم في التطبيقات.

5. انقر على **إضافة**.
تفتح النافذة **قاعدة التحكم في التطبيقات**.

6. قم بأحد الإجراءات التالية:

- إذا كنت تريد إنشاء فئة جديدة:

a. انقر على **إنشاء فئة**.

يبدأ معالج إنشاء فئة المستخدم.

b. اتبع تعليمات معالج إنشاء فئة المستخدم.

c. في القائمة المنسدلة **الفئة**حدد فئة التطبيق التي تم إنشاؤها.

- إذا كنت تريد تحرير فئة موجودة:

a. في القائمة المنسدلة **الفئة**، حدد فئة التطبيق التي تم إنشاؤها والمراد تحريرها.

b. انقر على **الخصائص**.

c. قم بتعديل إعدادات فئة التطبيق المختارة.

d. احفظ تغييراتك.

e. في القائمة المنسدلة **الفئة**، حدد فئة التطبيق التي تم إنشاؤها والتي تريد إنشاء قاعدة بناءً عليها.

7. في الجدول **التابعون وحقوقهم**، انقر فوق الزر **إضافة**.

8. في النافذة التي تفتح، حدد قائمة المستخدمين و/أو مجموعات المستخدمين التي تريد تكوين أذونات لها لبدء التطبيقات من الفئة المحددة.

9. في الجدول **التابعون وحقوقهم**، نفذ التالي:

- إذا كنت تريد تحديد مستخدمين و/أو مجموعات ببدء التطبيقات التي تنتمي إلى الفئة المحددة، حدد خانة الاختيار **سماح** في الصفوف ذات الصلة.
- إذا كنت تريد منع المستخدمين و /أو مجموعات المستخدمين من بدء التطبيقات التي تنتمي للفئة المحددة، فحدد خانة الاختيار **رفض** في الصفوف ذات الصلة.

10. حدد خانة الاختيار **رفض للمستخدمين الآخرين** إذا كنت تريد منع جميع المستخدمين الذين لا يظهرون في العمود **الموضوع** والذين ليسوا جزءًا من مجموعة المستخدمين المحددة في العمود **الموضوع** من بدء التطبيقات التي تنتمي للفئة المحددة.

11. إذا كنت تريد أن يضع برنامج Kaspersky Endpoint Security في الاعتبار التطبيقات التي تتضمنها فئة التطبيقات المحددة كبرامج تحديث موثوقة مسموح لها بإنشاء الملفات التنفيذية سيتم السماح لها لاحقًا بالعمل، حدد خانة الاختيار **برامج التحديث الموثوقة**.

عند ترحيل إعدادات Kaspersky Endpoint Security، يتم ترحيل قائمة الملفات القابلة للتنفيذ التي تم إنشاؤها من جانب برامج التحديث الموثوقة كذلك.

12. احفظ تغييراتك.

لإضافة قاعدة للتحكم في التطبيقات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.

3. انقر فوق الزر **تطبيقات ممنوعة** أو **التطبيقات المسموح بها**.

يفتح هذا قائمة قواعد التحكم في التطبيقات.

4. انقر على **إضافة**.

يؤدي هذا إلى فتح نافذة إعدادات قاعدة التحكم في التطبيقات.

5. في علامة التبويب **الإعدادات العامة**، حدد الإعدادات الرئيسية للقاعدة:

a. في الحقل **اسم القاعدة** أدخل اسم القاعدة.

b. في الحقل **الوصف** أدخل وصفًا للقاعدة.

c. قم بتجميع أو تحرير قائمة مستخدمين و/أو مجموعات مستخدمين المسموح لهم ببدء التطبيقات التي تتوافق مع شروط تشغيل القاعدة أو غير المسموح لهم بذلك. ولفعل ذلك، انقر فوق الزر **إضافة** في الجدول **التابعون وحقوقهم**.

تُطبق القاعدة على كل المستخدمين افتراضيًا.

إذا لم يتم تحديد مستخدم في الجدول، فلا يمكن حفظ القاعدة.

d. في الجدول **التابعون وحقوقهم**، استخدم مفتاح التبديل لتحديد حق المستخدمين في بدء التطبيقات.

e. حدد خانة الاختيار **رفض للمستخدمين الآخرين** إذا كنت تريد من التطبيق أن يمنع التطبيقات التي تلبي شروط تشغيل القاعدة من التشغيل لجميع المستخدمين غير المدرجين في الجدول **التابعون وحقوقهم** وليسوا أعضاء في مجموعات المستخدمين المدرجة في الجدول **التابعون وحقوقهم**.

إذا تم إلغاء تحديد خانة الاختيار **رفض للمستخدمين الآخرين**، فإن Kaspersky Endpoint Security لا يتحكم في بدء تشغيل التطبيقات بواسطة المستخدمين غير المحددين في الجدول **التابعون وحقوقهم** والذين لا ينتمون إلى مجموعات المستخدمين المحددة في الجدول **التابعون وحقوقهم**.

f. حدد خانة الاختيار **برامج التحديث الموثوقة** إذا كنت تريد أن يضع Kaspersky Endpoint Security في الاعتبار التطبيقات المطابقة لشروط تشغيل القاعدة كبرامج تحديث موثوقة. برامج التحديث الموثوقة هي التطبيقات التي يُسمح لها بإنشاء ملفات قابلة للتنفيذ أخرى سيسمح بتشغيلها لاحقًا.

إذا قام أحد التطبيقات بتشغيل قواعد متعددة، فإن Kaspersky Endpoint Security يعيّن علامة برامج التحديث الموثوقة في حالة استيفاء الشروط التالية:

- تسمح كل القواعد بتشغيل التطبيق.
- تمتلك قاعدة واحدة على الأقل خانة الاختيار **برامج التحديث الموثوقة**.

6. في علامة التبويب **الشروط: N**، أنشئ أو حرر قائمة تضمين الشروط لتشغيل القاعدة.

7. في علامة التبويب **الاستثناءات: N**، أنشئ قائمة شروط الاستثناء أو قم بتحريرها لتشغيل القاعدة.

عند ترحيل إعدادات Kaspersky Endpoint Security، يتم ترحيل قائمة الملفات القابلة للتنفيذ التي تم إنشاؤها من جانب برامج التحديث الموثوقة كذلك.

8. احفظ تغييراتك.

تغيير حالة قاعدة التحكم في التطبيق عبر Kaspersky Security Center

لتغيير حالة قاعدة التحكم في التطبيق في وحدة تحكم الإدارة:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان ← التحكم في التطبيقات**.

في الجزء الأيسر من النافذة، يتم عرض إعدادات مكون التحكم في التطبيقات.

5. في العمود **الحالة**، انقر بزر الماوس الأيسر لعرض قائمة السياق وتحديد أحد ما يلي:

- **تشغيل**. تعني هذه الحالة أن القاعدة مستخدمة عند تشغيل مكون التحكم في التطبيقات.
- **إيقاف**. تعني هذه الحالة أن القاعدة يتم تجاهلها عند تشغيل مكون التحكم في التطبيقات.
- **اختبار**. تعني هذه الحالة أن Kaspersky Endpoint Security يسمح دائمًا ببدء تشغيل التطبيقات التي تنطبق عليها القاعدة ولكنه يسجل معلومات حول بدء تشغيل هذه التطبيقات في التقرير.

6. احفظ تغييراتك.

لتغيير حالة قاعدة التحكم في التطبيق في وحدة تحكم الإدارة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.
3. انقر فوق الزر **تطبيقات ممنوعة** أو **التطبيقات المسموح بها**.
يفتح هذا قائمة قواعد التحكم في التطبيقات.
4. في العمود **الحالة**، افتح قائمة السياق وحدد أحد الخيارات التالية:

- **تم التمكين**. تعني هذه الحالة أن القاعدة مستخدمة عند تشغيل مكون التحكم في التطبيقات.
- **تم التعطيل**. تعني هذه الحالة أن القاعدة يتم تجاهلها عند تشغيل مكون التحكم في التطبيقات.
- **الاختبار**. تعني هذه الحالة أن Kaspersky Endpoint Security يسمح دائمًا ببدء تشغيل التطبيقات التي تنطبق عليها هذه القاعدة ولكنه يسجل معلومات حول بدء تشغيل هذه التطبيقات في التقرير.

5. احفظ تغييراتك.

تصدير واستيراد قواعد التحكم في التطبيقات

يمكنك تصدير قائمة قواعد التحكم في التطبيقات إلى ملف XML. يمكنك استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة قواعد التحكم في التطبيقات أو لترحيل القائمة إلى خادم مختلف.

عند تصدير واستيراد قواعد التحكم في التطبيقات، يرجى مراعاة الاعتبارات الخاصة التالية:

- يستطيع Kaspersky Endpoint Security تصدير قائمة القواعد فقط لوضع التحكم في التطبيقات الفعال. بمعنى آخر، إذا كان التحكم في التطبيقات يعمل في وضع قائمة الرفض، فإن Kaspersky Endpoint Security يستطيع تصدير قواعد لهذا الوضع فقط. ولتصدير قائمة القواعد الخاصة بوضع قائمة السماح، تحتاج إلى تبديل الوضع وتشغيل عملية التصدير مرة أخرى.
- يستخدم Kaspersky Endpoint Security فئات التطبيقات لكي تعمل قواعد التحكم في التطبيقات. وعند ترحيل قائمة قواعد التحكم في التطبيقات إلى خادم مختلف، فإنك تحتاج أيضًا إلى ترحيل قائمة فئات التطبيقات. وللمزيد من التفاصيل عن تصدير أو استيراد فئات التطبيقات، يرجى الرجوع إلى تعليمات Kaspersky Security Center.

كيفية تصدير واستيراد قائمة قواعد التحكم في التطبيقات في وحدة التحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في التطبيقات**.

5. لتصدير قائمة قواعد التحكم في التطبيقات:

   a. حدد القواعد التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

   إذا لم تحدد أي قاعدة، فسيقوم Kaspersky Endpoint Security بتصدير كل القواعد.

   b. انقر على رابط **تصدير**.

   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة القواعد إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.

   d. احفظ الملف.

   يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد بالكامل إلى ملف XML.

6. لاستيراد قائمة قواعد التحكم في التطبيقات:

   a. انقر على رابط **استيراد**.

   في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

   b. افتح الملف.

   إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد التحكم في التطبيق في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Security Controls** ← **Application Control**.

5. انقر على رابط **Rules Lists Settings**.

6. حدد قائمة القواعد: قائمة الرفض أو قائمة السماح الخاصة بالتطبيق.

7. لتصدير قائمة قواعد التحكم في التطبيقات:

   a. حدد القواعد التي تريد تصديرها.

   b. انقر على **Export**.

   c. أكد أنك تريد تصدير القواعد المحددة فقط، أو تصدير القائمة بأكملها.

   d. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف XML في مجلد التنزيلات الافتراضي.

8. لاستيراد قائمة قواعد التحكم في التطبيقات:

   a. انقر على رابط **Import**.
   في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

   b. افتح الملف.
   إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

9. احفظ تغييراتك.

عرض الأحداث الناتج عن تشغيل مكون التحكم في التطبيقات

لعرض الأحداث الناتجة عن تشغيل مكون التحكم في التطبيقات المستلمة بواسطة Kaspersky Security Center:

1. افتح Kaspersky Security Center Administration Console.

2. في العقدة **خادم الإدارة** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **الأحداث**.

3. انقر فوق الزر **إنشاء مجموعة محددة**.

4. في النافذة التي تفتح، حدد القسم **الأحداث**.

5. انقر فوق الزر **مسح الكل**.

6. في الجدول **Events**، حدد خانة الاختيار **تم حظر بدء تشغيل التطبيق**.

7. احفظ تغييراتك.

8. في القائمة المنسدلة **تحديدات الأحداث**، حدد المجموعة التي تم إنشاؤها.

9. انقر فوق الزر **تشغيل التحديد**.

عرض تقرير حول التطبيقات المحجوبة

لعرض تقرير حول التطبيقات المحجوبة:

1. افتح Kaspersky Security Center Administration Console.

2. في العقدة **خادم الإدارة** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **تقارير**.

3. انقر فوق الزر **قالب التقارير الجديد**.
بدء تشغيل معالج قالب تقرير جديد.

4. اتبع تعليمات معالج قالب التقرير. في الخطوة **تحديد نوع قالب التقرير**، حدد **أخرى ← تقرير حول التطبيقات الممنوعة**.
بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول في علامة التبويب **تقارير**.

5. افتح التقرير بالنقر المزدوج عليه.

تبدأ عملية إنشاء التقرير. يتم عرض التقرير في نافذة جديدة.

اختبار قواعد التحكم في التطبيق

للتأكد من عدم منع قواعد التحكم في التطبيقات للتطبيقات المطلوبة للعمل، يوصى بتمكين اختبار قواعد التحكم في التطبيقات وتحليل عملياتها بعد إنشاء القواعد الجديدة. عند تمكين اختبار قواعد التحكم في التطبيقات، لن يمنع Kaspersky Endpoint Security التطبيقات الممنوع بدء تشغيلها بواسطة التحكم في التطبيقات، ولكنه سيرسل إخطارات حول بدء تشغيلها إلى خادم الإدارة.

يتطلب تحليل قواعد التحكم في التطبيق مراجعة لأحداث التحكم في التطبيقات الناتجة التي تم إبلاغها إلى Kaspersky Security Center. إذا تسبب وضع الاختبار في عدم وجود أحداث بدء تشغيل ممنوعة لكل التطبيقات المطلوبة لعمل مستخدم الكمبيوتر، فإن هذا يعني أنه تم إنشاء القواعد الصحيحة. وإلا فإننا ننصحك بتحديث إعدادات القواعد التي قمت بإنشائها أو إنشاء قواعد إضافية أو حذف القواعد الحالية.

الوضع الافتراضي أن Kaspersky Endpoint Security يسمح لبدء تشغيل جميع التطبيقات باستثناء التطبيقات التي تحظرها القواعد.

تمكين وتعطيل اختبار قاعدة التحكم في التطبيقات

لتمكين أو تعطيل اختبار قواعد التحكم في التطبيقات في Kaspersky Security Center:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان ← التحكم في التطبيقات**.
في الجزء الأيسر من النافذة، يتم عرض إعدادات مكون التحكم في التطبيقات.

5. في القائمة المنسدلة **وضع التحكم**، حدد أحد العناصر التالية:

- **قائمة الرفض**. في حالة تحديد هذا الخيار، يسمح التحكم في التطبيقات لكل المستخدمين بدء تشغيل أي تطبيقات، إلا في الحالات التي تفي بشروط قواعد منع التحكم في التطبيقات.
- **قائمة السماح**. في حالة تحديد هذا الخيار، يمنع التحكم في التطبيقات جميع المستخدمين من بدء تشغيل أي تطبيقات، إلا في الحالات التي تفي بشروط قواعد السماح بالتحكم في التطبيقات.

6. قم بأحد الإجراءات التالية:

- إذا كنت تريد تمكين الاختبار لقواعد التحكم في التطبيقات، حدد خيار **اختبار القواعد** في القائمة المنسدلة **الإجراء**.
- إذا كنت ترغب في تمكين التحكم في التطبيقات لإدارة بدء تشغيل التطبيقات على أجهزة كمبيوتر المستخدم، في القائمة المنسدلة، حدد **تطبيق القواعد**.

7. احفظ تغييراتك.

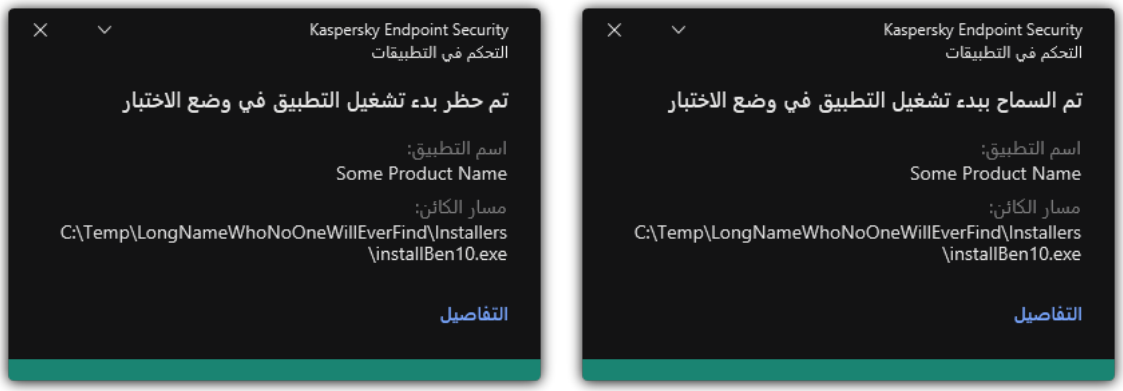
لتمكين اختبار قواعد التحكم في التطبيقات أو لتحديد إجراء منع للتحكم في التطبيقات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.
3. انقر فوق الزر **تطبيقات ممنوعة** أو **التطبيقات المسموح بها**.

   يفتح هذا قائمة قواعد التحكم في التطبيقات.
4. في العمود **الحالة**، حدد **الاختبار**.

   تعني هذه الحالة أن Kaspersky Endpoint Security يسمح دائمًا ببدء تشغيل التطبيقات التي تنطبق عليها هذه القاعدة ولكنه يسجل معلومات حول بدء تشغيل هذه التطبيقات في التقرير.
5. احفظ تغييراتك.

لن يمنع Kaspersky Endpoint Security التطبيقات الممنوع بدء تشغيلها بواسطة مكون التحكم في التطبيقات، ولكنه سيرسل إخطارات حول بدء تشغيلها إلى خادم الإدارة. ومكنك أيضا تكوين عرض الإخطارات حول اختبار القواعد على كمبيوتر المستخدم (انظر الشكل أدناه).



إخطارات التحكم في التطبيقات في وضع الاختبار

لعرض التقرير الخاص بالتطبيقات المحجوبة في وضع الاختبار

لعرض التقرير الخاص بالتطبيقات المحجوبة في وضع الاختبار:

1. افتح Kaspersky Security Center Administration Console.

2. في العقدة **خادم الإدارة** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **تقارير**.

3. انقر فوق الزر **قالب التقارير الجديد**.
بدء تشغيل معالج قالب تقرير جديد.

4. اتبع تعليمات معالج قالب التقرير. في الخطوة **تحديد نوع قالب التقرير**، حدد **أخرى ← تقرير عن التطبيقات الممنوعة في وضع الاختبار**.
بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول في علامة التبويب **تقارير**.

5. افتح التقرير بالنقر المزدوج عليه.

تبدأ عملية إنشاء التقرير. يتم عرض التقرير في نافذة جديدة.

عرض الأحداث الناتجة عن عملية اختبار مكون التحكم في التطبيقات

لعرض أحداث اختبار التحكم في التطبيقات بواسطة Kaspersky Security Center:

1. افتح Kaspersky Security Center Administration Console.

2. في العقدة **خادم الإدارة** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **الأحداث**.

3. انقر فوق الزر **إنشاء مجموعة محددة**.

4. في النافذة التي تفتح، حدد القسم **الأحداث**.

5. انقر فوق الزر **مسح الكل**.

6. في الجدول **Events**، حدد خانتي الاختيار **تم حظر بدء تشغيل التطبيق في وضع الاختبار** و**تم السماح ببدء تشغيل التطبيق في وضع الاختبار**.

7. احفظ تغييراتك.

8. في القائمة المنسدلة **تحديدات الأحداث**، حدد المجموعة التي تم إنشاؤها.

9. انقر فوق الزر **تشغيل التحديد**.

مراقبة نشاط التطبيقات

مراقبة نشاط التطبيقات أداة مصممة لعرض معلومات حول نشاط التطبيقات على كمبيوتر المستخدم في الوقت الحقيقي.

يتطلب استخدام مراقبة نشاط التطبيقات تثبيت مكوني التحكم في التطبيقات ومنع اختراق المضيف. وإذا لم يتم تثبيت هذين المكونين، فإن قسم مراقبة نشاط التطبيقات في نافذة التطبيق الرئيسية يكون مخفيًا.

لبدء مراقبة نشاط التطبيقات:

في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **مراقبة نشاط التطبيقات**.

في هذه النافذة، يتم تقديم معلومات حول نشاط التطبيقات على كمبيوتر المستخدم في ثلاث علامات تبويب:

- تعرض علامة التبويب **كل التطبيقات** معلومات حول كل التطبيقات المثبتة على الكمبيوتر.
- تعرض علامة التبويب **قيد التشغيل** معلومات حول استهلاك موارد الكمبيوتر بواسطة كل تطبيق في الوقت الحقيقي. ويمكنك من علامة التبويب هذه أيضًا المتابعة إلى تكوين الأذونات لتطبيق فردي.
- تعرض علامة التبويب **تشغيل عند بدء التشغيل** قائمة التطبيقات التي تم تشغيلها عند بدء تشغيل نظام التشغيل.

إذا كنت تريد إخفاء معلومات نشاط التطبيق على كمبيوتر المستخدم، فيمكنك تقييد وصول المستخدم إلى أداة مراقبة نشاط التطبيق.

كيفية إخفاء مراقبة نشاط التطبيق في واجهة التطبيق باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الواجهة**.
5. استخدم خانة الاختيار **إخفاء قسم مراقبة نشاط التطبيقات** لمنح حق الوصول إلى الأداة أو إبطاله.
6. احفظ تغييراتك.

كيفية إخفاء مراقبة نشاط التطبيقات في واجهة التطبيق باستخدام Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General settings** ← **Interface**.
5. استخدم خانة الاختيار **Hide Application Activity Monitor section** لمنح حق الوصول إلى الأداة أو إبطاله.
6. احفظ تغييراتك.

قواعد لإنشاء أقنعة أسماء للملفات أو المجلدات

قناع اسم الملف أو المجلد هو تمثيل لاسم مجلد أو اسم وامتداد لملف باستخدام أحرف شائعة.

يمكنك استخدام الأحرف الشائعة التالية لتشكيل قناع اسم ملف أو مجلد:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة). على سبيل المثال، سيتضمن القناع `C:\*.txt` كل المسارات إلى الملفات بامتداد `txt` الموجودة في المجلدات على محرك الأقراص (C:).

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

تحرير قوالب رسالة التحكم في التطبيقات

عندما يحاول أحد المستخدمين بدء تشغيل تطبيق تم منعه بواسطة قاعدة التحكم في التطبيق، يعرض Kaspersky Endpoint Security رسالة تفيد بأن التطبيق قد تم منع بدء تشغيله. إذا كان المستخدم يظن بأن التطبيق قد تم منعه من البداية عن طريق الخطأ، فيمكنه استخدام الرابط الموجود في نص الرسالة لإرسال رسالة لمسؤول شبكة الشركة المحلية.

تتوفر قوالب خاصة للرسالة التي يتم عرضها عند منع تشغيل التطبيق وللرسالة التي يتم إرسالها إلى المسؤول. ويمكنك تعديل قوالب الرسالة.

لتحرير قالب رسالة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.
3. في القسم **قوالب رسائل عن منع التطبيق**، كوّن قوالب لرسائل التحكم في التطبيقات:
   - **رسالة حول المنع**. قالب الرسالة التي يتم عرضها عندما يتم بدء تشغيل قاعدة التحكم في التطبيق التي تمنع بدء تشغيل تطبيق ما. نعرض الإخطار حول تطبيق ممنوع في الشكل أدناه.

     لا يمكنك تكوين قوالب الرسائل للتحكم في التطبيقات في وضع الاختبار. ويعرض التحكم في التطبيقات في وضع الاختبار إخطارات محددة مسبقًا.
   - **رسالة إلى المسؤول**. قالب الرسالة التي يمكن للمستخدم إرسالها إلى مسؤول الشبكة المحلية للشركة إذا كان المستخدم يعتقد أنه قد تم حظر التطبيق عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع بدء تشغيل التطبيق إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.
4. احفظ تغييراتك.

إشعار التحكم في التطبيقات

أفضل الممارسات لتنفيذ قائمة التطبيقات المسموح بها

عند تخطيط تنفيذ قائمة تطبيقات مسموح بها، يوصى بتنفيذ الإجراءات التالية:

1. من أنواع المجموعات التالية:

- مجموعات المستخدمين. مجموعات المستخدمين الذين تحتاج السماح لهم باستخدام مجموعات التطبيقات المتنوعة.
- مجموعات الإدارة. مجموعة واحدة أو عدة مجموعات من أجهزة الكمبيوتر التي سيطبق Kaspersky Security Center عليها قائمة التطبيقات المسموح بها. من الضروري إنشاء مجموعات متعددة من أجهزة الكمبيوتر في حالة استخدام إعدادات مختلفة لقائمة السماح لتلك المجموعات.

2. إنشاء قائمة بالتطبيقات التي يجب السماح ببدء تشغيلها.

قبل إنشاء قائمة، ننصحك بتنفيذ ما يلي:

a. تشغيل مهمة المخزون.

وتتوافر معلومات حول إنشاء وإعادة تكوين وبدء تشغيل مهمة مخزون في القسم إدارة المهام.

b. اعرض قائمة الملفات القابلة للتنفيذ.

تكوين وضع قائمة السماح للتطبيقات

عند تكوين وضع قائمة السماح، يوصى بتنفيذ الإجراءات التالية:

1. إنشاء فئات التطبيق التي تحتوي على التطبيقات التي يجب السماح ببدء تشغيلها.

يمكنك تحديد واحدة من الطرق التالية لإنشاء فئات التطبيق:

- **فئة ذات محتوى مضاف يدويًا**. يمكنك يدويًا إضافة هذه الفئة باستخدام الشروط التالية:
  - بيانات تعريف الملف. يضيف Kaspersky Security Center كل الملفات القابلة للتنفيذ مصحوبة بالبيانات الوصفية المحددة إلى فئة التطبيق.
  - رمز تجزئة الملف. يضيف Kaspersky Security Center كل الملفات القابلة للتنفيذ مع التجزئة المحددة إلى فئة التطبيق.

> يستثني استخدام هذا الشرط القدرة على تثبيت التحديثات تلقائيًا لأن الإصدارات المختلفة من الملفات ستتضمن تجزئة مختلفة.

  - شهادة الملف. يضيف Kaspersky Security Center كل الملفات القابلة للتنفيذ مع الشهادة المحددة إلى فئة التطبيق.
  - فئة KL. يضيف Kaspersky Security Center كل التطبيقات الموجودة في فئة KL المحددة إلى فئة التطبيق.
  - مجلد التطبيق. يضيف Kaspersky Security Center الملفات القابلة للتنفيذ من هذا المجلد إلى الفئة المخصصة.

> قد يكون استخدام مجلد التطبيق غير آمن لأن أي تطبيق من المجلد المحدد سيتم السماح ببدء تشغيله. ويوصى بتطبيق القواعد التي تستخدم فئات التطبيق مع حالة مجلد التطبيق فقط للمستخدمين الذين يجب السماح لهم بالتثبيت التلقائي للتحديثات.

- **فئة تحتوي على ملفات تنفيذية من مجلد محدد**. يمكنك تحديد مجلد سيتم تعيين الملفات القابلة للتنفيذ منه تلقائيًا إلى فئة التطبيق التي تم إنشاؤها.
- **فئة تتضمن ملفات تنفيذية من الأجهزة المحددة**. يمكنك تحديد كمبيوتر سيتم تعيين كل الملفات القابلة للتنفيذ له تلقائيًا إلى فئة التطبيق التي تم إنشاؤها.

> عند استخدام طريقة إنشاء فئات التطبيق هذه، يستلم Kaspersky Security Center معلومات حول التطبيقات على الكمبيوتر من المجلد **الملفات القابلة للتنفيذ**.

2. تحديد وضع قائمة السماح لمكون التحكم في التطبيقات.

3. إنشاء قواعد التحكم في التطبيقات باستخدام فئات التطبيق التي تم إنشاؤها.

يتم تحديد القاعدة **صورة ذهبية** والقاعدة **برامج التحديث الموثوقة** مبدئيًا لوضع قائمة السماح. تتوافق قواعد التحكم في التطبيقات هذه مع فئات KL. تتضمن فئة KL "صورة ذهبية" برامج تضمن التشغيل العادي لنظام التشغيل. تتضمن فئة KL "برامج التحديث الموثوقة" برامج تحديث لبائعي البرامج الأكثر شهرة. كما لا يمكنك حذف تلك القواعد. ولا يمكن تحرير إعدادات هذه القواعد. بشكل افتراضي، يتم تمكين القاعدة **صورة ذهبية**، وتعطيل القاعدة **برامج التحديث الموثوقة**. يتم السماح لكل المستخدمين من بدء تشغيل التطبيقات التي تطابق شروط تشغيل تلك القواعد.

4. تحديد التطبيقات التي يجب السماح لها بالتثبيت التلقائي للتحديثات.

يمكنك السماح بالتثبيت التلقائي للتحديثات بواحدة من الطرق التالية:

- تحديد قائمة موسعة بالتطبيقات المسموح بها عن طريق السماح ببدء تشغيل كل التطبيقات التي تنتمي إلى أي فئة KL.
- تحديد قائمة موسعة بالتطبيقات المسموح بها عن طريق السماح ببدء تشغيل كل التطبيقات التي تم توقيعها بالشهادات.

للسماح ببدء تشغيل كل التطبيقات الموقعة بالشهادات، يمكنك إنشاء فئة بشرط مستند إلى شهادة يستخدم المعلمة **الموضوع** فقط مع القيمة *.

- فيما يتعلق بقواعد التحكم في التطبيقات، حدد المعلمة **برامج التحديث الموثوقة**. إذا تم تحديد خانة الاختيار هذه، فإن Kaspersky Endpoint Security سيعتبر التطبيقات التي تشملها القاعدة بمثابة برامج تحديث موثوقة. ويسمح Kaspersky Endpoint Security ببدء تشغيل التطبيقات التي تم تثبيتها أو تحديثها بواسطة التطبيقات التي تشملها القاعدة، شريطة عدم تطبيق قواعد المنع على هذه التطبيقات.

عند ترحيل إعدادات Kaspersky Endpoint Security، يتم ترحيل قائمة الملفات القابلة للتنفيذ التي تم إنشاؤها من جانب برامج التحديث الموثوقة كذلك.

- قم بإنشاء مجلد وضع بداخله الملفات القابلة للتنفيذ الخاصة بالتطبيقات التي ترغب في السماح بالتثبيت التلقائي للتحديثات الخاصة بها. ثم قم بإنشاء فئة التطبيق من خلال الشرط "مجلد التطبيق" وحدد المسار المؤدي إلى ذلك المجلد. ثم قم بإنشاء قاعدة سماح وحدد هذه الفئة.

قد يكون استخدام مجلد التطبيق غير آمن لأن أي تطبيق من المجلد المحدد سيتم السماح ببدء تشغيله. ويوصى بتطبيق القواعد التي تستخدم فئات التطبيق مع حالة مجلد التطبيق فقط للمستخدمين الذين يجب السماح لهم بالتثبيت التلقائي للتحديثات.

اختبار وضع قائمة السماح

للتأكد من عدم منع قواعد التحكم في التطبيقات للتطبيقات المطلوبة للعمل، يوصى بتمكين اختبار قواعد التحكم في التطبيقات وتحليل عملياتها بعد إنشاء القواعد الجديدة. عند تمكين الاختبار، لن يمنع Kaspersky Endpoint Security التطبيقات الممنوع بدء تشغيلها بواسطة قواعد التحكم في التطبيقات، ولكن سيرسل إخطارات حول بدء تشغيلها إلى خادم الإدارة.

عند اختبار وضع قائمة السماح، يوصى بتنفيذ الإجراءات التالية:

1. تحديد فترة الاختبار (تتراوح من عدة أيام إلى شهرين).

2. تمكين اختبار قواعد التحكم في التطبيقات.

3. افحص الأحداث الناتجة عن اختبار تشغيل التحكم في التطبيقات والتقارير حول التطبيقات المحجوبة في وضع الاختبار لتحليل نتائج الاختبار.

4. بناءً على نتائج التحليل، قم بإجراء تغييرات على إعدادات وضع قائمة السماح.

على وجه الخصوص بناءً على نتائج الاختبار، يمكنك إضافة الملفات القابلة للتنفيذ متعلقة بأحداث إلى فئة تطبيق.

دعم وضع قائمة السماح

بعد تحديد إجراء منع للتحكم في التطبيقات، يوصى بمواصلة دعم وضع قائمة السماح عن طريق تنفيذ الإجراءات التالية:

- فحص الأحداث الناتجة عن تشغيل التحكم في التطبيقات والتقارير حول مرات التشغيل الممنوعة لتحليل فعالية التحكم في التطبيقات.
- تحليل طلبات المستخدمين للوصول إلى التطبيقات.
- حلل الملفات القابلة للتنفيذ غير المألوفة بالتحقق من سمعتها في Kaspersky Security Network.
- قبل تثبيت التحديثات لنظام التشغيل أو البرامج، قم بتثبيت هذه التحديثات في مجموعة اختبار من أجهزة الكمبيوتر لمعرفة كيف سيتم معالجتها بواسطة قواعد التحكم في التطبيقات.
- أضف التطبيقات اللازمة إلى الفئات المستخدمة في قواعد التحكم في التطبيقات.

مراقبة منافذ الشبكة

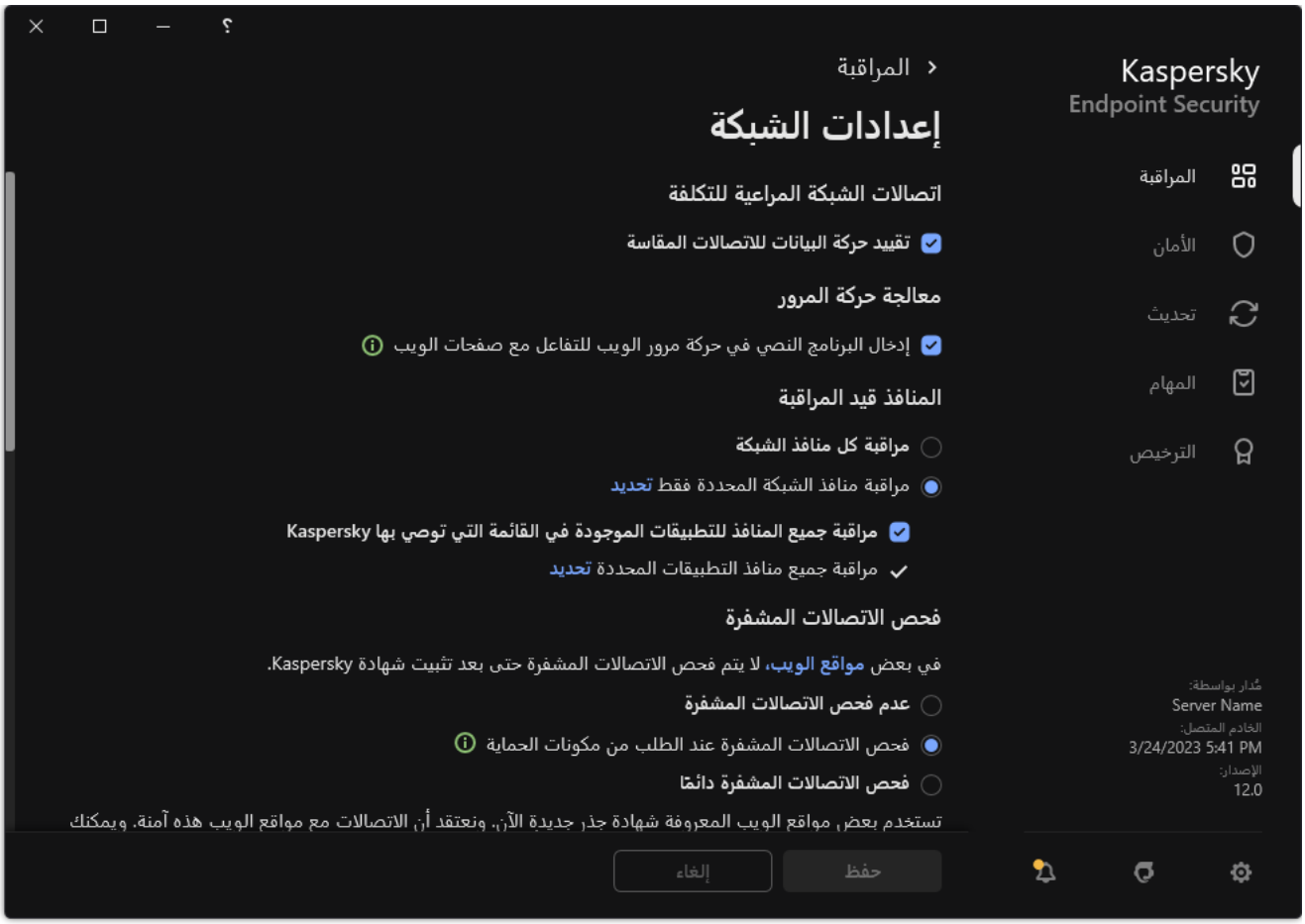
أثناء تشغيل برنامج Kaspersky Endpoint Security، تراقب مكونات التحكم في الويب، والحماية من تهديدات البريد، والحماية من تهديدات الويب تدفقات البيانات التي يتم إرسالها عبر بروتوكولات محددة والتي تمر عبر منافذ TCP وUDP مفتوحة محددة على كمبيوتر المستخدم. على سبيل المثال، يحلل مكون الحماية من تهديدات البريد المعلومات التي يتم إرسالها عبر SMTP، بينما يحلل مكون الحماية من تهديدات الويب المعلومات التي يتم إرسالها عبر HTTP وFTP.

يقوم Kaspersky Endpoint Security بتقسيم منافذ TCP وUDP الخاصة بكمبيوتر المستخدم إلى مجموعات متعددة، وفقًا لاحتمالية تكوينها. تم حجز بعض منافذ الشبكة للخدمات القابلة للاختراق. أنت مُوصى بمراقبة هذه المنافذ بعناية أكبر لأنه توجد احتمالية أكبر لاستهدافها من قِبل هجوم شبكة اتصال. إذا كنت تستخدم خدمات غير قياسية تعتمد على منافذ شبكة غير قياسية، فإن منافذ الشبكة هذه قد تكون مستهدفة أيضًا من قبل كمبيوتر مهاجم. يمكنك تحديد قائمة بمنافذ الشبكة وقائمة بالتطبيقات التي تتطلب الوصول إلى الشبكة. وبعد ذلك تحصل هذه المنافذ والتطبيقات على اهتمام خاص من مكوني الحماية من تهديدات البريد والحماية من تهديدات الويب أثناء مراقبة حركة المرور على شبكة الاتصال.

تمكين مراقبة جميع منافذ الشبكة

لتمكين مراقبة جميع منافذ الشبكة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.



إعدادات مراقبة منافذ الشبكة

3. في القسم **المنافذ قيد المراقبة**، حدد **مراقبة كل منافذ الشبكة**.

4. احفظ تغييراتك.

إنشاء قائمة بمنافذ الشبكة المراقبة

لإنشاء قائمة بمنافذ الشبكة المراقبة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.

3. في القسم **المنافذ قيد المراقبة**، حدد **مراقبة منافذ الشبكة المحددة فقط**.

4. انقر على **تحديد**.

يؤدي هذا إلى فتح قائمة تتضمن منافذ الشبكة التي تُستخدم عادة لإرسال البريد الإلكتروني وحركة شبكة الاتصال. هذه القائمة من منافذ الشبكة مضمنة في حزمة برنامج Kaspersky Endpoint Security.

5. استخدم مفتاح التبديل في عمود **الحالة** لتمكين أو تعطيل مراقبة منفذ شبكة الاتصال.

6. إذا لم يظهر منفذ شبكة في قائمة منافذ الشبكة، فيجب إضافته بإجراء ما يلي:

a. انقر على **إضافة**.

b. في النافذة التي تفتح، أدخل رقم منفذ شبكة الاتصال ووصفًا موجزًا.

c. قم بتعيين الحالة على **فعال** أو **غير فعال** لمراقبة منفذ شبكة الاتصال.

7. احفظ تغييراتك.

عند عمل بروتوكول FTP في الوضع الخامل، يمكن إجراء الاتصال عبر منفذ شبكة عشوائي، والذي تتم إضافته إلى قائمة منافذ الشبكة المُرَاقَبة. لحماية هذه الاتصالات، يرجى تمكين مراقبة كل منافذ شبكة الاتصال' أو تكوين التحكم في منافذ شبكة الاتصال للتطبيقات التي تنشئ اتصالات FTP.

إنشاء قائمة بالتطبيقات التي يتم مراقبة كافة منافذ الشبكة من أجلها

يمكنك إنشاء قائمة بالتطبيقات التي يقوم برنامج Kaspersky Endpoint Security بمراقبة جميع منافذ الشبكة الخاصة بها.

ونوصي بتضمين التطبيقات التي تستلم البيانات أو ترسلها عبر بروتوكول FTP في قائمة التطبيقات التي يقوم برنامج Kaspersky Endpoint Security بمراقبة جميع منافذ الشبكة الخاصة بها.

لإنشاء قائمة بالتطبيقات التي تتم مراقبة جميع منافذ الشبكة الخاصة بها:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات الشبكة**.

3. في القسم **المنافذ قيد المراقبة**، حدد **مراقبة منافذ الشبكة المحددة فقط**.

4. حدد خانة الاختيار **مراقبة جميع المنافذ للتطبيقات الموجودة في القائمة التي توصي بها Kaspersky**.

إذا تم تحديد خانة الاختيار هذه، فإن Kaspersky Endpoint Security يراقب جميع المنافذ المخصصة للتطبيقات التالية:

- Adobe Acrobat Reader.
- Apple Application Support (دعم تطبيق Apple).
- Google Chrome.
- Microsoft Edge.
- Mozilla Firefox.
- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.
- Mail.ru Agent.
- مستعرض Yandex.

5. حدد خانة الاختيار **مراقبة جميع منافذ التطبيقات المحددة**.

6. انقر على **تحديد**.
يؤدي ذلك إلى فتح قائمة بالتطبيقات التي يراقب Kaspersky Endpoint Security منافذ الشبكة الخاصة بها.

7. استخدم مفتاح التبديل في عمود **الحالة** لتمكين أو تعطيل مراقبة منفذ شبكة الاتصال.

8. إذا لم يكن التطبيق مضمنًا في قائمة التطبيقات، فقم بإضافته كالتالي:

a. انقر على **إضافة**.

b. في النافذة التي تفتح، أدخل المسار إلى الملف القابل للتنفيذ الخاص بالتطبيق ووصفًا موجزًا.

c. قم بتعيين الحالة على **فعال** أو **غير فعال** لمراقبة منافذ شبكة الاتصال.

9. احفظ تغييراتك.

تصدير واستيراد قوائم المنافذ قيد المراقبة

يستخدم Kaspersky Endpoint Security القوائم التالية لمراقبة منافذ شبكة الاتصال: قائمة منافذ شبكة الاتصال وقائمة التطبيقات التي تتم مراقبة منافذها بواسطة Kaspersky Endpoint Security. يمكنك تصدير قوائم المنافذ قيد المراقبة إلى ملف XML. ثم يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من المنافذ بالوصف نفسه. يمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قوائم المنافذ قيد المراقبة أو لترحيل القوائم إلى خادم مختلف.

كيفية تصدير واستيراد قوائم المنافذ قيد المراقبة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.

5. في القسم **المنافذ قيد المراقبة**، حدد **مراقبة منافذ الشبكة المحددة فقط**.

6. انقر على **الإعدادات**.

تفتح النافذة **منافذ شبكة الاتصال**. تعرض النافذة **منافذ شبكة الاتصال** قائمة بمنافذ الشبكة التي يتم استخدامها بشكل طبيعي في إرسال البريد الإلكتروني وحركة مرور الشبكة. هذه القائمة من منافذ الشبكة مضمنة في حزمة برنامج Kaspersky Endpoint Security.

7. لتصدير قائمة منافذ شبكة الاتصال:

a. في قائمة منافذ شبكة الاتصال، حدد المنافذ التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

إذا لم تحدد أي منفذ، فسيقوم Kaspersky Endpoint Security بتصدير كل المنافذ.

b. انقر على **تصدير**.

c. في النافذة التي تفتح، أدخل اسم ملف XML الذي تريد تصدير قائمة منافذ شبكة الاتصال إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة منافذ الشبكة بالكامل إلى ملف XML.

8. لتصدير قائمة التطبيقات التي تتم مراقبة منافذها بواسطة Kaspersky Endpoint Security:

a. حدد خانة الاختيار **مراقبة جميع منافذ التطبيقات المحددة**.

b. في قائمة التطبيقات، حدد التطبيقات التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

إذا لم تحدد أي تطبيق، فسيقوم Kaspersky Endpoint Security بتصدير كل التطبيقات.

c. انقر على **تصدير**.

d. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة التطبيقات إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.

e. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة التطبيقات بالكامل إلى ملف XML.

9. لاستيراد قائمة منافذ شبكة الاتصال:

a. في قائمة منافذ شبكة الاتصال انقر فوق الزر **استيراد**.

في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة منافذ الشبكة منه.

b. افتح الملف.

إذا كان جهاز الكمبيوتر يحتوي بالفعل على قائمة بمنافذ شبكة الاتصال، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

10. لاستيراد قائمة التطبيقات التي تتم مراقبة منافذها بواسطة Kaspersky Endpoint Security:

a. في قائمة التطبيقات، انقر فوق الزر **استيراد**.

في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة التطبيقات منه.

b. افتح الملف.

إذا كان جهاز الكمبيوتر يحتوي بالفعل على قائمة تطبيقات، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

11. احفظ تغييراتك.

كيفية تصدير / استيراد قوائم المنافذ قيد المراقبة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Network Settings**.

5. لتصدير قائمة منافذ شبكة الاتصال:

a. في القسم **Monitored ports**، حدد **Monitor selected network ports only**.

b. انقر فوق الرابط **selected N ports**.
تفتح النافذة **Network ports**. تعرض النافذة **Network ports** قائمة بمنافذ الشبكة التي يتم استخدامها بشكل طبيعي في إرسال البريد الإلكتروني وحركة مرور الشبكة. هذه القائمة من منافذ الشبكة مضمنة في حزمة برنامج Kaspersky Endpoint Security.

c. في قائمة منافذ شبكة الاتصال، حدد المنافذ التي تريد تصديرها.

d. انقر على **Export**.

e. في النافذة التي تفتح، أدخل اسم ملف XML الذي تريد تصدير قائمة منافذ شبكة الاتصال إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

f. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة منافذ الشبكة بالكامل إلى ملف XML.

6. لتصدير قائمة التطبيقات التي تتم مراقبة منافذها بواسطة Kaspersky Endpoint Security:

a. في القسم **Monitored ports**، حدد خانة الاختيار **Monitor all ports for specified applications**.

b. انقر فوق الرابط **selected N applications**.

c. في قائمة التطبيقات، حدد التطبيقات التي تريد تصديرها.

d. انقر على **Export**.

e. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة التطبيقات إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.

f. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة التطبيقات بالكامل إلى ملف XML.

7. لاستيراد قائمة منافذ شبكة الاتصال:

a. في قائمة منافذ شبكة الاتصال انقر فوق الزر **Import**.
في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة منافذ الشبكة منه.

b. افتح الملف.
إذا كان جهاز الكمبيوتر يحتوي بالفعل على قائمة بمنافذ شبكة الاتصال، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. لاستيراد قائمة التطبيقات التي تتم مراقبة منافذها بواسطة Kaspersky Endpoint Security:

a. في قائمة التطبيقات، انقر فوق الزر **Import**.

في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة التطبيقات منه.

b. افتح الملف.

إذا كان جهاز الكمبيوتر يحتوي بالفعل على قائمة تطبيقات، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

9. احفظ تغييراتك.

فحص السجل

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم. ولا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل.

بدءً من الإصدار 11.11.0 يتضمن Kaspersky Endpoint Security for Windows مكون فحص السجل. يراقب فحص السجل سلامة البيئة المحمية استنادًا إلى تحليل سجل أحداث Windows. وعندما يكتشف التطبيق علامات سلوك غير نمطي في النظام، فإنه يُبلغ المسؤول، لأن هذا السلوك قد يشير إلى محاولة هجوم إلكتروني.

يحلل Kaspersky Endpoint Security سجلات أحداث Windows ويكتشف الانتهاك وفقًا للقواعد. ويتضمن المكون predefined rules. ويتم تشغيل القواعد المحددة مسبقًا من خلال التحليل المساعد على الاكتشاف. ويمكنك أيضا إضافة القواعد الخاصة بك (قواعد مخصصة). وعند تشغيل قاعدة، ينشئ التطبيق حدثًا بحالة Critical (انظر الشكل أدناه).

إذا كنت ترغب في استخدام فحص السجل، تأكد من تكوين سياسة التدقيق وأن النظام يسجل الأحداث ذات الصلة (للحصول على التفاصيل، يرجى الرجوع إلى موقع ويب الدعم الفني من Microsoft).

إخطار فحص السجل

تكوين القواعد المحددة مسبقًا

تتضمن القواعد المحددة مسبقًا قوالب للنشاط غير الطبيعي على الكمبيوتر المحمي. ويمكن أن يشير النشاط غير الطبيعي إلى محاولة هجوم. ويتم تشغيل القواعد المحددة مسبقًا من خلال التحليل المساعد على الاكتشاف. تتوفر سبع قواعد محددة مسبقًا لفحص السجل. ويمكنك تمكين أو تعطيل هذه القواعد. ولا يمكن حذف القواعد المحددة مسبقًا.

يمكنك تكوين معايير بدء تشغيل القواعد التي تراقب الأحداث للعمليات التالية:

- اكتشاف هجوم فك الشفرة لكلمة المرور
- اكتشاف تسجيل الدخول إلى الشبكة

[كيفية تكوين القواعد المحددة مسبقًا في وحدة تحكم الإدارة (MMC)](#)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **فحص السجل**.

5. تأكد من تحديد خانة الاختيار **فحص السجل**.

6. في القسم **القواعد المحددة مسبقًا**، انقر على الزر **الإعدادات**.

7. حدد خانات الاختيار أو امسحها لتكوين القواعد المحددة مسبقًا:

- **توجد أنماط لهجوم محتمل باستخدام فك الشفرة في النظام**.
- **يوجد نشاط غير نمطي تم اكتشافه أثناء جلسة عمل تسجيل الدخول إلى الشبكة**.
- **توجد أنماط لإساءة استخدام محتملة لسجل أحداث Windows**.
- **تم اكتشاف إجراءات غير نمطية نيابة عن خدمة جديدة مثبتة**.
- **تم اكتشاف تسجيل دخول غير نمطي يستخدم بيانات اعتماد صريحة**.
- **توجد أنماط لهجوم Kerberos forged PAC (MS14-068) محتمل في النظام**.
- **تم اكتشاف تغييرات مريبة في مجموعة المسؤولين المضمنة ذات الامتيازات**.

8. إذا لزم الأمر، قم بتكوين القاعدة **توجد أنماط لهجوم محتمل باستخدام فك الشفرة في النظام**:

a. انقر فوق الزر **الإعدادات** تحت القاعدة.

b. في النافذة التي تفتح، حدد عدد المحاولات والفترة الزمنية التي يجب خلالها تنفيذ محاولات إدخال كلمة المرور حتى يتم تشغيل القاعدة.

c. انقر فوق **موافق**.

9. إذا حددت القاعدة **يوجد نشاط غير نمطي تم اكتشافه أثناء جلسة عمل تسجيل الدخول إلى الشبكة**، تحتاج إلى تكوين إعداداتها:

a. انقر فوق الزر **الإعدادات** تحت القاعدة.

b. في القسم **اكتشاف تسجيل الدخول إلى الشبكة**، حدد بداية الفاصل الزمني ونهايته.

يعتبر Kaspersky Endpoint Security محاولات تسجيل الدخول التي يتم إجراؤها خلال هذا الفاصل الزمني المحدد نشاطًا غير طبيعي.

بشكل افتراضي، لا يتم تعيين الفاصل الزمني ولا يراقب التطبيق محاولات تسجيل الدخول. ولكي يراقب التطبيق محاولات تسجيل الدخول بشكل مستمر، قم بتعيين الفاصل الزمني إلى 12:00 صباحًا – 11:59 مساءً. ويجب ألا تتطابق بداية الفاصل الزمني مع نهايته. وإذا كانت متطابقين، لا يراقب التطبيق محاولات تسجيل الدخول.

c. أنشئ قائمة بالمستخدمين الموثوق بهم وعناوين IP الموثوقة (IPv4 وIPv6).

لا يراقب Kaspersky Endpoint Security محاولات تسجيل الدخول لهؤلاء المستخدمين وأجهزة الكمبيوتر.

d. انقر فوق **موافق**.

10. احفظ تغييراتك.

[كيفية تكوين القواعد المحددة مسبقًا في Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Security Controls** ← **Log Inspection**.

5. تأكد أن مفتاح التبديل **Log Inspection** قيد التشغيل.

6. في القسم **Predefined rules** قم بتمكين او تعطيل القواعد المحددة مسبقًا باستخدام مفاتيح التبديل:

- **There are patterns of a possible brute-force attack in the system**.
- **There is an atypical activity detected during a network logon session**.
- **There are patterns of a possible Windows Event Log abuse**.
- **Atypical actions detected on behalf of a new service installed**.
- **Atypical logon that uses explicit credentials detected**.
- **There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system**.

a. **Suspicious changes detected in the privileged built-in Administrators group**.

7. إذا لزم الأمر، قم بتكوين القاعدة **There are patterns of a possible brute-force attack in the system**:

a. انقر فوق **Settings** تحت القاعدة.

b. في النافذة التي تفتح، حدد عدد المحاولات والفترة الزمنية التي يجب خلالها تنفيذ محاولات إدخال كلمة المرور حتى يتم تشغيل القاعدة.

c. انقر على **OK**.

8. إذا حددت القاعدة **There is an atypical activity detected during a network logon session**، تحتاج إلى تكوين إعداداتها:

a. انقر فوق **Settings** تحت القاعدة.

b. في القسم **Network logon detection**، حدد بداية الفاصل الزمني ونهايته.
يعتبر Kaspersky Endpoint Security محاولات تسجيل الدخول التي يتم إجراؤها خلال هذا الفاصل الزمني المحدد نشاطًا غير طبيعي.
بشكل افتراضي، لا يتم تعيين الفاصل الزمني ولا يراقب التطبيق محاولات تسجيل الدخول. ولكي يراقب التطبيق محاولات تسجيل الدخول بشكل مستمر، قم بتعيين الفاصل الزمني إلى 12:00 صباحًا – 11:59 مساءً. ويجب ألا تتطابق بداية الفاصل الزمني مع نهايته. وإذا كانت متطابقين، لا يراقب التطبيق محاولات تسجيل الدخول.

c. في القسم **Exclusions** أضف مستخدمين موثوقين وعناوين IP موثوقة (IPv4 وIPv6).
لا يراقب Kaspersky Endpoint Security محاولات تسجيل الدخول لهؤلاء المستخدمين وأجهزة الكمبيوتر.

d. انقر على **OK**.

9. احفظ تغييراتك.

كيفية تكوين القواعد المحددة مسبقًا في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **فحص السجل**.
3. تأكد أن مفتاح التبديل **فحص السجل** قيد التشغيل.
4. في القسم **القواعد المحددة مسبقًا**، انقر على الزر **تكوين**.
5. حدد خانات الاختيار أو امسحها لتكوين القواعد المحددة مسبقًا:
   - **توجد أنماط لهجوم محتمل باستخدام فك الشفرة في النظام**.
   - **يوجد نشاط غير نمطي تم اكتشافه أثناء جلسة عمل تسجيل الدخول إلى الشبكة**.
   - **توجد أنماط لإساءة استخدام محتملة لسجل أحداث Windows**.
   - **تم اكتشاف إجراءات غير نمطية نيابة عن خدمة جديدة مثبتة**.
   - **تم اكتشاف تسجيل دخول غير نمطي يستخدم بيانات اعتماد صريحة**.
   - **توجد أنماط لهجوم Kerberos forged PAC (MS14-068) محتمل في النظام**.
   a. **تم اكتشاف تغييرات مريبة في مجموعة المسؤولين المضمنة ذات الامتيازات**.
6. إذا لزم الأمر، قم بتكوين القاعدة **توجد أنماط لهجوم محتمل باستخدام فك الشفرة في النظام**:
   a. انقر فوق **الإعدادات** تحت القاعدة.
   b. في النافذة التي تفتح، حدد عدد المحاولات والفترة الزمنية التي يجب خلالها تنفيذ محاولات إدخال كلمة المرور حتى يتم تشغيل القاعدة.
7. إذا حددت القاعدة **يوجد نشاط غير نمطي تم اكتشافه أثناء جلسة عمل تسجيل الدخول إلى الشبكة**، تحتاج إلى تكوين إعداداتها:
   a. انقر فوق **الإعدادات** تحت القاعدة.
   b. في القسم **اكتشاف تسجيل الدخول إلى الشبكة**، حدد بداية الفاصل الزمني ونهايته.
   يعتبر Kaspersky Endpoint Security محاولات تسجيل الدخول التي يتم إجراؤها خلال هذا الفاصل الزمني المحدد نشاطًا غير طبيعي.
   بشكل افتراضي، لا يتم تعيين الفاصل الزمني ولا يراقب التطبيق محاولات تسجيل الدخول. ولكي يراقب التطبيق محاولات تسجيل الدخول بشكل مستمر، قم بتعيين الفاصل الزمني إلى 12:00 صباحًا – 11:59 مساءً. ويجب ألا تتطابق بداية الفاصل الزمني مع نهايته. وإذا كانت متطابقين، لا يراقب التطبيق محاولات تسجيل الدخول.
   c. في القسم **الاستثناءات** أضف مستخدمين موثوقين وعناوين IP موثوقة (IPv4 وIPv6).
   لا يراقب Kaspersky Endpoint Security محاولات تسجيل الدخول لهؤلاء المستخدمين وأجهزة الكمبيوتر.
8. احفظ تغييراتك.

نتيجة لذلك، عند تشغيل القاعدة، ينشئ Kaspersky Endpoint Security حدث Critical.

إضافة قواعد مخصصة

يمكنك تعيين معايير تشغيل قاعدة فحص السجل الخاصة بك. ولفعل ذلك، يجب عليك إدخال معرف الحدث وتحديد مصدر حدث. ويمكنك البحث عن معرف الحدث على موقع ويب الدعم الفني من Microsoft. ويمكنك تحديد مصدر حدث من بين السجلات القياسية: Application أو Security أو System. ويمكنك أيضًا تحديد سجل تطبيق جهة خارجية. ويمكنك معرفة اسم سجل تطبيق الجهة الخارجية باستخدام أداة عارض الأحداث. ويتم الاحتفاظ بسجلات تطبيقات الجهة الخارجية في مجلد "Application and Services Logs" (على سبيل المثال، سجل Windows PowerShell).

لا يتحقق التطبيق مما إذا كان السجل المحدد موجودًا بالفعل في سجل أحداث Windows. وإذا كان هناك خطأ في اسم السجل، فلن يراقب التطبيق الأحداث من ذلك السجل.

تتضمن قائمة القواعد المخصصة بالفعل ثلاث قواعد أنشأها خبراء Kaspersky.

كيفية إضافة قواعد مخصصة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **ضوابط الأمان** ← **فحص السجل**.
5. تأكد من تحديد خانة الاختيار **فحص السجل**.
6. في القسم **قواعد مخصصة**، انقر على الزر **الإعدادات**.
7. في النافذة التي تفتح، حدد خانات الاختيار بجوار القواعد المخصصة التي تريد تمكينها.
8. إذا لزم الأمر، انقر فوق **إضافة** لإنشاء القواعد المخصصة الخاصة بك.
9. يفتح نافذة هذا وفي تلك النافذة، كوّن القاعدة المخصصة:
   - **اسم القاعدة**.
   - **اسم السجل**. سجلات أحداث Windows. تتاح السجلات التالية: Application أو Security أو System.
   - **المصدر**. سجلات تطبيق الجهة الخارجية. ويمكنك معرفة اسم سجل تطبيق الجهة الخارجية باستخدام أداة عارض الأحداث. ويتم الاحتفاظ بسجلات تطبيقات الجهة الخارجية في مجلد "Application and Services Logs" (على سبيل المثال، سجل Windows PowerShell).
   - **معرفات الحدث**. معرفات الحدث في سجل أحداث Windows. يمكنك البحث عن معرف الحدث في المستندات الفنية من Microsoft.
10. احفظ تغييراتك.

كيفية إضافة قاعدة مخصصة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Security Controls** ← **Log Inspection**.

5. تأكد أن مفتاح التبديل **Log Inspection** قيد التشغيل.

6. في القسم **Custom rules**، حدد القواعد المخصصة التي تريد تمكينها.

7. إذا لزم الأمر، انقر فوق **Add** لإنشاء القواعد المخصصة الخاصة بك.

8. يفتح نافذة هذا وفي تلك النافذة، كوّن القاعدة المخصصة:

- **Rule name**.
- **Windows Event Log name**. سجلات أحداث Windows. تتاح السجلات التالية: Application أو Security أو System.
- **Source**. سجلات تطبيق الجهة الخارجية. ويمكنك معرفة اسم سجل تطبيق الجهة الخارجية باستخدام أداة عارض الأحداث. ويتم الاحتفاظ بسجلات تطبيقات الجهة الخارجية في مجلد "Application and Services Logs" (على سبيل المثال، سجل Windows PowerShell).
- **Windows Event Log identifier**. معرفات الحدث في سجل أحداث Windows. يمكنك البحث عن معرف الحدث في المستندات الفنية من Microsoft.

9. احفظ تغييراتك.

كيفية إضافة قاعدة مخصصة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **فحص السجل**.

3. تأكد أن مفتاح التبديل **فحص السجل** قيد التشغيل.

4. في القسم **قواعد مخصصة**، انقر على الزر **تكوين**.

5. في النافذة التي تفتح، حدد خانات الاختيار بجوار القواعد المخصصة التي تريد تمكينها.

6. إذا لزم الأمر، انقر فوق **إضافة** لإنشاء القواعد المخصصة الخاصة بك.

7. يفتح نافذة هذا وفي تلك النافذة، كوّن القاعدة المخصصة:

- **اسم القاعدة**.
- **اسم السجل**. سجلات أحداث Windows. تتاح السجلات التالية: Application أو Security أو System.
- **المصدر**. سجلات تطبيق الجهة الخارجية. ويمكنك معرفة اسم سجل تطبيق الجهة الخارجية باستخدام أداة عارض الأحداث. ويتم الاحتفاظ بسجلات تطبيقات الجهة الخارجية في مجلد "Application and Services Logs" (على سبيل المثال، سجل Windows PowerShell).
- **معرف الحدث**. معرفات الحدث في سجل أحداث Windows. يمكنك البحث عن معرف الحدث في المستندات الفنية من Microsoft.

8. احفظ تغييراتك.

نتيجة لذلك، عند تشغيل القاعدة، ينشئ Kaspersky Endpoint Security حدث Critical.

مراقبة سلامة الملف

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم. ولا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل.

يعمل مكون مراقبة سلامة الملف فقط على الخوادم التي تحتوي على نظام ملفات NTFS أو ReFS.

بدءً من الإصدار 11.11.0 يتضمن Kaspersky Endpoint Security for Windows مكون مراقبة سلامة الملف. ويكتشف مكون مراقبة سلامة الملف التغييرات في الكائنات (الملفات والمجلدات) في منطقة مراقبة معينة. وقد تشير هذه التغييرات إلى حدوث خرق لأمان الكمبيوتر. وعند اكتشاف تغييرات الكائن، يُبلغ التطبيق المسؤول.

لاستخدام مكون مراقبة سلامة الملف تحتاج إلى تكوين نطاق المكون، أي تحديد الكائنات التي يجب أن يراقب المكون حالتها.

يمكنك عرض معلومات حول نتائج عملية مراقبة سلامة الملف في Kaspersky Security Center وفي واجهة Kaspersky Endpoint Security for Windows.

تحرير نطاق المراقبة

لا يمكن أن يعمل مكون مراقبة سلامة الملف بدون نطاق مراقبة محدد. ويعني هذا أنه يجب عليك تحديد المسارات إلى الملفات والمجلدات التي يتحكم في تغييراتها مراقبة سلامة الملف. ونوصي بإضافة الكائنات التي نادرًا ما يتم تعديلها أو الكائنات التي يمتلك المسؤول فقط حق الوصول إليها. وسيؤدي هذا إلى تقليل عدد أحداث مراقبة سلامة الملف.

لتقليل عدد الأحداث، يمكنك أيضًا إضافة استثناءات إلى قواعد المراقبة. وتتمتع إدخالات الاستثناء بأولوية أعلى من إدخالات نطاق المراقبة. على سبيل المثال، تستخدم المؤسسة تطبيقًا تريد مراقبة ملفاته للتأكد من سلامتها. ولفعل ذلك، تحتاج إلى إضافة المسار إلى المجلد الذي يحتوي على التطبيق (على سبيل المثال، `C:\Users\Testadmin\Desktop\Utilities`). ويمكنك استثناء ملفات السجل من قاعدة المراقبة لأن هذه الملفات لا تؤثر على أمان النظام. علاوة على ذلك، يقوم التطبيق بتعديل ملفات السجل باستمرار، مما ينتج عنه عددًا كبيرًا من الأحداث المماثلة. ولتجنب ذلك، أضف ملفات السجل إلى الاستثناءات (على سبيل المثال، `C:\Users\Testadmin\Desktop\Utilities\*.log`).

كيفية إنشاء نطاق المراقبة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **مراقبة سلامة الملف**.

5. تأكد من تحديد خانة الاختيار **مراقبة سلامة الملف**.

6. في القسم **قواعد المراقبة**، انقر على الزر **إضافة**.

7. يفتح نافذة هذا وفي تلك النافذة، كوّن قاعدة المراقبة:

- **اسم القاعدة**. أدخل اسم القاعدة، على سبيل المثال ، مراقبة التطبيق أ.
- **مستوى خطورة الحدث**. حدد مستوى خطورة الحدث الذي سيسجله مكون مراقبة سلامة الملف: معلوماتي، تحذير، حرج.
- **نطاق المراقبة**. أدخل المسار إلى الملف أو المجلد.

عند تكوين نطاق المراقبة، تأكد أن المسار إلى المجلد أو الملف يبدأ بحرف محرك أقراص أو متغير بيئة النظام. ولا يدعم التطبيق متغيرات البيئة بواسطة المستخدم. وفي حالة تحديد المسار إلى المجلد أو الملف بشكل غير صحيح، فلن يضيف Kaspersky Endpoint Security نطاق المراقبة المحدد.

استخدم الأقنعة:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص C:، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع `C:\**\*.txt` مستوى تداخل واحد على الأقل. القناع هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

- **الاستثناءات**. أدخل المسار إلى الملف أو المجلد. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع. وتتمتع إدخالات الاستثناء بأولوية أعلى من إدخالات نطاق المراقبة.

8. انقر فوق **موافق**.

تمت إضافة قاعدة جديدة إلى قائمة قواعد المراقبة. ويمكنك تعطيل قاعدة المراقبة دون إزالتها من قائمة القواعد. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

9. احفظ تغييراتك.

[كيفية تحرير نطاق مراقبة في Web Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Security Controls** ← **File Integrity Monitor**.

5. تأكد أن مفتاح التبديل **File Integrity Monitor** قيد التشغيل.

6. في القسم **Monitoring rules**، انقر على الزر **Add**.

7. يفتح نافذة هذا وفي تلك النافذة، كوّن قاعدة المراقبة:

- **Rule name**. أدخل اسم القاعدة، على سبيل المثال ، مراقبة التطبيق أ.
- **Event severity level**. حدد مستوى خطورة الحدث الذي سيسجله مكون مراقبة سلامة الملف: Warning ⚠، Informational ⓘ، Critical [!].
- **Monitoring scope**. أدخل المسار إلى الملف أو المجلد.

عند تكوين نطاق المراقبة، تأكد أن المسار إلى المجلد أو الملف يبدأ بحرف محرك أقراص أو متغير بيئة النظام. ولا يدعم التطبيق متغيرات البيئة بواسطة المستخدم. وفي حالة تحديد المسار إلى المجلد أو الملف بشكل غير صحيح، فلن يضيف Kaspersky Endpoint Security نطاق المراقبة المحدد.

استخدم الأقنعة:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص C:، ولكنه ليس موجودًا في المجلدات الفرعية.
- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.
- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.
- **Exclusions**. أدخل المسار إلى الملف أو المجلد. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع. وتتمتع إدخالات الاستثناء بأولوية أعلى من إدخالات نطاق المراقبة.

8. انقر على **OK**.

تمت إضافة قاعدة جديدة إلى قائمة قواعد المراقبة. ويمكنك تعطيل قاعدة المراقبة دون إزالتها من قائمة القواعد. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.

9. احفظ تغييراتك.

كيفية تحرير نطاق مراقبة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة سلامة الملف**.

3. تأكد أن مفتاح التبديل **مراقبة سلامة الملف** قيد التشغيل.

4. في القسم **قواعد المراقبة** انقر على **تكوين القواعد**.

5. في القسم **قواعد المراقبة**، انقر على الزر **إضافة**.

6. يفتح نافذة هذا وفي تلك النافذة، كوّن قاعدة المراقبة:

- **اسم القاعدة**. أدخل اسم القاعدة، على سبيل المثال ، مراقبة التطبيق أ.
- **مستوى خطورة الحدث**. حدد مستوى خطورة الحدث الذي سيسجله مكون مراقبة سلامة الملف: معلوماتي ⓘ، تحذير ⚠، حرج ❗.
- **نطاق المراقبة**. أدخل المسار إلى الملف أو المجلد.

عند تكوين نطاق المراقبة، تأكد أن المسار إلى المجلد أو الملف يبدأ بحرف محرك أقراص أو متغير بيئة النظام. ولا يدعم التطبيق متغيرات البيئة بواسطة المستخدم. وفي حالة تحديد المسار إلى المجلد أو الملف بشكل غير صحيح، فلن يضيف Kaspersky Endpoint Security نطاق المراقبة المحدد.

استخدم الأقنعة:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص C:، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

- **الاستثناءات**. أدخل المسار إلى الملف أو المجلد. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع. وتتمتع إدخالات الاستثناء بأولوية أعلى من إدخالات نطاق المراقبة.

7. انقر على **موافق**.

تمت إضافة قاعدة جديدة إلى قائمة قواعد المراقبة. ويمكنك تعطيل قاعدة المراقبة دون إزالتها من قائمة القواعد. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.

8. احفظ تغييراتك.

عرض معلومات سلامة النظام

يتم عرض المعلومات حول نتائج عملية مراقبة سلامة الملف بالطرق التالية:

الأحداث في Kaspersky Security Center Console وفي واجهة Kaspersky Endpoint Security

يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center في حالة اكتشاف تغيير في الملفات. ويمكنك تكوين تحديد الحدث لعرض الأحداث من مكون مراقبة سلامة الملف. وللمزيد من التفاصيل حول إعدادات تحديد الحدث، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

توفر واجهة Kaspersky Endpoint Security تقريرًا منفصلاً عن مكون مراقبة سلامة الملف.

يحتوي Kaspersky Endpoint Security على أدوات تجميع الأحداث لتقليل عدد أحداث مراقبة سلامة الملف. ويتيح Kaspersky Endpoint Security تجميع الأحداث في الحالات التالية:

- كثرة التغييرات المتكررة لكائن واحد (أكثر من خمس مرات في الدقيقة)
- كثرة التشغيل المتكرر لقاعدة مراقبة واحدة (أكثر من 10 مرات في الدقيقة)

نتيجة لذلك، ينشئ Kaspersky Endpoint Security أحداثًا منفصلة عن تعديلات الكائن حتى يتم تشغيل أدوات التجميع. وفي هذه المرحلة، يتيح Kaspersky Endpoint Security تجميع الأحداث وينشئ حدثًا مطابقًا. ينفذ Kaspersky Endpoint Security تجميع الأحداث لمدة 24 ساعة (فترة التجميع) أو حتى يتم إيقاف Kaspersky Endpoint Security. بعد إعادة تشغيل Kaspersky Endpoint Security أو بعد انتهاء فترة التجميع، يُنشئ التطبيق أحداثًا خاصة: الإبلاغ عن حدث غير نمطي لفترة التجميع والإبلاغ عن حدوث تغيير في الكائن لفترة التجميع. تحتوي هذه التقارير على معلومات عن بداية ونهاية فترة التجميع وعدد الأحداث المجمعة.

حالة أجهزة الكمبيوتر في Kaspersky Security Center Console

عندما تكون الأحداث في مستوى الخطورة حرج أو تحذير قد تم استلامها من مكون File Integrity Monitor، يقوم Kaspersky Security Center بتغيير حالة الكمبيوتر إلى حرج أو تحذير.

يجب تفعيل استلام حالة الكمبيوتر من تطبيق مُدار (حالة **الجهاز المحددة بواسطة التطبيق**) في Kaspersky Security Center في قوائم الشروط التي يجب الوفاء بها لتعيين حالة حرج أو تحذير للجهاز. ويتم تكوين شروط تعيين حالة لجهاز في نافذة الخصائص الخاصة بمجموعة الإدارة.

يتم عرض حالة الكمبيوتر وجميع أسباب تغييرات الحالة في قائمة الأجهزة الخاصة بمجموعة الإدارة. وللمزيد من التفاصيل حول حالات الكمبيوتر، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

التقارير في Kaspersky Security Center Console

يوفر Kaspersky Security Center نوعين من التقارير:

- أكثر 10 أجهزة يتم تشغيلها بشكل متكرر مزودة بقواعد مراقبة سلامة الملف/مراقبة نظام التكامل.
- أكثر 10 أجهزة يتم تشغيلها بشكل متكرر على الأجهزة المزودة بقواعد مراقبة سلامة الملف/مراقبة نظام التكامل.

الحماية بكلمة مرور

يمكن للعديد من المستخدمين ذوي مستويات المعرفة المختلفة بالكمبيوتر مشاركة جهاز كمبيوتر. إذا كان المستخدمون يتمتعون بإمكانية وصول غير مقيد إلى Kaspersky Endpoint Security وإعداداته، فقد ينخفض مستوى حماية الكمبيوتر الإجمالي. تتيح لك الحماية بكلمة المرور تقييد وصول المستخدمين إلى Kaspersky Endpoint Security طبقا للأذونات الممنوحة لهم (على سبيل المثال، إذن الخروج من التطبيق).

إذا كان المستخدم الذي بدأ جلسة عمل Windows (مستخدم الجلسة) لديه الإذن بتنفيذ الإجراء، فإن Kaspersky Endpoint Security لا يطلب اسم المستخدم وكلمة المرور أو كلمة المرور المؤقتة. يتلقى المستخدم الوصول إلى Kaspersky Endpoint Security وفقًا للأذونات الممنوحة.

إذا لم يكن لدى مستخدم الجلسة إذن للقيام بعمل ما، يمكن للمستخدم الحصول على حق الوصول إلى التطبيق بالطرق التالية:

- أدخل اسم المستخدم وكلمة المرور.

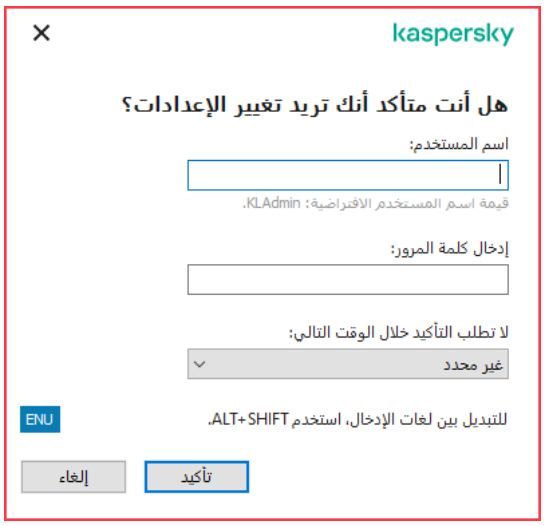
هذه الطريقة ملائمة للعمليات اليومية. لتنفيذ إجراء محمي بكلمة مرور، يجب إدخال بيانات اعتماد حساب المجال الخاصة بالمستخدم مع الإذن المطلوب. في هذه الحالة، يجب أن يكون جهاز الكمبيوتر في المجال. أما إذا لم يكن الكمبيوتر في المجال، يمكنك استخدام حساب KLAdmin.

- أدخل كلمة مرور مؤقتة.

هذه الطريقة ملائمة لمنح أذونات مؤقتة لتنفيذ الإجراءات المحظورة (على سبيل المثال، الخروج من التطبيق) للمستخدمين خارج شبكة الشركة. عند انتهاء صلاحية كلمة مرور مؤقتة أو انتهاء جلسة، سيعيد Kaspersky Endpoint Security الإعدادات الخاصة به إلى حالتها السابقة.

عندما يحاول المستخدم تنفيذ إجراء محمي بكلمة مرور، سيطالب Kaspersky Endpoint Security المستخدم باسم المستخدم وكلمة المرور أو كلمة المرور المؤقتة (انظر الشكل أدناه).

في نافذة إدخال كلمة المرور، يمكنك تبديل اللغات فقط بالضغط على **ALT+SHIFT**. ولا يؤدي استخدام اختصارات أخرى، حتى لو تم تكوينها في نظام التشغيل، للتبديل بين اللغات.



كلمة مرور الوصول إلى Kaspersky Endpoint Security يطالب

اسم المستخدم وكلمة المرور

للوصول إلى Kaspersky Endpoint Security، يجب عليك إدخال بيانات اعتماد حساب المجال الخاص بك. الحماية بكلمة المرور تدعم الحسابات التالية:

- **KLAdmin**. حساب المسؤول مع وصول غير مقيد إلى Kaspersky Endpoint Security. لحساب KLAdmin الحق في اتخاذ أي إجراء محمي بكلمة مرور. لا يمكن إبطال الأذونات الخاصة بحساب KLAdmin. عندما تقوم بتمكين الحماية بكلمة المرور، سيطالبك Kaspersky Endpoint Security بتعيين كلمة مرور لحساب KLAdmin.

- **مجموعة "الكل"**. مجموعة Windows مدمجة والتي تتضمن جميع المستخدمين داخل شبكة الشركة. يمكن للمستخدمين في المجموعة "الكل" الوصول إلى التطبيق طبقا للأذونات الممنوحة لهم.

- **مستخدمين أفراد أو مجموعات**. حسابات المستخدمين التي يمكنك تكوين أذونات فردية لها. على سبيل المثال، إذا تم حظر إجراء لمجموعة "الكل"، يمكنك السماح بهذا الإجراء لمستخدم فردي أو مجموعة.

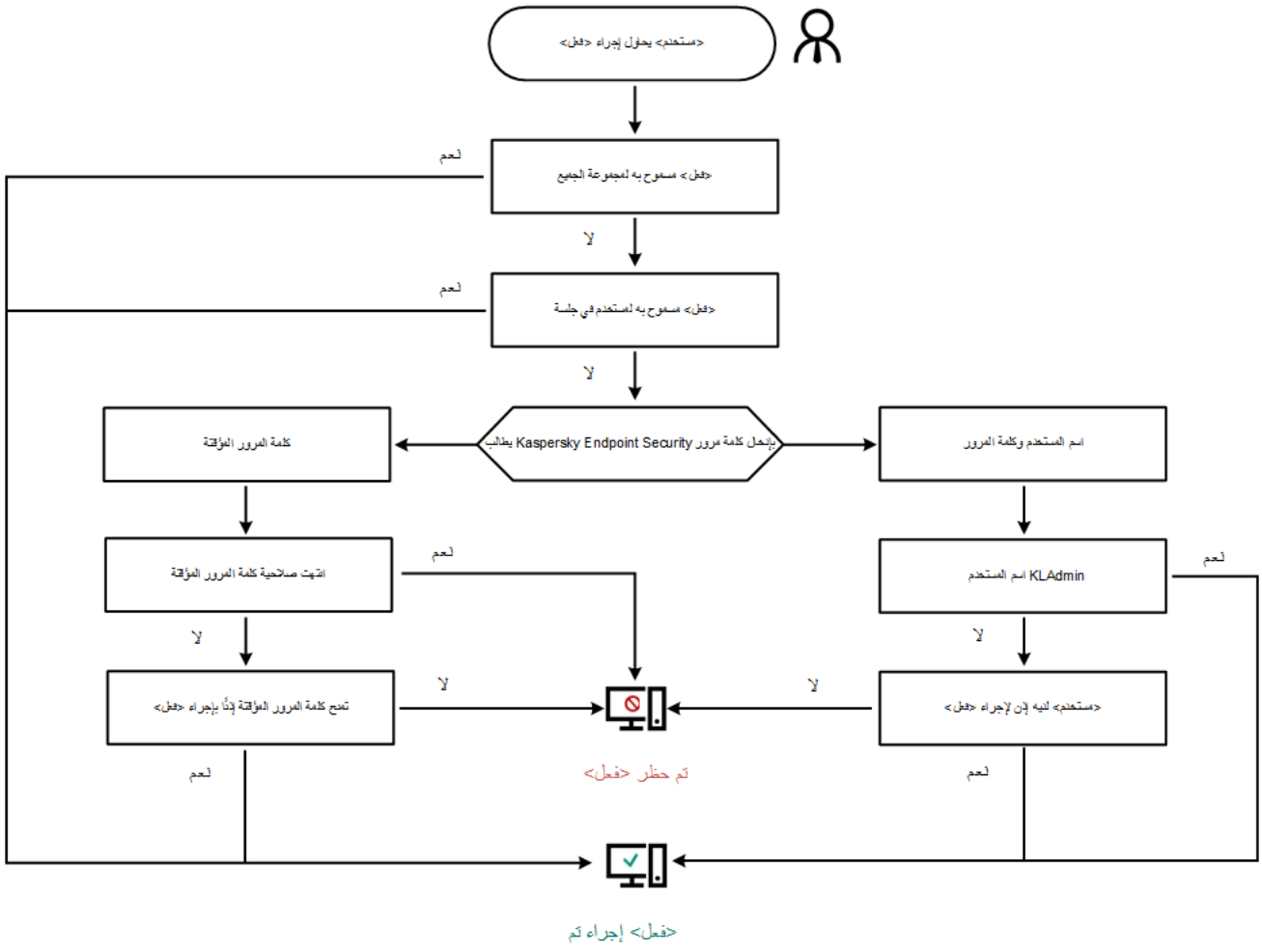
- **مستخدم جلسة**. حساب المستخدم الذي بدأ جلسة Windows. يمكنك التبديل إلى مستخدم جلسة آخر عندما تتم مطالبتك بكلمة مرور (خانة الاختيار **حفظ كلمة المرور للجلسة الحالية**). في هذه الحالة، يعتبر Kaspersky Endpoint Security المستخدم الذي تم إدخال بيانات اعتماد حسابه كمستخدم جلسة بدلا من المستخدم الذي بدأ جلسة Windows.

كلمة المرور المؤقتة

يمكن استخدام كلمة مرور مؤقتة لمنح وصول مؤقت إلى Kaspersky Endpoint Security لكمبيوتر فردي خارج شبكة الشركة. يقوم المسؤول بإنشاء كلمة مرور مؤقتة لكمبيوتر فردي في خصائص الكمبيوتر في Kaspersky Security Center. يختار المسؤول الإجراءات التي سيتم حمايتها بكلمة المرور المؤقتة، ويحدد فترة صلاحية كلمة المرور المؤقتة.

الحماية بكلمة المرور خوارزمية التشغيل

يقرر Kaspersky Endpoint Security إذا كان يجب السماح بإجراء محمي بكلمة مرور أو حظره استنادًا على الخوارزمية التالية (انظر الشكل أدناه).



الحماية بكلمة المرور خوارزمية التشغيل

تمكين الحماية بكلمة مرور

تتيح لك الحماية بكلمة المرور تقييد وصول المستخدمين إلى Kaspersky Endpoint Security طبقا للأذونات الممنوحة لهم (على سبيل المثال، إذن الخروج من التطبيق).

لتمكين الحماية بكلمة مرور:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الواجهة**.

3. استخدم مفتاح تبديل **الحماية بكلمة مرور** لتمكين المكون أو تعطيله.

4. حدد كلمة المرور الخاصة بحساب KLAdmin وقم بتأكيدها.

لحساب KLAdmin الحق في اتخاذ أي إجراء محمي بكلمة مرور.

إذا كان الكمبيوتر يعمل بموجب سياسة، فيمكن للمسؤول إعادة تعيين كلمة المرور الخاصة بحساب KLAdmin في خصائص السياسة. إذا لم يكن الكمبيوتر متصلاً بـ Kaspersky Security Center ونسيت كلمة المرور الخاصة بحساب KLAdmin، فلن يكون من الممكن استرداد كلمة المرور.

5. تعيين/حدد الأذونات لجميع المستخدمين داخل شبكة الشركة المحلية:

a. في جدول الحساب، انقر فوق **تحرير** لفتح قائمة الأذونات لمجموعة "الجميع".

مجموعة "الكل" هي مجموعة Windows مدمجة والتي تتضمن جميع المستخدمين داخل شبكة الشركة.

b. حدد خانات الاختيار بجانب الإجراءات التي سيسمح للمستخدمين بتنفيذها دون إدخال كلمة المرور.

إذا تم إلغاء تحديد خانة اختيار، فسيتم حظر المستخدمين من تنفيذ الإجراء. على سبيل المثال، إذا تم إلغاء تحديد خانة الاختيار الموجودة بجوار إذن **إنهاء التطبيق**، فيمكنك الخروج من التطبيق فقط إذا كنت قد قمت بتسجيل الدخول باسم KLAdmin، أو باسم مستخدم فردي لديه الإذن المطلوب، أو إذا كنت قد قمت بإدخال كلمة مرور مؤقتة.

لدى أذونات حماية كلمة المرور بعض الجوانب التي يجب وضعها في الاعتبار والتي تعتبر مهمة. تأكد من استيفاء جميع الشروط للوصول إلى Kaspersky Endpoint Security.

6. احفظ تغييراتك.

عند تمكين الحماية بكلمة مرور، سيقيد التطبيق وصول المستخدمين إلىKaspersky Endpoint Security وفقًا للأذونات الممنوحة لمجموعة "الكل". يمكنك تنفيذ الإجراءات المحظورة لمجموعة "الكل" فقط إذا كنت تستخدم حساب KLAdmin، حساب آخر تم منحه الأذونات المطلوبة، أو إذا أدخلت كلمة مرور مؤقتة.

لا يمكنك تعطيل الحماية بكلمة المرور إلا إذا قمت بتسجيل الدخول كـKLAdmin. من غير الممكن القيام بتعطيل الحماية بكلمة مرور إذا كنت تستخدم أي حساب مستخدم آخر أو كلمة مرور مؤقتة.

أثناء التحقق من كلمة المرور، يمكنك تحديد خانة الاختيار **حفظ كلمة المرور للجلسة الحالية**. في هذه الحالة، لن يطالب Kaspersky Endpoint Security بكلمة مرور عندما يحاول المستخدم تنفيذ إجراء آخر محمي بكلمة مرور خلال المدة الزمنية للجلسة.

منح أذونات للمستخدمين الأفراد أو المجموعات

يمكنك منح حق الوصول إلى Kaspersky Endpoint Security للمستخدمين الأفراد أو المجموعات. على سبيل المثال، إذا تم حظر الخروج من التطبيق لمجموعة "الكل"، فيمكنك منح إذن **إنهاء التطبيق** إلى مستخدم فردي. نتيجة لذلك، لا يمكنك الخروج من التطبيق إلا إذا كنت قد قمت بتسجيل الدخول كمستخدم أو باسم KLAdmin.

لا يمكنك استخدام بيانات اعتماد الحساب في الوصول إلى التطبيق إلا إذا كان الكمبيوتر في المجال. أما إذا لم يكن الكمبيوتر في المجال، يمكنك استخدام حساب KLAdmin أو كلمة مرور مؤقتة.

لمنح أذونات للمستخدمين الأفراد أو المجموعات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الواجهة**.

3. في جدول الحساب، انقر فوق **إضافة**.

4. في النافذة التي تفتح، انقر فوق الزر **تحديد مستخدم أو مجموعة**.

يفتح مربع الحوار الخيار القياسي تحديد المستخدمين أو المجموعات .

5. حدد مستخدم أو مجموعة في Active Directory وقم بتأكيد اختيارك.

6. في القائمة **الأذونات**، حدد خانات الاختيار الموجودة بجوار الإجراءات التي سيُسمح للمستخدم أو المجموعة المحددة بتنفيذها دون المطالبة بكلمة مرور.

إذا تم إلغاء تحديد خانة اختيار، فسيتم حظر المستخدمين من تنفيذ الإجراء. على سبيل المثال، إذا تم إلغاء تحديد خانة الاختيار الموجودة بجوار إذن **إنهاء التطبيق**، فيمكنك الخروج من التطبيق فقط إذا كنت قد قمت بتسجيل الدخول باسم KLAdmin، أو باسم مستخدم فردي لديه الإذن المطلوب، أو إذا كنت قد قمت بإدخال كلمة مرور مؤقتة.

لدى أذونات حماية كلمة المرور بعض الجوانب التي يجب وضعها في الاعتبار والتي تعتبر مهمة. تأكد من استيفاء جميع الشروط للوصول إلى Kaspersky Endpoint Security.

7. احفظ تغييراتك.

نتيجة لذلك، إذا كان الوصول إلى التطبيق تم تقييده لمجموعة "الكل"، فسيتم منح المستخدمين أذونات للوصول إلى Kaspersky Endpoint Security طبقا للأذونات الفردية للمستخدمين.

استخدام كلمة مرور مؤقتة لمنح الأذونات

يمكن استخدام كلمة مرور مؤقتة لمنح وصول مؤقت إلى Kaspersky Endpoint Security لكمبيوتر فردي خارج شبكة الشركة. هذا ضروري للسماح للمستخدم بتنفيذ إجراء محظور دون الحصول على بيانات اعتماد حساب KLAdmin. لاستخدام كلمة مرور مؤقتة، يجب إضافة الكمبيوتر إلى Kaspersky Security Center.

كيفية السماح لمستخدم بتنفيذ إجراء محظور باستخدام كلمة مرور مؤقتة من خلال وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في مجلد **الأجهزة المدارة** الخاص بشجرة وحدة تحكم الإدارة، افتح المجلد الذي يحمل اسم مجموعة الإدارة التي تنتمي إليها أجهزة الكمبيوتر العميلة ذات الصلة.

3. في مساحة العمل، حدد علامة تبويب **الأجهزة**.

4. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.

5. من نافذة خصائص الكمبيوتر، حدد القسم **التطبيقات**.

6. في قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر، حدد **Kaspersky Endpoint Security for Windows** وانقر نقرًا مزدوجًا لفتح خصائص التطبيق.

7. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الواجهة**.

8. في القسم **الحماية بكلمة مرور**، انقر على الزر **الإعدادات**.

9. في القسم **كلمة المرور المؤقتة**، انقر فوق الزر **الإعدادات**.

10. تفتح النافذة **إنشاء كلمة مرور مؤقتة**.

11. في حقل **تاريخ انتهاء الصلاحية**، حدد تاريخ انتهاء الصلاحية عندما تنتهي صلاحية كلمة المرور المؤقتة.

12. في الجدول **نطاق كلمة المرور المؤقتة**، حدد خانات الاختيار الموجودة جانب العمليات التي يجب إتاحتها للمستخدم بعد إدخال كلمة المرور المؤقتة.

13. انقر على **إنشاء**.
تفتح نافذة تحتوي على كلمة المرور المؤقتة (انظر الشكل أدناه).

14. انسخ كلمة المرور وقدمها للمستخدم.

[كيفية السماح لمستخدم بتنفيذ إجراء محظور باستخدام كلمة مرور مؤقتة من خلال Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Managed devices** ← **Devices**.

2. انقر فوق اسم الكمبيوتر الذي تريد السماح لمستخدم بتنفيذ إجراء محظور عليه.

3. حدد علامة التبويب **Applications**.

4. انقر على **Kaspersky Endpoint Security for Windows**.
تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.

5. حدد علامة التبويب **Application settings**.

6. في نافذة إعدادات التطبيق، اختر **Interface** ← **General settings**.

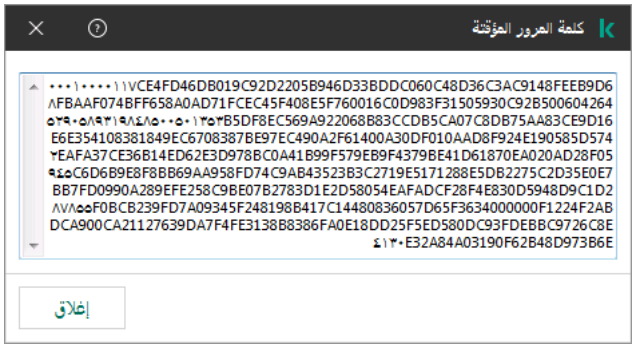
7. في القسم **الحماية بكلمة مرور**، انقر على الزر **كلمة المرور المؤقتة**.

8. في حقل **تاريخ انتهاء الصلاحية**، حدد تاريخ انتهاء الصلاحية عندما تنتهي صلاحية كلمة المرور المؤقتة.

9. في الجدول **نطاق كلمة المرور المؤقتة**، حدد خانات الاختيار الموجودة جانب العمليات التي يجب إتاحتها للمستخدم بعد إدخال كلمة المرور المؤقتة.

10. انقر على **إنشاء**.
تفتح نافذة تحتوي على كلمة المرور المؤقتة.

11. انسخ كلمة المرور وقدمها للمستخدم.



كلمة المرور المؤقتة

الجوانب الخاصة لأذونات الحماية بكلمة المرور

أذونات الحماية بكلمة المرور لها بعض الجوانب والحدود المهمة التي يجب وضعها في الاعتبار.

تكوين إعدادات التطبيق

إذا كان كمبيوتر المستخدم يعمل بموجب سياسة، فتأكد من أن جميع الإعدادات المطلوبة في السياسة متاحة للتحرير (السمات مفتوحة).

إنهاء التطبيق

لا توجد اعتبارات خاصة أو حدود.

تعطيل مكونات الحماية

- من غير الممكن منح إذن تعطيل مكونات الحماية لمجموعة الكل. للسماح للمستخدمين غير KLAdmin بتعطيل مكونات التحكم، قم بإضافة مستخدم أو مجموعة لديهم إذن **تعطيل مكونات الحماية** في إعدادات الحماية بكلمة المرور.
- إذا كان كمبيوتر المستخدم يعمل بموجب سياسة، فتأكد من أن جميع الإعدادات المطلوبة في السياسة متاحة للتحرير (السمات مفتوحة).
- لتعطيل مكونات الحماية في إعدادات التطبيق، يجب أن يكون لدى المستخدم إذن **تكوين إعدادات التطبيق**.
- لتعطيل مكونات الحماية من قائمة السياق (باستخدام عنصر قائمة **إيقاف الحماية مؤقتًا**)، يجب أن يكون لدى المستخدم إذن **تعطيل مكونات الحماية** بالإضافة إلى إذن **تعطيل مكونات التحكم**.

تعطيل مكونات التحكم

- من غير الممكن منح إذن تعطيل مكونات التحكم لمجموعة الكل. للسماح للمستخدمين غير KLAdmin بتعطيل مكونات التحكم، قم بإضافة مستخدم أو مجموعة لديهم إذن **تعطيل مكونات التحكم** في إعدادات الحماية بكلمة المرور.
- إذا كان كمبيوتر المستخدم يعمل بموجب سياسة، فتأكد من أن جميع الإعدادات المطلوبة في السياسة متاحة للتحرير (السمات مفتوحة).
- لتعطيل مكونات التحكم في إعدادات التطبيق، يجب أن يكون لدى المستخدم إذن **تكوين إعدادات التطبيق**.
- لتعطيل مكونات التحكم من قائمة السياق (باستخدام عنصر القائمة **إيقاف الحماية مؤقتًا**)، يجب أن يكون لدى المستخدم إذن **تعطيل مكونات التحكم** بالإضافة إلى إذن **تعطيل مكونات الحماية**.

تعطيل سياسة مركز Kaspersky Security Center

لا يمكنك منح مجموعة "الجميع" الإذن لتعطيل سياسة Kaspersky Security Center. للسماح للمستخدمين غير KLAdmin بتعطيل إعدادات التطبيق، قم بإضافة مستخدم أو مجموعة لديها إذن **تعطيل سياسة مركز Kaspersky Security Center** في إعدادات الحماية بكلمة مرور.

إزالة المفتاح

لا توجد اعتبارات خاصة أو حدود.

إزالة / تعديل / استعادة التطبيق

إذا سمحت بإزالة التطبيق وتعديله واستعادته لمجموعة "الكل"، لا يطلب Kaspersky Endpoint Security كلمة مرور عندما يحاول المستخدم تنفيذ هذه العمليات. ولذلك، يستطيع أي مستخدم بما في ذلك المستخدمين من خارج المجال تثبيت التطبيق أو تعديله أو استعادته.

استعادة الوصول إلى البيانات على محركات الأقراص المشفرة

يمكنك استعادة الوصول إلى البيانات على محركات الأقراص المشفرة فقط إذا قمت بتسجيل الدخول كـ KLAdmin. لا يمكن منح الإذن بتنفيذ هذا الإجراء لأي مستخدم آخر.

عرض التقارير

لا توجد اعتبارات خاصة أو حدود.

الاستعادة من نسخة احتياطية

لا توجد اعتبارات خاصة أو حدود.

إعادة تعيين كلمة مرور KLAdmin

إذا نسيت كلمة مرور حساب KLAdmin، فيمكنك إعادة تعيين كلمة المرور في خصائص السياسة. ولا يمكنك إعادة تعيين كلمة المرور في واجهة التطبيق.

يمكنك تنفيذ إجراءات محمية بكلمة مرور باستخدام كلمة مرور مؤقتة. وفي هذه الحالة لا تحتاج إلى إدخال بيانات اعتماد KLAdmin.

إذا لم يكن الكمبيوتر متصلاً بـ Kaspersky Security Center ونسيت كلمة المرور الخاصة بحساب KLAdmin، فلن يكون من الممكن استرداد كلمة المرور.

كيفية إعادة تعيين كلمة مرور حساب KLAdmin باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الواجهة**.
5. في القسم **الحماية بكلمة مرور**، انقر على الزر **الإعدادات**.
6. في النافذة التي تفتح، امسح خانة الاختيار **تمكين الحماية بكلمة مرور**
7. احفظ تغييراتك.
8. حدد خانة الاختيار **تمكين الحماية بكلمة مرور** مرة أخرى.
9. انقر فوق **موافق**.
   يفتح هذا نافذة كلمة مرور المسؤول.
10. حدد كلمة المرور الجديدة لحساب KLAdmin وقم بتأكيدها.
11. احفظ تغييراتك.

كيفية إعادة تعيين كلمة مرور حساب KLAdmin في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Managed devices**.

2. حدد الكمبيوتر الذي تريد تكوين إعدادات التطبيق المحلية له.
تقوم هذه الخطوة بفتح خصائص الكمبيوتر.

3. حدد علامة التبويب **Applications**.

4. انقر على **Kaspersky Endpoint Security for Windows**.
تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.

5. حدد علامة التبويب **Application settings**.

6. انتقل إلى **General settings** ← **Interface**.

7. تحت **الحماية بكلمة مرور**، أوقف تشغيل المفتاح **الحماية بكلمة مرور**.

8. احفظ تغييراتك.

9. أعد تشغيل **الحماية بكلمة مرور** مرة أخرى.

10. حدد كلمة المرور الجديدة لحساب KLAdmin وقم بتأكيدها.

11. احفظ تغييراتك.

نتيجة لذلك، يتم تحديث كلمة مرور حساب KLAdmin الخاص بك بعد تطبيق السياسة.

منطقة موثوقة

تُعد المنطقة الموثوقة بمثابة قائمة يتم تكوينها بواسطة مسؤول النظام تضم كائنات وتطبيقات لا يقوم Kaspersky Endpoint Security بمراقبتها عندما يكون نشطًا.

يقوم المسؤول بتكوين المنطقة الموثوقة بشكل فردي، مع الأخذ في الاعتبار الميزات المتوفرة بالكائنات التي تمت معالجتها والتطبيقات التي تم تثبيتها على الكمبيوتر. قد يكون من الضروري تضمين الكائنات والتطبيقات في المنطقة الموثوقة عند قيام Kaspersky Endpoint Security بمنع الوصول إلى كائن أو تطبيق معين، إذا كنت على يقين بأن الكائن أو التطبيق غير ضار. يستطيع المسؤول أيضًا السماح لمستخدم بإنشاء منطقته الموثوقة المحلية لجهاز كمبيوتر معين. وبهذه الطريقة، يستطيع المستخدمون إنشاء قوائم محلية من الاستثناءات والتطبيقات الموثوقة الخاصة بهم بالإضافة إلى المنطقة العامة الموثوقة في سياسة ما.

إنشاء استثناء من الفحص

استثناءات من الفحص هي عبارة عن مجموعة من الشروط التي يجب تنفيذها حتي لا يقوم Kaspersky Endpoint Security بفحص كائن معين للبحث عن الفيروسات والتهديدات الأخرى.

تجعل استثناءات من الفحص من الممكن استخدام البرامج القانونية التي يمكن استغلالها من قِبل المجرمين للإضرار بالكمبيوتر أو بيانات المستخدم. على الرغم من عدم احتوائها على أية وظائف ضارة، يمكن للدخلاء استغلال مثل هذه التطبيقات. وللحصول على تفاصيل حول البرامج الشرعية التي يمكن أن يستخدمها المجرمون للإضرار بجهاز الكمبيوتر أو البيانات الشخصية لمستخدم ما، يرجى الرجوع إلى موقع ويب موسوعة تكنولوجيا معلومات Kaspersky.

قد يتم منع هذه التطبيقات بواسطة Kaspersky Endpoint Security. لمنع أن يتم حظرهم، يمكنك تكوين استثناءات من الفحص للتطبيقات التي يتم استخدامها. للقيام بذلك، قم بإضافة الاسم أو قناع الاسم المدرج في موسوعة تكنولوجيا المعلومات من Kaspersky إلى المنطقة الموثوقة. على سبيل المثال، تستخدم في معظم الأحيان تطبيق Radmin لإدارة أجهزة الكمبيوتر عن بُعد. يعتبر Kaspersky Endpoint Security هذا النشاط نشاطًا مشكوكًا فيه وربما يقوم بمنعه. لمنع التطبيق من الحظر، قم بإنشاء استثناء من الفحص يحمل الاسم أو قناع الاسم المدرج في موسوعة تكنولوجيا المعلومات من Kaspersky.

إذا كان أحد التطبيقات التي تجمع المعلومات وترسلها لكي تتم معالجتها مثبت على الكمبيوتر لديك، فقد يُصنف Kaspersky Endpoint Security هذا التطبيق كبرمجيات ضارة. ولتجنب حدوث ذلك، يمكنك استثناء التطبيق من الفحص عبر تكوين Kaspersky Endpoint Security على النحو الموضح في هذا المستند.

يمكن استخدام استثناءات من الفحص بواسطة مكونات التطبيقات التالية والمهام التي تم تكوينها بواسطة مسؤول النظام:

- اكتشاف السلوك.
- منع الاستغلال.
- منع اختراق المضيف.
- الحماية من تهديدات الملفات.
- الحماية من تهديدات الويب.
- الحماية من تهديدات البريد.
- مهام فحص البرامج الضارة.

لا يفحص Kaspersky Endpoint Security كائن ما إذا كان محرك القرص أو المجلد الذي يحتوي هذا الملف مضمن في نطاق الفحص عند بدء إحدى مهام الفحص. ومع هذا، لا يتم تطبيق استثناء من الفحص عندما يتم بدء مهمة فحص مخصص لهذا الكائن الخاص.

كيفية إنشاء استثناء من الفحص في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات**.

5. في القسم **استثناءات من الفحص والتطبيقات الموثوقة**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، حدد القسم **استثناءات الفحص**.

   يفتح هذا نافذة تحتوي على قائمة استثناءات.

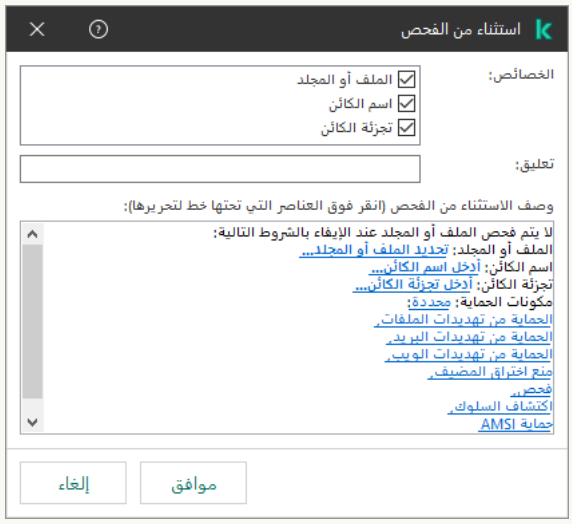
7. حدد خانة الاختيار **دمج القيم عند التوريث** إذا كنت ترغب في إنشاء قائمة موحدة بالاستثناءات لجميع أجهزة الكمبيوتر في الشركة. سيتم دمج قوائم الاستثناءات في السياسات الأصلية والفرعية. سيتم دمج القوائم بشرط أن تكون قيم الدمج مفعلة عند التوريث. ويتم عرض الاستثناءات من السياسة الأصلية في السياسات الفرعية في عرض قراءة فقط. لا يمكن تغيير الاستثناءات أو حذفها من السياسة الرئيسية.

8. حدد خانة الاختيار **السماح باستخدام الاستثناءات المحلية** إذا كنت تريد تمكين المستخدم لإنشاء قائمة استثناءات محلية. وبهذه الطريقة، يستطيع المستخدم إنشاء قائمة الاستثناءات المحلية الخاصة به بالإضافة إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر.

   في حالة تحديد خانة الاختيار، يستطيع المستخدم الوصول فقط إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة.

9. انقر على **إضافة**.

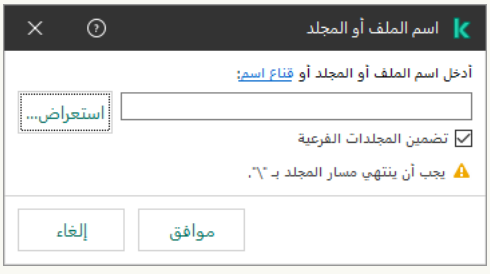
10. لاستثناء ملف أو مجلد من الفحص:



إعدادات الاستثناءات

a. في القسم **الخصائص**، حدد خانة الاختيار **الملف أو المجلد**.

b. انقر فوق الرابط **select file or folder** في القسم **وصف الاستثناء من الفحص (انقر فوق العناصر التي تحتها خط لتحريرها)** لفتح النافذة **اسم الملف أو المجلد**.



a. أدخل اسم الملف أو المجلد أو قناع اسم الملف أو المجلد أو حدد الملف أو المجلد من شجرة المجلدات عبر النقر فوق **استعراض**.

استخدم الأقنعة:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

يمكنك استخدام الأقنعة في بداية مسار الملف أو في منتصفه أو في نهايته. على سبيل المثال، إذا كنت تريد إضافة مجلد لجميع المستخدمين إلى الاستثناءات، أدخل القناع `C:\Users\*\Folder\`.

يدعم Kaspersky Endpoint Security متغيرات البيئة

لا يدعم Kaspersky Endpoint Security متغير البيئة `%userprofile%` عند توليد قائمة الاستثناءات باستخدام وحدة تحكم Kaspersky Security Center. ولتطبيق الإدخال على كل حسابات المستخدمين، يمكنك استخدام الحرف * (على سبيل المثال، `C:\Users\*\Documents\File.exe`). كلما أضفت متغير بيئة جديدًا، فأنت بحاجة إلى إعادة تشغيل التطبيق.

b. احفظ تغييراتك.

11. لاستبعاد كائنات ذات اسم محدد من الفحص:

a. في القسم **الخصائص**، حدد خانة الاختيار **اسم الكائن**.

b. انقر فوق الرابط **enter object name** في القسم **وصف الاستثناء من الفحص (انقر فوق العناصر التي تحتها خط لتحريرها)** لفتح النافذة **اسم الكائن**.

تحديد كائن

a. أدخل اسم الكائن وفقًا لتصنيف موسوعة Kaspersky (على سبيل المثال، `Email-Worm` أو `Rootkit` أو `RemoteAdmin`).

يمكنك استخدام الأقنعة مع حرف `?` (يستبدل أي حرف مفرد) و`*` (يحل محل أي عدد من الأحرف). على سبيل المثال، في حالة تحديد القناع `Client*`، يستثني Kaspersky Endpoint Security كائنات `Client-IRC` و`Client-P2P` و`Client-SMTP` من عمليات الفحص.

b. احفظ تغييراتك.

12. إذا كنت ترغب في استثناء ملف فردي من عمليات الفحص:

a. في القسم **الخصائص**، حدد خانة الاختيار **تجزئة الكائن**.

b. انقر على رابط **enter object hash** لفتح النافذة **تجزئة الكائن**.

تحديد ملف

a. أدخل تجزئة الملف أو حدد الملف بالنقر فوق الزر **استعراض**.

في حالة تعديل الملف، سيتم أيضًا تعديل تجزئة الملف. إذا حدث هذا، فلن تتم إضافة الملف المعدل إلى الاستثناءات.

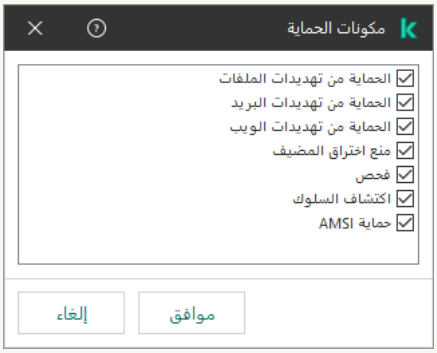
b. احفظ تغييراتك.

13. إذا لزم الأمر، في الحقل **تعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

14. حدد مكونات Kaspersky Endpoint Security التي يجب أن تستخدم استثناء من الفحص:

a. انقر فوق الرابط **any** في القسم **وصف الاستثناء من الفحص (انقر فوق العناصر التي تحتها خط لتحريرها)** لتفعيل الرابط **select components**.

b. انقر فوق الرابط **تحديد المكونات** لفتح النافذة **مكونات الحماية**.



تحديد مكونات الحماية

a. حدد خانات الاختيار المقابلة للمكونات التي يجب تطبيق استثناء من الفحص إليها.

b. احفظ تغييراتك.

في حالة تحديد المكونات في إعدادات استثناء من الفحص، فإنه يتم تطبيق هذا الاستثناء فقط أثناء الفحص بواسطة مكونات Kaspersky Endpoint Security هذه.

في حالة عدم تحديد المكونات في إعدادات استثناء من الفحص يتم تطبيق هذا الاستثناء أثناء الفحص بواسطة جميع مكونات Kaspersky Endpoint Security.

15. يمكنك إيقاف الاستثناءات في أي وقت باستخدام خانة الاختيار.

16. احفظ تغييراتك.

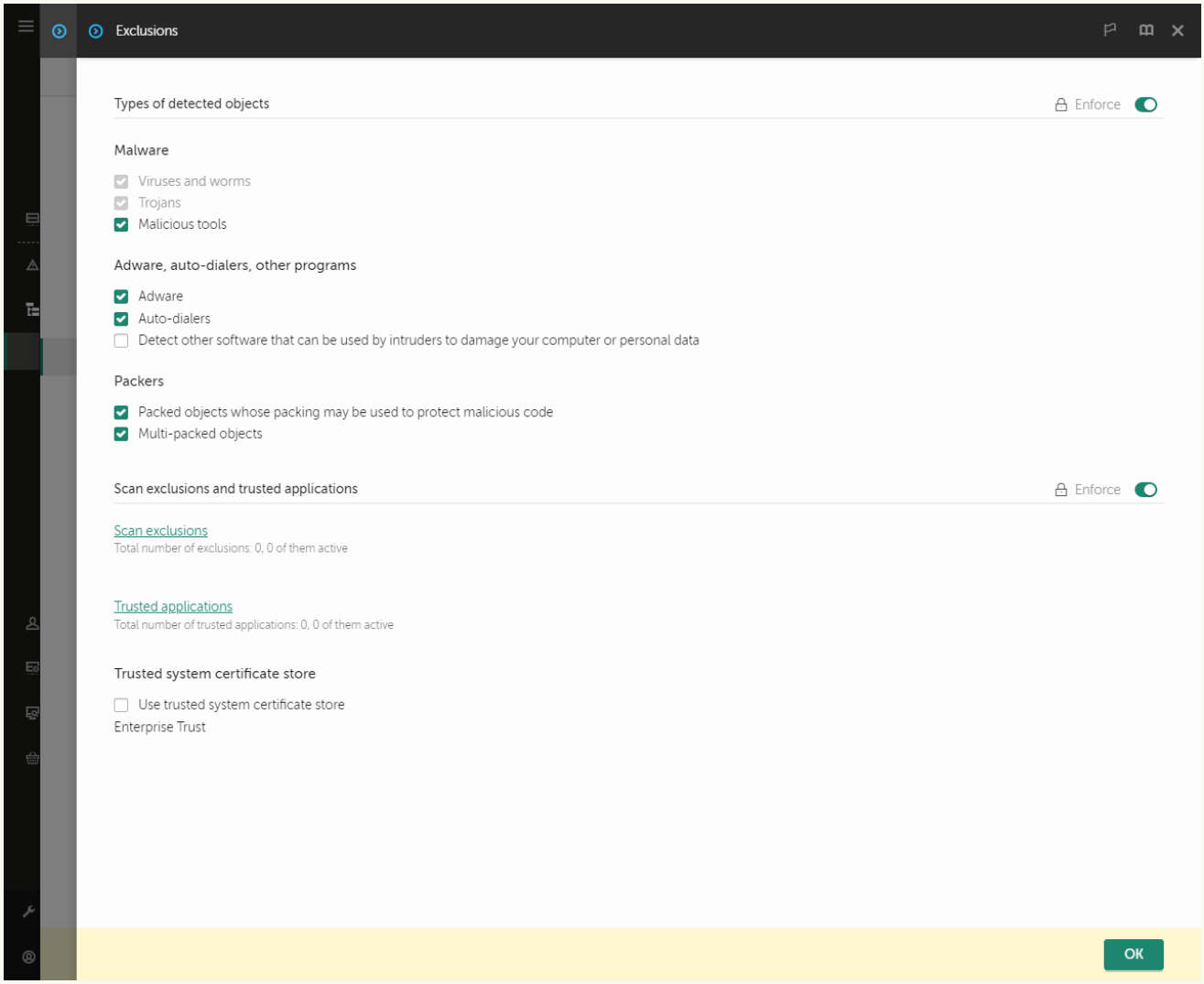
كيفية إنشاء استثناء من الفحص في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Exclusions and types of detected objects**.



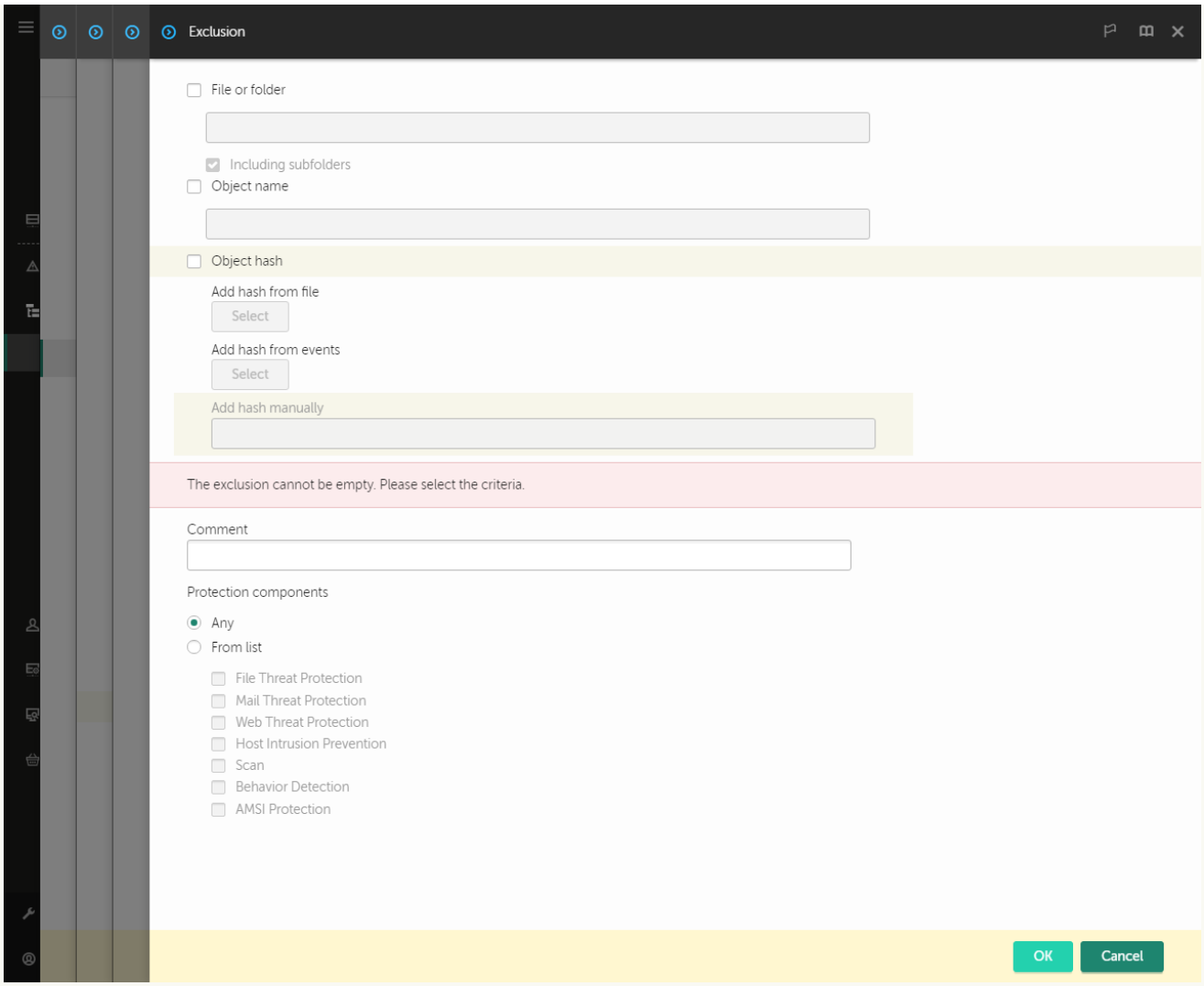
إعدادات الاستثناءات

5. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Scan exclusions**.

6. حدد خانة الاختيار **Merge values when inheriting** إذا كنت ترغب في إنشاء قائمة موحدة بالاستثناءات لجميع أجهزة الكمبيوتر في الشركة. سيتم دمج قوائم الاستثناءات في السياسات الأصلية والفرعية. سيتم دمج القوائم بشرط أن تكون قيم الدمج مفعلة عند التوريث. ويتم عرض الاستثناءات من السياسة الأصلية في السياسات الفرعية في عرض قراءة فقط. لا يمكن تغيير الاستثناءات أو حذفها من السياسة الرئيسية.

7. حدد خانة الاختيار **Allow use of local exclusions** إذا كنت تريد تمكين المستخدم لإنشاء قائمة استثناءات محلية. وبهذه الطريقة، يستطيع المستخدم إنشاء قائمة الاستثناءات المحلية الخاصة به بالإضافة إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر.
في حالة تحديد خانة الاختيار، يستطيع المستخدم الوصول فقط إلى قائمة الاستثناءات العامة التي تم إنشاؤها في السياسة.

8. انقر على الزر **Add**.



إعدادات الاستثناءات

9. حدد كيف تريد إضافة الاستثناء: **File or folder** أو **Object name** أو **Object hash**.

10. لاستثناء ملف أو مجلد من الفحص، أدخل المسار يدويًا. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

  يمكنك استخدام الأقنعة في بداية مسار الملف أو في منتصفه أو في نهايته. على سبيل المثال، إذا كنت تريد إضافة مجلد لجميع المستخدمين إلى الاستثناءات، أدخل القناع `C:\Users\*\Folder\`.

11. إذا كنت ترغب في استثناء نوع معين من الكائنات من عمليات الفحص، في الحقل **Object name** أدخل اسم نوع الكائن وفقًا لتصنيف موسوعة Kaspersky (على سبيل المثال، `البريد الإلكتروني-فيروس متنقل` أو `مجموعة الجذر` أو `الإدارة عن بُعد`).

يمكنك استخدام الأقنعة مع حرف `?` (يستبدل أي حرف مفرد) و `*` (يحل محل أي عدد من الأحرف). على سبيل المثال، في حالة تحديد القناع `Client*`، يستثني Kaspersky Endpoint Security كائنات `Client-IRC` و `Client-P2P` و `Client-SMTP` من عمليات الفحص.

12. إذا كنت ترغب في استثناء ملف فردي من عمليات الفحص، فأدخل تجزئة الملف في الحقل **Object hash**.

في حالة تعديل الملف، سيتم أيضًا تعديل تجزئة الملف. إذا حدث هذا، فلن تتم إضافة الملف المعدل إلى الاستثناءات.

13. في القسم **Protection components**، حدد المكونات التي تريد تطبيق استثناء الفحص عليها.

14. إذا لزم الأمر، في الحقل **Comment**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

15. يمكنك استخدام مفتاح التبديل إيقاف استثناء في أي وقت.

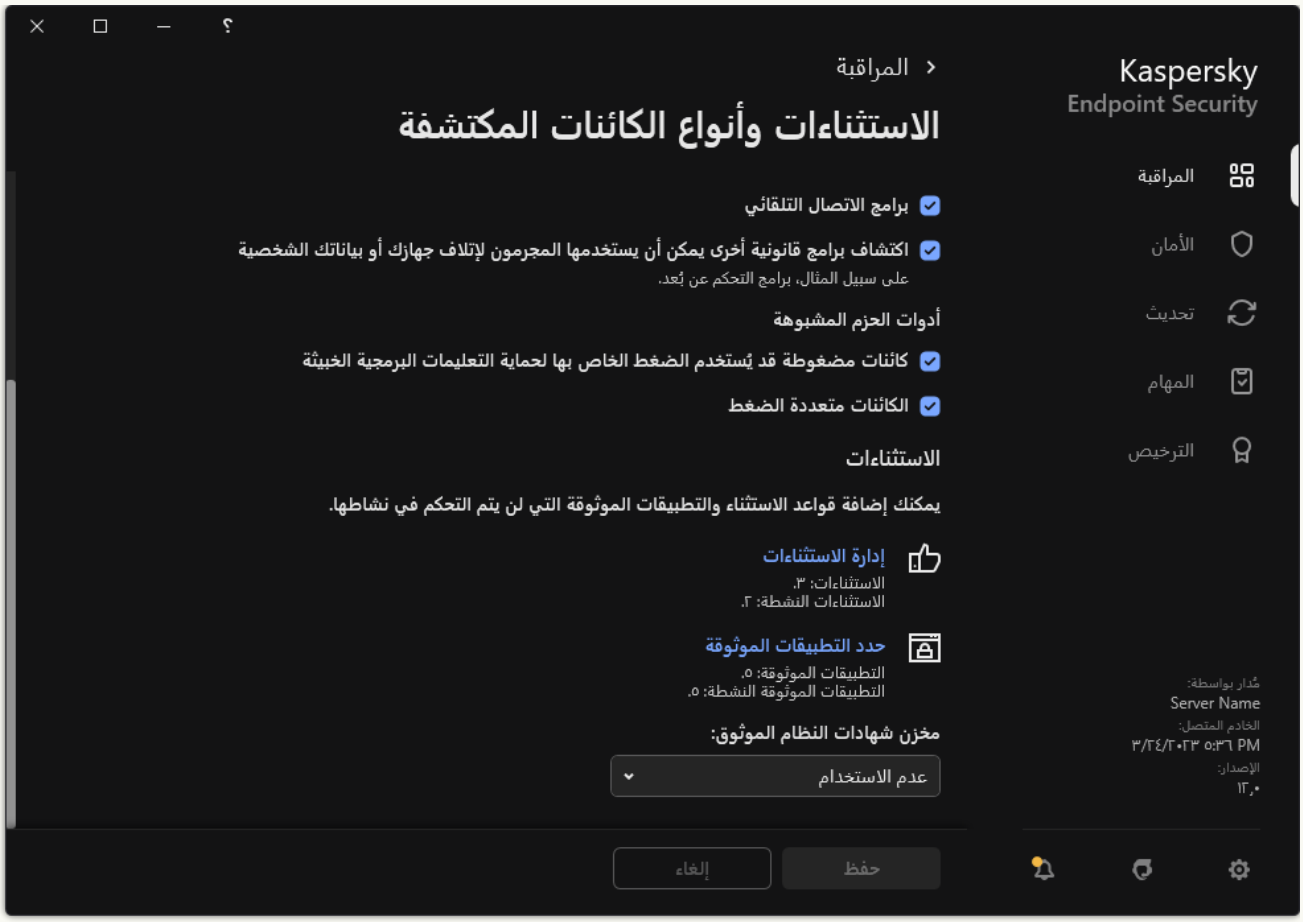
16. احفظ تغييراتك.

كيفية إنشاء استثناء من الفحص في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات المكتشفة**.

3. في القسم **الاستثناءات**، انقر على الرابط **إدارة الاستثناءات**.



إعدادات الاستثناءات

4. انقر على **إضافة**.

5. إذا كنت ترغب في استثناء ملف أو مجلد من عمليات الفحص، فحدد الملف أو المجلد بالنقر فوق الزر **استعراض**.

يمكنك أيضًا إدخال المسار يدويًا. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

  يمكنك استخدام الأقنعة في بداية مسار الملف أو في منتصفه أو في نهايته. على سبيل المثال، إذا كنت تريد إضافة مجلد لجميع المستخدمين إلى الاستثناءات، أدخل القناع `C:\Users\*\Folder\`.

6. إذا كنت ترغب في استثناء نوع معين من الكائنات من عمليات الفحص، في الحقل **الكائن** أدخل اسم نوع الكائن وفقًا لتصنيف موسوعة Kaspersky (على سبيل المثال، `البريد الإلكتروني-فيروس متنقل` أو `مجموعة الجذر` أو `الإدارة عن بُعد`).

يمكنك استخدام الأقنعة مع حرف `?` (يستبدل أي حرف مفرد) و`*` (يحل محل أي عدد من الأحرف). على سبيل المثال، في حالة تحديد القناع `Client*`، يستثني Kaspersky Endpoint Security كائنات `Client-IRC` و`Client-P2P` و`Client-SMTP` من عمليات الفحص.

7. إذا كنت ترغب في استثناء ملف فردي من عمليات الفحص، فأدخل تجزئة الملف في الحقل **رمز تجزئة الملف**.

في حالة تعديل الملف، سيتم أيضًا تعديل تجزئة الملف. إذا حدث هذا، فلن تتم إضافة الملف المعدل إلى الاستثناءات.

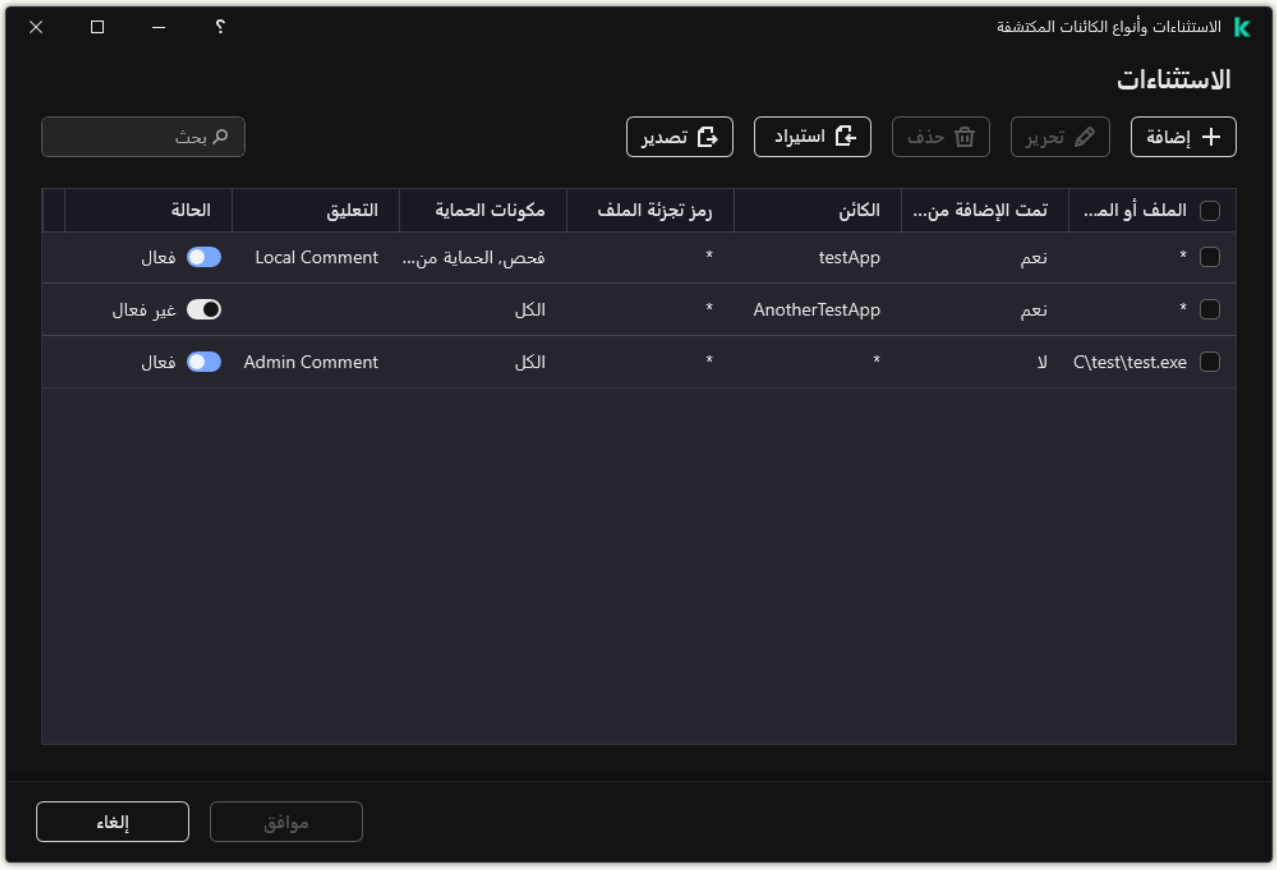
8. في القسم **مكونات الحماية**، حدد المكونات التي تريد تطبيق استثناء الفحص عليها.

9. إذا لزم الأمر، في الحقل **التعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

10. حدد الحالة **فعال** للاستثناء.

يمكنك إيقاف الاستثناءات في أي وقت باستخدام مفتاح التبديل.

11. احفظ تغييراتك.



قائمة الاستثناءات

أمثلة قناع المسار:

مسارات الملفات الموجودة في أي مجلد:

- سيشمل القناع `*.exe` كافة المسارات إلى الملفات التي لها امتداد exe.
- سيشمل `example*` القناع كل المسارات إلى الملفات المسماة EXAMPLE.

مسارات الملفات الموجودة في مجلد محدد:

- سيشمل القناع `C:\dir\*.*` جميع المسارات إلي الملفات الموجودة في مجلد C:\dir\ ولكنها ليست موجودة في الملف الفرعي C:\dir\.
- سيشمل القناع `C:\dir\*` كل المسارات إلي الملفات الموجودة في المجلد C:\dir\ بما في ذلك المجلدات الفرعية.
- سيشمل القناع `C:\dir\*` كل المسارات إلي الملفات الموجودة في المجلد C:\dir\، بما في ذلك المجلدات الفرعية.
- سيشمل القناع `C:\dir\*.exe` جميع المسارات إلى الملفات ذات امتداد EXE الموجود في مجلد C:\dir\ ولكنها ليست موجودة في المجلدات الفرعية لـ C:\dir\.
- سيشمل القناع `C:\dir\test` جميع المسارات إلى الملفات المسماة "test" والموجودة في مجلد C:\dir\ ولكنها ليست موجودة في المجلدات الفرعية لـ C:\dir\.
- سيشمل القناع `C:\dir\*\test` جميع المسارات إلى الملفات المسماة 'test' والموجودة في المجلد C:\dir\ وفي المجلدات الفرعية C:\dir\.
- سوف يشمل القناع `C:\dir1\*\dir3\` جميع مسارات الملفات الموجودة في مجلدات dir3 الفرعية بمستوى واحد في المجلد C:\dir1\.
- سوف يشمل القناع `C:\dir1\**\dirN\` جميع مسارات الملفات في مجلدات dirN الفرعية في المجلد C:\dir1\ على أي مستوى.

المسارات إلى الملفات الموجودة في جميع المجلدات ذات الاسم المحدد:

- سيشمل القناع `"*.*\dir` جميع المسارات إلى الملفات في مجلدات باسم "dir" ولكنها ليست موجودة في المجلدات الفرعية لهذه المجلدات.
- سيشمل القناع `*\dir` " جميع المسارات إلى الملفات في مجلدات باسم "dir" ولكنها ليست موجودة في المجلدات الفرعية لهذه المجلدات.
- سيشمل القناع `\dir` جميع المسارات إلى الملفات في مجلدات باسم "dir" ولكنها ليست موجودة في المجلدات الفرعية لهذه المجلدات.
- سيشمل القناع `dir\*.exe` جميع المسارات إلى الملفات ذات امتداد EXE في المجلدات المسماة "dir" ولكنها ليست موجودة في المجلدات الفرعية لهذه المجلدات.
- سيشمل القناع `dir\test` كافة المسارات إلى الملفات المسماة "test" في مجلدات باسم "dir" ولكنها ليست موجودة في المجلدات الفرعية لهذه المجلدات.

تحديد أنواع الكائنات القابلة للاكتشاف

لتحديد أنواع الكائنات القابلة للاكتشاف:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات المكتشفة**.
3. في القسم **أنواع الكائنات المكتشفة**، حدد خانات الاختيار المقابلة لأنواع الكائنات التي تريد أن يكتشفها Kaspersky Endpoint Security:
   - **الفيروسات وفيروسات الدودة**؛

الفئة الفرعية: الفيروسات والفيروسات المتنقلة (الفيروسات_و_الفيروسات المتنقلة)

مستوى التهديد: عالي

تقوم الفيروسات التقليدية والفيروسات المتنقلة بإجراءات غير مسموح بها من قِبل المستخدم. فيمكنها إنشاء نسخ من أنفسها كما تتمكن هذه النسخ من نسخ نفسها.

الفيروس التقليدي

عند اختراق فيروس تقليدي للكمبيوتر، فإنه يصيب أحد الملفات، ويقوم بتفعيل نفسه، وينفذ إجراءات ضارة، ويضيف نُسخًا من نفسه إلى ملفات أخرى.

يتضاعف الفيروس التقليدي فقط على الموارد المحلية للكمبيوتر؛ ولا يمكنه اختراق أجهزة الكمبيوتر الأخرى بمفرده. ويمكنه فقط المرور إلى كمبيوتر آخر إذا قام بإضافة نسخة من نفسه على ملف مُخزن في مجلد مشترك أو مُخزن على قرص مدمج، أو إذا قام المستخدم بإعادة توجيه رسالة بريد إلكتروني وكان بها ملف مرفق مصاب.

يتمكن رمز الفيروس التقليدي من اختراق مناطق مختلفة في أجهزة الكمبيوتر وأنظمة التشغيل والتطبيقات. حسب بيئة التشغيل, يتم تقسيم الفيروسات إلى فيروسات الملفات وفيروسات التمهيد وفيروسات البرامج النصية وفيروسات الماكرو.

تتمكن الفيروسات من إصابة الملفات باستخدام مجموعة متنوعة من الأساليب. الكتابة فوق الملفات بكتابة رمزها الخاص فوق الرمز الخاص بالملف المصاب، ومن ثم تمسح محتواه. ولذا، يتوقف ملف مصاب عن العمل ويتعذر استعادته. التطفلية على تعديل الملفات مع تركها تعمل كليًا أو جزئيًا. الفيروسات المصاحبة بتعديل الملفات، ولكنها تنشئ نُسخ متماثلة. عندما يتم فتح ملف مصاب، يبدأ النسخ المتماثل من هذا الملف (والذي يكون في الواقع عبارة عن فيروس). تتم أيضًا مواجهة الأنواع التالية من الفيروسات: فيروسات الروابط وفيروسات OBJ وفيروسات LIB ورمز المصدر والعديد من الفيروسات الأخرى.

Worm

وكما هو الحال مع الفيروس التقليدي، يتم تفعيل رمز الفيروس المتنقل وينفذ هذا الفيروس إجراءات ضارة بعد اختراقه للكمبيوتر. تم تسمية الفيروسات المتنقلة بهذا الاسم نظرًا لقدرتها على "التسلل" من كمبيوتر إلى آخر ونشر نُسخها عبر العديد من قنوات بيانات دون إذن المستخدم.

أما السمة الرئيسية التي تتيح التفريق بين الأنواع المختلفة من الفيروسات المتنقلة هي الطريقة التي تنتشر بها. يوفر الجدول التالي نظرة عامة على الأنواع المختلفة من الفيروسات المتنقلة، والتي يتم تصنيفها حسب طريقة انتشارها.

طرق انتشار الفيروسات المتنقلة

النوع	الاسم	الوصف
Email-Worm	Email-Worm	تنتشر عبر البريد الإلكتروني. تحتوي رسالة البريد الإلكتروني المصابة على ملف مرفق بنسخة من فيروس متنقل أو تحتوي على ارتباط إلى ملف تم إيداعه على أحد مواقع الويب الذي يحتمل تعرضه للقرصنة أو قد يكون تم إنشاؤه خصيصًا لهذا الغرض. عندما تفتح الملف المرفق، يتم تنشيط فيروس متنقل. وعند النقر على الارتباط، تحميل، ثم فتح الملف، يبدأ فيروس الدودة في اتخاذ إجراءاته الضارة. وبعد ذلك، يستمر في نشر نفسه، بحثًا عن عناوين بريد إلكتروني أخرى وإرسال الرسائل المصابة إليها.
IM-Worm	الفيروسات المتنقلة لعميل المراسلة الفورية	تنتشر عبر عملاء المراسلة الفورية. عادةً مل ترسل الفيروسات المتنقلة رسائل تحتوي على ارتباط إلى ملف به نسخة من الفيروس المتنقل على موقع ويب، مما يعني استخدام قوائم اتصال المستخدم. عندما يقوم المستخدم بتحميل ذلك الملف وفتحه، يتم تنشيط الفيروس المتنقل.
IRC-Worm	الفيروسات المتنقلة في المحادثة عبر الإنترنت	تنتشر من خلال المحادثات عبر الإنترنت، والتي تتمثل في أنظمة الخدمة التي تسمح بالاتصال بالآخرين عبر الإنترنت في الوقت الحقيقي. تقوم الفيروسات المتنقلة هذه بنشر ملف به نسخة منها أو ارتباط إلى هذا الملف في المحادثة عبر الإنترنت. عندما يقوم المستخدم بتحميل ذلك الملف وفتحه، يتم تنشيط الفيروس المتنقل.
Net-Worm	فيروسات الشبكة	تنتشر الفيروسات المتنقلة هذه عبر شبكات الكمبيوتر.

	المتنقلة	وعلى عكس الأنواع الأخرى من الفيروسات المتنقلة، فإن فيروس الشبكة النموذجي المتنقل ينتشر دون تدخل المستخدم. فهو يفحص الشبكة المحلية لأجهزة الكمبيوتر التي تحتوي على برامج بها ثغرات أمنية. وللقيام بذلك، فهو يقوم بإرسال حزمة شبكة اتصال مكوّنة خصيصًا (فيروس تعطيل الأمان) وتحتوي على رمز الفيروس المتنقل أو جزء منه. في حالة وجود كمبيوتر "به ثغرات أمنية" على الشبكة، فإنه يتلقى حزمة الشبكة هذه. ويتم تنشيط الفيروس المتنقل بمجرد اختراقه التام للكمبيوتر.
P2P-Worm	فيروسات شبكة مشاركة الملفات المتنقلة	تنتشر عبر شبكات مشاركة الملفات من نظير إلى نظير. للتسلل إلى شبكة P2P، يقوم الفيروس المتنقل بنسخ نفسه في مجلد مشاركة ملفات يوجد عادةً في كمبيوتر المستخدم. تعرض شبكة P2P معلومات حول هذا الملف لهذا بطريقة تجعل المستخدم قد "يجد" ملف مصاب على الشبكة مثل أي ملف آخر، ثم يقوم بتنزيله وفتحه. أما الفيروسات المتنقلة الأكثر تعقيدًا فتقوم بمحاكاة بروتوكول شبكة P2P معينة. وتوفر هذه الفيروسات استجابة إيجابية لاستعلامات البحث وعرض نُسخ من نفسها للتنزيل.
Worm	أنواع أخرى من الفيروسات المتنقلة	تتضمن الأنواع الأخرى من الفيروسات المتنقلة: • الفيروسات المتنقلة تنشر نُسخًا من نفسها عبر موارد الشبكة. باستخدام وظائف نظام التشغيل، تقوم بفحص مجلدات الشبكة المتاحة، والاتصال بأجهزة الكمبيوتر على الإنترنت، ومحاولة الحصول على الوصول الكامل إلى محركات الأقراص الخاصة بها. على عكس الأنواع الموضحة مسبقًا من الفيروسات المتنقلة، لا تقوم الأنواع الأخرى من الفيروسات المتنقلة بتفعيل نفسها، ولكن يتم تنشيطها عندما يقوم المستخدم بفتح ملف يحتوي على نسخة منها. • الفيروسات المتنقلة التي لا تستخدم أي من الوسائل المذكورة في الجدول السابق للانتشار (على سبيل المثال، الفيروسات التي تنتشر عبر الهواتف المحمولة).

- **فيروسات حصان طروادة (بما في ذلك برامج طلب الفدية)**:

الفئة الفرعية: فيروسات حصان طروادة

مستوى التهديد: عالي

على عكس الفيروسات التقليدية، لا تقوم برامج حصان طروادة بالنسخ المتماثل لنفسها. على سبيل المثال، فإنها تخترق الكمبيوتر عبر البريد الإلكتروني أو المستعرض عند زيارة المستخدم لصفحة ويب مصابة. يتم بدء برامج حصان طروادة بعد تدخل من المستخدم. تبدأ في اتخاذ إجراءاتها الضارة مباشرة بعد أن يبدأ تشغيلها.

وتعمل برامج حصان طروادة الأخرى بشكل مختلف على أجهزة الكمبيوتر المصابة. تتضمن الوظائف الأساسية لبرامج حصان طروادة منع المعلومات أو تعديلها أو تدميرها، وتعطيل أجهزة الكمبيوتر أو الشبكات. يمكن أيضًا لبرامج حصان طروادة استلام الملفات أو إرسالها، وتشغيلها، وعرض الرسائل على الشاشة، وطلب صفحات الويب، وتنزيل البرامج وتثبيتها، وإعادة تشغيل جهاز الكمبيوتر.

غالبًا ما يستخدم القراصنة "مجموعات" من برامج حصان طروادة.

يوضح الجدول التالي أنواع سلوكيات برامج حصان طروادة.

أنواع سلوكيات برامج حصان طروادة على الكمبيوتر المصاب

النوع	الاسم	الوصف
Trojan-ArcBomb	برامج حصان طروادة – "قنابل الأرشيف"	عند فك حزم الأرشيفات، يزداد حجمها بشكل يؤثر على تشغيل الكمبيوتر. عندما يحاول المستخدم فك حزمة الأرشيف، قد يبدأ الكمبيوتر في العمل ببطء أو يتجمد؛ وقد يتم ملء القرص الثابت ببيانات "فارغة". وتمثل "قنابل الأرشيف" خطورة بالنسبة لخوادم البريد الإلكتروني والملفات على وجه الخصوص. إذا كان الخادم يستخدم نظام تلقائي لمعالجة البيانات الواردة، فإن "قنابل الأرشيف" قد تؤدي إلى توقف عمل الخادم.
Backdoor	برامج حصان طروادة للإدارة عن بُعد	تعتبر أخطر نوع من بين كل أنواع برامج حصان طروادة. ومن حيث وظائفها، فإنها تشبه تطبيقات الإدارة عن بُعد المُثبتة على أجهزة الكمبيوتر. تقوم تلك البرامج بتثبيت نفسها على الكمبيوتر دون أن يلاحظها المستخدم، مما يتيح للدخلاء أن يديروا الكمبيوتر عن بُعد.
Trojan	أحصنة طروادة	تتضمن التطبيقات الضارة التالية: • **برامج حصان طروادة التقليدية**. تقوم تلك البرامج فقط بأداء الوظائف الأساسية لبرامج حصان طروادة: منع المعلومات أو تعديلها أو تدميرها، وتعطيل أجهزة الكمبيوتر أو الشبكات. ولا تتضمن أي ميزات متقدمة على عكس الأنواع الأخرى من برامج حصان طروادة الموضحة في الجدول. • **برامج حصان طروادة متعددة الاستخدامات**. لدى هذه البرامج ميزات متقدمة مطابقة للعديد من أنواع برامج حصان طروادة.
Trojan-Ransom	برامج حصان طروادة للفدية	تقوم هذه البرامج بأخذ معلومات المستخدم "كرهينة" وتقوم بتعديلها أو منعها، أو التأثير على تشغيل الكمبيوتر لكي يفقد المستخدم القدرة على استخدام المعلومات. يطلب الدخيل فدية من المستخدم، مع التعهد بإرسال تطبيق يستعيد أداء الكمبيوتر والبيانات المخزنة عليه.
Trojan-Clicker	الأشخاص الذين ينقرون فوق برامج حصان طروادة	تصل إلى صفحات الويب من كمبيوتر المستخدم، إما بإرسال أوامر إلى المستعرض من تلقاء نفسها أو بتغيير عناوين الويب المحددة في ملفات النظام. باستخدام هذه البرامج، يقوم الدخلاء بهجمات على الشبكة وزيادة زيارات مواقع الويب، مما يزيد من عدد عرض الشعارات الإعلانية.
Trojan-Downloader	برامج حصان طروادة للتنزيل	تصل هذه البرامج إلى صفحة ويب الدخيل، وتقوم بتنزيل تطبيقات ضارة أخرى منها، وتثبيتها على كمبيوتر المستخدم. وقد تتضمن هذه البرامج اسم ملف التطبيق الخبيث لتنزيله أو استلامه من صفحة الويب التي يتم الوصول إليها.
Trojan-Dropper	برامج حصان طروادة للإسقاط	تتضمن برامج حصان طروادة أخرى تقوم بتثبيتها على القرص الثابت. قد يستخدم الدخلاء برامج حصان طروادة للإسقاط من أجل الأهداف التالية: • تثبيت برنامج ضار دور أن يلاحظه المستخدم: لا تعرض تطبيق حصان طروادة للإسقاط أية رسائل، أو أنها تعرض رسائل مزيفة تخبرك على سبيل المثال بوجود خطأ في أرشيف

		أو في إصدار غير متوافق مع نظام التشغيل. • حماية تطبيق خبيث معروف آخر من الاكتشاف: ليس بإمكان جميع برامج مكافحة الفيروسات اكتشاف تطبيق خبيث موجود داخل برامج حصان طروادة للإسقاط.
Trojan-Notifier	برامج حصان طروادة للإخطار	تقوم هذه البرامج بإخطار الدخيل بإمكانية الوصول إلى الكمبيوتر المصاب، وترسل إليه معلومات عن الكمبيوتر: عنوان IP أو عدد المنافذ المفتوحة أو عنوان البريد الإلكتروني. وهي تتصل بالدخيل عبر البريد الإلكتروني أو عن طريق FTP أو عن طريق الوصول إلى صفحة الويب الخاصة بالدخيل أو بأي طريقة أخرى. عادةً ما يتم استخدام برامج حصان طروادة للإخطار في مجموعات تتكون من برامج حصان طروادة متعددة. وهي تخطر الدخيل بنجاح تثبيت برامج حصان طروادة الأخرى على كمبيوتر المستخدم.
Trojan-Proxy	برامج حصان طروادة لخوادم الوكيل	تسمح للدخيل الوصول إلى صفحات الويب بشكل مجهول من خلال استخدام كمبيوتر المستخدم؛ وعادةً ما يتم استخدامها لإرسال رسائل بريد إلكتروني غير مرغوب فيها.
Trojan-PSW	برمجيات سرقة كلمة المرور	تعتبر برمجيات سرقة كلمة المرور نوعًا من برامج حصان طروادة يسرق حسابات المستخدم، مثل بيانات تسجيل البرامج. تعثر برامج حصان طروادة هذه على بيانات الخصوصية في ملفات النظام وفي السجل وإرسالها إلى "المهاجم" عن طريق البريد الإلكتروني، أو عن طريق FTP أو عن طريق الوصول إلى صفحة ويب الدخيل، أو بأي طريقة أخرى. يتم تصنيف بعض فيروسات حصان طروادة هذه إلى أنواع منفصلة موضحة في هذا الجدول. إنها برامج حصان طروادة التي تسرق حسابات البنوك (Trojan-Banker)، وتسرق البيانات من مستخدمي عملاء المراسلة الفورية (Trojan-IM) (IM)، وتسرق المعلومات من مستخدمي ألعاب الإنترنت (Trojan-GameThief).
Trojan-Spy	برامج حصان طروادة للتجسس	تتجسس هذه البرامج على المستخدم بجمع معلومات عن الإجراءات التي يقوم بها أثناء العمل على الكمبيوتر. ويمكن أن تعترض البيانات التي يدخلها المستخدم عن طريق لوحة المفاتيح أو تأخذ لقطات شاشة أو تجمع قوائم بالتطبيقات النشطة. وبعد استلامها للمعلومات، تقوم هذه البرامج بإرسالها إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة ويب الدخيل أو باستخدام طريقة أخرى.
Trojan-DDoS	برامج حصان طروادة للهجوم على الشبكة	تقوم بإرسال العديد من الطلبات من جهاز كمبيوتر المستخدم إلى خادم بعيد. ويفتقر الخادم إلى الموارد اللازمة لمعالجة جميع الطلبات، بحيث يتوقف عن العمل (رفض الخدمة أو DoS ببساطة). غالبًا ما يصيب القراصنة العديد من أجهزة الكمبيوتر بهذه البرامج بحيث يمكنهم استخدامها للهجوم على خادم واحد في نفس الوقت. تقوم برامج رفض الخدمة (DoS) بارتكاب هجوم من جهاز كمبيوتر واحد بمعرفة المستخدم. وتقوم برامج رفض الخدمة الموزعة (DDoS) بارتكاب هجمات موزعة من العديد من أجهزة الكمبيوتر دون أن تتم ملاحظتها من جانب مستخدم جهاز الكمبيوتر المصاب.
Trojan-IM	برامج حصان طروادة التي تسرق معلومات من مستخدمي عملاء المراسلة الفورية (IM)	تسرق أرقام الحسابات وكلمات المرور الخاصة بمستخدمي عملاء المراسلة الفورية (IM). وتقوم هذه البرامج بنقل البيانات إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة ويب الدخيل أو باستخدام طريقة أخرى.
Rootkit	فيروسات الجذر	تقوم هذه الفيروسات بحجب التطبيقات الضارة الأخرى ونشاطها، وبالتالي تطيل من استمرار التطبيق في نظام التشغيل. ويمكن أيضًا أن تقوم بإلغاء ملفات أو عمليات في ذاكرة جهاز كمبيوتر مصاب أو مفاتيح تسجيل تقوم بتشغيل التطبيقات الضارة. كما يمكن أن تقوم فيروسات الجذر بحجب تبادل البيانات بين التطبيقات في جهاز كمبيوتر المستخدم وأجهزة الكمبيوتر الأخرى على شبكة الاتصال.
Trojan-SMS	برامج حصان طروادة في شكل رسائل SMS	تصيب هذه البرامج الهواتف الخلوية وتقوم بإرسال رسائل SMS إلى أرقام الهواتف ذات الأسعار العالية.
Trojan-GameThief	برامج حصان طروادة التي تسرق معلومات من مستخدمي	تسرق هذه البرامج بيانات اعتماد الحساب من مستخدمي الألعاب عبر الإنترنت، ثم تقوم بعد ذلك بإرسال البيانات إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة الويب الخاصة بالدخيل أو باستخدام طريقة أخرى.

	الألعاب عبر الإنترنت	
Trojan-Banker	برامج حصان طروادة التي تسرق حسابات البنوك	تقوم هذه البرامج بسرقة بيانات حسابات البنوك أو بيانات الأنظمة المالية الإلكترونية ثم بعد ذلك ترسل البيانات إلى المتسلل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة الويب الخاصة بالمتسلل أو باستخدام طريقة أخرى.
Trojan-Mailfinder	برامج حصان طروادة التي تجمع عناوين البريد الإلكتروني	تقوم هذه البرامج بجمع عناوين البريد الإلكتروني المخزنة على جهاز كمبيوتر وبإرسالها إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة ويب الدخيل أو باستخدام طريقة أخرى. ويمكن أن يقوم الدخلاء بإرسال بريد إلكتروني غير مرغوب فيه إلى العناوين التي قاموا بجمعها.

- **أدوات خبيثة**:

الفئة الفرعية: الأدوات الخبيثة

مستوى الخطر: متوسط

على عكس الأنواع الأخرى من البرمجيات الضارة، لا تقوم الأدوات الخبيثة بإجراءاتها فور بدء تشغيلها. فيمكن تخزينها بأمان وبدء تشغلها على كمبيوتر المستخدم. وغالبًا ما يستخدم الدخلاء ميزات هذه البرامج لإنشاء فيروسات وفيروسات دودة وبرامج حصان طروادة أو القيام بهجمات الشبكة على الخوادم البعيدة أو قرصنة أجهزة كمبيوتر أو القيام بأنشطة ضارة أخرى.

يتم تصنيف مختلف ميزات الأدوات الخبيثة وفقًا للأنواع الوارد وصفها في الجدول التالي.

خصائص الأدوات الخبيثة

النوع	الاسم	الوصف
Constructor	دوال إنشائية	تسمح بإنشاء فيروسات وفيروسات دودة وبرامج حصان طروادة جديدة. يتباهى بعض منشئ الفيروسات بأن لديهم واجهة نوافذ قياسية يمكن للمستخدم أن يقوم فيها بتحديد نوع التطبيق الخبيث المطلوب إنشائه وطريقة مقاومة المصححين وغير ذلك من الخصائص.
Dos	هجمات شبكة الاتصال	تقوم بإرسال العديد من الطلبات من جهاز كمبيوتر المستخدم إلى خادم بعيد. ويفتقر الخادم إلى الموارد اللازمة لمعالجة جميع الطلبات، بحيث يتوقف عن العمل (رفض الخدمة أو DoS ببساطة).
Exploit	فيروسات معطلة للأمان	فيروس الاستغلال عبارة عن مجموعة من البيانات أو رمز برنامج يستخدم ثغرات أمنية بالتطبيق الذي تتم معالجته فيه، لأجل القيام بإجراء خبيث على الكمبيوتر. فعلى سبيل المثال، يمكن للفيروس المعطل للأمان كتابة أو قراءة الملفات أو طلب صفحات ويب "مصابة". تستخدم الفيروسات المعطلة للأمان المختلفة ثغرات أمنية في خدمات شبكة اتصال أو تطبيقات مختلفة. ويتم إرسال الفيروسات المعطلة للأمان مخفيةً على هيئة حزمة شبكة اتصال إلى أجهزة كمبيوتر متعددة عبر الشبكة، بحثًا عن أجهزة كمبيوتر بها خدمات شبكة اتصال قابلة للاختراق. ويستخدم الفيروس المعطل للأمان الموجود في ملف DOC ثغرات أمنية لمحرر نصوص. وقد يبدأ هذا الفيروس بتنفيذ إجراءات مبرمجة من قبل أحد القراصنة عند قيام المستخدم بفتح ملف مصاب. ويبحث الفيروس المعطل للأمان المضمن في رسالة بريد إلكتروني عن ثغرات أمنية في أي من عملاء البريد الإلكتروني. وقد يبدأ بتنفيذ إجراء خبيث بمجرد فتح المستخدم للرسالة المصابة في عميل البريد الإلكتروني هذا. تنتشر فيروسات دودة الشبكة عبر الشبكات باستخدام الفيروسات المعطلة للأمان. ففيروسات الاستغلال عبارة عن حزم شبكة تقوم بتعطيل أجهزة الكمبيوتر.
FileCryptor	مشفرون	تقوم بترميز التطبيقات الضارة الأخرى لإخفائها من تطبيق مكافحة الفيروسات.
Flooder	برامج "لتلويث" شبكات الاتصال	تقوم بإرسال العديد من الرسائل عبر قنوات شبكة الاتصال. ويتضمن هذا النوع من الأدوات، على سبيل المثال، برامج تلوث المحادثات عبر الإنترنت. لا تتضمن الأدوات التي من هذا النوع من الفيروسات أي برامج "تلوث" القنوات المستخدمة بواسطة البريد الإلكتروني وعملاء المراسلة الفورية (IM) وأنظمة الاتصالات المتنقلة. ويتم تمييز هذه البرامج على أنها أنواع مستقلة وارد وصفها في هذا الجدول (فيروسات فيضان البريد الإلكتروني وفيروس إرسال كميات ضخمة من المراسلات الفورية المراسلات الفورية وفيروسات فيضان رسائل SMS).
HackTool	أدوات قرصنة	تتيح التسلل إلى الكمبيوتر الذي يتم تثبيتها عليه، أو مهاجمة كمبيوتر آخر (على سبيل المثال، عن طريق إضافة حسابات جديدة بالنظام دون إذن المستخدم، أو عن طريق مسح سجلات النظام لإخفاء ما يدل على وجودها في نظام التشغيل). ويتضمن هذا النوع من الأدوات بعض برامج مراقبة الشبكة التي تتميز بوظائف ضارة، منها على سبيل المثال اعتراض كلمات المرور. وبرامج مراقبة الشبكة هي عبارة عن برامج تسمح بإمكانية عرض حركة مرور الشبكة.
Hoax	برامج خداعية	تخطر المستخدم برسائل تشبه الفيروسات: وقد "تكتشف فيروسًا" في ملف غير مصاب وتخطر المستخدم بأنه تم تنسيق القرص على الرغم من عدم حدوث ذلك في الواقع.
Spoofer	أدوات محاكاة	ترسل رسائل وطلبات شبكة اتصال بعنوان مزيف للمرسل. ويستخدم الدخلاء أدوات من نوع محاكي المستخدم المصرح له لإظهار أنفسهم كمرسلين حقيقيين للرسائل على سبيل المثال.
VirTool	أدوات تعدل	وهي تسمح بتعديل البرمجيات الضارة الأخرى، مع إخفائها من تطبيقات مكافحة الفيروسات.

	التطبيقات الضارة	
Email-Flooder	برامج "تلوث" عناوين البريد الإلكتروني	ترسل العديد من الرسائل إلى عناوين بريد إلكتروني مختلفة، وبالتالي يتم "تلويثها". ويمنع وجود قدر كبير من الرسائل الواردة المستخدمين من عرض الرسائل المفيدة في صناديق الوارد الخاصة بهم.
IM-Flooder	برامج تؤدي إلى تلوث حركة عملاء المراسلة الفورية	وهي تغمر مستخدمي عملاء المراسلة الفورية (IM) بالرسائل. ويمنع وجود قدر كبير من الرسائل المستخدمين من عرض الرسائل الواردة المفيدة.
SMS-Flooder	برامج "تلوث" الحركة برسائل SMS	ترسل العديد من رسائل SMS إلى الهواتف الخلوية.

- **برمجيات إعلانية**:

الفئة الفرعية: البرامج الإعلانية (Adware)؛

مستوى التهديد: متوسط

البرمجيات الإعلانية هي برمجيات تعرض معلومات إعلانية للمستخدم. وتقوم البرامج الإعلانية بعرض شعارات إعلانية في واجهات برامج أخرى وتعيد توجيه استعلامات البحث إلى مواقع ويب إعلانية. وتقوم بعضها بجمع معلومات تسويقية عن المستخدم وإرسالها إلى المطور: وقد تتضمن هذه المعلومات أسماء مواقع الويب التي تمت زيارتها من جانب المستخدم أو محتوى استعلامات البحث الخاصة به. وعلى عكس برامج حصان طروادة-Spy، ترسل البرامج الإعلانية هذه المعلومات إلى المطور بإذن المستخدم.

- **برامج الاتصال التلقائي**:

الفئة الفرعية: البرامج القانونية التي يمكن أن يستخدمها المجرمون لإتلاف الكمبيوتر أو بياناتك الشخصية.

مستوي الخطر: متوسط

معظم هذه التطبيقات مفيدة، ولذلك يقوم الكثير من المستخدمين بتشغيلها. تتضمن هذه التطبيقات عملاء المحادثة عبر الإنترنت (IRC)، وبرامج الاتصال التلقائي، وبرامج تنزيل الملفات، وبرامج مراقبة أنشطة نظام الكمبيوتر، والأدوات المساعدة لكلمات المرور، وخوادم الإنترنت لشبكات FTP وHTTP وTelnet.

ومع ذلك، إذا تمكن الدخلاء من الوصول إلى هذه البرامج أو إذا زرعوها على كمبيوتر المستخدم، قد يتم استخدام هذه ميزات التطبيق لانتهاك الأمان.

تختلف هذه التطبيقات حسب الوظيفة؛ ويتم توضيح أنواعها في الجدول التالي.

النوع	الاسم	الوصف
Client-IRC	عملاء المحادثة عبر الإنترنت	يقوم المستخدمين بتثبيت هذه البرامج للتحدث مع آخرين عبر الإنترنت. ويستخدمها الدخلاء لنشر البرمجيات الضارة.
Dialer	برامج الاتصال التلقائي	يمكنها إجراء اتصالات عبر الهاتف عن طريق مودم في الوضع "مخفي".
Downloader	برامج التنزيل	يتمكنون من تحميل الملفات من صفحات الإنترنت في الوضع "مخفي".
Monitor	برامج للمراقبة	تسمح تلك البرامج بنشاط المراقبة على جهاز الكمبيوتر الذي تم تثبيتها عليه (مما يؤدي إلى معرفة التطبيقات قيد التشغيل وكيف تتبادل البيانات مع التطبيقات المثبتة على أجهزة الكمبيوتر الأخرى).
PSWTool	أدوات استعادة كلمات المرور	تسمح بعرض واستعادة كلمات المرور المنسية. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض.
RemoteAdmin	برامج الإدارة عن بعد	يتم استخدامها على نطاق واسع من قبل مديري النظام. وتسمح هذه البرامج بالوصول إلى واجهة كمبيوتر بعيد لمراقبته وإدارته. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض: لمراقبة أجهزة الكمبيوتر البعيدة وإدارتها. تختلف برامج الإدارة عن بُعد القانونية عن برامج حصان طروادة من نوع الباب الخلفي للإدارة عن بُعد. تتوفر لدى برامج حصان طروادة القدرة على اختراق نظام التشغيل بشكل مستقل وتثبيت نفسها؛ بينما لا يمكن للبرامج القانونية القيام بذلك.
Server-FTP	خوادم FTP	تعمل كخوادم FTP. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول FTP.
Server-Proxy	خوادم الوكيل	تعمل كخوادم وكيلة. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
Server-Telnet	خوادم Telnet	تعمل كخوادم Telnet. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول Telnet.
Server-Web	خوادم الويب	تعمل كخوادم ويب. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول HTTP.
RiskTool	أدوات للعمل على كمبيوتر محلي	تزود المستخدم بخيارات إضافية أثناء العمل على الكمبيوتر الخاص به. وتسمح هذه الأدوات للمستخدم بإخفاء الملفات أو نوافذ التطبيقات قيد التشغيل وإنهاء العمليات قيد التشغيل.
NetTool	أداوت شبكة	تزود المستخدم بخيارات إضافية أثناء العمل على أجهزة كمبيوتر أخرى على الشبكة. وتسمح هذه الأدوات بإعادة تشغيلها واكتشاف المنافذ المفتوحة وبدء تشغيل التطبيق المثبتة على أجهزة

	الاتصال	الكمبيوتر.
Client-P2P	عملاء شبكة اتصال النظراء P2P	تسمح بالعمل على شبكات الاتصال من نظير إلى نظير. ويمكن أن يستخدمها الدخلاء لنشر البرمجيات الضارة.
Client-SMTP	عملاء SMTP	يرسلون رسائل بريد إلكترونية دون علم المستخدم. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
WebToolbar	أشرطة أدوات الويب	تضيف أشرطة أدوات إلى واجهات التطبيقات الأخرى لاستخدام محركات البحث.
FraudTool	برامج زائفة	تظهر نفسها في هيئة برامج أخرى. على سبيل المثال، توجد برامج زائفة لحماية ضد الفيروسات تعرض رسائل حول اكتشاف البرمجيات الضارة. برغم ذلك، فإنها لا تكتشف في الواقع أي شيء أو تنظفه.

- **اكتشاف برامج قانونية أخرى يمكن أن يستخدمها المجرمون لإتلاف جهازك أو بياناتك الشخصية**؛

الفئة الفرعية: البرامج القانونية التي يمكن أن يستخدمها المجرمون لإتلاف الكمبيوتر أو بياناتك الشخصية.

مستوى الخطر: متوسط

معظم هذه التطبيقات مفيدة، ولذلك يقوم الكثير من المستخدمين بتشغيلها. تتضمن هذه التطبيقات عملاء المحادثة عبر الإنترنت (IRC)، وبرامج الاتصال التلقائي، وبرامج تنزيل الملفات، وبرامج مراقبة أنشطة نظام الكمبيوتر، والأدوات المساعدة لكلمات المرور، وخوادم الإنترنت لشبكات FTP وHTTP وTelnet.

ومع ذلك، إذا تمكن الدخلاء من الوصول إلى هذه البرامج أو إذا زرعوها على كمبيوتر المستخدم، قد يتم استخدام هذه ميزات التطبيق لانتهاك الأمان.

تختلف هذه التطبيقات حسب الوظيفة؛ ويتم توضيح أنواعها في الجدول التالي.

النوع	الاسم	الوصف
Client-IRC	عملاء المحادثة عبر الإنترنت	يقوم المستخدمين بتثبيت هذه البرامج للتحدث مع آخرين عبر الإنترنت. ويستخدمها الدخلاء لنشر البرمجيات الضارة.
Dialer	برامج الاتصال التلقائي	يمكنها إجراء اتصالات عبر الهاتف عن طريق مودم في الوضع "مخفي".
Downloader	برامج التنزيل	يتمكنون من تحميل الملفات من صفحات الإنترنت في الوضع "مخفي".
Monitor	برامج للمراقبة	تسمح تلك البرامج بنشاط المراقبة على جهاز الكمبيوتر الذي تم تثبيتها عليه (مما يؤدي إلى معرفة التطبيقات قيد التشغيل وكيف تتبادل البيانات مع التطبيقات المثبتة على أجهزة الكمبيوتر الأخرى).
PSWTool	أدوات استعادة كلمات المرور	تسمح بعرض واستعادة كلمات المرور المنسية. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض.
RemoteAdmin	برامج الإدارة عن بعد	يتم استخدامها على نطاق واسع من قبل مديري النظام. وتسمح هذه البرامج بالوصول إلى واجهة كمبيوتر بعيد لمراقبته وإدارته. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض: لمراقبة أجهزة الكمبيوتر البعيدة وإدارتها. تختلف برامج الإدارة عن بُعد القانونية عن برامج حصان طروادة من نوع الباب الخلفي للإدارة عن بُعد. تتوفر لدى برامج حصان طروادة القدرة على اختراق نظام التشغيل بشكل مستقل وتثبيت نفسها؛ بينما لا يمكن للبرامج القانونية القيام بذلك.
Server-FTP	خوادم FTP	تعمل كخوادم FTP. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول FTP.
Server-Proxy	خوادم الوكيل	تعمل كخوادم وكيلة. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
Server-Telnet	خوادم Telnet	تعمل كخوادم Telnet. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول Telnet.
Server-Web	خوادم الويب	تعمل كخوادم ويب. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول HTTP.
RiskTool	أدوات للعمل على كمبيوتر محلي	تزود المستخدم بخيارات إضافية أثناء العمل على الكمبيوتر الخاص به. وتسمح هذه الأدوات للمستخدم بإخفاء الملفات أو نوافذ التطبيقات قيد التشغيل وإنهاء العمليات قيد التشغيل.
NetTool	أداوت شبكة	تزود المستخدم بخيارات إضافية أثناء العمل على أجهزة كمبيوتر أخرى على الشبكة. وتسمح هذه الأدوات بإعادة تشغيلها واكتشاف المنافذ المفتوحة وبدء تشغيل التطبيق المثبتة على أجهزة

	الاتصال	الكمبيوتر.
Client-P2P	عملاء شبكة اتصال النظراء P2P	تسمح بالعمل على شبكات الاتصال من نظير إلى نظير. ويمكن أن يستخدمها الدخلاء لنشر البرمجيات الضارة.
Client-SMTP	عملاء SMTP	يرسلون رسائل بريد إلكترونية دون علم المستخدم. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
WebToolbar	أشرطة أدوات الويب	تضيف أشرطة أدوات إلى واجهات التطبيقات الأخرى لاستخدام محركات البحث.
FraudTool	برامج زائفة	تظهر نفسها في هيئة برامج أخرى. على سبيل المثال، توجد برامج زائفة لحماية ضد الفيروسات تعرض رسائل حول اكتشاف البرمجيات الضارة. برغم ذلك، فإنها لا تكتشف في الواقع أي شيء أو تنظفه.

- **كائنات مضغوطة قد يُستخدم الضغط الخاص بها لحماية التعليمات البرمجية الخبيثة**:

يقوم Kaspersky Endpoint Security بمسح الكائنات المضغوطة والوحدة النمطية لفك الحزمة داخل الأرشيفات ذاتية الاستخراج (SFX).

لإخفاء البرامج الخطرة من تطبيقات مكافحة الفيروسات، يقوم الدخلاء بأرشفتها باستخدام منشئي حزم خاصة أو إنشاء الملفات متعددة الحزم.

حدد محللو الفيروسات في Kaspersky برامج الحزم الأكثر شيوعًا بين القراصنة.

إذا اكتشف Kaspersky Endpoint Security وجود أحد برامج الحزم من هذا النوع في ملف، فيكون من الأرجح أن يحتوي هذا الملف على تطبيق ضار أو تطبيق ربما يتم استخدامه بواسطة المجرمين للإضرار بالكمبيوتر أو بياناتك الشخصية.

ينتقي Kaspersky Endpoint Security الأنواع التالية من البرامج:

- الملفات المضغوطة التي قد تسبب ضررًا – يتم استخدامها لحزم البرمجيات الضارة مثل الفيروسات التقليدية والفيروسات المتنقلة وبرامج حصان طروادة.
- الملفات متعددة الحزم (مستوى التهديد المتوسط) – تم حزم الكائن ثلاث مرات بواسطة واحد أو أكثر من برامج الحزم.

- **الكائنات متعددة الضغط**.

يقوم Kaspersky Endpoint Security بمسح الكائنات المضغوطة والوحدة النمطية لفك الحزمة داخل الأرشيفات ذاتية الاستخراج (SFX).

لإخفاء البرامج الخطرة من تطبيقات مكافحة الفيروسات، يقوم الدخلاء بأرشفتها باستخدام منشئي حزم خاصة أو إنشاء الملفات متعددة الحزم.

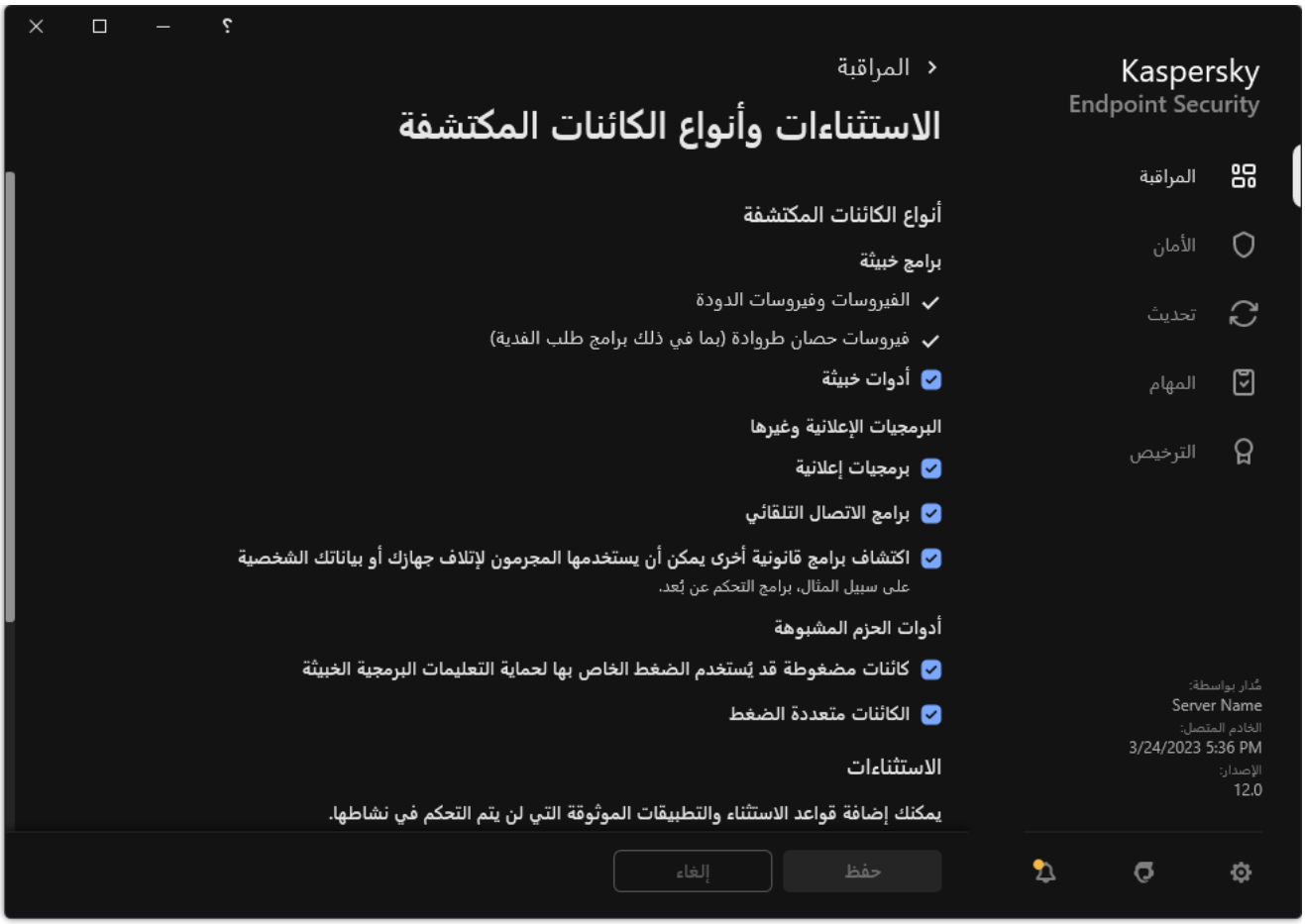
حدد محللو الفيروسات في Kaspersky برامج الحزم الأكثر شيوعًا بين القراصنة.

إذا اكتشف Kaspersky Endpoint Security وجود أحد برامج الحزم من هذا النوع في ملف، فيكون من الأرجح أن يحتوي هذا الملف على تطبيق ضار أو تطبيق ربما يتم استخدامه بواسطة المجرمين للإضرار بالكمبيوتر أو بياناتك الشخصية.

ينتقي Kaspersky Endpoint Security الأنواع التالية من البرامج:

- الملفات المضغوطة التي قد تسبب ضررًا – يتم استخدامها لحزم البرمجيات الضارة مثل الفيروسات التقليدية والفيروسات المتنقلة وبرامج حصان طروادة.
- الملفات متعددة الحزم (مستوى التهديد المتوسط) – تم حزم الكائن ثلاث مرات بواسطة واحد أو أكثر من برامج الحزم.

4. احفظ تغييراتك.



أنواع الكائنات القابلة للاكتشاف

تحرير قائمة التطبيقات الموثوقة

قائمة التطبيقات الموثوقة عبارة عن قائمة تطبيقات لا يتم مراقبة نشاط الملف والشبكة (بما في ذلك النشاط الخبيث) والوصول إلى سجل النظام بواسطة Kaspersky Endpoint Security. افتراضيًا، يراقب برنامج Kaspersky Endpoint Security الكائنات التي يتم فتحها أو تشغيلها أو حفظها بواسطة أي عملية تطبيق، ويراقب نشاط كل التطبيقات وحركة الشبكة التي تنشئها هذه التطبيقات. بعد إضافة تطبيق إلى قائمة التطبيقات الموثوقة، يتوقف Kaspersky Endpoint Security عن مراقبة نشاط التطبيقات.

يتمثل الاختلاف بين استثناءات الفحص والتطبيقات الموثوقة أنه بالنسبة للاستثناءات لا يفحص Kaspersky Endpoint Security الملفات، بينما بالنسبة للتطبيقات الموثوقة، فإنه لا يتحكم في العمليات التي بدأت. وإذا أنشأ تطبيق موثوق ملفًا ضارًا في مجلد غير مُضمن في استثناءات الفحص، سيكتشف Kaspersky Endpoint Security الملف ويزيل التهديد. وإذا تمت إضافة المجلد إلى الاستثناءات، سيتخطى Kaspersky Endpoint Security هذا الملف.

على سبيل المثال، إذا اعتبرتَ أن الكائنات التي يتم استخدامها بواسطة تطبيق Microsoft Windows Notepad القياسي آمنة، بمعنى أنك تثق في هذا التطبيق، يمكنك إضافة Microsoft Windows Notepad إلى قائمة التطبيقات الموثوقة بحيث لا تتم مراقبة الكائنات المستخدمة بواسطة هذا التطبيق. وسيؤدي ذلك إلى زيادة أداء الكمبيوتر، وهو أمر مهم خاصة عند استخدام تطبيقات الخادم.

بالإضافة إلى ذلك، قد تكون بعض التطبيقات التي تم تصنيفها بواسطة Kaspersky Endpoint Security كتطبيقات ضارة آمنة في سياق الوظائف المتوفرة بعدد من التطبيقات. على سبيل المثال، يكون اعتراض النص الذي تمت كتابته من لوحة المفاتيح عملية روتينية لتطبيقات تبديل تخطيط لوحة المفاتيح تلقائيًا (مثل Punto Switcher). لتقديم تفاصيل هذه البرامج واستثناء نشاطها من المراقبة، نوصي بإضافة هذه التطبيقات إلى قائمة التطبيقات الموثوقة.

تساعد التطبيقات الموثوقة على تجنب مشكلات التوافق بين Kaspersky Endpoint Security والتطبيقات الأخرى (على سبيل المثال، مشكلة الفحص المزدوج لحركة شبكة الاتصال لجهاز كمبيوتر تابع لجهة خارجية بواسطة Kaspersky Endpoint Security وتطبيق آخر لمكافحة الفيروسات).

في نفس الوقت، يستمر فحص الملف التنفيذي وعملية التطبيق الموثوق للبحث عن الفيروسات والبرمجيات الضارة الأخرى. يمكن استثناء تطبيق بالكامل من فحص Kaspersky Endpoint Security عن طريق استثناءات من الفحص.

كيفية إضافة تطبيق إلى القائمة الموثوقة في وحدة التحكم الإدارية (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات**.

5. في القسم **استثناءات من الفحص والتطبيقات الموثوقة**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، حدد القسم **التطبيقات الموثوقة**.

   يفتح هذا نافذة تحتوي على قائمة بالتطبيقات الموثوقة.

7. حدد خانة الاختيار **دمج القيم عند التوريث** إذا كنت ترغب في إنشاء قائمة موحدة بالتطبيقات الموثوقة لجميع أجهزة الكمبيوتر في الشركة. سيتم دمج قوائم التطبيقات الموثوقة في السياسات الأصلية والفرعية. سيتم دمج القوائم بشرط أن تكون قيم الدمج مفعلة عند التوريث. التطبيقات الموثوقة من السياسة الأصلية ستصبح معروضة في السياسات الفرعية في عرض القراءة فقط. تغيير التطبيقات الموثوقة أو حذفها من السياسة الرئيسية أمر غير ممكن.

8. حدد خانة الاختيار **السماح باستخدام التطبيقات الموثوقة المحلية** إذا كنت تريد تمكين المستخدم من إنشاء قائمة محلية بالتطبيقات الموثوقة. بهذه الطريقة، يستطيع المستخدم إنشاء القائمة المحلية الخاصة للتطبيقات الموثوقة بالإضافة إلى القائمة العامة للتطبيقات الموثوقة التي يتم إنشاؤها في السياسة. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر.

   في حالة إلغاء تحديد خانة الاختيار، لا يستطيع المستخدم الوصول سوى إلى القائمة العامة للتطبيقات الموثوقة التي يتم إنشاؤها في السياسة.

9. انقر على **إضافة**.

10. في النافذة التي تفتح، أدخل المسار إلى الملف القابل للتنفيذ للتطبيق الموثوق (انظر الشكل أدناه).

    يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

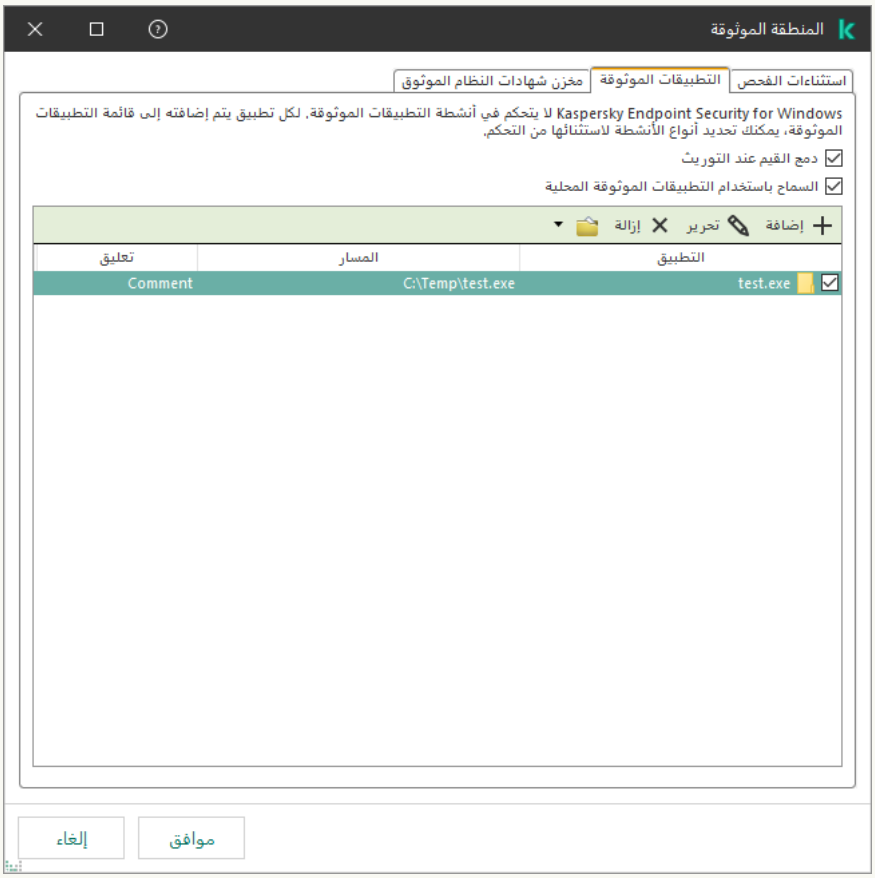
لا يدعم Kaspersky Endpoint Security متغير البيئة `%userprofile%` عند توليد قائمة بالتطبيقات الموثوقة على وحدة تحكم Kaspersky Security Center. ولتطبيق الإدخال على كل حسابات المستخدمين، يمكنك استخدام الحرف * (على سبيل المثال، `C:\Users\*\Documents\File.exe`). كلما أضفت متغير بيئة جديدًا، فأنت بحاجة إلى إعادة تشغيل التطبيق.

إعدادات التطبيق الموثوق

11. قم بتكوين الإعدادات المتقدمة للتطبيق الموثوق به (انظر الجدول أدناه).

12. يمكنك استخدام مربع الاختيار لاستثناء تطبيق من المنطقة الموثوقة في أي وقت (انظر الشكل أدناه).

13. احفظ تغييراتك.



قائمة التطبيقات الموثوقة

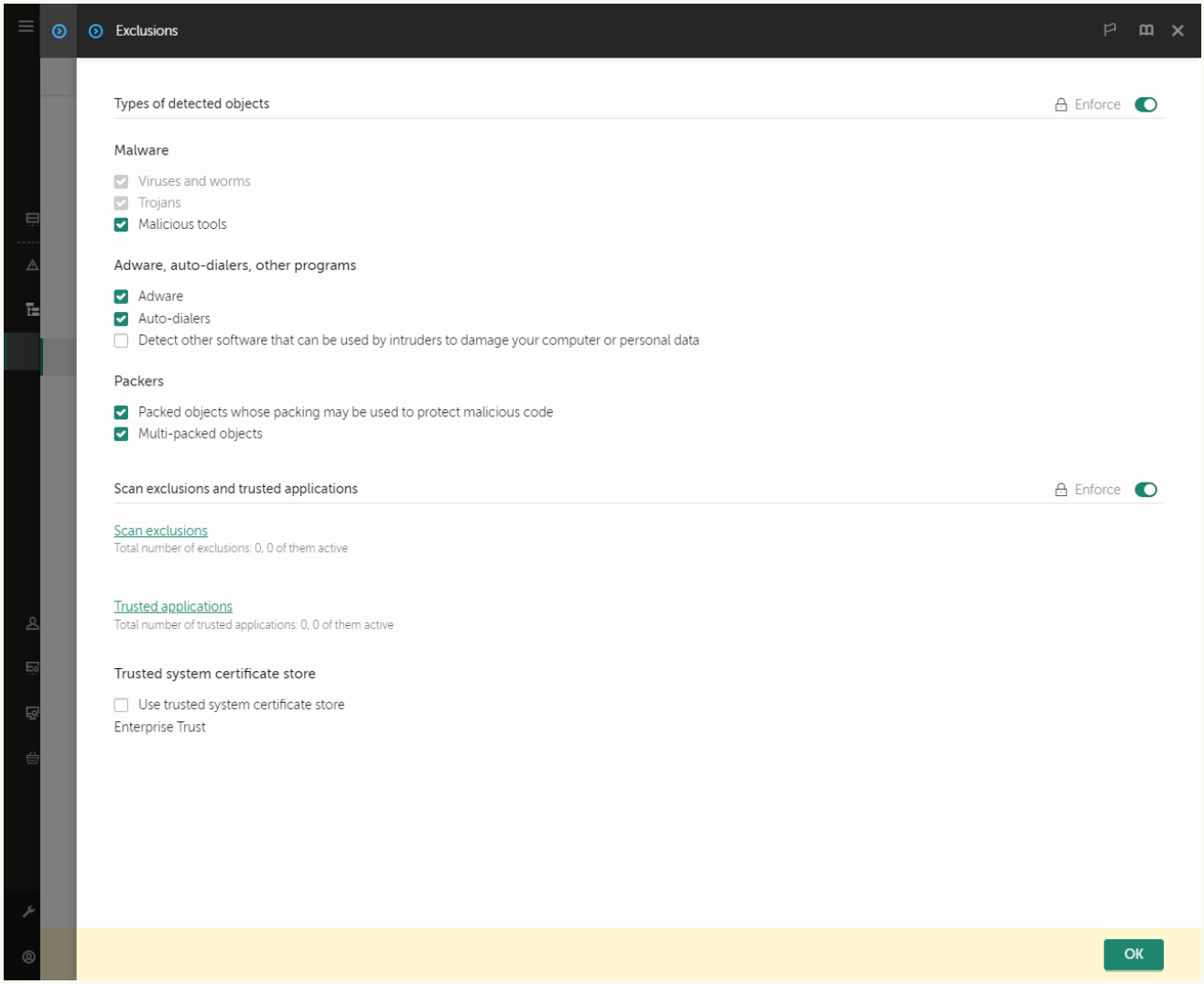
[كيفية إضافة تطبيق إلى القائمة الموثوقة في Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Exclusions and types of detected objects**.



إعدادات الاستثناءات

5. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Trusted applications**.
يفتح هذا نافذة تحتوي على قائمة بالتطبيقات الموثوقة.

6. حدد خانة الاختيار **Merge values when inheriting** إذا كنت ترغب في إنشاء قائمة موحدة بالتطبيقات الموثوقة لجميع أجهزة الكمبيوتر في الشركة. سيتم دمج قوائم التطبيقات الموثوقة في السياسات الأصلية والفرعية. سيتم دمج القوائم بشرط أن تكون قيم الدمج مفعلة عند التوريث. التطبيقات الموثوقة من السياسة الأصلية ستصبح معروضة في السياسات الفرعية في عرض القراءة فقط. تغيير التطبيقات الموثوقة أو حذفها من السياسة الرئيسية أمر غير ممكن.

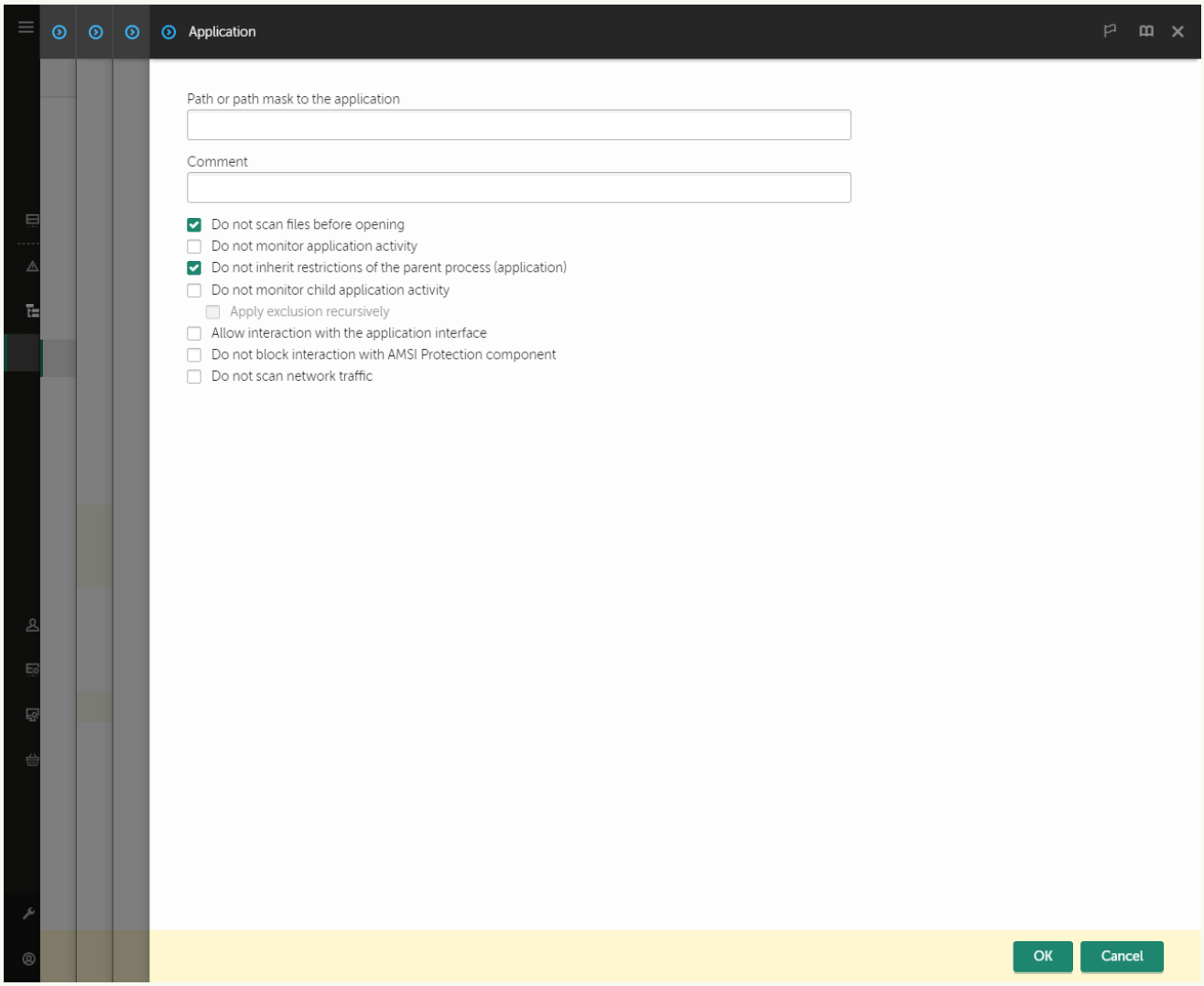
7. حدد خانة الاختيار **Allow use of local trusted applications** إذا كنت تريد تمكين المستخدم من إنشاء قائمة محلية بالتطبيقات الموثوقة. بهذه الطريقة، يستطيع المستخدم إنشاء القائمة المحلية الخاصة للتطبيقات الموثوقة بالإضافة إلى القائمة العامة للتطبيقات الموثوقة التي يتم إنشاؤها في السياسة. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر.
في حالة إلغاء تحديد خانة الاختيار، لا يستطيع المستخدم الوصول سوى إلى القائمة العامة للتطبيقات الموثوقة التي يتم إنشاؤها في السياسة.

8. انقر فوق الزر **إضافة**.

9. في النافذة التي تفتح، أدخل المسار إلى الملف القابل للتنفيذ للتطبيق الموثوق (انظر الشكل أدناه).

يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

لا يدعم Kaspersky Endpoint Security متغير البيئة `%userprofile%` عند توليد قائمة بالتطبيقات الموثوقة على وحدة تحكم Kaspersky Security Center. ولتطبيق الإدخال على كل حسابات المستخدمين، يمكنك استخدام الحرف * (على سبيل المثال، `C:\Users\*\Documents\File.exe`). كلما أضفت متغير بيئة جديدًا، فأنت بحاجة إلى إعادة تشغيل التطبيق.



إعدادات التطبيق الموثوق

10. قم بتكوين الإعدادات المتقدمة للتطبيق الموثوق به (انظر الجدول أدناه).

11. يمكنك استخدام مربع الاختيار لاستثناء تطبيق من المنطقة الموثوقة في أي وقت (انظر الشكل أدناه).

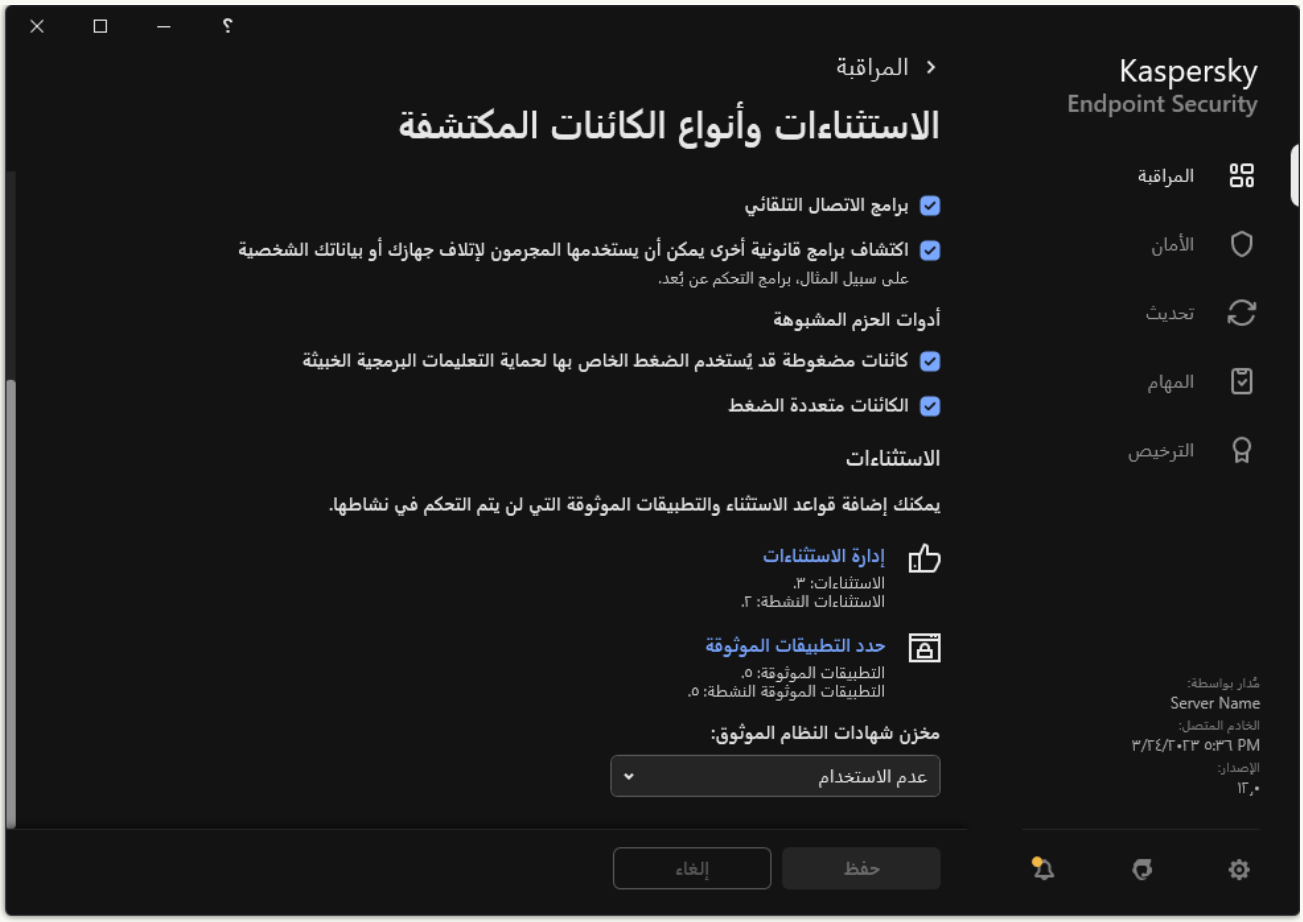
12. احفظ تغييراتك.

كيفية إضافة تطبيق إلى القائمة الموثوقة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة ← الاستثناءات وأنواع الكائنات المكتشفة**.

3. في القسم **الاستثناءات**، انقر على الرابط **حدد التطبيقات الموثوقة**.



إعدادات الاستثناءات

4. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

5. حدد الملف القابل للتنفيذ للتطبيق الموثوق.

يمكنك أيضًا إدخال المسار يدويًا. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

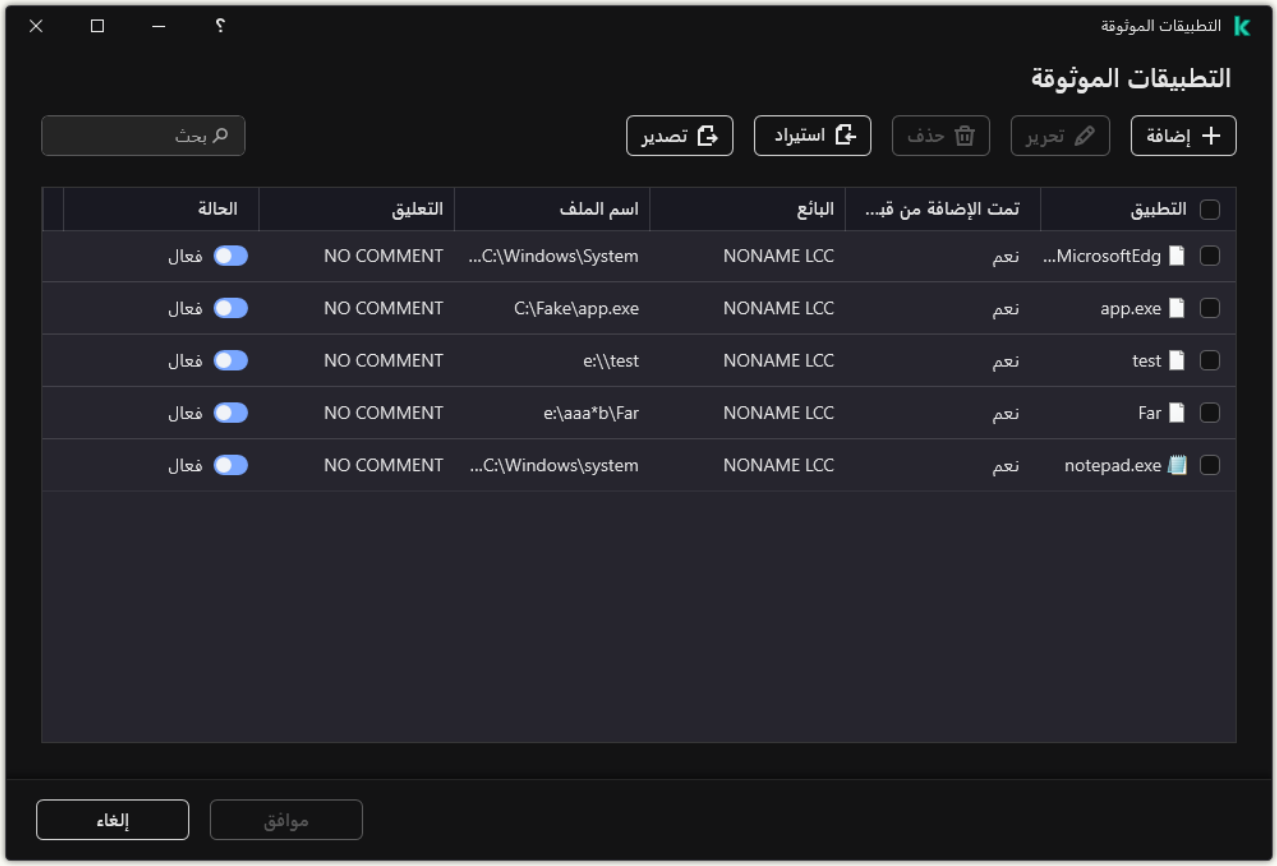
يدعم Kaspersky Endpoint Security متغيرات البيئة ويحول المسار في الواجهة المحلية للتطبيق. بعبارة أخرى، إذا أدخلت مسار الملف `%userprofile%\Documents\File.exe`، يتم إضافة سجل `C:\Users\Fred123\Documents\File.exe` في الواجهة المحلية للتطبيق للمستخدم Fred123. ووفقًا لذلك، يتجاهل Kaspersky Endpoint Security البرنامج الموثوق `File.exe` للمستخدمين الآخرين. ولتطبيق الإدخال على كل حسابات المستخدمين، يمكنك استخدام الحرف `*` (على سبيل المثال، `C:\Users\*\Documents\File.exe`).

كلما أضفت متغير بيئة جديدًا، فأنت بحاجة إلى إعادة تشغيل التطبيق.

6. في نافذة خصائص التطبيق الموثوق، كوّن الإعدادات المتقدمة (انظر الجدول أدناه).

7. يمكنك استخدام مفتاح التبديل لاستثناء تطبيق من المنطقة الموثوقة في أي وقت (انظر الشكل أدناه).

8. احفظ تغييراتك.



قائمة التطبيقات الموثوقة

إعدادات التطبيق الموثوق

المعلمة	الوصف
عدم فحص الملفات قبل الفتح	يتم استثناء كل الملفات المفتوحة بواسطة التطبيق من عمليات الفحص بواسطة Kaspersky Endpoint Security. على سبيل المثال، إذا كنت تستخدم تطبيقات لنسخ الملفات احتياطيًا، فتساعد هذه الميزة في تقليل استهلاك الموارد بواسطة Kaspersky Endpoint Security.
عدم مراقبة نشاط التطبيق	لن يراقب Kaspersky Endpoint Security نشاط الملف والشبكة الخاص بالتطبيق في نظام التشغيل. تتم مراقبة نشاط التطبيق من خلال المكونات التالية: اكتشاف السلوك ومنع الاستغلال ومنع اختراق المضيف ومحرك المعالجة وجدار الحماية.
عدم وراثة القيود من العملية الأصلية (للتطبيق)	لن يتم تطبيق القيود التي تم تكوينها للعملية الرئيسية بواسطة Kaspersky Endpoint Security على عملية فرعية. تبدأ العملية الأصلية بواسطة تطبيق تم تكوين حقوق التطبيق (منع اختراق المضيف) وقواعد الشبكة للتطبيق (جدار الحماية) له.
عدم مراقبة نشاط التطبيق التابع	لن يراقب Kaspersky Endpoint Security نشاط الملف ونشاط الشبكة للتطبيقات التي يتم بدء تشغيلها بواسطة التطبيق.
السماح بالتفاعل مع واجهة التطبيق	يمنع الدفاع الذاتي في Kaspersky Endpoint Security جميع محاولات إدارة خدمات التطبيقات من كمبيوتر بعيد. في حالة تحديد خانة الاختيار، يتم السماح بتطبيق الوصول عن بعد عن طريق إدارة إعدادات Kaspersky Endpoint Security من خلال واجهة Kaspersky Endpoint Security.
عدم منع التفاعل مع مكون حماية AMSI	لن يراقب Kaspersky Endpoint Security طلبات التطبيق الموثوق للكائنات التي سيتم فحصها بواسطة مكون حماية AMSI.
عدم جمع بيانات القياس عن بعد للإدخال التفاعلي لوحدة التحكم	لا يرسل Kaspersky Endpoint Security بيانات القياس عن بُعد عن إدارة التطبيق على وحدة التحكم. ويتم استخدام بيانات القياس عن بعد بواسطة Kaspersky Anti Targeted Attack Platform (EDR).
عدم فحص حركة شبكة الاتصال	سيتم استثناء حركة شبكة الاتصال التي بدأها التطبيق من عمليات الفحص بواسطة Kaspersky Endpoint Security. يمكنك استثناء كل حركة المرور أو حركة المرور المشفرة فقط من عمليات الفحص. يمكنك أيضًا استثناء عناوين IP فردية وأرقام المنافذ من عمليات الفحص.

التعليق	إذا لزم الأمر، يمكنك تقديم تعليق موجز للتطبيق الموثوق. تساعد التعليقات في تبسيط عمليات البحث وفرز التطبيقات الموثوقة.
الحالة	حالة التطبيق الموثوق: • تعني الحالة **فعال** أن التطبيق موجود في المنطقة الموثوقة. • تعني الحالة **غير فعال** أن التطبيق مستثنى من المنطقة الموثوقة.

تصدير واستيراد المنطقة الموثوقة

تُعد المنطقة الموثوقة بمثابة قائمة يتم تكوينها بواسطة مسؤول النظام تضم كائنات وتطبيقات لا يقوم Kaspersky Endpoint Security بمراقبتها عندما يكون نشطًا. تتكون المنطقة الموثوقة من القوائم التالية: scan exclusions وtrusted applications. ويمكنك تصدير هذه القوائم إلى ملفات XML وتنسيقات أخرى. ثم يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من الاستثناءات من النوع نفسه. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة الاستثناءات وقائمة تطبيقات الموثوقة أو لترحيل القوائم إلى خادم مختلف.

يستخدم التطبيق التنسيقات التالية لتصدير واستيراد قائمة الاستثناءات:

- يتوفر XML في وحدة تحكم الإدارة (MMC) وCloud Console وCloud Console.
- يتوفر DAT فقط للاستيراد في وحدة تحكم الإدارة (MMC). ويكون الغرض من هذا التنسيق الحفاظ على التوافق مع الإصدارات القديمة من التطبيق. ويمكنك تحويل ملف DAT إلى XML في وحدة تحكم الإدارة (MMC) لترحيل قوائم الاستثناء إلى Web Console.
- يتوفر CSV فقط في الواجهة المحلية للتطبيق.

يستخدم Kaspersky Endpoint Security تنسيق XML لتصدير واستيراد قائمة التطبيقات الموثوقة.

كيفية تصدير واستيراد المنطقة الموثوقة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات**.

5. في القسم **استثناءات من الفحص والتطبيقات الموثوقة**، انقر على الزر **الإعدادات**.

6. لتصدير قائمة القواعد:

a. حدد علامة التبويب **استثناءات الفحص**.

يفتح هذا نافذة تحتوي على قائمة استثناءات.

b. حدد الاستثناءات التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

إذا لم تحدد أي استثناء، فسيقوم Kaspersky Endpoint Security بتصدير كل الاستثناءات.

c. انقر على رابط **تصدير**.

d. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

e. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML. يدعم Kaspersky Endpoint Security أيضًا تصدير قائمة الاستثناءات إلى ملف DAT.

7. لتصدير قائمة التطبيقات الموثوقة:

a. حدد علامة التبويب **التطبيقات الموثوقة**.

يفتح هذا نافذة تحتوي على قائمة بالتطبيقات الموثوقة.

b. حدد التطبيقات الموثوقة التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

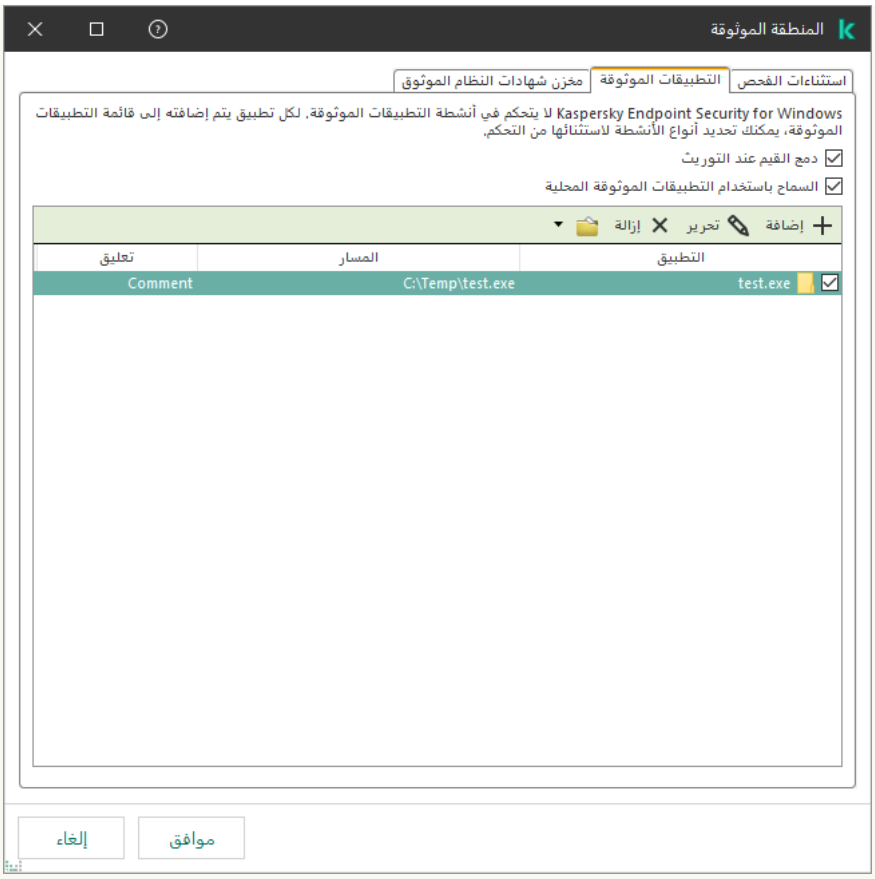
إذا لم تحدد أي تطبيق موثوق، سيقوم Kaspersky Endpoint Security بتصدير كل التطبيقات الموثوقة.

c. انقر على رابط **تصدير**.

d. يفتح هذا نافذة، وفي تلك النافذة، أدخل اسم ملف XML الذي تريد تصدير قائمة التطبيقات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

e. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة التطبيقات الموثوقة إلى ملف XML.



قائمة التطبيقات الموثوقة

8. لاستيراد قائمة الاستثناءات:

a. حدد علامة التبويب **استثناءات الفحص**.

يفتح هذا نافذة تحتوي على قائمة استثناءات.

b. انقر على **استيراد**.

c. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

d. افتح الملف.

إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML. يدعم Kaspersky Endpoint Security أيضًا استيراد قائمة الاستثناءات من ملف DAT.

9. لاستيراد قائمة التطبيقات الموثوقة:

a. حدد علامة التبويب **التطبيقات الموثوقة**.

يفتح هذا نافذة تحتوي على قائمة بالتطبيقات الموثوقة.

b. انقر على **استيراد**.

c. يفتح هذا نافذة، وفي تلك النافذة، حدد ملف XML الذي ترغب في استيراد قائمة التطبيقات منه.

d. افتح الملف.

إذا كان جهاز الكمبيوتر يحتوي على قائمة تطبيقات موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

10. احفظ تغييراتك.

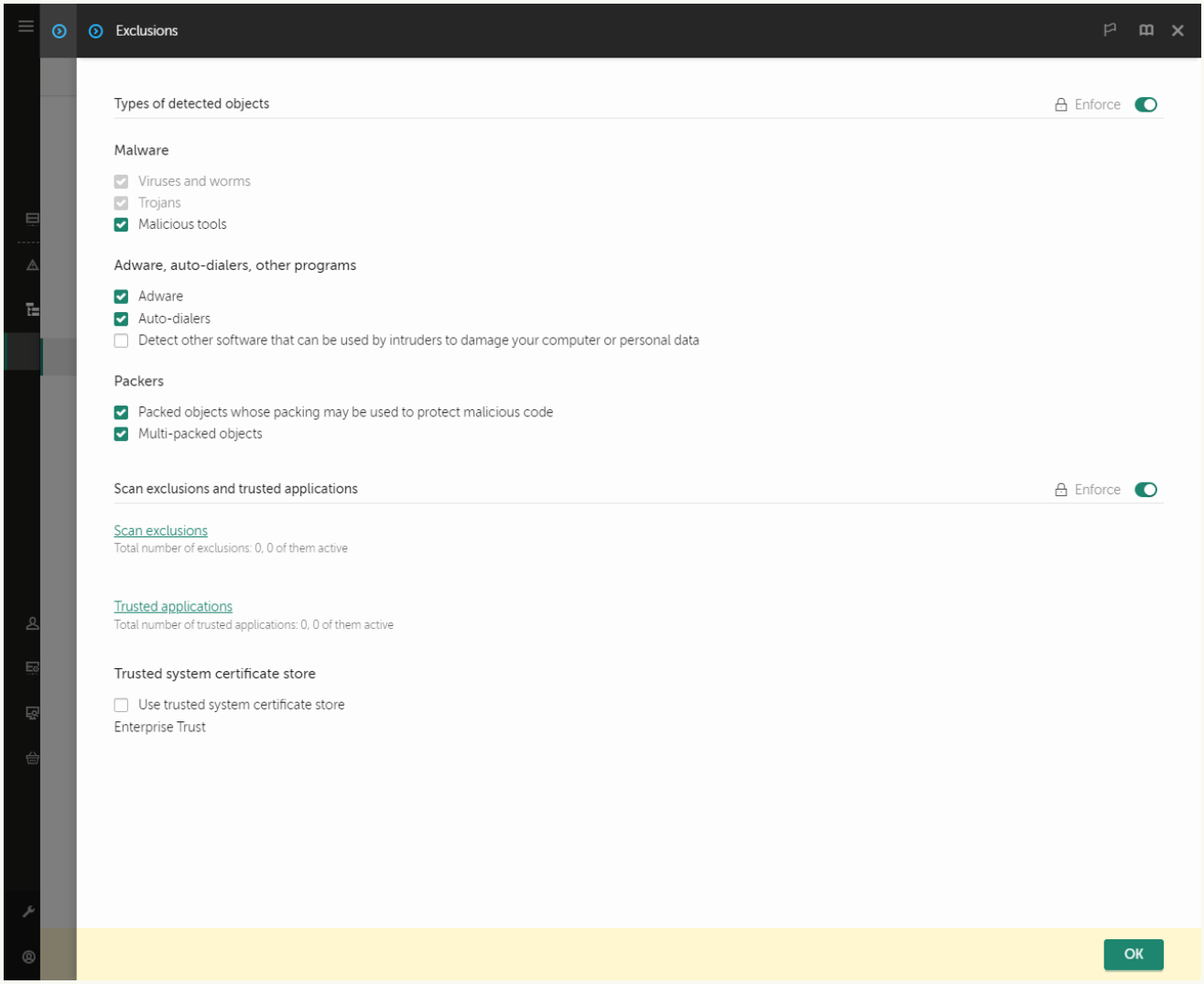
كيفية تصدير واستيراد المنطقة الموثوقة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **General settings** ← **Exclusions and types of detected objects**.



إعدادات الاستثناءات

5. لتصدير قائمة القواعد:

a. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Scan exclusions**.

b. حدد الاستثناءات التي تريد تصديرها.

c. انقر على **Export**.

d. أكد أنك تريد تصدير الاستثناءات المحددة فقط، أو تصدير قائمة الاستثناءات بأكملها.

e. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

f. احفظ الملف.

g. يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

6. لتصدير قائمة التطبيقات الموثوقة:

a. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Trusted applications**.

b. حدد الاستثناءات التي تريد تصديرها.

c. انقر على **Export**.

d. أكد أنك تريد تصدير الاستثناءات المحددة فقط، أو تصدير قائمة الاستثناءات بأكملها.

e. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

f. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

7. لاستيراد قائمة الاستثناءات:

a. انقر على **Import**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

c. افتح الملف.

إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. لاستيراد قائمة التطبيقات الموثوقة:

a. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Trusted applications**.

b. انقر على **Import**.

c. يفتح هذا نافذة، وفي تلك النافذة، حدد ملف XML الذي ترغب في استيراد قائمة التطبيقات منه.

d. افتح الملف.

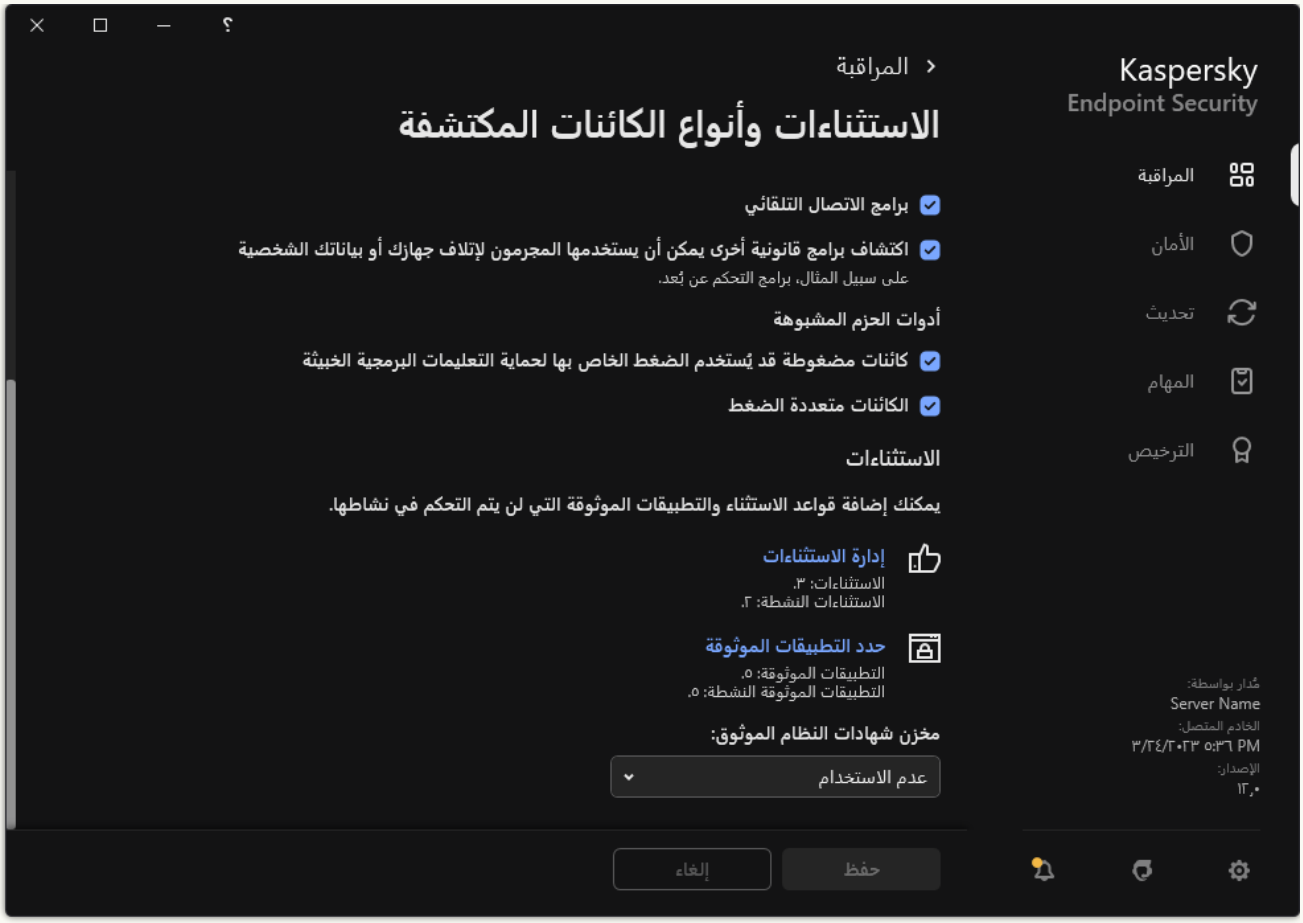
إذا كان جهاز الكمبيوتر يحتوي على قائمة تطبيقات موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

9. احفظ تغييراتك.

كيفية تصدير أو استيراد المنطقة الموثوقة في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات المكتشفة**.



إعدادات الاستثناءات

3. لتصدير قائمة القواعد:

a. في القسم **الاستثناءات**، انقر على الرابط **إدارة الاستثناءات**.

b. حدد الاستثناءات التي تريد تصديرها.

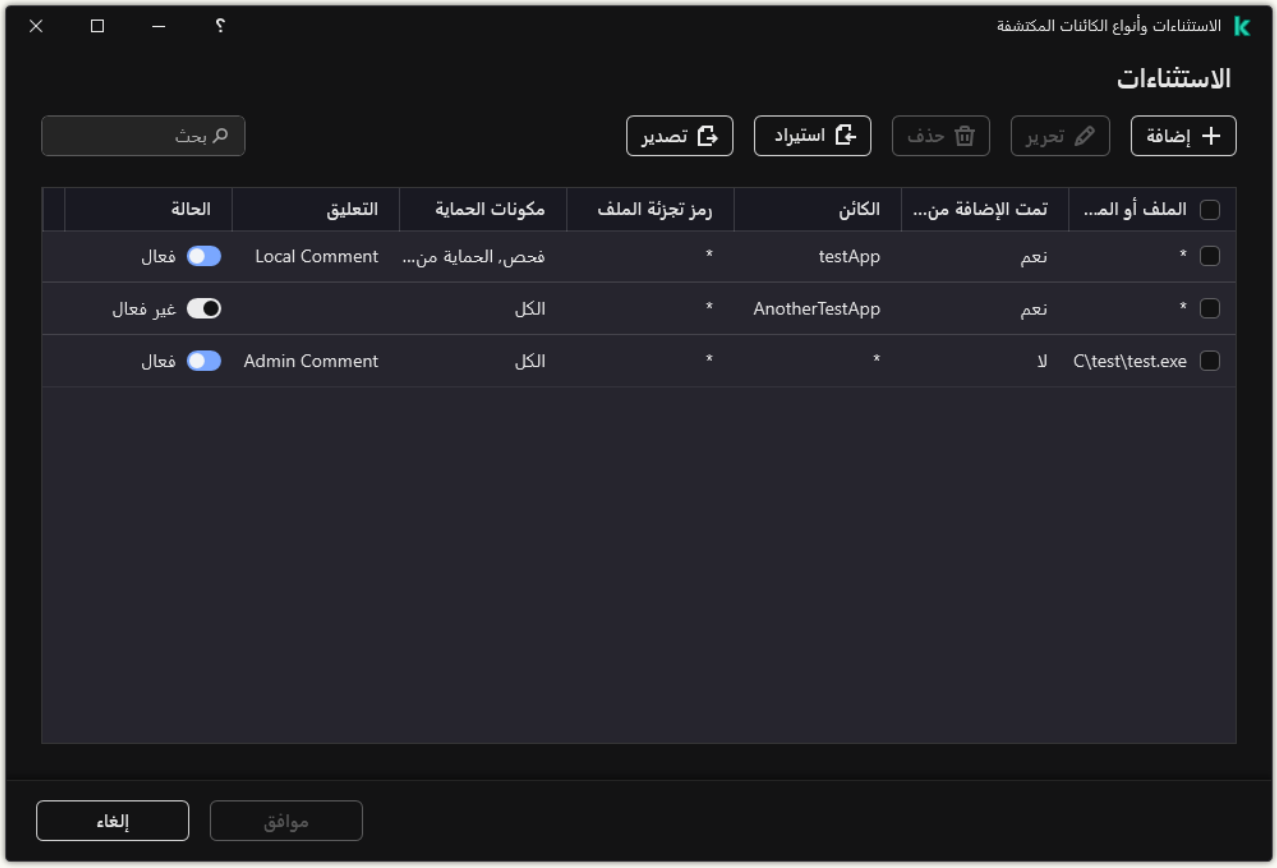
c. انقر على **تصدير**.

d. أكد أنك تريد تصدير الاستثناءات المحددة فقط، أو تصدير قائمة الاستثناءات بأكملها.

e. في النافذة التي تفتح، حدد اسم ملف CSV الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

f. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف CSV.



قائمة الاستثناءات

4. لتصدير قائمة التطبيقات الموثوقة:

a. في القسم **الاستثناءات**، انقر على الرابط **حدد التطبيقات الموثوقة**.

b. حدد التطبيقات الموثوقة التي تريد تصديرها.

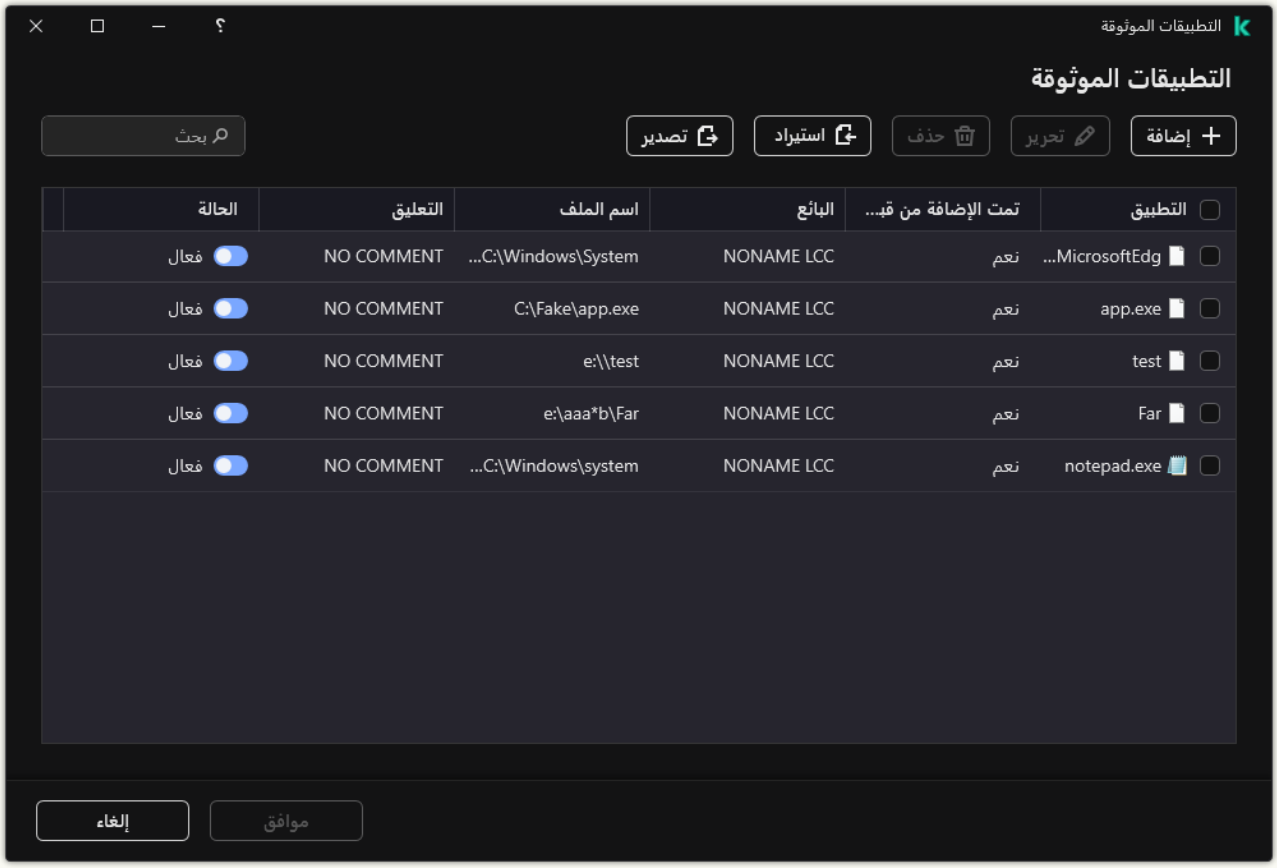
c. انقر على **تصدير**.

d. أكد أنك تريد تصدير القواعد المحددة فقط، أو التطبيقات الموثوقة أو تصدير القائمة بأكملها.

e. يفتح هذا نافذة، وفي تلك النافذة، أدخل اسم ملف XML الذي تريد تصدير قائمة التطبيقات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

f. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة التطبيقات الموثوقة بالكامل إلى ملف XML.



قائمة التطبيقات الموثوقة

5. لاستيراد قائمة الاستثناءات:

a. في القسم **الاستثناءات**، انقر على الرابط **إدارة الاستثناءات**.

b. انقر على **استيراد**.

c. في النافذة التي تفتح، حدد ملف CSV الذي ترغب في استيراد قائمة الاستثناءات منه.

d. افتح الملف.

إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف CSV.

6. لاستيراد قائمة التطبيقات الموثوقة:

a. في القسم **الاستثناءات**، انقر على الرابط **حدد التطبيقات الموثوقة**.

b. انقر على **استيراد**.

c. يفتح هذا نافذة، وفي تلك النافذة، حدد ملف XML الذي ترغب في استيراد قائمة التطبيقات منه.

d. افتح الملف.

إذا كان جهاز الكمبيوتر يحتوي على قائمة تطبيقات موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

7. احفظ تغييراتك.

استخدام مخزن شهادات النظام الموثوق

يتيح لك استخدام مخزن شهادات النظام استثناء التطبيقات الموقعة بواسطة توقيع رقمي موثوق من عمليات الفحص بحثًا عن فيروسات. ويُعين Kaspersky Endpoint Security تلقائيًا هذه التطبيقات إلى المجموعة الموثوقة.

لبدء استخدام مخزن شهادات النظام الموثوق:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات المكتشفة**.
3. في القائمة المنسدلة **مخزن شهادات النظام الموثوق**، حدد مخزن النظام الذي يجب وضعه في الاعتبار كموثوق بواسطة Kaspersky Endpoint Security.
4. احفظ تغييراتك.

إدارة النسخ الاحتياطي

يخزن النسخ الاحتياطي نسخًا احتياطية من الملفات التي تم حذفها أو تعديلها أثناء التنظيف. ويتم تعريف النسخة الاحتياطية بأنها نسخة ملف يتم إنشاؤها قبل تنظيف الملف أو حذفه. ويتم تخزين ملفات النسخ الاحتياطي بتنسيق خاص ولا تُمثل تهديدًا.

يتم تخزين النسخ الاحتياطية للملفات في المجلد `C:\ProgramData\Kaspersky Lab\KES.21.13\QB`.

يتم منح المستخدمين في مجموعة المسؤولين الإذن الكامل للوصول إلى هذا المجلد. ويتم منح حقوق الوصول المحدود إلى هذا المجلد للمستخدم الذي تم استخدام حسابه لتثبيت Kaspersky Endpoint Security.

لا يوفر Kaspersky Endpoint Security القدرة على تكوين أذونات وصول المستخدم إلى النسخ الاحتياطية من الملفات.

في بعض الأحيان يكون من غير الممكن الحفاظ على تكامل الملفات أثناء عملية التنظيف. إذا فقدت القدرة جزئيًا أو كليًا على الوصول إلى بعض المعلومات الهامة الموجودة في ملف تم تنظيفه بعد التنظيف، يمكنك محاولة استعادة الملف من النسخ الاحتياطي إلى المجلد الأصلي الخاص به.

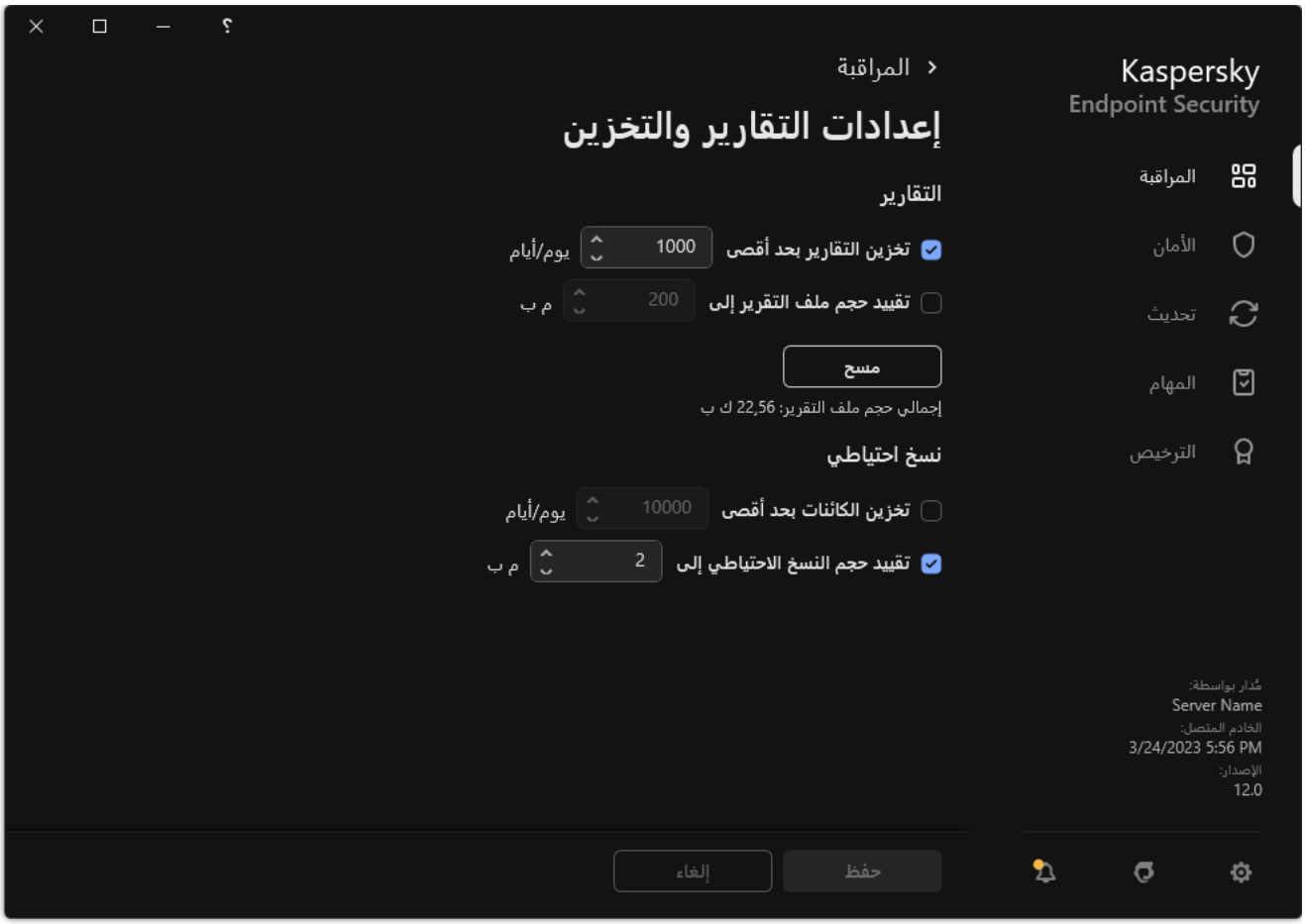
إذا كان Kaspersky Endpoint Security يعمل تحت إدارة Kaspersky Security Center، فقد يتم نقل النسخ الاحتياطية من الملفات إلى خادم إدارة Kaspersky Security Center. للحصول المزيد من التفاصيل حول إدارة النسخ الاحتياطية من الملفات في Kaspersky Security Center، يرجى الرجوع إلى نظام تعليمات Kaspersky Security Center.

تكوين أقصى فترة تخزين للملفات في النسخ الاحتياطي

أقصى فترة تخزين افتراضية لنسخ الملفات في النسخ الاحتياطي هي 30 يومًا. وبعد انتهاء فترة التخزين القصوى، يحذف Kaspersky Endpoint Security أقدم الملفات من النسخ الاحتياطي.

لتكوين أقصى فترة تخزين لنُسخ الملفات في النسخ الاحتياطي:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **التقارير والمخزن**.



إعدادات النسخ الاحتياطي

3. إذا كنت تريد تحديد فترة التخزين لنُسخ الملفات في النسخ الاحتياطي، فاختر خانة الاختيار **تخزين الكائنات بحد أقصى N يومًا (أيام)** في القسم **نسخ احتياطي**.
أدخل أقصى مدة تخزين للملفات في النسخ الاحتياطي.

4. احفظ تغييراتك.

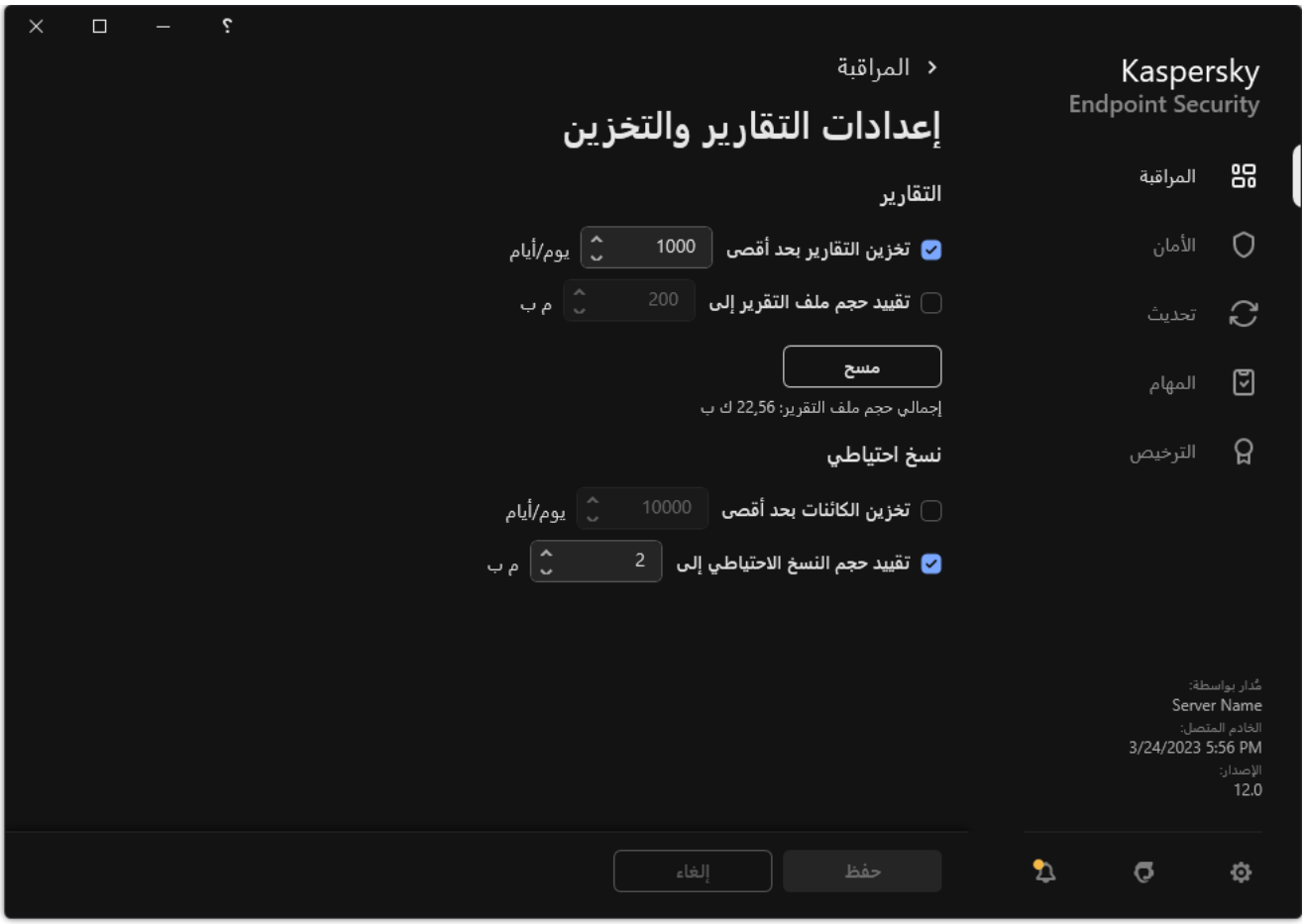
تكوين أقصى حجم للنسخ الاحتياطي

يمكنك تحديد الحجم الأقصى للنسخ الاحتياطي. يكون حجم النسخ الاحتياطي غير محدود بشكل افتراضي. بعد الوصول إلى الحد الأقصى للحجم، يحذف Kaspersky Endpoint Security تلقائيًا أقدم الملفات من النسخ الاحتياطي.

لتكوين أقصى حجم للنسخ الاحتياطي:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **التقارير والمخزن**.



إعدادات النسخ الاحتياطي

3. في القسم **نسخ احتياطي**، حدد خانة الاختيار **تقييد حجم النسخ الاحتياطي إلى N MB**. إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لحجم التخزين ليكون بالقيمة المُحددة. والإعداد الافتراضي لهذا الخيار هو 1024 ميجا بايت. لتجنب تجاوز الحد الأقصى لحجم التخزين، يقوم برنامج Kaspersky Endpoint Security بشكل تلقائي بحذف الملفات القديمة من المخزن عندما يتم الوصول إلى الحد الأقصى لحجم التخزين.

4. احفظ تغييراتك.

استعادة الملفات من النسخ الاحتياطي

في حالة اكتشاف تعليمات برمجية ضارة في ملف، يمنع Kaspersky Endpoint Security الملف ويعني الحالة مصاب له ويضع نسخة منه في النسخ الاحتياطي ويحاول تنظيفه. في حالة نجاح تنظيف الملف، تتغير حالة النسخة الاحتياطية للملف إلى تم التنظيف. ويصبح الملف متوفرًا في مجلده الأصلي. وفي حالة تعذّر تنظيف ملف ما، يقوم Kaspersky Endpoint Security بحذفه من مجلده الأصلي. يمكنك استعادة الملف من نسخته الاحتياطية إلى مجلده الأصلي.

لا يمكن استعادة الملفات التي تنطبق عليها حالة سيتم حذفها عند إعادة تشغيل الكمبيوتر. أعد تشغيل الكمبيوتر ليتم تغيير حالة الملف إلى تم التنظيف أو تم الحذف. يمكنك أيضًا استعادة الملف من نسخته الاحتياطية إلى مجلده الأصلي.

عند اكتشاف تعليمات برمجية ضارة في ملف يمثل جزءًا من تطبيق متجر Windows، يقوم Kaspersky Endpoint Security على الفور بحذف الملف دون نقل نسخة منه إلى النسخ الاحتياطي. يمكنك استعادة سلامة تطبيق متجر Windows باستخدام أدوات المناسبة لنظام تشغيل Microsoft Windows 8 (راجع ملفات تعليمات Microsoft Windows 8 للحصول على تفاصيل عند استعادة تطبيق متجر Windows).

يتم عرض مجموعة النسخ الاحتياطية للملفات في جدول. يتم عرض المسار إلى المجلد الأصلي للملف فيما يتعلق بنسخة احتياطية من ملف. وقد يحتوي المسار إلى المجلد الأصلي للملف على بيانات شخصية.

في حالة نقل العديد من الملفات ذات أسماء متطابقة ومحتوى مختلف موجودة في نفس المجلد إلى النسخ الاحتياطي، فمن الممكن استعادة آخر ملفات تم وضعها في النسخ الاحتياطي فقط.

لاستعادة الملفات من النسخ الاحتياطي:

1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **نسخ احتياطي**.
2. يفتح هذا قائمة الملفات في النسخ الاحتياطي؛ وفي تلك القائمة، حدد الملفات التي تريد استعادتها وانقر فوق **استعادة**.

يستعيد Kaspersky Endpoint Security الملفات المحددة من النسخ الاحتياطي إلى مجلداتها الأصلية.

حذف النسخ الاحتياطية للملفات من النسخ الاحتياطي

يحذف Kaspersky Endpoint Security تلقائيًا النسخ الاحتياطية للملفات بأي حالة من النسخ الاحتياطي بعد انقضاء فترة التخزين المحددة في إعدادات التطبيق. ويمكنك أيضًا حذف أي نسخة من الملف من النسخ الاحتياطي يدويًا.

لحذف النسخ الاحتياطية للملفات من النسخ الاحتياطي:

1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **نسخ احتياطي**.
2. يفتح هذا قائمة الملفات في النسخ الاحتياطي؛ وفي هذه القائمة، حدد الملفات التي تريد حذفها من النسخة الاحتياطية وانقر فوق **حذف**.

يحذف Kaspersky Endpoint Security النسخ الاحتياطية المحددة للملفات من النسخ الاحتياطي.

خدمة الإخطارات

تقع جميع أنواع الأحداث أثناء تشغيل Kaspersky Endpoint Security. قد تكون إخطارات هذه الأحداث إما معلوماتية بحتة أو تحتوي على معلومات مهمة. على سبيل المثال، قد تخبرك الإخطارات بنجاح تحديث قاعدة البيانات والوحدات النمطية للتطبيق أو أخطاء مكونات السجل الواجب إصلاحها.

يدعم برنامج Kaspersky Endpoint Security تسجيل دخول معلومات حول الأحداث عند تشغيل سجل تطبيق Microsoft Windows و/أو سجل أحداث Kaspersky Endpoint Security.

يقدم Kaspersky Endpoint Security إخطارات بالطرق التالية:

- باستخدام الإخطارات المنبثقة في منطقة إخطارات شريط المهام لـ Microsoft Windows؛
- عن طريق البريد الإلكتروني.

يمكنك تكوين إرسال إخطارات الأحداث. يتم تكوين طريقة عرض الإخطارات لكل نوع من أنواع الأحداث المختلفة.

عند استخدام جدول الأحداث لتكوين خدمة الإخطارات، يمكنك تنفيذ الإجراءات التالية:

- تصفية أحداث خدمة الإخطارات بواسطة قيم العمود أو حالات عامل التصفية المخصصة.
- استخدام وظيفة البحث لأحداث خدمة الإخطارات.
- تصنيف أحداث خدمة الإخطارات.
- تغيير ترتيب الأعمدة المعروضة في قائمة أحداث خدمة الإخطارات وتعيينها.

تكوين إعدادات سجل الحدث

لتكوين إعدادات سجل الأحداث:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الواجهة**.
3. في القسم **الإخطارات**، انقر على الزر **إعدادات الإخطار**.

تظهر مكونات ومهام برنامج Kaspersky Endpoint Security في الجزء الأيسر من النافذة. يظهر بالجزء الأيمن من النافذة سردًا للأحداث التي تم إنشاؤها للمكون أو المهمة المحددة.

قد تتضمن الأحداث بيانات المستخدم التالية:

- المسارات إلى الملفات التي يتم فحصها بواسطة Kaspersky Endpoint Security.
- المسارات المؤدية إلى مفاتيح التسجيل المُعدّلة في أثناء تشغيل Kaspersky Endpoint Security.
- اسم مستخدم Microsoft Windows.
- عناوين صفحات الويب المفتوحة بواسطة المستخدم.

4. في الجزء الأيسر من النافذة، حدد المكون أو المهمة التي ترغب في تكوين إعدادات سجل الأحداث بشأنها.
5. حدد خانات الاختيار المقابلة للأحداث ذات الصلة الموجودة في العمود **حفظ في تقرير محلي** والعمود **حفظ في سجل أحداث Windows**.

يتم عرض الأحداث التي تم تحديد خانات الاختيار الخاصة بها في العمود **حفظ في تقرير محلي** في application logs. يتم عرض الأحداث التي تم تحديد خانات الاختيار الخاصة بها في العمود **حفظ في سجل أحداث Windows** في سجلات Windows في القسم `Application`.

6. احفظ تغييراتك.

تكوين عرض وتسليم الإخطارات

لتكوين عرض الإخطارات وتسليمها:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة ← الواجهة**.

3. في القسم **الإخطارات**، انقر على الزر **إعدادات الإخطار**.

تظهر مكونات ومهام برنامج Kaspersky Endpoint Security في الجزء الأيسر من النافذة. يظهر في الجزء الأيمن من النافذة سردًا لأحداث تم إنشاؤها للمكون أو المهمة المحددة.

قد تتضمن الأحداث بيانات المستخدم التالية:

- المسارات إلى الملفات التي يتم فحصها بواسطة Kaspersky Endpoint Security.
- المسارات المؤدية إلى مفاتيح التسجيل المُعدّلة في أثناء تشغيل Kaspersky Endpoint Security.
- اسم مستخدم Microsoft Windows.
- عناوين صفحات الويب المفتوحة بواسطة المستخدم.

4. في الجزء الأيسر من النافذة، حدد المكون أو المهمة التي ترغب في تكوين إرسال الإخطارات بشأنها.

5. في العمود **إشعار على الشاشة**، حدد خانات الاختيار بجوار الأحداث ذات الصلة.

يتم عرض معلومات حول الأحداث المحددة على الشاشة كرسائل منبثقة في منطقة إخطار شريط المهام بنظام التشغيل Microsoft Windows.

6. في العمود **إشعار عبر البريد الإلكتروني**، حدد خانات الاختيار بجوار الأحداث ذات الصلة.

يتم تسليم المعلومات حول الأحداث المحددة عبر البريد الإلكتروني في حالة تكوين إعدادات تسليم إخطارات البريد.

7. انقر على **موافق**.

8. إذا قمت بتمكين إخطارات البريد الإلكتروني، فقم بتكوين الإعدادات لتسليم البريد الإلكتروني:

a. انقر على **إعدادات إخطارات البريد الإلكتروني**.

b. حدد خانة الاختيار **إخطار بالأحداث** لتمكين تسليم المعلومات حول أحداث Kaspersky Endpoint Security المحددة في العمود **إشعار عبر البريد الإلكتروني**.

c. حدد إعدادات تسليم إشعار عبر البريد الإلكتروني.

d. انقر على **موافق**.

9. احفظ تغييراتك.

تكوين عرض التحذيرات حول حالة التطبيق في منطقة الإخطارات

لتكوين عرض تحذيرات حالة التطبيق في منطقة الإخطارات:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الواجهة**.

3. في القسم **إظهار حالة التطبيق في منطقة الإخطارات**، حدد خانات الاختيار المقابلة لفئات الأحداث التي تريد رؤية الإخطارات في منطقة الإخطارات حولها في نظام Microsoft Windows.

4. احفظ تغييراتك.

عند وقوع أحداث مرتبطة بالفئات المحددة، سوف يتغير رمز التطبيق في منطقة الإخطارات إلى أو وفقًا لمدى خطورة التحذير.

تبادل الرسائل بين المستخدمين والمدير

تقوم المكونات التحكم في التطبيقات، والتحكم في الجهاز، وWeb Control، ومراقبة عيوب التكيف بتمكين مستخدمي الشبكة المحلية الذين يمتلكون أجهزة كمبيوتر مثبت عليها برنامج Kaspersky Endpoint Security من إرسال رسائل إلى المسؤول.

قد يحتاج المستخدم إلى إرسال رسالة إلى مسؤول شبكة الشركة المحلية في الحالات التالية:

- منع مكون التحكم في الجهاز الوصول إلى الجهاز.

  يتوفر قالب الرسالة لطلب الوصول إلى جهاز ممنوع في واجهة Kaspersky Endpoint Security في القسم التحكم في الجهاز.

- منع التحكم في التطبيقات من بدء تشغيل تطبيق.

  يتوفر قالب الرسالة لطلب إتاحة بدء تشغيل تطبيق ممنوع في واجهة Kaspersky Endpoint Security في القسم التحكم في التطبيقات.

- منع مكون Web Control أحد موارد الويب.

  يتوفر قالب الرسالة لطلب الوصول إلى مورد ويب ممنوع في واجهة Kaspersky Endpoint Security في القسم Web Control.

تعتمد طريقة إرسال الرسائل والقالب المستخدم على ما إذا كانت هناك سياسة نشطة لـ Kaspersky Security Center تعمل على الكمبيوتر المثبت عليه Kaspersky Endpoint Security، وما إذا كان هناك اتصال مع خادم إدارة Kaspersky Security Center. السيناريوهات التالية ممكنة:

- في حالة عدم وجود سياسة Kaspersky Security Center تعمل على الكمبيوتر المثبت عليه Kaspersky Endpoint Security، فيتم إرسال رسالة مستخدم إلى مسؤول الشبكة المحلية عن طريق البريد الإلكتروني.

  يتم ملء حقول الرسائل بقيم الحقول من القالب المحدد في الواجهة المحلية لـ Kaspersky Endpoint Security.

- في حالة عمل سياسة Kaspersky Security Center على الكمبيوتر المثبت عليه Kaspersky Endpoint Security، فيتم إرسال الرسالة القياسية إلى خادم إدارة Kaspersky Security Center.

  وفي هذه الحالة، تتوفر رسائل المستخدمين للعرض في مخزن أحداث Kaspersky Security Center (انظر التعليمات أدناه). يتم ملء حقول الرسائل بقيم الحقول من القالب المحدد في سياسة Kaspersky Security Center.

- في حالة عمل سياسة الوجود خارج المكتب الخاصة بـ Kaspersky Security Center على الكمبيوتر المثبت عليه Kaspersky Endpoint Security، فتعتمد طريقة إرسال الرسائل على ما إذا كان هناك اتصال بـ Kaspersky Security Center أم لا.

  - في حالة وجود اتصال بـ Kaspersky Security Center، فيقوم Kaspersky Endpoint Security بإرسال الرسالة القياسية إلى خادم إدارة Kaspersky Security Center.

  - في حالة عدم وجود اتصال بـ Kaspersky Security Center، فيتم إرسال رسالة مستخدم إلى مسؤول الشبكة المحلية عن طريق البريد الإلكتروني.

  وفي كلتا الحالتين، يتم ملء حقول الرسائل بقيم الحقول من القالب المحدد في سياسة Kaspersky Security Center.

لعرض شكاوى المستخدم في مخزن أحداث Kaspersky Security Center:

1. افتح Kaspersky Security Center Administration Console.

2. في العقدة **خادم الإدارة** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **الأحداث**.

تعرض مساحة عمل Kaspersky Security Center كل الأحداث التي تحدث أثناء تشغيل Kaspersky Endpoint Security، بما في ذلك الرسائل إلى المسؤول التي تم تلقيها من مستخدمي شبكة LAN.

3. لتكوين تصفية الأحداث، في القائمة المنسدلة **تحديدات الأحداث**، حدد **طلبات المستخدم**.

4. حدد الرسالة التي تم إرسالها إلى المسؤول.

5. انقر فوق الزر **فتح نافذة خصائص الحدث** في الجزء الأيسر من مساحة عمل وحدة تحكم الإدارة.

إدارة التقارير

يتم تسجيل معلومات حول تشغيل كل مكون من مكونات Kaspersky Endpoint Security، وحالات تشفير البيانات، وأداء كل مهمة فحص، ومهمة التحديث، ومهمة التحقق من السلامة، والتشغيل الإجمالي للتطبيق في التقارير.

يتم تخزين التقارير في المجلد `C:\ProgramData\Kaspersky Lab\KES.21.13\Report`.

قد تتضمن التقارير بيانات المستخدم التالية:

- المسارات إلى الملفات التي يتم فحصها بواسطة Kaspersky Endpoint Security.
- المسارات المؤدية إلى مفاتيح التسجيل المُعدّلة في أثناء تشغيل Kaspersky Endpoint Security.
- اسم مستخدم Microsoft Windows.
- عناوين صفحات الويب المفتوحة بواسطة المستخدم.

البيانات في التقرير معروضة في شكل مجدول. ويحتوي كل صف في الجدول على معلومات حول حدث منفصل. وتوجد سمات الحدث في أعمدة الجدول. ويتم تجميع بعض الأعمدة التي تحتوي على أعمدة متداخلة مع سمات إضافية. لعرض السمات الإضافية، انقر فوق الزر ⊞ الموجود بجوار اسم العمود. تمتلك الأحداث التي يتم تسجيلها أثناء عمل مكونات مختلفة أو أثناء أداء مهام مختلفة مجموعات مختلفة من السمات.

تتوافر التقارير التالية:

- تقرير **تدقيق النظام**. يحتوي على معلومات حول أحداث حدثت أثناء التفاعل بين المستخدم والتطبيق وأثناء تشغيل التطبيق بوجه عام، وليس لها صلة بأي مكونات أو مهام لبرنامج Kaspersky Endpoint Security.
- التقارير عن عمل مكونات Kaspersky Endpoint Security.
- تقارير مهام Kaspersky Endpoint Security.
- تقرير **تشفير البيانات**. يحتوي على معلومات حول الأحداث التي تحدث أثناء تشفير وفك تشفير البيانات.

تستخدم التقارير مستويات أهمية الحدث التالية:

ⓘ **رسائل معلوماتية**. الأحداث المرجعية التي لا تحتوي عادة على معلومات هامة.

⚠ **تحذيرات**. أحداث تحتاج إلى الانتباه لأنها تعكس مواقف هامة أثناء تشغيل برنامج Kaspersky Endpoint Security.

❗ **أحداث حرجة**. الأحداث ذات الأهمية الحرجة التي تشير إلى مشكلات في تشغيل Kaspersky Endpoint Security أو وجود ثغرات أمنية في حماية كمبيوتر المستخدم.

للحصول على معالجة مناسبة للتقارير، يمكنك تعديل عرض البيانات على الشاشة بالطرق التالية:

- تصفية قائمة الأحداث حسب معايير مختلفة.
- استخدام وظيفة البحث للعثور على حدث محدد.
- عرض حدث محدد في قسم منفصل.
- فرز قائمة الأحداث حسب كل عمود في التقرير.
- عرض وإخفاء الأحداث المجمعة بواسطة عامل تصفية الأحداث باستخدام زر ⊞.
- تغيير ترتيب الأعمدة التي تظهر في التقرير وتنظيمها.

يمكنك حفظ التقرير الناتج كملف نصي، عند الضرورة. ويمكنك أيضًا حذف معلومات التقرير الموجودة على مكونات Kaspersky Endpoint Security ومهامه المجمعة في مجموعات.

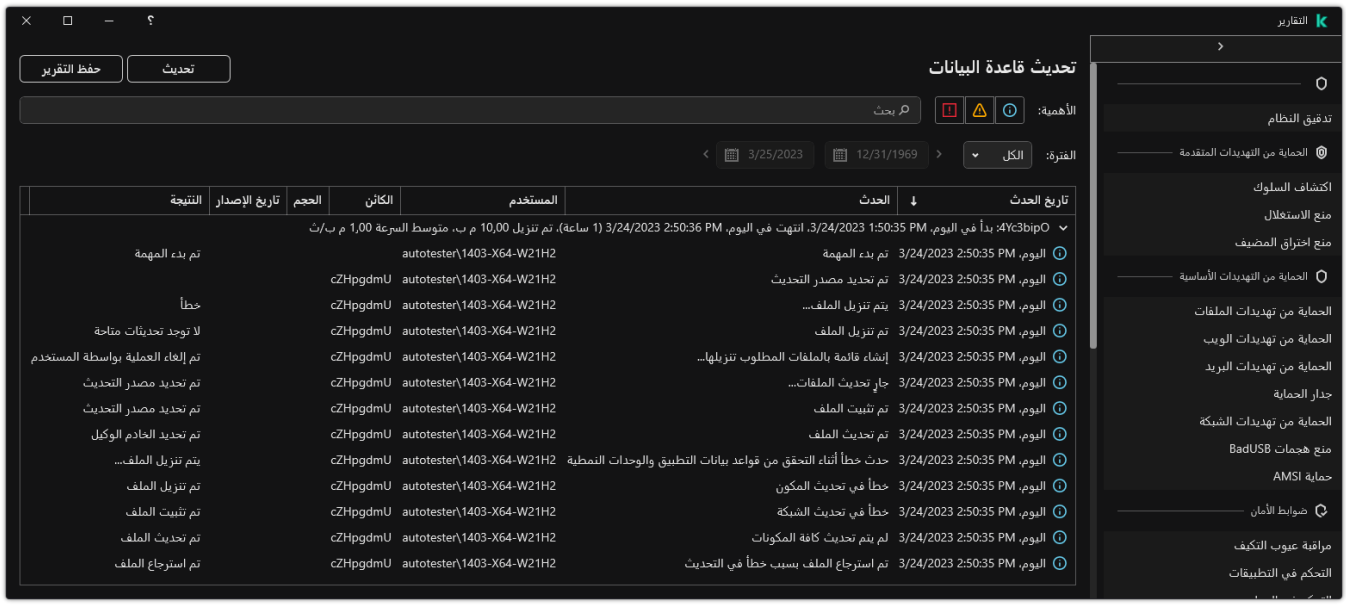
إذا كان Kaspersky Endpoint Security يعمل تحت إدارة Kaspersky Security Center، فإن المعلومات المتوفرة عن الأحداث قد تُرحل إلى خادم إدارة Kaspersky Security Center (للمزيد من التفاصيل، يرجى الرجوع إلى تعليمات Kaspersky Security Center).

عرض التقارير

إذا كان أحد المستخدمين يستطيع عرض التقارير، فإن المستخدم يستطيع أيضًا عرض كل الأحداث المذكورة في التقارير.

لعرض التقارير:

1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **التقارير**.



التقارير

2. في قائمة المكونات والمهام، حدد مكونًا أو مهمة.

يعرض الجزء الأيمن من النافذة تقريرًا يتضمن قائمة بالأحداث الناتجة عن تشغيل المكون المحدد أو مهمة Kaspersky Endpoint Security المحددة. يمكنك فرز الأحداث في التقرير بناءً على القيم في خلايا أحد الأعمدة.

3. لعرض معلومات تفصيلية عن حدث، حدد الحدث في التقرير.

يتم عرض قسم يحتوي على ملخص الحدث في الجزء السفلي من النافذة.

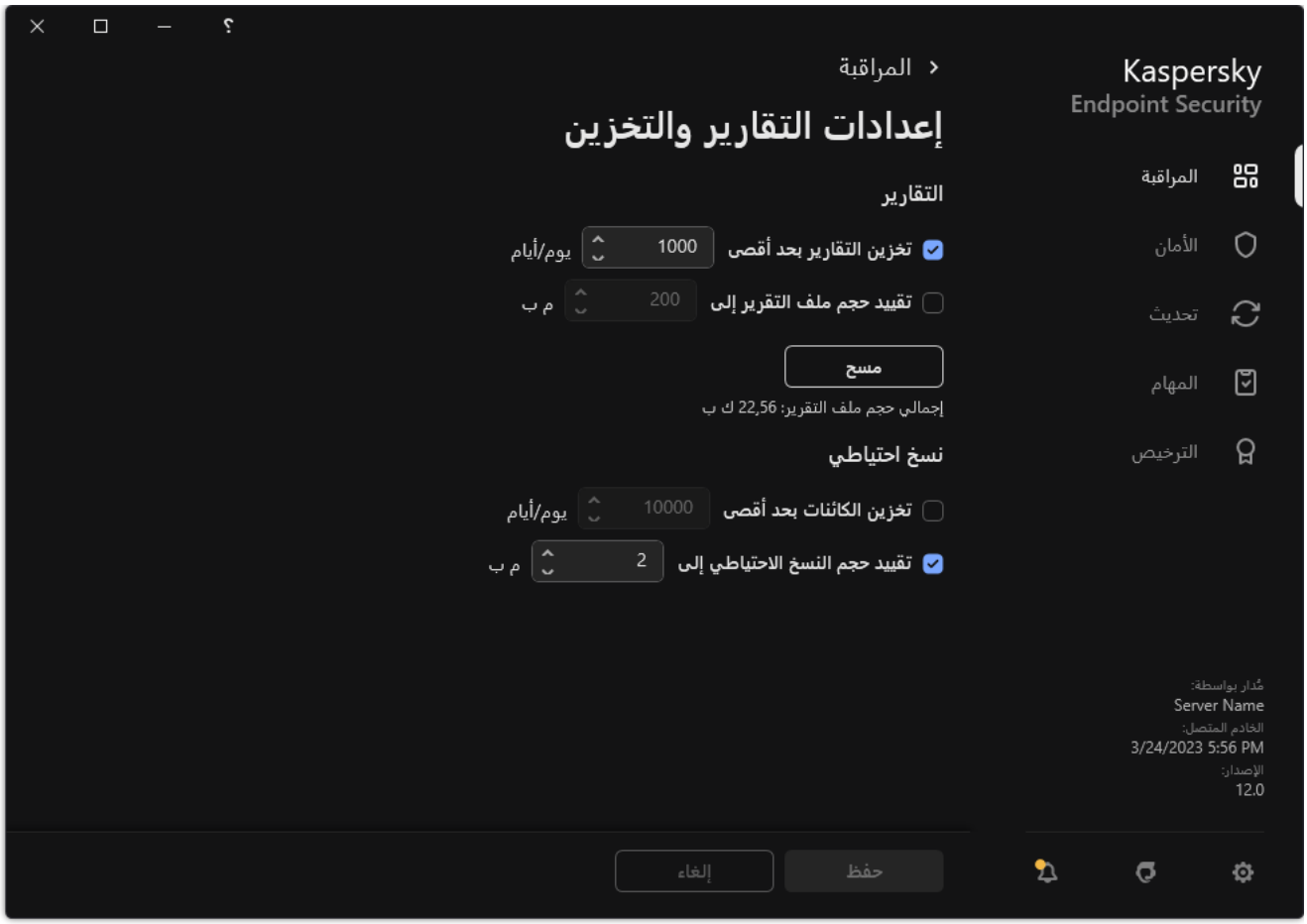
تكوين الفترة الزمنية القصوى لتخزين التقرير

تصل القيمة الافتراضية للحد الأقصى لمدة تخزين التقارير الخاصة بالأحداث المسجلة بواسطة برنامج Kaspersky Endpoint Security إلى 30 يومًا. وبعد انتهاء هذه الفترة، يقوم برنامج Kaspersky Endpoint Security بشكل تلقائي بحذف الإدخالات القديمة من ملف التقارير.

لتعديل الفترة الزمنية القصوى لتخزين التقرير:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **التقارير والمخزن**.



إعدادات التقرير

3. إذا كنت تريد تقييد مدة تخزين التقرير، حدد خانة الاختيار **تخزين التقارير بحد أقصى N days** في القسم **التقارير**. تحديد أقصى فترة زمنية لتخزين التقرير.

4. احفظ تغييراتك.

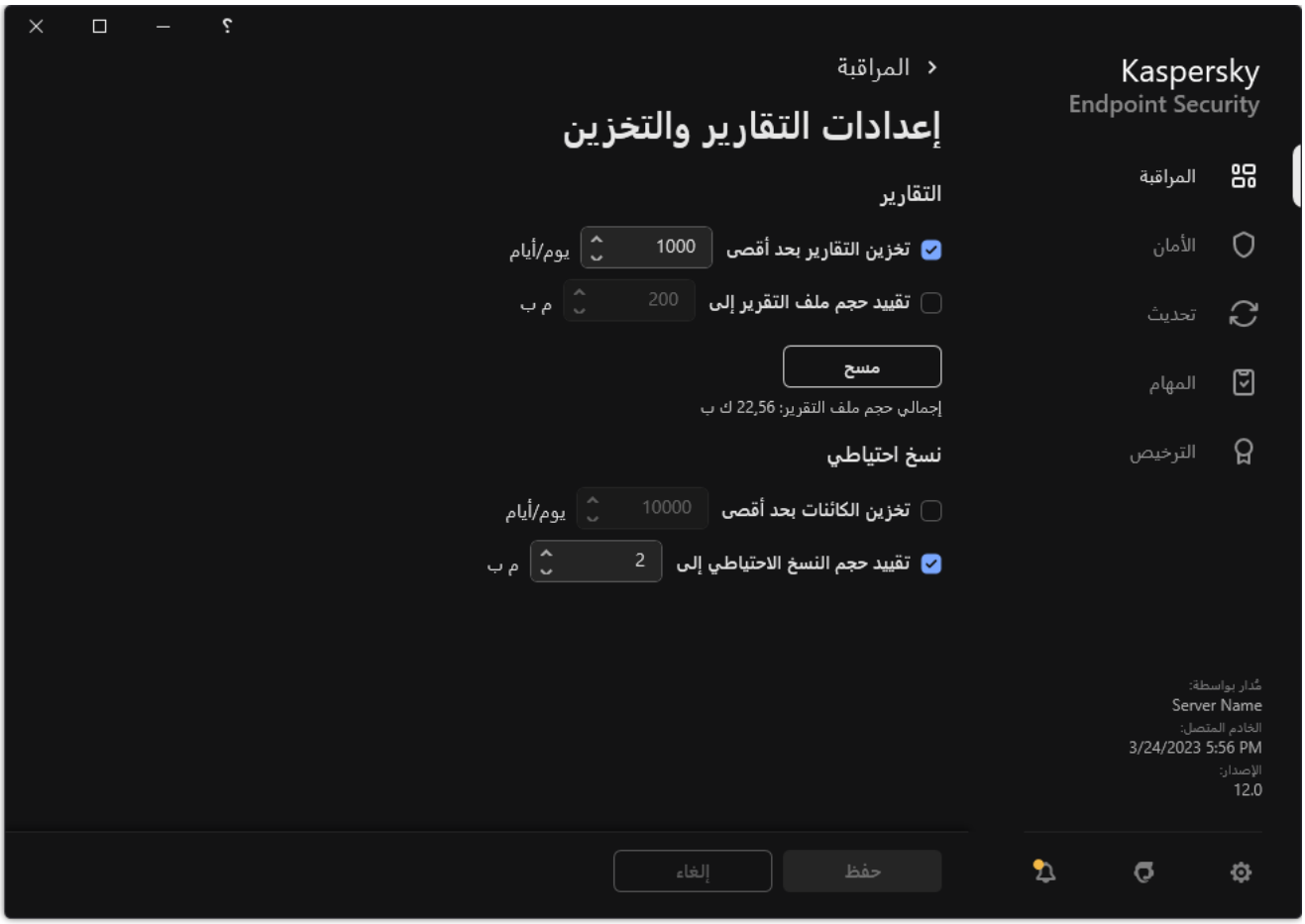
تكوين الحجم الأقصى لملف التقرير

يمكنك تحديد الحد الأقصى لحجم الملف الذي يحتوي على التقارير. والإعداد الافتراضي للحد الأقصى لحجم ملف التقارير هو 1024 ميجا بايت. لتجنب تجاوز الحد الأقصى لحجم ملف التقارير، يقوم برنامج Kaspersky Endpoint Security بشكل تلقائي بحذف الإدخالات القديمة من ملف التقارير عندما يتم الوصول إلى الحد الأقصى لحجم ملف التقارير.

لتكوين الحجم الأقصى لملف التقرير:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **التقارير والمخزن**.



إعدادات التقرير

3. في القسم **التقارير**، حدد خانة الاختيار **تقييد حجم ملف التقرير إلى N MB** إذا كنت تريد تحديد حجم ملف التقرير. تحديد أقصى حجم لملف التقرير.

4. احفظ تغييراتك.

حفظ التقرير إلى ملف

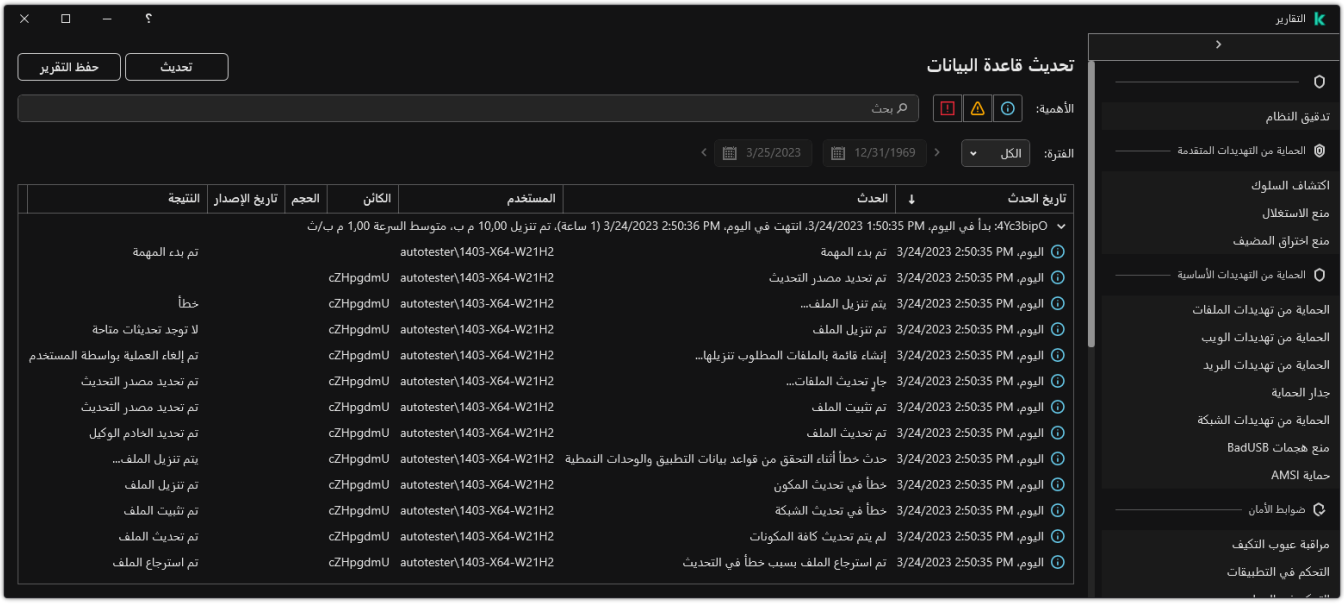
يتحمل المستخدم شخصيًا مسؤولية ضمان أمن المعلومات من تقرير تم حفظه إلى ملف، وخاصة لمراقبة وتقييد الوصول إلى هذه المعلومات.

يمكنك حفظ التقرير الذي قمت بإنشائه إلى ملف بتنسيق نص (TXT) أو ملف CSV.

يقوم برنامج Kaspersky Endpoint Security بتسجيل الأحداث في التقرير بنفس الطريقة التي يتم عرضها على الشاشة: أو بمعنى آخر، أن يكون لها نفس مجموعة سمات الأحداث وتتابعها.

لحفظ تقرير إلى ملف:

1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **التقارير**.



التقارير

2. يفتح هذا نافذة؛ وفي هذه النافذة، حدد المكون أو المهمة.

يتم عرض تقرير في الجزء الأيمن من النافذة، التي تحتوي على قائمة الأحداث التي تقوم بتشغيل المكون أو المهمة المحددة لبرنامج Kaspersky Endpoint Security.

3. إذا لزم الأمر، يمكنك تعديل تمثيل البيانات في التقرير عن طريق:

- تصفية الأحداث
- تشغيل البحث عن الأحداث
- إعادة ترتيب الأعمدة
- فرز الأحداث

4. انقر فوق الزر **حفظ التقرير** في الجزء العلوي بالجانب الأيمن من النافذة.

5. في النافذة التي تفتح، حدد مجلد الوجهة لملف التقرير.

6. أدخل اسم ملف التقرير.

7. تحديد تنسيق ملف التقرير اللازم: TXT أو CSV.

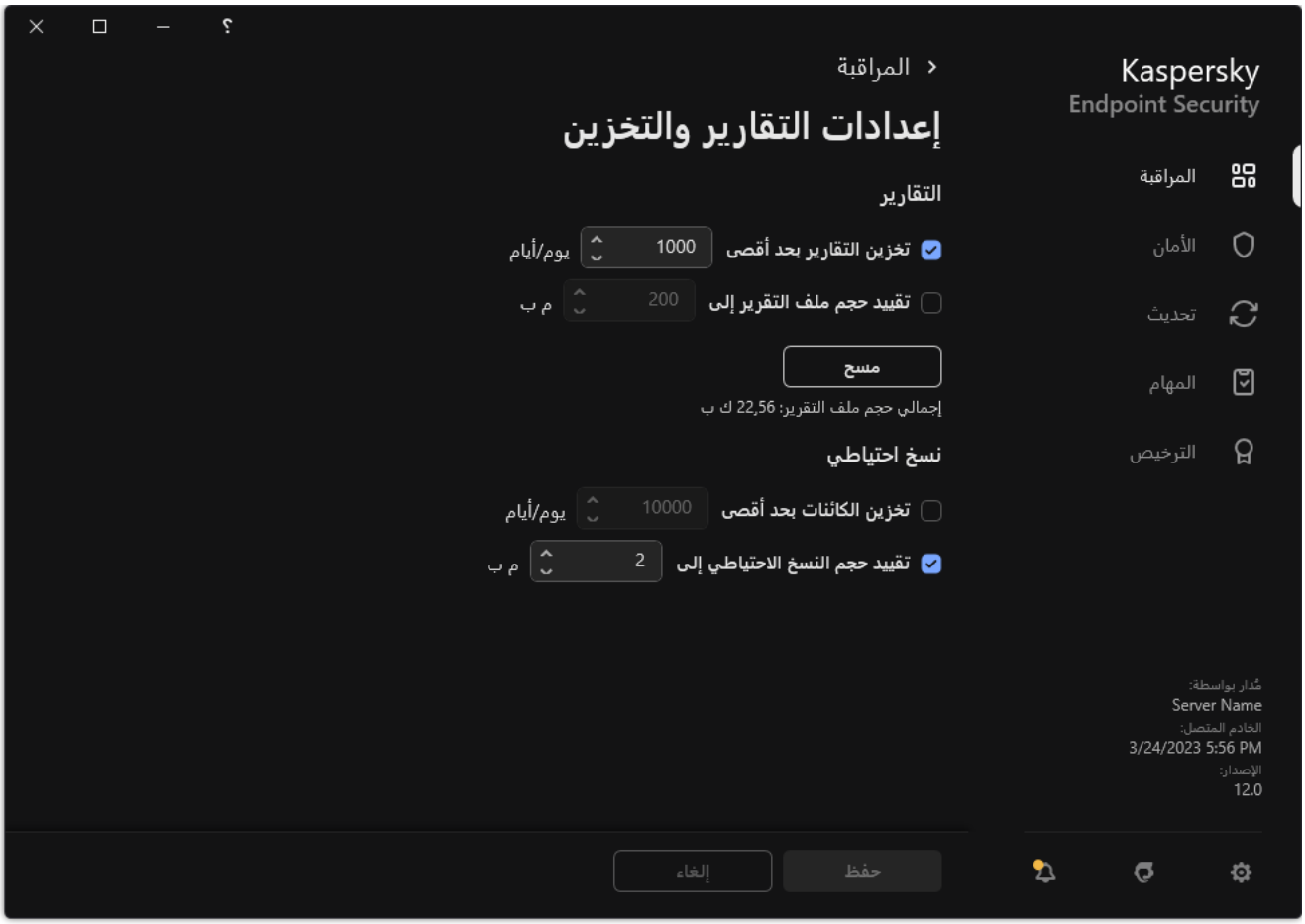
8. احفظ تغييراتك.

مسح التقارير

لإزالة معلومات من التقارير:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **التقارير والمخزن**.



إعدادات التقرير

3. في القسم **التقارير**، انقر على الزر **مسح**.

4. في حالة تمكين الحماية بكلمة مرور، قد يطالبك Kaspersky Endpoint Security ببيانات اعتماد حساب المستخدم. يطالب التطبيق ببيانات اعتماد الحساب إذا لم يكن المستخدم يمتلك الأذونات المطلوبة.

سيحذف Kaspersky Endpoint Security كل التقارير لكل مكونات التطبيق ومهامه.

الدفاع الذاتي لبرنامج Kaspersky Endpoint Security

يمنع الدفاع الذاتي التطبيقات الأخرى من تنفيذ الإجراءات التي يمكن أن تتداخل مع تشغيل Kaspersky Endpoint Security، على سبيل المثال، إزالة Kaspersky Endpoint Security من الكمبيوتر. وتعتمد مجموعة تقنيات الدفاع الذاتي المتوفرة لتطبيق Kaspersky Endpoint Security على ما إذا كان نظام التشغيل 32 بت أو 64 بت (راجع الجدول أدناه).

الدفاع الذاتي لتطبيق Kaspersky Endpoint Security

التقنية	الوصف	كمبيوتر x86	كمبيوتر x64
آلية الدفاع الذاتي	تمنع التقنية الوصول إلى مكونات التطبيق التالية: • الملفات الموجودة في مجلد تثبيت Kaspersky Endpoint Security والملفات الأخرى للتطبيق؛ • مفاتيح التسجيل التي تتضمن سجلات تنتمي إلى التطبيق؛ • العمليات التي يقوم التطبيق بتشغيلها.	✓	✓
AM-PPL (Antimalware Protected Process Light)	تحمي التقنية عمليات Kaspersky Endpoint Security من الإجراءات الضارة. للحصول على المزيد من التفاصيل حول تقنية AM-PPL، يُرجى زيارة موقع ويب Microsoft. إن تقنية AM-PPL متاحة للإصدار 1703 من نظام التشغيل Windows 10 (RS2) أو إصدار أحدث، ونظام التشغيل Windows Server 2019.	✓	–
آلية دفاع الإدارة الخارجية	تمنع هذه التقنية تطبيقات الإدارة عن بُعد (على سبيل المثال، TeamViewer أو RemotelyAnywhere) من الوصول إلى Kaspersky Endpoint Security.	✓	– (باستثناء Windows 7)

تمكين وتعطيل الدفاع الذاتي

يتم تمكين آلية الدفاع الذاتي ببرنامج Kaspersky Endpoint Security افتراضيًا.

لتمكين الدفاع الذاتي:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.

إعدادات Kaspersky Endpoint Security for Windows

3. استخدم خانة الاختيار **تمكين الدفاع الذاتي** لتمكين أو تعطيل آلية الدفاع الذاتي.

4. احفظ تغييراتك.

تمكين دعم AM-PPL وتعطيله

يدعم Kaspersky Endpoint Security تقنية Antimalware Protected Process Light (المشار إليها فيما يلي في هذا المستند باسم "AM-PPL") المقدمة من شركة Microsoft. تحمي تقنية AM-PPL العمليات التي يتم تنفيذها من خلال Kaspersky Endpoint Security من الإجراءات الضارة (على سبيل المثال، إنهاء التطبيق). وتسمح تقنية AM-PPL بتفعيل العمليات الموثوق بها فقط. تم تصميم العمليات التي تتم من خلال Kaspersky Endpoint Security وفقًا لمتطلبات الأمان في نظام Windows، وبناءً على ذلك تكتسب الثقة. للحصول على المزيد من التفاصيل حول تقنية AM-PPL، يُرجى زيارة موقع ويب Microsoft. يتم تمكين تقنية AM-PPL بشكل افتراضي.

يوجد في Kaspersky Endpoint Security أيضًا آليات مدمجة لحماية العمليات التي تتم من خلال التطبيق. يتيح لك دعم تقنية AM-PPL تفويض نظام التشغيل لأداء العملية الخاصة بوظائف أمان. ويمكنك بالتالي زيادة سرعة التطبيق وتقليل استهلاك موارد الكمبيوتر.

إن تقنية AM-PPL متاحة للإصدار 1703 من نظام التشغيل Windows 10 (RS2) أو إصدار أحدث، ونظام التشغيل Windows Server 2019.

تتوافر تقنية AM-PPL فقط لأجهزة الكمبيوتر التي تعمل بأنظمة تشغيل 32 بت. ولا تتوافر هذه التقنية لأجهزة الكمبيوتر التي تعمل بأنظمة تشغيل 64 بت.

لتمكين أو تعطيل تقنية AM-PPL:

1. أوقف تشغيل آلية الدفاع الذاتي بالتطبيق.

تمنع آلية الدفاع الذاتي التعديل في العمليات التي تتم من خلال التطبيق وحذفها في ذاكرة الكمبيوتر، بما يشمل تغيير حالة تقنية AM-PPL.

2. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.

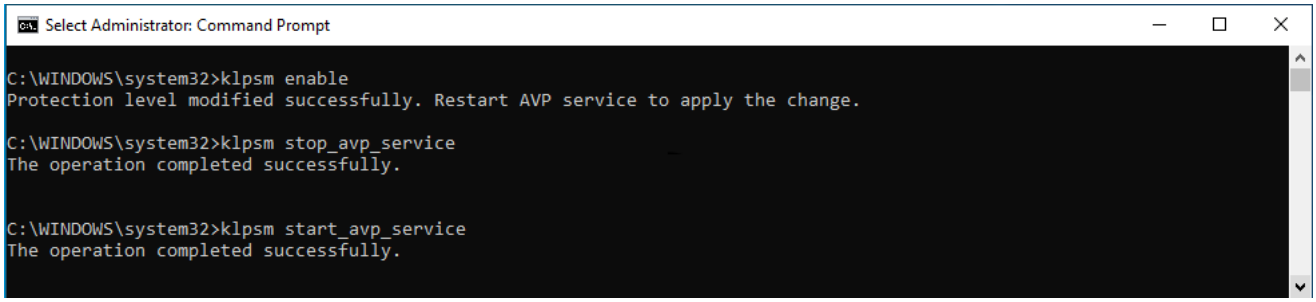
3. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.

4. اكتب ما يلي في سطر الأوامر:

- `klpsm.exe enable` – تمكين دعم تقنية AM-PPL (انظر الشكل أدناه).
- `klpsm.exe disable` – تعطيل دعم تقنية AM-PPL.

5. إعادة تشغيل Kaspersky Endpoint Security.

6. استئناف تشغيل آلية الدفاع الذاتي بالتطبيق.



تمكين دعم تقنية AM-PPL

حماية خدمات التطبيق من الإدارة الخارجية

تحظر حماية خدمات التطبيق من الإدارة الخارجية محاولات المستخدمين والتطبيقات الأخرى لإيقاف خدمات Kaspersky Endpoint Security. وتضمن الحماية تشغيل الخدمات التالية:

- خدمة Kaspersky Endpoint Security (avp)
- خدمة التحديث السلس من Kaspersky (avpsus)

لإيقاف التطبيق من سطر الأوامر، قم بتعطيل حماية خدمات Kaspersky Endpoint Security من الإدارة الخارجية.

لتمكين أو تعطيل حماية خدمات التطبيق من الإدارة الخارجية:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.

إعدادات Kaspersky Endpoint Security for Windows

3. استخدم مربع الاختيار **تمكين الإدارة الخارجية لخدمات النظام** لتمكين أو تعطيل حماية خدمات Kaspersky Endpoint Security من الإدارة الخارجية.

4. احفظ تغييراتك.

نتيجة لذلك ، عندما يحاول المستخدم إيقاف خدمات التطبيق، تظهر نافذة نظام تتضمن رسالة خطأ. ويستطيع المستخدم إدارة خدمات التطبيقات فقط من واجهة Kaspersky Endpoint Security.

دعم تطبيقات الإدارة عن بعد

قد تحتاج أحيانًا إلى استخدام تطبيق الإدارة عن بُعد بينما تكون دفاع الإدارة الخارجية ممكَّنًا.

لتمكين تشغيل تطبيقات الإدارة عن بعد:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات المكتشفة**.

3. في القسم **الاستثناءات**، انقر على الرابط **حدد التطبيقات الموثوقة**.

4. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

5. حدد الملف القابل للتنفيذ لتطبيق الإدارة عن بُعد.

يمكنك أيضًا إدخال المسار يدويًا. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

6. حدد خانة الاختيار **السماح بالتفاعل مع واجهة تطبيق Kaspersky Endpoint Security**.

7. احفظ تغييراتك.

أداء Kaspersky Endpoint Security والتوافق مع التطبيقات الأخرى

يشير أداء Kaspersky Endpoint Security إلى عدد أنواع الكائنات التي تم اكتشافها والتي قد تلحق الضرر بالكمبيوتر، بالإضافة إلى استهلاك الطاقة واستخدام موارد الكمبيوتر.

تحديد أنواع الكائنات القابلة للاكتشاف

يسمح لك Kaspersky Endpoint Security بتكوين الحماية الخاصة بجهازك وتحديد أنواع الكائنات التي يكتشفها التطبيق خلال التشغيل. يقوم أمان نقطة النهاية من Kaspersky دائمًا بفحص نظام التشغيل بحثًا عن فيروسات أو الفيروسات المتنقلة أو فيروسات أحصنة طروادة. لا يمكنك تعطيل فحص هذه الأنواع من الكائنات. فقد تؤدي مثل هذه البرمجيات الضارة إلى حدوث ضرر بالغ بالكمبيوتر. للمزيد من الحماية على جهازك، يمكنك توسيع نطاق أنواع الكائنات القابلة للاكتشاف بواسطة تمكين مراقبة البرامج القانونية التي يمكن للمجرمين استخدامها لإلحاق الضرر بالكمبيوتر أو بياناتك الشخصية.

استخدام وضع توفير الطاقة

يعتبر استهلاك التطبيقات للطاقة أمرًا هامًا بالنسبة لأجهزة الكمبيوتر المحمولة. وعادةً ما تستخدم المهام المجدولة من Kaspersky Endpoint Security موارد كبيرة. فعندما يعمل الكمبيوتر على طاقة البطارية، يمكنك استخدام وضع توفير الطاقة لاستهلاك الطاقة باعتدال أكثر.

في وضع توفير الطاقة، يتم تأجيل المهام المجدولة التالية تلقائيًا:

- مهمة التحديث؛
- مهمة الفحص الكامل؛
- مهمة فحص المناطق الحرجة؛
- مهمة فحص مخصص؛
- مهمة التحقق من السلامة.

سواء تم تمكين وضع توفير الطاقة أم لا، يوقف Kaspersky Endpoint Security مهام التشفير عندما يتحول الكمبيوتر المحمول إلى طاقة البطارية. يستأنف التطبيق مهام التشفير عندما يتحول الكمبيوتر المحمول من طاقة البطارية إلى طاقة التيار الرئيسي.

منح موارد الكمبيوتر إلى التطبيقات الأخرى

قد يؤدي استهلاك موارد الكمبيوتر بواسطة Kaspersky Endpoint Security عند فحص الكمبيوتر إلى زيادة الحمل على الأنظمة الفرعية لوحدة المعالجة المركزية ومحرك الأقراص الثابت بالإضافة إلى التأثير على أداء التطبيقات الأخرى. لحل مشكلة التشغيل الفوري خلال الحمل الزائد على وحدة المعالجة المركزية والنظم الفرعية لمحرك القرص الثابت، يستطيع Kaspersky Endpoint Security منح الموارد للتطبيقات الأخرى.

استخدام تقنية التنظيف المتقدمة

يمكن للتطبيقات الضارة الآن اختراق أضعف مستويات نظام التشغيل، مما يجعل من القضاء عليها أمرًا مستحيلاً بشكل فعلي. بعد اكتشاف نشاط خبيث في نظام التشغيل، يقوم Kaspersky Endpoint Security بإجراء تنظيف شامل يستخدم فيه تقنية التنظيف المتقدمة. تقنية التنظيف المتقدمة تهدف إلى تطهير نظام التشغيل من التطبيقات الضارة التي بدأت بالفعل عملياتها في ذاكرة الوصول العشوائي والتي تمنع Kaspersky Endpoint Security من إزالتها باستخدام طرق أخرى. يتم إبطال التهديد كنتيجة. أثناء تقدم إجراء التنظيف المتقدم، ننصحك بعدم بدء أي عمليات جديدة أو تحرير تسجيل نظام التشغيل. تستخدم تقنية التنظيف المتقدمة موارد نظام التشغيل بدرجة كبيرة، وهو ما يبطئ من التطبيقات الأخرى.

بعد إتمام عملية التنظيف المتقدم على كمبيوتر يعمل بنظام التشغيل Microsoft Windows لمحطات العمل، يطلب Kaspersky Endpoint Security إذن المستخدم لإعادة تمهيد الكمبيوتر. بعد إعادة تمهيد النظام، يقوم Kaspersky Endpoint Security بحذف ملفات البرمجيات الضارة وبدء فحص كامل "بسيط" للكمبيوتر.

يستحيل المطالبة بإعادة التشغيل على كمبيوتر يعمل بنظام التشغيل Microsoft Windows للخوادم نظرًا لخصائص Kaspersky Endpoint Security. وقد يؤدي إعادة تمهيد خادم الملفات غير المخطط له إلى حدوث مشاكل تتضمن عدم توفر بيانات خادم الملفات مؤقتًا أو فقدان البيانات غير المحفوظة. ويوصى بإعادة تمهيد خادم الملفات وفقًا للجدول تمامًا. هذا هو السبب وراء تعطيل تقنية التنظيف المتقدمة بشكل افتراضي لخوادم الملفات.

في حالة اكتشاف إصابة نشطة على خادم الملفات، يتم ترحيل حدث إلى Kaspersky Security Center مع معلومات بالحاجة إلى التنظيف النشط. لتنظيف عدوى نشطة لخادم، قم بتمكين تقنية التنظيف النشط للخوادم وابدأ مهمة جماعية فحص البرامج الضارة في وقت مناسب لمستخدمي الخادم.

تمكين أو تعطيل وضع توفير الطاقة

لتمكين أو تعطيل وضع توفير الطاقة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.

إعدادات Kaspersky Endpoint Security for Windows

3. في القسم **الأداء**، استخدم خانة الاختيار **تأجيل تشغيل المهام المجدولة أثناء التشغيل على طاقة البطارية** لتمكين وضع توفير الطاقة أو تعطيله.

عند تمكين وضع توفير الطاقة وتشغيل الكمبيوتر باستخدام طاقة البطارية، لا يتم تشغيل المهام التالية حتى وإن كانت مجدولة:

- تحديث
- فحص كامل
- فحص المناطق الحرجة
- فحص مخصص

- التحقق من السلامة
- فحص IOC.

4. احفظ تغييراتك.

تمكين أو تعطيل منح الموارد للتطبيقات الأخرى

قد يؤدي استهلاك موارد الكمبيوتر بواسطة Kaspersky Endpoint Security عند فحص الكمبيوتر إلى زيادة الحمل على الأنظمة الفرعية لوحدة المعالجة المركزية. وقد يؤدي هذا إلى إبطاء التطبيقات الأخرى. ولتحسين الأداء، يوفر Kaspersky Endpoint Security وضعًا لنقل الموارد إلى التطبيقات الأخرى. وفي هذا الوضع، يستطيع نظام التشغيل تقليل أولوية سلاسل مهام فحص Kaspersky Endpoint Security عندما يكون حمل وحدة المعالجة المركزية مرتفعًا. ويسمح هذا بإعادة توزيع موارد نظام التشغيل على التطبيقات الأخرى. وبالتالي، ستتلقى مهام الفحص وقتًا أقل لوحدة المعالجة المركزية. ونتيجة لذلك، سيستغرق Kaspersky Endpoint Security وقتًا أطول لفحص الكمبيوتر. بشكل افتراضي، يتم تكوين التطبيق بحيث يتم السماح بالتنازل عن الموارد للتطبيقات الأخرى.

لتمكين التنازل عن الموارد لتطبيقات أخرى أو تعطيله:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.

2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.

إعدادات Kaspersky Endpoint Security for Windows

3. في القسم **الأداء**، استخدم خانة الاختيار **التنازل عن موارد لتطبيقات أخرى** لتمكين أو تعطيل التنازل عن الموارد للتطبيقات الأخرى.

4. احفظ تغييراتك.

أفضل الممارسات لتحسين أداء Kaspersky Endpoint Security

عند نشر Kaspersky Endpoint Security لنظام التشغيل Windows، يمكنك استخدام التوصيات التالية لتكوين حماية الكمبيوتر وتحسين الأداء.

عام

قم بتكوين الإعدادات العامة للتطبيق وفقًا للتوصيات التالية:

1. قم ترقية Kaspersky Endpoint Security إلى أحدث إصدار.

   في الإصدارات الأحدث من التطبيق تم إصلاح الأخطاء وتحسين الاستقرار وتحسين الأداء.

2. قم بتمكين مكونات الحماية بالإعدادات الافتراضية.

   تعتبر الإعدادات الافتراضية هي الأمثل. ويوصي خبراء Kaspersky بهذه الإعدادات. وتوفر الإعدادات الافتراضية مستوى الحماية الموصى به والاستخدام الأمثل للموارد. وإذا لزم الأمر، يمكنك استعادة إعدادات التطبيق الافتراضية.

3. قم بتمكين ميزات تحسين أداء التطبيق.

   يحتوي التطبيق على ميزات تحسين الأداء: وضع توفير الطاقة والتنازل عن الموارد لتطبيقات أخرى. وتأكد من تمكين هذه الخيارات.

فحص البرامج الضارة في محطات العمل

يوصى بتمكين "الفحص في الخلفية" لفحص البرامج الضارة لمحطات العمل. الفحص في الخلفية هو وضع فحص من Kaspersky Endpoint Security لا يقوم بعرض إخطارات للمستخدم. تتطلب عملية الفحص في الخلفية استخدام موارد أقل من جهاز الكمبيوتر بخلاف أنواع الفحص الأخرى (مثل الفحص الكامل). وفي هذا الوضع يفحص برنامج Kaspersky Endpoint Security كائنات بدء التشغيل ومقطع التمهيد وذاكرة النظام وقسم النظام. وتعتبر إعدادات الفحص في الخلفية هي الأمثل. ويوصي خبراء Kaspersky بهذه الإعدادات. وبالتالي لإجراء فحص برامج ضارة للكمبيوتر، يمكنك استخدام وضع الفحص في الخلفية فقط دون استخدام مهام الفحص الأخرى.

إذا كان الفحص في الخلفية لا يناسب احتياجاتك، فقم بتكوين مهمة فحص البرامج الضارة وفقًا للتوصيات التالية:

1. قم بتكوين جدولة فحص الكمبيوتر المثلى.

   يمكنك تكوين المهمة لتعمل عندما يعمل الكمبيوتر تحت الحد الأدنى من الحمل. على سبيل المثال، يمكنك تكوين المهمة لتعمل ليلاً أو في عطلات نهاية الأسبوع.

   إذا أوقف المستخدمون تشغيل أجهزة الكمبيوتر الخاصة بهم في نهاية اليوم، فيمكنك تكوين مهمة الفحص على النحو التالي:

   - قم بتمكين التشغيل عن بُعد عبر الشبكة المحلية. وتتيح ميزة التشغيل عن بُعد عبر الشبكة المحلية تشغيل الكمبيوتر عن بُعد بواسطة إرسال إشارة خاصة عبر الشبكة المحلية. ولاستخدام هذه الميزة، يجب تمكين التشغيل عن بُعد عبر الشبكة المحلية في إعدادات BIOS. يمكنك أيضًا إيقاف تشغيل الكمبيوتر تلقائيًا بعد انتهاء الفحص.
   - قم بتعطيل ميزة "تشغيل المهام الفائتة". وسيتخطى Kaspersky Endpoint Security المهام الفائتة عندما يقوم المستخدم بتشغيل الكمبيوتر. وقد يؤدي تشغيل المهام بعد تشغيل الكمبيوتر إلى إزعاج المستخدم لأن الفحص يتطلب التزامًا كبيرًا بالموارد.

   إذا لم تتمكن من تكوين جدولة الفحص المثلى، فاضبط المهام لتعمل فقط عندما يكون الكمبيوتر خاملاً. يبدأ Kaspersky Endpoint Security مهمة الفحص إذا كان الكمبيوتر مقفلاً أو إذا كانت شاشة التوقف قيد التشغيل. إذا قاطعت تنفيذ المهمة، على سبيل المثال بواسطة إلغاء تأمين الكمبيوتر، يجري Kaspersky Endpoint Security تشغيل المهمة تلقائيًا، ويستمر من النقطة التي توقفت عندها.

2. حدد نطاق فحص.

   حدد الكائنات التالية لفحصها:

   - ذاكرة Kernel؛

- العمليات قيد التشغيل وكائنات بدء التشغيل؛
- قطاعات التمهيد؛
- محرك أقراص النظام (%systemdrive%).

3. قم بتشغيل تقنيتي iSwift وiChecker.

- تقنية iSwift.

تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.

- تقنية iChecker.

تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).

يمكنك فقط تشغيل تقنيي iSwift و iChecker في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint Security. ولا يمكنك تشغيل هاتين التقنيتين في Kaspersky Security Center Web Console.

4. قم بتعطيل فحص الأرشيفات المحمية بكلمة مرور.

في حالة تم تمكين فحص الأرشيفات المحمية بكلمة مرور، سيتم عرض مطالبة بكلمة مرور قبل فحص الأرشيف. ولأنه يوصى بجدولة المهمة خارج ساعات العمل، لا يستطيع المستخدم إدخال كلمة المرور. ويمكنك فحص الأرشيفات المحمية بكلمة مرور يدويًا.

فحص البرامج الضارة على الخوادم

قم بتكوين مهمة فحص البرامج الضارة وفقًا للتوصيات التالية:

1. قم بتكوين جدولة فحص الكمبيوتر المثلى.

يمكنك تكوين المهمة لتعمل عندما يعمل الكمبيوتر تحت الحد الأدنى من الحمل. على سبيل المثال، يمكنك تكوين المهمة لتعمل ليلاً أو في عطلات نهاية الأسبوع.

2. قم بتشغيل تقنيتي iSwift وiChecker.

- تقنية iSwift.

تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.

- تقنية iChecker.

تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).

يمكنك فقط تشغيل تقنيي iSwift و iChecker في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint Security. ولا يمكنك تشغيل هاتين التقنيتين في Kaspersky Security Center Web Console.

3. قم بتعطيل فحص الأرشيفات المحمية بكلمة مرور.

في حالة تم تمكين فحص الأرشيفات المحمية بكلمة مرور، سيتم عرض مطالبة بكلمة مرور قبل فحص الأرشيف. ولأنه يوصى بجدولة المهمة خارج ساعات العمل، لا يستطيع المستخدم إدخال كلمة المرور. ويمكنك فحص الأرشيفات المحمية بكلمة مرور يدويًا.

Kaspersky Security Network

لحماية الكمبيوتر الخاص بك بشكل أكثر فاعلية، يستخدم برنامج Kaspersky Endpoint Security بيانات تم تلقيها من المستخدمين من جميع أنحاء العالم. تم تصميم Kaspersky Security Network للحصول على هذه البيانات.

تعتبر شبكة Kaspersky Security Network (KSN) بنية تحتية من الخدمات السحابية التي توفر الوصول إلى قاعدة معارف Kaspersky على الإنترنت والتي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج. ويعد استخدام البيانات من Kaspersky Security Network ضمانًا لسرعة وقت استجابات Kaspersky Endpoint Security عند مواجهة تهديدات جديدة، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية ويقلل من خطر وقوع الحالات الإيجابية الزائفة. إذا كنت تشارك في شبكة Kaspersky Security Network، فإن خدمات شبكة KSN تقوم بتزويد برنامج Kaspersky Endpoint Security بمعلومات حول فئة وسمعة الملفات التي تم فحصها، بالإضافة إلى معلومات حول سمعة عناوين الويب التي تم فحصها.

قم بتحرير إعدادات Kaspersky Security Network وفقًا للتوصيات التالية:

1. تعطيل وضع KSN الموسع.

إن وضع KSN الموسع هو وضع يقوم فيه Kaspersky Endpoint Security بإرسال بيانات إضافية إلى Kaspersky.

2. تكوين Kaspersky Private Security Network.

Kaspersky Private Security Network عبارة عن حل يتيح لمستخدمي أجهزة الكمبيوتر التي تستضيف Kaspersky Endpoint Security أو غيره من تطبيقات Kaspersky الحصول على حق الوصول إلى قواعد بيانات السمعة من Kaspersky، وإلى البيانات الإحصائية الأخرى دون إرسال بيانات إلى Kaspersky من أجهزة الكمبيوتر الخاصة بهم.

3. تمكين وضع السحابة.

الوضع السحابي تُشير إلى وضع تشغيل التطبيق الذي يستخدم فيه برنامج Kaspersky Endpoint Security إصدارًا خفيفًا من قواعد بيانات مكافحة الفيروسات. تدعم Kaspersky Security Network تشغيل التطبيق عند استخدام إصدار خفيف من قواعد بيانات مكافحة الفيروسات. يُتيح لك الإصدار الخفيف من قواعد بيانات مكافحة الفيروسات استخدام نصف ذاكرة الوصول العشوائي الموجودة بجهاز الكمبيوتر تقريبًا والتي يمكن استخدامها مع قواعد البيانات المعتادة بطريقة أخرى. إذا لم تشارك في Kaspersky Security Network أو إذا تم تعطيل الوضع السحابي، يقوم برنامج Kaspersky Endpoint Security بتنزيل الإصدار الكامل من قواعد بيانات مكافحة الفيروسات من خوادم Kaspersky.

تشفير البيانات

يتيح لك Kaspersky Endpoint Security تشفير الملفات والمجلدات المخزنة على محركات الأقراص المحلية ومحركات الأقراص القابلة للإزالة، أو محركات الأقراص القابلة للإزالة ومحركات الأقراص الصلبة بأكملها. ويقلل تشفير البيانات من خطورة تسريب المعلومات والذي قد يحدث عند فقدان كمبيوتر محمول أو محرك قرص قابل للإزالة أو محرك قرص صلب أو سرقته، أو عند الوصول إلى البيانات عن طريق مستخدمين أو تطبيقات غير مصرح به. يستخدم برنامج Kaspersky Endpoint Security خوارزمية التشفير معيار التشفير المتقدم (AES).

في حالة انتهاء صلاحية الترخيص، لا يقوم التطبيق بتشفير البيانات الجديدة مع الاحتفاظ بتشفير البيانات القديمة المشفرة والمتوفرة للاستخدام. وفي هذه الحالة، يتطلب تشفير بيانات جديدة تفعيل التطبيق بترخيص جديد يسمح باستخدام التشفير.

إذا انتهت صلاحية الترخيص أو تم انتهاك اتفاقية ترخيص المستخدم النهائي أو تمت إزالة مفتاح ترخيص أو Kaspersky Endpoint Security أو مكونات التشفير، فلا يمكن أن نضمن حالة تشفير الملفات التي تم تشفيرها سابقًا. وذلك بسبب أن بعض التطبيقات، مثل Microsoft Office Word، تقوم بإنشاء نسخة مؤقتة للملفات أثناء التحرير. عند حفظ الملف الأصلي، تستبدل النسخة المؤقتة الملف الأصلي. ونتيجة لذلك، يظل الملف غير مشفر على كمبيوتر ليس له وظيفة تشفير أو يتعذّر الوصول إليه.

يعرض Kaspersky Endpoint Security جوانب حماية البيانات التالية:

- **التشفير على مستوى الملف على محركات الأقراص الثابتة المحلية**. يمكنك تجميع قوائم الملفات حسب الملحق أو مجموعة الملحقات وقوائم المجلدات المخزنة على محركات أقراص الكمبيوتر المحلية، وإنشاء قواعد لتشفير الملفات التي تم إنشاؤها بواسطة تطبيقات محددة. بعد تطبيق سياسة، يقوم Kaspersky Endpoint Security بتشفير الملفات التالية وفك تشفيرها:
  - الملفات التي تمت إضافتها بشكل فردي إلى قوائم التشفير وفك التشفير؛
  - الملفات المخزنة في المجلدات التي تمت إضافتها إلى قوائم التشفير وفك التشفير؛
  - الملفات التي تم إنشاؤها بواسطة تطبيقات منفصلة.
- **تشفير محركات الأقراص القابلة للإزالة**. يمكنك تحديد قاعدة التشفير الافتراضية وفقًا لأي تطبيق يقوم بتطبيق نفس الإجراء على جميع محركات الأقراص القابلة للإزالة، أو تحديد قواعد التشفير لمحركات الأقراص القابلة للإزالة الفردية.

  تمتلك قاعدة التشفير الافتراضية أولوية منخفضة عن قواعد التشفير التي تم إنشاؤها لمحركات الأقراص القابلة للإزالة الفردية. تمتلك قواعد التشفير التي تم إنشاؤها لمحركات الأقراص القابلة للإزالة ذات طراز الأجهزة المحدد أولوية منخفضة عن قواعد التشفير التي تم إنشاؤها لمحركات الأقراص القابلة للإزالة ذات مُعرف جهاز محدد.

  لتحديد قاعدة تشفير للملفات على محرك قرص قابل للإزالة، يقوم Kaspersky Endpoint Security بفحص ما إذا كان طراز ومعرف الجهاز معروفين أم لا. ثم يقوم التطبيق بإجراء إحدى العمليات التالية:
  - إذا كان طراز الجهاز معروفًا فقط، فيستخدم التطبيق قاعدة التشفير (إن وجدت) التي تم إنشاؤها لمحركات لأقراص القابلة للإزالة الخاصة بطراز الجهاز المحدد.
  - إذا كان معرف الجهاز معروفًا فقط، فيستخدم التطبيق قاعدة التشفير (إن وجدت) التي تم إنشاؤها لمحركات الأقراص القابلة للإزالة ذات معرف الجهاز المحدد.
  - إذا كان طراز ومعرف الجهاز معروفان، فيطبق التطبيق قاعدة التشفير (إن وجدت) التي تم إنشاؤها لمحركات الأقراص القابلة للإزالة ذات معرف الجهاز المحدد. إذا لم توجد مثل هذه القاعدة، ولكن توجد قاعدة تشفير تم إنشاؤها لمحركات الأقراص القابلة للإزالة ذات طراز الجهاز المحدد، فيطبق التطبيق هذه القاعدة. إذا لم يتم تحديد قاعدة تشفير لمعرف الجهاز المحدد ولا لطراز الجهاز المحدد، فيطبق التطبيق قاعدة التشفير الافتراضية.
  - إذا لم يكن طراز أو معرف الجهاز معروفين، فيستخدم التطبيق قاعدة التشفير الافتراضية.

  يتيح لك التطبيق إعداد قرص قابل للإزالة لاستخدام البيانات المشفرة المخزنة عليه في الوضع المحمول. بعد تمكين الوضع المحمول، يمكنك الوصول إلى الملفات المشفرة على محركات الأقراص القابلة للإزالة المتصلة بكمبيوتر بدون وظائف تشفير.
- **إدارة قواعد وصول التطبيق إلى الملفات المشفرة**. بالنسبة لأي تطبيق، يمكنك إنشاء قاعدة وصول للملف المشفر التي تمنع الوصول إلى الملفات المشفرة أو تتيح الوصول إليها كنص مشفر فقط، والذي يتكون من سلسلة من الأحرف تم الحصول عليها عند تطبيق التشفير.

- **إنشاء حزم مشفرة**. يمكنك إنشاء أرشيفات مشفرة وحماية الوصول إلى مثل هذه الأرشيفات باستخدام كلمة مرور. يمكن الوصول إلى محتويات الأرشيفات المشفرة فقط عن طريق إدخال كلمات المرور التي من خلالها قمت بحماية الوصول إلى تلك الأرشيفات. ويمكن نقل هذه الأرشيفات بأمان عبر الشبكات أو على محركات الأقراص القابلة للإزالة.

- **تشفير القرص بالكامل**. يمكنك تحديد تقنية تشفير: تشفير القرص من Kaspersky أو تشفير محرك الأقراص من BitLocker (المشار إليها فيما بعد بمجرد "BitLocker").

إن BitLocker تقنية تمثل جزءًا من نظام التشغيل Windows. إذا كان الكمبيوتر مجهزًا بالوحدة النمطية للنظام الأساسي الموثوق به (TPM)، فتستخدمها تقنية BitLocker لتخزين ملفات الاسترداد التي توفر الوصول إلى محرك الأقراص المشفر. عند بدء الكمبيوتر، تطلب تقنية BitLocker مفاتيح استرداد محرك الأقراص الصلبة من الوحدة النمطية للنظام الأساسي الموثوق به وتقوم بإلغاء قفل الجهاز. يمكنك تكوين استخدام كلمة مرور و/أو رمز PIN للوصول إلى مفاتيح الاسترداد.

يمكنك تحديد قاعد تشفير القرص بالكامل الافتراضية وإنشاء قائمة بمحركات الأقراص الثابتة ليتم استثناؤها من التشفير. ينفذ Kaspersky Endpoint Security تشفير القرص بالكامل حسب المقطع بعد تطبيق سياسة Kaspersky Security Center. يقوم التطبيق بتشفير جميع الأجزاء المنطقية لمحركات الأقراص الصلبة في وقت واحد.

بعد تشفير محركات الأقراص الصلبة للنظام، عند بدء التشغيل التالي للكمبيوتر، يجب أن يكمل المستخدم المصادقة باستخدام وكيل المصادقة قبل إمكانية الوصول إلى محركات الأقراص الصلبة وتحميل نظام التشغيل. ويتطلب ذلك إدخال كلمة المرور للرمز المميز أو البطاقة الذكية الموصلة بالكمبيوتر، أو اسم المستخدم وكلمة مرور حساب وكيل المصادقة الذي تم إنشاؤه بواسطة مسؤول الشبكة المحلية باستخدام مهمة إدارة حسابات وكيل المصادقة. وتعتمد هذه الحسابات على حسابات Microsoft Windows التي يقوم المستخدمون من خلالها بتسجيل الدخول إلى نظام التشغيل. يمكنك كذلك استخدام تقنية تسجيل الدخول الأحادي (SSO) التي تتيح لك الولوج تلقائيًا إلى نظام التشغيل باستخدام اسم المستخدم وكلمة المرور لحساب وكيل المصادقة.

إذا قمت بنسخ الكمبيوتر احتياطيًا ثم قمت بتشفير بيانات الكمبيوتر، ثم بعد ذلك قمت باستعادة النسخة الاحتياطية للكمبيوتر وتشفير بيانات الكمبيوتر مرة أخرى، فيقوم Kaspersky Endpoint Security بإنشاء تكرارات حسابات وكيل المصادقة. لإزالة الحسابات المكررة، يجب استخدام أداة klmover المزودة بمفتاح `dupfix`. يتم تضمين أداة klmover في إصدار Kaspersky Security Center. يمكنك قراءة المزيد حول تشغيلها في تعليمات Kaspersky Security Center.

لا يمكن الوصول إلى محركات الأقراص الصلبة المشفرة إلا من أجهزة الكمبيوتر التي تم تثبيت Kaspersky Endpoint Security المزود بوظائف تشفير القرص بالكامل عليها. ويقلل هذا الإجراء الاحتياطي من مخاطر تسريب البيانات من محرك قرص صلب مشفر عند محاولة الوصول إليه خارج الشبكة المحلية للشركة.

لتشفير محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة، يمكنك استخدام وظيفة تشفير مساحة القرص المستخدمة فقط. من المستحسن استخدام هذه الوظيفة للأجهزة الجديدة فقط التي لم يتم استخدامها مسبقًا. إذا كنت تقوم بتشفير جهاز ما مستخدم بالفعل، فمن المستحسن تشفير الجهاز بالكامل. يضمن ذلك حماية كل البيانات – حتى الملفات التي تم حذفها والتي قد لا تزال تحتوي على معلومات يمكن استرجاعها.

قبل بدء التشفير، يحصل Kaspersky Endpoint Security على خريطة قطاعات نظام الملفات. تتضمن الدفعة الأولى من التشفير القطاعات الممتلئة بالملفات في اللحظة التي يبدأ فيها التشفير. وتتضمن الدفعة الثانية من التشفير القطاعات التي تمت الكتابة عليها بعد بدء التشفير. بعد اكتمال التشفير، تكون كل القطاعات التي تحتوي على بيانات قد تم تشفيرها.

بعد اكتمال التشفير وقيام المستخدم بحذف ملف، تصبح القطاعات التي كان قد تم تخزين الملف الذي تم حذفه عليها متوفرة لتخزين معلومات جديدة على مستوى نظام الملفات ولكن تظل مشفرة. وهكذا، عندما تتم كتابة الملفات إلى جهاز جديد ويتم تشفير الجهاز بشكل منتظم باستخدام وظيفة **تشفير مساحة القرص المستخدمة فقط**، سيتم تشفير جميع القطاعات بعد مرور بعض الوقت.

ويتم تقديم البيانات التي تحتاج إلى فك تشفير من قبل خادم إدارة Kaspersky Security Center الذي يتحكم في الكمبيوتر في وقت التشفير. إذا خضع الكمبيوتر المحتوي على الكائنات المشفرة إلى الإدارة من خلال خادم إدارة مختلف لسببٍ ما، فيمكنك الحصول على صلاحية الوصول إلى البيانات المشفرة بإحدى الطرق التالية:

- خوادم الإدارة بنفس الترتيب التسلسلي:

- إنك لا تحتاج إلى اتخاذ أي إجراءات إضافية. سيظل المستخدم متمتعًا بإمكانية الوصول إلى الكائنات المشفرة. يتم توزيع مفاتيح التشفير لكل خوادم الإدارة.

- خوادم إدارة منفصلة:

- اطلب الحصول على صلاحية الوصول إلى الكائنات المشفرة من مسؤول شبكة LAN.

- استعادة البيانات الموجودة على الأجهزة المشفرة باستخدام أداة الاستعادة.

- استعادة تكوين خادم إدارة Kaspersky Security Center الذي تحكم في الكمبيوتر في وقت التشفير من نسخة احتياطية واستخدم هذا التكوين على خادم الإدارة الذي يتحكم الآن في الكمبيوتر الذي يتضمن الكائنات المشفرة.

في حال عدم توافر وصول إلى البيانات المشفرة، اتبع التعليمات الخاصة للعمل مع البيانات المشفرة (استعادة الوصول إلى الملفات المشفرة، العمل مع الأجهزة المشفرة في حالة عدم توافر الوصول إليها).

قيود وظيفة التشفير

يخضع تشفير البيانات للقيود التالية:

- يقوم التطبيق بإنشاء ملفات الخدمة أثناء التشفير. يلزم توفر 0.5% من المساحة الخالية غير المجزئة على محرك الأقراص الصلبة لتخزينها. في حال عدم وجود ما يكفي من المساحة المتاحة غير المجزأة على محرك الأقراص الصلبة، فإن التشفير لن يبدأ حتى يتم توفير مساحة كافية.
- يمكنك إدارة كل مكونات تشفير البيانات في Kaspersky Security Center وفي Kaspersky Security Center Web Console. في Kaspersky Security Center Cloud Console، يمكنك فقط إدارة Bitlocker.
- يتوافر تشفير البيانات فقط عند استخدام Kaspersky Endpoint Security مع نظام إدارة Kaspersky Security Center أو Kaspersky Security Center Cloud Console (BitLocker فقط). لا يمكن تشفير البيانات عند استخدام Kaspersky Endpoint Security في وضع عدم الاتصال بالإنترنت لأن Kaspersky Endpoint Security يخزن مفاتيح التشفير في Kaspersky Security Center.
- إذا كان Kaspersky Endpoint Security مثبتًا على كمبيوتر يعمل بنظام تشغيل Microsoft Windows for File Servers، فلن يتوفر إلا تشفير القرص بالكامل باستخدام تقنية تشفير محرك الأقراص من BitLocker. إذا كان Kaspersky Endpoint Security مثبتًا على كمبيوتر يعمل بنظام Windows لأجهزة محطات العمل، فسوف تتوفر وظيفة تشفير البيانات بشكلٍ كامل.

لا يتوفر تشفير القرص بالكامل باستخدام تقنية تشفير القرص من Kaspersky لمحركات الأقراص الصلبة التي لا تفي بمتطلبات الأجهزة والبرامج.

التوافق بين تشفير القرص بالكامل من Kaspersky Endpoint Security وتطبيق Kaspersky Anti-Virus for UEFI غير مدعوم. يبدأ تطبيق Kaspersky Anti-Virus for UEFI قبل تحميل نظام التشغيل. عند استخدام تشفير القرص بالكامل، فإن التطبيق سيكتشف عدم وجود نظام تشغيل مثبت على جهاز الكمبيوتر. ونتيجةً لذلك، عمل Kaspersky Anti-Virus for UEFI سوف ينتهي بخطأ. التشفير على مستوى الملف (FLE) لا يؤثر على عمل Kaspersky Anti-Virus for UEFI.

يدعم Kaspersky Endpoint Security التكوينات التالية:

- محركات أقراص HDD وSSD وUSB.

تدعم تقنية تشفير القرص من Kaspersky (FDE) العمل مع أقراص SSD مع الحفاظ على الأداء وعمر الخدمة لمحركات أقراص SSD.

- محركات الأقراص الموصلة عبر ناقل: SCSI وATA وIEEE1934 وUSB وRAID وSAS وSATA وNVME.
- محركات الأقراص غير القابلة للإزالة المتصلة عبر ناقل SD أو MMC.
- محركات الأقراص ذات مقاطع 512 بايت.
- محركات الأقراص ذات مقاطع 4096 بايت التي تحاكي 512 بايت.
- محركات الأقراص من النوع التالي من المقاطع: GPT وMBR وVBR (محركات الأقراص القابلة للإزالة).
- برنامج مضمن لمعيار UEFI 64 وLegacy BIOS.
- برنامج مضمن لمعيار UEFI مع دعم التمهيد الآمن.

التمهيد الآمن تقنية مصممة للتحقق من التوقيعات الرقمية لتطبيقات وبرامج تشغيل أداة تحميل UEFI. يمنع التمهيد الآمن بدء تشغيل تطبيقات وبرامج تشغيل UEFI غير الموقعة أو الموقعة من قبل ناشرين غير معروفين. يدعم تشفير القرص من Kaspersky (FDE) التمهيد الآمن بالكامل. ويتم توقيع عامل المصادقة بواسطة شهادة Microsoft Windows UEFI Driver Publisher.

على بعض الأجهزة (على سبيل المثال، Microsoft Surface Pro وMicrosoft Surface Pro 2)، قد يتم تثبيت قائمة قديمة من شهادات التحقق من التوقيع الرقمي افتراضيًا. قبل تشفير محرك الأقراص، تحتاج إلى تحديث قائمة الشهادات.

- برنامج مضمن لمعيار UEFI مع دعم التمهيد السريع.

التمهيد السريع تقنية تساعد الكمبيوتر على بدء التشغيل بشكل أسرع. وعند تمكين تقنية التمهيد السريع، يقوم الكمبيوتر عادة بتحميل الحد الأدنى من مجموعة برامج تشغيل UEFI المطلوبة لبدء نظام التشغيل. عند تمكين تقنية التمهيد السريع، قد لا تعمل لوحات مفاتيح USB وأجهزة الماوس ورموز USB المميزة ولوحات اللمس وشاشات اللمس أثناء تشغيل وكيل المصادقة.

لاستخدام تشفير القرص من Kaspersky (FDE)، يوصى بتعطيل تقنية التمهيد السريع. يمكنك استخدام أداة اختبار FDE لاختبار تشغيل تشفير القرص من Kaspersky (FDE).

لا يدعم Kaspersky Endpoint Security التكوينات التالية:

- يوجد مُحمل التمهيد على محرك أقراص بينما يوجد نظام التشغيل على محرك أقراص مختلف.
- يتضمن النظام برنامج مضمن للمقياس UEFI 32.
- يحتوي النظام على تقنية Intel® Rapid Start Technology ومحركات الأقراص التي تتضمن قسم إسبات حتى عند تعطيل تقنية Intel® Rapid Start.
- محركات الأقراص بتنسيق MBR التي تتضمن أكثر من 10 أقسام ممتدة.
- يحتوي النظام على ملف مبادلة موجود على محرك أقراص غير تابع للنظام.
- نظام متعدد التمهيد مع أنظمة تشغيل متعددة مثبتة في الوقت نفسه.
- أقسام ديناميكية (يتم دعم الأقسام الرئيسية فقط).
- محركات الأقراص مع مساحة القرص غير المجزئة الخالية بنسبة أقل من 0.5%.
- محركات الأقراص مع حجم قطاع مختلف عن 512 بايت أو 4096 بايت والتي تحاكي 512 بايت.
- محركات أقراص مختلطة.
- يحتوي النظام على أدوات تحميل خارجية.
- محركات الأقراص التي تتضمن أدلة NTFS مضغوطة.
- لا تتوافق تقنية تشفير القرص من Kaspersky (FDE) مع تقنيات تشفير القرص الكامل الأخرى (مثل BitLocker وMcAfee Drive Encryption وWinMagic SecureDoc).
- لا تتوافق تقنية تشفير القرص من Kaspersky (FDE) مع تقنية ExpressCache.
- لا يتم دعم إنشاء أقسام وحذفها وتعديلها على محرك أقراص مشفر. قد تفقد البيانات.
- تنسيق نظام الملفات غير مدعوم. قد تفقد البيانات.

إذا كنت بحاجة إلى تهيئة محرك أقراص تم تشفيره باستخدام تقنية تشفير القرص من Kaspersky (FDE)، فقم بتهيئة محرك الأقراص على جهاز كمبيوتر لا يحتوي على Kaspersky Endpoint Security for Windows واستخدم تشفير القرص الكامل فقط.

قد يتم تحديد محرك أقراص مشفر مهيأ بخيار التهيئة السريعة عن طريق الخطأ على أنه مشفر في المرة التالية التي يتم فيها توصيله بجهاز كمبيوتر مثبت عليه Kaspersky Endpoint Security for Windows. ولن تكون بيانات المستخدم متاحة.

- لا يدعم وكيل المصادقة أكثر من 100 حساب.
- لا تتوافق تقنية تسجيل الدخول الأحادي مع التقنيات الأخرى لمطوري الطرف الثالث.
- لا يتم دعم تقنية تشفير القرص من Kaspersky (FDE) في طرازات الأجهزة التالية:
  - Dell Latitude E6410 (وضع UEFI)
  - HP Compaq nc8430 (وضع BIOS القديم)
  - Lenovo ThinkCenter 8811 (وضع BIOS القديم).
- لا يدعم عامل المصادقة العمل مع رموز USB المميزة عند تمكين دعم USB القديم. ستكون المصادقة المستندة إلى كلمة المرور فقط ممكنة على الكمبيوتر.
- عند تشفير محرك أقراص في وضع BIOS القديم، يُنصح بتمكين دعم USB القديم على الطرازات التالية من الأجهزة:
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550

- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (اللوحة الأم)

تغيير طول مفتاح التشفير (AES56 / AES256)

يستخدم برنامج Kaspersky Endpoint Security خوارزمية التشفير معيار التشفير المتقدم (AES). يدعم Kaspersky Endpoint Security خوارزمية تشفير AES بطول مفتاح فعال يبلغ 256 أو 56 بت. تعتمد خوارزمية تشفير البيانات على مكتبة تشفير AES المضمنة في حزمة التوزيع: تشفير قوي (AES256) أو تشفير خفيف (AES56). يتم تثبيت مكتبة تشفير AES مع التطبيق.

إن تغيير طول مفتاح التشفير متاح فقط في الإصدار 11.2.0 من Kaspersky Endpoint Security أو إصدار أحدث.

يتألف تغيير طول مفتاح التشفير من الخطوات التالية:

1. قم بفك تشفير الكائنات التي قام بتشفيرها Kaspersky Endpoint Security قبل بدء تغيير طول مفتاح التشفير:
   a. فك تشفير محركات الأقراص الصلبة.
   b. فك تشفير الملفات الموجودة على محركات الأقراص المحلية.
   c. فك تشفير محركات الأقراص القابلة للإزالة.

بعد تغيير طول مفتاح التشفير، تُصبح الكائنات التي تم تشفيرها مسبقًا غير متوفرة.

2. إزالة Kaspersky Endpoint Security.
3. قم بتثبيت Kaspersky Endpoint Security من حزمة توزيع Kaspersky Endpoint Security التي تحتوي على مكتبة تشفير مختلفة.

يمكنك أيضًا تغيير طول مفتاح التشفير عن طريق ترقية التطبيق. يمكن تغيير طول المفتاح من خلال ترقية التطبيق فقط إذا تم استيفاء الشروط التالية:

- يتم تثبيت Kaspersky Endpoint Security إصدار 10 Service Pack 2 أو الأحدث على الكمبيوتر.
- مكونات تشفير البيانات (التشفير على مستوى الملفات، تشفير القرص بالكامل) غير مثبتة على الكمبيوتر.

بشكل افتراضي، لا يتم تضمين مكونات تشفير البيانات في Kaspersky Endpoint Security. لا يؤثر مكون إدارة BitLocker على التغيير في طول مفتاح التشفير.

لتغيير طول مفتاح التشفير، قم بتشغيل ملف kes_win.msi أو ملف setup_kes.exe من حزمة التوزيع التي تحتوي على مكتبة التشفير الضرورية. يمكنك أيضًا ترقية التطبيق عن بُعد باستخدام حزمة التثبيت.

يستحيل تغيير طول مفتاح التشفير باستخدام حزمة التوزيع الخاصة بنفس إصدار التطبيق الذي تم تثبيته على جهاز الكمبيوتر الخاص بك دون إلغاء تثبيت التطبيق أولاً.

تشفير القرص من Kaspersky

تشفير القرص من Kaspersky غير متوفر إلا لأجهزة الكمبيوتر العاملة بنظام التشغيل Windows لمحطات العمل. لأجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows للخوادم، استخدم تقنية تشفير محرك الأقراص من BitLocker.

يدعم Kaspersky Endpoint Security تشفير القرص بالكامل في ملفات النظام FAT32 و NTFS.

قبل بدء تشفير القرص بالكامل، يُجري التطبيق سلسلة من الفحوصات لتحديد ما إذا كان من الممكن تشفير الجهاز وتتضمن فحص محرك الأقراص الصلبة الخاص بالنظام للتحقق من توافقه مع وكيل المصادقة أو مع مكونات التشفير من BitLocker. للتحقق من التوافق، يجب إعادة تشغيل الكمبيوتر. بعد إعادة تشغيل الكمبيوتر، يُجري التطبيق جميع الفحوصات اللازمة تلقائيًا. إذا نجح فحص التوافق، سيبدأ تشفير القرص بالكامل بعد تمهيد نظام التشغيل وتشغيل التطبيق. إذا تم تحديد أن محرك الأقراص الصلبة الخاص بالنظام غير متوافق مع وكيل المصادقة أو مع مكونات التشفير من BitLocker، فيجب إعادة تشغيل الكمبيوتر من خلال الضغط على زر إعادة ضبط الجهاز (Reset). يسجل Kaspersky Endpoint Security معلومات حول عدم التوافق. وفقًا لهذه المعلومات، لا يبدأ التطبيق عملية تشفير القرص بالكامل عند بدء نظام التشغيل. يتم تسجيل معلومات حول هذا الحدث في تقارير Kaspersky Security Center.

إذا تم تغيير مواصفات مكونات الكمبيوتر المادية، فينبغي حذف معلومات عدم التوافق المسجلة بواسطة التطبيق من أجل فحص محرك الأقراص الصلبة الخاص بالنظام للتحقق من توافقه مع وكيل المصادقة ومكونات التشفير من BitLocker. للقيام بذلك، أدخل `avp pbatestreset` في سطر الأوامر قبل تشفير القرص بالكامل. إذا فشل تحميل نظام التشغيل بعد الانتهاء من فحص محرك الأقراص الصلبة الخاص بالنظام للتحقق من توافقه مع وكيل المصادقة، فيجب إزالة الكائنات والبيانات المتبقية بعد التشغيل الاختباري لوكيل المصادقة باستخدام أداة الاستعادة، ثم قم ببدء Kaspersky Endpoint Security وتنفيذ الأمر `avp pbatestreset` مرة أخرى.

بعد بدء تشفير القرص بالكامل، يشفر Kaspersky Endpoint Security جميع البيانات التي تمت كتابتها إلى محركات الأقراص الصلبة.

إذا قام المستخدم بإيقاف تشغيل الكمبيوتر أو إعادة تشغيله أثناء تشفير القرص بالكامل، يتم تحميل وكيل المصادقة قبل بدء التشغيل التالي لنظام التشغيل. يستأنف Kaspersky Endpoint Security تشفير القرص بالكامل بعد المصادقة الناجحة في وكيل المصادقة وبدء تشغيل نظام التشغيل.

إذا تحول نظام التشغيل إلى وضع الإسبات أثناء تشفير القرص بالكامل، يتم تحميل وكيل المصادقة عند تحول نظام التشغيل مرة أخرى من وضع الإسبات. يستأنف Kaspersky Endpoint Security تشفير القرص بالكامل بعد المصادقة الناجحة في وكيل المصادقة وبدء تشغيل نظام التشغيل.

في حالة انتقال نظام التشغيل إلى وضع السكون أثناء تشفير القرص بالكامل، يستأنف Kaspersky Endpoint Security تشفير محرك الأقراص الصلبة عند خروج نظام التشغيل من وضع السكون دون تحميل وكيل المصادقة.

يمكن إجراء مصادقة المستخدم في وكيل المصادقة بطريقتين:

- أدخل اسم وكلمة مرور حساب وكيل المصادقة الذي تم إنشاؤه بواسطة مسؤول الشبكة المحلية باستخدام أدوات Kaspersky Security Center.
- أدخل كلمة مرور الرمز المميز أو البطاقة الذكية المتصلة بالكمبيوتر.

يتوفر استخدام رمز مميز أو بطاقة ذكية فقط إذا تم تشفير محركات الأقراص الصلبة للكمبيوتر باستخدام لوغاريتم التشفير AES256. إذا تم تشفير محركات الأقراص الصلبة في الكمبيوتر باستخدام خوارزمية التشفير AES56، فسيتم رفض إضافة ملف الشهادة الإلكترونية إلى الأمر.

يدعم وكيل المصادقة تخطيطات لوحة المفاتيح للغات التالية:

- الإنجليزية (المملكة المتحدة)
- الإنجليزية (الولايات المتحدة الأمريكية)
- العربية (الجزائر، المغرب، تونس، تخطيط AZERTY)
- الإسبانية (أمريكا اللاتينية)
- الإيطالية
- الألمانية (ألمانيا والنمسا)
- الألمانية (سويسرا)
- البرتغالية (البرازيل، تخطيط ABNT2)
- الروسية (للوحات المفاتيح 105-Windows / IBM key بتخطيط QWERTY)
- التركية (تخطيط QWERTY)
- الفرنسية (فرنسا)
- الفرنسية (سويسرا)
- الفرنسية (بلجيكا، تخطيط AZERTY)
- اليابانية (للوحات المفاتيح 106-key بتخطيط QWERTY)

يصبح تخطيط لوحة المفاتيح متوفرًا في وكيل المصادقة في حالة إضافة هذا التخطيط في إعدادات اللغة والمعايير الإقليمية لنظام التشغيل وأصبح متوفرًا على شاشة ترحيب Microsoft Windows.

إذا كان اسم حساب وكيل المصادقة يحتوى على الرموز التي لا يمكن إدخالها باستخدام تخطيطات لوحة المفاتيح المتوفرة في وكيل المصادقة، يمكن الوصول إلى محركات الأقراص الصلبة المشفرة فقط بعد أن يتم استعادتهم باستخدام أداة المساعدة أو عقب استعادة اسم وكلمة مرور حساب وكيل المصادقة.

ميزات خاصة لتشفير محرك أقراص SSD

يدعم التطبيق تشفير محركات أقراص SSD ومحركات أقراص SSHD الهجينة ومحركات الأقراص المزودة بميزة Intel Smart Response. لا يدعم التطبيق تشفير محركات الأقراص باستخدام ميزة Intel Rapid Start. قم بتعطيل ميزة Intel Rapid Start قبل تشفير محرك الأقراص هذا.

يتضمن تشفير محركات أقراص SSD المزايا الخاصة التالية:

- إذا كان محرك أقراص SSD جديدًا ولا يحتوي على بيانات سرية، فقم بتمكين تشفير المساحة المشغولة فقط. يتيح لك ذلك الكتابة فوق مقاطع محرك الأقراص ذات الصلة.
- إذا كان محرك أقراص SSD قيد الاستخدام ويحتوي على بيانات سرية، فحدد أحد الخيارات التالية:
  - امسح محرك أقراص SSD بالكامل (المسح الآمن)، وقم بتثبيت نظام التشغيل وقم بتشغيل تشفير محرك أقراص SSD مع تمكين خيار تشفير المساحة المشغولة فقط.
  - قم بتشغيل تشفير محرك أقراص SSD مع خيار تعطيل تشفير المساحة المشغولة فقط.

يتطلب تشفير محرك أقراص SSD مساحة خالية تتراوح من 5 إلى 10 جيجابايت. يتم توفير متطلبات المساحة الخالية لتخزين بيانات إدارة التشفير في الجدول أدناه.

متطلبات المساحة الخالية لتخزين بيانات إدارة التشفير

حجم محرك أقراص SSD (جيجابايت)	المساحة الخالية على القسم الأساسي لمحرك أقراص SSD (ميجا بايت)	المساحة الخالية على القسم الثانوي لمحرك أقراص SSD (ميجا بايت)
128	250	64
256	250	640
512	300	128

بدء تشفير القرص من Kaspersky

قبل بدء ي تشفير القرص بالكامل، ننصحك بالتأكد من عدم تعرض الكمبيوتر للإصابة. للقيام بذلك، ابدأ مهمة الفحص الكامل أو فحص المناطق الحرجة. وقد يتسبب تنفيذ تشفير القرص بالكامل على جهاز كمبيوتر مصاب بفيروس جذر إلى جعل الكمبيوتر غير صالح للعمل.

قبل أن تبدأ تشفير القرص، يجب عليك التحقق من إعدادات حسابات وكيل المصادقة. وكيل المصادقة مطلوب للعمل مع المحركات المحمية باستخدام تقنية تشفير القرص من Kaspersky (FDE). قبل تحميل نظام التشغيل، يحتاج المستخدم إلى إكمال المصادقة مع الوكيل. Kaspersky Endpoint Security يتيح لك إنشاء حسابات وكيل المصادقة بشكل آلي قبل تشفير محرك أقراص. ويمكنك تفعيل الإنشاء الآلي لحسابات وكيل المصادقة في إعدادات سياسة تشفير القرص بالكامل (انظر التعليمات أدناه). يمكنك كذلك استخدام تقنية تسجيل الدخول الأحادي (SSO).

يتيح لك Kaspersky Endpoint Security إنشاء وكيل مصادقة تلقائيًا لمجموعات المستخدمين التالية:

- **جميع الحسابات على الكمبيوتر**. جميع الحسابات على الكمبيوتر التي كانت نشطة في أي وقت.
- **جميع حسابات المجال على الكمبيوتر**. جميع الحسابات على الكمبيوتر التي تنتمي إلى مجال ما والتي كانت نشطة في أي وقت.
- **جميع الحسابات المحلية على الكمبيوتر**. جميع الحسابات المحلية على الكمبيوتر التي كانت نشطة في أي وقت.
- **حساب الخدمة مع كلمة مرور لمرة واحدة**. ويعد حساب الخدمة ضروريًا للوصول إلى الكمبيوتر، على سبيل المثال، عندما ينسى المستخدم كلمة المرور. ويمكنك أيضًا استخدام حساب الخدمة كحساب احتياطي. يجب عليك إدخال اسم الحساب (افتراضيًا، `ServiceAccount`). يُنشئ Kaspersky Endpoint Security كلمة مرور تلقائيًا. ويمكنك العثور على كلمة المرور في وحدة تحكم Kaspersky Security Center.
- **المسؤول المحلي**. ينشئ Kaspersky Endpoint Security حساب مستخدم وكيل مصادقة للمسؤول المحلي للكمبيوتر.
- **إدارة الكمبيوتر**. يُنشئ Kaspersky Endpoint Security حساب مستخدم وكيل مصادقة لحساب إدارة الكمبيوتر. يمكنك معرفة الحساب الذي يتمتع بدور إدارة الكمبيوتر في خصائص الكمبيوتر في Active Directory. وبشكل افتراضي، لم يتم تحديد دور إدارة الكمبيوتر، أي أنه لا يتوافق مع أي حساب.
- **الحساب النشط**. يُنشئ Kaspersky Endpoint Security تلقائيًا حساب وكيل مصادقة للحساب النشط في وقت تشفير القرص.

تم تصميم مهمة إدارة حسابات وكيل المصادقة لتكوين إعدادات المصادقة للمستخدم. ويمكنك استخدام هذه المهمة لإضافة حسابات جديدة أو تعديل إعدادات الحسابات الحالية أو إزالة الحسابات إذا لزم الأمر. يمكنك استخدام المهام المحلية لأجهزة كمبيوتر فردية أو مهام جماعية لأجهزة كمبيوتر لمجموعات إدارة متفرقة أو مجموعة محددة من أجهزة الكمبيوتر.

كيفية تشغيل تشفير القرص من Kaspersky من خلال وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.

5. في القائمة المنسدلة **تقنية التشفير** حدد **تشفير القرص من Kaspersky**.

يتعذر استخدام تشفير القرص من Kaspersky في حالة وجود محركات أقراص صلبة على الكمبيوتر تم تشفيرها بواسطة BitLocker.

6. في القائمة المنسدلة **وضع التشفير** حدد **تشفير جميع محركات الأقراص الصلبة**.

في حالة تثبيت العديد من أنظمة التشغيل على الكمبيوتر، فسوف يمكنك بعد تشفير كل محركات الأقراص الثابتة تحميل نظام التشغيل المثبت عليه التطبيق فقط.

إذا كنت بحاجة إلى استثناء بعض من محركات الأقراص الصلبة من التشفير، قم بإنشاء قائمة بمحركات الأقراص الصلبة هذه.

7. قم بتكوين خيارات تشفير القرص من Kaspersky المتقدمة (انظر الجدول أدناه).

8. احفظ تغييراتك.

كيفية تشغيل تشفير القرص من Kaspersky من خلال Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Data Encryption** ← **Full Disk Encryption**.

5. في القسم **Manage encryption**، حدد **Kaspersky Disk Encryption**.

6. انقر على رابط **Kaspersky Disk Encryption**.
سيفتح هذا نافذة إعدادات تشفير القرص من Kaspersky.

يتعذر استخدام تشفير القرص من Kaspersky في حالة وجود محركات أقراص صلبة على الكمبيوتر تم تشفيرها بواسطة BitLocker.

7. في القائمة المنسدلة **Encryption mode** حدد **Encrypt all hard drives**.

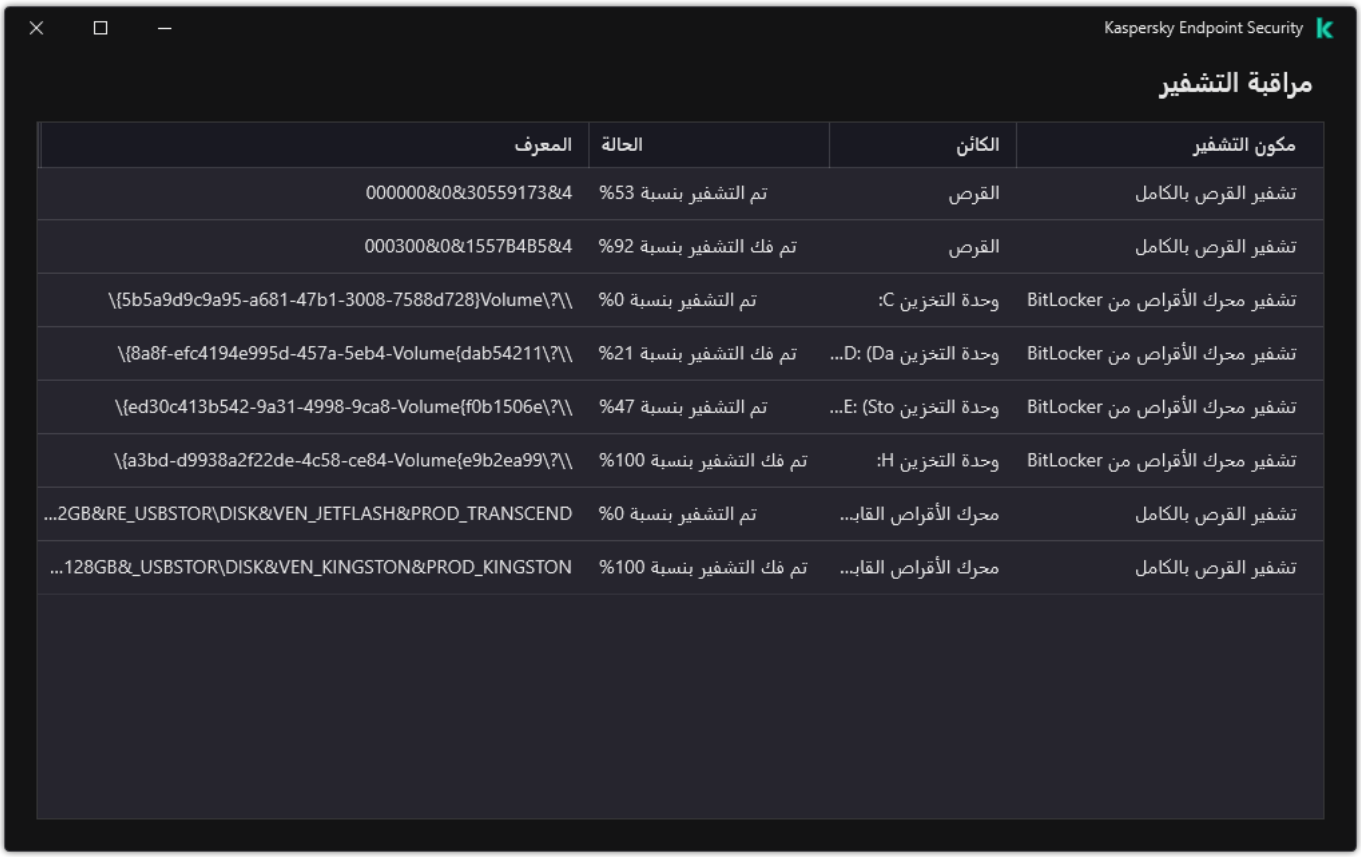
في حالة تثبيت العديد من أنظمة التشغيل على الكمبيوتر، فسوف يمكنك بعد التشفير تحميل نظام التشغيل الذي تم إجراء التشفير عليه.

إذا كنت بحاجة إلى استثناء بعض من محركات الأقراص الصلبة من التشفير، قم بإنشاء قائمة بمحركات الأقراص الصلبة هذه.

8. قم بتكوين خيارات تشفير القرص من Kaspersky المتقدمة (انظر الجدول أدناه).

9. احفظ تغييراتك.

يمكنك استخدام أداة مراقبة التشفير للتحكم في عملية تشفير القرص أو فك تشفيره على كمبيوتر المستخدم. يمكنك تشغيل أداة مراقبة التشفير من نافذة التطبيق الرئيسية.



مراقبة التشفير

إذا تم تشفير محركات الأقراص الصلبة للنظام، يتم تحميل وكيل المصادقة قبل بدء تشغيل نظام التشغيل. استخدم وكيل المصادقة لإكمال المصادقة للحصول على حق الوصول إلى محركات الأقراص الصلبة المشفرة للنظام وتحميل نظام التشغيل. بعد اكتمال إجراء المصادقة بنجاح، يتم تحميل نظام التشغيل. يتم تكرار عملية المصادقة كل مرة يتم فيها إعادة تشغيل نظام التشغيل.

إعدادات مكون تشفير القرص من Kaspersky

المعلمة	الوصف
إنشاء حسابات وكيل المصادقة تلقائيًا لأجل المستخدمون أثناء التشفير	وفي حالة تحديد خانة الاختيار هذه، ينشئ التطبيق حسابات وكيل المصادقة استنادًا إلى قائمة حسابات مستخدمي Windows على الكمبيوتر. بشكل افتراضي، Kaspersky Endpoint Security يستخدم جميع الحسابات المحلية والمجالية التي قام المستخدم من خلالها بتسجيل الدخول إلى نظام التشغيل في آخر 30 يومًا.
أنشئ تلقائيًا حسابات وكيل المصادقة لجميع مستخدمي هذا الكمبيوتر عند تسجيل الدخول	في حالة تحديد خانة الاختيار هذه، يتحقق التطبيق من المعلومات حول حسابات مستخدمي Windows على الكمبيوتر قبل بدء وكيل المصادقة. إذا اكتشف Kaspersky Endpoint Security حساب مستخدم Windows ليس له حساب وكيل مصادقة، فسوف ينشئ التطبيق حسابًا جديدًا للوصول إلى محركات الأقراص المشفرة. وسوف يتضمن حساب وكيل المصادقة الجديد الإعدادات الافتراضية التالية: تسجيل الدخول المحمي بكلمة مرور فقط وتغيير كلمة المرور عند المصادقة الأولى. لذلك، لا تحتاج إلى إضافة حسابات وكيل المصادقة يدويًا باستخدام مهمة إدارة حسابات وكيل المصادقة لأجهزة الكمبيوتر التي تحتوي على محركات أقراص مشفرة بالفعل.
حفظ اسم المستخدم المدخل في وكيل المصادقة	إذا تم تحديد خانة الاختيار، فسيحفظ التطبيق اسم حساب وكيل المصادقة. لن تتم مطالبتك بإدخال اسم الحساب في المحاولة التالية لإكمال المصادقة في وكيل المصادقة بموجب نفس الحساب.
تشفير	يؤدي تحديد خانة الاختيار هذه إلى تمكين / تعطيل الخيار الذي يقيد منطقة التشفير لمقاطع محرك الأقراص الصلبة الممتلئة فقط. ويتيح

مساحة القرص المستخدمة فقط (يحد من وقت التشفير)	لك هذا الحد تقليل وقت التشفير. لا يؤدي تمكين أو تعطيل ميزة **تشفير مساحة القرص المستخدمة فقط (يحد من وقت التشفير)** بعد بدء التشفير إلى تعديل هذا الإعداد حتى يتم فك تشفير محركات الأقراص الثابتة. يجب تحديد أو إلغاء تحديد خانة الاختيار قبل بدء التشفير. في حالة تحديد خانة الاختيار، يتم تشفير أجزاء محرك القرص الصلب الممتلئة بالملفات فقط. ويقوم Kaspersky Endpoint Security تلقائيًا بتشفير البيانات الجديدة بمجرد إضافتها. في حالة إلغاء تحديد خانة الاختيار، يتم تشفير محرك القرص الصلب بالكامل، بما في ذلك القطاعات المتبقية من الملفات التي تم حذفها وتعديلها سابقًا. هذا الخيار مستحسن لمحركات الأقراص الصلبة الجديدة التي لم يتم تعديل بياناتها أو حذفها. وإذا كنت تقوم بتشفير محرك أقراص صلبة مستخدم بالفعل، فمن المستحسن تشفير محرك الأقراص الصلبة بالكامل. ويضمن هذا حماية كل البيانات، وحتى حذف البيانات التي يحتمل أن تكون قابلة للاسترداد. ويتم إلغاء تحديد خانة الاختيار هذه بشكل افتراضي.
استخدام دعم USB القديم (غير موصى به)	خانة الاختيار هذه تقوم بتفعيل/تعطيل وظيفة دعم USB القديم. دعم USB القديم **هو** وظيفة في BIOS/UEFI تتيح لك استخدام أجهزة USB (مثل رمز أمان مميز) أثناء مرحلة إقلاع جهاز الكمبيوتر قبل بدء نظام التشغيل (وضع BIOS). دعم USB القديم لا يؤثر على دعم أجهزة USB بعد بدء تشغيل نظام التشغيل. في حالة تحديد خانة الاختيار، سوف يتم تمكين دعم أجهزة USB أثناء بدء التشغيل المبدئي للكمبيوتر. عند تفعيل وظيفة دعم USB القديم، فإن وكيل المصادقة في وضع BIOS لا يدعم العمل مع الرموز مع USB. ومن المستحسن استخدام هذا الخيار فقط عند وجود مشكلة في توافق الأجهزة وفقط لأجهزة الكمبيوتر التي حدثت عليها المشكلة.

إنشاء قائمة بمحركات الأقراص الصلبة التي تم استثناؤها من التشفير

يمكنك إنشاء قائمة بالاستثناءات من التشفير فقط لتقنية تشفير القرص من Kaspersky.

لتشكيل قائمة بمحركات الأقراص الصلبة التي تم استثناؤها من التشفير:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.
5. في القائمة المنسدلة **تقنية التشفير** حدد **تشفير القرص من Kaspersky**.

   تظهر الإدخالات المتوافقة مع محركات الأقراص الصلبة التي تم استثناؤها من التشفير في الجدول **لا تشفر محركات الأقراص الصلبة التالية**. يكون هذا الجدول فارغًا إذا لم تقم مسبقًا بتشكيل قائمة بمحركات الأقراص الصلبة التي تم استثناؤها من التشفير.
6. لإضافة محركات أقراص صلبة إلى قائمة محركات الأقراص الصلبة التي تم استثناؤها من التشفير:

   a. انقر على **إضافة**.

b. في النافذة التي تفتح، حدد قيم **اسم الجهاز** و**اسم الكمبيوتر** و**نوع القرص** و**تشفير القرص من Kaspersky**.

c. انقر على **تحديث**.

d. في العمود **الاسم** حدد خانات الاختيار الموجودة في صفوف الجدول المتوافقة مع محركات الأقراص الصلبة التي تريد إضافتها إلى قائمة محركات الأقراص الصلبة التي تم استثناؤها من التشفير.

e. انقر على **موافق**.

تظهر محركات الأقراص الصلبة المحددة في الجدول **لا تشفر محركات الأقراص الصلبة التالية**.

7. احفظ تغييراتك.

تصدير واستيراد قائمة بمحركات الأقراص الصلبة التي تم استثناؤها من التشفير

يمكنك تصدير قائمة استثناءات تشفير محرك الأقراص الصلبة إلى ملف XML. ثم يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من الاستثناءات من النوع نفسه. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة الاستثناءات أو لترحيل الاستثناءات إلى خادم مختلف.

كيفية تصدير واستيراد قائمة استثناءات تشفير محرك الأقراص الصلبة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.

5. في القائمة المنسدلة **تقنية التشفير** حدد **تشفير القرص من Kaspersky**.
تظهر الإدخالات المتوافقة مع محركات الأقراص الصلبة التي تم استثناؤها من التشفير في الجدول **لا تشفر محركات الأقراص الصلبة التالية**.

6. لتصدير قائمة الاستثناءات:

a. حدد الاستثناءات التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.
إذا لم تحدد أي استثناء، فسيقوم Kaspersky Endpoint Security بتصدير كل الاستثناءات.

b. انقر على رابط **تصدير**.

c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

7. لاستيراد قائمة القواعد:

a. انقر على **استيراد**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

c. افتح الملف.
إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة استثناءات تشفير محرك الأقراص الصلبة في وحدة تحكم الويب

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Data Encryption** ← **Full Disk Encryption**.

5. حدد تقنية **Kaspersky Disk Encryption** واتبع الرابط لتكوين الإعدادات.
ستفتح إعدادات التشفير.

6. انقر على رابط **Exclusions**.

7. لتصدير قائمة القواعد:

a. حدد الاستثناءات التي تريد تصديرها.

b. انقر على **Export**.

c. أكد أنك تريد تصدير الاستثناءات المحددة فقط، أو تصدير قائمة الاستثناءات بأكملها.

d. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة الاستثناءات الموثوقة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

e. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات بالكامل إلى ملف XML.

8. لاستيراد قائمة القواعد:

a. انقر على **Import**.

b. في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة الاستثناءات منه.

c. افتح الملف.
إذا كان جهاز الكمبيوتر يتضمن قائمة استثناءات بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

9. احفظ تغييراتك.

تمكين تقنية تسجيل الدخول الأحادي (SSO)

تقنية تسجيل الدخول الأحادي (SSO) تتيح لك الولوج بشكل تلقائي إلى نظام التشغيل باستخدام بيانات اعتماد وكيل المصادقة. وهذا يعني أن المستخدم يحتاج إلى إدخال كلمة مرور مرة واحدة فقط عند تسجيل الدخول إلى Windows (كلمة مرور حساب وكيل المصادقة). وتتيح لك تقنية تسجيل الدخول الأحادي أيضًا تحديث كلمة مرور حساب وكيل المصادقة تلقائيًا عند تغيير كلمة مرور حساب Windows.

عند استخدام تقنية تسجيل الدخول الأحادي فإن وكيل المصادقة يتجاهل متطلبات قوة كلمة المرور المحددة في Kaspersky Security Center. يمكنك وضع متطلبات قوة كلمة المرور في إعدادات نظام التشغيل.

تمكين تقنية تسجيل الدخول الأحادي

كيفية تمكين استخدام تقنية تسجيل الدخول الأحادي في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Data Encryption** ← **إعدادات التشفير العامة**.
5. في القسم **إعدادات كلمة المرور**، انقر على الزر **الإعدادات**.
6. في النافذة التي تفتح، في علامة تبويب **وكيل المصادقة**، حدد خانة الاختيار **استخدام تقنية تسجيل الدخول الأحادي (SSO)**.
7. إذا كنت تستخدم موفر بيانات اعتماد خارجيًا، حدد خانة الاختيار **Wrap third-party credential providers**.
8. احفظ تغييراتك.

ونتيجة لذلك، يحتاج المستخدم إلى إكمال إجراء المصادقة مرة واحدة فقط مع الوكيل. إجراء المصادقة غير مطلوب لتحميل نظام التشغيل. يتم تحميل نظام التشغيل تلقائيًا.

كيفية تمكين استخدام تقنية تسجيل الدخول الأحادي في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Data Encryption** ← **Full Disk Encryption**.
5. حدد تقنية **Kaspersky Disk Encryption** واتبع الرابط لتكوين الإعدادات.
   ستفتح إعدادات التشفير.
6. في القسم **Password settings**، حدد خانة الاختيار **Use Single Sign-On (SSO) technology**.
7. إذا كنت تستخدم موفر بيانات اعتماد خارجيًا، حدد خانة الاختيار **Wrap third-party credential providers**.
8. احفظ تغييراتك.

ونتيجة لذلك، يحتاج المستخدم إلى إكمال إجراء المصادقة مرة واحدة فقط مع الوكيل. إجراء المصادقة غير مطلوب لتحميل نظام التشغيل. يتم تحميل نظام التشغيل تلقائيًا.

كي تعمل تقنية تسجيل الدخول الأحادي، فإن كلمة مرور حساب Windows وكلمة مرور حساب وكيل المصادقة يجب أن يتطابقا. إذا كانت كلمتا المرور غير متطابقتين، فإن المستخدم يحتاج إلى تنفيذ إجراء المصادقة مرتين: مرة في واجهة وكيل المصادقة والأخرى قبل تحميل نظام التشغيل. ويجب تنفيذ هذه الإجراءات مرة واحدة فقط لمزامنة كلمات المرور. بعد ذلك، سوف يستبدل Kaspersky Endpoint Security كلمة مرور حساب وكيل المصادقة ويستخدم بدلاً منها كلمة مرور حساب Windows. وعندما يتم تغيير كلمة مرور حساب Windows، سيقوم التطبيق تلقائيًا بتحديث كلمة المرور لحساب وكيل المصادقة.

موفرة بيانات الاعتماد الخارجيون

يضيف Kaspersky Endpoint Security 11.10.0 الدعم لموفري بيانات الاعتماد الخارجيين.

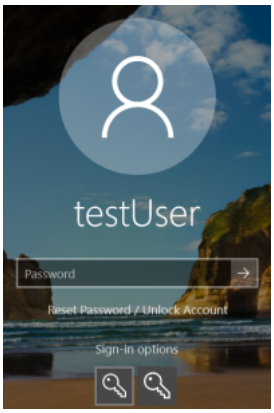
يدعم Kaspersky Endpoint Security موفر بيانات الاعتماد الخارجي ADSelfService Plus.

عند العمل مع موفري بيانات اعتماد خارجيين، يعترض عامل المصادقة كلمة المرور قبل تحميل نظام التشغيل. وهذا يعني أن المستخدم يحتاج إلى إدخال كلمة مرور مرة واحدة فقط عند تسجيل الدخول إلى Windows. وبعد تسجيل الدخول إلى Windows، يستطيع المستخدم الاستفادة من إمكانات موفر بيانات اعتماد خارجي للمصادقة على سبيل المثال في خدمات الشركات. ويسمح موفرو بيانات الاعتماد الخارجيون كذلك للمستخدمين بإعادة تعيين كلمات المرور الخاصة بهم بشكل مستقل. وفي هذه الحالة، سيقوم Kaspersky Endpoint Security تلقائيًا بتحديث كلمة المرور لوكيل المصادقة.

إذا كنت تستخدم موفر بيانات اعتماد خارجيًا لا يدعمه التطبيق، فقد تواجه بعض القيود في تشغيل تقنية تسجيل الدخول الأحادي. وعند تسجيل الدخول إلى Windows، سيتوفر ملفا تعريف للمستخدم: موفر بيانات الاعتماد داخل النظام وموفر بيانات الاعتماد الخارجي. وستكون أيقونتا ملفا التعريف هذين متطابقين (انظر الشكل أدناه). وسيكون لدى المستخدم الخيارات التالية للمتابعة:

- إذا اختار المستخدم موفر بيانات الاعتماد الخارجي، لن يتمكن وكيل المصادقة من مزامنة كلمة المرور مع حساب Windows. لذلك، إذا قام المستخدم بتغيير كلمة مرور حساب Windows، فلن يتمكن Kaspersky Endpoint Security من تحديث كلمة المرور لحساب وكيل المصادقة. ونتيجة لذلك، يحتاج المستخدم إلى تنفيذ إجراء المصادقة مرتين: مرة في واجهة وكيل المصادقة والأخرى قبل تحميل نظام التشغيل. وفي هذه الحالة، يستطيع المستخدم الاستفادة من إمكانات موفر بيانات اعتماد خارجي للمصادقة على سبيل المثال في خدمات الشركات.

- إذا اختار المستخدم موفر بيانات الاعتماد داخل النظام، سيزامن وكيل المصادقة كلمات المرور مع حساب Windows. وفي هذه الحالة، لا يستطيع المستخدم الاستفادة من إمكانيات موفر بيانات اعتماد خارجي للمصادقة على سبيل المثال في خدمات الشركة.



ملف تعريف مصادقة النظام وملف تعريف مصادقة الجهة الخارجية لتسجيل الدخول إلى Windows

إدارة حسابات وكيل المصادقة

وكيل المصادقة مطلوب للعمل مع المحركات المحمية باستخدام تقنية تشفير القرص من Kaspersky (FDE). قبل تحميل نظام التشغيل، يحتاج المستخدم إلى إكمال المصادقة مع الوكيل. إن مهمةإدارة حسابات وكيل المصادقة مصممة لتكوين إعدادات المصادقة للمستخدم. يمكنك استخدام المهام المحلية لأجهزة كمبيوتر فردية أو مهام جماعية لأجهزة كمبيوتر لمجموعات إدارة متفرقة أو مجموعة محددة من أجهزة الكمبيوتر.

لا يمكنك تكوين جدول لبدء مهمة إدارة حسابات وكيل المصادقة. من المستحيل كذلك إجبار مهمة على التوقف.

كيفية نشاء مهمة إدارة حسابات وكيل المصادقة في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (12.1)** ← **إدارة حسابات وكيل المصادقة**.

الخطوة الثانية: تحديد أمر إدارة حساب وكيل المصادقة

أنشئ قائمة بأوامر إدارة حساب وكيل المصادقة. تسمح لك أوامر الإدارة بإضافة حسابات وكيل المصادقة وتعديلها وحذفها (راجع التعليمات أدناه). لا يمكن إلا للمستخدمين الذين لديهم حساب وكيل مصادقة إكمال إجراء المصادقة وتحميل نظام التشغيل والوصول إلى محرك الأقراص المشفر.

الخطوة الثالثة: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الرابعة: تحديد اسم المهمة

أدخل اسم المهمة، مثل حسابات المسؤول.

الخطوة 5 إكمال إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

ونتيجةً لذلك، بعد اكتمال المهمة عند بدء تشغيل الكمبيوتر التالي، يمكن للمستخدم الجديد إكمال إجراء المصادقة وتحميل نظام التشغيل والوصول إلى محرك الأقراص المشفر.

كيفية نشاء مهمة إدارة حسابات وكيل المصادقة في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة 1. تكوين إعدادات المهمة العامة

تكوين إعدادات المهمة:

1. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.
2. في القائمة المنسدلة **Task type** حدد **Manage Authentication Agent accounts**.
3. في الحقل **Task name**، أدخل وصفًا موجزًا، مثل حسابات المسؤول.
4. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

الخطوة الثانية: إدارة حسابات وكيل المصادقة

أنشئ قائمة بأوامر إدارة حساب وكيل المصادقة. تسمح لك أوامر الإدارة بإضافة حسابات وكيل المصادقة وتعديلها وحذفها (راجع التعليمات أدناه). لا يمكن إلا للمستخدمين الذين لديهم حساب وكيل مصادقة إكمال إجراء المصادقة وتحميل نظام التشغيل والوصول إلى محرك الأقراص المشفر.

الخطوة 3 إكمال إنشاء المهمة

أغلق المعالج. سيتم عرض مهمة جديدة في قائمة المهام.

لتشغيل المهمة، حدد خانة الاختيار المقابلة لها وانقر فوق الزر **Start**.

ونتيجةً لذلك، بعد اكتمال المهمة عند بدء تشغيل الكمبيوتر التالي، يمكن للمستخدم الجديد إكمال إجراء المصادقة وتحميل نظام التشغيل والوصول إلى محرك الأقراص المشفر.

لإضافة حساب وكيل المصادقة، ستحتاج إلى إضافة أمر خاص إلى مهمة إدارة حسابات وكيل المصادقة. قد يكون من المريح استخدام مهمة جماعية، مثل إضافة حساب مسؤول إلى جميع أجهزة الكمبيوتر.

Kaspersky Endpoint Security يتيح لك إنشاء حسابات وكيل المصادقة بشكل آلي قبل تشفير محرك أقراص. يمكنك تفعيل الإنشاء الآلي لحسابات وكيل المصادقة في إعدادات سياسة تشفير القرص بالكامل. يمكنك كذلك استخدام تقنية تسجيل الدخول الأحادي (SSO).

كيفية إضافة حساب وكيل المصادقة من خلال وحدة تحكم الإدارة (MMC)

1. افتح خصائص مهمة إدارة حسابات وكيل المصادقة.

2. في خصائص المهمة، حدد القسم **الإعدادات**.

3. انقر فوق **إضافة** ← **أمر إضافة الحساب**.

4. في النافذة التي تفتح، في حقل **حساب Windows**، حدد اسم حساب Microsoft Windows الذي سيتم استخدامه في إنشاء حساب وكيل المصادقة.

5. إذا أدخلت اسم حساب Windows يدويًا، فانقر فوق الزر **سماح** لتعريف معرف أمان الحساب (SID).

إذا اخترت عدم تحديد معرف الأمان عن طريق النقر فوق الزر **سماح** فسيتم تحديده عند تنفيذ المهمة على الكمبيوتر.

> تحديد معرف أمان حساب Windows أمر ضروري للتحقق من أنك أدخلت اسم حساب Windows بشكل صحيح. إذا كان حساب Windows غير موجود على الكمبيوتر أو في المجال الموثوق به، فإن مهمة إدارة حسابات وكيل المصادقة سوف تنتهي بخطأ.

6. حدد خانة الاختيار **استبدال الحساب الحالي** إذا كنت تريد استبدال حساب تم إنشاؤه سابقًا لوكيل المصادقة بالحساب الذي يتم إنشاؤه.

> تتوفر هذه الخطوة عند إضافة أمر إنشاء حساب وكيل المصادقة في خصائص مهمة جماعية لإدارة حسابات وكيل المصادقة. لا تتوفر هذه الخطوة عندما تضيف أمر إنشاء حساب وكيل المصادقة في خصائص المهمة المحلية إدارة حسابات وكيل المصادقة.

7. في الحقل **اسم المستخدم** اكتب اسم حساب وكيل المصادقة الذي يجب إدخاله أثناء المصادقة من أجل الوصول إلى محركات الأقراص الصلبة المشفرة.

8. حدد خانة الاختيار **السماح بالمصادقة القائمة على كلمة مرور** إذا كنت ترغب في أن يقوم التطبيق بمطالبة المستخدم بإدخال كلمة مرور حساب وكيل المصادقة أثناء المصادقة لأجل الوصول إلى محركات الأقراص الصلبة المشفرة. قم بتعيين كلمة مرور لحساب وكيل المصادقة. يمكنك طلب كلمة مرور جديدة من المستخدم بعد المصادقة الأولى، إذا كان ذلك ضروريًا.

9. حدد خانة الاختيار **السماح بالمصادقة القائمة على شهادة** إذا أردت أن يقوم التطبيق بمطالبة المستخدم بتوصيل الرمز المميز أو البطاقة الذكية بالكمبيوتر أثناء المصادقة لأجل الوصول إلى محركات الأقراص الصلبة المشفرة. حدد ملف شهادة للمصادقة باستخدام بطاقة ذكية أو رمز مميز.

10. في حالة المطالبة بذلك، في الحقل **وصف الأمر** أدخل تفاصيل حساب وكيل المصادقة التي تحتاجها لإدارة الأمر.

11. في القسم **الوصول إلى المصادقة في وكيل المصادقة**، كوّن الوصول إلى المصادقة في وكيل المصادقة للمستخدم الذي يستخدم الحساب المحدد في الأمر.

12. احفظ تغييراتك.

كيفية إضافة حساب وكيل المصادقة من خلال Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق المهمة **Manage Authentication Agent accounts** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

3. حدد علامة التبويب **Application settings**.

4. في قائمة حسابات وكيل المصادقة، انقر فوق زر **Add**.

يؤدي هذا إلى تشغيل معالج إدارة حساب وكيل المصادقة.

5. حدد نوع الأمر **Add**.

6. حدد حساب مستخدم. يمكنك تحديد حساب من قائمة حسابات المجال أو إدخال اسم الحساب يدويًا. انتقل إلى الخطوة التالية.

يحدد Kaspersky Endpoint Security معرف أمان الحساب (SID). هذا ضروري للتحقق من الحساب. إذا أدخلت اسم المستخدم بشكل غير صحيح، فسيقوم Kaspersky Endpoint Security بإنهاء المهمة مع خطأ.

7. قم بتكوين إعدادات حساب وكيل المصادقة.

- **Create a new Authentication Agent account to replace the existing account**. Kaspersky Endpoint Security يفحص الحسابات الموجودة على الكمبيوتر. إذا كان معرّف أمان المستخدم على الكمبيوتر وفي المهمة متطابقًا، فسوف يغير Kaspersky Endpoint Security إعدادات حساب مستخدم وفقًا للمهمة.
- **User name**. يتوافق اسم المستخدم الافتراضي لحساب وكيل المصادقة مع اسم مجال المستخدم.
- **Allow password-based authentication**. قم بتعيين كلمة مرور لحساب وكيل المصادقة. يمكنك طلب كلمة مرور جديدة من المستخدم بعد المصادقة الأولى، إذا كان ذلك ضروريًا. بهذه الطريقة سيكون لكل مستخدم كلمة مرور فريدة خاصة به. يمكنك كذلك تعيين متطلبات قوة كلمة المرور لحساب وكيل المصادقة في السياسة.
- **Allow certificate-based authentication**. حدد ملف شهادة للمصادقة باستخدام بطاقة ذكية أو رمز مميز. بهذه الطريقة، سيحتاج المستخدم إلى إدخال كلمة مرور البطاقة الذكية أو الرمز المميز.
- **Account access to encrypted data**. قم بتكوين وصول المستخدم إلى محرك الأقراص المشفر. يمكنك مثلًا أن تقوم بتعطيل مصادقة المستخدم مؤقتًا بدلًا من حذف حساب وكيل المصادقة.
- **Comment**. أدخل وصفًا للحساب إذا لزم الأمر.

8. احفظ تغييراتك.

9. حدد خانة الاختيار المقابلة للمهمة وانقر فوق الزر **Start**.

ونتيجةً لذلك، بعد اكتمال المهمة عند بدء تشغيل الكمبيوتر التالي، يمكن للمستخدم الجديد إكمال إجراء المصادقة وتحميل نظام التشغيل والوصول إلى محرك الأقراص المشفر.

لتغيير كلمة المرور والإعدادات الأخرى لحساب وكيل المصادقة، ستحتاج إلى إضافة أمر خاص إلى مهمة إدارة حسابات وكيل المصادقة. قد يكون من المريح استخدام مهمة جماعية، مثل استبدال شهادة الرمز المميز للمسؤول علة جميع أجهزة الكمبيوتر.

كيفية تغيير حساب وكيل المصادقة من خلال وحدة تحكم الإدارة (MMC)

1. افتح خصائص مهمة إدارة حسابات وكيل المصادقة.

2. في خصائص المهمة، حدد القسم **الإعدادات**.

3. انقر فوق **إضافة** ← **أمر تحرير الحساب**.

4. في النافذة التي تفتح، في حقل **حساب Windows**، حدد اسم حساب مستخدم Microsoft Windows الذي ترغب في تغييره.

5. إذا أدخلت اسم حساب Windows يدويًا، فانقر فوق الزر **سماح** لتعريف معرف أمان الحساب (SID).

إذا اخترت عدم تحديد معرف الأمان عن طريق النقر فوق الزر **سماح** فسيتم تحديده عند تنفيذ المهمة على الكمبيوتر.

> تحديد معرف أمان حساب Windows أمر ضروري للتحقق من أنك أدخلت اسم حساب Windows بشكل صحيح. إذا كان حساب Windows غير موجود على الكمبيوتر أو في المجال الموثوق به، فإن مهمة إدارة حسابات وكيل المصادقة سوف تنتهي بخطأ.

6. حدد خانة الاختيار **تغيير اسم المستخدم** وأدخل اسمًا جديدًا لحساب وكيل المصادقة إذا كنت ترغب في أن يقوم Kaspersky Endpoint Security بتغيير اسم المستخدم لجميع حسابات وكيل المصادقة التي تم إنشاؤها باستخدام حساب Microsoft Windows بالاسم المشار إليه في الحقل **حساب Windows** إلى الاسم الذي تمت كتابته في الحقل أدناه.

7. حدد خانة الاختيار **تعديل إعدادات المصادقة القائمة على كلمة مرور** لجعل إعدادات المصادقة المستندة إلى كلمة المرور قابلة للتحرير.

8. حدد خانة الاختيار **السماح بالمصادقة القائمة على كلمة مرور** إذا كنت ترغب في أن يقوم التطبيق بمطالبة المستخدم بإدخال كلمة مرور حساب وكيل المصادقة أثناء المصادقة لأجل الوصول إلى محركات الأقراص الصلبة المشفرة. قم بتعيين كلمة مرور لحساب وكيل المصادقة.

9. حدد خانة الاختيار **تحرير قاعدة تغيير كلمة المرور عند المصادقة في وكيل المصادقة** إذا كنت ترغب أن يُغير Kaspersky Endpoint Security قيمة إعداد تغيير كلمة المرور لجميع حسابات وكيل المصادقة التي تم إنشاؤها باستخدام حساب Microsoft Windows بالاسم المشار إليه في حقل **حساب Windows** إلى قيمة الإعداد المحدد أدناه.

10. حدد قيمة إعداد تغيير كلمة المرور عند المصادقة في وكيل المصادقة.

11. حدد خانة الاختيار **تعديل إعدادات المصادقة القائمة على شهادة** لجعل إعدادات المصادقة المستندة إلى الشهادة الإلكترونية للرمز المميز أو البطاقة الذكية قابلة للتحرير.

12. حدد خانة الاختيار **السماح بالمصادقة القائمة على شهادة** إذا أردت أن يقوم التطبيق بمطالبة المستخدم بإدخال كلمة المرور إلى الرمز المميز أو البطاقة الذكية المتصلة بالكمبيوتر أثناء عملية المصادقة لأجل الوصول إلى محركات الأقراص الصلبة المشفرة. حدد ملف شهادة للمصادقة باستخدام بطاقة ذكية أو رمز مميز.

13. حدد خانة الاختيار **تحرير وصف الأمر** وقم بتحرير وصف الأمر إذا كنت ترغب في تغيير Kaspersky Endpoint Security وصف الأمر لجميع حسابات وكيل المصادقة التي تم إنشاؤها باستخدام حساب Microsoft Windows بالاسم المشار إليه في الحقل **حساب Windows**.

14. حدد خانة الاختيار **تحرير قاعدة الوصول إلى المصادقة في وكيل المصادقة** إذا كنت ترغب أن يُغير Kaspersky Endpoint Security قاعدة وصول المستخدم إلى حوار المصادقة في وكيل المصادقة إلى القيمة المحددة أدناه لجميع حسابات وكيل المصادقة التي تم إنشاؤها باستخدام حساب Microsoft Windows بالاسم المشار إليه في الحقل **حساب Windows**.

15. حدد القاعدة للوصول إلى حوار المصادقة في وكيل المصادقة.

16. احفظ تغييراتك.

كيفية تغيير حساب وكيل المصادقة من خلال Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق المهمة **Manage Authentication Agent accounts** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

3. حدد علامة التبويب **Application settings**.

4. في قائمة حسابات وكيل المصادقة، انقر فوق زر **Add**.

يؤدي هذا إلى تشغيل معالج إدارة حساب وكيل المصادقة.

5. حدد نوع الأمر **Change**.

6. حدد حساب مستخدم. يمكنك تحديد حساب من قائمة حسابات المجال أو إدخال اسم الحساب يدويًا. انتقل إلى الخطوة التالية.

يحدد Kaspersky Endpoint Security معرف أمان الحساب (SID). هذا ضروري للتحقق من الحساب. إذا أدخلت اسم المستخدم بشكل غير صحيح، فسيقوم Kaspersky Endpoint Security بإنهاء المهمة مع خطأ.

7. حدد خانات الاختيار المجاورة للإعدادات التي ترغب في تعديلها.

8. قم بتكوين إعدادات حساب وكيل المصادقة.

- **Create a new Authentication Agent account to replace the existing account**. Kaspersky Endpoint Security يفحص الحسابات الموجودة على الكمبيوتر. إذا كان معرّف أمان المستخدم على الكمبيوتر وفي المهمة متطابقًا، فسوف يغير Kaspersky Endpoint Security إعدادات حساب مستخدم وفقًا للمهمة.
- **User name**. يتوافق اسم المستخدم الافتراضي لحساب وكيل المصادقة مع اسم مجال المستخدم.
- **Allow password-based authentication**. قم بتعيين كلمة مرور لحساب وكيل المصادقة. يمكنك طلب كلمة مرور جديدة من المستخدم بعد المصادقة الأولى، إذا كان ذلك ضروريًا. بهذه الطريقة سيكون لكل مستخدم كلمة مرور فريدة خاصة به. يمكنك كذلك تعيين متطلبات قوة كلمة المرور لحساب وكيل المصادقة في السياسة.
- **Allow certificate-based authentication**. حدد ملف شهادة للمصادقة باستخدام بطاقة ذكية أو رمز مميز. بهذه الطريقة، سيحتاج المستخدم إلى إدخال كلمة مرور البطاقة الذكية أو الرمز المميز.
- **Account access to encrypted data**. قم بتكوين وصول المستخدم إلى محرك الأقراص المشفر. يمكنك مثلًا أن تقوم بتعطيل مصادقة المستخدم مؤقتًا بدلًا من حذف حساب وكيل المصادقة.
- **Comment**. أدخل وصفًا للحساب إذا لزم الأمر.

9. احفظ تغييراتك.

10. حدد خانة الاختيار المقابلة للمهمة وانقر فوق الزر **Start**.

لحذف حساب وكيل المصادقة، ستحتاج إلى إضافة أمر خاص إلى مهمة إدارة حسابات وكيل المصادقة. قد يكون من المريح استخدام مهمة جماعية، مثل لحذف حساب موظف مفصول.

كيفية حذف حساب وكيل المصادقة من خلال وحدة تحكم الإدارة (MMC)

1. افتح خصائص مهمة إدارة حسابات وكيل المصادقة.

2. في خصائص المهمة، حدد القسم **الإعدادات**.

3. انقر فوق **إضافة** ← **أمر حذف الحساب**.

4. في النافذة التي تفتح، في حقل **حساب Windows**، حدد اسم حساب مستخدم Windows الذي تم استخدامه لإنشاء حساب وكيل المصادقة الذي تريد حذفه.

5. إذا أدخلت اسم حساب Windows يدويًا، فانقر فوق الزر **سماح** لتعريف معرف أمان الحساب (SID).

إذا اخترت عدم تحديد معرف الأمان عن طريق النقر فوق الزر **سماح** فسيتم تحديده عند تنفيذ المهمة على الكمبيوتر.

تحديد معرف أمان حساب Windows أمر ضروري للتحقق من أنك أدخلت اسم حساب Windows بشكل صحيح. إذا كان حساب Windows غير موجود على الكمبيوتر أو في المجال الموثوق به، فإن مهمة إدارة حسابات وكيل المصادقة سوف تنتهي بخطأ.

6. احفظ تغييراتك.

كيفية حذف حساب وكيل المصادقة من خلال Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Tasks** ← **Devices**.

تفتح قائمة المهام.

2. انقر فوق المهمة **Manage Authentication Agent accounts** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

3. حدد علامة التبويب **Application settings**.

4. في قائمة حسابات وكيل المصادقة، انقر فوق زر **Add**.

يؤدي هذا إلى تشغيل معالج إدارة حساب وكيل المصادقة.

5. حدد نوع الأمر **Delete**.

6. حدد حساب مستخدم. يمكنك تحديد حساب من قائمة حسابات المجال أو إدخال اسم الحساب يدويًا.

7. احفظ تغييراتك.

8. حدد خانة الاختيار المقابلة للمهمة وانقر فوق الزر **بدء التشغيل**.

نتيجةً لذلك، بعد إكمال المهمة في بدء التشغيل التالي، لن يقدر المستخدم على إكمال إجراء المصادقة وتحميل نظام التشغيل. Kaspersky Endpoint Security سوف يرفض الوصول إلى البيانات المشفرة.

لعرض قائمة بالمستخدمين الذين يمكنهم إكمال المصادقة مع الوكيل وتحميل نظام التشغيل، ستحتاج إلى الذهاب إلى خصائص الكمبيوتر المدار.

كيفية عرض قائمة حسابات وكيل المصادقة من خلال وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Devices**.

3. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.

4. من نافذة خصائص الكمبيوتر، حدد قسم **المهام**.

5. في قائمة المهام، حدد **إدارة حسابات وكيل المصادقة** وافتح خصائص المهمة عن طريق النقر المزدوج.

6. في خصائص المهمة، حدد القسم **الإعدادات**.

ونتيجة لذلك، ستتمكن من الوصول إلى قائمة حسابات وكيل المصادقة على هذا الكمبيوتر. لا يمكن إلا للمستخدمين في القائمة إكمال المصادقة مع الوكيل وتحميل نظام التشغيل.

كيفية عرض قائمة حسابات وكيل المصادقة من خلال Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Managed devices**.

2. انقر فوق اسم الكمبيوتر الذي ترغب في عرض قائمة حسابات وكيل المصادقة عليه.

3. في خصائص الكمبيوتر، حدد علامة التبويب **Tasks**.

4. في قائمة المهام، حدد **Manage Authentication Agent accounts**.

5. من خصائص الكمبيوتر، حدد قسم **Application Settings**.

ونتيجة لذلك، ستتمكن من الوصول إلى قائمة حسابات وكيل المصادقة على هذا الكمبيوتر. لا يمكن إلا للمستخدمين في القائمة إكمال المصادقة مع الوكيل وتحميل نظام التشغيل.

استخدام رمز مميز وبطاقة ذكية مع وكيل المصادقة

يمكن استخدام رمز مميز أو بطاقة ذكية للمصادقة عند الوصول لمحركات الأقراص الصلبة المشفرة. لفعل ذلك، يجب أن تضيف ملف الشهادة الإلكترونية لرمز مميز أو بطاقة ذكية إلى مهمة إدارة حسابات وكيل المصادقة.

يتوفر استخدام رمز مميز أو بطاقة ذكية فقط إذا تم تشفير محركات الأقراص الصلبة للكمبيوتر باستخدام لوغاريتم التشفير AES256. إذا تم تشفير محركات الأقراص الصلبة في الكمبيوتر باستخدام خوارزمية التشفير AES56، فسيتم رفض إضافة ملف الشهادة الإلكترونية إلى الأمر.

يدعم Kaspersky Endpoint Security الرموز المميزة وأجهزة قراءة البطاقات الذكية والبطاقات الذكية التالية:

- SafeNet eToken PRO 64K (4.2b)؛
- SafeNet eToken PRO 72K Java؛
- SafeNet eToken 4100-72K Java؛
- SafeNet eToken 5100؛

- SafeNet eToken 5105؛
- SafeNet eToken 7300؛
- EMC RSA SID 800؛
- Gemalto IDPrime.NET 510؛
- Gemalto IDPrime.NET 511؛
- Rutoken ECP؛
- Rutoken ECP Flash؛
- Athena IDProtect Laser؛
- SafeNet eToken PRO 72K Java؛
- Aladdin-RD JaCarta PKI.

لإضافة ملف الشهادة الإلكترونية للرمز المميز أو البطاقة الذكية إلى الأمر الخاص بإنشاء حساب وكيل مصادقة، يجب أولاً حفظ الملف باستخدام برنامج لإدارة الشهادات تابع لجهة خارجية.

يجب أن يكون لشهادة الرمز المميز أو الشهادة الإلكترونية الخصائص التالية:

- يجب أن تكون الشهادة متوافقة مع معيار X.509، ويجب أن يكون لملف الشهادة ترميز DER.
- تحتوي الشهادة على مفتاح RSA بطول لا يقل عن 1024 بت.

إذا كانت الشهادة الإلكترونية لرمز الترميز أو البطاقة الذكية لا تفي بهذه المتطلبات، فلن تتمكن من تحميل ملف الشهادة في أمر إنشاء حساب وكيل المصادقة.

يجب أن يكون لمعلمة `KeyUsage` للشهادة القيمة `keyEncipherment` أو `dataEncipherment`. تحدد معلمة `KeyUsage` غرض الشهادة. إذا كان للمعلمة قيمة مختلفة، فإن Kaspersky Security Center سوف يقوم بتحميل ملف الشهادة ولكن سيعرض تحذيرًا.

إذا فقد المستخدم الرمز المميز أو البطاقة الذكية، فيجب على المسؤول إضافة ملف الشهادة الإلكترونية للمرز المميز أو البطاقة الذكية إلى الأمر لإنشاء حساب وكيل المصادقة. يجب على المستخدم بعد ذلك إكمال إجراء استلام الوصول إلى الأجهزة المشفرة أو استعادة البيانات على الأجهزة المشفرة.

فك تشفير محرك الأقراص الصلبة

يمكنك فك تشفير محركات الأقراص الصلبة حتى إذا لم يكن هناك أي ترخيص حالي يسمح بتشفير البيانات.

لفك تشفير محركات الأقراص الصلبة:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.
5. في القائمة المنسدلة **تقنية التشفير**، حدد التقنية التي سيتم تشفير محركات الأقراص الصلبة باستخدامها.

6. قم بأحد الإجراءات التالية:

- في القائمة المنسدلة **وضع التشفير** حدد الخيار **فك تشفير جميع محركات الأقراص الصلبة** إذا كنت تريد فك تشفير جميع محركات الأقراص الصلبة المشفرة.
- قم بإضافة محركات الأقراص الصلبة التي تريد فك تشفيرها إلى جدول **لا تشفر محركات الأقراص الصلبة التالية**.

يتوفر هذا الخيار فقط لتقنية تشفير القرص من Kaspersky.

7. احفظ تغييراتك.

يمكنك استخدام أداة مراقبة التشفير للتحكم في عملية تشفير القرص أو فك تشفيره على كمبيوتر المستخدم. يمكنك تشغيل أداة مراقبة التشفير من نافذة التطبيق الرئيسية.

مراقبة التشفير

إذا قام المستخدم بإيقاف تشغيل الكمبيوتر أو إعادة تشغيله أثناء فك تشفير محركات الأقراص الصلبة التي تم تشفيرها باستخدام تقنية تشفير القرص من Kaspersky، فسيتم تحميل وكيل المصادقة قبل بدء التشغيل التالي لنظام التشغيل. يستأنف Kaspersky Endpoint Security فك تشفير محرك الأقراص الصلبة بعد المصادقة الناجحة في وكيل المصادقة وبدء تشغيل نظام التشغيل.

إذا تحول نظام التشغيل إلى وضع الإسبات أثناء تشفير محركات الأقراص الصلبة التي تم تشفيرها باستخدام تقنية تشفير القرص من Kaspersky، فسيتم تحميل وكيل المصادقة عند خروج نظام التشغيل من وضع الإسبات. يستأنف Kaspersky Endpoint Security فك تشفير محرك الأقراص الصلبة بعد المصادقة الناجحة في وكيل المصادقة وبدء تشغيل نظام التشغيل. بعد فك تشفير محرك الأقراص الصلبة، لا يتوفر وضع الإسبات حتى إعادة التمهيد الأولي لنظام التشغيل.

في حالة انتقال نظام التشغيل إلى وضع النوم أثناء فك تشفير محرك الأقراص الصلبة، يستأنف Kaspersky Endpoint Security فك تشفير محرك الأقراص الصلبة عند خروج نظام التشغيل من وضع النوم دون تحميل وكيل المصادقة.

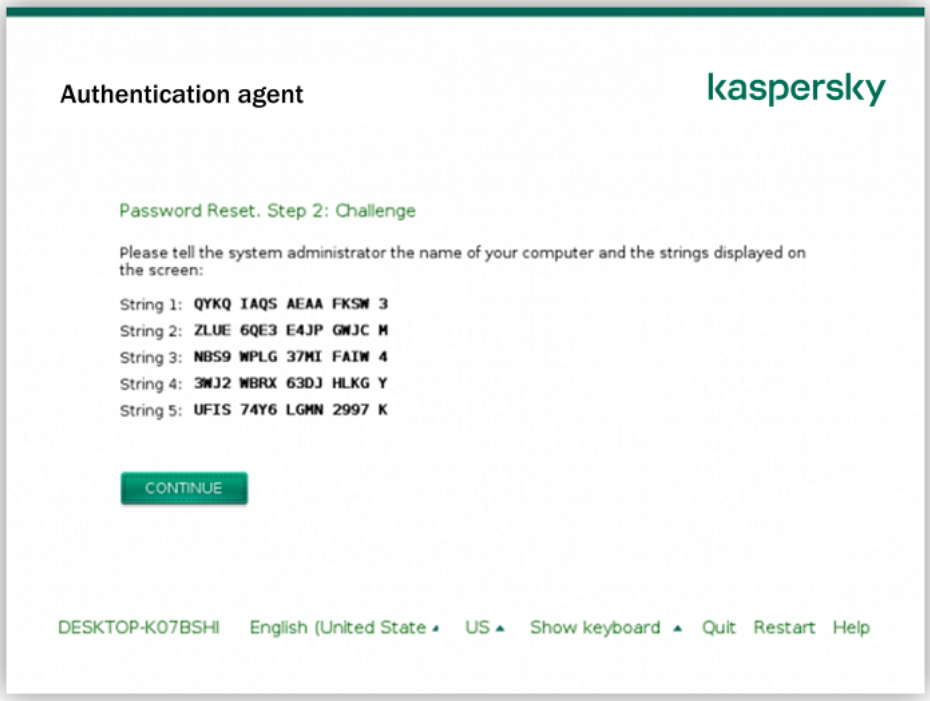
استعادة الوصول إلى محرك محمي بواسطة تقنية تشفير القرص من Kaspersky

إذا نسي مستخدم كلمة المرور للوصول إلى محرك أقراص صلب محمي بتقنية تشفير القرص من Kaspersky، فسوف تحتاج إلى بدء إجراء الاستعادة (طلب-رد). يمكنك أيضًا استخدام حساب الخدمة للوصول إلى القرص الثابت في حالة تمكين هذه الميزة في إعدادات تشفير القرص.

استعادة الوصول إلى محرك الأقراص الصلبة للنظام

استعادة الوصول إلى محرك أقراص ثابتة لنظام محمي بتقنية تشفير القرص من Kaspersky يتكون من الخطوات التالية:

1. يبلغ المستخدم المسؤول بكتل الطلب (راجع الشكل أدناه).
2. يدخل المسؤول كتل الطلب في Kaspersky Security Center ويستلم كتل الرد ثم يبلغ المستخدم بكتل الرد.
3. يدخل المستخدم كتل الرد في واجهة وكيل المصادقة ويطلب الوصول إلى محرك الأقراص الصلبة.



استعادة الوصول إلى محرك أقراص لنظام محمي بواسطة تقنية تشفير القرص من Kaspersky

لبدء إجراء الاستعادة، يحتاج المستخدم إلى النقر فوق الزر **Forgot your password** في واجهة وكيل المصادقة.

كيفية الحصول على كتل الرد لمحرك أقراص نظام محمي بتقنية تشفير القرص من Kaspersky في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Devices**.

3. في علامة التبويب **الأجهزة**، حدد اسم الكمبيوتر الخاص بالمستخدم الذي يطالب بالوصول إلى الملفات المشفرة وانقر بزر الماوس الأيمن لفتح القائمة السياقية.

4. في قائمة السياق، حدد **منح إمكانية الوصول في وضع عدم الاتصال**.

5. في النافذة التي تفتح، حدد القسم **وكيل المصادقة**.

6. في القسم **خوارزمية التشفير قيد الاستخدام**، حدد خوارزمية التشفير: **AES56** أو **AES256**.

تعتمد خوارزمية تشفير البيانات على مكتبة تشفير AES المضمنة في حزمة التوزيع: تشفير قوي (AES256) أو تشفير خفيف (AES56). يتم تثبيت مكتبة تشفير AES مع التطبيق.

7. في القائمة المنسدلة **الحساب**، حدد اسم وكيل المصادقة للمستخدم الذي طلب استعادة الوصول إلى المحرك.

8. في القائمة المنسدلة **محرك الأقراص الثابت**، حدد محرك الأقراص الصلبة المشفر الذي تريد استعادة الوصول إليه.

9. في القسم **طلب المستخدم** أدخل كتل الطلب التي تم أملاها المستخدم.

ونتيجةً لهذا، سيتم عرض محتويات كتل الرد إلى طلب المستخدم لاستعادة اسم المستخدم وكلمة مرور حساب وكيل المصادقة في الحقل **مفتاح الوصول**. نقل محتويات كتل الرد إلى المستخدم.

منح إمكانية الوصول في وضع عدم الاتصال

كيفية الحصول على كتل الرد لمحرك أقراص نظام محمي بتقنية تشفير القرص من Kaspersky في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Managed devices** ← **Devices**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى محركه.

3. انقر على الزر **Grant access to the device in offline mode**.

4. في النافذة التي تفتح، حدد القسم **Authentication Agent**.

5. في القائمة المنسدلة **Account**، حدد اسم وكيل المصادقة الذي تم إنشاؤه للمستخدم الذي يطلب استعادة اسم وكلمة مرور حساب وكيل المصادقة.

6. أدخل كتل الطلب التي ينقلها المستخدم.

سيتم عرض محتويات كتل الرد إلى طلب المستخدم لاستعادة اسم المستخدم وكلمة مرور حساب وكيل المصادقة في أسفل النافذة. نقل محتويات كتل الرد إلى المستخدم.

بعد إكمال إجراء الاستعادة، سوف يطلب وكيل المصادقة من المستخدم تغيير كلمة المرور.

استعادة الوصول إلى محرك أقراص ثابتة غير خاص بالنظام

استعادة الوصول إلى محرك أقراص ثابتة غير خاص بالنظام محمي بتقنية تشفير القرص من Kaspersky يتكون من الخطوات التالية:

1. يقوم المستخدم بإرسال ملف طلب الوصول إلى المسؤول.

2. يضيف المسؤول ملف الوصول إلى الطلب إلى Kaspersky Security Center ثم ينشئ ملف مفتاح وصول ويرسل الملف إلى المستخدم.

3. يضيف المستخدم ملف مفتاح الوصول إلى Kaspersky Endpoint Security ويحصل على الوصول إلى محرك الأقراص الصلبة.

لبدء إجراء الاستعادة، فإن المستخدم يحتاج إلى محاولة الوصول إلى محرك أقراص ثابتة. ونتيجة لذلك، سيقوم Kaspersky Endpoint Security بإنشاء ملف وصول طلب (ملف بامتداد KESDC)، والذي يحتاج المستخدم إلى إرساله إلى المسؤول (عبر البريد الإلكتروني على سبيل المثال).

كيفية الحصول على ملف مفتاح الوصول لمحرك أقراص ثابتة غير خاص بالنظام مشفر في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Devices**.

3. في علامة التبويب **الأجهزة**، حدد اسم الكمبيوتر الخاص بالمستخدم الذي يطالب بالوصول إلى الملفات المشفرة وانقر بزر الماوس الأيمن لفتح القائمة السياقية.

4. في قائمة السياق، حدد **منح إمكانية الوصول في وضع عدم الاتصال**.

5. في النافذة التي تفتح، حدد القسم **تشفير البيانات**.

6. في علامة التبويب **تشفير البيانات**، انقر فوق الزر **استعراض**.

7. في نافذة تحديد ملف وصول طلب، حدد المسار للملف المستلم من المستخدم.

سترى معلومات حول طلب المستخدم. يقوم Kaspersky Security Center بإنشاء ملف مفتاح. أرسل ملف مفتاح الوصول إلى البيانات المشفرة الذي تم إنشاؤه إلى المستخدم بالبريد الإلكتروني. أو احفظ ملف الوصول واستخدم أي طريقة متاحة لنقل الملف.

منح إمكانية الوصول في وضع عدم الاتصال

[كيفية الحصول على ملف مفتاح وصول إلى ملف مفتاح محرك أقراص ثابتة غير خاص بالنظام في Web Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Managed devices**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى بياناته.

3. انقر على الزر **Grant access to the device in offline mode**.

4. حدد **Data Encryption**.

5. انقر فوق الزر **Select file** وحدد ملف وصول الطلب الذي تلقيته من المستخدم (ملف بامتداد KESDC).
سيعرض مكون Web Console معلومات حول الطلب. وسيشمل هذا اسم الكمبيوتر الذي يطلب المستخدم الوصول إلى الملف عليه.

6. انقر على الزر **Save key** وحدد مجلدًا لحفظ ملف مفتاح الوصول إلى البيانات المشفرة (ملف بامتداد KESDR).

ونتيجة لذلك، ستتمكن من الحصول على مفتاح الوصول إلى البيانات المشفرة، والذي ستحتاج إلى نقله إلى المستخدم.

تسجيل الدخول باستخدام حساب خدمة وكيل المصادقة

يتيح لك Kaspersky Endpoint Security إضافة حساب خدمة وكيل المصادقة عند تشفير محرك أقراص. ويعد حساب الخدمة ضروريًا للوصول إلى الكمبيوتر، على سبيل المثال، عندما ينسى المستخدم كلمة المرور. ويمكنك أيضًا استخدام حساب الخدمة كحساب احتياطي. ولإضافة حساب، حدد حساب الخدمة في إعدادات تشفير القرص وأدخل اسم حساب المستخدم (افتراضيًا، `ServiceAccount`). وللمصادقة باستخدام الوكيل، ستحتاج إلى كلمة مرور لمرة واحدة.

كيفية معرفة كلمة المرور لمرة واحدة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Devices**.

3. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.

4. من نافذة خصائص الكمبيوتر، حدد قسم **المهام**.

5. في قائمة المهام، حدد **إدارة حسابات وكيل المصادقة** وافتح خصائص المهمة عن طريق النقر المزدوج.

6. من نافذة خصائص المهام، حدد القسم **الإعدادات**.

7. في قائمة الحسابات، حدد حساب خدمة وكيل المصادقة (على سبيل المثال، `WIN10-USER\ServiceAccount`).

8. في القائمة المنسدلة **الإجراء** حدد **عرض الحساب**.

9. في خصائص الحساب، حدد خانة الاختيار **عرض كلمة المرور الأصلية**.

10. انسخ كلمة المرور لمرة واحدة لتسجيل الدخول باستخدام حساب الخدمة.

كيفية معرفة كلمة المرور لمرة واحدة في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Managed devices** ← **Devices**.

2. انقر فوق اسم الكمبيوتر الذي ترغب في عرض قائمة حسابات وكيل المصادقة عليه.
تقوم هذه الخطوة بفتح خصائص الكمبيوتر.

3. في خصائص الكمبيوتر، حدد علامة التبويب **Tasks**.

4. في قائمة المهام، حدد **Manage Authentication Agent accounts**.

5. من خصائص الكمبيوتر، حدد قسم **Application Settings**.

6. في قائمة الحسابات، حدد حساب خدمة وكيل المصادقة (على سبيل المثال، `WIN10-USER\ServiceAccount`).

7. في خصائص الحساب، حدد خانة الاختيار **Show password**.

8. انسخ كلمة المرور لمرة واحدة لتسجيل الدخول باستخدام حساب الخدمة.

يتولى Kaspersky Endpoint Security تلقائيًا تحديث كلمة المرور في كل مرة يقوم فيها المستخدم بالمصادقة باستخدام حساب الخدمة. وبعد المصادقة باستخدام الوكيل، يجب عليك إدخال كلمة مرور حساب Windows. وعند تسجيل الدخول باستخدام حساب الخدمة، لا يمكنك استخدام تقنية تسجيل الدخول الأحادي (SSO).

تحديث نظام التشغيل

هناك عدد من الاعتبارات الخاصة لتحديث نظام التشغيل لجهاز كمبيوتر محمي بواسطة تشفير القرص بالكامل (FDE). قم بتحديث نظام التشغيل كما يلي: قم أولاً بتحديث نظام التشغيل على جهاز كمبيوتر واحد، ثم قم بتحديث نظام التشغيل على جزء صغير من أجهزة الكمبيوتر، ثم قم بتحديث نظام التشغيل على جميع أجهزة الكمبيوتر على الشبكة.

إذا كنت تستخدم تقنية تشفير القرص من Kaspersky، فسيتم تحميل وكيل المصادقة قبل بدء تشغيل نظام التشغيل. باستخدام وكيل المصادقة، يمكن للمستخدم تسجيل الدخول إلى النظام وتلقي الوصول إلى محركات الأقراص المشفرة. ثم يبدأ نظام التشغيل في التحميل.

إذا قمت ببدء تحديث لنظام التشغيل على جهاز كمبيوتر محمي باستخدام تقنية تشفير القرص من Kaspersky، فسيقوم معالج تحديث نظام التشغيل بإزالة وكيل المصادقة. نتيجة لذلك، يمكن قفل الكمبيوتر لأن محمل نظام التشغيل لن يكون قادرًا على الوصول إلى محرك الأقراص المشفر.

للحصول على تفاصيل حول تحديث نظام التشغيل بأمان، يُرجى الرجوع إلى قاعدة معارف الدعم الفني.

التحديث الآلي لنظام التشغيل متوفر في الظروف التالية:

1. يتم تحديث نظام التشغيل من خلال WSUS (Windows Server Update Services).

2. إصدار Windows 10 1607 (RS1) أو الإصدار الأحدث مثبت على الكمبيوتر.

3. Kaspersky Endpoint Security إصدار 11.2.0 أو أحدث مثبت على الكمبيوتر.

إذا تم تحقيق جميع الشروط، يمكنك تحديث نظام التشغيل بالطريقة المعتادة.

إذا كنت تستخدم تقنية تشفير القرص من Kaspersky (FDE) وكان الإصدار 11.1.0 أو 11.1.1 من Kaspersky Endpoint Security for Windows مثبتًا على الكمبيوتر، فلن تحتاج إلى فك تشفير محركات الأقراص الصلبة لتحديث Windows 10.

لتحديث نظام التشغيل، يجب عليك تنفيذ ما يلي:

1. قبل تحديث النظام، انسخ برامج التشغيل المسماة cm_km.inf وcm_km.sys وklfde.cat وklfde.inf وklfde.sys وklfdefsf.cat وklfdefsf.inf وklfdefsf.sys إلى مجلد محلي. على سبيل المثال، C:\fde_drivers.

2. قم بتشغيل تثبيت تحديث النظام باستخدام مفتاح التبديل `/ ReflectDrivers` وحدد المجلد الذي يحتوي على برامج التشغيل المحفوظة:

```
setup.exe /ReflectDrivers C:\fde_drivers
```

إذا كنت تستخدم تقنية تشفير محرك الأقراص من BitLocker، فلن تحتاج إلى فك تشفير محركات الأقراص الثابتة لتحديث نظام التشغيل Windows 10. للحصول على المزيد من المعلومات حول BitLocker، يُرجى زيارة موقع Microsoft الإلكتروني.

استبعاد الأخطاء الخاصة بتحديث وظيفة التشفير

يتم تحديث وظيفة تشفير القرص بالكامل عندما تتم ترقية إصدار سابق من التطبيق إلى Kaspersky Endpoint Security for Windows 12.1.

عند البدء في تحديث وظيفة تشفير القرص بالكامل، قد تحدث الأخطاء التالية:

- يتعذر بدء التحديث.
- الجهاز غير متوافق مع وكيل المصادقة.

قم بما يلي لاستبعاد الأخطاء التي حدثت عند قيامك ببدء عملية التحديث لوظيفة تشفير القرص بالكامل في إصدار التطبيق الجديد:

1. فك تشفير محركات الأقراص الصلبة.
2. تشفير محركات الأقراص الصلبة مرة أخرى.

في أثناء تحديث وظيفة تشفير القرص بالكامل، قد تحدث الأخطاء التالية:

- يتعذر استكمال التحديث.
- اكتملت إجراءات التراجع عن ترقية تشفير القرص بالكامل مع ظهور خطأ.

لاستبعاد الأخطاء التي حدثت أثناء عملية التحديث لوظيفة تشفير القرص بالكامل،

قم باستعادة الوصول إلى الأجهزة المشفرة باستخدام أداة الاستعادة المساعدة.

تحديد مستوى تتبع وكيل المصادقة

يقوم التطبيق بتسجيل معلومات الخدمة حول تشغيل وكيل المصادقة والمعلومات حول عمليات المستخدم مع وكيل المصادقة في ملف التتبع.

لتحديد مستوى تتبع وكيل المصادقة:

1. بمجرد بدء تشغيل الكمبيوتر ذو محركات الأقراص الصلبة المشفرة، اضغط على الزر **F3** لاستدعاء نافذة تكوين إعدادات وكيل المصادقة.
2. حدد مستوى التتبع في نافذة إعدادات وكيل المصادقة:

- **Disable debug logging (default)**. إذا تم تحديد هذا الخيار، لا يسجل التطبيق المعلومات حول أحداث وكيل المصادقة في ملف التتبع.
- **Enable debug logging**. إذا تم تحديد هذا الخيار، يقوم التطبيق بتسجيل المعلومات حول تشغيل وكيل المصادقة وعمليات المستخدم التي تم إجراؤها باستخدام وكيل المصادقة في ملف التتبع.
- **Enable verbose logging**. إذا تم تحديد هذا الخيار، يقوم التطبيق بتسجيل معلومات تفصيلية حول تشغيل وكيل المصادقة وعمليات المستخدم التي تم إجراؤها باستخدام وكيل المصادقة في ملف التتبع.

يكون مستوى تفاصيل الإدخالات بموجب هذا الخيار أعلى مقارنة بمستوى الخيار **Enable debug logging**. يؤدي مستوى تفاصيل الإدخالات العالي إلى إبطاء بدء تشغيل وكيل المصادقة ونظام التشغيل.

- **Enable debug logging and select serial port**. إذا تم تحديد هذا الخيار، يقوم التطبيق بتسجيل معلومات حول تشغيل وكيل المصادقة وعمليات المستخدم التي تم إجراؤها مع وكيل المصادقة في ملف التتبع وترحيلهم عبر المنفذ COM.

  في حالة اتصال كمبيوتر ذو محركات أقراص صلبة مشفرة بكمبيوتر آخر عبر المنفذ COM، فيمكن فحص أحداث وكيل المصادقة من الكمبيوتر الآخر.

- **Enable verbose debug logging and select serial port**. إذا تم تحديد هذا الخيار، يقوم التطبيق بتسجيل معلومات تفصيلية حول تشغيل وكيل المصادقة وعمليات المستخدم التي تم إجراؤها مع وكيل المصادقة في ملف التتبع وترحيلهم عبر المنفذ COM.

يكون مستوى تفاصيل الإدخالات بموجب هذا الخيار أعلى مقارنة بمستوى الخيار **Enable debug logging and select serial port**. يؤدي مستوى تفاصيل الإدخالات العالي إلى إبطاء بدء تشغيل وكيل المصادقة ونظام التشغيل.

يتم تسجيل البيانات في ملف تتبع وكيل المصادقة إذا كانت هناك محركات أقراص صلبة مشفرة على الكمبيوتر أو أثناء تشفير القرص بالكامل.

لا يتم إرسال ملف تتبع وكيل المصادقة إلى Kaspersky وذلك بعكس ملفات تتبع التطبيق الأخرى. إذا لزم الأمر، يمكنك إرسال ملف تتبع وكيل المصادقة يدويًا إلى Kaspersky لتحليله.

تحرير نصوص تعليمات وكيل المصادقة

قبل تحرير رسائل التعليمات لوكيل المصادقة، الرجاء مراجعة قائمة الأحرف المدعومة في بيئة ما قبل التمهيد (اطلع عليها أدناه).

لتحرير رسائل تعليمات وكيل المصادقة:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **إعدادات التشفير العامة**.
5. في القسم **القوالب**، انقر على الزر **تعليمات**.
6. في النافذة التي تفتح، افعل ما يلي:
   - حدد علامة التبويب **المصادقة** لتحرير نص التعليمات الموضح في نافذة وكيل المصادقة عند إدخال بيانات اعتماد الحساب.
   - حدد علامة التبويب **تغيير كلمة المرور** لتحرير نص التعليمات الموضح في نافذة وكيل المصادقة عند تغيير كلمة المرور لحساب وكيل المصادقة.
   - حدد علامة التبويب **استرداد كلمة المرور** لتحرير نص التعليمات الموضح في نافذة وكيل المصادقة عند استرداد كلمة المرور لحساب وكيل المصادقة.
7. تحرير رسائل التعليمات.

   إذا كنت تريد استعادة النص الأصلي، انقر فوق الزر **افتراضيًا**.

يمكنك إدخال نص التعليمات الذي يحتوي على 16 سطرًا أو أقل. الحد الأقصى لطول سطر هو 64 حرفًا.

8. احفظ تغييراتك.

دعم محدود للأحرف في رسائل تعليمات وكيل المصادقة

في بيئة ما قبل التشغيل، يتم دعم أحرف Unicode التالية:

- الأبجدية اللاتينية الأساسية (0000 - 007F)
- أحرف إضافية لاتينية (0080 - 00FF) (Latin-1)
- اللاتينية الموسعة (0100 - 017F) (Latin-A)
- اللاتينية الموسعة (0180 - 024F) (Latin-B)
- أحرف المعرف الممتدة غير المدمجة (02B0 - 02FF)
- علامات التشكيل المدمجة (0300 - 036F)
- الأبجدية اليونانية والقبطية (0370 - 03FF)
- السيريلية (0400 - 04FF)
- العبرية (0590 - 05FF)
- الخط العربي (0600 - 06FF)
- اللاتينية الإضافية الموسعة (1E00 - 1EFF)
- علامات الترقيم (2000 - 206F)
- رموز العملات (20A0 - 20CF)
- الرموز شبيهة الأحرف (2100 - 214F)
- الأشكال الهندسية (25A0 - 25FF)
- أشكال العرض من الكتابة العربية-Arabic script-B (FE70 - FEFF)

لا يتم دعم الأحرف غير المحددة في هذه القائمة في بيئة ما قبل التشغيل. ولا يوصى باستخدام هذه الأحرف في رسائل تعليمات وكيل المصادقة.

إزالة الكائنات والبيانات الباقية بعد اختبار تشغيل وكيل المصادقة

إثناء إزالة تثبيت التطبيق، إذا اكتشف Kaspersky Endpoint Security كائنات وبيانات متبقية على محرك قرص النظام بعد التشغيل الاختباري لوكيل المصادقة، فسيتم قطع عملية إزالة تثبيت التطبيق ويصبح من المستحيل إجراؤها حتى يتم إزالة تلك الكائنات والبيانات.

قد تتبقى كائنات وبيانات على محرك الأقراص الصلبة الخاص بالنظام بعد التشغيل الاختباري لوكيل المصادقة في حالات استثنائية فقط. على سبيل المثال، قد يحدث ذلك إذا لم تتم إعادة تشغيل الكمبيوتر بعد أن تم تطبيق سياسة Kaspersky Security Center مع إعدادات التشفير، أو إذا فشل بدء التطبيق بعد التشغيل الاختباري لوكيل المصادقة.

يمكنك إزالة الكائنات والبيانات المتبقية على محرك الأقراص الصلبة الخاص بالنظام بعد التشغيل الاختباري لوكيل المصادقة بالطرق التالية:

- استخدام سياسة Kaspersky Security Center.
- استخدام أداة الاستعادة.

لاستخدام سياسة Kaspersky Security Center لإزالة الكائنات والبيانات المتبقية بعد التشغيل الاختباري لوكيل المصادقة:

1. طبق على الكمبيوتر إحدى سياسات Kaspersky Security Center مع تهيئة الإعدادات لفك تشفير جميع محرك الأقراص الصلبة بالكمبيوتر.

2. ابدأ تشغيل Kaspersky Endpoint Security.

لإزالة المعلومات حول عدم توافق التطبيق مع وكيل المصادقة،

أدخل الأمر `avp pbatestreset` في سطر الأوامر.

إدارة BitLocker

BitLocker هي تقنية تشفير مدمجة في نظام التشغيل Windows. Kaspersky Endpoint Security يسمح لك بالتحكم في Bitlocker وإدارتها باستخدام Kaspersky Security Center. BitLocker تقوم بتشفير أحجام منطقية. لا يمكن استخدام تقنية BitLocker في تشفير محركات الأقراص القابلة للإزالة. وللحصول على مزيد من التفاصيل عن BitLocker، يُرجى الرجوع إلى مستندات Microsoft.

BitLocker توفر تخزين آمن لمفاتيح الوصول باستخدام وحدة نمطية للنظام الأساسي الموثوق به. الوحدة النمطية للنظام الأساسي الموثوق به (TPM) هي رقاقة إلكترونية تم تصميمها لتوفير الوظائف الأساسية المرتبطة بالأمن (على سبيل المثال، لتخزين مفاتيح التشفير). عادة يتم تركيب الوحدة النمطية للنظام الأساسي الموثوق به على اللوحة الأم في جهاز الكمبيوتر وتتفاعل مع كل مكونات النظام الأخرى عبر ناقل الأجهزة. استخدام TPM هي أكثر طريقة آمنة لتخزين مفاتيح وصول BitLocker حيث إن TPM توفر تحقق من سلامة النظام قبل التشغيل. لا يزال بإمكانك تشفير محركات الأقراص على جهاز كمبيوتر بدون استخدام TPM. في هذه الحالة، سيتم تشفير مفتاح الوصول بكلمة مرور. BitLocker يستخدم أساليب المصادقة التالية:

- TPM.
- TPM ورمز PIN.
- كلمة المرور.

بعد تشفير محرك أقراص، يقوم BitLocker بإنشاء مفتاح رئيسي. يقوم Kaspersky Endpoint Security بإرسال المفتاح الرئيسي إلى Kaspersky Security Center حتى يمكنك استعاد الوصول إلى القرص إذا، مثلًا، نسي المستخدم كلمة المرور.

إذا قام مستخدم بتشفير قرص باستخدام BitLocker، فسوف يرسل Kaspersky Endpoint Security معلومات عن تشفير القرص إلى Kaspersky Security Center. مع ذلك، سوف يقوم Kaspersky Endpoint Security بإرسال المفتاح الرئيسي إلى Kaspersky Security Center حتى يكون من المستحيل استعادة الوصول إلى القرص باستخدام Kaspersky Security Center. كي تعمل تقنية BitLocker بشكل صحيح مع Kaspersky Security Center، قم بفك تشفير محرك الأقراص وأعد تشفيره باستخدام سياسة. يمكنك فك تشفير محرك أقراص محليًا أو باستخدام سياسة.

بعد تشفير محرك أقراص النظام، يحتاج المستخدم إلى تجاوز مصادقة BitLocker لإقلاع نظام التشغيل. وبعد إجراء المصادقة، سوف تسمح تقنية BitLocker للمستخدمين بتسجيل الدخول. ولا تدعم BitLocker تقنية تسجيل الدخول الأحادي (SSO).

إذا كنت تستخدم سياسات مجموعات Windows، أوقف تشغيل إدارة BitLocker في إعدادات السياسة. يمكن أن تتعارض إعدادات السياسة لنظام Windows مع إعدادات سياسة Kaspersky Endpoint Security. عند تشفير محرك أقراص، يمكن أن تحدث أخطاء.

بدء تشغيل تشفير محرك الأقراص من BitLocker

قبل بدء ي تشفير القرص بالكامل، ننصحك بالتأكد من عدم تعرض الكمبيوتر للإصابة. للقيام بذلك، ابدأ مهمة الفحص الكامل أو فحص المناطق الحرجة. وقد يتسبب تنفيذ تشفير القرص بالكامل على جهاز كمبيوتر مصاب بفيروس جذر إلى جعل الكمبيوتر غير صالح للعمل.

لاستخدام تشفير محرك الأقراص من BitLocker على أجهزة الكمبيوتر التي تعمل بأنظمة التشغيل Windows للخوادم، فإن تثبيت مكون تشفير محرك الأقراص من BitLocker قد يكون مطلوبًا. تثبيت المكون باستخدام أدوات نظام التشغيل (إضافة أدوار ومعالج المكونات). وللمزيد من المعلومات عن تثبيت تشفير محرك الأقراص من BitLocker، يرجى الرجوع إلى مستندات Microsoft.

كيفية تشغيل تشفير محرك الأقراص باستخدام BitLocker من خلال وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.
5. في القائمة المنسدلة **تقنية التشفير** حدد **تشفير محرك الأقراص من BitLocker**.
6. في القائمة المنسدلة **وضع التشفير** حدد **تشفير جميع محركات الأقراص الصلبة**.

في حالة تثبيت العديد من أنظمة التشغيل على الكمبيوتر، فسوف يمكنك بعد التشفير تحميل نظام التشغيل الذي تم إجراء التشفير عليه.

7. قم بتكوين خيارات تشفير محرك الأقراص من BitLocker المتقدمة (انظر الجدول أدناه).
8. احفظ تغييراتك.

كيفية تشغيل تشفير محرك الأقراص باستخدام BitLocker من خلال Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Data Encryption** ← **Full Disk Encryption**.

5. في القسم **Manage encryption**، حدد **BitLocker Drive Encryption**.

6. انقر على رابط **BitLocker Drive Encryption**.
هذا سيفتح نافذة إعدادات تشفير محرك الأقراص من BitLocker.

7. في القائمة المنسدلة **Encryption mode** حدد **Encrypt all hard drives**.

في حالة تثبيت العديد من أنظمة التشغيل على الكمبيوتر، فسوف يمكنك بعد التشفير تحميل نظام التشغيل الذي تم إجراء التشفير عليه.

8. قم بتكوين خيارات تشفير محرك الأقراص من BitLocker المتقدمة (انظر الجدول أدناه).

9. احفظ تغييراتك.

يمكنك استخدام أداة مراقبة التشفير للتحكم في عملية تشفير القرص أو فك تشفيره على كمبيوتر المستخدم. يمكنك تشغيل أداة مراقبة التشفير من نافذة التطبيق الرئيسية.

مراقبة التشفير

بعد تطبيق السياسة، سيعرض التطبيق الاستعلامات التالية، بناءً على إعدادات المصادقة:

- TPM فقط. لا يوجد إدخال مطلوب من المستخدم. سيتم تشفير القرص عند إعادة تشغيل الكمبيوتر.
- TPM + PIN / كلمة المرور. إذا كانت الوحدة النمطية للنظام الأساسي الموثوق به (TPM) متاحة، فستظهر نافذة المطالبة برمز PIN. إذا كانت الوحدة النمطية للنظام الأساسي الموثوق به (TPM) غير متاحة، فسترى نافذة المطالبة بكلمة المرور لمصادقة ما قبل التشغيل.
- كلمة المرور فقط. وسترى نافذة مطالبة بكلمة المرور لمصادقة ما قبل التمهيد.

إذا تم تمكين وضع التوافق مع معيار معالجة المعلومات الفيدرالية لنظام التشغيل بالكمبيوتر، فعندئذ يتم عرض طلب لتوصيل جهاز تخزين لحفظ ملف مفتاح الاسترداد، وذلك في إصدار نظام التشغيل Windows 8 والإصدارات الأقدم. يمكنك حفظ عدة ملفات لمفاتيح الاسترداد على جهاز تخزين واحد.

بعد تعيين كلمة مرور أو رمز PIN، سوف يطلب منك BitLocker إعادة تشغيل الكمبيوتر لإكمال التشفير. بعد ذلك، سيحتاج المستخدم إلى العمل من خلال إجراء مصادقة BitLocker. بعد إجراء المصادقة، يجب على المستخدم تسجيل الدخول على النظام. بعد تحميل نظام التشغيل، سوف يكمل BitLocker التشفير.

إذا لم تكن هناك إمكانية الوصول إلى مفاتيح التشفير، فقد يطلب المستخدم من مسؤول الشبكة المحلية بتوفير مفتاح الاسترداد (إذا لم يكن مفتاح الاسترداد قد تم حفظه في وقت سابق على جهاز تخزين أو تم فقدانه).

إعدادات مكون تشفير محرك BitLocker

المعلمة	الوصف
تمكين استخدام مصادقة BitLocker التي تتطلب إدخال لوحة المفاتيح قبل التشغيل على أجهزة الكمبيوتر اللوحية	تؤدي خانة الاختيار هذه إلى تمكين / تعطيل استخدام المصادقة التي تتطلب إدخال بيانات في بيئة مسبقة التمهيد، حتى وإن كان النظام الأساسي ليس لديه قدرة الإدخال مسبق التمهيد (على سبيل المثال، لوحات المفاتيح التي تعمل باللمس على أجهزة الكمبيوتر اللوحية). إن شاشة اللمس الخاصة بأجهزة الكمبيوتر اللوحية غير متاحة في بيئة ما قبل التشغيل. لإكمال مصادقة BitLocker على أجهزة الكمبيوتر اللوحية، يجب على المستخدم، على سبيل المثال، توصيل لوحة مفاتيح USB. إذا تم تحديد خانة الاختيار، يتم السماح باستخدام المصادقة التي تتطلب إدخال مسبق التهيئة. من المستحسن استخدام هذا الإعداد فقط للأجهزة التي لديها أدوات إدخال بيانات بديلة في بيئة مسبقة التهيئة، مثل لوحة مفاتيح USB بالإضافة إلى لوحات المفاتيح التي تعمل باللمس على الشاشة. في حال عدم تحديد خانة الاختيار، فإن تشفير محرك الأقراص من BitLocker يكون غير ممكنًا على الأجهزة اللوحية.
استخدام تشفير الأجهزة (Windows 8 والإصدارات الأحدث)	إذا تم تحديد خانة الاختيار، يقوم التطبيق بتطبيق تشفير الأجهزة. يتيح لك ذلك زيادة سرعة التشفير واستخدام أقل لموارد الكمبيوتر.
تشفير مساحة القرص المستخدمة فقط (يحد من وقت التشفير)	يؤدي تحديد خانة الاختيار هذه إلى تمكين / تعطيل الخيار الذي يقيد منطقة التشفير لمقاطع محرك الأقراص الصلبة الممتلئة فقط. ويتيح لك هذا الحد تقليل وقت التشفير. لا يؤدي تمكين أو تعطيل ميزة **تشفير مساحة القرص المستخدمة فقط (يحد من وقت التشفير)** بعد بدء التشفير إلى تعديل هذا الإعداد حتى يتم فك تشفير محركات الأقراص الثابتة. يجب تحديد أو إلغاء تحديد خانة الاختيار قبل بدء التشفير. في حالة تحديد خانة الاختيار، يتم تشفير أجزاء محرك القرص الصلب الممتلئة بالملفات فقط. ويقوم Kaspersky Endpoint Security تلقائيًا بتشفير البيانات الجديدة بمجرد إضافتها. في حالة إلغاء تحديد خانة الاختيار، يتم تشفير محرك القرص الصلب بالكامل، بما في ذلك القطاعات المتبقية من الملفات التي تم حذفها وتعديلها سابقًا.

	هذا الخيار مستحسن لمحركات الأقراص الصلبة الجديدة التي لم يتم تعديل بياناتها أو حذفها. وإذا كنت تقوم بتشفير محرك أقراص صلبة مستخدم بالفعل، فمن المستحسن تشفير محرك الأقراص الصلبة بالكامل. ويضمن هذا حماية كل البيانات، وحتى حذف البيانات التي يحتمل أن تكون قابلة للاسترداد. ويتم إلغاء تحديد خانة الاختيار هذه بشكل افتراضي.
طريقة المصادقة	**كلمة المرور فقط (Windows 8 والإصدارات الأحدث)** في حالة تحديد هذا الاختيار، فإن Kaspersky Endpoint Security يطلب من المستخدم إدخال كلمة مرور عندما يحاول المستخدم الوصول إلى محرك مشفر. يمكن تحديد هذا الاختيار في حالة عدم استخدام وحدة نمطية للنظام الأساسي الموثوق به (TPM). **الوحدة النمطية للنظام الأساسي الموثوق بها (TPM)** إذا تم تحديد هذا الخيار، فيستخدم BitLocker الوحدة النمطية للنظام الأساسي الموثوق به (TPM). الوحدة النمطية للنظام الأساسي الموثوق به (TPM) هي رقاقة إلكترونية تم تصميمها لتوفير الوظائف الأساسية المرتبطة بالأمن (على سبيل المثال، لتخزين مفاتيح التشفير). عادة يتم تركيب الوحدة النمطية للنظام الأساسي الموثوق به على اللوحة الأم في جهاز الكمبيوتر وتتفاعل مع كل مكونات النظام الأخرى عبر ناقل الأجهزة. بالنسبة لأجهزة الكمبيوتر التي تعمل بنظام Windows 7 أو Windows Server 2008 R2، يتوفر التشفير باستخدام الوحدة TPM فقط. إذا لم يتم تثبيت وحدة TPM، فلن يكون تشفير BitLocker ممكنًا. استخدام كلمة مرور على أجهزة الكمبيوتر هذه غير مدعوم. يمكن للجهاز المزود بوحدة نمطية لنظام أساسي موثوق به إنشاء مفاتيح تشفير لا يمكن فك تشفيرها إلا باستخدام الجهاز. تقوم الوحدة النمطية للنظام الأساسي الموثوق به بتشفير مفاتيح التشفير باستخدام مفتاح تخزين الجذر الخاص بها. ويتم تخزين مفتاح تخزين الجذر داخل الوحدة النمطية للنظام الأساسي الموثوق به. يوفر ذلك مستوى إضافي من الحماية ضد محاولات اختراق مفاتيح التشفير. ويتم تحديد هذا الإجراء بصورة افتراضية. يمكنك تعيين طبقة حماية إضافية للوصول إلى مفتاح التشفير، وتشفير المفتاح بكلمة مرور أو رمز PIN: • **استخدام رمز PIN لأجل TPM**. إذا كانت خانة الاختيار هذه محددة، يمكن للمستخدم استخدام رمز PIN للحصول على الوصول إلى مفتاح تشفير مخزن في وحدة نمطية للنظام الأساسي الموثوق به (TPM). إذا كانت خانة الاختيار هذه غير محددة، فإنه لا يجوز للمستخدمين استخدام رموز PIN. للوصول إلى مفتاح التشفير، يجب على المستخدم إدخال كلمة المرور. يمكنك السماح للمستخدم باستخدام رمز PIN المحسن. ويسمح رمز PIN المحسّن باستخدام أحرف أخرى بالإضافة إلى الأحرف الرقمية: الأحرف اللاتينية الكبيرة والصغيرة والأحرف الخاصة والمسافات. • **وحدة النظام الأساسي الموثوق بها (TPM) أو كلمة المرور إذا لم تكن وحدة النظام الأساسي الموثوق بها متاحة**. إذا تم تحديد خانة الاختيار، فبإمكان المستخدم استخدام كلمة مرور للحصول على حق الوصول إلى مفاتيح التشفير عند عدم توفر الوحدة النمطية للنظام الأساسي الموثوق به. في حال عدم تحديد خانة الاختيار وكان TPM غير متوفرًا، فإن تشفير القرص بالكامل لن يبدأ.

فك تشفير محرك أقراص محمي بتقنية BitLocker

يمكن للمستخدمين فك محرك أقراص باستخدام نظام التشغيل (وظيفة إيقاف BitLocker). بعد ذلك، سوف يطلب Kaspersky Endpoint Security من المستخدم تشفير القرص مرة أخرى. Kaspersky Endpoint Security سوف يطلب تشفير القرص إلا إذا قمت بتفعيل تشفير القرص في السياسة.

كيفية فك تشفير محرك أقراص محمي بتقنية BitLocker من خلال وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.

5. في القائمة المنسدلة **تقنية التشفير** حدد **تشفير محرك الأقراص من BitLocker**.

6. في القائمة المنسدلة **وضع التشفير** حدد **فك تشفير جميع محركات الأقراص الصلبة**.

7. احفظ تغييراتك.

كيفية فك تشفير محرك أقراص صلبة مشفر باستخدام BitLocker من خلال Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

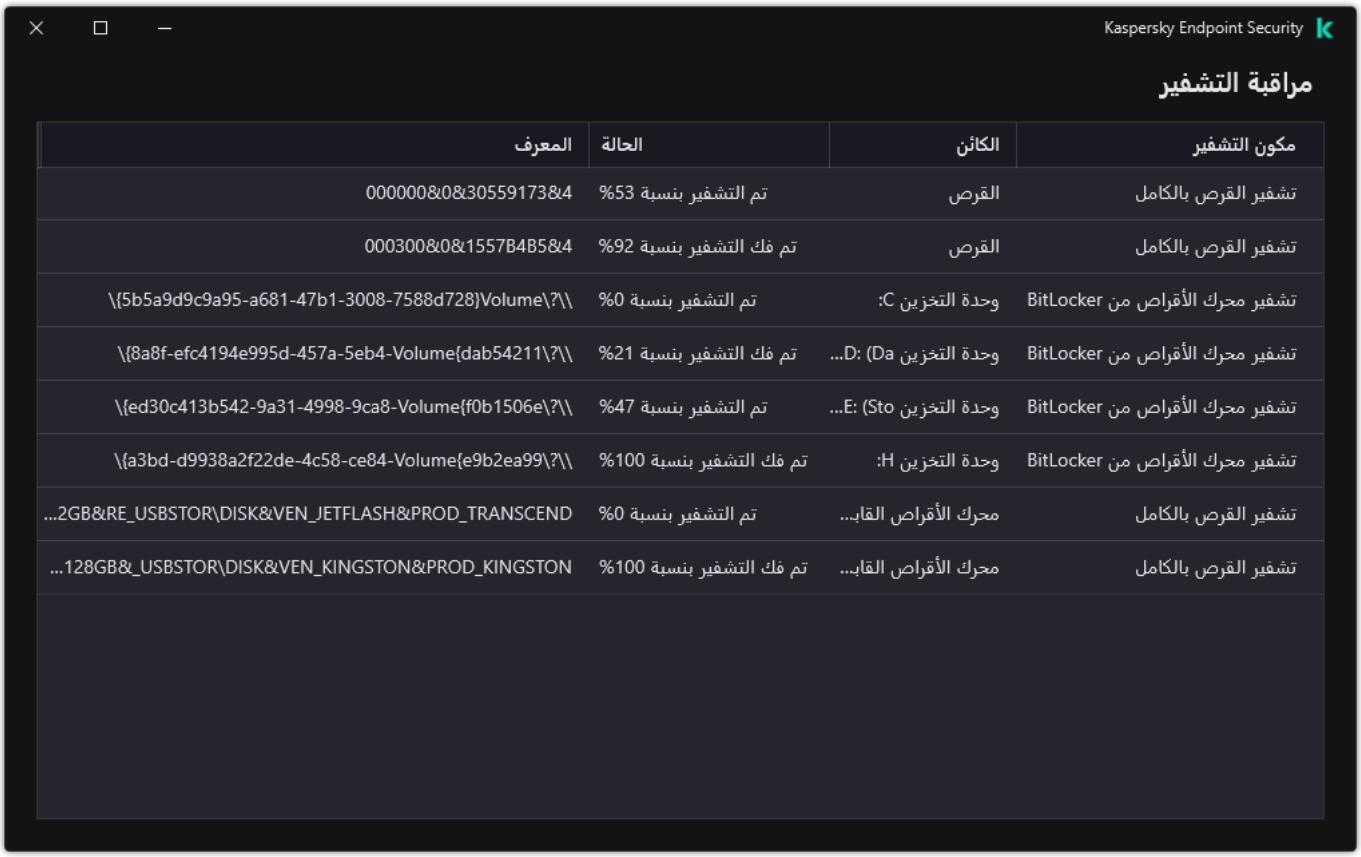
4. انتقل إلى **Data Encryption** ← **Full Disk Encryption**.

5. حدد تقنية **BitLocker Drive Encryption** واتبع الرابط لتكوين الإعدادات.
ستفتح إعدادات التشفير.

6. في القائمة المنسدلة **Encryption mode** حدد **Decrypt all hard drives**.

7. احفظ تغييراتك.

يمكنك استخدام أداة مراقبة التشفير للتحكم في عملية تشفير القرص أو فك تشفيره على كمبيوتر المستخدم. يمكنك تشغيل أداة مراقبة التشفير من نافذة التطبيق الرئيسية.



مراقبة التشفير

استعادة الوصول إلى محرك محمي باستخدام BitLocker

إذا نسي مستخدم كلمة المرور للوصول إلى محرك أقراص صلب محمي بتقنية تشفير من BitLocker، فسوف تحتاج إلى بدء إجراء الاسترداد (طلب-رد).

إذا كان نظام تشغيل الكمبيوتر عليه وضع التوافق مع معيار معالجة المعلومات الفيدرالية مفعلًا، فإنه في إصدارات Windows 8 والأقدم منها يتم حفظ ملف مفتاح الاسترداد في محرك الأقراص القابل للإزالة قبل التشفير. لاستعادة الوصول إلى المحرك، أدخل محرك الأقراص القابل للإزالة واتبع التعليمات الظاهرة على الشاشة.

استعادة الوصول إلى قرص صلب مشفر بتقنية BitLocker يتضمن الخطوات التالية:

1. إخبار المستخدم للمسؤول بمعرف مفتاح الاسترداد (انظر الشكل أدناه).
2. تحقق المسؤول من معرف مفتاح الاسترداد في خصائص الكمبيوتر في Kaspersky Security Center. يجب أن يتطابق المعرف المقدم من قبل المستخدم مع المعرف المعروض في إعدادات الكمبيوتر.
3. إذا كان معرف مفتاح الاسترداد متطابقين، يقوم المسؤول بتوفير للمستخدم مفتاح الاسترداد أو يرسل إليه ملف مفتاح الاسترداد.

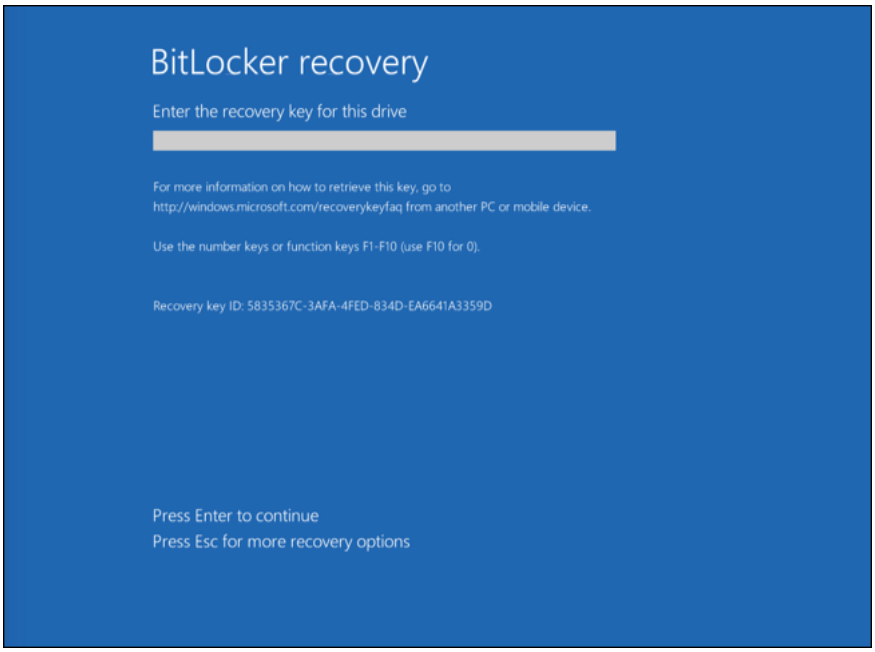
يتم استخدام ملف مفتاح الاسترداد مع أجهزة الكمبيوتر التي تعمل بأنظمة التشغيل التالية:

- Windows 7؛
- Windows 8؛
- Windows Server 2008؛
- Windows Server 2011؛

- Windows Server 2012.

لجميع أنظمة التشغيل الأخرى، يتم استخدام مفتاح الاسترداد.

4. يدخل المستخدم مفتاح الاسترداد ويكتسب حق الوصول إلى محرك الأقراص الصلبة.



استعادة الوصول إلى محرك أقراص مشفر باستخدام BitLocker

استعادة الوصول إلى محرك خاص بالنظام

لبدء إجراء الاسترداد، فإن المستخدم يحتاج إلى الضغط على مفتاح **Esc** في مرحلة المصادقة قبل الإقلاع.

كيفية عرض مفتاح الاسترداد لمحرك أقراص نظامي مشفر بتقنية BitLocker في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Devices**.

3. في علامة التبويب **الأجهزة**، حدد اسم الكمبيوتر الخاص بالمستخدم الذي يطالب بالوصول إلى الملفات المشفرة وانقر بزر الماوس الأيمن لفتح القائمة السياقية.

4. في قائمة السياق، حدد **منح إمكانية الوصول في وضع عدم الاتصال**.

5. في النافذة التي تفتح، حدد القسم **الوصول إلى محرك ميزة BitLocker المحمي**.

6. قم بمطالبة المستخدم بمعرف مفتاح الاسترداد الموضح في نافذة إدخال كلمة مرور BitLocker، وقم بمقارنته بالمعرف الموجود في الحقل **معرف مفتاح الاسترداد**.

في حالة عدم تطابق المعرفات، يكون هذا المفتاح غير صالح لاستعادة الوصول إلى محرك النظام المحدد. تأكد من تطابق اسم الكمبيوتر المحدد مع اسم كمبيوتر المستخدم.

ونتيجةً لذلك، سوف تحصل على الوصول إلى مفتاح الاسترداد أو ملف مفتاح الاسترداد، والذي ستحتاج إلى نقله إلى المستخدم.

استعادة الوصول إلى محرك أقراص مشفر باستخدام BitLocker

[كيفية عرض مفتاح الاسترداد لمحرك أقراص نظام مشفر بتقنية BitLocker في Web Console وCloud Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Managed devices**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى محركه.

3. انقر على الزر **Grant access to the device in offline mode**.

4. في النافذة التي تفتح، حدد القسم **BitLocker**.

5. تحقق من معرف مفتاح الاسترداد. المعرف الذي يوفره المستخدم يجب أن يطابق المعرف المعروض في إعدادات الكمبيوتر.

في حالة عدم تطابق المعرفات، يكون هذا المفتاح غير صالح لاستعادة الوصول إلى محرك النظام المحدد. تأكد من تطابق اسم الكمبيوتر المحدد مع اسم كمبيوتر المستخدم.

6. انقر على **Receive key**.

ونتيجةً لذلك، سوف تحصل على الوصول إلى مفتاح الاسترداد أو ملف مفتاح الاسترداد، والذي ستحتاج إلى نقله إلى المستخدم.

بعد تحميل نظام التشغيل، يطالب Kaspersky Endpoint Security المستخدم بتغيير كلمة المرور أو رمز PIN. بعد تعيين كلمة مرور جديدة أو رمز PIN جديد، سينشئ BitLocker مفتاحًا رئيسيًا جديدًا ويرسل المفتاح إلى Kaspersky Security Center. نتيجة لذلك، سيتم تحديث مفتاح الاسترداد وملف مفتاح الاسترداد. إذا لم يغير المستخدم كلمة المرور، يمكنك استخدام مفتاح الاسترداد القديم في المرة القادمة التي يحمل فيها نظام التشغيل.

لا تسمح أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 7 بتغيير كلمة المرور أو رمز PIN. وبعد إدخال مفتاح الاسترداد وتحميل نظام التشغيل، لن يطالب Kaspersky Endpoint Security المستخدم بتغيير كلمة المرور أو رمز PIN. وبالتالي، من المستحيل تعيين كلمة مرور جديدة أو رمز PIN جديد. وتنشأ هذه المشكلة من خصوصيات نظام التشغيل. وللمتابعة، تحتاج إلى إعادة تشفير محرك الأقراص الصلبة.

استعادة الوصول إلى محرك أقراص غير خاص بالنظام

لبدء إجراء الاسترداد، يحتاج المستخدم إلى النقر فوق الزر **هل نسيت كلمة المرور؟** في النافذة التي توفر الوصول إلى المحرك. بعد الحصول على الوصول إلى محرك مشفر، يمكن للمستخدم تفعيل إلغاء القفل الآلي للمحرك أثناء مصادقة Windows في إعدادات BitLocker.

كيفية عرض مفتاح الاسترداد لمحرك أقراص غير خاص بالنظام مشفر بتقنية BitLocker في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

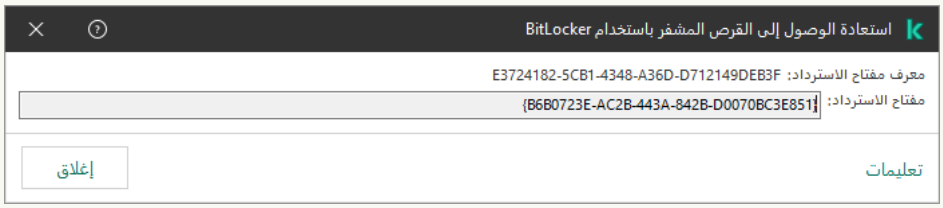
2. في شجرة وحدة تحكم الإدارة، حدد المجلد **إضافي** ← **تشفير البيانات وحمايتها** ← المجلد **برامج التشغيل المشفرة**.

3. في مساحة العمل، حدد الجهاز المشفر الذي تريد إنشاء ملف مفتاح وصول له، ثم في قائمة سياق الجهاز، انقر فوق **الحصول على حق الوصول إلى الجهاز في Kaspersky Endpoint Security for Windows**.

4. قم بمطالبة المستخدم بمعرف مفتاح الاسترداد الموضح في نافذة إدخال كلمة مرور BitLocker، وقم بمقارنته بالمعرف الموجود في الحقل **معرف مفتاح الاسترداد**.

في حالة عدم تطابق المعرفات، يكون هذا المفتاح غير صالح لاستعادة الوصول إلى المحرك المحدد. تأكد من تطابق اسم الكمبيوتر المحدد مع اسم كمبيوتر المستخدم.

5. أرسل إلى المستخدم المفتاح الموضح في الحقل **مفتاح الاسترداد**.



استعادة الوصول إلى محرك أقراص مشفر باستخدام BitLocker

كيفية عرض مفتاح الاسترداد لمحرك أقراص نظام غير مشفر بتقنية BitLocker في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Operations** ← **Data encryption and protection** ← **Encrypted Drives**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى محركه.

3. انقر على الزر **Grant access to the device in offline mode**.
هذا يبدأ المعالج لمنح الوصول إلى جهاز.

4. اتبع تعليمات المعالج لمنح الوصول إلى جهاز:

a. تحديد المكون الإضافي **Kaspersky Endpoint Security for Windows**.

b. تحقق من معرف مفتاح الاسترداد. المعرف الذي يوفره المستخدم يجب أن يطابق المعرف المعروض في إعدادات الكمبيوتر.

في حالة عدم تطابق المعرفات، يكون هذا المفتاح غير صالح لاستعادة الوصول إلى محرك النظام المحدد. تأكد من تطابق اسم الكمبيوتر المحدد مع اسم كمبيوتر المستخدم.

c. انقر على **Receive key**.

ونتيجةً لذلك، سوف تحصل على الوصول إلى مفتاح الاسترداد أو ملف مفتاح الاسترداد، والذي ستحتاج إلى نقله إلى المستخدم.

إيقاف حماية BitLocker مؤقتًا لتحديث البرنامج

يوجد عدد من الاعتبارات الخاصة لتحديث نظام التشغيل أو تثبيت حزم التحديث لنظام التشغيل أو تحديث البرامج الأخرى وحماية BitLocker قيد التشغيل. وقد يتطلب تثبيت التحديثات إعادة تشغيل الكمبيوتر عدة مرات. وبعد كل إعادة تشغيل، يجب على المستخدم إكمال مصادقة BitLocker. للتأكد من تثبيت التحديثات بشكل صحيح، يمكنك إيقاف تشغيل مصادقة BitLocker مؤقتًا. وفي هذه الحالة يظل القرص مشفرًا ويمكن للمستخدم الوصول إلى البيانات بعد تسجيل الدخول إلى النظام. ولإدارة مصادقة BitLocker، يمكنك استخدام مهمة إدارة حماية BitLocker. ويمكنك استخدام هذه المهمة لتحديد عدد مرات إعادة تشغيل الكمبيوتر التي لا تتطلب مصادقة BitLocker. وبهذه الطريقة، بعد تثبيت التحديثات و اكتمال مهمة إدارة حماية BitLocker ، يتم تمكين مصادقة BitLocker تلقائيًا. زيمكنك تمكين مصادقة BitLocker في أي وقت.

كيفية إيقاف حماية BitLocker مؤقتًا باستخدام وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى مجلد **خادم الإدارة** ← **المهام** .

   تفتح قائمة المهام.

2. انقر فوق زر **مهمة جديدة**.

   يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (12.1)** ← **إدارة حماية BitLocker**.

الخطوة 2: إدارة حماية BitLocker

كوّن مصادقة BitLocker. لإيقاف حماية BitLocker مؤقتًا، حدد **السماح مؤقتًا بتخطي مصادقة BitLocker** وأدخل عدد مرات إعادة التشغيل بدون مصادقة BitLocker (من 1 إلى 15 مرة). وإذا لزم الأمر، أدخل تاريخ ووقت انتهاء الصلاحية للمهمة. وفي الوقت المحدد، يتم إيقاف المهمة تلقائيًا، ويجب على المستخدم إكمال مصادقة BitLocker عند إعادة تشغيل الكمبيوتر.

الخطوة الثالثة: تحديد الأجهزة التي سيتم تعيين المهمة إليها

حدد أجهزة الكمبيوتر التي سيتم تنفيذ المهمة عليها. الخيارات التالية متاحة:

- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.
- حدد أجهزة الكمبيوتر التي تم اكتشافها بواسطة خادم الإدارة في الشبكة :الأجهزة غير المخصصة. يمكن أن تتضمن الأجهزة المحددة أجهزة خاصة بمجموعة الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- حدد عناوين الأجهزة يدويًا أو قم باستيراد عناوين من القائمة. يمكنك تحديد أسماء NetBIOS وعناوين IP وشبكات IP الفرعية للأجهزة التي تريد تعيين المهمة لها.

الخطوة الرابعة: تحديد اسم المهمة

أدخل اسم المهمة، مثل التحديث إلى Windows 10.

الخطوة 5 إكمال إنشاء المهمة

أغلق المعالج. حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية إيقاف حماية BitLocker مؤقتًا باستخدام Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.

تفتح قائمة المهام.

2. انقر على الزر **Add**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة 1. تكوين إعدادات المهمة العامة

تكوين إعدادات المهمة:

1. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.
2. في القائمة المنسدلة **Task type** حدد **BitLocker protection management**.
3. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، التحديث إلى Windows 10.
4. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

الخطوة 2: إدارة حماية BitLocker

كوّن مصادقة BitLocker. لإيقاف حماية BitLocker مؤقتًا، حدد **Temporarily allow skipping BitLocker authentication** وأدخل عدد مرات إعادة التشغيل بدون مصادقة BitLocker (من 1 إلى 15 مرة). وإذا لزم الأمر، أدخل تاريخ ووقت انتهاء الصلاحية للمهمة. وفي الوقت المحدد، يتم إيقاف المهمة تلقائيًا، ويجب على المستخدم إكمال مصادقة BitLocker عند إعادة تشغيل الكمبيوتر.

الخطوة 3 إكمال إنشاء المهمة

أغلق المعالج. سيتم عرض مهمة جديدة في قائمة المهام.

لتشغيل المهمة، حدد خانة الاختيار المقابلة لها وانقر فوق الزر **Start**.

ونتيجة لذلك، عند تشغيل المهمة، بعد إعادة التشغيل التالية للكمبيوتر، لا يطالب BitLocker المستخدم بالمصادقة. وبعد كل إعادة تشغيل للكمبيوتر بدون مصادقة BitLocker، ينشئ Kaspersky Endpoint Security حدثًا مطابقًا ويسجل عدد عمليات إعادة التشغيل المتبقية. ثم يرسل Kaspersky Endpoint Security الحدث إلى Kaspersky Security Center لتتم مراقبته من قبل المسؤول. ويمكنك أيضًا معرفة عدد عمليات إعادة التشغيل المتبقية في خصائص الكمبيوتر في وحدة تحكم Kaspersky Security Center.

عند الوصول إلى العدد المحدد لعمليات إعادة التشغيل أو وقت انتهاء صلاحية المهمة، يتم تشغيل مصادقة BitLocker تلقائيًا. وللوصول إلى البيانات، يجب على المستخدم إكمال مصادقة BitLocker.

على أجهزة الكمبيوتر التي تعمل بنظام Windows 7، لا يستطيع BitLocker إحصاء عمليات إعادة تشغيل الكمبيوتر. وتتم معالجة إحصاء عمليات إعادة التشغيل على أجهزة الكمبيوتر التي تعمل بنظام Windows 7 بواسطة Kaspersky Endpoint Security. وبالتالي، لتشغيل مصادقة BitLocker تلقائيًا بعد كل إعادة تشغيل، يجب بدء تشغيل Kaspersky Endpoint Security.

لتشغيل مصادقة BitLocker مسبقًا، افتح خصائص مهمة إدارة حماية BitLocker وحدد **طلب المصادقة في كل مرة قبل التمهيد**.

التشفير على مستوى الملف على محركات الأقراص الثابتة المحلية

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل. لا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم.

يحتوي تشفير الملف على الميزات الخاصة التالية:

- يقوم Kaspersky Endpoint Security بتشفير / فك تشفير الملفات في المجلدات المحددة مسبقًا فقط لملفات بيانات المستخدمين المحليين لنظام التشغيل. لا يقوم Kaspersky Endpoint Security بتشفير/فك تشفير الملفات في المجلدات المحددة مسبقًا لملفات بيانات مستخدمي التجوال وملفات بيانات المستخدم الإلزامي وملفات بيانات المستخدمين المؤقتين والمجلدات المعاد توجيهها.
- لا يشفر Kaspersky Endpoint Security الملفات التي قد يتسبب تعديلها في الإضرار بنظام التشغيل والتطبيقات المثبتة. على سبيل المثال، توجد الملفات والمجلدات التالية ذات المجلدات المتداخلة في قسم استثناءات التشفير:
  - %WINDIR%؛
  - %PROGRAMFILES% وكذلك %PROGRAMFILES(X86)%؛
  - ملفات تسجيل Windows.

لا يمكن عرض قائمة استثناءات التشفير أو تحريرها. على الرغم من إمكانية إضافة الملفات والمجلدات الموجودة في قائمة استثناءات التشفير إلى قائمة التشفير، فإنه لن يتم تشفيرها أثناء تشفير الملفات.

تشفير الملفات على محركات أقراص الكمبيوتر المحلية

لا يشفر Kaspersky Endpoint Security الملفات الموجودة في التخزين السحابي في OneDrive أو في مجلدات أخرى يكون اسمها OneDrive. ويحظر Kaspersky Endpoint Security أيضًا نسخ الملفات المشفرة إلى مجلدات OneDrive إذا لم تتم إضافة هذه الملفات إلى قاعدة فك التشفير.

لتشفير الملفات على محركات الأقراص المحلية:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Data Encryption ← File Level Encryption**.
5. في القائمة المنسدلة **وضع التشفير** حدد **وفقًا للقواعد**.
6. في علامة التبويب **التشفير**، انقر فوق الزر **إضافة**، وحدد أحد العناصر التالية في القائمة المنسدلة:

a. حدد العنصر **المجلدات المحددة مسبقًا** لإضافة ملفات من المجلدات الخاصة بملفات تعريف المستخدمين المحلية المقترحة بواسطة خبراء Kaspersky إلى قاعدة التشفير.

- **المستندات**. الملفات في مجلد المستندات القياسي لنظام التشغيل والمجلدات الفرعية به.
- **المفضلات**. الملفات في مجلد المفضلة القياسي لنظام التشغيل والمجلدات الفرعية به.
- **سطح المكتب**. الملفات في مجلد سطح المكتب القياسي لنظام التشغيل والمجلدات الفرعية به.
- **ملفات مؤقتة**. الملفات المؤقتة المتعلقة بعمل التطبيقات المثبتة على الكمبيوتر. على سبيل المثال: تطبيقات Microsoft Office تنشئ ملفات مؤقتة تحتوي على نسخ احتياطية من المستندات.

لا يوصى بتشفير الملفات المؤقتة، لأن ذلك قد يؤدي إلى فقدان البيانات. على سبيل المثال، ينشئ Microsoft Word ملفات مؤقتة عند معالجة مستند. وفي حالة تشفير الملفات المؤقتة، لكن لم يتم تشفير الملف الأصلي، فقد يتلقى المستخدم خطأ تم رفض الوصول عند محاولة حفظ المستند. بالإضافة إلى ذلك، قد يحفظ Microsoft Word الملف، لكن لن يكون من الممكن فتح المستند في المرة القادمة، أي ستفقد البيانات.

- **ملفات Outlook**. الملفات المتعلقة بعمل عميل بريد Outlook: ملفات البيانات (PST)، وملفات بيانات عدم الاتصال (OST)، وملفات دفتر العناوين غير المتصل (OAB)، وملفات دفتر العناوين الشخصي (PAB).

b. حدد العنصر **مجلد مخصص** لإضافة مسار مجلد تم إدخاله يدويًا إلى قاعدة التشفير.

عند إضافة مسار مجلد، التزم بالقواعد التالية:

- استخدم متغير بيئة (على سبيل المثال: `%FOLDER%\UserFolder`). يمكنك استخدام متغير بيئة مرة واحدة وفقط في بداية المسار.
- لا تستخدم المسارات النسبية.
- لا تستخدم الحروف `*` أو `?`.
- لا تستخدم مسارات UNC.
- ستخدم `;` أو `,` كحرف فاصل.

c. حدد العنصر **الملفات حسب الملحق** لإضافة ملحقات ملف واحد إلى قاعدة تشفير. يقوم Kaspersky Endpoint Security بتشفير الملفات باستخدام الملحقات المحددة على جميع محركات أقراص الكمبيوتر المحلية.

d. حدد العنصر **الملفات حسب مجموعات الملحقات** لإضافة مجموعات ملحقات الملفات إلى قاعدة تشفير (على سبيل المثال Microsoft Office documents). يقوم Kaspersky Endpoint Security بتشفير الملفات ذات الامتدادات المدرجة في مجموعات الامتدادات على كل محركات الأقراص المحلية للكمبيوتر.

7. احفظ تغييراتك.

بمجرد تطبيق السياسة، يقوم Kaspersky Endpoint Security بتشفير الملفات المضمنة في قاعدة التشفير وغير المضمنة في قاعدة فك التشفير.

يحتوي تشفير الملف على الميزات الخاصة التالية:

- في حال إضافة الملف نفسه إلى كلٍ من قاعدة تشفير وقاعدة فك تشفير، فإن Kaspersky Endpoint Security سيتخذ الإجراءات التالية:
  - إذا كان الملف غير مشفرٍ، فإن Kaspersky Endpoint Security لا يشفر هذا الملف.
  - أما إذا كان الملف مشفرًا، فإن Kaspersky Endpoint Security يفك تشفير هذا الملف.
- يستمر Kaspersky Endpoint Security في تشفير الملفات الجديدة إذا كانت توافق معايير قاعدة التشفير. على سبيل المثال: عندما تغير خصائص ملف غير مشفر (مساره أو امتداده) فإن الملف يفي بمعايير قاعدة التشفير. عندها يشفر Kaspersky Endpoint Security هذا الملف.
- عندما يقوم المستخدم بإنشاء ملف جديد تتطابق خصائصه مع معايير قاعدة التشفير، يقوم Kaspersky Endpoint Security بتشفير الملف بمجرد فتحه.
- يقوم Kaspersky Endpoint Security بتأجيل تشفير الملفات المفتوحة حتى يتم غلقها.
- إذا قمت بنقل ملف مشفر إلى مجلد آخر على محرك القرص المحلي، فيظل الملف مشفرًا بغض النظر عما إذا كان هذا المجلد في قاعدة التشفير أم لا.
- إذا قمت بفك تشفير ملف ونسخه إلى مجلد محلي آخر غير مدرج في قاعدة التشفير، فيمكن تشفير هذه النسخة. ولمنع تشفير الملف المنسوخ، قم بإنشاء قاعدة فك تشفير للمجلد الهدف.

تشكيل قواعد الوصول إلى الملفات المشفرة للتطبيقات

لتشكيل قواعد الوصول إلى الملفات المشفرة للتطبيقات:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **Data Encryption ← File Level Encryption**.

5. في القائمة المنسدلة **وضع التشفير** حدد **وفقًا للقواعد**.

يتم تطبيق قواعد الوصول فقط في وضع **وفقًا للقواعد**. بعد تطبيق قواعد الوصول في وضع **وفقًا للقواعد**، إذا قمت بالتحويل إلى وضع **عدم التغيير**، فسيتجاهل Kaspersky Endpoint Security كل قواعد الوصول. وسيكون لكل التطبيقات حق الوصول إلى كل الملفات المشفرة.

6. في الجزء الأيسر من النافذة، حدد علامة التبويب **قواعد التطبيقات**.

7. إذا كنت تريد تحديد التطبيقات من قائمة Kaspersky Security Center بشكل حصري، انقر فوق الزر **إضافة** وحدد العنصر **تطبيقات من قائمة Kaspersky Security Center** في القائمة المنسدلة.

a. حدد عوامل التصفية لتضييق قائمة التطبيقات في الجدول. ولفعل ذلك، حدد قيم المعلمات **التطبيق** و**البائع** و**الفترة المضافة**، وكل خانات الاختيار في القسم **المجموعة**.

b. انقر على **تحديث**.

c. يدرج الجدول التطبيقات التي تطابق مع عوامل التصفية المطبقة.

d. في العمود **التطبيق** حدد خانات الاختيار المقابلة للتطبيقات التي تريد تشكيل قواعد الوصول إلى الملف المشفر لها.

e. في القائمة المنسدلة **قاعدة التطبيقات**، حدد القاعدة التي سوف تحدد وصول التطبيقات إلى الملفات المشفرة.

f. في القائمة المنسدلة **إجراءات التطبيقات التي تم تحديدها مسبقًا** حدد الإجراء الذي سيتم اتخاذه بواسطة Kaspersky Endpoint Security على قواعد الوصول إلى الملف المشفر والتي تم تشكيلها مسبقًا لهذه التطبيقات.

تظهر تفاصيل قاعدة الوصول إلى ملف مشفر للتطبيقات في الجدول الموجود في علامة التبويب **قواعد التطبيقات**.

8. إذا كنت تريد تحديد تطبيقات يدويًا، فانقر فوق الزر **إضافة**، وحدد العنصر **التطبيقات المخصصة** في القائمة المنسدلة.

a. في حقل الإدخال، اكتب اسم أو قائمة أسماء الملفات القابلة للتنفيذ الخاصة بالتطبيقات بما في ذلك ملحقاتها.

لإضافة أسماء الملفات التنفيذية الخاصة بالتطبيقات من قائمة Kaspersky Security Center، انقر فوق الزر **إضافة من قائمة Kaspersky Security Center**.

b. إذا لزم الأمر، في الحقل **الوصف** أدخل وصفًا لقائمة التطبيقات.

c. في القائمة المنسدلة **قاعدة التطبيقات**، حدد القاعدة التي سوف تحدد وصول التطبيقات إلى الملفات المشفرة.

تظهر تفاصيل قاعدة الوصول إلى ملف مشفر للتطبيقات في الجدول الموجود في علامة التبويب **قواعد التطبيقات**.

9. احفظ تغييراتك.

تشفير الملفات التي تم إنشاؤها أو تعديلها بواسطة تطبيقات محددة

يمكنك إنشاء قاعدة يقوم بموجبها Kaspersky Endpoint Security بتشفير جميع الملفات التي تم إنشاؤها أو تعديلها بواسطة التطبيقات المحددة في القاعدة.

ولن يتم تشفير الملفات التي كان قد تم إنشاؤها أو تعديلها بواسطة التطبيقات المحددة قبل أن يتم تطبيق قاعدة التشفير.

لتكوين تشفير الملفات التي تم إنشاؤها أو تعديلها بواسطة تطبيقات محددة:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.
5. في القائمة المنسدلة **وضع التشفير** حدد **وفقًا للقواعد**.

يتم تطبيق قواعد التشفير في وضع **وفقًا للقواعد** فقط. بعد تطبيق قواعد التشفير في وضع **وفقًا للقواعد**، إذا قمت بالتبديل إلى الوضع **عدم التغيير**، فسيتجاهل Kaspersky Endpoint Security كل قواعد التشفير. وستظل الملفات التي تم تشفيرها مسبقًا مشفرة.

6. في الجزء الأيسر من النافذة، حدد علامة التبويب **قواعد التطبيقات**.
7. إذا كنت تريد تحديد التطبيقات من قائمة Kaspersky Security Center بشكل حصري، انقر فوق الزر **إضافة** وحدد العنصر **تطبيقات من قائمة Kaspersky Security Center** في القائمة المنسدلة.
   a. حدد عوامل التصفية لتضييق قائمة التطبيقات في الجدول. ولفعل ذلك، حدد قيم المعلمات **التطبيق** و**البائع** و**الفترة المضافة**، وكل خانات الاختيار في القسم **المجموعة**.
   b. انقر على **تحديث**.
   يدرج الجدول التطبيقات التي تطابق مع عوامل التصفية المطبقة.
   c. في العمود **التطبيق**، حدد خانات الاختيار بجوار التطبيقات التي تريد تشفير الملفات التي تم إنشاؤها بواسطتها.
   d. في القائمة المنسدلة **قاعدة التطبيقات** حدد **تشفير جميع الملفات التي تم إنشاؤها**.
   e. في القائمة المنسدلة **إجراءات التطبيقات التي تم تحديدها مسبقًا** حدد الإجراء الذي سيتم اتخاذه بواسطة Kaspersky Endpoint Security على قواعد تشفير الملفات والتي تم تشكيلها للتطبيقات المذكورة مسبقًا.

   تظهر المعلومات حول قواعد تشفير الملفات التي تم إنشاؤها أو تعديلها بواسطة التطبيقات المحددة في الجدول في علامة التبويب **قواعد التطبيقات**.
8. إذا كنت تريد تحديد تطبيقات يدويًا، فانقر فوق الزر **إضافة**، وحدد العنصر **التطبيقات المخصصة** في القائمة المنسدلة.
   a. في حقل الإدخال، اكتب اسم أو قائمة أسماء الملفات القابلة للتنفيذ الخاصة بالتطبيقات بما في ذلك ملحقاتها.
   لإضافة أسماء الملفات التنفيذية الخاصة بالتطبيقات من قائمة Kaspersky Security Center، انقر فوق الزر **إضافة من قائمة Kaspersky Security Center**.
   b. إذا لزم الأمر، في الحقل **الوصف** أدخل وصفًا لقائمة التطبيقات.
   c. في القائمة المنسدلة **قاعدة التطبيقات** حدد **تشفير جميع الملفات التي تم إنشاؤها**.

تظهر المعلومات حول قواعد تشفير الملفات التي تم إنشاؤها أو تعديلها بواسطة التطبيقات المحددة في الجدول في علامة التبويب **قواعد التطبيقات**.

9. احفظ تغييراتك.

إنشاء قاعدة فك تشفير

لإنشاء قاعدة فك تشفير:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.
5. في القائمة المنسدلة **وضع التشفير** حدد **وفقًا للقواعد**.
6. في علامة التبويب **فك التشفير**، انقر فوق الزر **إضافة**، وحدد أحد العناصر التالية في القائمة المنسدلة:
   a. حدد العنصر **المجلدات المحددة مسبقًا** لإضافة ملفات من المجلدات الخاصة بملفات تعريف المستخدمين المحليين المقترحة بواسطة خبراء Kaspersky إلى قاعدة فك التشفير.
   b. حدد العنصر **مجلد مخصص** لإضافة مسار مجلد تم إدخاله يدويًا إلى قاعدة فك التشفير.
   c. حدد العنصر **الملفات حسب الملحق** لإضافة ملحقات ملف واحد إلى قاعدة فك التشفير. لا يقوم Kaspersky Endpoint Security بتشفير الملفات باستخدام الملحقات المحددة على جميع محركات الأقراص المحلية.
   d. حدد العنصر **الملفات حسب مجموعات الملحقات** لإضافة مجموعات ملحقات الملفات إلى قاعدة فك تشفير (على سبيل المثال Microsoft Office documents). لا يقوم Kaspersky Endpoint Security بتشفير الملفات ذات الامتدادات المدرجة في مجموعات الامتدادات على كل محركات الأقراص المحلية للكمبيوتر.
7. احفظ تغييراتك.

إذا تمت إضافة نفس الملف إلى قاعدة التشفير وقاعدة فك التشفير، لا يقوم Kaspersky Endpoint Security بتشفير هذا الملف في حالة عدم تشفيره ويقوم بفك تشفير الملف إذا تم تشفيره.

فك تشفير الملفات على محركات أقراص الكمبيوتر المحلية

لفك تشفير الملفات الموجودة على محركات الأقراص المحلية:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.

5. في الجزء الأيسر من النافذة، حدد علامة التبويب **التشفير**.

6. قم بإزالة الملفات والمجلدات التي تريد فك تشفيرها من قائمة التشفير. للقيام بذلك، حدد الملفات وحدد العنصر **حذف القاعدة وفك تشفير الملفات** في قائمة السياق للزر **إزالة**.

تتم إضافة الملفات والمجلدات التي تمت إزالتها من قائمة التشفير تلقائيًا إلى قائمة فك التشفير.

7. تشكيل قائمة فك تشفير الملفات.

8. احفظ تغييراتك.

بمجرد تطبيق السياسة، يقوم Kaspersky Endpoint Security بفك تشفير الملفات المشفرة التي تمت إضافتها إلى قائمة فك التشفير.

يقوم Kaspersky Endpoint Security بفك تشفير الملفات غير المشفرة إذا تم تغيير المعلمات الخاصة بها (مسار الملف / اسم الملف / ملحق الملف) لتطابق معلمات الكائنات التي تمت إضافتها إلى قائمة فك التشفير.

يقوم Kaspersky Endpoint Security بتأجيل فك تشفير الملفات المفتوحة حتى يتم غلقها.

إنشاء حزم مشفرة

يمكنك استخدام الحزم المشفرة عند إرسال ملفات إلى مستخدمين خارج شبكة الشركة من أجل حماية بياناتك. يمكن أن تكون الحزم المشفرة ملائمة لنقل ملفات كبيرة الحجم على محركات أقراص قابلة للإزالة بما أن خدمات البريد الإلكتروني تضع قيودًا على أحجام الملفات.

قبل إنشاء حزم مشفرة، سوف يطلب Kaspersky Endpoint Security من المستخدم إدخال كلمة المرور. لحماية بياناتك بشكل موثوق، يمكنك تفعيل التحقق من قوة كلمة المرور وتحديد متطلبات قوة كلمة المرور. هذا سوف يمنع المستخدمين من استخدام كلمات مرور بسيطة وقصيرة، مثل 1234.

كيفية تفعيل التحقق من قوة كلمة المرور عند إنشاء أجهزة مشفرة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **تشفير البيانات** ← **إعدادات التشفير العامة**.

5. في القسم **إعدادات كلمة المرور**، انقر على الزر **الإعدادات**.

6. في النافذة التي تفتح، حدد القسم **الحزم المشفرة**.

7. إعدادات تكوين كلمة المرور عند إنشاء حزم مشفرة.

كيفية تفعيل التحقق من قوة كلمة المرور عند إنشاء أجهزة مشفرة في وحدة تحكم الويب

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Data Encryption** ← **File Level Encryption**.

5. في القسم **Encrypted package password settings**، كوّن معايير قوة كلمة المرور المطلوبة عند إنشاء حزم مشفرة.

يمكنك إنشاء حزم مشفرة على أجهزة الكمبيوتر المثبت عليها Kaspersky Endpoint Security مع تفعيل التشفير على مستوى الملف.

عند إضافة ملف ما إلى الحزمة المشفرة التي تتواجد محتوياتها في التخزين السحابي لـ OneDrive، يقوم Kaspersky Endpoint Security بتنزيل محتويات الملف وإجراء عملية التشفير.

لإنشاء حزمة مشفرة:

1. في أي مدير ملفات، اختر الملفات أو المجلدات التي ترغب في إضافتها إلى الحزمة المشفر. انقر بزر الماوس الأيمن لفتح القائمة السياقية الخاصة بها.

2. في القائمة السياقية، حدد **حزم جديدة مشفرة** (انظر الشكل أدناه).

إنشاء حزمة مشفرة

3. في النافذة التي تفتح، حدد كلمة المرور وقم بالتأكيد عليها.
يجب أن تفي كلمة المرور بمعايير التعقيد المحددة في السياسة.

4. انقر على **إنشاء**.

تبدأ عملية إنشاء حزمة مشفرة. لا يقوم Kaspersky Endpoint Security بضغط الملف عند إنشاء حزمة مشفرة. عند انتهاء العملية، يتم إنشاء حزمة مشفرة محمية بكلمة مرور ذاتية الاستخراج (ملف تنفيذي بامتداد .exe –) في المجلد الواجهة المحدد.

للوصول إلى الملفات في الحزمة المشفرة، انقر مرتين عليها لبدء معالج فك الحزمة ثم أدخل كلمة المرور. إذا نسيت كلمة المرور أو فقدتها، فلا يمكن استرداد الملفات الموجودة في الحزمة المشفرة أو الوصول إليها. يمكنك إعادة إنشاء الحزمة المشفرة.

طلب الوصول إلى الملفات المشفرة

عند تشفير الملفات، فإن Kaspersky Endpoint Security يستقبل مفتاح تشفير مطلوب للوصول إلى الملفات المشفرة مباشرةً. باستخدام مفتاح التشفير هذا، يمكن لمستخدم يعمل تحت أي حساب مستخدم Windows تم تفعيله أثناء تشفير الملف الوصول مباشرةً إلى الملفات المشفرة. ينبغي على المستخدمين الذي يعملون تحت حسابات Windows غير النشطة أثناء تشفير الملفات الاتصال بمركز Kaspersky Security Center من أجل الوصول إلى الملفات المشفرة.

قد يتعذّر الوصول إلى الملفات المشفرة في الظروف التالية:

- قيام كمبيوتر المستخدم بتخزين مفاتيح التشفير، لكن لا يوجد اتصال مع Kaspersky Security Center لإدارتها. في هذه الحالة، يجب على المستخدم طلب الوصول إلى الملفات المشفرة من مسؤول الشبكة المحلية.

  في حالة تعذّر الوصول إلى Kaspersky Security Center، فيجب عليك القيام بما يلي:

  - طلب مفتاح وصول للوصول إلى الملفات المشفرة على محركات الأقراص الصلبة للكمبيوتر؛
  - للوصول إلى الملفات المشفرة المخزنة على محركات الأقراص القابلة للإزالة، اطلب مفاتيح وصول منفصلة للملفات المشفرة على كل محرك أقراص قابل للإزالة.

- يتم حذف مكونات التشفير من كمبيوتر المستخدم. وفي هذه الحالة، قد يقوم المستخدم بفتح الملفات المشفرة على أقراص محلية وأقراص قابلة للإزالة لكن سوف تظهر محتويات هذه الملفات مشفرة.

  قد يتم استخدام الملفات المشفرة من قِبل المستخدم في ظل الظروف التالية:

  - وضع الملفات داخل الحزم المشفرة التي تم إنشاؤها على كمبيوتر مثبت عليه Kaspersky Endpoint Security.
  - تخزين الملفات على محرك أقراص قابل للإزالة يسمح بـ الوضع المحمول عليه.

للتمتع بالوصول إلى الملفات المشفرة، يحتاج المستخدم إلى بدء إجراء الاسترداد (طلب-رد).

الحصول على الوصول إلى الملفات المشفرة يتضمن الخطوات التالية:

1. إرسال المستخدم لملف طلب الوصول إلى المسؤول (راجع الشكل أدناه).
2. يضيف المسؤول ملف الوصول إلى الطلب إلى Kaspersky Security Center ثم ينشئ ملف مفتاح وصول ويرسل الملف إلى المستخدم.
3. يضيف المستخدم ملف مفتاح الوصول إلى Kaspersky Endpoint Security ويتمتع بالوصول إلى الملفات.

طلب الوصول إلى الملفات المشفرة

لبدء إجراء الاسترداد، فإن المستخدم يحتاج إلى محاولة الوصول إلى ملف. ونتيجة لذلك، سيقوم Kaspersky Endpoint Security بإنشاء ملف وصول طلب (ملف بامتداد KESDC)، والذي يحتاج المستخدم إلى إرساله إلى المسؤول (عبر البريد الإلكتروني على سبيل المثال).

ينشئ Kaspersky Endpoint Security ملف طلب وصول للوصول إلى كل الملفات المشفرة المخزنة على محرك أقراص الكمبيوتر (محرك الأقراص المحلي أو محرك الأقراص القابل للإزالة).

كيفية الحصول على ملف مفتاح الوصول إلى البيانات المشفرة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Devices**.

3. في علامة التبويب **الأجهزة**، حدد اسم الكمبيوتر الخاص بالمستخدم الذي يطالب بالوصول إلى الملفات المشفرة وانقر بزر الماوس الأيمن لفتح القائمة السياقية.

4. في قائمة السياق، حدد **منح إمكانية الوصول في وضع عدم الاتصال**.

5. في النافذة التي تفتح، حدد القسم **تشفير البيانات**.

6. في علامة التبويب **تشفير البيانات**، انقر فوق الزر **استعراض**.

7. في نافذة تحديد ملف وصول طلب، حدد المسار للملف المستلم من المستخدم.

سترى معلومات حول طلب المستخدم. يقوم Kaspersky Security Center بإنشاء ملف مفتاح. أرسل ملف مفتاح الوصول إلى البيانات المشفرة الذي تم إنشاؤه إلى المستخدم بالبريد الإلكتروني. أو احفظ ملف الوصول واستخدم أي طريقة متاحة لنقل الملف.

منح إمكانية الوصول في وضع عدم الاتصال

[كيفية الحصول على ملف مفتاح الوصول إلى البيانات المشفرة في Web Console]

1. في النافذة الرئيسية لـ Web Console، حدد **Managed devices** ← **Devices**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى بياناته.

3. انقر على الزر **Grant access to the device in offline mode**.

4. حدد **Data Encryption**.

5. انقر فوق الزر **Select file** وحدد ملف وصول الطلب الذي تلقيته من المستخدم (ملف بامتداد KESDC).
سيعرض مكون Web Console معلومات حول الطلب. وسيشمل هذا اسم الكمبيوتر الذي يطلب المستخدم الوصول إلى الملف عليه.

6. انقر على الزر **Save key** وحدد مجلدًا لحفظ ملف مفتاح الوصول إلى البيانات المشفرة (ملف بامتداد KESDR).

ونتيجة لذلك، ستتمكن من الحصول على مفتاح الوصول إلى البيانات المشفرة، والذي ستحتاج إلى نقله إلى المستخدم.

بعد استلام مفتاح الوصول إلى الملفات المشفرة، فإن المستخدم يحتاج إلى تشغيل الملف بالنقر المزدوج عليه. ونتيجةً لهذا، فإن Kaspersky Endpoint Security سوف يمنح الوصول إلى جميع الملفات المشفرة المخزنة على محرك الأقراص. للوصول إلى الملفات المشفرة المخزنة على محركات أقراص أخرى، يجب عليك الحصول على ملف مفتاح وصول منفصل لكل محرك أقراص.

استعادة الوصول إلى البيانات المشفرة بعد فشل نظام التشغيل

يمكنك استعادة الوصول إلى البيانات بعد فشل نظام التشغيل فقط للتشفير على مستوى الملف (FLE). لا يمكنك استعادة الوصول إلى البيانات إذا تم استخدام تشفير القرص بالكامل (FDE).

استعادة الوصول إلى البيانات المشفرة بعد فشل نظام التشغيل:

1. قم بإعادة تثبيت نظام التشغيل بدون تهيئة محرك الأقراص الصلبة.

2. تثبيت Kaspersky Endpoint Security.

3. تأسيس اتصال بين الكمبيوتر وخادم إدارة Kaspersky Security Center الذي تحكم في الكمبيوتر عندما تم تشفير البيانات.

سيتم منح الوصول إلى البيانات المشفرة في نفس الحالات المطبقة قبل فشل نظام التشغيل.

تحرير قوالب رسائل الوصول إلى الملفات المشفرة

لتحرير قوالب رسائل الوصول إلى الملفات المشفرة:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **تشفير البيانات** ← **إعدادات التشفير العامة**.

5. في القسم **القوالب**، انقر على الزر **القوالب**.

6. في النافذة التي تفتح، افعل ما يلي:

- إذا كنت تريد تحرير قالب رسالة المستخدم، فحدد علامة التبويب **رسالة المستخدم**. تفتح النافذة التالية عند محاولة المستخدم الوصول إلى ملف مشفر أثناء عدم وجود مفتاح متوفر على الكمبيوتر للوصول إلى الملفات المشفرة. يؤدي النقر فوق الزر **إرسال عن طريق البريد الإلكتروني** إلى إنشاء رسالة مستخدم تلقائيًا. يتم إرسال هذه الرسالة إلى مسؤول الشبكة المحلية للشركة إلى جانب ملف طلب الوصول إلى الملفات المشفرة.

- إذا كنت تريد تحرير قالب رسالة المسؤول، فحدد علامة التبويب **رسالة المسؤول**. ويتلقى المستخدم هذه الرسالة بعد منح الوصول إلى الملفات المشفرة.

7. قم بتحرير قوالب الرسالة.

8. احفظ تغييراتك.

طلب الوصول إلى الملفات المشفرة

تشفير محركات الأقراص القابلة للإزالة

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل. لا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم.

يدعم Kaspersky Endpoint Security تشفير الملفات في أنظمة ملفات FAT32 وNTFS. في حالة توصيل محرك أقراص قابل للإزالة مزود بنظام ملفات غير مدعوم بجهاز الكمبيوتر، تنتهي مهمة التشفير الخاصة بمحرك الأقراص القابل للإزالة هذا بالخطأ ويقوم Kaspersky Endpoint Security بتعيين الحالة للقراءة فقط إلى محرك الأقراص القابل للإزالة.

لحماية البيانات الموجودة على محركات الأقراص القابلة للإزالة، يمكنك استخدام أنواع التشفير التالية:

- تشفير القرص بالكامل (FDE).

  تشفير محرك الأقراص القابل للإزالة بالكامل، بما في ذلك نظام الملفات.

  لا يمكن الوصول إلى البيانات المشفرة خارج شبكة الشركة. من المستحيل أيضًا الوصول إلى البيانات المشفرة داخل شبكة الشركة إذا لم يكن الكمبيوتر متصلاً بـ Kaspersky Security Center (مثل على كمبيوتر "الضيف").

- التشفير على مستوى الملف (FLE).

تشفير الملفات الموجودة على محرك الأقراص القابل للإزالة فقط. نظام الملفات يبقى دون تغيير.

تشفير الملفات الموجودة على محركات الأقراص القابلة للإزالة يوفر القدرة على الوصول إلى البيانات خارج شبكة الشركة باستخدام وضع خاص يسمى الوضع المحمول .

أثناء التشفير، يقوم Kaspersky Endpoint Security بإنشاء مفتاح رئيسي. يحفظ Kaspersky Endpoint Security المفتاح الرئيسي في المستودعات التالية:

- Kaspersky Security Center.
- كمبيوتر المستخدم.

  يتم تشفير المفتاح الرئيسي باستخدام المفتاح السري للمستخدم.
- محرك أقراص قابل للإزالة.

  يتم تشفير المفتاح الرئيسي بالمفتاح العام لـ Kaspersky Security Center.

بعد اكتمال التشفير، يمكن الوصول إلى البيانات الموجودة على محرك الأقراص القابل للإزالة داخل شبكة الشركة كما لو كانت على محرك أقراص قابل للإزالة من النوع التقليدي بدون تشفير.

الوصول إلى البيانات المشفرة

عند توصيل محرك أقراص قابل للإزالة مع بيانات مشفرة، يقوم Kaspersky Endpoint Security باتخاذ الإجراءات التالية:

1. التحقق من وجود مفتاح رئيسي في التخزين المحلي على كمبيوتر المستخدم.

   إذا تم العثور على المفتاح الرئيسي، يحصل المستخدم على حق الوصول إلى البيانات الموجودة على محرك الأقراص القابل للإزالة.

   إذا لم يتم العثور على المفتاح الرئيسي، يقوم Kaspersky Endpoint Security بتنفيذ الإجراءات التالية:

   a. يرسل طلبًا إلى Kaspersky Security Center.

      بعد استلام الطلب، يرسل Kaspersky Security Center ردًا يحتوي على المفتاح الرئيسي.

   b. يحفظ Kaspersky Endpoint Security المفتاح الرئيسي في التخزين المحلي على كمبيوتر المستخدم للعمليات اللاحقة باستخدام محرك الأقراص القابل للإزالة المشفر.

2. يفك تشفير البيانات.

ميزات خاصة لتشفير محرك الأقراص القابل للإزالة

تشفير محركات الأقراص القابلة للإزالة له المزايا الخاصة التالية:

- يتم تشكيل السياسة المزودة بالإعدادات المعدة مسبقًا لتشفير محرك الأقراص القابل للإزالة لمجموعة محددة من أجهزة الكمبيوتر المدارة. لذلك، فإن نتيجة تطبيق سياسة Kaspersky Security Center المكونة لتشفير / فك تشفير الأقراص القابلة للإزالة تعتمد على الكمبيوتر الذي يتم توصيل محرك الأقراص القابلة للإزالة به.
- لا يقوم Kaspersky Endpoint Security بتشفير/فك تشفير ملفات القراءة فقط والمخزنة على محركات الأقراص القابلة للإزالة.
- يتم دعم أنواع الأجهزة التالية كمحركات أقراص قابلة للإزالة:
  - وسائط البيانات المتصلة عبر ناقل USB
  - محركات الأقراص الصلبة المتصلة عبر نواقل USB وFireWire

- محركات أقراص SSD المتصلة عبر نواقل USB وFireWire

بدء تشفير محركات الأقراص القابلة للإزالة

يمكنك استخدام سياسة لفك تشفير محرك أقراص قابل للإزالة. يتم إنشاء سياسة ذات إعدادات محددة لتشفير محرك الأقراص القابل للإزالة لمجموعة إدارة محددة. لذلك، تعتمد نتيجة فك تشفير البيانات على محركات الأقراص القابلة للإزالة على الكمبيوتر المتصل به محرك القرص القابل للإزالة.

يدعم Kaspersky Endpoint Security تشفير ملفات النظام FAT32 وNTFS. في حالة توصيل محرك أقراص قابل للإزالة مزود بنظام ملفات غير مدعوم بجهاز الكمبيوتر، ينتهي تشفير محرك الأقراص القابل للإزالة هذا بالخطأ ويقوم برنامج Kaspersky Endpoint Security بتعيين الوصول للقراءة فقط لمحرك الأقراص القابل للإزالة.

قبل تشفير الملفات على محرك أقراص قابل للإزالة، تأكد من تهيئته وعدم وجود أقسام مخفية (مثل قسم نظام EFI). وإذا كان محرك الأقراص يحتوي على أقسام غير مهيأة أو مخفية، فقد يفشل تشفير الملف مع حدوث خطأ.

لتشفير محركات الأقراص القابلة للإزالة:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.
5. في القائمة المنسدلة **وضع التشفير**، حدد الإجراء الافتراضي الذي تريد أن يتم إجراؤه بواسطة برنامج Kaspersky Endpoint Security على محركات الأقراص القابلة للإزالة:
   - **تشفير محرك الأقراص القابل للإزالة بالكامل** (FDE). يقوم برنامج Kaspersky Endpoint Security بتشفير محتويات قطاع محرك الأقراص القابل للإزالة حسب القطاع. كنتيجة لذلك، لا يقوم التطبيق بتشفير الملفات التي تم تخزينها على محرك الأقراص القابل للإزالة فحسب، بل أيضًا أنظمة الملفات الخاصة به، بما في ذلك أسماء الملفات وهياكل المجلدات الموجودة على محرك الأقراص القابل للإزالة.
   - **تشفير جميع الملفات** (FLE). يقوم برنامج Kaspersky Endpoint Security بتشفير جميع الملفات التي تم تخزينها على محرك الأقراص القابل للإزالة. لا يقوم التطبيق بتشفير أنظمة ملفات محركات الأقراص القابلة للإزالة، بما في ذلك أسماء الملفات المشفرة وهياكل المجلدات.
   - **تشفير الملفات الجديدة فقط** (FLE). لا يقوم برنامج Kaspersky Endpoint Security إلا بتشفير الملفات التي تمت إضافتها إلى محركات الأقراص القابلة للإزالة أو التي تم تخزينها على محركات أقراص القابلة للإزالة و التي تم تعديلها بعد تطبيق سياسة Kaspersky Security Center آخر مرة.

لا يقوم برنامج Kaspersky Endpoint Security بتشفير محرك الأقراص القابل للإزالة الذي تم تشفيره بالفعل.

6. إذا كنت تريد استخدام الوضع المحمول لتشفير محركات الأقراص القابلة للإزالة، حدد خانة الاختيار **الوضع المحمول**.

الوضع المحمول هو وضع لتشفير الملفات (FLE) على محركات الأقراص القابلة للإزالة يوفر القدرة على الوصول إلى البيانات خارج شبكة الشركة. الوضع المحمول يوفر لك كذلك القدرة على العمل مع البيانات المشفرة على أجهزة الكمبيوتر غير المثبت عليها Kaspersky Endpoint Security.

7. إذا أردت تشفير محرك أقراص قابل للإزالة جديد، يُوصى بتحديد خانة الاختيار **تشفير مساحة القرص المستخدمة فقط**. إذا تم إلغاء تحديد خانة الاختيار، فسيقوم برنامج Kaspersky Endpoint Security بتشفير جميع الملفات، بما في ذلك القطاعات المتبقية من الملفات التي تم حذفها أو تعديلها.
8. إذا كنت تريد تكوين تشفير لمحركات الأقراص الفردية القابلة للإزالة، قم بتحديد قواعد التشفير.

9. إذا كنت تريد استخدام تشفير محركات الأقراص بالكامل لمحركات الأقراص القابلة للإزالة في وضع عدم الاتصال، حدد خانة الاختيار **السماح بتشفير محركات الأقراص القابلة للإزالة في وضع عدم الاتصال**.

وضع التشفير غير متصل يشير إلى تشفير محركات الأقراص القابلة للإزالة (FDE) أثناء عدم وجود اتصال بـ Kaspersky Security Center. أثناء عملية التشفير، يحفظ برنامج Kaspersky Endpoint Security المفتاح الأساسي على كمبيوتر المستخدم فقط. سيرسل برنامج Kaspersky Endpoint Security المفتاح الأساسي إلى Kaspersky Security Center أثناء إجراء المزامنة التالية.

في حالة تلف جهاز الكمبيوتر الذي تم حفظ المفتاح الأساسي فيه ولم يتم إرسال البيانات إلى Kaspersky Security Center، لا يمكن الحصول على حق الوصول إلى محرك الأقراص القابل للإزالة.

في حالة إلغاء تحديد خانة الاختيار **السماح بتشفير محركات الأقراص القابلة للإزالة في وضع عدم الاتصال** ولا يوجد اتصال بـ Kaspersky Security Center، فلا يمكن تشفير محرك الأقراص القابل للإزالة.

10. احفظ تغييراتك.

بعد تطبيق السياسة، عندما يقوم المستخدم بتوصيل محرك أقراص قابل للإزالة أو إذا كان محرك أقراص قابل للإزالة متصلاً بالفعل، يطالب برنامج Kaspersky Endpoint Security المستخدم بتأكيد إجراء عملية التشفير (انظر الشكل أدناه).

يُتيح لك التطبيق تنفيذ الإجراءات التالية:

- إذا أكد المستخدم طلب التشفير، يقوم برنامج Kaspersky Endpoint Security بتشفير البيانات.
- إذا رفض المستخدم طلب التشفير، يترك برنامج Kaspersky Endpoint Security البيانات دون تغيير ويقوم بتعيين الوصول للقراءة فقط لمحرك الأقراص القابل للإزالة هذا.
- إذا لم يستجب المستخدم لطلب التشفير، يترك برنامج Kaspersky Endpoint Security البيانات دون تغيير ويقوم بتعيين الوصول للقراءة فقط لمحرك الأقراص القابل للإزالة هذا. يطالبك التطبيق بالتأكيد مرة أخرى عند تطبيق سياسة لاحقًا أو في المرة التالية التي يتم فيها توصيل محرك الأقراص القابل للإزالة هذا.

إذا بدأ المستخدم بالإزالة الآمنة لمحرك قرص قابل للإزالة أثناء تشفير البيانات، فيقوم Kaspersky Endpoint Security بمقاطعة عملية تشفير البيانات والسماح بإزالة محرك القرص القابل للإزالة قبل انتهاء عملية التشفير. سيستمر تشفير البيانات في المرة التالية التي يتصل فيها محرك الأقراص القابل للإزالة بجهاز الكمبيوتر هذا.

في حال تعذر تشفير محرك أقراص قابل للإزالة، يمكن عرض تقرير **تشفير البيانات** في واجهة Kaspersky Endpoint Security. يمكن أن يكون الوصول إلى البيانات محجوبًا بسبب تطبيق آخر. في هذه الحالة، جرب فصل محرك الأقراص القابل للإزالة من الكمبيوتر ثم إعادة توصيله مرة أخرى.

طلب تشفير محرك الأقراص القابل للإزالة

إضافة قاعدة تشفير لمحركات الأقراص القابلة للإزالة

لإضافة قاعدة تشفير لمحركات الأقراص القابلة للإزالة:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.
5. انقر على الزر **إضافة** وفي القائمة المنسدلة حدد أحد العناصر التالية:
   - إذا كنت تريد إضافة قواعد تشفير لمحركات الأقراص القابلة للإزالة الموجودة في قائمة الأجهزة الموثوقة من مكون التحكم في الجهاز، فحدد **من قائمة الأجهزة الموثوقة الخاصة بهذه السياسة**.
   - إذا كنت تريد إضافة قواعد تشفير لمحركات الأقراص القابلة للإزالة الموجودة في قائمة Kaspersky Security Center، فحدد **من قائمة الأجهزة الخاصة بـ Kaspersky Security Center**.
6. في القائمة المنسدلة **وضع تشفير الأجهزة المحددة** حدد الإجراء الذي تريد تنفيذه بواسطة Kaspersky Endpoint Security على الملفات المخزنة على محركات الأقراص القابلة للإزالة المحددة.
7. حدد خانة الاختيار **الوضع المحمول** إذا كنت ترغب في أن يقوم Kaspersky Endpoint Security بإعداد محركات الأقراص القابلة للإزالة قبل التشفير، مما يجعل من السهل استخدام الملفات المشفرة المخزنة عليها في الوضع المحمول.

   يتيح لك الوضع المحمول استخدام الملفات المشفرة المخزنة على محركات الأقراص القابلة للإزالة المتصلة بأجهزة الكمبيوتر بدون وظائف التشفير.
8. حدد خانة الاختيار **تشفير مساحة القرص المستخدمة فقط** إذا كنت تريد أن يقوم Kaspersky Endpoint Security بتشفير قطاعات القرص الممتلئة بالملفات فقط.

   إذا كنت تقوم بتشفير محرك أقراص مستخدم بالفعل، فمن المستحسن تشفير محرك الأقراص بالكامل. يضمن ذلك حماية كل البيانات – حتى الملفات التي تم حذفها والتي قد لا تزال تحتوي على معلومات يمكن استرجاعها. يوصى باستخدام وظيفة **تشفير مساحة القرص المستخدمة فقط** لمحركات الأقراص الجديدة التي لم يتم استخدامها مسبقًا.

> إذا تم تشفير جهاز مسبقًا باستخدام وظيفة **تشفير مساحة القرص المستخدمة فقط**، وبعد تطبيق سياسة في وضع **تشفير محرك الأقراص القابل للإزالة بالكامل**، سوف تزال القطاعات غير الممتلئة بالملفات غير مشفرة.

9. في القائمة المنسدلة **إجراءات الأجهزة التي تم تحديدها مسبقًا** حدد الإجراء الذي تريد تنفيذه بواسطة Kaspersky Endpoint Security وفقًا لقواعد التشفير التي تم تحديدها مسبقًا لمحركات الأقراص القابلة للإزالة:
   - إذا كنت تريد أن تظل قاعدة التشفير التي تم إنشاؤها مسبقًا لمحرك الأقراص القابل للإزالة دون تغيير، فحدد **تخطي**.
   - إذا كنت تريد استبدال قاعدة التشفير التي تم إنشاؤها مسبقًا لمحرك الأقراص القابل للإزالة بقاعدة جديدة، فحدد **تحديث**.
10. احفظ تغييراتك.

سوف يتم تطبيق قواعد التشفير المضافة لمحركات الأقراص القابلة للإزالة على محركات الأقراص القابلة للإزالة المتصلة بأي جهاز كمبيوتر في المؤسسة.

تصدير واستيراد قائمة بقواعد التشفير لمحركات الأقراص القابلة للإزالة

يمكنك تصدير قائمة قواعد تشفير محرك الأقراص القابل للإزالة إلى ملف XML. ثم يمكنك تعديل الملف، على سبيل المثال، لإضافة عدد كبير من القواعد للنوع نفسه من محركات الأقراص القابلة للإزالة. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة القواعد أو لترحيل القواعد إلى خادم مختلف.

كيفية تصدير واستيراد قائمة قواعد تشفير محرك الأقراص القابل للإزالة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.
5. لتصدير قائمة قواعد التشفير لمحركات الأقراص القابلة للإزالة:
   a. حدد القواعد التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.
   إذا لم تحدد أي قاعدة، فسيقوم Kaspersky Endpoint Security بتصدير كل القواعد.
   b. انقر على رابط **تصدير**.
   c. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة القواعد إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.
   d. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد بالكامل إلى ملف XML.
6. لاستيراد قائمة قواعد التشفير لمحركات الأقراص القابلة للإزالة:
   a. انقر على رابط **استيراد**.
   في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.
   b. افتح الملف.
   إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.
7. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد تشفير محرك الأقراص القابل للإزالة في وحدة تحكم الويب

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Data Encryption** ← **Encryption of removable drives**.

5. في القسم **Encryption rules for selected devices**، انقر على الرابط **Encryption rules**.
يفتح هذا قائمة قواعد التشفير لمحركات الأقراص القابلة للإزالة.

6. لتصدير قائمة قواعد التشفير لمحركات الأقراص القابلة للإزالة:

   a. حدد القواعد التي تريد تصديرها.

   b. انقر على **Export**.

   c. أكد أنك تريد تصدير القواعد المحددة فقط، أو تصدير القائمة بأكملها.

   d. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف XML في مجلد التنزيلات الافتراضي.

7. لاستيراد قائمة القواعد:

   a. انقر على رابط **Import**.
   في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

   b. افتح الملف.
   إذا كان جهاز الكمبيوتر يحتوي على قائمة قواعد بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف XML.

8. احفظ تغييراتك.

الوضع المحمول للوصول إلى الملفات المشفرة على محركات الأقراص القابلة للإزالة

الوضع المحمول هو وضع لتشفير الملفات (FLE) على محركات الأقراص القابلة للإزالة يوفر القدرة على الوصول إلى البيانات خارج شبكة الشركة. الوضع المحمول يوفر لك كذلك القدرة على العمل مع البيانات المشفرة على أجهزة الكمبيوتر غير المثبت عليها Kaspersky Endpoint Security.

يمكن استخدام الوضع المحمول في الحالات التالية:

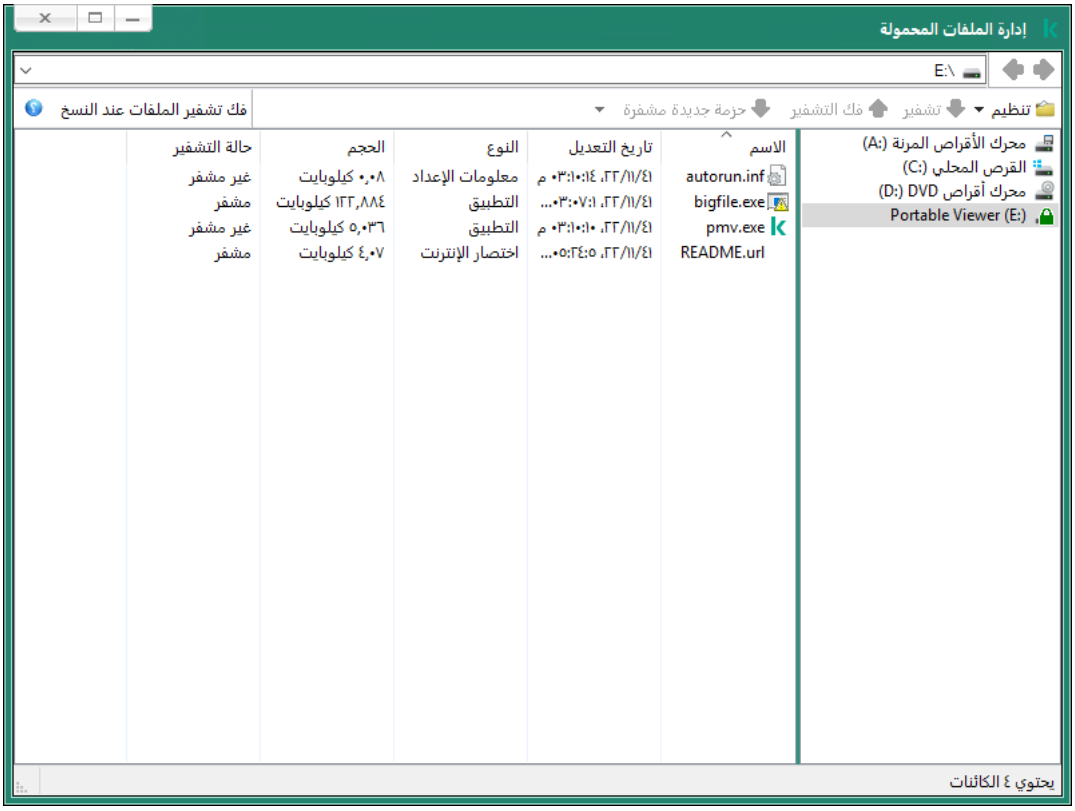
- لا يوجد اتصال بين الكمبيوتر وخادم إدارة Kaspersky Security Center.
- قد تغيرت البنية التحتية بتغير خادم إدارة Kaspersky Security Center.
- Kaspersky Endpoint Security غير مثبت على الكمبيوتر.

إدارة الملفات المحمولة

للعمل في الوضع المحمول، فإن Kaspersky Endpoint Security يقوم بتثبيت وحدة تشفير خاصة اسمها مدير الملفات المحمولة على محرك الأقراص القابل للإزالة. مدير الملفات المحمولة توفر واجهة للعمل مع الملفات المشفرة إذا كان Kaspersky Endpoint Security غير مثبت على الكمبيوتر (انظر الشكل أدناه). إذا كان Kaspersky Endpoint Security مثبتًا على جهاز الكمبيوتر، يمكنك العمل مع محركات الأقراص القابلة للإزالة المشفرة باستخدام مدير الملفات المعتاد (Explorer على سبيل المثال).

يقوم مدير الملفات المحمولة بتخزين مفتاح لتشفير الملفات على محرك أقراص قابل للإزالة. يتم تشفير المفتاح بكلمة مرور المستخدم. يضع المستخدم كلمة مرور قبل تشفير الملفات على محرك أقراص قابل للإزالة.

يبدأ مدير الملفات المحمولة في العمل بشكل تلقائي عند توصيل محرك أقراص قابل للإزالة بجهاز كمبيوتر غير مثبت عليه Kaspersky Endpoint Security. إذا كان بدء التشغيل التلقائي للتطبيقات معطل على جهاز الكمبيوتر، ابدأ بنفسك تشغيل مدير الملفات المحمولة. لفعل هذا، قم بفتح الملف باسم pmv.exe الموجود على محرك الأقراص القابل للإزالة.



إدارة الملفات المحمولة

دعم الوضع المحمول للعمل مع الملفات المشفرة

كيفية تفعيل دعم الوضع المحمول للعمل مع الملفات المشفرة الموجودة على محركات الأقراص القابلة للإزالة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.

5. في القائمة المنسدلة **وضع تشفير الأجهزة المحددة**، حدد **تشفير جميع الملفات** أو **تشفير الملفات الجديدة فقط**.

الوضع المحمول متوفر فقط مع التشفير على مستوى الملف (FLE). من غير الممكن تفعيل دعم الوضع المحمول لتشفير القرص بالكامل (FDE).

6. حدد خانة الاختيار **الوضع المحمول**.

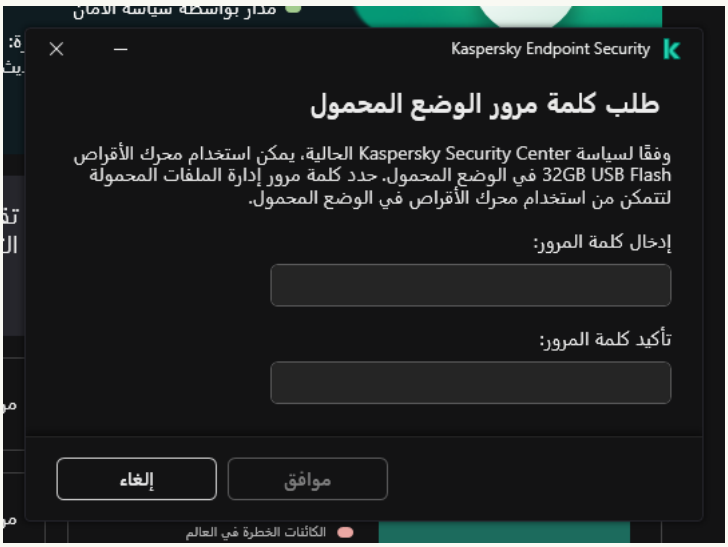
7. يمكنك إضافة قواعد التشفير لمحركات الأقراص القابلة للإزالة الفردية إذا كان ذلك ضروريًا.

8. احفظ تغييراتك.

9. بعد تطبيق السياسة، قم بتوصيل محرك الأقراص القابل للإزالة بجهاز الكمبيوتر.

10. قم بتأكيد عملية تشفير محرك الأقراص القابل للإزالة.

سيؤدي هذا إلى فتح نافذة يمكنك فيها إنشاء كلمة مرور لمدير الملفات المحمولة.



طلب كلمة مرور الوضع المحمول

11. حدد كلمة مرور تفي بمتطلبات القوة وقم بالتأكيد عليها.

12. احفظ تغييراتك.

كيفية تفعيل دعم الوضع المحمول للعمل مع الملفات المشفرة الموجودة على محركات الأقراص القابلة للإزالة في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Data Encryption** ← **Encryption of removable drives**.

5. تحت القسم **Manage encryption**، حدد **Encrypt all files** أو **Encrypt new files only**.

الوضع المحمول متوفر فقط مع التشفير على مستوى الملف (FLE). من غير الممكن تفعيل دعم الوضع المحمول لتشفير القرص بالكامل (FDE).

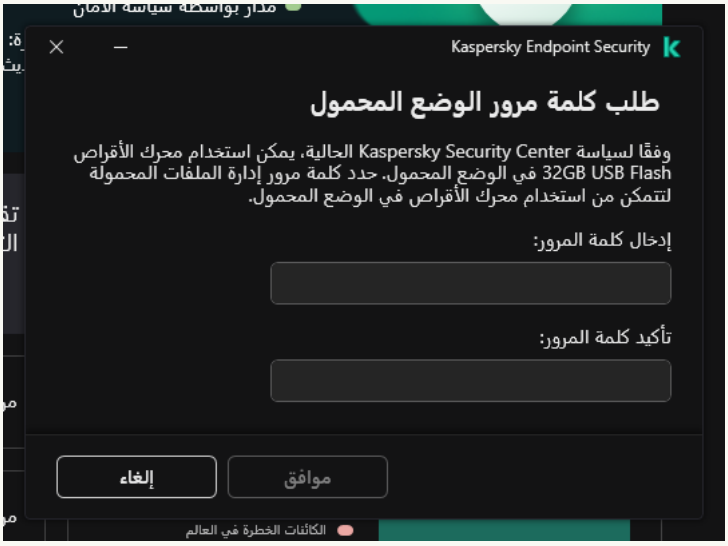
6. حدد خانة الاختيار **Portable mode**.

7. يمكنك إضافة قواعد التشفير لمحركات الأقراص القابلة للإزالة الفردية إذا كان ذلك ضروريًا.

8. احفظ تغييراتك.

9. بعد تطبيق السياسة، قم بتوصيل محرك الأقراص القابل للإزالة بجهاز الكمبيوتر.

10. قم بتأكيد عملية تشفير محرك الأقراص القابل للإزالة.
سيؤدي هذا إلى فتح نافذة يمكنك فيها إنشاء كلمة مرور لمدير الملفات المحمولة.



طلب كلمة مرور الوضع المحمول

11. حدد كلمة مرور تفي بمتطلبات القوة وقم بالتأكيد عليها.

12. احفظ تغييراتك.

سيقوم Kaspersky Endpoint Security بتشفير الملفات على محرك الأقراص القابل للإزالة. ستتم أيضًا إضافة مدير الملفات المحمولة المستخدم للعمل مع الملفات المشفرة إلى محرك الأقراص القابل للإزالة. إذا كان يوجد بالفعل ملفات مشفرة على محرك الأقراص القابل للإزالة، فإن Kaspersky Endpoint Security سوف يشفر جميع الملفات مرة أخرى باستخدام مفتاحه الخاص. هذا يتيح للمستخدم الوصول إلى جميع الملفات الموجودة على محرك الأقراص القابل للإزالة في الوضع المحمول.

الوصول إلى الملفات المشفرة على محرك الأقراص القابل للإزالة

بعد تشفير الملفات على محرك أقراص قابل للإزالة مع دعم الوضع المحمول، فإن طرق الوصول للملفات التالية تكون متوفرة:

- إذا كان Kaspersky Endpoint Security غير مثبت على الكمبيوتر، فإن مدير الملفات المحمولة سوف يطلب منك إدخال كلمة المرور. سوف تحتاج إلى إدخال كلمة المرور في كل مرة تعيد فيها تشغيل الكمبيوتر أو تعيد توصيل محرك قرص قابل للإزالة.

- إذا كان الكمبيوتر موجودًا خارج شبكة الشركة وكان Kaspersky Endpoint Security مثبتًا على الكمبيوتر، فإن التطبيق سوف يطلب منك إدخال كلمة المرور أو إرسال طلب الوصول إلى الملفات إلى المسؤول. بعد الحصول على الوصول إلى الملفات على محرك أقرص قابل للإزالة، سيقوم Kaspersky Endpoint Security بحفظ المفتاح السري في تخزين مفاتيح الكمبيوتر. وسوف يسمح هذا بالوصول إلى الملفات في المستقبل دون الحاجة إلى إدخال كلمة مرور أو طلب ذلك من المرور (انظر الشكل أدناه).

- ذا كان الكمبيوتر موجودًا داخل شبكة الشركة وكان Kaspersky Endpoint Security مثبتًا على الكمبيوتر، فسوف يكون بإمكانك الوصول إلى الجهاز دون إدخال كلمة المرور. سوف يقوم Kaspersky Endpoint Security باستلام المفتاح السري من خادم إدارة Kaspersky Security Center المتصل به الكمبيوتر.

الوصول إلى الملفات المشفرة على محرك الأقراص القابل للإزالة

استعادة كلمة المرور للعمل في الوضع المحمول

إذا كنت قد نسيت كلمة مرور العمل في الوضع المحمول، فأنت بحاجة إلى توصيل محرك القراص القابل للإزالة بجهاز كمبيوتر مثبت عليه Kaspersky Endpoint Security داخل شبكة الشركة. سوف تتمكن من الوصول إلى الملفات لأن المفتاح السري مخزن في مخزن المفاتيح على الكمبيوتر أو على خادم الإدارة. فك تشفير الملفات وتشفيرها بكلمة مرور جديدة.

مزايا الوضع المحمول عند توصيل محرك أقراص قابل للإزالة بجهاز كمبيوتر من شبكة أخرى

إذا كان الكمبيوتر موجودًا خارج شبكة الشركة وكان Kaspersky Endpoint Security مثبتًا على الكمبيوتر، فسوف يكون بإمكانك الوصول إلى الملفات بإحدى الطرق التالية:

- **الوصول القائم على كلمة مرور**

  بعد إدخال كلمة المرور، سوف تقدر على عرض الملفات الموجودة على محرك الأقراص القابل للإزالة وتعديلها وحفظها (وصول شفاف). يمكن أن يقوم Kaspersky Endpoint Security بوضع حق وصول القراءة فقط لمحرك أقراص قابل للإزالة إذا تم تهيئة المعلمات التالية في إعدادات السياسة من أجل تشفير محركات الأقراص القابلة للإزالة:

  - دعم الوضع المحمول معطل.
  - تم اختيار وضع **تشفير جميع الملفات** أو **تشفير الملفات الجديدة فقط**.

في جميع الحالات الأخرى، سوف تحصل على وصول كامل لمحرك الأقراص القابلة للإزالة (إذن القراءة/الكتابة). سوف تقدر على إضافة ملفات أو حذفها.

يمكنك تغيير أذونات الوصول إلى محرك الأقراص القابل للإزالة حتى عند توصيل محرك الأقراص القابل للإزالة بالكمبيوتر. في حالة تغيير أذونات الوصول لمحرك الأقراص القابلة للإزالة، فإن Kaspersky Endpoint Security سوف يحجب الوصول إلى الملفات ويطالبك بكلمة المرور مرة أخرى.

بعد إدخال كلمة المرور، لا يمكنك تطبيق إعدادات سياسة التشفير على محرك الأقراص القابلة للإزالة. في هذه الحالة، من المستحيل فك تشفير ملفات على محرك الأقراص القابلة للإزالة أو إعادة تشفيرها.

- **اطلب من المسؤول الوصول إلى الملفات**

إذا نسيت كلمة المرور للعمل في الوضع المحمول، اطلب الوصول إلى الملفات من المسؤول. للوصول إلى الملفات، يحتاج المستخدم أن يرسل إلى المسؤول طلب وصول للملفات (ملف بامتداد KESDC). يمكن للمستخدم إرسال ملف طلب الوصول عبر البريد الإلكتروني على سبيل المثال. سوف يرسل المسؤول ملف الوصول إلى البيانات المشفرة (ملف بامتداد KESDR).

بعد إكمال إجراء الطلب-الرد لاستعادة كلمة المرور، سوف تستلم وصول صريح إلى الملفات على محرك الأقراص القابل للإزالة، ووصول كامل إلى محرك الأقراص القابل للإزالة (إذن القراءة/الكتابة).

يمكنك على سبيل المثال تطبيق سياسة تشفير محرك الأقراص القابل للإزالة وإلغاء تشفير الملفات. بعد استعادة كلمة المرور، سيطلب Kaspersky Endpoint Security منك تأكيد التغييرات.

كيفية طلب ملف الوصول إلى البيانات المشفرة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Devices**.

3. في علامة التبويب **الأجهزة**، حدد اسم الكمبيوتر الخاص بالمستخدم الذي يطالب بالوصول إلى الملفات المشفرة وانقر بزر الماوس الأيمن لفتح القائمة السياقية.

4. في قائمة السياق، حدد **منح إمكانية الوصول في وضع عدم الاتصال**.

5. في النافذة التي تفتح، حدد القسم **تشفير البيانات**.

6. في علامة التبويب **تشفير البيانات**، انقر فوق الزر **استعراض**.

7. في نافذة تحديد ملف وصول طلب، حدد المسار للملف المستلم من المستخدم.

سترى معلومات حول طلب المستخدم. يقوم Kaspersky Security Center بإنشاء ملف مفتاح. أرسل ملف مفتاح الوصول إلى البيانات المشفرة الذي تم إنشاؤه إلى المستخدم بالبريد الإلكتروني. أو احفظ ملف الوصول واستخدم أي طريقة متاحة لنقل الملف.

منح إمكانية الوصول في وضع عدم الاتصال

[كيفية طلب ملف الوصول إلى البيانات المشفرة في Web Console](#)

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Managed devices**.
2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى بياناته.
3. انقر على الزر **Grant access to the device in offline mode**.
4. حدد **Data Encryption**.
5. انقر فوق الزر **Select file** وحدد ملف وصول الطلب الذي تلقيته من المستخدم (ملف بامتداد KESDC).
   سيعرض مكون Web Console معلومات حول الطلب. وسيشمل هذا اسم الكمبيوتر الذي يطلب المستخدم الوصول إلى الملف عليه.
6. انقر على الزر **Save key** وحدد مجلدًا لحفظ ملف مفتاح الوصول إلى البيانات المشفرة (ملف بامتداد KESDR).

ونتيجة لذلك، ستتمكن من الحصول على مفتاح الوصول إلى البيانات المشفرة، والذي ستحتاج إلى نقله إلى المستخدم.

فك تشفير محركات الأقراص القابلة للإزالة

يمكنك استخدام سياسة لفك تشفير محرك أقراص قابل للإزالة. يتم إنشاء سياسة ذات إعدادات محددة لتشفير محرك الأقراص القابل للإزالة لمجموعة إدارة محددة. لذلك، تعتمد نتيجة فك تشفير البيانات على محركات الأقراص القابلة للإزالة على الكمبيوتر المتصل به محرك القرص القابل للإزالة.

لفك تشفير محركات الأقراص القابلة للإزالة:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.
5. إذا كنت تريد فك تشفير جميع الملفات المشفرة المخزنة على محركات الأقراص القابلة للإزالة، في القائمة المنسدلة **وضع التشفير** حدد **فك تشفير محرك الأقراص القابل للإزالة بالكامل**.
6. لفك تشفير البيانات المخزنة على محركات الأقراص القابلة للإزالة الفردية، قم بتحرير قواعد التشفير لمحركات الأقراص القابلة للإزالة التي تريد فك تشفير البيانات الخاصة بها. للقيام بذلك:
   a. في قائمة محركات الأقراص القابلة للإزالة التي تم تكوين قواعد التشفير لها، حدد إدخال موافق لمحرك القرص القابل للإزالة الذي تحتاجه.
   b. انقر فوق الزر **تعيين قاعدة** لتحرير قاعدة التشفير لمحرك القرص القابل للإزالة المحدد.
   c. في قائمة السياق الخاصة بالزر **تعيين قاعدة**، انقر فوق **فك تشفير محرك الأقراص القابل للإزالة بالكامل**.
7. احفظ تغييراتك.

ونتيجةً لهذا، إذا كان المستخدم يوصل محرك أقراص قابل للإزالة أو إذا كان متصلاً بالفعل، فإن Kaspersky Endpoint Security سيفك تشفير محرك الأقراص القابل للإزالة. يحذر التطبيق المستخدم من أن عملية فك التشفير قد تستغرق بعض الوقت. إذا بدأ المستخدم بالإزالة الآمنة لمحرك قرص قابل للإزالة أثناء فك تشفير البيانات، فيقوم Kaspersky Endpoint Security بمقاطعة عملية فك تشفير البيانات والسماح بإزالة محرك القرص القابل للإزالة قبل انتهاء عملية فك التشفير. سيستمر فك تشفير البيانات في المرة التالية التي يتصل فيها محرك الأقراص القابل للإزالة بجهاز الكمبيوتر هذا.

في حال تعذر فك تشفير محرك أقراص قابل للإزالة، يمكن عرض تقرير **تشفير البيانات** في واجهة Kaspersky Endpoint Security. يمكن أن يكون الوصول إلى البيانات محجوبًا بسبب تطبيق آخر. في هذه الحالة، جرب فصل محرك الأقراص القابل للإزالة من الكمبيوتر ثم إعادة توصيله مرة أخرى.

عرض تفاصيل تشفير البيانات

أثناء تقدم عملية التشفير أو فك التشفير، يُرحل Kaspersky Endpoint Security معلومات حول حالة معلمات التشفير المطبقة على أجهزة الكمبيوتر العميلة إلى Kaspersky Security Center.

عرض حالة التشفير

يمكنك إلقاء نظرة على الحالة لمراقبة تشفير البيانات. ويعيّن Kaspersky Endpoint Security حالات التشفير التالية:

- **عدم استيفاء السياسة؛ تم الإلغاء بواسطة المستخدم**. ألغى المستخدم تشفير البيانات.
- **لا يتوافق مع السياسة بسبب وجود خطأ**. خطأ في تشفير البيانات، على سبيل المثال، ترخيص مفقود.
- **تطبيق السياسة. يلزم إعادة التشغيل**. تشفير البيانات قيد التقدم على الكمبيوتر. أعد تشغيل الكمبيوتر لإكمال تشفير البيانات.
- **لا توجد سياسة تشفير محددة**. تم إيقاف تشفير البيانات في إعدادات السياسة.
- **(غير مدعوم)**. لم يتم تثبيت مكونات تشفير البيانات على الكمبيوتر.
- **تطبيق السياسة**. تشفير و / أو فك تشفير البيانات قيد التقدم على الكمبيوتر.

لعرض حالة تشفير بيانات الكمبيوتر:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Managed Devices**.
3. من علامة التبويب **الأجهزة** في مساحة العمل، حرك شريط التمرير إلى اليسار. إذا كان العمود **حالة التشفير** غير معروض، أضف هذا العمود في إعدادات وحدة تحكم Kaspersky Security Center.

   يعرض عمود **حالة التشفير** حالة تشفير البيانات على أجهزة الكمبيوتر في مجموعة الإدارة المحددة. تتكون هذه الحالة بناءً على المعلومات حول تشفير الملف على الأقراص المحلية للكمبيوتر، وحول تشفير القرص بالكامل.
4. إذا كانت حالة تشفير البيانات للكمبيوتر هي **تطبيق السياسة**، يمكنك مراقبة لوحة تقدم التشفير:
   a. افتح خصائص الكمبيوتر التي تتضمن حالة **تطبيق السياسة** بالنقر المزدوج عليها.
   b. من نافذة خصائص الكمبيوتر، حدد القسم **التطبيقات**.
   c. في قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر، حدد **Kaspersky Endpoint Security for Windows**.
   d. انقر على **إحصائيات**.
   e. تحت **تشفير الأجهزة** يمكنك أن ترى التقدم الحالي لتشفير البيانات كنسبة مئوية.

عرض إحصائيات عن لوحات تحكم Kaspersky Security Center

لعرض حالة التشفير في لوحات تحكم Kaspersky Security Center:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد العقدة **خادم الإدارة**.
3. في محطة العمل الموجودة على يسار شجرة وحدة تحكم الإدارة، حدد علامة التبويب **الإحصائيات**.
4. قم بإنشاء صفحة جديدة تحتوي على أجزاء تفاصيل تحتوي على إحصائيات تشفير البيانات. للقيام بذلك:
   a. في علامة التبويب **الإحصائيات**، انقر فوق الزر **تخصيص العرض**.
   b. في النافذة التي ستفتح، انقر فوق الزر **إضافة**.
   c. يفتح هذا نافذة، وفي تلك النافذة، في القسم **عام**، أدخل اسم الصفحة.
   d. في القسم **جزء المعلومات**، انقر فوق الزر **إضافة**.
   e. في النافذة التي تفتح، في المجموعة **حالة الحماية**، حدد العنصر **تشفير الأجهزة**.
   f. انقر فوق **موافق**.
   g. إذا لزم الأمر، قم بتحرير إعدادات جزء التفاصيل. ولفعل هذا، استخدم القسمين **عرض** و**الأجهزة**.
   h. انقر فوق **موافق**.
   i. كرر الخطوات من د إلى ح من الإرشادات، مع تحديد العنصر **تشفير محركات الأقراص القابلة للإزالة** في القسم **حالة الحماية**.
   تظهر أجزاء التفاصيل التي تمت إضافتها في قائمة **لوحات المعلومات**.
   j. انقر فوق **موافق**.
   يظهر اسم الصفحة مع أجزاء التفاصيل التي تم إنشاؤها في الخطوات السابقة في قائمة **الصفحات**.
   k. انقر فوق الزر **إغلاق**.
5. في علامة التبويب **الإحصائيات**، افتح الصفحة التي تم إنشاؤها في خطوات التعليمات السابقة.

تظهر أجزاء التفاصيل، والتي توضح حالة تشفير أجهزة الكمبيوتر ومحركات الأقراص القابلة للإزالة.

عرض أخطاء تشفير الملفات على محركات أقراص الكمبيوتر المحلية

لعرض أخطاء تشفير الملفات على محركات أقراص الكمبيوتر المحلية:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Managed Devices**.
3. في علامة التبويب **الأجهزة**، حدد اسم الكمبيوتر في القائمة وانقر بزر الماوس الأيمن لفتح قائمة السياق.

4. في القائمة السياقية للكمبيوتر، حدد العنصر **الخصائص**. في النافذة التي تفتح، حدد القسم **الحماية**.

5. انقر فوق الرابط **عرض أخطاء تشفير البيانات** لفتح النافذة **أخطاء تشفير البيانات**.

تعرض هذه النافذة تفاصيل أخطاء تشفير الملفات على أقراص الكمبيوتر المحلية. عند تصحيح خطأ، يقوم Kaspersky Security Center بإزالة تفاصيل الخطأ من نافذة **أخطاء تشفير البيانات**.

عرض تقرير تشفير البيانات

يتيح لك Kaspersky Security Center إنشاء تقارير تشفير البيانات:

- **تقرير حالة تشفير الأجهزة المُدارة**. ويتضمن التقرير معلومات عما إذا كانت حالة تشفير الكمبيوتر تتوافق مع سياسة التشفير.
- **تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة**. ويتضمن التقرير معلومات عن حالة تشفير الأجهزة الخارجية وأجهزة التخزين.
- **الإبلاغ عن حقوق الوصول إلى برامج التشغيل المشفرة**. ويتضمن التقرير معلومات عن حالة الحسابات التي يمكنها الوصول إلى محركات الأقراص المشفرة.
- **تقرير حول أخطاء تشفير الملف**. ويتضمن التقرير معلومات عن الأخطاء التي حدثت أثناء تنفيذ مهام تشفير البيانات أو فك تشفيرها على أجهزة الكمبيوتر.
- **تقرير حول حجب الوصول إلى الملفات المشفرة**. ويتضمن التقرير معلومات عن التطبيقات التي تم حظرها من الوصول إلى الملفات المشفرة.

لعرض تقرير تشفير البيانات:

1. افتح Kaspersky Security Center Administration Console.

2. في العقدة **خادم الإدارة** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **تقارير**.

3. انقر فوق الزر **قالب التقارير الجديد**.
بدء تشغيل معالج قالب تقرير جديد.

4. اتبع تعليمات معالج قالب التقرير. في النافذة **تحديد نوع قالب التقرير** في القسم **غير ذلك** حدد أحد تقارير تشفير البيانات.
بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول في علامة التبويب **تقارير**.

5. حدد قالب التقرير الذي تم إنشاؤه في الخطوة السابقة من الإرشادات.

6. في قائمة السياق الخاصة القالب، حدد **إظهار التقرير**.

تبدأ عملية إنشاء التقرير. يتم عرض التقرير في نافذة جديدة.

استخدام الأجهزة المشفرة في حالة عدم توافر الوصول إليها

الحصول على حق الوصول إلى الأجهزة المشفرة

قد يحتاج المستخدم طلب الوصول إلى الأجهزة المشفرة في الحالات التالية:

- تم تشفير محرك الأقراص الصلبة على كمبيوتر آخر.

- مفتاح التشفير لجهاز ما غير موجود على الكمبيوتر (على سبيل المثال، عند أول محاولة للوصول إلى محرك الأقراص القابل للإزالة المشفّر على الكمبيوتر)، والكمبيوتر غير متصل بـ Kaspersky Security Center.

  بعد استخدام المستخدم لمفتاح الوصول إلى الجهاز المشفر، يحفظ Kaspersky Endpoint Security مفتاح التشفير على كمبيوتر المستخدم ويسمح بالوصول إلى هذا الجهاز عند محاولات الوصول اللاحقة حتى إذا لم يكن هناك أي اتصال بـ Kaspersky Security Center.

يمكن الحصول على حق الوصول إلى الأجهزة المشفرة على النحو التالي:

1. يقوم المستخدم باستخدام واجهة تطبيق Kaspersky Endpoint Security لإنشاء ملف طلب وصول بامتداد kesdc وإرساله إلى مسؤول الشبكة المحلية بالشركة.

2. يقوم المسؤول باستخدام وحدة تحكم إدارة Kaspersky Security Center لإنشاء ملف مفتاح الوصول بامتداد kesdr وإرساله إلى المستخدم.

3. يقوم المستخدم بتطبيق مفتاح الوصول.

استعادة البيانات الموجودة على الأجهزة المشفرة

يمكن للمستخدم استخدام أداة الاستعادة المساعدة للجهاز المشفر (والمشار إليه فيما بعد بأداة الاستعادة) للتعامل مع الأجهزة المشفرة. قد يكون ذلك مطلوبًا في الحالات التالية:

- كان الإجراء الخاص باستخدام مفتاح وصول للحصول على حق الوصول غير ناجحًا.
- لم يتم تثبيت مكونات التشفير على الكمبيوتر من خلال الجهاز المشفر.

البيانات اللازمة لاستعادة الوصول إلى الأجهزة المشفرة باستخدام "أداة الاستعادة" موجودة في ذاكرة كمبيوتر المستخدم في صورة غير مشفرة لبعض الوقت. لتقليل مخاطر الوصول غير المصرح به لمثل هذه البيانات، ننصحك باستعادة الوصول إلى الأجهزة المشفرة على أجهزة الكمبيوتر الموثوقة.

يمكن استعادة البيانات الموجودة على الأجهزة المشفرة على النحو التالي:

1. يقوم المستخدم باستخدام أداة الاستعادة لإنشاء ملف طلب الوصول بامتداد fdertc وإرساله إلى مسؤول الشبكة المحلية بالشركة.

2. يقوم المسؤول باستخدام وحدة تحكم إدارة Kaspersky Security Center لإنشاء ملف مفتاح الوصول بامتداد fdertr وإرساله إلى المستخدم.

3. يقوم المستخدم بتطبيق مفتاح الوصول.

لاستعادة البيانات الموجودة على محركات الأقراص الصلبة المشفرة للنظام، يمكن للمستخدم أيضًا تحديد بيانات اعتماد حساب وكيل المصادقة في "أداة الاستعادة". في حالة تلف بيانات تعريف حساب وكيل المصادقة، يجب على المستخدم إكمال إجراء الاستعادة باستخدام ملف طلب الوصول.

قبل استعادة البيانات على الأجهزة المشفرة، من المستحسن إلغاء سياسة Kaspersky Security Center أو تعطيل التشفير في إعدادات سياسة Kaspersky Security Center على الكمبيوتر حيث سيتم تنفيذ هذا الإجراء. يمنع هذا الجهاز من التشفير مرة أخرى.

استرداد البيانات باستخدام الأداة المساعدة FDERT

في حال فشل عمل محرك الأقراص الصلبة، فإن نظام الملفات قد يكون تالفًا. إذا كان هذا هو السبب، فإن البيانات المحمية بتقنية تشفير القرص من Kaspersky ستكون غير متاحة. يمكنك فك تشفير البيانات ونسخها إلى محرك أقراص جديد.

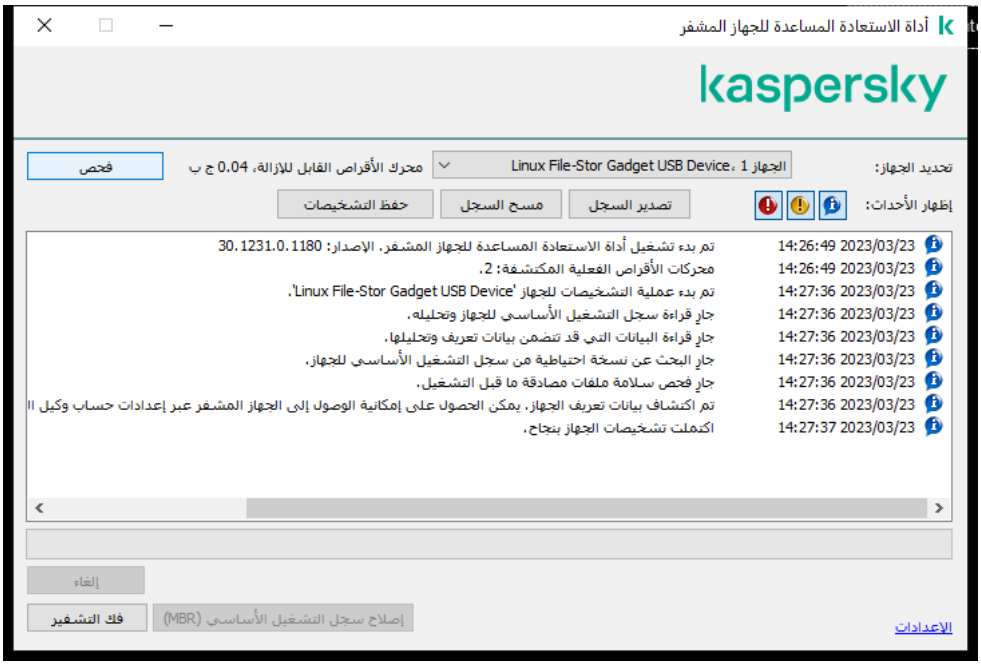
استرداد البيانات إلى محرك أقراص محمي بتقنية تشفير القرص من Kaspersky يتكون من الخطوات التالية:

1. إنشاء أداة الاستعادة المساعدة المستقلة (راجع الشكل أدناه).

2. توصيل محرك أقراص بالكمبيوتر غير مثبت عليه مكونات تشفير Kaspersky Endpoint Security.

3. تشغيل أداة الاستعادة وتشخيص محرك الأقراص الصلبة.

4. الوصول للبيانات على محرك الأقراص. لفعل ذلك، أدخل بيانات الاعتماد لوكيل المصادقة أو ابدأ إجراء الاسترداد (طلب–رد).



أداة الاستعادة FDERT

إنشاء أداة الاستعادة المساعدة المستقلة

لإنشاء ملف تنفيذي لأداة الاستعادة:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر .

2. في النافذة التي تفتح، انقر فوق الزر **استعادة الجهاز المشفر**.
تبدأ أداة الاستعادة المساعدة للجهاز المشفر.

3. انقر فوق الزر **إنشاء أداة الاستعادة المساعدة المستقلة** في نافذة أداة الاستعادة.

4. احفظ أداة الاستعادة المساعدة المستقلة على ذاكرة الكمبيوتر.

نتيجةً لذلك، سيتم حفظ الملف التنفيذي لأداة الاستعادة (fdert.exe) في المجلد المحدد. انسخ أداة الاستعادة على كمبيوتر غير مثبت عليه مكونات تشفير Kaspersky Endpoint Security. يمنع هذا محرك الأقراص من تشفيره مرة أخرى.

البيانات اللازمة لاستعادة الوصول إلى الأجهزة المشفرة باستخدام "أداة الاستعادة" موجودة في ذاكرة كمبيوتر المستخدم في صورة غير مشفرة لبعض الوقت. لتقليل مخاطر الوصول غير المصرح به لمثل هذه البيانات، ننصحك باستعادة الوصول إلى الأجهزة المشفرة على أجهزة الكمبيوتر الموثوقة.

استرداد البيانات على محرك أقراص ثابتة

لاستعادة الوصول إلى جهاز مشفر باستخدام أداة الاستعادة:

1. قم بتشغيل الملف باسم fdert.exe، وهو الملف التنفيذي لأداة الاستعادة. تم إنشاء هذا الملف بواسطة Kaspersky Endpoint Security.

2. في نافذة Restore Utility (أداة الاستعادة)، حدد الجهاز المشفر الذي تريد استعادة الوصول إليه.

3. انقر فوق الزر **فحص** للسماح للأداة بتحديد أي الإجراءات التي ينبغي اتخاذها على الجهاز: سواء كانت إلغاء القفل أو فك التشفير.

إذا كان للكمبيوتر حق الوصول إلى وظيفة تشفير Kaspersky Endpoint Security، فسوف تطالبك أداة الاستعادة بإلغاء تأمين الجهاز. وعلى الرغم من أن إلغاء منع الجهاز لا يؤدي إلى فك تشفيره، يمكن الوصول إلى الجهاز مباشرة نتيجة إلغاء المنع. إذا لم يكن للكمبيوتر حق الوصول إلى وظيفة تشفير Kaspersky Endpoint Security، فسوف تطالبك أداة الاستعادة بفك تشفير الجهاز.

4. إذا كنت ترغب في استرداد معلومات التشخيص، انقر فوق زر **حفظ التشخيصات**.

ستقوم الأداة بحفظ أرشيف بالملفات التي تحتوي على معلومات التشخيص.

5. انقر فوق زر **إصلاح سجل التشغيل الأساسي (MBR)** إذا عادت عمليات تشخيص محرك قرص النظام المشفر برسالة حول المشكلات التي تخص سجل التشغيل الرئيسي (MBR) للجهاز.

يمكن أن يؤدي إصلاح سجل التشغيل الرئيسي للجهاز إلى تسريع عملية الحصول على المعلومات الضرورية لإلغاء منع الجهاز أو فك تشفيره.

6. انقر فوق الزر **إلغاء تأمين** أو **فك التشفير** وفقًا لنتائج التشخيص.

7. إذا كنت ترغب في استعادة البيانات باستخدام حساب وكيل المصادقة، حدد خيار **استخدام إعدادات حساب وكيل المصادقة** وأدخل بيانات اعتماد وكيل المصادقة.

لن تكون هذه الطريقة ممكنة إلا عند استعادة البيانات الموجودة على محرك أقراص النظام. إذا تم تلف محرك أقراص النظام وتم فقد بيانات حساب وكيل المصادقة، فيجب عليك الحصول على مفتاح وصول من مسؤول الشبكة المحلية بالشركة لاستعادة البيانات الموجودة على الجهاز المشفر.

8. إذا كنت ترغب في بدء إجراء الاسترداد، اتبع الخطوات التالية:

a. فحدد الخيار **حدد مفتاح الوصول للجهاز يدويًا**.

b. انقر فوق زر **تلقي مفتاح الوصول** واحفظ ملف طلب الوصول على ذاكرة الكمبيوتر (ملف بامتداد FDERTC).

c. أرسل ملف طلب الوصول إلى مسؤول الشبكة المحلية بالشركة.

لا تغلق نافذة **استقبال مفتاح الوصول للجهاز** حتى تحصل على مفتاح الوصول. عندما يتم فتح هذه النافذة مرة أخرى، لن يكون بإمكانك استخدام مفتاح الوصول الذي تم إنشاؤه مسبقًا من قِبل المسؤول.

d. استقبل واحفظ ملف الوصول (ملف بامتداد FDERTR) الذي تم إنشاؤه وإرساله إليك من قبل مسؤول الشبكة المحلية للشركة (راجع التعليمات أدناه).

e. قم بتحميل ملف الوصول في نافذة **استقبال مفتاح الوصول للجهاز**.

9. إذا كنت تعمل على فك تشفير ملف، فيجب أن تقوم بتكوين إعدادات فك التشفير الإضافية:

- حدد منطقة لفك التشفير:
- إذا كنت تريد فك تشفير الجهاز بأكمله، فحدد خيار **فك تشفير الجهاز بأكمله**.
- إذا كنت ترغب في فك تشفير جزء البيانات الموجود على جهاز ما، فحدد خيار **فك تشفير مناطق الجهاز الفردية** وحدد حدود منطقة فك التشفير.
- حدد موقعًا لكتابة البيانات التي تم فك تشفيرها:
- إذا كنت تريد إعادة كتابة البيانات الموجودة على الجهاز الأصلي من خلال البيانات التي تم فك تشفيرها، فامسح خانة الاختيار **فك تشفير لملف صورة القرص**.
- إذا كنت تريد حفظ البيانات التي تم فك تشفيرها بشكلٍ منفصل عن البيانات المشفرة الأصلية، فحدد خانة الاختيار **فك تشفير لملف صورة القرص** واستخدم الزر **استعراض** لتحديد المسار الذي سيتم حفظ ملف VHD فيه.

10. انقر على **موافق**.

تبدأ عملية إلغاء منع / فك تشفير الجهاز.

كيفية إنشاء ملف الوصول إلى البيانات المشفرة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة تحكم الإدارة، حدد المجلد **إضافي** ← **تشفير البيانات وحمايتها** ← المجلد **برامج التشغيل المشفرة**.

3. في مساحة العمل، حدد الجهاز المشفر الذي تريد إنشاء ملف مفتاح وصول له، ثم في قائمة سياق الجهاز، انقر فوق **الحصول على حق الوصول إلى الجهاز في Kaspersky Endpoint Security for Windows**.

إذا لم تكن متأكدًا من الكمبيوتر الذي تم إنشاء ملف طلب الوصول له، ففي شجرة وحدة تحكم الإدارة حدد المجلد **إضافي** ← **تشفير البيانات وحمايتها** وفي مساحة العمل انقر فوق **الحصول على مفتاح تشفير الجهاز في Kaspersky Endpoint Security for Windows**.

4. في النافذة التي تفتح، حدد خوارزمية التشفير لاستخدام: **AES256** أو **AES56**.

تعتمد خوارزمية تشفير البيانات على مكتبة تشفير AES المضمنة في حزمة التوزيع: تشفير قوي (AES256) أو تشفير خفيف (AES56). يتم تثبيت مكتبة تشفير AES مع التطبيق.

5. انقر فوق **استعراض** لفتح نافذة، وفي هذه النافذة، حدد المسار إلى ملف الطلب بامتداد fdertc الذي تم استلامه من المستخدم.

6. انقر فوق الزر **فتح**.

سترى معلومات حول طلب المستخدم. يقوم Kaspersky Security Center بإنشاء ملف مفتاح. أرسل ملف مفتاح الوصول إلى البيانات المشفرة الذي تم إنشاؤه إلى المستخدم بالبريد الإلكتروني. أو احفظ ملف الوصول واستخدم أي طريقة متاحة لنقل الملف.

كيفية إنشاء ملف الوصول إلى البيانات المشفرة في Web Console

1. في النافذة الرئيسية في Web Console، حدد **العمليات** ← **تشفير البيانات وحمايتها** ← **برامج التشغيل المشفرة**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي ترغب في استرداد البيانات عليه.

3. انقر على الزر **منح الوصول إلى الجهاز في وضع عدم الاتصال**.

هذا يبدأ المعالج لمنح الوصول إلى جهاز.

4. اتبع تعليمات المعالج لمنح الوصول إلى جهاز:

a. تحديد المكون الإضافي **Kaspersky Endpoint Security for Windows**.

b. حدد خوارزمية التشفير التي سيتم استخدامها: **AES256** أو **AES56**.

تعتمد خوارزمية تشفير البيانات على مكتبة تشفير AES المضمنة في حزمة التوزيع: تشفير قوي (AES256) أو تشفير خفيف (AES56). يتم تثبيت مكتبة تشفير AES مع التطبيق.

c. انقر فوق الزر **حدد ملف** وحدد ملف وصول الطلب الذي تلقيته من المستخدم (ملف بامتداد FDERTC).

d. انقر على الزر **حفظ المفتاح** وحدد مجلدًا لحفظ ملف مفتاح الوصول إلى البيانات المشفرة (ملف بامتداد FDERTR).

ونتيجة لذلك، ستتمكن من الحصول على مفتاح الوصول إلى البيانات المشفرة، والذي ستحتاج إلى نقله إلى المستخدم.

إنشاء قرص إنقاذ نظام تشغيل

يمكن أن يكون قرص إنقاذ نظام التشغيل مفيدًا عند تعذر الوصول إلى محرك الأقراص الصلبة المشفر لبعض الأسباب مع تعذر تحميل نظام التشغيل.

يمكنك تحميل صورة نظام تشغيل Windows باستخدام قرص الإنقاذ واستعادة الوصول إلى محرك الأقراص الصلبة المشفر باستخدام أداة الاستعادة المضمنة في صورة نظام التشغيل.

لإنشاء قرص إنقاذ نظام تشغيل:

1. قم بإنشاء الملف التنفيذي لأداة الاستعادة المساعدة للجهاز المشفر.

2. قم بإنشاء صورة مخصصة لبيئة ما قبل تمهيد Windows. أثناء إنشاء صورة مخصصة لبيئة ما قبل تمهيد Windows، قم بإضافة ملف تنفيذي لأداة استعادة الصورة.

3. قم بحفظ الصورة المخصصة لبيئة ما قبل تمهيد Windows إلى أحد الوسائط المحمولة مثل القرص المدمج أو محرك أقراص قابل للإزالة.

راجع ملفات تعليمات Microsoft للحصول على إرشادات حول إنشاء صورة مخصصة لبيئة ما قبل تمهيد Windows (على سبيل المثال، في مورد Microsoft TechNet).

حلول Detection and Response

يدعم Kaspersky Endpoint Security حلول Detection and Response باستخدام عامل مضمن. لاستخدام Detection and Response، يجب تمكين التكامل مع هذه الحلول عند تثبيت التطبيق. ويدعم العامل المضمن:

- Kaspersky Managed Detection and Response (MDR)؛
- Kaspersky Endpoint Detection and Response Optimum 2.0 (EDR Optimum)؛
- Kaspersky Endpoint Detection and Response Expert (EDR Expert)؛
- Kaspersky Anti Targeted Attack Platform (مكون Endpoint Detection and Response)؛
- Kaspersky Sandbox 2.0.

يمكنك استخدام Kaspersky Endpoint Security with Detection and Response في تكوينات مختلفة، على سبيل المثال ، [MDR+EDR Optimum 2.0+Kaspersky Sandbox 2.0].

Kaspersky Endpoint Agent

يدعم Kaspersky Endpoint Agent التفاعل بين التطبيق وحلول Kaspersky الأخرى لاكتشاف التهديدات المتقدمة (على سبيل المثال Kaspersky Sandbox). حلول Kaspersky متوافقة مع إصدارات معينة من Kaspersky Endpoint Agent.

لاستخدام Kaspersky Endpoint Agent كجزء من حلول Kaspersky، يجب عليك تفعيل هذه الحلول باستخدام مفتاح ترخيص مطابق.

للحصول على معلومات كاملة عن Kaspersky Endpoint Agent المضمن في حل البرنامج الذي تستخدمه، وللحصول على معلومات كاملة عن الحل المستقل، يرجى الرجوع إلى دليل التعليمات الخاص بالمنتج ذي الصلة:

- تعليمات Kaspersky Anti Targeted Attack Platform
- تعليمات Kaspersky Sandbox
- تعليمات Kaspersky Endpoint Detection and Response Optimum
- تعليمات Kaspersky Endpoint Detection and Response Expert
- تعليمات Kaspersky Managed Detection and Response

تتضمن مجموعة أدوات التوزيع لتطبيق Kaspersky Endpoint Security الإصدارات 11.2.0 - 11.8.0 مكون Kaspersky Endpoint Agent. ويمكنك تحديد Kaspersky Endpoint Agent عند تثبيت Kaspersky Endpoint Security for Windows. نتيجة لذلك، سيتم تثبيت تطبيقين على جهاز الكمبيوتر الخاص بك: KEA وKES. في Kaspersky Endpoint Security 11.9.0، لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من مجموعة توزيع Kaspersky Endpoint Security.

مطابقة إصدارات KEA (كجزء من KES) لإصدارات KES

Kaspersky Endpoint Agent	Kaspersky Endpoint Security for Windows
mr1.3.11.0.216	11.8.0
3.11	11.7.0
3.10	11.6.0
3.9	11.5.0

11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

تحوّل Kaspersky كل مهام Detection and Response للعمل مع عامل Kaspersky Endpoint Security المضمن بدلاً من Kaspersky Endpoint Agent. وتضيف Kaspersky دعمًا تدريجيًا لهذه الحلول وتتخلص تدريجيًا من Kaspersky Endpoint Agent (انظر الجدول أدناه). وبدءًا من الإصدار 12.1، يدعم التطبيق جميع حلول Detection and Response. بالإضافة إلى ذلك، بدءًا من الإصدار 12.1، لم يعد التطبيق متوافقًا مع Kaspersky Endpoint Agent، ولم يعد تثبيت كلا التطبيقين جنبًا إلى جنب على الكمبيوتر نفسه ممكنًا.

نشر العامل المضمن لإدارة حلول Detection and Response

إصدار Kaspersky Endpoint Security	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform (مكون Endpoint Detection and Response)
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent
11.9.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent
11.10.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent
11.11.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent
12	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent
12.1	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**

ترحيل السياسة والمهام لـ Kaspersky Endpoint Agent

بدءًا من الإصدار 11.7.0، يتضمن Kaspersky Endpoint Security for Windows معالجًا للترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security. ويمكنك ترحيل السياسة وإعدادات المهام للحلول التالية:

- Kaspersky Sandbox
- (Kaspersky Endpoint Detection and Response Optimum (EDR Optimum
- (Kaspersky Anti Targeted Attack Platform (EDR

لا يعمل معالج الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security إلا في Web Console وCloud Console. في وحدة تحكم الإدارة (MMC)، يمكنك فقط ترحيل إعدادات حل Kaspersky Anti Targeted Attack Platform (EDR) باستخدام معالج ترحيل سياسة ومهمة Kaspersky Security Center القياسي.

يوصى بالبدء بترحيل Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security على كمبيوتر واحد، ثم فعل ذلك على مجموعة من أجهزة الكمبيوتر، ثم إكمال الترحيل على كل أجهزة الكمبيوتر في المؤسسة.

لترحيل إعدادات السياسة والمهام من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security،

في نافذة Web Console الرئيسية، حدد **Operations ← Migration from Kaspersky Endpoint Agent**.

يؤدي هذا إلى تشغيل معالج ترحيل السياسة والمهمة. اتبع تعليمات المعالج.

الخطوة 1. سياسة الترحيل

ينشئ معالج الترحيل سياسة جديدة تدمج إعدادات Kaspersky Endpoint Security وسياسات Kaspersky Endpoint Agent. وفي قائمة السياسات، حدد سياسات Kaspersky Endpoint Agent التي تريد دمج إعداداتها مع سياسة Kaspersky Endpoint Security. وانقر فوق سياسة Kaspersky Endpoint Agent لتحديد Kaspersky Endpoint Security الذي تريد دمج الإعدادات معه. وتأكد من تحديد السياسات الصحيحة وانتقل إلى الخطوة التالية.

الخطوة 2. ترحيل المهام

ينشئ معالج الترحيل مهام جديدة لبرنامج Kaspersky Endpoint Security. في قائمة المهام، حدد مهام Kaspersky Endpoint Agent التي تريد إنشاءها لسياسة Kaspersky Endpoint Security. ويدعم المعالج مهام Kaspersky Endpoint Detection and Response وKaspersky Sandbox. انتقل إلى الخطوة التالية.

الخطوة 3. اكتمال المعالج

أغلق المعالج. نتيجة لذلك، ينفذ المعالج ما يلي:

- ينشئ سياسة Kaspersky Endpoint Security جديدة.

تدمج السياسة الإعدادات من Kaspersky Endpoint Security وKaspersky Endpoint Agent. ويطلق على السياسة اسم <اسم سياسة Kaspersky Endpoint Security> و<اسم سياسة Kaspersky Endpoint Agent>. وتكون حالة السياسة الجديدة Inactive. وللمتابعة، قم بتغيير حالات سياسات Kaspersky Endpoint Agent وKaspersky Endpoint Security إلى Inactive وقم بتفعيل السياسة المدمجة الجديدة.

بعد الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows، يرجى التأكد أن السياسة الجديدة تتضمن إعداد وظيفة نقل البيانات إلى خادم الإدارة (بيانات ملف العزل وبيانات سلسلة تطوير التهديد). ولا يتم ترحيل قيم معلمات نقل البيانات من سياسة في برنامج Kaspersky Endpoint Agent.

عند الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security لحل Kaspersky Anti Targeted Attack Platform (EDR)، قد تواجه أخطاء عند توصيل الكمبيوتر بخوادم Central Node. ويرجع السبب في ذلك إلى أن معالج الترحيل في وحدة تحكم الويب يتخطى إعدادات السياسة التالية ولا يقوم بترحيلها:

- حظر تعديل الإعدادات **Settings for connecting to KATA servers** ("قفل").

بشكل افتراضي، يمكن تعديل الإعدادات ("القفل" مفتوح). لذلك لا يتم تطبيق الإعدادات على الكمبيوتر. ويجب حظر تعديل الإعدادات وإغلاق "القفل".

- حاوية التشفير.

إذا كنت تستخدم المصادقة ثنائية الاتجاه للاتصال بخوادم Central Node، فيجب إعادة إضافة حاوية التشفير. ويقوم معالج الترحيل بترحيل شهادة TLS الخاصة بالخادم بشكل صحيح.

يقوم معالج ترحيل السياسة والمهام في وحدة تحكم الإدارة (MMC) بترحيل جميع الإعدادات الخاصة بحل Kaspersky Anti Targeted Attack Platform (EDR).

- ينشئ مهام Kaspersky Endpoint Security جديدة.

تكون المهام الجديدة نسخًا من مهام Kaspersky Endpoint Agent لحل Kaspersky Endpoint Detection and Response وKaspersky Sandbox. وفي الوقت نفسه، يترك المعالج مهام وكيل Kaspersky Endpoint دون تغيير.

1. في وحدة تحكم الإدارة ، حدد خادم الإدارة وانقر بزر الماوس الأيمن لفتح قائمة السياق.
2. حدد **كل المهام** ← **معالج تحويل تصحيح المهام والسياسات**.

سيبدأ معالج تحويل تصحيح المهام والسياسات. اتبع تعليمات المعالج.

الخطوة 1. حدد التطبيق الذي ترغب في تحويل السياسات والمهام الخاصة به

في هذه الخطوة، تحتاج إلى تحديد Kaspersky Endpoint Security for Windows. انتقل إلى الخطوة التالية.

الخطوة 2. تحويل السياسات

ينشئ معالج الترحيل سياسة Kaspersky Endpoint Security جديدة حيث سيتم ترحيل إعدادات سياسة Kaspersky Endpoint Agent إليها. وفي قائمة السياسات، حدد سياسات Kaspersky Endpoint Agent التي تريد نقل إعداداتها إلى سياسة Kaspersky Endpoint Security. انتقل إلى الخطوة التالية.

سيبدأ معالج الترحيل بعد ذلك في تحويل السياسات. وأثناء تحويل السياسة، يطالبك معالج الترحيل بقبول بيان Kaspersky Security Network. وسيتم تسمية السياسات الجديدة <Policy name> (محوّلة).

الخطوة 3. تحويل المهام

تخط هذه الخطوة. ويدعم المعالج مهام Kaspersky Endpoint Detection and Response Optimum وKaspersky Sandbox فقط. وتتوافر إدارة هذه المكونات فقط في Web Console. انتقل إلى الخطوة التالية.

الخطوة 4. اكتمال المعالج

أغلق المعالج. ونتيجة للمعالج، سيتم إنشاء سياسة Kaspersky Endpoint Security جديدة.

ترحيل تكوين [KES+KEA] إلى تكوين [KES+العامل المضمن]

يتضمن Kaspersky Endpoint Security عوامل مضمنة للعمل مع حلول Detection and Response. ولم تعد بحاجة إلى تطبيق Kaspersky Endpoint Agent منفصل للعمل مع هذين الحلين. وعند نشر Kaspersky Endpoint Security على أجهزة الكمبيوتر المُثبت عليها Kaspersky Endpoint Agent، ستستمر حلول Detection and Response في العمل مع Kaspersky Endpoint Security. بالإضافة إلى ذلك، تتم إزالة Kaspersky Endpoint Agent من الكمبيوتر.

تتضمن مجموعة أدوات التوزيع لتطبيق Kaspersky Endpoint Security الإصدارات 11.2.0 - 11.8.0 مكون Kaspersky Endpoint Agent. ويمكنك تحديد Kaspersky Endpoint Agent عند تثبيت Kaspersky Endpoint Security for Windows. نتيجة لذلك، سيتم تثبيت تطبيقين على جهاز الكمبيوتر الخاص بك: KEA وKES. في Kaspersky Endpoint Security 11.9.0، لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من مجموعة توزيع Kaspersky Endpoint Security.

يتضمن ترحيل تكوين [KES+KEA] إلى [KES+العامل المضمن] الخطوات التالية:

1. **ترقية Kaspersky Security Center**

   ترقية كل مكونات Kaspersky Security Center إلى الإصدار 13.2 أو أحدث، بما في ذلك عامل الإدارة: على أجهزة كمبيوتر المستخدم ووحدة تحكم الويب.

2. **ترقية المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security**

   في Kaspersky Security Center Web Console، ترقية المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security إلى الإصدار 11.7.0 أو أحدث. ولإدارة مكوني EDR Optimum وKaspersky Sandbox، يجب عليك استخدام وحدة تحكم الويب.

   لاستخدام Kaspersky Anti Targeted Attack Platform (EDR)، ستحتاج إلى مكون ويب إضافي للإصدار 12.1 من Kaspersky Endpoint Security أو أحدث.

3. **ترحيل السياسة والمهام**

   استخدم معالج ترحيل سياسة ومهام Kaspersky Endpoint Agent لترحيل إعدادات Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows.

   ينشئ هذا سياسة Kaspersky Endpoint Security جديدة. وتكون حالة السياسة الجديدة Inactive. ولتطبيق السياسة، افتح خصائص السياسة، واقبل بيان Kaspersky Security Network واضبط الحالة على Active.

4. **وظيفة الترخيص**

   إذا كنت تستخدم ترخيص Kaspersky Endpoint Detection and Response Optimum أو Kaspersky Optimum Security لتفعيل Kaspersky Endpoint Security لنظام التشغيل Windows وKaspersky Endpoint Agent، فسيتم تفعيل وظيفة EDR Optimum تلقائيًا بعد ترقية التطبيق إلى الإصدار 11.7.0. ولست بحاجة إلى فعل أي شيء آخر.

   إذا كنت تستخدم ترخيص المكون الإضافي Kaspersky Endpoint Detection and Response Optimum مستقلاً لتفعيل وظيفة EDR Optimum، فيجب عليك التأكد من إضافة مفتاح EDR Optimum إلى مستودع Kaspersky Security Center وتمكين وظيفة توزيع مفتاح الترخيص التلقائي. وبعد ترقية التطبيق إلى الإصدار 11.7.0، يتم تفعيل وظيفة EDR Optimum تلقائيًا.

   إذا كنت تستخدم ترخيص Kaspersky Endpoint Detection and Response Optimum أو Kaspersky Optimum Security لتفعيل Kaspersky Endpoint Agent، وترخيصًا مختلفًا لتفعيل Kaspersky Endpoint Security for Windows، فيجب عليك استبدال مفتاح Kaspersky Endpoint Security for Windows ليحل محله مفتاح Kaspersky Endpoint Detection المشترك ومفتاح Response Optimum أو Kaspersky Optimum Security. يمكنك استبدال المفتاح باستخدام مهمة Add key.

   لا تحتاج إلى تفعيل وظيفة Kaspersky Sandbox. وستتوفر وظيفة Kaspersky Sandbox فور ترقية وتفعيل Kaspersky Endpoint Security for Windows.

   يمكن استخدام ترخيص Kaspersky Anti Targeted Attack Platform فقط لتفعيل Kaspersky Endpoint Security كجزء من حل Kaspersky Anti Targeted Attack Platform. وبعد ترقية التطبيق إلى الإصدار 12.1، يتم تفعيل وظيفة EDR (KATA) تلقائيًا. ولست بحاجة إلى فعل أي شيء آخر.

5. **ترقية تطبيق Kaspersky Endpoint Security**

   لترقية التطبيق وترحيل وظائف EDR Optimum وKaspersky Sandbox، يوصى بمهمة التثبيت عن بُعد.

   ولترقية التطبيق باستخدام مهمة التثبيت عن بُعد، يجب عليك تحرير الإعدادات التالية:

   - حدد مكونات حلول Detection and Response في إعدادات حزمة التثبيت.
   - قم باستثناء مكون Kaspersky Endpoint Agent في إعدادات حزمة التثبيت (لتطبيق Kaspersky Endpoint Security for Windows الإصدارات 11.2.0 - 11.8.0).

يمكنك أيضًا ترقية التطبيق باستخدام الطرق التالية:

- استخدام خدمة التحديث من Kaspersky (التحديث المستمر - SMU).
- محليًا، عن طريق استخدام معالج الإعداد.

يدعم Kaspersky Endpoint Security تحديد المكونات تلقائيًا عند ترقية التطبيق على جهاز كمبيوتر مُثبت عليه تطبيق Kaspersky Endpoint Agent. ويعتمد التحديد التلقائي للمكونات على أذونات حساب المستخدم الذي ينفذ ترقية التطبيق.

إذا كنت تقوم بترقية Kaspersky Endpoint Security باستخدام ملف EXE أو MSI تحت حساب النظام (SYSTEM)، فإن Kaspersky Endpoint Security يكتسب الوصول إلى التراخيص الحالية لحلول Kaspersky. ولذلك، إذا كان الكمبيوتر مُثبتًا عليه على سبيل المثال، Kaspersky Endpoint Agent وتم تفعيل حل EDR Optimum، فإن برنامج تثبيت Kaspersky Endpoint Security يكوّن تلقائيًا مجموعة المكونات ويحدد مكون EDR Optimum. ويؤدي هذا إلى تبديل Kaspersky Endpoint Security إلى استخدام العامل المضمن ويزيل Kaspersky Endpoint Agent. ويتم عادة تشغيل مُثبّت MSI تحت حساب النظام (SYSTEM) عند الترقية عبر خدمة تحديث Kaspersky (SMU) أو عند نشر حزمة تثبيت عبر Kaspersky Security Center.

إذا كنت تنفذ ترقية Kaspersky Endpoint Security باستخدام ملف MSI تحت حساب مستخدم غير ذي امتيازات، فإن Kaspersky Endpoint Security يفتقر إلى الوصول إلى التراخيص الحالية لحلول Kaspersky. وفي هذه الحالة، يحدد Kaspersky Endpoint Security تلقائيًا المكونات بناءً على تكوين Kaspersky Endpoint Agent. وبعد ذلك، يقوم Kaspersky Endpoint Security بالتبديل إلى استخدام العامل المضمن ويزيل Kaspersky Endpoint Agent.

6. **إعادة تشغيل الكمبيوتر**

أعد تشغيل الكمبيوتر لإنهاء ترقية التطبيق باستخدام العامل المضمن. عند ترقية التطبيق، يزيل المثبّت Kaspersky Endpoint Agent قبل إعادة تشغيل الكمبيوتر. بعد إعادة تشغيل الكمبيوتر، يضيف المُثبت العامل المضمن. ويعني هذا أن Kaspersky Endpoint Security لا يؤدي وظائف EDR وKaspersky Sandbox حتى يتم إعادة تشغيل الكمبيوتر.

7. **التحقق من صحة Kaspersky Endpoint Detection and Response Optimum وKaspersky Sandbox**

إذا كانت حالة الكمبيوتر بعد الترقية هي Critical في Kaspersky Security Center console:

- تأكد من تثبيت عامل الإدارة الإصدار 13.2 أو أحدث.
- تحقق من حالة تشغيل العامل المُضمن عن طريق عرض Application components status report. إذا كانت حالة أحد المكونات Not installed ، فقم بتثبيت المكونات باستخدام مهمة Change application components.
- تأكد من قبولك لبيان Kaspersky Security Network في السياسة الجديدة لتطبيق Kaspersky Endpoint Security for Windows.
- تأكد من تفعيل وظيفة EDR Optimum باستخدام Application components status report. وإذا كانت حالة مكون ما غير مشمول بالترخيص ، فتأكد من تشغيل وظيفة توزيع مفتاح الترخيص التلقائي لمكون EDR Optimum.

Managed Detection and Response

بدءًا من الإصدار 11.6.0، يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا لحل Managed Detection and Response. يكتشف حل Kaspersky Managed Detection and Response (MDR) تلقائيًا ويحلل الحوادث الأمنية في البنية التحتية الخاصة بك. ولفعل ذلك، يستخدم MDR بيانات القياس عن بُعد الواردة من نقاط النهاية والتعلم الآلي. ويرسل MDR بيانات الحادث إلى خبراء Kaspersky. ويستطيع الخبراء بعد ذلك معالجة الحادث، وعلى سبيل المثال، إضافة إدخال جديد إلى قواعد بيانات مكافحة الفيروسات. وبدلاً من ذلك، يستطيع الخبراء إصدار توصيات بشأن معالجة الحادث، وعلى سبيل المثال، اقتراح عزل الكمبيوتر من الشبكة. وللحصول على معلومات مفصلة حول طريقة عمل الحل، يرجى الرجوع إلى تعليمات Kaspersky Managed Detection and Response.

التكامل مع MDR

لإعداد التكامل مع Kaspersky Managed Detection and Response، يجب عليك تمكين مكون Managed Detection and Response وتكوين Kaspersky Endpoint Security.

يجب عليك تمكين المكونات التالية لكي يعمل مكون Managed Detection and Response:

- Kaspersky Security Network (الوضع الموسع).
- اكتشاف السلوك.

تمكين هذه المكونات غير اختياري. وبخلاف ذلك، لا يستطيع مكون Kaspersky Managed Detection and Response العمل لأنه لا يتلقى بيانات القياس عن بُعد المطلوبة.

بالإضافة إلى ذلك، يستخدم مكون Kaspersky Managed Detection and Response البيانات الواردة من مكونات التطبيق الأخرى. تمكين هذه المكونات اختياري. تتضمن المكونات التي توفر بيانات إضافية ما يلي:

- الحماية من تهديدات الويب.
- الحماية من تهديدات البريد.
- جدار الحماية.

لكي يعمل Kaspersky Managed Detection and Response مع Administration Server عبر Kaspersky Security Center Web Console، يجب عليك أيضًا إنشاء اتصال آمن جديد، اتصال في الخلفية. ويطالبك Kaspersky Managed Detection and Response بإنشاء اتصال في الخلفية عند نشر الحل. تأكد من إنشاء اتصال في الخلفية. وللحصول على تفاصيل حول تكامل Kaspersky Security Center مع حلول Kaspersky الأخرى، يرجى الرجوع إلى تعليمات Kaspersky Security Center.

يتكون التكامل مع Kaspersky Managed Detection and Response من الخطوات التالية:

1. **تكوين Kaspersky Private Security Network**

تخط هذه الخطوة إذا كنت تستخدم Kaspersky Security Center Cloud Console. ويتولى Kaspersky Security Center Cloud Console تلقائيًا تكوين Kaspersky Private Security Network عند تثبيت المكون الإضافي MDR.

Kaspersky Private Security Network عبارة عن حل يتيح لمستخدمي أجهزة الكمبيوتر التي تستضيف Kaspersky Endpoint Security أو غيره من تطبيقات Kaspersky الحصول على حق الوصول إلى قواعد بيانات السمعة من Kaspersky، وإلى البيانات الإحصائية الأخرى دون إرسال بيانات إلى Kaspersky من أجهزة الكمبيوتر الخاصة بهم.

تحميل ملف تكوين Kaspersky Security Network في خصائص خادم الإدارة. ويوجد ملف تكوين Kaspersky Security Network داخل أرشيف ZIP الخاص بملف تكوين MDR. ويمكنك الحصول على أرشيف ZIP في لوحة تحكم Kaspersky Managed Detection and Response. وللحصول على التفاصيل عن تكوين Kaspersky Private Security Network، يرجى الرجوع إلى تعليمات Kaspersky Security Center. ويمكنك أيضًا تحميل ملف تكوين Kaspersky Security Network على الكمبيوتر من سطر الأوامر (انظر التعليمات أدناه).

كيفية تكوين Kaspersky Private Security Network من سطر الأوامر

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.

2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.

3. قم بتشغيل الأمر التالي:

```
avp.com KSN /private <file name>
```

حيث <اسم الملف> هو اسم ملف التكوين الذي يحتوي على إعدادات Kaspersky Private Security Network (تنسيق الملف PKCS7 أو PEM).

مثال:

```
avp.com KSN /private C:\kpsn_config.pkcs7
```

نتيجة لذلك، سيستخدم Kaspersky Endpoint Security شبكة Kaspersky Private Security Network لتحديد سمعة الملفات والتطبيقات ومواقع الويب. سيعرض قسم **Kaspersky Security Network** في إعدادات السياسة حالة التشغيل التالية: موفر خدمة KSN: Kaspersky Private Security Network.

يجب عليك تمكين وضع KSN الموسع لكي يعمل مكون Managed Detection and Response.

2 تمكين مكون Managed Detection and Response

قم بتحميل ملف تكوين BLOB في سياسة Kaspersky Endpoint Security (انظر التعليمات أدناه). ويحتوي ملف BLOB على معرّف العميل ومعلومات حول ترخيص Kaspersky Managed Detection and Response. ويوجد ملف BLOB داخل أرشيف ZIP الخاص بملف تكوين MDR. ويمكنك الحصول على أرشيف ZIP في لوحة تحكم Kaspersky Managed Detection and Response. وللحصول على معلومات تفصيلية عن ملف BLOB، يرجى الرجوع إلى تعليمات Kaspersky Managed Detection and Response.

كيفية تمكين مكون Managed Detection and Response في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **Detection and Response** ← **Managed Detection and Response**.

5. حدد خانة الاختيار **Managed Detection and Response**.

6. في القسم **الإعدادات**، انقر فوق **استيراد** وحدد ملف BLOB المستلم في وحدة تحكم Kaspersky Managed Detection and Response. يكون امتداد الملف P7.

7. احفظ تغييراتك.

كيفية تكوين مكون Managed Detection and Response في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response** ← **Managed Detection and Response**.

5. قم بتشغيل مفتاح **Managed Detection and Response**.

6. انقر فوق **Import** وحدد ملف BLOB الذي تم الحصول عليه في وحدة تحكم Kaspersky Managed Detection and Response. يكون امتداد الملف P7.

7. احفظ تغييراتك.

كيفية تمكين مكون Managed Detection and Response من سطر الأوامر

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.

2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.

3. قم بتشغيل الأمر التالي:

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **تكوين إعدادات التطبيق**.

نتيجة لذلك، سوف يتحقق Kaspersky Endpoint Security من ملف BLOB. ويتضمن التحقق من ملف BLOB التحقق من التوقيع الرقمي ومدة الترخيص. وفي حالة التحقق من ملف BLOB بنجاح، سوف يقوم Kaspersky Endpoint Security بتحميل الملف وإرسال الملف إلى الكمبيوتر أثناء المزامنة التالية مع Kaspersky Security Center. تحقق من حالة تشغيل المكون عن طريق عرض تقرير حالة مكونات التطبيق. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Managed Detection and Response** إلى قائمة مكونات Kaspersky Endpoint Security.

الترحيل من Kaspersky Endpoint Agent

يدعم الإصدار 11 من Kaspersky Endpoint Security والإصدارات الأحدث حل MDR. ترسل الإصدارات 11 - 11.5.0 من Kaspersky Endpoint Security بيانات القياس عن بُعد فقط إلى مكون Kaspersky Managed Detection and Response لتمكين اكتشاف التهديدات. ويحتوي الإصدار 11.6.0 من Kaspersky Endpoint Security على جميع وظائف العامل المضمن (Kaspersky Endpoint Agent).

إذا كنت تستخدم Kaspersky Endpoint Security 11 - 11.5.0، فيجب عليك تحديث قواعد البيانات إلى أحدث إصدار للعمل مع حل MDR. ويجب عليك أيضًا تثبيت Kaspersky Endpoint Agent.

إذا كنت تستخدم Kaspersky Endpoint Security 11.6.0 أو إصدارًا أحدث، فلن تحتاج إلى تثبيت Kaspersky Endpoint Agent لاستخدام حل MDR.

للترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows:

1. كوّن التكامل مع Kaspersky Managed Detection and Response في سياسة Kaspersky Endpoint Security.

2. قم بتعطيل مكون Managed Detection and Response في سياسة Kaspersky Endpoint Agent.

إذا كانت سياسة Kaspersky Endpoint Security تنطبق أيضًا على أجهزة الكمبيوتر التي لم يتم تثبيت Kaspersky Endpoint Security 11 – 11.5.0 عليها، فيجب عليك أولاً إنشاء سياسة Kaspersky Endpoint Agent منفصلة لأجهزة الكمبيوتر هذه. وفي السياسة الجديدة، كوّن التكامل مع Kaspersky Managed Detection and Response.

Endpoint Detection and Response

بدءًا من الإصدار 11.7.0، يتضمن Kaspersky Endpoint Security for Windows عاملًا مضمنًا لحل Kaspersky Endpoint Detection and Response Optimum (يشار إليه فيما يلي أيضًا باسم "EDR Optimum"). وبدءًا من الإصدار 11.8.0، يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا لحل Kaspersky Endpoint Detection and Response Expert (يشار إليه فيما يلي أيضًا باسم "EDR Expert"). ويعد Kaspersky Endpoint Detection and Response مجموعة حلول لحماية البنية التحتية لتكنولوجيا المعلومات في الشركة من التهديدات الإلكترونية المتقدمة. وتجمع وظائف الحلول بين الاكتشاف التلقائي للتهديدات والقدرة على الرد على هذه التهديدات لمواجهة الهجمات المتقدمة بما في ذلك عمليات الاستغلال الجديدة وبرامج الفدية والهجمات الخالية من الملفات، بالإضافة إلى الأساليب التي تستخدم أدوات النظام المشروعة. ويوفر EDR Expert وظائف أكثر لرصد التهديدات والاستجابة لها من EDR Optimum. وللحصول على التفاصيل عن الحلول، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

يراجع حل Kaspersky Endpoint Detection and Response ويحلل تطور التهديدات ويزود أفراد الأمن أو المسؤول بمعلومات حول الهجوم المحتمل اللازمة للاستجابة في وقت مناسب. يعرض Kaspersky Endpoint Detection and Response تفاصيل الاكتشاف في نافذة منفصلة. تفاصيل الاكتشاف عبارة عن أداة لعرض كامل المعلومات التي تم جمعها حول التهديد المكتشف. وتتضمن تفاصيل الاكتشاف، على سبيل المثال، محفوظات الملفات التي تظهر على الكمبيوتر. وللحصول على التفاصيل عن إدارة تفاصيل الاكتشاف، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

يستخدم Kaspersky Endpoint Detection and Response أدوات معلومات التهديدات التالية:

- البنية التحتية السحابية لشبكة Kaspersky Security Network (المشار إليها فيما يلي أيضًا باسم "KSN")، التي توفر الوصول إلى معلومات سمعة البرامج وموقع الويب والملف في الوقت الحقيقي من قاعدة معارف Kaspersky. ويضمن استخدام البيانات من Kaspersky Security Network استجابات أسرع من قبل تطبيقات Kaspersky للتهديدات، ويحسن أداء بعض مكونات الحماية، ويقلل من احتمالية الاكتشافات الإيجابية الزائفة. يستخدم EDR Expert حل Kaspersky Private Security Network (KPSN)، الذي يرسل البيانات إلى خوادم إقليمية دون إرسال البيانات من الأجهزة إلى شبكة KSN.
- التكامل مع Kaspersky Threat Intelligence Portal، الذي يحتوي على معلومات عن سمعة الملفات وعناوين الويب ويعرضها.
- قاعدة بيانات التهديدات الخاصة بشركة Kaspersky.
- تقنية Cloud Sandbox التي تتيح لك تشغيل الملفات المكتشفة في بيئة معزولة والتحقق من سمعتها.

التكامل مع Kaspersky Endpoint Detection and Response

للتكامل مع Kaspersky Endpoint Detection and Response، يجب إضافة مكون Endpoint Detection and Response Optimum (EDR Optimum)) أو مكون Endpoint Detection and Response Expert (EDR Expert) وتكوين Kaspersky Endpoint Security.

لا تتوافق المكونات EDR Optimum وEDR Expert وKATA (EDR) مع بعضها البعض.

يجب استيفاء الشروط التالية لكي يعمل Endpoint Detection and Response:

- Kaspersky Security Center الإصدار 13.2 أو أحدث. في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة Endpoint Detection and Response.
- يمكن إدارة EDR Optimum في Kaspersky Security Center Web Console وKaspersky Security Center Cloud Console.

  يمكن إدارة EDR Expert فقط باستخدام Kaspersky Security Center Web Console. لا يمكنك إدارة هذه الوظيفة باستخدام وحدة تحكم الإدارة (MMC).
- تم تفعيل التطبيق ويغطي الترخيص الوظيفة.
- تم تشغيل مكون Endpoint Detection and Response.
- يتم تمكين وتشغيل مكونات التطبيق التي يعتمد عليها Endpoint Detection and Response. ويعتمد Endpoint Detection and Response على المكونات التالية:
  - الحماية من تهديدات الملفات.
  - الحماية من تهديدات الويب.
  - الحماية من تهديدات البريد.
  - منع الاستغلال.
  - اكتشاف السلوك.
  - منع اختراق المضيف.
  - محرك المعالجة.
  - مراقبة عيوب التكيف.

يتكون التكامل مع Kaspersky Endpoint Detection and Response من الخطوات التالية:

1. **تثبيت مكون Endpoint Detection and Response**

   يمكنك تحديد مكون EDR Optimum or EDR Expert أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

   يجب إعادة تشغيل الكمبيوتر لإنهاء ترقية التطبيق بالمكونات الجديدة.

2. **تفعيل Kaspersky Endpoint Detection and Response**

   يمكنك الحصول على ترخيص لاستخدام Kaspersky Endpoint Detection and Response بالطرق التالية:

   - يتم تضمين وظائف Endpoint Detection and Response في ترخيص Kaspersky Endpoint Security for Windows.

     ستتوفر الميزة فور تفعيل Kaspersky Endpoint Security for Windows.
   - شراء ترخيص منفصل لمكون EDR Optimum أو EDR Expert (الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response).

     ستتوفر الميزة بعد إضافة مفتاح منفصل لحل Kaspersky Endpoint Detection and Response. ونتيجة لذلك، يتم تثبيت مفتاحين على الكمبيوتر: مفتاح لحل Kaspersky Endpoint Security ومفتاح لحل Kaspersky Endpoint Detection and Response.

     الترخيص لوظيفة Endpoint Detection and Response المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

   تأكد من تضمين وظيفة EDR Optimum أو EDR Expert في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

3. **تمكين مكون Endpoint Detection and Response**

يمكنك تمكين أو تعطيل المكون في إعدادات سياسة Kaspersky Endpoint Security for Windows.

كيفية تمكين أو تعطيل مكون Endpoint Detection and Response في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Endpoint Detection and Response ← Detection and Response**.
5. قم بتشغيل مفتاح **Endpoint Detection and Response**.
6. احفظ تغييراتك.

يتم تمكين مكون Kaspersky Endpoint Detection and Response. تحقق من حالة تشغيل المكون عن طريق عرض تقرير حالة مكونات التطبيق. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Endpoint Detection and Response Optimum** أو **Endpoint Detection and Response Expert** إلى قائمة مكونات Kaspersky Endpoint Security.

4 **تمكين نقل البيانات إلى خادم الإدارة**

لتمكين كل ميزات Endpoint Detection and Response، يجب تمكين النقل لأنواع البيانات التالية:

- بيانات ملف العزل.

  البيانات مطلوبة للحصول على معلومات حول الملفات المعزولة على جهاز كمبيوتر من خلال Web Console وCloud Console. على سبيل المثال، يمكنك تنزيل ملف من العزل للتحليل في Web Console وCloud Console.

- بيانات سلسلة تطور التهديد.

  البيانات مطلوبة للحصول على معلومات عن التهديدات المكتشفة على جهاز كمبيوتر في Web Console وCloud Console. ويمكنك عرض تفاصيل الاكتشاف واتخاذ إجراءات الاستجابة في Web Console وCloud Console.

كيفية تمكين نقل البيانات إلى خادم الإدارة في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Reports and Storage ← General settings**.
5. يرجى اختيار الخانات التالية في القسم **Data transfer to Administration Server**:
   - **About Quarantine files**.
   - **About a threat development chain**.
6. احفظ تغييراتك.

الترحيل من Kaspersky Endpoint Agent

إذا كنت تستخدم Kaspersky Endpoint Security 11.7.0 أو أحدث مع تثبيت مكون EDR Optimum (العامل المضمن)، يتوفر دعم التكامل مع حل Kaspersky Endpoint Detection and Response Optimum فورًا بعد التثبيت. لا يتوافق مكون EDR Optimum مع Kaspersky Endpoint Agent. في حالة تثبيت Kaspersky Endpoint Agent على الكمبيوتر، عند تحديث Kaspersky Endpoint Security إلى الإصدار 11.7.0 ، يستمر Kaspersky Endpoint Detection and Response Optimum في العمل مع Kaspersky Endpoint Security (ترحيل تكوين [KES+KEA] إلى [KES+العامل المضمن]). بالإضافة إلى ذلك، ستتم إزالة Kaspersky Endpoint Agent من الكمبيوتر. ولإكمال الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows، تحتاج إلى نقل إعدادات السياسة والمهام باستخدام معالج الترحيل.

إذا كنت تستخدم Kaspersky Endpoint Security 11.4.0–11.6.0 لإمكانية التشغيل التفاعلي مع Kaspersky Endpoint Detection and Response Optimum، فإن التطبيق يتضمن Kaspersky Endpoint Agent. يمكنك تثبيت Kaspersky Endpoint Agent مع تثبيت Kaspersky Endpoint Security.

تتضمن مجموعة أدوات التوزيع لتطبيق Kaspersky Endpoint Security الإصدارات 11.2.0 - 11.8.0 مكون Kaspersky Endpoint Agent. ويمكنك تحديد Kaspersky Endpoint Agent عند تثبيت Kaspersky Endpoint Security for Windows. نتيجة لذلك، سيتم تثبيت تطبيقين على جهاز الكمبيوتر الخاص بك: KEA وKES. في Kaspersky Endpoint Security 11.9.0، لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من مجموعة توزيع Kaspersky Endpoint Security.

لا يدعم حل Kaspersky Endpoint Detection and Response Expert قابلية التشغيل التبادلي مع Kaspersky Endpoint Agent. ويستخدم حل Kaspersky Endpoint Detection and Response Expert تطبيق Kaspersky Endpoint Security مع العامل المدمج (الإصدار 11.8.0 وأحدث).

يدعم مكون EDR Optimum كجزء من Kaspersky Endpoint Security التفاعل مع حل Kaspersky Endpoint Detection and Response Optimum 2.0. ولا يتم دعم التفاعل مع Kaspersky Endpoint Detection and Response Optimum الإصدار 1.0.

الفحص للبحث عن مؤشرات الاختراق (مهمة قياسية).

مؤشر الاختراق (IOC) عبارة عن مجموعة من البيانات حول كائن أو نشاط يشير إلى وصول غير مصرح به إلى الكمبيوتر (اختراق البيانات). على سبيل المثال، من الممكن أن تشكل العديد من المحاولات الفاشلة لتسجيل الدخول إلى النظام مؤشرًا على الاختراق. تتيح مهمة فحص IOC العثور على مؤشرات الاختراق على الكمبيوتر واتخاذ إجراءات الاستجابة للتهديدات.

يبحث Kaspersky Endpoint Security عن مؤشرات الاختراق باستخدام ملفات IOC. ملفات IOC هي ملفات تحتوي على مجموعات المؤشرات التي يحاول التطبيق مطابقتها لإحصاء الاكتشاف. ويجب أن تتوافق ملفات IOC مع معيار OpenIOC.

وضع تشغيل مهمة فحص IOC

يتيح لك Kaspersky Endpoint Detection and Response إنشاء مهام فحص IOC قياسية لاكتشاف البيانات المخترقة. مهمة فحص IOC القياسية هي مجموعة أو مهمة محلية يتم إنشاؤها وتكوينها يدويًا في Web Console. ويتم تشغيل المهام باستخدام ملفات IOC التي أعدها المستخدم. إذا كنت ترغب في إضافة مؤشر الاختراق يدويًا، فيرجى قراءة متطلبات ملفات IOC.

يحتوي الملف الذي يمكنك تنزيله بالنقر فوق الارتباط أدناه على جدول يحتوي على قائمة كاملة بشروط IOC لمعيار OpenIOC.

تنزيل ملف DOWNLOAD THE IOC_TERMS.XLSX

يدعم Kaspersky Endpoint Security أيضًا مهام مسح IOC المستقلة عند استخدام التطبيق كجزء من حل Kaspersky Sandbox.

إنشاء مهمة فحص IOC

تستطيع إنشاء مهام فحص IOC يدويًا:

- في تفاصيل التنبيه (لتطبيق EDR Optimum فقط).

تفاصيل الاكتشاف عبارة عن أداة لعرض كامل المعلومات التي تم جمعها حول التهديد المكتشف. وتتضمن تفاصيل الاكتشاف، على سبيل المثال، محفوظات الملفات التي تظهر على الكمبيوتر. وللحصول على التفاصيل عن إدارة تفاصيل الاكتشاف، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

- استخدام معالج المهام.

يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة فحص IOC:

1. في النافذة الرئيسية لـ Web Console، حدد **Tasks** ← **Devices**.
تفتح قائمة المهام.
2. انقر على الزر **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.
   b. في القائمة المنسدلة **Task type** حدد **IOC Scan**.
   c. في الحقل **Task name**، أدخل وصفًا مختصرًا.
   d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.
5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انتقل إلى الخطوة التالية.

افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

لا يمتلك حساب النظام (SYSTEM) إذنًا لأداء مهمة فحص IOC على محركات أقراص الشبكة. وإذا كنت تريد تشغيل المهمة لمحرك أقراص الشبكة، فحدد حساب المستخدم الذي يمتلك حق الوصول إلى محرك الأقراص هذا.

لمهام فحص IOC المستقلة على محركات أقراص الشبكة، في خصائص المهمة، تحتاج إلى تحديد حساب المستخدم الذي يمتلك حق الوصول إلى محرك الأقراص هذا يدويًا.

6. أغلق المعالج.
سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.

نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. انتقل إلى القسم **IOC scan settings**.

10. قم بتحميل ملفات IOC للبحث عن مؤشرات الاختراق.

بعد تحميل ملفات IOC، يمكنك عرض قائمة المؤشرات من ملفات IOC.

لا يوصى بإضافة ملفات IOC أو إزالتها بعد تشغيل المهمة. ومن الممكن أن يتسبب هذا في عرض نتائج فحص IOC بشكل غير صحيح لعمليات التشغيل السابقة للمهمة. وللبحث في مؤشرات الاختراق حسب ملفات IOC الجديدة، يوصى بإضافة مهام جديدة.

11. تكوين الإجراءات عند اكتشاف IOC:

- **Isolate computer from the network**. في حالة تحديد هذا الخيار، يعزل Kaspersky Endpoint Security الكمبيوتر من الشبكة لمنع انتشار التهديد. ويمكنك تكوين مدة العزل في إعدادات مكون Endpoint Detection and Response.
- **Move copy to Quarantine, delete object**. في حالة تحديد هذا الخيار، يحذف Kaspersky Endpoint Security الكائن الضار الموجود على الكمبيوتر. قبل حذف الكائن، يُنشئ Kaspersky Endpoint Security نسخة احتياطية في حالة الحاجة إلى استعادة الكائن لاحقًا. ينقل Kaspersky Endpoint Security النسخة الاحتياطية إلى العزل.
- **Run scan of critical areas**. في حالة تحديد هذا الخيار، يُشغل Kaspersky Endpoint Security مهمة فحص المناطق الحرجة. بشكلٍ افتراضي، يفحص Kaspersky Endpoint Security ذاكرة kernel والعمليات قيد التشغيل وقطاعات تمهيد القرص.

12. انتقل إلى القسم **Advanced**.

13. حدد أنواع البيانات (مستندات IOC) التي يجب تحليلها كجزء من المهمة.

يحدد Kaspersky Endpoint Security تلقائيًا أنواع البيانات (مستندات IOC) لمهمة فحص IOC وفقًا لمحتوى ملفات IOC الذي تم تحميله. ولا يوصى بإلغاء تحديد أنواع البيانات.

يمكنك أيضًا تكوين نطاقات الفحص لأنواع البيانات التالية:

- **Files - FileItem**. قم بتعيين نطاق فحص IOC على الكمبيوتر باستخدام نطاقات محددة مسبقًا.

  بشكل افتراضي، يبحث Kaspersky Endpoint Security عن مهام IOC فقط في المناطق المهمة على الكمبيوتر، مثل مجلد التنزيلات وسطح المكتب والمجلد الذي يحتوي على ملفات نظام التشغيل المؤقتة، وما إلى ذلك. ويمكنك أيضًا إضافة نطاق الفحص يدويًا.

- **Windows event logs - EventLogItem**. أدخل الفترة الزمنية التي تم تسجيل الأحداث فيها. يمكنك أيضًا تحديد سجلات أحداث Windows التي يجب استخدامها لفحص IOC. وبشكل افتراضي، يتم تحديد سجلات الأحداث التالية: سجل أحداث التطبيق وسجل أحداث النظام وسجل أحداث الأمان.

لنوع البيانات **Windows registry - RegistryItem**، يفحص Kaspersky Endpoint Security مجموعة من مفاتيح التسجيل.

14. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

15. تكوين جدول المهمة.

لا يتوفر التشغيل عن بُعد عبر الشبكة المحلية لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

16. احفظ تغييراتك.

17. حدد خانة الاختيار المجاورة للمهمة.

18. انقر على الزر **Run**.

نتيجة لذلك، يقوم Kaspersky Endpoint Security بتشغيل البحث عن مؤشرات الاختراق على الكمبيوتر. ويمكنك عرض نتائج المهمة في خصائص المهمة في القسم **Results**. ويمكنك عرض المعلومات حول المؤشرات المكتشفة للاختراق في خصائص المهمة: **Application settings** ← **IOC Scan Results**.

يتم الاحتفاظ بنتائج فحص IOC لمدة 30 يومًا. وبعد هذه الفترة، يحذف برنامج Kaspersky Endpoint Security تلقائيًا الإدخالات القديمة.

نقل الملف إلى العزل

عند الرد على التهديدات، يستطيع مكون Kaspersky Endpoint Detection and Response إنشاء مهام نقل الملف إلى العزل. وهذا ضروري لتقليل عواقب التهديد. العزل هو مخزن محلي خاص على الكمبيوتر. ويستطيع المستخدم عزل الملفات التي يعتبرها المستخدم خطرة على جهاز الكمبيوتر. ويتم تخزين الملفات المعزولة في حالة مشفرة ولا تهدد أمن الجهاز. ولا يستخدم Kaspersky Endpoint Security العزل إلا عند العمل مع حلول Detection and Response: EDR Optimum وEDR Expert (EDR) وKATA) وKaspersky Sandbox. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل حول إدارة العزل كجزء من الحلول، يرجى الرجوع إلى تعليمات Kaspersky Sandbox وتعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert وتعليمات Kaspersky Anti Targeted Attack Platform.

تستطيع أن تنشئ مهام نقل الملف إلى العزل بالطرق التالية:

- في تفاصيل التنبيه (لتطبيق EDR Optimum فقط).

  تفاصيل الاكتشاف عبارة عن أداة لعرض كامل المعلومات التي تم جمعها حول التهديد المكتشف. وتتضمن تفاصيل الاكتشاف، على سبيل المثال، محفوظات الملفات التي تظهر على الكمبيوتر. وللحصول على التفاصيل عن إدارة تفاصيل الاكتشاف، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

- استخدام معالج المهام.

  يجب إدخال مسار الملف أو التجزئة (SHA256 أو MD5)، أو كل من مسار الملف وتجزئة الملف.

تتضمن مهمة نقل الملف إلى العزل القيود التالية:

1. يجب ألا يتجاوز حجم الملف 100 ميجابايت.

2. لا يمكن عزل كائنات النظام الحرجة (SCO). SCO هي الملفات التي يتطلبها نظام التشغيل وتطبيق Kaspersky Endpoint Security for Windows ليتمكن من العمل.

3. يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة نقل الملف إلى العزل:

1. في النافذة الرئيسية لـ Web Console، حدد **Tasks** ← **Devices**.

   تفتح قائمة المهام.

2. انقر على الزر **Add**.

   يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

   a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type** حدد **Move file to Quarantine**.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر على الزر **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر على الزر **Next**.

افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

6. قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**.

سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.

نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. في قائمة الملفات، انقر فوق **Add**.

يبدأ معالج إضافة الملف.

10. لإضافة الملف، يجب عليك إدخال المسار الكامل للملف، أو كل من التجزئة والمسار.

إذا كان الملف موجودًا على محرك أقراص شبكي، أدخل مسار الملف بدءًا من `\\`، وليس حرف محرك الأقراص. على سبيل المثال، `\\server\shared_folder\file.exe`. إذا كان مسار الملف يحتوي على حرف محرك أقراص الشبكة، فمن الممكن تلقي الخطأ لم يتم العثور على الملف.

11. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

12. تكوين جدول المهمة.

لا يتوفر التشغيل عن بُعد عبر الشبكة المحلية لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. انقر على الزر **Save**.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر على الزر **Run**.

نتيجة لذلك، ينقل Kaspersky Endpoint Security الملف إلى العزل. وفي حالة تأمين الملف من خلال عملية مختلفة، يتم عرض المهمة على أنها مكتملة، لكن يتم عزل الملف نفسه فقط بعد إعادة تشغيل الكمبيوتر. وبعد إعادة تشغيل الكمبيوتر، تأكد من حذف الملف.

من الممكن أن تنتهي مهمة نقل الملف إلى العزل بالخطأ تم رفض الوصول إذا كنت تحاول عزل ملف تنفيذي قيد التشغيل حاليًا. قم بإنشاء مهمة عملية إنهاء للملف وحاول مرة أخرى.

من الممكن أن تفشل مهمة نقل الملف إلى العزل بالخطأ لا تتوفر مساحة كافية في مخزن العزل إذا كنت تحاول عزل ملف كبير جدًا. أفرغ العزل أو قم بزيادة مساحة العزل. ثم حاول مرة أخرى.

يمكنك استعادة ملف من العزل أو إفراغ العزل باستخدام Web Console. ويمكنك استعادة الكائنات محليًا على الكمبيوتر باستخدام سطر الأوامر.

الحصول على الملف

يمكنك الحصول على الملفات من أجهزة كمبيوتر المستخدم. على سبيل المثال، يمكنك تكوين الحصول على ملف سجل أحداث تم إنشاؤه بواسطة تطبيق طرف ثالث. وللحصول على الملف، يجب عليك إنشاء مهمة مخصصة. ونتيجة لتنفيذ المهمة، يتم حفظ الملف في العزل. ويمكنك تنزيل هذا الملف من العزل إلى جهاز الكمبيوتر الخاص بك باستخدام Web Console. وعلى جهاز الكمبيوتر الخاص بالمستخدم، يظل الملف في مجلده الأصلي.

يجب ألا يتجاوز حجم الملف 100 ميجابايت.

يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة الحصول على الملف:

1. في النافذة الرئيسية لـ Web Console، حدد **Tasks** ← **Devices**.
تفتح قائمة المهام.

2. انقر على الزر **Add**.
يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type** حدد **Get file**.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر على الزر **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر على الزر **Next**.

افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

6. قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**.
سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.
نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. في قائمة الملفات، انقر فوق **Add**.
يبدأ معالج إضافة الملف.

10. لإضافة الملف، يجب عليك إدخال المسار الكامل للملف، أو كل من التجزئة والمسار.

إذا كان الملف موجودًا على محرك أقراص شبكي، أدخل مسار الملف بدءًا من `\\`، وليس حرف محرك الأقراص. على سبيل المثال، `\\server\shared_folder\file.exe`. إذا كان مسار الملف يحتوي على حرف محرك أقراص الشبكة، فمن الممكن تلقي الخطأ لم يتم العثور على الملف.

11. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

12. تكوين جدول المهمة.

لا يتوفر التشغيل عن بُعد عبر الشبكة المحلية لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. انقر على الزر **Save**.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر على الزر **Run**.

نتيجة لذلك، يُنشئ Kaspersky Endpoint Security نسخة من الملف وينقل تلك النسخة إلى العزل. ويمكنك تنزيل الملف من العزل في Web Console.

حذف الملف

يمكنك حذف الملفات عن بعد باستخدام المهمة حذف الملف. على سبيل المثال، يمكنك حذف ملف عن بُعد عند الاستجابة للتهديدات.

تتضمن مهمة حذف الملف القيود التالية:

- يتعذر حذف كائنات النظام الحرجة (SCO). SCO هي الملفات التي يتطلبها نظام التشغيل وتطبيق Kaspersky Endpoint Security for Windows ليتمكن من العمل.
- يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة حذف الملف:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.
تفتح قائمة المهام.

2. انقر على الزر **Add**.
يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type** حدد **Delete file**.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر على الزر **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر على الزر **Next**.

افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

6. قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**.

سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.

نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. في قائمة الملفات، انقر فوق **Add**.

يبدأ معالج إضافة الملف.

10. لإضافة الملف، يجب عليك إدخال المسار الكامل للملف، أو كل من التجزئة والمسار.

إذا كان الملف موجودًا على محرك أقراص شبكي، أدخل مسار الملف بدءًا من `\\`، وليس حرف محرك الأقراص. على سبيل المثال، `\\server\shared_folder\file.exe`. إذا كان مسار الملف يحتوي على حرف محرك أقراص الشبكة، فمن الممكن تلقي الخطأ لم يتم العثور على الملف.

11. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

12. تكوين جدول المهمة.

لا يتوفر التشغيل عن بُعد عبر الشبكة المحلية لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. انقر على الزر **Save**.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر على الزر **Run**.

نتيجة لذلك، يحذف Kaspersky Endpoint Security الملف من الكمبيوتر. وفي حالة تأمين الملف من خلال عملية مختلفة، يتم عرض المهمة على أنها مكتملة، لكن يتم حذف الملف نفسه فقط بعد إعادة تشغيل الكمبيوتر. وبعد إعادة تشغيل الكمبيوتر، تأكد من حذف الملف.

من الممكن أن تنتهي مهمة حذف الملف بالخطأ تم رفض الوصول إذا كنت تحاول حذف ملف تنفيذي قيد التشغيل حاليًا. قم بإنشاء مهمة عملية إنهاء للملف وحاول مرة أخرى.

بدء العملية

يمكنك تشغيل الملفات عن بعد باستخدام المهمة بدء العملية. على سبيل المثال، يمكنك تشغيل أداة مساعدة تنشئ ملف تكوين الكمبيوتر عن بُعد. بعد ذلك يمكنك استخدام المهمة الحصول على الملف لتلقي الملف الذي تم إنشاؤه في Kaspersky Security Center Web Console.

يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة بدء العملية:

1. في النافذة الرئيسية لـ Web Console، حدد **Tasks** ← **Devices**.
تفتح قائمة المهام.

2. انقر على الزر **Add**.
يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type** حدد **Start process**.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر على الزر **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر على الزر **Next**.

افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

6. قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**.
سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.

8. نافذة خصائص المهمة.

9. حدد علامة التبويب **Application settings**.

10. أدخل أمر بدء العملية.

على سبيل المثال، إذا كنت تريد تشغيل أداة مساعدة (`Utility.exe`) تحفظ المعلومات حول تكوين الكمبيوتر في ملف يسمى `conf.txt`، يجب عليك إدخال القيم التالية:

- **Executable command** – `utility.exe`
- **Command line arguments (optional)** – `/R conf.txt`
- **Path to the working folder (optional)** – `C:\Users\admin\Diagnostic\`

بدلا من ذلك، في الحقل **Executable command** ، يمكنك إدخال `C:\Users\admin\Diagnostic\utility.exe /R conf.txt`. وفي هذه الحالة لا تحتاج إلى إدخال باقي الإعدادات.

11. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

12. تكوين جدول المهمة.

لا يتوفر التشغيل عن بُعد عبر الشبكة المحلية لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. انقر على الزر **Save**.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر على الزر **Run**.

نتيجة لذلك، يقوم Kaspersky Endpoint Security بتشغيل الأمر في الوضع الصامت ويبدأ العملية. ويمكنك عرض نتائج المهمة في خصائص المهمة في القسم **Execution results**.

إنهاء العملية

يمكنك إنهاء العمليات عن بعد باستخدام المهمة إنهاء العملية. على سبيل المثال، يمكنك عن بُعد إنهاء أداة مساعدة اختبار سرعة الإنترنت التي كانت قد بدأت باستخدام المهمة تشغيل العملية.

إذا كنت تريد منع تشغيل أحد الملفات، فيمكنك تكوين مكون منع التنفيذ. ويمكنك منع تنفيذ الملفات القابلة للتنفيذ والبرامج النصية وملفات تنسيق Office.

تتضمن مهمة إنهاء العملية القيود التالية:

- يتعذر إنهاء عمليات كائنات النظام الحرجة (SCO). SCO هي الملفات التي يتطلبها نظام التشغيل وتطبيق Kaspersky Endpoint Security for Windows ليتمكن من العمل.
- يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة إنهاء العملية:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.
تفتح قائمة المهام.

2. انقر على الزر **Add**.
يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows (12.1)**.

b. في القائمة المنسدلة **Task type** حدد **Terminate process**.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا.

d. في القسم **Select devices to which the task will be assigned**، حدد نطاق المهمة.

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر على الزر **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر على الزر **Next**.

افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

6. قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**.

سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.

نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. لإكمال العملية، يجب عليك تحديد الملف الذي تريد إنهاءه. يمكنك تحديد ملف بإحدى الطرق التالية:

- أدخل الاسم الكامل للملف.
- أدخل تجزئة الملف والمسار إلى الملف.
- أدخل معرف العملية (للمهام المحلية فقط).

إذا كان الملف موجودًا على محرك أقراص شبكي، أدخل مسار الملف بدءًا من `\\`، وليس حرف محرك الأقراص. على سبيل المثال، `\\server\shared_folder\file.exe`. إذا كان مسار الملف يحتوي على حرف محرك أقراص الشبكة، فمن الممكن تلقي الخطأ لم يتم العثور على الملف.

10. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

11. تكوين جدول المهمة.

لا يتوفر التشغيل عن بُعد عبر الشبكة المحلية لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

12. انقر على الزر **Save**.

13. حدد خانة الاختيار المجاورة للمهمة.

14. انقر على الزر **Run**.

نتيجة لذلك، ينهي Kaspersky Endpoint Security العملية على الكمبيوتر. على سبيل المثال، إذا كان تطبيق "GAME" قيد التشغيل وأنهيت عملية game.exe، فسيتم إغلاق التطبيق دون حفظ البيانات. ويمكنك عرض نتائج المهمة في خصائص المهمة في القسم **Results**.

منع التنفيذ

يسمح منع التنفيذ بإدارة تشغيل الملفات القابلة للتنفيذ والبرامج النصية، بالإضافة إلى فتح ملفات تنسيق Office. وبهذه الطريقة، يمكنك ،على سبيل المثال، منع تنفيذ التطبيقات التي تعتبرها غير آمنة. نتيجة لذلك، يمكن وقف انتشار التهديد. ويدعم منع التنفيذ مجموعة من امتدادات ملفات Office ومجموعة من مترجمي البرنامج النصي.

قاعدة منع التنفيذ

يدير منع التنفيذ وصول المستخدم إلى الملفات عن طريق قواعد منع التنفيذ. قاعدة منع التنفيذ هي مجموعة من المعايير التي يضعها التطبيق في الاعتبار عند الاستجابة لتنفيذ كائن، على سبيل المثال عند منع تنفيذ الكائن. يتعرف التطبيق على الملفات حسب مساراتها أو المجاميع الاختبارية المحسوبة باستخدام خوارزميات التجزئة MD5 وSHA256.

يمكنك إنشاء قواعد منع التنفيذ:

- في تفاصيل التنبيه (لتطبيق EDR Optimum فقط).

تفاصيل الاكتشاف عبارة عن أداة لعرض كامل المعلومات التي تم جمعها حول التهديد المكتشف. وتتضمن تفاصيل الاكتشاف، على سبيل المثال، محفوظات الملفات التي تظهر على الكمبيوتر. وللحصول على التفاصيل عن إدارة تفاصيل الاكتشاف، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

- استخدام سياسة المجموعة أو إعدادات التطبيق المحلية.

يجب إدخال مسار الملف أو التجزئة (SHA256 أو MD5)، أو كل من مسار الملف وتجزئة الملف.

يمكنك أيضًا إدارة منع التنفيذ محليًا باستخدام سطر الأوامر.

يخضع منع التنفيذ للقيود التالية:

1. لا تغطي قواعد المنع الملفات الموجودة على الأقراص المضغوطة أو في صور ISO. ولا يمنع التطبيق تنفيذ أو فتح هذه الملفات.

2. من المستحيل منع بدء تشغيل كائنات النظام الحرجة (SCO). SCO هي الملفات التي يتطلبها نظام التشغيل وتطبيق Kaspersky Endpoint Security for Windows ليتمكن من العمل.

3. لا يوصى بإنشاء أكثر من 5000 قاعدة لمنع التشغيل، حيث يمكن أن يتسبب ذلك في عدم استقرار النظام.

أوضاع قاعدة منع التنفيذ

من الممكن أن يعمل مكون منع التنفيذ في وضعين:

- **الإحصائيات فقط**

في هذا الوضع، ينشر Kaspersky Endpoint Security حدثًا حول محاولات تشغيل الكائنات القابلة للتنفيذ أو فتح مستندات تطابق معايير قاعدة المنع مع سجل أحداث Windows وKaspersky Security Center، لكنها لا تمنع محاولة تشغيل أو فتح الكائن أو المستند. ويتحدد هذا الوضع بشكل افتراضي.

- **فعال**

في هذا الوضع، يحظر التطبيق تنفيذ الكائنات أو فتح المستندات التي تطابق معايير قاعدة المنع. وينشر التطبيق أيضًا حدثًا حول محاولات تنفيذ الكائنات أو فتح المستندات في سجل أحداث Windows وسجل أحداث Kaspersky Security Center.

إدارة منع التنفيذ

يمكنك تكوين إعدادات المكون فقط في Web Console.

لمنع التنفيذ:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response** ← **Endpoint Detection and Response**.

5. قم بتشغيل مفتاح **Execution Prevention ENABLED**.

6. في القسم **Action on execution or opening of forbidden object**، حدد وضع تشغيل المكون:

- **Block and write to report**. في هذا الوضع، يحظر التطبيق تنفيذ الكائنات أو فتح المستندات التي تطابق معايير قاعدة المنع. وينشر التطبيق أيضًا حدثًا حول محاولات تنفيذ الكائنات أو فتح المستندات في سجل أحداث Windows وسجل أحداث Kaspersky Security Center.

- **Log events only**. في هذا الوضع، ينشر Kaspersky Endpoint Security حدثًا حول محاولات تشغيل الكائنات القابلة للتنفيذ أو فتح مستندات تطابق معايير قاعدة المنع مع سجل أحداث Windows وKaspersky Security Center، لكنها لا تمنع محاولة تشغيل أو فتح الكائن أو المستند. ويتحدد هذا الوضع بشكل افتراضي.

7. إنشاء قائمة بقواعد منع التنفيذ:

a. انقر على **Add**.

b. يفتح هذا نافذة؛ وفي هذه النافذة، أدخل اسم قاعدة منع التنفيذ (على سبيل المثال ، التطبيق أ).

c. في القائمة المنسدلة **Type**، حدد الكائن الذي تريد منعه: **Executable file** أو **Script** أو **Microsoft Office document**.

إذا حددت نوع كائن خطأ، فلن يمنع Kaspersky Endpoint Security الملف أو البرنامج النصي.

d. لإضافة الملف، يجب عليك إدخال تجزئة الملف (SHA256 أو MD5)، أو المسار الكامل للملف، أو كل من التجزئة والمسار.

إذا كان الملف موجودًا على محرك أقراص شبكي، أدخل مسار الملف بدءًا من `\\`، وليس حرف محرك الأقراص. على سبيل المثال، `\\server\shared_folder\file.exe`. وإذا كان مسار الملف يحتوي على حرف محرك أقراص شبكة، فلن يمنع Kaspersky Endpoint Security الملف أو البرنامج النصي.

ويدعم منع التنفيذ مجموعة من امتدادات ملفات Office ومجموعة من مترجمي البرنامج النصي.

e. انقر على **OK**.

8. احفظ تغييراتك.

نتيجة لذلك، يمنع Kaspersky Endpoint Security تنفيذ الكائنات: تشغيل الملفات القابلة للتنفيذ والبرامج النصية وفتح ملفات تنسيق Office. ومع ذلك، يمكنك، على سبيل المثال، فتح ملف نصي في محرر نصوص حتى في حالة منع تشغيل البرنامج النصي. عند منع تنفيذ كائن، يعرض Kaspersky Endpoint Security إخطارًا قياسيًا (انظر الشكل أدناه) في حالة تمكين الإخطارات في إعدادات التطبيق.

إخطار منع التنفيذ

عزل شبكة الاتصال

يسمح عزل شبكة الاتصال الخاصة بالكمبيوتر تلقائيًا بعزل كمبيوتر عن الشبكة استجابة لاكتشاف مؤشر اختراق (IOC) - هذا هو الوضع التلقائي. ويمكنك تشغيل عزل الشبكة يدويًا أثناء التحقيق في التهديد المكتشف - هذا هو الوضع اليدوي.

وعند تشغيل عزل شبكة الاتصال، يقطع التطبيق جميع الاتصالات النشطة ويحظر جميع اتصالات TCP/IP الجديدة على الكمبيوتر باستثناء الاتصالات التالية:

- الاتصالات المدرجة في استثناءات عزل شبكة الاتصال.

- الاتصالات التي بدأتها خدمات Kaspersky Endpoint Security.
- الاتصالات التي بدأها عميل شبكة Kaspersky Security Center.

يمكنك تكوين إعدادات المكون فقط في Web Console.

وضع عزل الشبكة التلقائي

يمكنك تكوين عزل شبكة الاتصال لتشغيله تلقائيًا استجابة لاكتشاف مؤشر اختراق (IOC). يمكنك تكوين وضع عزل الشبكة التلقائي من خلال سياسة المجموعة.

كيفية تكوين عزل شبكة الاتصال لتشغيله تلقائيًا استجابة لاكتشاف مؤشر اختراق (IOC)

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Tasks**.
   تفتح قائمة المهام.
2. انقر فوق المهمة **IOC Scan** في برنامج Kaspersky Endpoint Security.
   نافذة خصائص المهمة.
   إذا لزم الأمر، أنشئ مهمة فحص IOC.
3. حدد علامة التبويب **Application settings**.
4. في القسم **Action on IOC detection**، حدد خانتي الاختيار **Take response actions after an IOC is found** و**Isolate computer from the network**.
5. احفظ تغييراتك.

نتيجة لذلك، عند اكتشاف مؤشر اختراق (IOC)، يعزل التطبيق الكمبيوتر عن الشبكة لمنع انتشار التهديد.

يمكنك تكوين عزل شبكة الاتصال لإيقاف تشغيله تلقائيًا بعد انقضاء فترة زمنية محددة. وافتراضيًا، يوقف التطبيق تشغيل عزل شبكة الاتصال بعد مرور 8 ساعات من وقت تشغيله. ويمكنك أيضًا إيقاف تشغيل عزل الشبكة يدويًا (انظر التعليمات أدناه). وبعد إيقاف تشغيل عزل شبكة الاتصال، يستطيع الكمبيوتر استخدام الشبكة دون قيود.

كيفية تكوين التأخير لإيقاف عزل الشبكة لجهاز الكمبيوتر في الوضع التلقائي

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response ← Endpoint Detection and Response**.

5. في القسم **Network isolation** انقر على **Configure computer unlock settings**.

6. يفتح هذا نافذة؛ وفي هذه النافذة، حدد خانة الاختيار **Automatically unlock isolated computer in N ساعة** وأدخل التأخير لإيقاف تشغيل عزل شبكة الاتصال تلقائيًا.

7. احفظ تغييراتك.

وضع عزل الشبكة اليدوي

يمكنك تشغيل عزل شبكة الاتصال وإيقاف تشغيله يدويًا. يمكنك تكوين وضع عزل الشبكة اليدوي باستخدام خصائص الكمبيوتر في وحدة تحكم Kaspersky Security Center.

يمكنك تشغيل عزل شبكة الاتصال:

- في تفاصيل التنبيه (لتطبيق EDR Optimum فقط).

تفاصيل الاكتشاف عبارة عن أداة لعرض كامل المعلومات التي تم جمعها حول التهديد المكتشف. وتتضمن تفاصيل الاكتشاف، على سبيل المثال، محفوظات الملفات التي تظهر على الكمبيوتر. وللحصول على التفاصيل عن إدارة تفاصيل الاكتشاف، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

- استخدام إعدادات التطبيق المحلية.

كيفية تشغيل عزل شبكة الاتصال لجهاز الكمبيوتر يدويًا

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Managed devices**.

2. حدد الكمبيوتر الذي تريد تكوين إعدادات التطبيق المحلية له.
تقوم هذه الخطوة بفتح خصائص الكمبيوتر.

3. حدد علامة التبويب **Applications**.

4. انقر على **Kaspersky Endpoint Security for Windows**.
تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.

5. حدد علامة التبويب **Application settings**.

6. انتقل إلى **Detection and Response ← Endpoint Detection and Response**.

7. في القسم **Network isolation** انقر على **Isolate computer from the network**.

يمكنك تكوين عزل شبكة الاتصال لإيقاف تشغيله تلقائيًا بعد انقضاء فترة زمنية محددة. وافتراضيًا، يوقف التطبيق تشغيل عزل شبكة الاتصال بعد مرور 8 ساعات من وقت تشغيله. وبعد إيقاف تشغيل عزل شبكة الاتصال ، يستطيع الكمبيوتر استخدام الشبكة دون قيود.

كيفية تكوين التأخير لإيقاف عزل الشبكة لجهاز الكمبيوتر في الوضع اليدوي

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Managed devices**.
2. حدد الكمبيوتر الذي تريد تكوين إعدادات التطبيق المحلية له.
   تقوم هذه الخطوة بفتح خصائص الكمبيوتر.
3. حدد علامة التبويب **Tasks**.
   يؤدي ذلك إلى عرض قائمة المهام المتاحة على الكمبيوتر.
4. حدد مهمة **Network isolation**.
5. حدد علامة التبويب **Application settings**.
6. يفتح هذا نافذة، في هذه النافذة، حدد التأخير لإيقاف تشغيل عزل الشبكة.
7. احفظ تغييراتك.

كيفية إيقاف تشغيل عزل شبكة الاتصال لجهاز الكمبيوتر يدويًا

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Managed devices**.
2. حدد الكمبيوتر الذي تريد تكوين إعدادات التطبيق المحلية له.
   تقوم هذه الخطوة بفتح خصائص الكمبيوتر.
3. حدد علامة التبويب **Applications**.
4. انقر على **Kaspersky Endpoint Security for Windows**.
   تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.
5. حدد علامة التبويب **Application settings**.
6. انتقل إلى **Detection and Response ← Endpoint Detection and Response**.
7. في القسم **Network isolation** انقر على **Unblock computer isolated from the network**.

يمكنك أيضًا تعطيل عزل شبكة الاتصال محليًا باستخدام سطر الأوامر.

استثناءات عزل شبكة الاتصال

يمكنك تكوين استثناءات عزل شبكة الاتصال. لا يتم حظر اتصالات شبكة الاتصال التي تطابق القواعد على الكمبيوتر عند تشغيل عزل شبكة الاتصال.

لتكوين استثناءات عزل الشبكة، يمكنك استخدام قائمة ملفات تعريف الشبكة القياسية. افتراضيًا، تتضمن الاستثناءات ملفات تعريف الشبكة التي تحتوي على قواعد تضمن التشغيل المتواصل للأجهزة مع خادم DNS/DHCP وأدوار عميل DNS/DHCP. ويمكنك أيضًا تعديل إعدادات ملفات تعريف الشبكة القياسية أو تحديد الاستثناءات يدويًا (انظر التعليمات أدناه).

يتم تطبيق الاستثناءات المحددة في خصائص السياسة فقط في حالة تشغيل عزل شبكة الاتصال تلقائيًا استجابة لتهديد مكتشف. ويتم تطبيق الاستثناءات المحددة في خصائص الكمبيوتر فقط في حالة تشغيل عزل شبكة الاتصال يدويًا في خصائص الكمبيوتر في وحدة تحكم Kaspersky Security Center أو في تفاصيل التنبيه.

لا تمنع سياسة نشطة تطبيق الاستثناءات من عزل شبكة الاتصال المكونة في خصائص الكمبيوتر لأن هذه المعلمات تتضمن سيناريوهات استخدام مختلفة.

كيفية إضافة استثناء عزل الشبكة في الوضع التلقائي

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Endpoint Detection and Response ← Detection and Response**.
5. في القسم **Network isolation exclusions** انقر على **Exclusions**.
6. يفتح هذا نافذة؛ وفي هذه النافذة، انقر فوق **Add from profile** وحدد ملفات تعريف الشبكة القياسية لتكوين الاستثناءات.
   تتم إضافة استثناءات عزل شبكة الاتصال من ملف التعريف إلى قائمة استثناءات عزل شبكة الاتصال. ويمكنك عرض خصائص اتصالات الشبكة. وإذا لزم الأمر، يمكنك تعديل إعدادات اتصال الشبكة.
7. إذا لزم الأمر، أضف استثناء عزل شبكة الاتصال يدويًا. ولفعل ذلك، في النافذة التي تتضمن قائمة الاستثناءات، انقر فوق **Add** وحرر إعدادات اتصال الشبكة يدويًا.
8. احفظ تغييراتك.

كيفية إضافة استثناءات عزل شبكة الاتصال في الوضع اليدوي

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Managed devices**.

2. حدد الكمبيوتر الذي تريد تكوين إعدادات التطبيق المحلية له.

   تقوم هذه الخطوة بفتح خصائص الكمبيوتر.

3. حدد علامة التبويب **Tasks**.

   يؤدي ذلك إلى عرض قائمة المهام المتاحة على الكمبيوتر.

4. حدد مهمة **Network isolation**.

5. حدد علامة التبويب **Application settings**.

6. يفتح هذا نافذة، في هذه النافذة، انقر فوق **Exclusions**.

7. يفتح هذا نافذة؛ وفي هذه النافذة، انقر فوق **Add from profile** وحدد ملفات تعريف الشبكة القياسية لتكوين الاستثناءات.

   تتم إضافة استثناءات عزل شبكة الاتصال من ملف التعريف إلى قائمة استثناءات عزل شبكة الاتصال. ويمكنك عرض خصائص اتصالات الشبكة. وإذا لزم الأمر، يمكنك تعديل إعدادات اتصال الشبكة.

8. إذا لزم الأمر، أضف استثناء عزل شبكة الاتصال يدويًا. ولفعل ذلك، في النافذة التي تتضمن قائمة الاستثناءات، انقر فوق **Add** وحرر إعدادات اتصال الشبكة يدويًا.

9. احفظ تغييراتك.

يمكنك أيضًا عرض استثناء عزل شبكة الاتصال محليًا باستخدام سطر الأوامر. في هذه الحالة، يجب أن يكون جهاز الكمبيوتر معزولاً.

Cloud Sandbox

Cloud Sandbox هي تقنية تتيح لك اكتشاف التهديدات المتقدمة على جهاز كمبيوتر. ويعيد Kaspersky Endpoint Security تلقائيًا توجيه الملفات المكتشفة إلى Cloud Sandbox لتحليلها. ويقوم Cloud Sandbox بتشغيل هذه الملفات في بيئة معزولة لتحديد النشاط الضار وتحديد سمعتها. ثم يتم إرسال البيانات الموجودة في هذه الملفات إلى Kaspersky Security Network. لذلك، إذا اكتشف Cloud Sandbox ملفًا ضارًا، فسوف ينفذ Kaspersky Endpoint Security الإجراء المناسب للقضاء على هذا التهديد على جميع أجهزة الكمبيوتر التي تم اكتشاف هذا الملف عليها.

لكي يعمل Cloud Sandbox، يجب عليك تمكين استخدام Kaspersky Security Network.

إذا كنت تستخدم Kaspersky Private Security Network، فإن تقنية Cloud Sandbox ستكون غير متاحة.

يتم تمكين تقنية Cloud Sandbox بشكل دائم وهي متاحة لجميع مستخدمي Kaspersky Security Network بغض النظر عن نوع الترخيص الذي يستخدمونه. وإذا نشرت بالفعل Endpoint Detection and Response Optimum، يمكنك تمكين عداد منفصل للتهديدات المكتشفة بواسطة Cloud Sandbox. ويمكنك استخدام هذا العداد لإنشاء إحصائيات أثناء تحليل التهديدات المكتشفة.

لتمكين عداد Cloud Sandbox:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response** ← **Endpoint Detection and Response**.

5. قم بتشغيل مفتاح **Cloud Sandbox**.

6. احفظ تغييراتك.

عند وجود تهديد، يقوم Kaspersky Endpoint Security بتفعيل عداد التهديدات المكتشفة باستخدام Cloud Sandbox في نافذة التطبيق الرئيسية تحت **تقنيات اكتشاف التهديدات**. وسيشير Kaspersky Endpoint Security أيضًا إلى تقنية اكتشاف التهديدات في Cloud Sandbox في التقرير عن التهديدات وفي وحدة تحكم Kaspersky Security Center.

Kaspersky Sandbox

بدءًا من الإصدار 11.7.0، يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا للتكامل مع حل Kaspersky Sandbox. ويكتشف حل Kaspersky Sandbox ويمنع تلقائيًا التهديدات المتقدمة على أجهزة الكمبيوتر. ويحلل Kaspersky Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Kaspersky Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Kaspersky Sandbox). وللحصول على تفاصيل حول الحل، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

يمكن إجراء التكوينات التالية لحل Kaspersky Sandbox:

Kaspersky Sandbox 2.0

يدعم Kaspersky Sandbox 2.0 تكوين [KES+العميل المدمج].

الحد الأدنى للمتطلبات:

- Kaspersky Endpoint Security 11.7.0 for Windows أو أحدث.
- Kaspersky Endpoint Agent ليس مطلوبًا.
- Kaspersky Security Center 13.2.

Kaspersky Sandbox 1.0

يدعم Kaspersky Sandbox 1.0 تكوين [KES+KEA].

الحد الأدنى للمتطلبات:

- Kaspersky Endpoint Security 11.2.0 – 11.6.0 for Windows.
- Kaspersky Endpoint Agent 3.8.
  يمكنك تثبيت Kaspersky Endpoint Agent من مجموعة توزيع Kaspersky Endpoint Security for Windows.
- Kaspersky Security Center 11.

التكامل مع Kaspersky Sandbox

إضافة مكون Kaspersky Sandbox مطلوبة للتكامل مع مكون Kaspersky Sandbox. ويمكنك تحديد مكون Kaspersky Sandbox أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

لاستخدام المكون، يجب استيفاء الشروط التالية:

- Kaspersky Security Center 13.2. ولا تسمح الإصدارات السابقة من Kaspersky Security Center بإنشاء مهام فحص IOC مستقلة للاستجابة للتهديدات.
- يمكن إدارة المكون فقط باستخدام Web Console. لا يمكنك إدارة هذا المكون باستخدام وحدة تحكم الإدارة (MMC).
- تم تفعيل التطبيق ويغطي الترخيص الوظيفة.
- يتم تمكين نقل البيانات إلى خادم الإدارة.

لاستخدام كل ميزات Kaspersky Sandbox، تأكد من تمكين نقل بيانات ملف العزل. البيانات مطلوبة للحصول على معلومات حول الملفات المعزولة على جهاز كمبيوتر من خلال وحدة تحكم الويب. على سبيل المثال، يمكنك تنزيل ملف من العزل للتحليل في وحدة تحكم ويب.

كيفية تمكين نقل البيانات إلى خادم الإدارة في وحدة تحكم الويب

1. في النافذة الرئيسية لـ Web Console، حدد **Policies & Profiles** ← **Devices**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General settings** ← **Reports and Storage**.
5. في القسم **Data transfer to Administration Server**، حدد خانة الاختيار **About Quarantine files**.
6. احفظ تغييراتك.

- يتم إنشاء اتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة

لكي يعمل Kaspersky Sandbox مع Administration Server عبر Kaspersky Security Center Web Console، يجب عليك إنشاء اتصال آمن جديد، اتصال في الخلفية. وللحصول على تفاصيل حول تكامل Kaspersky Security Center مع حلول Kaspersky الأخرى، يرجى الرجوع إلى تعليمات Kaspersky Security Center.

إنشاء اتصال في الخلفية في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Integration** ← **Console settings**.
2. انتقل إلى القسم **Integration**.
3. قم بتشغيل مفتاح التبديل **Establish a background connection for integration**.
4. احفظ تغييراتك.

إذا لم يتم إنشاء اتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة، فلا يمكن إنشاء مهام فحص IOC المستقلة كجزء من الاستجابة للتهديدات.

- تم تمكين مكون Kaspersky Sandbox.

يمكنك تمكين أو تعطيل التكامل مع Kaspersky Sandbox في Web Console أو محليًا باستخدام سطر الأوامر.

لتمكين التكامل مع Kaspersky Sandbox أو تعطيله:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response** ← **Kaspersky Sandbox**.

5. استخدم مفتاح تبديل **Integration with Kaspersky Sandbox ENABLED** لتمكين المكون أو تعطيله.

6. احفظ تغييراتك.

نتيجة لذلك، يتم تمكين مكون Kaspersky Sandbox. تحقق من حالة تشغيل المكون عن طريق عرض تقرير حالة مكونات التطبيق. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Kaspersky Sandbox** إلى قائمة مكونات Kaspersky Endpoint Security.

يحفظ Kaspersky Endpoint Security معلومات حول أداء مكون Kaspersky Sandbox في تقرير. ويحتوي التقرير أيضًا على معلومات عن الأخطاء. وإذا تلقيت خطأ مع وصف يناسب تنسيق `Error code: XXX` (على سبيل المثال، `0xa67b01f4`)، اتصل بالدعم الفني.

الترحيل من Kaspersky Endpoint Agent

إذا كنت تستخدم Kaspersky Endpoint Security 11.7.0 أو أحدث مع تثبيت مكون Kaspersky Sandbox (العامل المضمن)، فستتوفر إمكانية التشغيل التفاعلي مع حل Kaspersky Sandbox فور التثبيت. لا يتوافق مكون Kaspersky Sandbox مع Kaspersky Endpoint Agent. في حالة تثبيت Kaspersky Endpoint Agent على الكمبيوتر، عند تحديث Kaspersky Endpoint Security إلى الإصدار 11.7.0 ، يستمر Kaspersky Sandbox في العمل مع Kaspersky Endpoint Security (ترحيل تكوين [KES+KEA] إلى [KES+العامل المضمن]). بالإضافة إلى ذلك، ستتم إزالة Kaspersky Endpoint Agent من الكمبيوتر. ولإكمال الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows، تحتاج إلى نقل إعدادات السياسة والمهام باستخدام معالج الترحيل.

إذا كنت تستخدم Kaspersky Endpoint Security 11.4.0–11.6.0 لإمكانية التشغيل التفاعلي مع Kaspersky Sandbox، فإن التطبيق يتضمن Kaspersky Endpoint Agent. يمكنك تثبيت Kaspersky Endpoint Agent مع تثبيت Kaspersky Endpoint Security.

تتضمن مجموعة أدوات التوزيع لتطبيق Kaspersky Endpoint Security الإصدارات 11.2.0 - 11.8.0 مكون Kaspersky Endpoint Agent. ويمكنك تحديد Kaspersky Endpoint Agent عند تثبيت Kaspersky Endpoint Security for Windows. نتيجة لذلك، سيتم تثبيت تطبيقين على جهاز الكمبيوتر الخاص بك: KEA وKES. في Kaspersky Endpoint Security 11.9.0، لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من مجموعة توزيع Kaspersky Endpoint Security.

يدعم مكون Kaspersky Sandbox الذي يعد جزءًا من Kaspersky Endpoint Security، إمكانية التشغيل التفاعلي مع حل Kaspersky Sandbox 2.0. لا يتم دعم حل Kaspersky Sandbox 1.0.

إضافة شهادة TLS

لتكوين اتصال موثوق به مع خوادم Kaspersky Sandbox، يجب عليك إعداد شهادة TLS. وبعد ذلك، يجب إضافة الشهادة إلى خوادم Kaspersky Sandbox وسياسة Kaspersky Endpoint Security. وللحصول على تفاصيل عن إعداد الشهادة وإضافة الشهادة إلى الخوادم، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

يمكنك أيضًا إضافة شهادة TLS إلى Web Console أو محليًا باستخدام سطر الأوامر.

لإضافة شهادة TLS في Web Console:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response** ← **Kaspersky Sandbox**.

5. انقر على رابط **Server connection settings**.
يفتح هذا نافذة إعدادات الاتصال بخادم Kaspersky Sandbox.

6. في القسم **Server TLS certificate**، انقر فوق **Add** وحدد ملف شهادة TLS.

من الممكن أن يتضمن Kaspersky Endpoint Security شهادة TLS واحدة فقط لخادم Kaspersky Sandbox. وإذا كنت قد أضفت شهادة TLS من قبل، فسيتم إبطال هذه الشهادة. ويتم استخدام آخر شهادة مضافة فقط.

7. تكوين إعدادات الاتصالات المتقدمة لخوادم Kaspersky Sandbox:

- **Timeout**. انتهت مهلة الاتصال لخادم Kaspersky Sandbox. بعد انقضاء المهلة التي تم تكوينها، يرسل Kaspersky Endpoint Security طلبًا إلى الخادم التالي. ويمكنك زيادة مهلة الاتصال لتطبيق Kaspersky Sandbox إذا كانت سرعة الاتصال لديك منخفضة أو إذا كان الاتصال غير مستقر. مهلة الطلب الموصى بها 0.5 ثانية أو أقل.

- **Kaspersky Sandbox request queue**. حجم مجلد قائمة انتظار الطلبات. عند الوصول إلى كائن على الكمبيوتر (تم تشغيل الملف القابل للتنفيذ أو فتح المستند، على سبيل المثال بتنسيق DOCX أو PDF)، يستطيع برنامج Kaspersky Endpoint Security أيضًا إرسال الكائن لفحصه بواسطة Kaspersky Sandbox. في حالة وجود طلبات متعددة، يُنشئ Kaspersky Endpoint Security قائمة انتظار الطلبات. وافتراضيًا، يقتصر حجم مجلد قائمة انتظار الطلبات على 100 ميجابايت. وبعد الوصول إلى الحد الأقصى للحجم، يتوقف Kaspersky Sandbox عن إضافة طلبات جديدة إلى قائمة الانتظار ويرسل الحدث المقابل إلى Kaspersky Security Center. ويمكنك تكوين حجم مجلد قائمة انتظار الطلبات بناءً على تكوين خادمك.

8. احفظ تغييراتك.

نتيجة لذلك، يتحقق Kaspersky Endpoint Security من ملف TLS. وفي حالة التحقق من الشهادة بنجاح، يقوم Kaspersky Endpoint Security بتحميل ملف الشهادة إلى الكمبيوتر أثناء المزامنة التالية مع Kaspersky Security Center. إذا أضفت شهادتي TLS، سيستخدم Kaspersky Sandbox أحدث شهادة لإنشاء اتصال موثوق.

إضافة خوادم Kaspersky Sandbox

لتوصيل أجهزة الكمبيوتر بخوادم Kaspersky Sandbox باستخدام صور افتراضية لأنظمة التشغيل، يجب إدخال عنوان الخادم والمنفذ. وللحصول على التفاصيل حول نشر الصور الافتراضية وتكوين خوادم Kaspersky Sandbox، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

لإضافة خوادم Kaspersky Sandbox إلى Web Console:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response ← Kaspersky Sandbox**.

5. في القسم **Kaspersky Sandbox servers** انقر على **Add**.

6. يفتح هذا نافذة؛ وداخل النافذة، أدخل عنوان خادم Kaspersky Sandbox (IPv4 وIPv6 وDNS) والمنفذ.

7. احفظ تغييراتك.

الفحص للبحث عن مؤشرات الاختراق (مهمة مستقلة)

مؤشر الاختراق (IOC) عبارة عن مجموعة من البيانات حول كائن أو نشاط يشير إلى وصول غير مصرح به إلى الكمبيوتر (اختراق البيانات). على سبيل المثال، من الممكن أن تشكل العديد من المحاولات الفاشلة لتسجيل الدخول إلى النظام مؤشرًا على الاختراق. تتيح مهمة فحص IOC العثور على مؤشرات الاختراق على الكمبيوتر واتخاذ إجراءات الاستجابة للتهديدات.

يبحث Kaspersky Endpoint Security عن مؤشرات الاختراق باستخدام ملفات IOC. ملفات IOC هي ملفات تحتوي على مجموعات المؤشرات التي يحاول التطبيق مطابقتها لإحصاء الاكتشاف. ويجب أن تتوافق ملفات IOC مع معيار OpenIOC. يُنشئ Kaspersky Endpoint Security تلقائيًا ملفات IOC لحل Kaspersky Sandbox.

وضع تشغيل مهمة فحص IOC

ينشئ التطبيق مهام فحص IOC مستقلة لحل Kaspersky Sandbox. مهمة فحص IOC المستقلة هي مهمة جماعية يتم إنشاؤها تلقائيًا عند الرد على تهديد تم اكتشافه بواسطة Kaspersky Sandbox. وينشئ Kaspersky Endpoint Security ملف IOC تلقائيًا. ولا يتم دعم ملفات IOC المخصصة. ويتم حذف المهام تلقائيًا بعد 30 يومًا من وقت الإنشاء. وللمزيد من التفاصيل حول مهام فحص IOC المستقلة، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

إعدادات مهمة فحص IOC

قد ينشئ Kaspersky Sandbox ويُشّغل مهام فحص IOC تلقائيًا عند الرد على التهديدات.

يمكنك تكوين الإعدادات فقط في Web Console.

وتحتاج إلى برنامج Kaspersky Security Center 13.2 لكي تعمل مهام فحص IOC المستقلة في Kaspersky Sandbox.

لتغيير إعدادات مهمة فحص IOC:

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Tasks**.
تفتح قائمة المهام.

2. انقر فوق المهمة **IOC Scan** في برنامج Kaspersky Endpoint Security.
نافذة خصائص المهمة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى القسم **IOC scan settings**.

5. تكوين الإجراءات عند اكتشاف IOC:

- **Move copy to Quarantine, delete object**. في حالة تحديد هذا الخيار، يحذف Kaspersky Endpoint Security الكائن الضار الموجود على الكمبيوتر. قبل حذف الكائن، يُنشئ Kaspersky Endpoint Security نسخة احتياطية في حالة الحاجة إلى استعادة الكائن لاحقًا. ينقل Kaspersky Endpoint Security النسخة الاحتياطية إلى العزل.

- **Run scan of critical areas**. في حالة تحديد هذا الخيار، يُشغل Kaspersky Endpoint Security مهمة فحص المناطق الحرجة. بشكلٍ افتراضي، يفحص Kaspersky Endpoint Security ذاكرة kernel والعمليات قيد التشغيل وقطاعات تمهيد القرص.

6. قم بتكوين وضع تشغيل مهمة فحص IOC باستخدام خانة الاختيار **Run only when the computer is idle**. تؤدي خانة الاختيار هذه إلى تمكين/تعطيل وظيفة فحص IOC عندما تكون موارد الكمبيوتر محدودة. يوقف Kaspersky Endpoint Security مهمة فحص IOC مؤقتًا في حالة إيقاف تشغيل حافظة الشاشة وإلغاء قفل الكمبيوتر.

   يتيح لك خيار الجدولة هذا الحفاظ على موارد الكمبيوتر عند استخدام الكمبيوتر.

7. احفظ تغييراتك.

ويمكنك عرض نتائج المهمة في خصائص المهمة في القسم **Results**. ويمكنك عرض المعلومات حول المؤشرات المكتشفة للاختراق في خصائص المهمة: **Application settings ← IOC Scan Results**.

يتم الاحتفاظ بنتائج فحص IOC لمدة 30 يومًا. وبعد هذه الفترة، يحذف برنامج Kaspersky Endpoint Security تلقائيًا الإدخالات القديمة.

(Kaspersky Anti Targeted Attack Platform (EDR

بدءًا من الإصدار 12.1، يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا لإدارة مكون Kaspersky Endpoint Detection and Response كجزء من حل Kaspersky Anti Targeted Attack Platform. منصة Kaspersky Anti Targeted Attack عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. ويتضمن Kaspersky Anti Targeted Attack Platform مكونين وظيفيين: Kaspersky Anti Targeted Attack (ويشار إليه هنا باسم "KATA") والثاني Kaspersky Endpoint Detection and Response (ويشار إليه هنا باسم "EDR (KATA"). ويمكنك شراء EDR (KATA) بشكل منفصل. وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

يستخدم Kaspersky Endpoint Detection and Response أدوات معلومات التهديدات التالية:

- البنية التحتية السحابية لشبكة Kaspersky Security Network (المشار إليها فيما يلي أيضًا باسم "KSN")، التي توفر الوصول إلى معلومات سمعة البرامج وموقع الويب والملف في الوقت الحقيقي من قاعدة معارف Kaspersky. ويضمن استخدام البيانات من Kaspersky Security Network استجابات أسرع من قبل تطبيقات Kaspersky للتهديدات، ويحسن أداء بعض مكونات الحماية، ويقلل من احتمالية الاكتشافات الإيجابية الزائفة.

- التكامل مع Kaspersky Threat Intelligence Portal، الذي يحتوي على معلومات عن سمعة الملفات وعناوين الويب ويعرضها.

- قاعدة بيانات التهديدات الخاصة بشركة Kaspersky.

يتم تثبيت Kaspersky Endpoint Security على أجهزة كمبيوتر فردية على البنية التحتية لتكنولوجيا المعلومات بالشركة ويراقب باستمرار العمليات واتصالات الشبكة المفتوحة والملفات التي يتم تعديلها. ويتم إرسال معلومات عن الأحداث على الكمبيوتر (بيانات القياس عن بُعد) إلى خادم Kaspersky Anti Targeted Attack Platform. وفي هذه الحالة، يرسل Kaspersky Endpoint Security أيضًا معلومات إلى خادم Kaspersky Anti Targeted Attack Platform حول التهديدات التي اكتشفتها Kaspersky بالإضافة إلى معلومات عن نتائج معالجة هذه التهديدات.

تم تكوين تكامل EDR (KATA) على وحدة تحكم Kaspersky Security Center. وبعد ذلك تتم إدارة العامل المضمن باستخدام وحدة تحكم Kaspersky Anti Targeted Attack Platform، بما في ذلك مهام التشغيل وإدارة الكائنات المعزولة وعرض التقارير والإجراءات الأخرى.

التكامل مع EDR (KATA)

للتكامل مع EDR (KATA)، يجب عليك إضافة مكون Endpoint Detection and Response (KATA). ويمكنك تحديد مكون EDR (KATA) أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

لا تتوافق المكونات EDR Optimum وEDR Expert وEDR (KATA) مع بعضها البعض.

يجب استيفاء الشروط التالية لكي يعمل Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform الإصدار 4.1 أو أحدث.
- Kaspersky Security Center الإصدار 13.2 أو أحدث. في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة Endpoint Detection and Response (KATA).
- تم تفعيل التطبيق ويغطي الترخيص الوظيفة.
- تم تشغيل مكون Endpoint Detection and Response (KATA).
- يتم تمكين وتشغيل مكونات التطبيق التي يعتمد عليها Endpoint Detection and Response (KATA). وتضمن المكونات التالية تشغيل EDR (KATA):
  - الحماية من تهديدات الملفات.
  - الحماية من تهديدات الويب.
  - الحماية من تهديدات البريد.
  - منع الاستغلال.
  - اكتشاف السلوك.
  - منع اختراق المضيف.
  - محرك المعالجة.
  - مراقبة عيوب التكيف.

يتكون التكامل مع Kaspersky Endpoint Detection and Response من الخطوات التالية:

1. **تثبيت مكون Endpoint Detection and Response (KATA)**

   ويمكنك تحديد مكون EDR (KATA) أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

   يجب إعادة تشغيل الكمبيوتر لإنهاء ترقية التطبيق بالمكونات الجديدة.

2. **تفعيل Endpoint Detection and Response (KATA)**

   يمكنك الحصول على ترخيص لاستخدام Kaspersky Endpoint Detection and Response (KATA) بالطرق التالية:

   - يتم تضمين وظائف Endpoint Detection and Response (KATA) في ترخيص Kaspersky Endpoint Security for Windows.

     ستتوفر الميزة فور تفعيل Kaspersky Endpoint Security for Windows.

   - شراء ترخيص منفصل لمكون EDR (KATA) (الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response (KATA)).

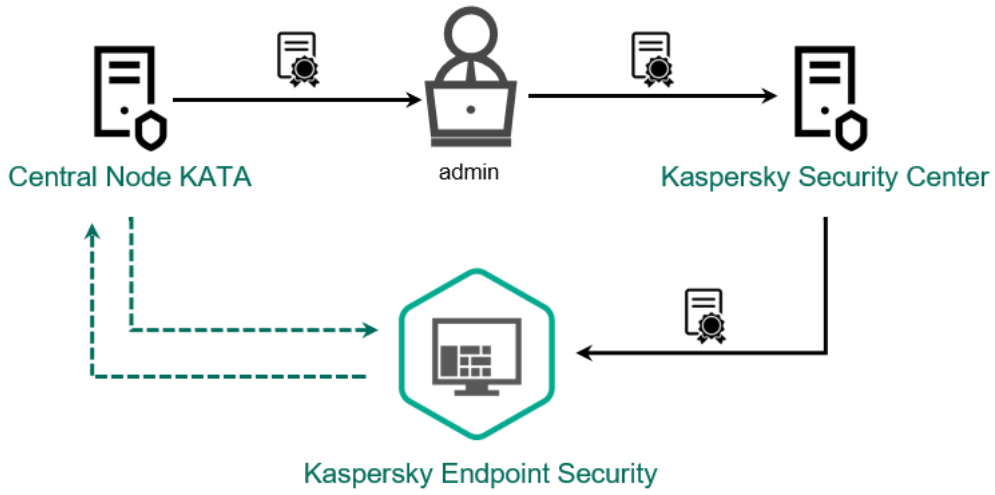
     ستتوفر الميزة بعد إضافة مفتاح منفصل لحل Kaspersky Endpoint Detection and Response (KATA). ونتيجة لذلك، يتم تثبيت مفتاحين على الكمبيوتر: مفتاح لحل Kaspersky Endpoint Security ومفتاح لحل Kaspersky Endpoint Detection and Response (KATA).

الترخيص لوظيفة Endpoint Detection and Response (KATA) المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

تأكد من تضمين وظيفة EDR (KATA) في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

3 الاتصال بمكون Central Node

يتطلب Kaspersky Anti Targeted Attack Platform إنشاء اتصال موثوق به بين Kaspersky Endpoint Security ومكوّن Central Node. لتكوين اتصال موثوق، يجب عليك استخدام شهادة TLS. ويمكنك الحصول على شهادة TLS في وحدة تحكم Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform). وبعد ذلك يجب عليك إضافة شهادة TLS إلى Kaspersky Endpoint Security (انظر الإرشادات أدناه).



إضافة شهادة TLS إلى Kaspersky Endpoint Security

بشكل افتراضي، يتحقق Kaspersky Endpoint Security فقط من شهادة TLS لمكون Central Node. ولجعل الاتصال أكثر أمانًا، يمكنك أيضًا تمكين التحقق من الكمبيوتر على مكون Central Node (المصادقة ثنائية الاتجاه). ولتمكين هذا التحقق، يجب عليك تشغيل المصادقة ثنائية الاتجاه في إعدادات Central Node وKaspersky Endpoint Security. ولاستخدام المصادقة ثنائية الاتجاه، ستحتاج أيضًا إلى حاوية تشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. ويمكنك الحصول على حاوية تشفير في Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform).

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون Central Node باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **Detection and Response ← Endpoint Detection and Response (KATA)**.

5. حدد خانة الاختيار **Endpoint Detection and Response (KATA)**.

6. انقر على **Settings for connecting to KATA servers**.

7. تكوين اتصال الخادم:

- **Timeout**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
- **Server TLS certificate**. شهادة TLS لإنشاء اتصال موثوق به مع خادم Central Node. ويمكنك الحصول على شهادة TLS في وحدة تحكم Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform).
- **Use two-way authentication**. تسمح المصادقة ثنائية الاتجاه بتمكين عملية تحقق إضافية للكمبيوتر على Central Node. ولتمكين هذا التحقق، يجب عليك تشغيل المصادقة ثنائية الاتجاه في إعدادات Central Node وKaspersky Endpoint Security. ولاستخدام المصادقة ثنائية الاتجاه، ستحتاج أيضًا إلى حاوية تشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. ويمكنك الحصول على حاوية تشفير في Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform).

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

8. انقر على **OK**.

9. أضف خوادم العقدة المركزية. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

10. احفظ تغييراتك.

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون Central Node باستخدام Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Detection and Response ← Endpoint Detection and Response (KATA)**.

5. قم بتشغيل مفتاح **Endpoint Detection and Response (KATA) ENABLED**.

6. انقر على **Settings for connecting to KATA servers**.

7. تكوين اتصال الخادم:

- **Timeout**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
- **Server TLS certificate**. شهادة TLS لإنشاء اتصال موثوق به مع خادم Central Node. ويمكنك الحصول على شهادة TLS في وحدة تحكم Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform).
- **Use two-way authentication**. تسمح المصادقة ثنائية الاتجاه بتمكين عملية تحقق إضافية للكمبيوتر على Central Node. ولتمكين هذا التحقق، يجب عليك تشغيل المصادقة ثنائية الاتجاه في إعدادات Central Node وKaspersky Endpoint Security. ولاستخدام المصادقة ثنائية الاتجاه، ستحتاج أيضًا إلى حاوية تشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. ويمكنك الحصول على حاوية تشفير في Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform).

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

8. انقر على **OK**.

9. أضف خوادم العقدة المركزية. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

10. احفظ تغييراتك.

نتيجة لذلك، تمت إضافة الكمبيوتر إلى وحدة تحكم Kaspersky Anti Targeted Attack Platform. تحقق من حالة تشغيل المكون عن طريق عرض تقرير حالة مكونات التطبيق. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Endpoint Detection and Response (KATA)** إلى قائمة مكونات Kaspersky Endpoint Security.

تكوين القياس عن بعد

القياس عن بعد عبارة عن قائمة الأحداث التي وقعت على الكمبيوتر المحمي. ويحلل Kaspersky Endpoint Security بيانات القياس عن بُعد ويرسلها إلى Kaspersky Anti Targeted Attack Platform أثناء المزامنة. وتصل أحداث التتبع عن بُعد إلى الخادم بشكل شبه مستمر. ويبدأ Kaspersky Endpoint Security المزامنة مع الخادم عند استيفاء أي من الشروط التالية:

- نفد الفاصل الزمني للمزامنة.
- عدد الأحداث في المخزن المؤقت يتجاوز الحد الأعلى.

لذلك، يتزامن التطبيق افتراضيًا كل 30 ثانية أو كلما احتوى المخزن المؤقت على 1024 حدثًا. ويمكنك تكوين سلوك المزامنة في سياسة Kaspersky Endpoint Security وتحديد القيم المثلى لمطابقة حمل الشبكة (انظر التعليمات أدناه).

إذا لم يكن هناك اتصال بين Kaspersky Endpoint Security والخادم، فإن التطبيق يضع الأحداث الجديدة في قائمة الانتظار. وعند استعادة الاتصال، يرسل Kaspersky Endpoint Security الأحداث في قائمة الانتظار إلى الخادم بالترتيب الصحيح. ولتجنب الحمل الزائد على الخادم، قد يتخطى Kaspersky Endpoint Security بعض الأحداث. ولتمكين هذا، يمكنك تحسين إعدادات إرسال الأحداث، على سبيل المثال، لتعيين الحد الأقصى لقيمة الأحداث في الساعة (انظر الإرشادات أدناه).

وإذا كنت تستخدم Kaspersky Anti Targeted Attack Platform جنبًا إلى جنب مع حل آخر يستخدم أيضًا القياس عن بُعد، يمكنك إيقاف تشغيل القياس عن بُعد لحل KATA (EDR) (راجع الإرشادات أعلاه). ويتيح لك هذا تحسين حمل الخادم لهذه الحلول. على سبيل المثال، إذا كان لديك حل Managed Detection and Response وتم نشر KATA (EDR)، يمكنك استخدام القياس عن بُعد في MDR وإنشاء مهام الاستجابة للتهديد في KATA (EDR).

كيفية تكوين القياس عن بُعد في EDR على وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Detection and Response ← Endpoint Detection and Response (KATA)**.
5. كوّن إعداد **إرسال طلب مزامنة إلى خادم KATA كل (دقيقة)**. عدد مرات إرسال طلبات المزامنة إلى خادم العقدة المركزية. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.
6. تأكد من تحديد خانة الاختيار **إرسال القياس عن بعد إلى KATA**.
7. إذا لزم الأمر، كوّن إعداد **الحد الأقصى لتأخير إرسال الأحداث (ثانية)** في القسم **إعدادات نقل البيانات**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
8. إذا لزم الأمر ، حدد خانة الاختيار **تمكين تقييد الطلب** في القسم **تقييد الطلب**.

   تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تحديد خانة الاختيار، فإن التطبيق يُقيد الأحداث المرسلة. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث.
9. تكوين إعدادات التحسين لإرسال الأحداث إلى الخادم:
   - **الحد الأقصى لعدد الأحداث في الساعة**. يحلل التطبيق تدفق بيانات القياس عن بُعد ويُقيد إرسال الأحداث إذا تجاوز تدفق الحدث حد الأحداث المكون لكل ساعة. ويستأنف Kaspersky Endpoint Security إرسال الأحداث بعد ساعة. الإعداد الافتراضي هو 3000 حدث في الساعة.
   - **النسبة المئوية لفائض حد الحدث**. يفرز التطبيق الأحداث حسب النوع (على سبيل المثال" أحداث "التغييرات في السجل") ويقيد إرسال الأحداث إذا تجاوزت نسبة الأحداث من النوع نفسه إلى العدد الإجمالي للأحداث الحد الذي تم تكوينه بالنسبة المئوية. ويستأنف Kaspersky Endpoint Security إرسال الأحداث عندما تصبح نسبة الأحداث الأخرى إلى العدد الإجمالي للأحداث كبيرة بما يكفي مرة أخرى. الإعداد الافتراضي هو 15%.
10. احفظ تغييراتك.

كيفية تكوين EDR عن بعد على Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices ← Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Endpoint Detection and Response (KATA ← Detection and Response**.

5. كوّن إعداد **Send sync request to KATA server every (min)**. عدد مرات إرسال طلبات المزامنة إلى خادم العقدة المركزية. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.

6. تأكد من تحديد خانة الاختيار **إرسال القياس عن بعد إلى KATA**.

7. إذا لزم الأمر، كوّن إعداد **Maximum events transmission delay (sec)** في القسم **Data transmission settings**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.

8. إذا لزم الأمر ، حدد خانة الاختيار **Enable request throttling** في القسم **Request throttling**.

تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تحديد خانة الاختيار، فإن التطبيق يُقيد الأحداث المرسلة. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث.

9. تكوين إعدادات التحسين لإرسال الأحداث إلى الخادم:

- **Maximum number of events per hour**. يحلل التطبيق تدفق بيانات القياس عن بُعد ويُقيد إرسال الأحداث إذا تجاوز تدفق الحدث حد الأحداث المكون لكل ساعة. ويستأنف Kaspersky Endpoint Security إرسال الأحداث بعد ساعة. الإعداد الافتراضي هو 3000 حدث في الساعة.

- **Percentage of event limit excess**. يفرز التطبيق الأحداث حسب النوع (على سبيل المثال" أحداث "التغييرات في السجل") ويقيد إرسال الأحداث إذا تجاوزت نسبة الأحداث من النوع نفسه إلى العدد الإجمالي للأحداث الحد الذي تم تكوينه بالنسبة المئوية. ويستأنف Kaspersky Endpoint Security إرسال الأحداث عندما تصبح نسبة الأحداث الأخرى إلى العدد الإجمالي للأحداث كبيرة بما يكفي مرة أخرى. الإعداد الافتراضي هو 15%.

10. احفظ تغييراتك.

استثناءات القياس عن بعد

لتحسين البيانات المرسلة، يمكنك ذلك إضافة ملف قابل للتنفيذ إلى قائمة التطبيقات الموثوقة. وفي هذه الحالة، لا يرسل Kaspersky Endpoint Security أحداث تتبع عن بُعد لهذا التطبيق. ويتيح لك هذا تقليل حركة شبكة الاتصال وتقليل مقدار الأحداث من الكائنات الموثوقة.

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **تكامل KATA** ← القسم **استثناءات القياس عن بعد**.

5. تحت **إعدادات نقل البيانات**، حدد خانة الاختيار **استخدام الاستثناءات**.

6. انقر على **إضافة** وقم بتكوين الاستثناءات:

يتم الجمع بين المعايير باستخدام المنطق AND.

- **المسار**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع. ولكي يعمل الاستثناء، يجب تحديد المسار إلى الملف.
- **سطر الأوامر**. الأمر المستخدم لتشغيل الكائن.
- **الوصف**. قيمة المعلمة FileDescription من مورد VersionInfo) RT_VERSION).
للحصول على المزيد من المعلومات عن مورد VersionInfo، يُرجى زيارة موقع ويب Microsoft.
- **اسم الملف الأصلي**. قيمة المعلمة OriginalFilename من مورد VersionInfo) RT_VERSION).
- **الإصدار**. قيمة معلمة FileVersion من مورد VersionInfo) RT_VERSION).
- **MD5**. تجزئة MD5 للملف.
- **SHA256**. تجزئة SHA256 للملف.
- **أنواع الأحداث**. لكي يعمل الاستثناء، يجب تحديد نوع حدث واحد على الأقل.

7. احفظ تغييراتك.

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **السياسات**.

3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة، حدد **تكامل KATA** ← **استثناءات القياس عن بعد**.

5. تحت **إعدادات نقل البيانات**، حدد خانة الاختيار **استخدام الاستثناءات**.

6. انقر على **إضافة** وقم بتكوين الاستثناءات:

يتم الجمع بين المعايير باستخدام المنطق AND.

- **المسار**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع. ولكي يعمل الاستثناء، يجب تحديد المسار إلى الملف.
- **سطر الأوامر**. الأمر المستخدم لتشغيل الكائن.
- **الوصف**. قيمة المعلمة FileDescription من مورد VersionInfo) RT_VERSION).
  للحصول على المزيد من المعلومات عن مورد VersionInfo، يُرجى زيارة موقع ويب Microsoft.
- **اسم الملف الأصلي**. قيمة المعلمة OriginalFilename من مورد VersionInfo) RT_VERSION).
- **الإصدار**. قيمة معلمة FileVersion من مورد VersionInfo) RT_VERSION).
- **MD5**. تجزئة MD5 للملف.
- **SHA256**. تجزئة SHA256 للملف.
- **أنواع الأحداث**. لكي يعمل الاستثناء، يجب تحديد نوع حدث واحد على الأقل.

7. احفظ تغييراتك.

دليل الترحيل من KEA إلى KES لحل KATA) EDR)

بدءًا من الإصدار 12.1، يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا لإدارة مكون Kaspersky Endpoint Detection and Response كجزء من حل Kaspersky Anti Targeted Attack Platform. ولم تعد بحاجة إلى تطبيق Kaspersky Endpoint Agent منفصل للعمل مع KATA) EDR). وسيتم تنفيذ جميع وظائف Kaspersky Endpoint Agent بواسطة Kaspersky Endpoint Security. وسيبقى الحمل على خوادم Kaspersky Anti Targeted Attack Platform كما هو.

عند نشر Kaspersky Endpoint Security على أجهزة الكمبيوتر المُثبت عليها Kaspersky Endpoint Agent، سيستمر حل Kaspersky Anti Targeted Attack Platform (EDR) في العمل مع Kaspersky Endpoint Security. بالإضافة إلى ذلك، ستتم إزالة Kaspersky Endpoint Agent من الكمبيوتر. وسيحدث السلوك نفسه في النظام عند تحديث Kaspersky Endpoint Security إلى الإصدار 12.1 أو أحدث.

لا يتوافق Kaspersky Endpoint Security مع Kaspersky Endpoint Agent. ولا يمكنك تثبيت كلا هذين التطبيقين على الكمبيوتر نفسه.

يجب استيفاء الشروط التالية لكي يعمل Kaspersky Endpoint Security كجزء من Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform الإصدار 4.1 أو أحدث.
- Kaspersky Security Center الإصدار 13.2 أو أحدث (بما في ذلك عميل الشبكة) في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة Endpoint Detection and Response (KATA).

خطوات ترحيل تكوين [KES+KEA] إلى [KES+العامل المدمج] لحل EDR (KATA)

1. **ترقية المكون الإضافي لتطبيق Kaspersky Endpoint Security Management**

   يمكن إدارة مكون EDR (KATA) باستخدام الإصدار 12.1 من Kaspersky Endpoint Security Management Plug-in أو أحدث. بناءً على نوع وحدة تحكم Kaspersky Security Center التي تستخدمها، قم بتحديث المكون الإضافي للإدارة في وحدة تحكم الإدارة (MMC) أو المكون الإضافي للويب في Web Console.

2. **ترحيل السياسات والمهام**

   انقل إعدادات Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows. الخيارات التالية متاحة:

   - معالج ترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security. لا يعمل معالج الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security إلا في Web Console

   كيفية ترحيل إعدادات السياسة والمهام من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security في Web Console

في النافذة الرئيسية لـ Web Console، حدد **Operations ← Migration from Kaspersky Endpoint Agent**.

يؤدي هذا إلى تشغيل معالج ترحيل السياسات والمهام. اتبع تعليمات المعالج.

الخطوة 1. سياسة الترحيل

ينشئ معالج الترحيل سياسة جديدة تدمج إعدادات Kaspersky Endpoint Security وسياسات Kaspersky Endpoint Agent. وفي قائمة السياسات، حدد سياسات Kaspersky Endpoint Agent التي تريد دمج إعداداتها مع سياسة Kaspersky Endpoint Security. وانقر فوق سياسة Kaspersky Endpoint Agent لتحديد سياسة Kaspersky Endpoint Security التي تريد دمج الإعدادات معها. وتأكد من تحديد السياسات الصحيحة وانتقل إلى الخطوة التالية.

الخطوة 2. ترحيل المهام

لا يدعم معالج الترحيل مهام EDR (KATA). تخط هذه الخطوة.

الخطوة 3. اكتمال المعالج

أغلق المعالج. ونتيجة للمعالج، سيتم إنشاء سياسة Kaspersky Endpoint Security جديدة. تدمج السياسة الإعدادات من Kaspersky Endpoint Security وKaspersky Endpoint Agent. ويطلق على السياسة اسم <اسم سياسة Kaspersky Endpoint Security> و<اسم سياسة Kaspersky Endpoint Agent>. وتكون حالة السياسة الجديدة Inactive. وللمتابعة، قم بتغيير حالات سياسات Kaspersky Endpoint Agent وKaspersky Endpoint Security إلى Inactive وقم بتفعيل السياسة المدمجة الجديدة.

يتخطى معالج الترحيل في Web Console إعدادات السياسة التالية ولا يقوم بترحيلها:

- حظر تعديل الإعدادات **Settings for connecting to KATA servers** ("قفل").

  بشكل افتراضي، يمكن تعديل الإعدادات ("القفل" مفتوح). لذلك لا يتم تطبيق الإعدادات على الكمبيوتر. ويجب حظر تعديل الإعدادات وإغلاق "القفل".

- حاوية التشفير.

  إذا كنت تستخدم المصادقة ثنائية الاتجاه للاتصال بخوادم Central Node، فيجب إعادة إضافة حاوية التشفير.

نظرًا لأن معالج الترحيل لا يقوم بترحيل هذه الإعدادات، فقد تواجه أخطاء عند توصيل الكمبيوتر بخوادم Central Node. ولإصلاح الأخطاء، تحتاج إلى الانتقال إلى خصائص السياسة وتكوين إعدادات الاتصال.

- معالج قياسي لتحويل مجموعة السياسات والمهام. لا يتوفر معالج تحويل مجموعة السياسات والمهام إلا في وحدة تحكم الإدارة (MMC). للحصول على المزيد من التفاصيل عن معالج تحويل مجموعة السياسات والمهام، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

للتأكد من عمل Kaspersky Endpoint Security بشكل صحيح على الخوادم، يوصى بإضافة الملفات المهمة لعمل الخادم إلى المنطقة الموثوقة. وبالنسبة لخوادم SQL، يجب إضافة ملفات قاعدة بيانات MDF وLDF. وبالنسبة لخوادم Microsoft Exchange، يجب إضافة ملفات CHK وEDB وJRS وLOG وJSL. ويمكنك استخدام الأقنعة، على سبيل المثال، `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

لا يتم ترحيل استثناءات القياس عن بعد لحل EDR من سياسة Kaspersky Endpoint Agent إلى سياسة Kaspersky Endpoint Security. ويحتوي Kaspersky Endpoint Security على أدوات استثناءات خاصة به - التطبيقات الموثوقة. وتم تحسين تشغيل Kaspersky Endpoint Security بحيث لا يتسبب غياب استثناءات القياس عن بعد الفردية لحل EDR في أي حمل إضافي على الكمبيوتر الخاص بك مقارنة بتطبيق Kaspersky Endpoint Agent. يستخدم Kaspersky Endpoint Security القياس عن بُعد ليس فقط لحل EDR (KATA)، لكن أيضًا لتشغيل مكونات حماية التطبيق. ولذلك، ليست هناك حاجة لنقل استثناءات القياس عن بعد الفردية لحل EDR. وإذا واجهت انخفاضًا في أداء الكمبيوتر، تحقق من تشغيل التطبيق (راجع الخطوة 7 التحقق من الأداء).

3 ترخيص وظيفة (KATA) EDR)

لتفعيل Kaspersky Endpoint Security كجزء من حل Kaspersky Anti Targeted Attack Platform، تحتاج إلى ترخيص منفصل للوظيفة الإضافية لحل Kaspersky Endpoint Detection and Response. يمكنك استبدال المفتاح باستخدام مهمة Add key. نتيجة لذلك، ستتم إضافة مفتاحين إلى التطبيق: Kaspersky Endpoint Security و(KATA) Kaspersky Endpoint Detection and Response).

يتضمن تفعيل ترخيص الوظيفة الإضافية لحل (KATA) Kaspersky Endpoint Detection and Response) على أجهزة الكمبيوتر المزودة بميزات EDR Optimum أو EDR Expert التي تم تفعيلها مسبقًا الاعتبارات الخاصة التالية:

- إذا كنت تستخدم ملف مفتاح لترخيص Kaspersky Endpoint Security مع ميزات EDR Optimum أو EDR Expert، لا يمكنك تفعيل ترخيص الوظيفة الإضافية لحل (KATA) Kaspersky Endpoint Detection and Response) المستقل. ويمكنك إما التبديل إلى استخدام رمز تفعيل للترخيص، أو الاتصال بمزود الخدمة للحصول على ملف مفتاح جديد لتفعيل ميزات Kaspersky Endpoint Security وEDR. وسيوفر مزود الخدمة ملف مفتاح واحدًا أو أكثر للترخيص.

- إذا كنت تستخدم ملف مفتاح لترخيص Kaspersky Endpoint Security بدون ميزات EDR Optimum أو EDR Expert، يمكنك تفعيل ترخيص الوظيفة الإضافية لحل (KATA) Kaspersky Endpoint Detection and Response) المستقل.

- إذا كنت تستخدم رمز تفعيل للترخيص، سيعيد خادم تفعيل Kaspersky إصدار المفاتيح تلقائيًا، وستصبح ميزات (KATA) EDR متاحة تلقائيًا. وفي هذه الحالة، سيتم تعطيل EDR Optimum وEDR Expert.

- يتيح لك Kaspersky Endpoint Security إضافة ما يصل إلى مفتاحين فعالين: مفتاح Kaspersky Endpoint Security ومفتاح نوع الوظيفة الإضافية. ويمكنك أيضًا إضافة ما يصل إلى مفتاحين احتياطيين. مفتاح احتياطي لتطبيق Kaspersky Endpoint Security واحد ومفتاح احتياطي لنوع الوظيفة الإضافية.

4 تثبيت / ترقية تطبيق Kaspersky Endpoint Security

لترحيل وظائف (KATA) EDR) أثناء تثبيت تطبيق أو ترقيته، يوصى باستخدام مهمة التثبيت عن بعد. وعند إنشاء مهمة تثبيت عن بُعد، تحتاج إلى تحديد مكون (KATA) EDR) في إعدادات حزمة التثبيت.

يمكنك أيضًا ترقية التطبيق باستخدام الطرق التالية:

- استخدام خدمة تحديث Kaspersky.

- محليًا، عن طريق استخدام معالج الإعداد.

يدعم Kaspersky Endpoint Security تحديد المكونات تلقائيًا عند ترقية التطبيق على جهاز كمبيوتر مُثبت عليه تطبيق Kaspersky Endpoint Agent. ويعتمد التحديد التلقائي للمكونات على أذونات حساب المستخدم الذي ينفذ ترقية التطبيق.

إذا كنت تقوم بترقية Kaspersky Endpoint Security باستخدام ملف EXE أو MSI تحت حساب النظام (SYSTEM)، فإن Kaspersky Endpoint Security يكتسب الوصول إلى التراخيص الحالية لحلول Kaspersky. ولذلك، إذا كان الكمبيوتر مُثبتًا عليه على سبيل المثال، Kaspersky Endpoint Agent وتم تفعيل حل (KATA) EDR)، يقوم مُثبّت Kaspersky Endpoint Security تلقائيًا بتكوين مجموعة المكونات ويحدد مكون (KATA) EDR). ويؤدي هذا إلى تبديل Kaspersky Endpoint Security إلى استخدام العامل المضمن ويزيل Kaspersky Endpoint Agent. ويتم عادة تشغيل مُثبّت MSI تحت حساب النظام (SYSTEM) عند الترقية عبر خدمة تحديث Kaspersky أو عند نشر حزمة تثبيت عبر Kaspersky Security Center.

إذا كنت تنفذ ترقية Kaspersky Endpoint Security باستخدام ملف MSI تحت حساب مستخدم غير ذي امتيازات، فإن Kaspersky Endpoint Security يفتقر إلى الوصول إلى التراخيص الحالية لحلول Kaspersky. وفي هذه الحالة، يحدد Kaspersky Endpoint Security تلقائيًا المكونات وفقًا لمجموعة من مكونات Kaspersky Endpoint Agent. وبعد ذلك، يقوم Kaspersky Endpoint Security بالتبديل إلى استخدام العامل المضمن ويزيل Kaspersky Endpoint Agent.

يدعم Kaspersky Endpoint Security الترقية بدون إعادة تشغيل الكمبيوتر. ويمكنك تحديد وضع ترقية التطبيق في خصائص السياسة.

5 التحقق من تشغيل التطبيق

إذا كانت حالة الكمبيوتر بعد تثبيت التطبيق أو ترقيته هي Critical في وحدة تحكم Kaspersky Security Center:

- تأكد من تثبيت الإصدار 13.2 أو أحدث من عميل الشبكة على الكمبيوتر.

- تحقق من حالة تشغيل العامل المُضمن عن طريق عرض Application components status report. إذا كانت حالة أحد المكونات Not installed ، فقم بتثبيت المكونات باستخدام مهمة Change application components. إذا كانت حالة أحد المكونات هي غير مشمول بالترخيص، تأكد من تفعيل الوظيفة المضمنة.

- تأكد من قبولك لبيان Kaspersky Security Network في السياسة الجديدة لتطبيق Kaspersky Endpoint Security for Windows.

6. **التحقق من الاتصال بخادم Kaspersky Anti Targeted Attack Platform**

التحقق من الاتصال بخادم Kaspersky Anti Targeted Attack Platform. للقيام بذلك:

1. التحقق من امتلاكك لشهادة صالحة.
2. التحقق من إعدادات اتصال الخادم.
3. التحقق من سجل الأحداث.

في حالة إنشاء اتصال بالخادم، يرسل التطبيق الحدث Successful connection to the Kaspersky Anti Targeted Attack Platform server. وإذا لم يكن هناك حدث اتصال ناجح ولم تكن هناك أحداث بها أخطاء اتصال، تحقق من إعدادات سجل الأحداث وقم بتمكين إرسال الأحداث لتطبيق Endpoint Detection and Response (KATA).

لا تؤثر حالة اتصال الخادم على حالة الكمبيوتر في وحدة تحكم Kaspersky Security Center. ولذلك، إذا لم يكن هناك اتصال بالخادم، فلا يزال بإمكان الكمبيوتر الحصول على الحالة OK. تحقق من سجل الأحداث للتحقق من الاتصال بالخادم.

7. **التحقق من الأداء**

إذا كان أداء الكمبيوتر الخاص بك قد تباطأ بعد تثبيت أو تحديث أحد التطبيقات، يمكنك تحسين نقل البيانات. للقيام بذلك:

1. قم بتعطيل مكون EDR (KATA) وتحقق من أن تدهور الأداء سببه EDR (KATA).
2. للتطبيقات الموثوقة، أوقف تشغيل مجموعة القياس عن بُعد في عمليات الإدخال لوحدة التحكم (يتم تمكينها افتراضيًا).
3. أضف التطبيقات التي تتسبب في انخفاض أداء الكمبيوتر إلى قائمة التطبيقات الموثوقة.
4. اتصل بالدعم الفني من Kaspersky. سيساعدك خبراء الدعم في تكوين تصفية القياس عن بُعد في Kaspersky Anti Targeted Attack Platform. وسيؤدي ذلك إلى تقليل حجم حركة المرور. وإذا تأثر أداء الكمبيوتر بتطبيق معين، فقم بإرفاق حزمة توزيع هذا التطبيق بالطلب.

إدارة العزل

العزل هو مخزن محلي خاص على الكمبيوتر. ويستطيع المستخدم عزل الملفات التي يعتبرها المستخدم خطرة على جهاز الكمبيوتر. ويتم تخزين الملفات المعزولة في حالة مشفرة ولا تهدد أمن الجهاز. ولا يستخدم Kaspersky Endpoint Security العزل إلا عند العمل مع حلول Detection and Response: EDR Optimum وEDR Expert وKATA (EDR) وKaspersky Sandbox. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل حول إدارة العزل كجزء من الحلول، يرجى الرجوع إلى تعليمات Kaspersky Sandbox وتعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert وتعليمات Kaspersky Anti Targeted Attack Platform.

يستخدم Kaspersky Endpoint Security حساب النظام (SYSTEM) لعزل الملفات.

يمكنك تكوين إعدادات العزل فقط في Kaspersky Security Center Web Console. ويمكنك أيضًا استخدام Kaspersky Security Center لإدارة الكائنات المعزولة (استعادة، حذف، إضافة، وما إلى ذلك). ومحليًا، على الكمبيوتر، يمكنك فقط استعادة الكائن باستخدام سطر الأوامر.

تكوين الحد الأقصى لحجم العزل

افتراضيًا، يقتصر حجم العزل على 200 ميجابايت. بعد الوصول إلى الحد الأقصى للحجم، يحذف Kaspersky Endpoint Security تلقائيًا أقدم الملفات من العزل.

في حالة نشر حل Kaspersky Anti Targeted Attack Platform (EDR) في مؤسستك، فنحن نوصي بزيادة حجم العزل. عند إجراء فحص YARA، قد يواجه التطبيق تفريغ ذاكرة كبير. وإذا تجاوز حجم تفريغ الذاكرة حجم العزل، فسينتهي فحص YARA بخطأ ولا يتم عزل تفريغ الذاكرة. ونوصي بتعيين حجم عزل مساويًا للحجم الإجمالي لذاكرة الوصول العشوائي على الكمبيوتر (على سبيل المثال، 8 جيجا بايت).

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **التقارير والمخزن**.
5. في قسم **العزل**، قم بتكوين حجم العزل:
   - **تقييد حجم العزل إلى N م ب**. الحد الأقصى لحجم العزل بالميجابايت. على سبيل المثال، يمكنك ضبط الحد الأقصى لحجم العزل على 200 ميجابايت. عندما يصل العزل إلى الحجم الأقصى، يرسل Kaspersky Endpoint Security الحدث المقابل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يوقف التطبيق عزل الكائنات الجديدة. ويجب إفراغ العزل يدويًا.
   - **إخطار عندما يصل تخزين العزل إلى N في المائة**. قيمة الحد للعزل. على سبيل المثال، يمكنك تعيين حد العزل إلى 50%. عندما يصل العزل إلى الحد، يرسل Kaspersky Endpoint Security الحدث المقابل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يستمر التطبيق في عزل الكائنات الجديدة.
6. احفظ تغييراتك.

كيفية تكوين الحد الأقصى لحجم العزل في Web Console وCloud Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General settings** ← **Reports and Storage**.
5. في قسم **Quarantine**، قم بتكوين حجم العزل:
   - **Limit the size of Quarantine to N MB**. الحد الأقصى لحجم العزل بالميجابايت. على سبيل المثال، يمكنك ضبط الحد الأقصى لحجم العزل على 200 ميجابايت. عندما يصل العزل إلى الحجم الأقصى، يرسل Kaspersky Endpoint Security الحدث المقابل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يوقف التطبيق عزل الكائنات الجديدة. ويجب إفراغ العزل يدويًا.
   - **Notify when the Quarantine storage reaches N percent**. قيمة الحد للعزل. على سبيل المثال، يمكنك تعيين حد العزل إلى 50%. عندما يصل العزل إلى الحد، يرسل Kaspersky Endpoint Security الحدث المقابل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يستمر التطبيق في عزل الكائنات الجديدة.
6. احفظ تغييراتك.

إرسال بيانات عن الملفات المعزولة إلى Kaspersky Security Center

لتنفيذ الإجراءات مع الكائنات المعزولة في Web Console، يجب تمكين إرسال بيانات الملفات المعزولة إلى خادم الإدارة. على سبيل المثال، يمكنك تنزيل ملف من العزل للتحليل في وحدة تحكم ويب. ويجب تمكين إرسال بيانات الملفات المعزولة لكي تعمل جميع وظائف Kaspersky Sandbox و Kaspersky Endpoint Detection and Response.

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **السياسات**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **التقارير والمخزن**.
5. في القسم **نقل البيانات إلى خادم الإدارة**، انقر على الزر **الإعدادات**.
6. في النافذة التي تفتح، حدد خانة الاختيار **حول ملفات العزل**.
7. احفظ تغييراتك.

كيفية تمكين نقل بيانات الملفات المعزولة إلى Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Devices** ← **Policies & Profiles**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General settings** ← **Reports and Storage**.
5. في القسم **Data transfer to Administration Server**، حدد خانة الاختيار **About Quarantine files**.
6. احفظ تغييراتك.

نتيجة لذلك، يمكنك عرض قائمة بالملفات المعزولة على جهاز الكمبيوتر الخاص بك في Kaspersky Security Center Console. ويمكنك استخدام Kaspersky Security Center لإدارة الكائنات المعزولة (استعادة، حذف، إضافة، وما إلى ذلك). وللمزيد من التفاصيل عن العمل مع العزل، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

استعادة الملفات من العزل

بشكل افتراضي، يستعيد Kaspersky Endpoint Security الملفات إلى مجلدها الأصلي. في حالة حذف المجلد الوجهة أو لم يكن لدى المستخدم حقوق الوصول إلى هذا المجلد، يضع التطبيق الملف في المجلد `%DataRoot%\QB\Restored`. ويجب عليك بعد ذلك نقل الملف يدويًا إلى المجلد الوجهة.

لاستعادة الملفات من العزل:

1. في نافذة Web Console الرئيسية، حدد **Operations** ← **Repositories** ← **Quarantine**.

2. يفتح هذا قائمة الملفات في العزل؛ وفي تلك القائمة، حدد الملفات التي تريد استعادتها وانقر فوق **Restore**.

يستعيد Kaspersky Endpoint Security هذا الملف. إذا كان المجلد الوجهة يحتوي بالفعل على ملف بالاسم نفسه، فسوف يلغي التطبيق استعادة الملف. بالنسبة لحلي EDR Optimum وEDR Expert، يحذف التطبيق الملف بعد الاستعادة. وبالنسبة للحلول الأخرى، تحتفظ التطبيقات بنسخة من الملف في العزل.

دليل الترحيل من KSWS إلى KES

بدءًا من الإصدار 11.8.0، يدعم Kaspersky Endpoint Security for Windows الوظائف الأساسية لحل Kaspersky Security for Windows Server (KSWS). يحمي Kaspersky Security for Windows Server الخوادم التي تعمل بأنظمة تشغيل Microsoft Windows والمخازن المتصلة بالشبكة ضد الفيروسات وتهديدات أمان الكمبيوتر الأخرى التي تتعرض لها الخوادم والمخازن المتصلة بالشبكة أثناء تبادل الملفات. وللحصول على معلومات مفصلة حول طريقة عمل الحل، يرجى الرجوع إلى تعليمات Kaspersky Security for Windows Server. بدءًا من Kaspersky Endpoint Security 11.8.12.0، يمكنك الترحيل من Kaspersky Security for Windows Server إلى Kaspersky Endpoint Security for Windows واستخدام الحل نفسه لحماية محطات العمل والخوادم.

متطلبات البرنامج

قبل أن تبدأ الترحيل من KSWS إلى KES، تأكد أن الخادم الخاص بك يلبي متطلبات الأجهزة والبرامج لتطبيق Kaspersky Endpoint Security for Windows. وتختلف قوائم إصدارات أنظمة التشغيل المدعومة لتطبيق KES وKSWS. على سبيل المثال، لا يدعم KES الخوادم التي تعمل بنظام Windows Server 2003.

الحد الأدنى لمتطلبات البرامج للترحيل من KSWS إلى KES:

- Kaspersky Endpoint Security for Windows 12.0.
- Kaspersky Security 11.0.1 for Windows Server.

  إذا كان لديك إصدار سابق مُثبت من Kaspersky Security for Windows Server، نوصي بترقية التطبيق إلى أحدث إصدار. ولا يدعم معالج تحويل السياسات والمهام الإصدارات السابقة من Kaspersky Security for Windows Server.
- Kaspersky Security Center 14.2

  إذا كان لديك إصدار مُثبت سابق من Kaspersky Security Center، قم بتحديثه إلى الإصدار 14.2 أو أحدث. وفي هذا الإصدار من Kaspersky Security Center، يتيح لك معالج تحويل مجموعة السياسات والمهام ترحيل السياسات إلى ملف تعريف بدلاً من سياسة. وفي هذا الإصدار من Kaspersky Security Center، يتيح لك معالج تحويل مجموعة السياسات والمهام أيضًا ترحيل نطاق أوسع من إعدادات السياسة.
- Kaspersky Endpoint Agent 3.10.

  إذا كان لديك إصدار سابق مُثبت من Kaspersky Endpoint Agent، نوصي بترقية التطبيق إلى أحدث إصدار. ويدعم Kaspersky Endpoint Security ترحيل تكوين [KSWS+KEA] إلى [KES+العامل المدمج] بدءًا من الإصدار Kaspersky Endpoint Agent 3.10.

توصيات الترحيل

عند الترحيل من KSWS إلى KES، اتبع التوصيات التالية:

- خطط لوقت الترحيل من KSWS إلى KES مقدمًا. واختر وقتًا تعمل فيه الخوادم تحت أخف حمل، على سبيل المثال، خلال عطلة نهاية الأسبوع.
- بعد الترحيل، قم بتشغيل مكونات التطبيق تدريجيًا. أي، على سبيل المثال، ابدأ بتمكين مكون الحماية من تهديدات الملفات وحده، ثم قم بتمكين مكونات الحماية الأخرى، ثم قم بتمكين مكونات التحكم، وما إلى ذلك. وفي كل خطوة، يجب التأكد من أن التطبيق يعمل بشكل صحيح، ومراقبة أداء الخادم. وتختلف بنية KES عن KSWS، وبالتالي قد يتصرف نظام التشغيل بشكل مختلف أيضًا.
- نفذ الترحيل بشكل تدريجي. قم أولاً بترحيل خادم واحد، ثم عدة خوادم، ثم نفذ الترحيل على جميع خوادم المؤسسة.
- قم بترحيل الأنواع مختلفة من الخوادم بشكل منفصل. وهذا يعني، على سبيل المثال، ترحيل خوادم قاعدة البيانات أولاً، ثم خوادم البريد، وما إلى ذلك.
- يتضمن الترحيل على الخوادم عالية التحميل بعض الاعتبارات الخاصة.

خطوات الترحيل

يتم إجراء الترحيل من KSWS إلى KES بشكل شبه تلقائي. وهذا ضروري بسبب اختلاف بنيات التطبيقات. ولترحيل إعدادات السياسة، يجب تشغيل معالج تحويل مجموعة السياسات والمهام (معالج الترحيل). وبعد ترحيل إعدادات السياسة، يجب عليك تكوين الإعدادات يدويًا التي يتعذر على معالج الترحيل ترحيلها تلقائيًا (على سبيل المثال، إعدادات حماية كلمة المرور). وبعد الترحيل، يوصى أيضًا بالتحقق مما إذا كان معالج الترحيل قد قام بترحيل جميع الإعدادات بشكل صحيح.

قم بالترحيل من KSWS إلى KES بالترتيب التالي:

1. **ترحيل مهام وسياسات KSWS**

   بعد ترحيل السياسات والمهام، يجب عليك تنفيذ خطوات تكوين إضافية. ونوصي أيضًا بالتأكد من أن Kaspersky Endpoint Security يوفر المستوى الضروري من الأمان بعد الترحيل من KSWS.

   لا يتوفر معالج تحويل مجموعة السياسات والمهام لتطبيق Kaspersky Security for Windows Server إلا في وحدة تحكم الإدارة (MMC). ولا يمكن ترحيل إعدادات السياسة والمهام في Web Console وKaspersky Security Center Cloud Console.

2. **تثبيت Kaspersky Endpoint Security**

   يمكنك تثبيت Kaspersky Endpoint Security بالطرق التالية:

   - تثبيت KES بعد إزالة KSWS (موصى به).
   - تثبيت KES فوق KSWS.

3. **تفعيل KES بمفتاح KSWS**

4. **تأكد أن التطبيق في حالة عمل بعد الترحيل**

   بعد الترحيل من KSWS إلى KES، تأكد أن التطبيق يعمل بشكل صحيح. تحقق من حالة الخادم في وحدة التحكم (يجب أن تكون جيدة). تأكد من عدم الإبلاغ عن أي أخطاء في التطبيق، وتحقق أيضًا من وقت آخر اتصال بخادم الإدارة ووقت آخر تحديث لقاعدة البيانات وحالة حماية الخادم.

انتبه بشكل خاص إلى ترحيل قوائم الاستثناء والتطبيقات الموثوقة وعناوين الويب الموثوقة وقواعد التحكم في التطبيقات.

مطابقة مكونات KSWS وKES

عند الترحيل من KSWS إلى KES، يتم ترحيل مجموعة المكونات فقط عند تثبيت التطبيق محليًا.

تطابق Kaspersky Security for Windows Server وKaspersky Endpoint Security for Windows

مكون Kaspersky Security for Windows Server	مكون Kaspersky Endpoint Security for Windows
Basic functionality	نواة البرنامج ومهام الفحص
Log Inspection	فحص السجل
Device Control	التحكم في الجهاز
Firewall Management	(غير مدعوم) يتم تنفيذ وظائف جدار حماية KSWS بواسطة جدار الحماية على مستوى النظام. وفي KES يكون مكون منفصل مسؤولاً عن وظيفة جدار الحماية. وبعد الترحيل، يمكنك تكوين جدار حماية Kaspersky Endpoint Security.
File Integrity Monitor	مراقبة سلامة الملف
Exploit Prevention	منع الاستغلال
System Tray Icon	(غير مدعوم)

	يمكنك تكوين تفاعل المستخدم في إعدادات واجهة التطبيق.
Integration with Kaspersky Security Center	موصّل وكيل الشبكة
Endpoint Agent	(غير مدعوم) في Kaspersky Endpoint Security 11.9.0، لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من مجموعة توزيع Kaspersky Endpoint Security. ويجب عليك تنزيل حزمة توزيع Kaspersky Endpoint Agent بشكل منفصل.
Network Threat Protection	الحماية من تهديدات الشبكة
Anti-Cryptor	اكتشاف السلوك
Anti-Cryptor for NetApp	(غير مدعوم)
Traffic Security	الحماية من تهديدات الويب الحماية من تهديدات البريد التحكم في الويب
On-Demand Scan	نواة البرنامج ومهام الفحص
ICAP Network Storage Protection	(غير مدعوم) لا يدعم Kaspersky Endpoint Security مكونات حماية المخازن الموصلة بالشبكة. وإذا كنت بحاجة إلى هذه المكونات، يمكنك الاستمرار في استخدام Kaspersky Security for Windows Server.
RPC Network Storage Protection	(غير مدعوم) لا يدعم Kaspersky Endpoint Security مكونات حماية المخازن الموصلة بالشبكة. وإذا كنت بحاجة إلى هذه المكونات، يمكنك الاستمرار في استخدام Kaspersky Security for Windows Server.
Real-Time File Protection	الحماية من تهديدات الملفات
Script Monitoring	(غير مدعوم) ويتم التعامل مع مراقبة البرنامج النصي بواسطة مكونات أخرى، على سبيل المثال، حماية AMSI.
KSN Usage	Kaspersky Security Network
Applications Launch Control	التحكم في التطبيقات
Performance counters	(غير مدعوم)

مطابقة إعدادات KSWS وKES

عند ترحيل السياسات والمهام، يتم تكوين KES وفقًا لإعدادات KSWS. ويتم تعيين إعدادات مكونات التطبيق التي لا يتضمنها KSWS على القيم الافتراضية.

Application settings

Scalability, interface and scanning settings

لا يتم دعم إعدادات التطبيق في Kaspersky Endpoint Security for Windows.

إعدادات التطبيق

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Scalability settings	(عدم الترحيل) يدير Kaspersky Endpoint Security جميع عمليات العمل.
Show System Tray Icon	(عدم الترحيل) على جهاز كمبيوتر عميل، تتوافر النافذة الرئيسية لبرنامج Kaspersky Endpoint Security والأيقونة الموجودة في منطقة إخطار Windows افتراضيًا. في قائمة السياق الخاصة بالرمز، يُمكن للمستخدم تنفيذ العمليات مع برنامج Kaspersky Endpoint Security. يعرض أيضًا برنامج Kaspersky Endpoint Security إخطارات فوق رمز التطبيق. يمكنك تكوين تفاعل المستخدم في إعدادات واجهة التطبيق.
Restore file attributes after scanning	(عدم الترحيل) يستعيد Kaspersky Endpoint Security سمات الملف تلقائيًا بعد فحص ملف.
Limit CPU usage for scanning threads	(عدم الترحيل) لا يحد Kaspersky Endpoint Security من استخدام وحدة المعالجة المركزية عند الفحص. ويمكنك تكوين مهمة للعمل عندما يعمل الكمبيوتر تحت الحد الأدنى من الحمل.
Folder for temporary files created during scanning	(عدم الترحيل) يضع Kaspersky Endpoint Security الملفات المؤقتة في المجلد C:\Windows\Temp folder.
HSM system settings	(عدم الترحيل) لا يدعم Kaspersky Endpoint Security أنظمة HSM.

Security and reliability

يتم ترحيل إعدادات أمان KSWS إلى القسم **الإعدادات العامة**، **إعدادات التطبيق** والقسم الفرعي **الواجهة**.

إعدادات أمان التطبيق

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Protect application processes from external threats	**تمكين الدفاع الذاتي** (القسم الفرعي **إعدادات التطبيق**)
Apply password protection	(عدم الترحيل) يحتوي Kaspersky Endpoint Security على ميزة حماية كلمة المرور المضمنة (انظر القسم الفرعي **الواجهة**).
Perform task recovery	(عدم الترحيل) يستعيد Kaspersky Endpoint Security تلقائيًا مهام فحص البرامج الضارة فقط. يدير Kaspersky Endpoint Security مهام أخرى وفقًا لجدولة.
Do not start scheduled scan tasks	**تأجيل تشغيل المهام المجدولة أثناء التشغيل على طاقة البطارية** (القسم الفرعي **إعدادات التطبيق**)
Stop current scan tasks	(عدم الترحيل) عندما يتم تشغيل الكمبيوتر بواسطة UPS (وحدة طاقة احتياطية)، لا يوقف Kaspersky Endpoint Security مهام الفحص التي يتم تشغيلها بالفعل.

Connection settings

يتم ترحيل إعدادات تفاعل خادم الإدارة إلى القسم **الإعدادات العامة**، **إعدادات الشبكة** والقسم الفرعي **إعدادات التطبيق**.

إعدادات تفاعل خادم الإدارة

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Proxy server settings	**إعدادات الخادم الوكيل** (القسم الفرعي **إعدادات الشبكة**)
Do not use proxy server for local addresses	**تجاوز الخادم الوكيل للعناوين المحلية** (القسم الفرعي **إعدادات الشبكة**)
Proxy server authentication settings	**استخدام مصادقة الخادم الوكيل** (القسم الفرعي **إعدادات الشبكة**) لا يدعم Kaspersky Endpoint Security مصادقة NTLM. وفي حالة تمكين مصادقة NTLM في إعدادات KSWS، يجب عليك بعد الترحيل تكوين مصادقة الخادم الوكيل وتكوين اسم مستخدم وكلمة مرور. لا يتم ترحيل كلمة مرور مصادقة الخادم الوكيل. وبعد ترحيل السياسة، يجب إدخال كلمة المرور يدويًا.
Use Kaspersky Security Center as a proxy server when activating the application	**استخدام Kaspersky Security Center كالخادم الوكيل للتفعيل** (القسم الفرعي **إعدادات التطبيق**)

Run local system tasks

يتجاهل Kaspersky Endpoint Security إعدادات تشغيل مهام النظام المحلي في Kaspersky Security for Windows Server. ويمكنك تكوين استخدام مهام KES المحلية تحت **المهام المحلية**، **إدارة المهام**. ويمكنك أيضًا تكوين جدول زمني لتشغيل مهام فحص البرامج الضارة وتحديث في خصائص هذه المهام.

Supplementary

Trusted zone

يتم ترحيل إعدادات المنطقة الموثوقة في KSWS إلى القسم **الإعدادات العامة**، القسم الفرعي **الاستثناءات**.

إعدادات المنطقة الموثوقة

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Object to scan ((Exclusions	**استثناءات الفحص** (استثناءات الفحص) تختلف الطرق المستخدمة بواسطة KSWS وKES لتحديد الكائنات. وعند الترحيل، يدعم KES الاستثناءات المحددة كملفات فردية أو مسارات إلى ملف / مجلد. وإذا كان KSWS يحتوي على استثناءات تم تكوينها كمنطقة محددة مسبقًا أو عنوان URL لبرنامج نصي، فلن يتم ترحيل هذه الاستثناءات. وبعد الترحيل، يجب إضافة هذه الاستثناءات يدويًا.
Apply also to subfolders ((Exclusions	**تضمين المجلدات الفرعية** (استثناءات الفحص)
Objects to detect ((Exclusions	**اسم الكائن** (استثناءات الفحص)
Exclusion usage scope ((Exclusions	**مكونات الحماية** (استثناءات الفحص) في حالة تحديد مكون واحد على الأقل في KSWS، فإن KES يطبق الاستثناءات على جميع مكونات التطبيق.
Comment ((Exclusions	**تعليق** (استثناءات الفحص)
Trusted process (Trusted (process	**التطبيقات الموثوقة** تختلف طرق اختيار العملية الموثوقة / التطبيق الموثوق في KSWS وKES. وعند الترحيل، يدعم KES التطبيقات الموثوقة التي تم تكوينها كمسار إلى الملف القابل للتنفيذ او قناع. وإذا كان KSWS يتضمن عمليات موثوقة تم تكوينها كملف، فلن يتم ترحيل هذه العمليات الموثوقة. وبعد الترحيل، يجب إضافة هذه العمليات الموثوقة يدويًا.
Do not check file backup operations (Trusted (process	**عدم مراقبة نشاط التطبيق** (التطبيقات الموثوقة)

Removable drives scan

يتم ترحيل إعدادات فحص محركات الأقراص القابلة للإزالة إلى القسم **المهام المحلية**، القسم الفرعي **فحص محركات الأقراص القابلة للإزالة**.

إعدادات فحص محركات الأقراص القابلة للإزالة

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Scan removable drives on connection via USB	**الإجراء عند توصيل محرك أقراص قابل للإزالة**
Scan removable drives if its stored data volume does (not exceed (MB	**الحد الأقصى لحجم الأقراص القابلة للإزالة**
Scan with security level: • Maximum protection • Recommended • Maximum performance	**الإجراء عند توصيل محرك أقراص قابل للإزالة**: • **فحص مفصل** • **فحص سريع** تتوافق مستويات أمان KSWS مع أوضاع فحص KES على النحو التالي: • Maximum protection – فحص مفصل. • Recommended – فحص سريع. • Maximum performance – فحص سريع.

User permissions for application management

لا يدعم Kaspersky Endpoint Security تعيين أذونات وصول المستخدم لإدارة التطبيق وإدارة خدمة التطبيق. ويمكنك تكوين إعدادات الوصول للمستخدمين ومجموعات المستخدمين لإدارة التطبيق في Kaspersky Security Center.

User access permissions for Kaspersky Security Service management

لا يدعم Kaspersky Endpoint Security تعيين أذونات وصول المستخدم لإدارة التطبيق وإدارة خدمة التطبيق. ويمكنك تكوين إعدادات الوصول للمستخدمين ومجموعات المستخدمين لإدارة التطبيق في Kaspersky Security Center.

Storages

يتم ترحيل إعدادات مخزن KSWS إلى القسم **الإعدادات العامة**، القسم الفرعي **التقارير والمخزن** والقسم **الحماية من التهديدات الأساسية**، القسم الفرعي **الحماية من تهديدات الشبكة**.

إعدادات المخزن

إعدادات Kaspersky Security for Windows Security	إعدادات Kaspersky Endpoint Security for Windows
Backup folder	(عدم الترحيل) يحفظ Kaspersky Endpoint Security النسخ الاحتياطية من الملفات في المجلد C:\ProgramData\Kaspersky Lab\KES.21.13\QB.
Maximum Backup size ((MB	**تقييد حجم النسخ الاحتياطي إلى N MB** (**الإعدادات العامة** ← القسم **التقارير والمخزن**)
Threshold value for (space available (MB	(عدم الترحيل) يسجل Kaspersky Endpoint Security حدث مساحة تخزين العزل على وشك النفاد عند الوصول إلى حد 50%.
Target folder for restoring objects	(عدم الترحيل) يستعيد Kaspersky Endpoint Security الملفات إلى مجلدها الأصلي.
Quarantine folder	(عدم الترحيل) يحفظ Kaspersky Endpoint Security النسخ الاحتياطية من الملفات في المجلد C:\ProgramData\Kaspersky Lab\KES.21.13\QB.
Maximum Quarantine size (MB)	(عدم الترحيل) يستخدم Kaspersky Endpoint Security النسخ الاحتياطي لتخزين الكائنات التي يحتمل إصابتها. وأثناء الترحيل، يتجاهل Kaspersky Endpoint Security إعدادات العزل.
Threshold value for space available (MB)	(عدم الترحيل) يستخدم Kaspersky Endpoint Security النسخ الاحتياطي لتخزين الكائنات التي يحتمل إصابتها. وأثناء الترحيل، يتجاهل Kaspersky Endpoint Security إعدادات العزل.
Target folder for restoring objects	(عدم الترحيل) يستعيد Kaspersky Endpoint Security الملفات إلى مجلدها الأصلي.
Unblock automatically in N	**حظر أجهزة الهجوم لأجل N دقيقة** (**الحماية من التهديدات الأساسية** ← القسم **الحماية من تهديدات الشبكة**)

Real-time server protection

Real-Time File Protection

يتم ترحيل إعدادات حماية الملفات في الوقت الحقيقي إلى القسم **الحماية من التهديدات الأساسية**، القسم الفرعي **الحماية من تهديدات الملفات**.

إعدادات حماية الملفات في الوقت الحقيقي

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Objects protection mode: • Smart mode • When run • On access • On access and modification	**وضع الفحص**: • **الوضع الذكي** • **عند التنفيذ** • **عند الوصول** • **عند الوصول والتعديل**.
Deeper analysis of launching processes	(عدم الترحيل) يدعم Kaspersky Endpoint Security وضع تحليل واحدًا فقط، وهو الوضع Optimal.
Heuristic analyzer: • Light • Medium • Deep	**التحليل المساعد على الاكتشاف**: • **فحص خفيف** • **فحص متوسط** • **فحص عميق**.
Apply Trusted Zone	(عدم الترحيل) يطبق Kaspersky Endpoint Security المنطقة الموثوقة على كل المكونات. ويمكنك تكوين الاستثناءات في إعدادات المنطقة الموثوقة.
Use KSN for protection	(عدم الترحيل) يستخدم Kaspersky Endpoint Security شبكة KSN لكل مكونات التطبيق.
Block access to network shared resources for the hosts that show malicious activity	(عدم الترحيل) بشكل افتراضي، يمنع Kaspersky Endpoint Security الوصول إلى موارد الشبكة المشتركة للمضيفين الذين يظهرون نشاطًا خبيثًا.
Launch critical areas scan when active infection is detected	(عدم الترحيل) لا يبدأ Kaspersky Endpoint Security مهمة فحص المناطق الحرجة عند اكتشاف إصابة نشطة.
Use Kaspersky Sandbox for protection	(عدم الترحيل) بشكل افتراضي، يرسل Kaspersky Endpoint Security الكائنات للفحص إلى Kaspersky Sandbox.
Protection scope	**نطاق الحماية**
Schedule settings	(عدم الترحيل) يستخدم Kaspersky Endpoint Security جدولته الخاصة لإيقاف الحماية من تهديدات الملفات مؤقتًا.

KSN Usage

يتم ترحيل إعدادات KSWS لشبكة Kaspersky Security Network إلى القسم **الحماية من التهديدات المتقدمة**، القسم الفرعي Kaspersky Security Network.

إعدادات Kaspersky Security Network

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
I confirm that I have fully read, understood, and accept the terms of participation in Kaspersky Security Network	**بيان Kaspersky Security Network** يطلب Kaspersky Endpoint Security الموافقة على بيان Kaspersky Security Network عند تثبيت التطبيق أو إنشاء سياسة جديدة أو تمكين استخدام Kaspersky Security Network.
Send data about scanned files	(عدم الترحيل) يرسل Kaspersky Endpoint Security بيانات حول الملفات المفحوصة تلقائيًا في حالة تمكين KSN.
Send data about requested URLs	(عدم الترحيل) يرسل Kaspersky Endpoint Security بيانات حول عناوين URL المطلوبة تلقائيًا في حالة تمكين KSN.
Send Kaspersky Security Network statistics	**تمكين وضع KSN الموسع**
Accept the terms of the Kaspersky Managed Protection Statement	(عدم الترحيل) لا يتضمن Kaspersky Endpoint Security خدمة KMP.
Action to perform on KSN untrusted objects	(عدم الترحيل) يمكنك تكوين الإجراء المطلوب اتخاذه عند اكتشاف تهديد في إعدادات مكون الحماية وإعدادات مهمة الفحص.
Do not calculate checksum before sending to KSN if file size exceeds N MB	(عدم الترحيل) يمكنك تكوين قيود فحص الملفات الكبيرة في إعدادات مكون الحماية وإعدادات مهمة الفحص.
Use Kaspersky Security Center as KSN Proxy	**استخدام وكيل شبكة KSN**
Schedule settings	(عدم الترحيل) لا يمكن تكوين جدولة منفصلة للمكون. يكون المكون قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.

Traffic Security

يتم ترحيل إعدادات أمان حركة مرور KSWS إلى القسم **الحماية من التهديدات الأساسية**، القسم الفرعي **الحماية من تهديدات الويب** و**الحماية من تهديدات البريد** القسم **ضوابط الأمان**، القسم الفرعي **التحكم في الويب** القسم **الإعدادات العامة**، القسم الفرعي **إعدادات الشبكة**.

إعدادات أمان حركة المرور

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Apply URL-based rules	**التحكم في الويب** (القسم الفرعي **التحكم في الويب**) يتم ترحيل القواعد المستندة على عنوان URL إلى قواعد منفصلة في Kaspersky Endpoint Security.
Apply certificate-based rules	(عدم الترحيل) لا يدعم Kaspersky Endpoint Security القواعد المستندة على الشهادة.
Apply rules for web traffic category control	**التحكم في الويب** (القسم الفرعي **التحكم في الويب**) يتم ترحيل قواعد الحظر الخاصة بالتحكم في فئة حركة المرور على الويب إلى قاعدة حظر واحدة في Kaspersky Endpoint Security. ويتجاهل Kaspersky Endpoint Security السماح بقواعد التحكم في الفئة. يتم سرد تطابق فئات KSWS و KES أدناه.
Allow access if the web page can not be categorized	(عدم الترحيل) يسمح Kaspersky Endpoint Security بالوصول إذا تعذر تصنيف صفحة الويب.
Allow access to legitimate web resources that can be used to damage a protected device	(عدم الترحيل) يسمح Kaspersky Endpoint Security بالوصول إلى موارد الويب القانونية التي يمكن استخدامها لإتلاف الجهاز المحمي.
Allow access to legitimate advertisement	(عدم الترحيل) يمكنك إدارة الوصول إلى الإعلانات القانونية باستخدام فئة موارد الويب الشعارات في إعدادات التحكم في الويب.
Operation mode: • Driver Interceptor • Redirector • External Proxy	(عدم الترحيل) يدعم Kaspersky Endpoint Security وضع Driver Interceptor فقط.
ICAP-service connection settings	(عدم الترحيل) لا يدعم Kaspersky Endpoint Security حماية مخزن شبكة ICAP.
Check safe connections through the HTTPS protocol	وضع **فحص الاتصالات المشفرة / فحص الاتصالات المشفرة دائمًا** (القسم الفرعي **إعدادات الشبكة**)
Use TLS protocol version	(عدم الترحيل) يفحص Kaspersky Endpoint Security حركة شبكة الاتصال المشفرة المنقولة عبر البروتوكولات التالية: • SSL 3.0. • TLS 1.0، TLS 1.1، TLS 1.2، TLS 1.3. يمكنك أيضًا منع اتصالات SSL 2.0 في إعدادات فحص الاتصالات المشفرة.
Do not trust web-servers with invalid certificate	**عند زيارة مجال له شهادة غير موثوق بها** (القسم الفرعي **إعدادات الشبكة**)
Intercept ports (Interception area)	**المنافذ قيد المراقبة** (القسم الفرعي **إعدادات الشبكة**)

	أثناء الترحيل، يمسح KES خانات الاختيار **مراقبة جميع المنافذ للتطبيقات الموجودة في القائمة التي توصي بها Kaspersky** و**مراقبة جميع منافذ التطبيقات المحددة**.
Exclude ports (Interception area)	(عدم الترحيل)
Exclude IP addresses ((Interception area	**العناوين الموثوقة** (القسم الفرعي **إعدادات الشبكة**)
Exclude processes (Interception area)	**التطبيقات الموثوقة** (القسم الفرعي **إعدادات الشبكة**) أثناء الترحيل، يكوّن KES الإعدادات التالية للتطبيق الموثوق به: • يتم تحديد خانة الاختيار **عدم فحص حركة شبكة الاتصال**. لا يفحص KES حركة شبكة الاتصال للبحث عن أي عناوين IP بعيدة وأي منافذ. • يتم مسح خانات الاختيار الأخرى في إعدادات التطبيق الموثوق به.
Security port	(عدم الترحيل)
Use malicious URL database to scan web links	**التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الخبيثة** (القسم الفرعي **الحماية من تهديدات الويب**)
Use anti-phishing database to scan web pages	**التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الاحتيالية** (القسم الفرعي **الحماية من تهديدات الويب**)
Use KSN for protection	(عدم الترحيل) يستخدم Kaspersky Endpoint Security شبكة KSN لكل مكونات التطبيق.
Use Trusted Zone	(عدم الترحيل) يطبق Kaspersky Endpoint Security المنطقة الموثوقة على كل المكونات. ويمكنك تكوين الاستثناءات في إعدادات المنطقة الموثوقة.
Use heuristic analyzer	**استخدام التحليل المساعد على الاكتشاف** (القسمان الفرعيان **الحماية من تهديدات الويب** و**الحماية من تهديدات البريد**)
Security level	(عدم الترحيل) يحتوي Kaspersky Endpoint Security على مستويات أمان خاصة به لمكوني الحماية من تهديدات الويب والحماية من تهديدات البريد. وبشكل افتراضي ، يعيّن Kaspersky Endpoint Security مستوى الأمان المستحسن.
Enable mail threat protection	**الحماية من تهديدات البريد** (القسم الفرعي **الحماية من تهديدات البريد**) **توصيل ملحق Microsoft Outlook** **الرسائل الواردة فقط** (نطاق الحماية) **الفحص عند الاستلام** (حماية البريد الإلكتروني)
Schedule settings	(عدم الترحيل) لا يمكن تكوين جدولة منفصلة للمكون. يكون المكون قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.

Exploit Prevention

يتم ترحيل إعدادات منع الاستغلال في KSWS إلى القسم **الحماية من التهديدات المتقدمة**، القسم الفرعي **منع الاستغلال**.

إعدادات منع الاستغلال

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Prevent vulnerable processes exploit: • Terminate on exploit • Notify only	**عند اكتشاف استغلال**: • **منع التشغيل** • **إخطار**.
Notify about abused processes via Terminal Service	(عدم الترحيل) لا يدعم Kaspersky Endpoint Security الخدمات الطرفية.
Prevent vulnerable processes exploit even if Kaspersky Security Service is disabled	(عدم الترحيل) يمنع Kaspersky Endpoint Security باستمرار عمليات استغلال العملية المعرضة للاختراق.
Protected processes	**تمكين حماية ذاكرة عملية النظام** لا يدعم Kaspersky Endpoint Security تحديد العمليات المحمية. ويمكنك فقط تمكين حماية ذاكرة عمليات النظام.
Exploit prevention techniques: • Apply all available exploit prevention techniques • Apply selected exploit prevention techniques	(عدم الترحيل) يطبق Kaspersky Endpoint Security كل أساليب منع الاستغلال المتاحة.

Network Threat Protection

يتم ترحيل إعدادات الحماية من تهديدات الشبكة إلى القسم **الحماية من التهديدات الأساسية**، القسم الفرعي **الحماية من تهديدات الشبكة**.

إعدادات الحماية من تهديدات الشبكة

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Operation mode: • Pass-through • Only inform about network attacks • Block connections when attack is detected	**الحماية من تهديدات الشبكة** في حالة تحديد وضع **Pass-through**، يتم تعطيل الحماية من تهديد الشبكة. في حالة تحديد وضع **Only inform about network attacks** أو **Block connections when attack is detected**، يتم تمكين الحماية من تهديدات الشبكة. يعمل Kaspersky Endpoint Security دائمًا في وضع **Block connections when attack is detected**.
Do not stop traffic analysis when the task is not running	(عدم الترحيل) يحلل Kaspersky Endpoint Security حركة المرور باستمرار في حالة تمكين المكون.
Do not control excluded IP-addresses	**الاستثناءات**
Schedule settings	(عدم الترحيل) لا يمكن تكوين جدولة منفصلة للمكون. يكون المكون قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.

Script Monitoring

لا يدعم Kaspersky Endpoint Security مكون مراقبة البرنامج النصي. ويتم التعامل مع مراقبة البرنامج النصي بواسطة مكونات أخرى، على سبيل المثال، حماية AMSI.

Website categories

لا يدعم Kaspersky Endpoint Security كل فئات Kaspersky Security for Windows Server. ولا يتم ترحيل الفئات غير الموجودة في Kaspersky Endpoint Security. لذلك، لا يتم ترحيل قواعد تصنيف مورد الويب التي تتضمن فئات غير مدعومة.

فئات مواقع الويب

فئات Kaspersky Security for Windows Server	فئات Kaspersky Endpoint Security for Windows
Wargaming	ألعاب الفيديو
Abortion	(عدم الترحيل)
(Lotteries (extended	المقامرة واليانصيب والمراهنات
Alcohol	الكحول والتبغ والمخدرات
Anonymous proxy servers	أدوات إخفاء الهوية
Anorexia	(عدم الترحيل)
Rentals for real estate	(عدم الترحيل)
Audio, video and software	البرامج والصوت والفيديو
Banks	البنوك
Blogs	المدونات
Military	الأسلحة والمتفجرات والألعاب النارية
For children	(عدم الترحيل)
Discrimination	العنف
Home and family	(عدم الترحيل)
Hosting and domain services	اتصالات الإنترنت
Pets and animals	(عدم الترحيل)
Law and politics	ممنوع بموجب القوانين الإقليمية
(Restricted by Roskomnadzor (RF	ممنوع حسب قوانين الاتحاد الروسي
(Restricted by Federal Law 436 (RF	ممنوع حسب قوانين الاتحاد الروسي
Restricted by RF legislation	ممنوع حسب قوانين الاتحاد الروسي
Restricted by global legislation	ممنوع بموجب القوانين الإقليمية
Adult dating	محتوى البالغين
Internet services	(عدم الترحيل)
Sex shops	محتوى البالغين
Information technologies	(عدم الترحيل)
Casinos, card games	المقامرة واليانصيب والمراهنات
Books and writing	(عدم الترحيل)
Computer games	ألعاب الفيديو
Health and beauty	(عدم الترحيل)
Culture and society	(عدم الترحيل)
LGBT	محتوى البالغين
Lotteries	المقامرة واليانصيب والمراهنات

Medicine	(عدم الترحيل)
Fashion	(عدم الترحيل)
Music	(عدم الترحيل)
Drugs	الكحول والتبغ والمخدرات
Violence	العنف
Discontent	(عدم الترحيل)
Illegal drugs	الكحول والتبغ والمخدرات
Hate and discrimination	العنف
Obscene vocabulary	الألفاظ النابية والفحش
Lingerie	محتوى البالغين
News	وسائل الإعلام
Nudism	محتوى البالغين
Education	(عدم الترحيل)
Online shopping	المتاجر على الإنترنت
All communication media	اتصالات الإنترنت
Payment by credit cards	أنظمة الدفع
(Online shopping (own payment system	المتاجر على الإنترنت
Online encyclopedias	(عدم الترحيل)
Online banking	البنوك
Weapons	الأسلحة والمتفجرات والألعاب النارية
Fishing and hunting	(عدم الترحيل)
Payment systems	أنظمة الدفع
Job search	البحث عن الوظائف
Search engines	(عدم الترحيل)
(Police decision (JP	ممنوع بواسطة شرطة اليابان
Trusted by KPSN	(عدم الترحيل)
Untrusted by KPSN	(عدم الترحيل)
Porn	محتوى البالغين
Media hosting and streaming	وسائل الإعلام
Web Mail	البريد الإلكتروني على الويب
Traveling	(عدم الترحيل)
TV and radio	وسائل الإعلام
Teasers and ads services	الشعارات
Religion	الأديان والجمعيات الدينية
Restaurants, cafe and food	(عدم الترحيل)
Dating sites	مواقع المواعدة

Sex education	محتوى البالغين
Social networks	الشبكات الاجتماعية
Sport	(عدم الترحيل)
Betting	المقامرة واليانصيب والمراهنات
Suicide	العنف
Tobacco	الكحول والتبغ والمخدرات
Torrents	ملفات Torrent
(Mentioned in Federal list of extremists (RF	ممنوع حسب قوانين الاتحاد الروسي
File sharing	مشاركة الملفات
Pharmacy	(عدم الترحيل)
Hobby and entertainment	(عدم الترحيل)
Chats and forums	الدردشة والمنتديات والمراسلة الفورية
Schools and universities pages	(عدم الترحيل)
Astrology and esoterica	(عدم الترحيل)
Extremism and racism	العنف
E-commerce	المتاجر على الإنترنت
Erotic	محتوى البالغين
Humor	(عدم الترحيل)

Local activity control

Applications Launch Control

يتم ترحيل إعدادات التحكم في التطبيقات في KSWS إلى القسم **ضوابط الأمان**، القسم الفرعي **التحكم في التطبيقات**.

إعدادات التحكم في التطبيقات

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Operation mode: • Statistics only • Active	**الإجراء** (التحكم في التطبيقات): • **اختبار القواعد** • **تطبيق القواعد**.
Repeat action taken for the first file launch on all the subsequent launches for this file	(عدم الترحيل) يفحص Kaspersky Endpoint Security التطبيق في كل مرة يحاول فيها العمل.
Deny the command interpreters launch with no command to execute	(عدم الترحيل) يسمح Kaspersky Endpoint Security بتشغيل مفسرات الأوامر إذا لم تكن محظورة بواسطة التحكم في التطبيقات.
Rules	**قواعد التحكم في التطبيق** (مدعوم مع قيود) يقدم Kaspersky Endpoint Security 11.11.0 دعمًا لترحيل قواعد التحكم في تشغيل التطبيقات. توجد بعض القيود في وظيفة ترحيل قاعدة التحكم في تشغيل التطبيقات. وبشكل افتراضي، يتضمن التحكم في تشغيل تطبيقات KSWS قاعدتين: • **Allow scripts and MSI by OS-trusted certificate** • **Allow executable by OS-trusted certificate** إذا كان هناك مصدر واحد على الأقل لقاعدة KSWS يتضمن نوع **Allow**، أثناء الترحيل، ينشئ KES قاعدة سماح جديدة، **التطبيقات ذات شهادات الجذر الموثوق بها**. أي أن التحكم في تطبيق KES يستخدم قاعدة واحدة للسماح بتشغيل البرامج النصية الموثوقة وحزم MSI والملفات التنفيذية. وإذا كان لكل من قواعد KSWS المصدر نوع **Deny**، لا يضيف KES قواعد لإدارة التطبيقات ذات شهادات الجذر الموثوقة.
Apply rules to executable files	(عدم الترحيل) لا يمكن تكوين نطاق تطبيق القاعدة في إعدادات التحكم في التطبيقات في KES. ويطبق التحكم في التطبيقات في KES القواعد على جميع أنواع الملفات: الملفات القابلة للتنفيذ والبرامج النصية وحزم MSI. وفي حالة تضمين جميع أنواع الملفات في نطاق تطبيق القاعدة في KSWS، أثناء الترحيل ينقل KES قواعد KSWS. وفي حالة استثناء بعض أنواع الملفات من نطاق تطبيق القاعدة في KSWS، أثناء الترحيل، ينقل KES أيضًا قواعد KSWS، لكن يتم تحديد **اختبار القواعد** كإجراء التحكم في التطبيقات.
Monitor loading of DLL modules	**التحكم في تحميل وحدات DLL (يؤدي إلى زيادة كبيرة في الحمل على النظام)**
Apply rules to scripts and MSI packages	(عدم الترحيل) لا يمكن تكوين نطاق تطبيق القاعدة في إعدادات التحكم في التطبيقات في KES. ويطبق التحكم في التطبيقات في KES القواعد على جميع أنواع الملفات: الملفات القابلة للتنفيذ والبرامج النصية وحزم MSI. وفي حالة تضمين جميع أنواع الملفات في نطاق تطبيق القاعدة في KSWS، أثناء الترحيل ينقل KES قواعد KSWS. وفي حالة استثناء بعض أنواع الملفات من نطاق تطبيق القاعدة في KSWS، أثناء الترحيل، ينقل KES ا قواعد KSWS، لكن يتم تحديد **اختبار القواعد** كإجراء التحكم في التطبيقات.
Deny applications untrusted by KSN	(عدم الترحيل) لا يضع Kaspersky Endpoint Security في الاعتبار سمعة التطبيقات ويسمح بتشغيل التطبيقات وفقًا للقواعد أو يرفضها.

Allow applications trusted by KSN	أثناء الترحيل، يضيف KES قاعدة سماح جديدة. ويتم تحديد فئة KL **Other Software** ← **Applications** **trusted according to reputation in KSN** كشرط لبدء تشغيل القاعدة.
Users and / or user groups allowed to run applications trusted by KSN	يسمح خيار **التابعون وحقوقهم** في قاعدة التحكم في التطبيقات فئة KL **تطبيقات أخرى** ← **التطبيقات الموثوقة وفقًا للسمعة في شبكة KSN**
Automatically allow software distribution via applications and packages listed	يعمل التحكم في توزيع البرامج في KSWS وKES بشكل مختلف. وأثناء الترحيل، يضيف KES قواعد السماح الجديدة للتطبيقات التي يُسمح عليها بالتوزيع التلقائي للبرامج. ويتم تحديد تجزئة الملف كشرط لبدء تشغيل القاعدة.
Always allow software distribution via Windows Installer	**استخدام مخزن شهادات النظام الموثوق** (القسم الفرعي **الاستثناءات**) يتضمن الإعداد **مخزن شهادات النظام الموثوق** القيمة **سلطات شهادات الجذر الموثوق بها**.
Always allow software distribution via SCCM using the Background Intelligent Transfer Service	(عدم الترحيل)
Software distribution applications and packages allowed	يعمل التحكم في توزيع البرامج في KSWS وKES بشكل مختلف. وأثناء الترحيل، يضيف KES قواعد السماح الجديدة للتطبيقات التي يُسمح عليها بالتوزيع التلقائي للبرامج. ويتم تحديد تجزئة الملف كشرط لبدء تشغيل القاعدة.
Schedule settings	(عدم الترحيل) في حالة تكوين جدول زمني للمكون في إعدادات KSWS، يتم تمكين مكون التحكم في التطبيقات عند الترحيل. وإذا لم يتم تكوين جدول زمني للمكون في إعدادات KSWS، يتم تعطيل التحكم في التطبيقات عند الترحيل. لا يمكن تكوين جدولة منفصلة للمكون. يكون المكون قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.

Device Control

يتم ترحيل إعدادات التحكم في الجهاز في KSWS إلى القسم **ضوابط الأمان**، القسم الفرعي **التحكم في الجهاز**.

إعدادات التحكم في الجهاز

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Operation mode: • **Active** • **Statistics only**	(عدم الترحيل) يعمل التحكم في التطبيقات في الوضع Active. ويتم توفير إحصائيات اتصال الجهاز بشكل مستمر بواسطة التدقيق.
Allow using all external devices when the Device Control task is not running	(عدم الترحيل) يكون التحكم في الجهاز قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.
Device Control rules	**الأجهزة الموثوقة** أثناء الترحيل، يتجاهل Kaspersky Endpoint Security قواعد KSWS المعطلة.
Schedule settings	(عدم الترحيل) يستخدم Kaspersky Endpoint Security جدوله الخاص للوصول إلى أنواع معينة من الأجهزة.

Network-Attached Storages Protection

RPC Network Storage Protection

لا يدعم Kaspersky Endpoint Security مكونات حماية المخازن الموصلة بالشبكة. وإذا كنت بحاجة إلى هذه المكونات، يمكنك الاستمرار في استخدام Kaspersky Security for Windows Server.

ICAP Network Storage Protection

لا يدعم Kaspersky Endpoint Security مكونات حماية المخازن الموصلة بالشبكة. وإذا كنت بحاجة إلى هذه المكونات، يمكنك الاستمرار في استخدام Kaspersky Security for Windows Server.

Anti-Cryptor for NetApp

لا يدعم Kaspersky Endpoint Security وظيفة Anti-Cryptor for NetApp. يتم توفير وظيفة Anti-Cryptor بواسطة مكونات التطبيق الأخرى، مثل اكتشاف السلوك.

Network activity control

Firewall Management

لا يدعم Kaspersky Endpoint Security إدارة جدار حماية KSWS. يتم تنفيذ وظائف جدار حماية KSWS بواسطة جدار الحماية على مستوى النظام. بعد الترحيل، يمكنك تكوين جدار حماية Kaspersky Endpoint Security.

Anti-Cryptor

يتم ترحيل إعدادات Network Anti-Cryptor إلى القسم **الحماية من التهديدات المتقدمة**، القسم الفرعي **اكتشاف السلوك**.

إعدادات Anti-Cryptor

إعدادات KSWS	إعدادات KES
Operation mode: • **Statistics only** • **Active**	**عند اكتشاف تشفير خارجي للمجلدات التي تتم مشاركتها**: • **إخطار** • **منع الاتصال**.
Heuristic analyzer	(عدم الترحيل) لا يستخدم Kaspersky Endpoint Security التحليل المساعد على الاكتشاف لاكتشاف السلوك.
Configuration of protection scope: • **All shared network folders on the protected device** • **Only specified shared folders**	(عدم الترحيل) يمنع Kaspersky Endpoint Security تشفير كل مجلدات الشبكة المشتركة على الكمبيوتر المحمي.
Exclusions	(عدم الترحيل) يتضمن Kaspersky Endpoint Security استثناءاته الخاصة لمكون اكتشاف السلوك. ويمكنك إضافة استثناءات يدويًا بعد الترحيل.
Schedule settings	(عدم الترحيل) لا يمكن تكوين جدولة منفصلة للمكون. يكون المكون قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.

System Inspection

File Integrity Monitor

يتم ترحيل إعدادات File Integrity Monitor من KSWS إلى القسم **ضوابط الأمان**، القسم الفرعي **مراقبة سلامة الملف**.

إعدادات مراقبة سلامة الملف

إعدادات KSWS	إعدادات KES
Log information about file operations that appear during the monitor interruption period	(عدم الترحيل) لا يسجل Kaspersky Endpoint Security الأحداث الخاصة بعمليات الملفات التي يتم تنفيذها أثناء فترة انقطاع المراقبة.
Block attempts to compromise the USN log	(عدم الترحيل) لا يمنع Kaspersky Endpoint Security محاولات اختراق سجل USN.
Monitoring scope	**نطاق المراقبة** (مدعوم مع قيود) لا يتم ترحيل سجلات نطاق المراقبة المعطلة إلى KES. ويضيف Kaspersky Endpoint Security السجلات التي تم تمكينها فقط إلى نطاق المراقبة.
Trusted users	(عدم الترحيل) يعتبر Kaspersky Endpoint Security جميع إجراءات المستخدمين في نطاق المراقبة خرقًا أمنيًا.
File operation markers	(عدم الترحيل) يأخذ Kaspersky Endpoint Security في الاعتبار جميع علامات تشغيل الملفات المتوفرة.
Calculate checksum for the file if possible	(عدم الترحيل) لا يحسب Kaspersky Endpoint Security المجموع الاختباري للملف المعدل.
Exclusions	**الاستثناءات**

Log Inspection

يتم ترحيل إعدادات فحص السجل في KSWS إلى القسم **ضوابط الأمان**، القسم الفرعي **فحص السجل**.

إعدادات فحص السجل

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Apply custom rules for log inspection	(عدم الترحيل) يطبق Kaspersky Endpoint Security جميع القواعد المخصصة التي تم تمكينها.
Custom rules	**قواعد مخصصة** لا يتم ترحيل القاعدة المحددة مسبقًا **A service was installed in the system (for Server 2003 OS)** إلى KES.
Apply predefined rules for log inspection	(عدم الترحيل) يطبق Kaspersky Endpoint Security جميع القواعد المحددة مسبقًا التي تم تمكينها.
Predefined rules	**القواعد المحددة مسبقًا**
Password brute-force detection	**اكتشاف هجوم فك الشفرة**
Network logon detection	**اكتشاف تسجيل الدخول إلى الشبكة**
Exclusions (IP addresses)	**الاستثناءات** (عنوان IP)
Exclusions (users)	**الاستثناءات** (المستخدمون)
Schedule settings	(عدم الترحيل) لا يمكن تكوين جدولة منفصلة للمكون. يكون المكون قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.

Logs and notifications

Task logs

يتم ترحيل إعدادات سجل KSWS إلى القسم **الإعدادات العامة**، **الواجهة** والقسم الفرعي **التقارير والمخزن**.

إعدادات السجلات

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Event logging	**الإخطارات** (القسم الفرعي **الواجهة**)
Logs folder	(عدم الترحيل) يحفظ Kaspersky Endpoint Security التقارير في المجلد `C:\ProgramData\Kaspersky Lab\KES.21.13\Report`.
Remove task logs older than (N day(s	(عدم الترحيل) يمكنك تكوين فترة التخزين لتقارير KES تحت **الإعدادات العامة** و**التقارير والمخزن**.
Remove from the audit log (events N day(s	(عدم الترحيل) يطبق Kaspersky Endpoint Security قيود تخزين التقارير على كل التقارير بما في ذلك تقارير تدقيق النظام.
Integration with SIEM	(عدم الترحيل) يمكنك تكوين تكامل SIEM في Kaspersky Security Center.

Event notifications

يتم ترحيل إعدادات الإخطارات في KSWS إلى القسم **الإعدادات العامة**، القسم الفرعي **الواجهة**.

إعدادات الإخطار

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Notifications	**الإخطارات**
Notify users: • By using terminal service • By using Windows Messenger Service command	(عدم الترحيل) لا يدعم Kaspersky Endpoint Security تعديل نص الإخطار. ويعرض Kaspersky Endpoint Security الإخطارات القياسية.
Notify administrators: • By using Windows Messenger Service command • By running executable file • By sending email	يتم ترحيل إعدادات إخطارات البريد الإلكتروني فقط إلى Kaspersky Endpoint Security – **إعدادات إخطارات البريد الإلكتروني** (قسم **الإخطارات**). لا يتم دعم الطرق الأخرى لإخطار المسؤولين.
Application database is out of date	**إرسال إخطار "قواعد بيانات قديمة" إذا لم يتم تحديث قواعد البيانات**
Application database is extremely out of date	**إرسال إخطار "قواعد بيانات قديمة جدًا" إذا لم يتم تحديث قواعد البيانات**
Critical areas scan has not been performed for a long time	(عدم الترحيل) يُنشئ Kaspersky Endpoint Security حدث فحص المناطق الحرجة المفقود بعد ثلاثة أيام.

Interaction with Administration Server

يتم ترحيل إعدادات تفاعل خادم الإدارة في KSWS إلى القسم **الإعدادات العامة**، القسم الفرعي **التقارير والمخزن**.

إعدادات تفاعل خادم الإدارة

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Quarantined files	**حول ملفات العزل**
Backed up files	**حول الملفات في النسخ الاحتياطي**
Blocked hosts	(عدم الترحيل) يرسل Kaspersky Endpoint Security تلقائيًا بيانات حول المضيفين الممنوعين.

Activation of the application

لا يدعم Kaspersky Endpoint Security مهمة Application activation (KSWS). يمكنك إنشاء مهمة إضافة مفتاح (KES)، وإضافة مفتاح ترخيص إلى حزمة التثبيتأو تمكين التوزيع التلقائي لمفتاح الترخيص.

Copying Updates

يتم ترحيل إعدادات مهمة Copying Updates (KSWS) إلى مهمة تحديث (KES).

نسخ إعدادات مهمة التحديثات

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Update source: • Kaspersky Security Center Administration Server • Kaspersky update servers • Custom HTTP or FTP servers, or network folders	مصدر التحديث: • Kaspersky Security Center • خوادم التحديث من Kaspersky • محدد من قبل المستخدم.
Use Kaspersky update servers if specified servers are not available	(عدم الترحيل) يسمح Kaspersky Endpoint Security بتحديد مصادر تحديث متعددة، بما في ذلك خوادم التحديث من Kaspersky. وإذا لم يكن مصدر التحديث الأول متاحًا، يتيح لك Kaspersky Endpoint Security الحصول على التحديثات من مصدر آخر في القائمة.
Use proxy server settings to connect to Kaspersky update servers	(عدم الترحيل) يستخدم Kaspersky Endpoint Security الخادم الوكيل لجميع المكونات. ويمكنك تكوين اتصال الخادم الوكيل في خيارات الشبكة للتطبيق.
Use proxy server settings to connect to other servers	(عدم الترحيل) يستخدم Kaspersky Endpoint Security الخادم الوكيل لجميع المكونات. ويمكنك تكوين اتصال الخادم الوكيل في خيارات الشبكة للتطبيق.
Copying updates settings: • Copy database updates • Copy critical software modules updates • Copy database updates and critical updates of application modules	(عدم الترحيل) ينسخ Kaspersky Endpoint Security تحديثات قاعدة البيانات والتحديثات الهامة للوحدات النمطية للتطبيق كحزمة واحدة.
Folder for local storage of copied updates	نسخ التحديثات إلى مجلد

Baseline File Integrity Monitor

لا يدعم Kaspersky Endpoint Security مهمة Baseline File Integrity Monitor. ويتم توفير وظيفة مراقبة سلامة الملفات بواسطة مكونات التطبيق الأخرى، مثل اكتشاف السلوك.

Database Update

يتم ترحيل إعدادات مهمة Database Update (KSWS) إلى مهمة تحديث (KES).

إعدادات مهمة تحديث قاعدة البيانات

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Update source: • Kaspersky Security Center Administration Server • Kaspersky update servers • Custom HTTP or FTP servers, or network folders	مصدر التحديث: • Kaspersky Security Center • خوادم التحديث من Kaspersky • محدد من قبل المستخدم.
Use Kaspersky update servers if specified servers are not available	(عدم الترحيل) يسمح Kaspersky Endpoint Security بتحديد مصادر تحديث متعددة، بما في ذلك خوادم التحديث من Kaspersky. وإذا لم يكن مصدر التحديث الأول متاحًا، يتيح لك Kaspersky Endpoint Security الحصول على التحديثات من مصدر آخر في القائمة.
Use proxy server settings to connect to Kaspersky update servers	(عدم الترحيل) يستخدم Kaspersky Endpoint Security الخادم الوكيل لجميع المكونات. ويمكنك تكوين اتصال الخادم الوكيل في خيارات الشبكة للتطبيق.
Use proxy server settings to connect to other servers	(عدم الترحيل) يستخدم Kaspersky Endpoint Security الخادم الوكيل لجميع المكونات. ويمكنك تكوين اتصال الخادم الوكيل في خيارات الشبكة للتطبيق.
Lower the load on the disk I/O	(عدم الترحيل)

Software modules updates

يتم ترحيل إعدادات مهمة Software Modules Update (KSWS) إلى مهمة تحديث (KES).

إعدادات مهمة تحديث الوحدات النمطية للبرامج

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Update source: • Kaspersky Security Center Administration Server • Kaspersky update servers • Custom HTTP or FTP servers, or network folders	**مصدر التحديث**: • **Kaspersky Security Center** • **خوادم التحديث من Kaspersky** • **محدد من قبل المستخدم**.
Use Kaspersky update servers if specified servers are not available	(عدم الترحيل) يسمح Kaspersky Endpoint Security بتحديد مصادر تحديث متعددة، بما في ذلك خوادم التحديث من Kaspersky. وإذا لم يكن مصدر التحديث الأول متاحًا، يتيح لك Kaspersky Endpoint Security الحصول على التحديثات من مصدر آخر في القائمة.
Use proxy server settings to connect to Kaspersky update servers	(عدم الترحيل) يستخدم Kaspersky Endpoint Security الخادم الوكيل لجميع المكونات. ويمكنك تكوين اتصال الخادم الوكيل في خيارات الشبكة للتطبيق.
Use proxy server settings to connect to other servers	(عدم الترحيل) يستخدم Kaspersky Endpoint Security الخادم الوكيل لجميع المكونات. ويمكنك تكوين اتصال الخادم الوكيل في خيارات الشبكة للتطبيق.
Copy and install critical software modules updates	**"تثبيت التحديثات المهمة والمصدق عليها**
Only check for critical software updates available	(عدم الترحيل) يتحقق Kaspersky Endpoint Security باستمرار من توفر التحديثات الهامة للوحدات النمطية للتطبيق.
Allow operating system restart	(عدم الترحيل) يطالب Kaspersky Endpoint Security المستخدم بالحصول على إذن لإعادة تشغيل الكمبيوتر.
Receive information about available scheduled software modules updates	(عدم الترحيل) يعرض Kaspersky Endpoint Security إخطارات حول تحديثات الوحدة النمطية للبرامج.

Rollback of Application Database Update

يتم ترحيل إعدادات مهمة Rollback of Application Database Update (KSWS) إلى مهمة تراجع عن التحديث (KES). وتتضمن مهمة تراجع عن التحديث (KES) الجديدة الجدولة Manually لبدء مهمتها.

On-Demand Scan

يتم ترحيل إعدادات مهمة On-Demand Scan (KSWS) إلى مهمة فحص البرامج الضارة (KES).

إعدادات مهمة فحص الفيروسات

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Scan scope	نطاق الفحص
Protection level: • Maximum protection • Recommended • Maximum performance	مستوى الأمان: • مرتفع • مستحسن • منخفض. تختلف إعدادات مستوى الأمان في KSWS وKES.
Objects to scan: • All objects • Objects scanned by format • Objects scanned according to list of extensions specified in anti-virus database • Objects scanned by specified list of extensions	أنواع الملفات: • كل الملفات • الملفات التي تم فحصها حسب التنسيق • الملفات التي تم فحصها حسب الامتداد. لا يسمح Kaspersky Endpoint Security بإنشاء قوائم امتدادات مخصصة. ويستبدل Kaspersky Endpoint Security قيمة **Objects scanned by specified list of extensions** لتحل محلها قيمة **الملفات التي تم فحصها حسب الامتداد**.
Subfolders	تضمين المجلدات الفرعية
Subfiles	(عدم الترحيل)
Scan disk boot sectors and MBR	(عدم الترحيل)
Scan alternate NTFS streams	(عدم الترحيل)
Scan only new and modified files	فحص الملفات الجديدة والتي تم تغييرها فقط
Scan of compound objects: • All archives • All SFX archives • All email databases • All packed objects • All plain email • All embedded OLE objects	فحص الملفات المركبة: • فحص الأرشيفات • فحص الأرشيفات المحمية بكلمة مرور • فحص حزم التوزيع • فحص تنسيقات البريد الإلكتروني • فحص الملفات بتنسيقات Microsoft Office.
Action to perform on infected and other objects: • Disinfect • Remove if disinfection .Disinfect fails • Remove	الإجراء المطلوب اتخاذه عند اكتشاف تهديد: • تنظيف؛ حذف إذا فشل التنظيف • تنظيف؛ إبلاغ إذا فشل التنظيف • إخطار.

• Perform recommended action • Notify only	
Action to perform on probably infected objects: • Quarantine • Remove • Perform recommended action • Notify only	(عدم الترحيل) يطبق Kaspersky Endpoint Security الإجراء في حالة اكتشاف أي تهديد.
Perform actions depending on the type of object detected	(عدم الترحيل)
Entirely remove compound file that cannot be modified by the application in case of embedded object detection	(عدم الترحيل)
Exclude files	(عدم الترحيل) يطبق Kaspersky Endpoint Security المنطقة الموثوقة على كل المكونات. ويمكنك تكوين الاستثناءات في إعدادات المنطقة الموثوقة.
Do not detect	(عدم الترحيل)
Stop scanning if it takes longer than N sec	**تخطي الملفات التي تم فحصها لأكثر من N ثانية**
Do not scan compound objects larger than N MB	**عدم فك ضغط الملفات المركبة كبيرة الحجم**
Use iSwift technology	**تقنية iSwift**
Use iChecker technology	**تقنية iChecker**
Action on the offline files: • Do not scan • Scan resident part of file only • Scan entire file • Only if the file has been accessed within the specified (period (days • Do not copy file to a local hard drive, if possible	(عدم الترحيل) يفحص Kaspersky Endpoint Security الملفات غير المتصلة بالإنترنت بالكامل.

Application Integrity Control

يتم ترحيل إعدادات مهمة Application Integrity Control (KSWS) إلى مهمة التحقق من السلامة (KES).

Rule Generator for Applications Launch Control

لا يدعم Kaspersky Endpoint Security مهمة Applications Launch Control Generator. ويمكنك إنشاء القواعد في إعدادات التحكم في التطبيقات.

Rule Generator for Device Control

لا يدعم Kaspersky Endpoint Security مهمة Rule Generator for Device Control. ويمكنك إنشاء قواعد الوصول في إعدادات التحكم في الجهاز.

ترحيل مكونات KSWS

قبل التثبيت المحلي، يتحقق تطبيق Kaspersky Endpoint Security من جهاز الكمبيوتر بحثًا عن وجود تطبيقات Kaspersky. وفي حالة تثبيت Kaspersky Security for Windows Server على جهاز الكمبيوتر، يكتشف KES مجموعة مكونات KSWS المثبتة ويحدد المكونات نفسها لتثبيتها.

ويتم تثبيت مكونات KES التي لا يتضمنها KSWS على النحو التالي:

- يتم تثبيت حماية AMSI، ومنع اختراق المضيف، ومحرك المعالجة بالإعدادات الافتراضية.
- يتم تجاهل مكونات منع هجمات BadUSB ومراقبة عيوب التكيف وتشفير البيانات وDetection and Response.

عند التثبيت عن بعد، يتجاهل تطبيق KES مجموعة مكونات KSWS المثبتة. ويقوم المثبت بتثبيت المكونات التي تحددها في خصائص حزمة التثبيت. بعد تثبيت Kaspersky Endpoint Security وترحيل السياسات والمهام، يتم تكوين إعدادات KES وفقًا لإعدادات KSWS.

ترحيل مهام وسياسات KSWS

ويمكنك ترحيل سياسة وإعدادات مهام KSWS بالطرق التالية:

- استخدام معالج تحويل تصحيح المهام والسياسات (المشار إليه فيما يلي أيضًا باسم "معالج الترحيل").

يتوفر معالج الترحيل لتطبيق KSWS فقط في وحدة تحكم الإدارة (MMC). ولا يمكن ترحيل إعدادات السياسة والمهام في Web Console وCloud Console.

يعمل معالج تحويل الدُفعة بشكل مختلف مع إصدارات مختلفة من Kaspersky Security Center. ونوصي بترقية الحل إلى الإصدار 14.2 أو أحدث. وفي هذا الإصدار من Kaspersky Security Center، يتيح لك معالج تحويل مجموعة السياسات والمهام ترحيل السياسات إلى ملف تعريف بدلاً من سياسة. وفي هذا الإصدار من Kaspersky Security Center، يتيح لك معالج تحويل مجموعة السياسات والمهام أيضًا ترحيل نطاق أوسع من إعدادات السياسة.

- استخدام معالج السياسة الجديد لتطبيق Kaspersky Endpoint Security for Windows.

  يتيح لك معالج السياسة الجديدة إنشاء سياسة KES بناءً على سياسة KSWS.

تختلف إجراءات ترحيل سياسة KSWS عند استخدام معالج الترحيل ومعالج الأسلوب الجديد.

معالج تحويل مجموعة السياسات والمهام

ينقل معالج الترحيل إعدادات سياسة KSWS إلى ملف تعريف السياسة بدلاً من إعدادات سياسة KES. ملف تعريف السياسة عبارة عن مجموعة من إعدادات السياسة التي يتم تفعيلها على جهاز كمبيوتر إذا كان الكمبيوتر يلبي قواعد التفعيل التي تم تكوينها. ويتم تحديد علامة الجهاز `UpgradedFromKSWS` كمعيار التشغيل لملف تعريف السياسة. ويضيف Kaspersky Security Center تلقائيًا العلامة `UpgradedFromKSWS` إلى جميع أجهزة الكمبيوتر التي قمت بتثبيت KES عليها فوق KSWS باستخدام مهمة التثبيت عن بُعد. وإذا اخترت طريقة تثبيت مختلفة، يمكنك تعيين العلامة للأجهزة يدويًا.

لإضافة علامة إلى جهاز:

1. أنشئ علامة جديدة للخوادم - `UpgradedFromKSWS`.

   وللمزيد من التفاصيل عن إنشاء العلامات للأجهزة، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

2. أنشئ مجموعة إدارة جديدة في وحدة تحكم Kaspersky Security Center وأضف الخوادم التي تريد تعيين العلامة إلى هذه المجموعة لها.

   يمكنك تجميع الخوادم باستخدام أداة التحديد. وللمزيد من التفاصيل عن العمل مع التحديدات، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

3. حدد جميع خوادم مجموعة الإدارة في وحدة تحكم Kaspersky Security Center، وافتح خصائص الخوادم المحددة وقم بتعيين العلامة.

إذا كنت تقوم بترحيل سياسات KSWS متعددة، يتم تحويل كل سياسة إلى ملف تعريف ضمن سياسة شاملة واحدة. وإذا كانت سياسة KSWS تحتوي بالفعل على ملفات تعريف، سيتم أيضًا ترحيل ملفات التعريف هذه كملفات تعريف. ونتيجة لذلك، ستحصل على سياسة واحدة تتضمن ملفات تعريف تتوافق مع جميع سياسات KSWS.

كيفية استخدام معالج تحويل تصحيح المهام والسياسات لترحيل إعدادات سياسة KSWS

1. في وحدة تحكم الإدارة ، حدد خادم الإدارة وانقر بزر الماوس الأيمن لفتح قائمة السياق.

2. حدد **كل المهام** ← **معالج تحويل تصحيح المهام والسياسات**.

سيبدأ معالج تحويل تصحيح المهام والسياسات. اتبع تعليمات المعالج.

الخطوة 1. حدد التطبيق الذي ترغب في تحويل السياسات والمهام الخاصة به

في هذه الخطوة، تحتاج إلى تحديد Kaspersky Endpoint Security for Windows. انتقل إلى الخطوة التالية.

الخطوة 2. تحويل السياسات

ينشئ معالج الترحيل ملفات تعريف سياسة KSWS داخل سياسة KES. حدد سياسات Kaspersky Security for Windows Server التي تريد تحويلها إلى ملفات تعريف السياسة. انتقل إلى الخطوة التالية.

سيبدأ معالج الترحيل بعد ذلك في تحويل السياسات. وستتوافق أسماء ملفات تعريف السياسة الجديدة مع سياسات KSWS الأصلية.

الخطوة 3. تقرير ترحيل السياسة

ينشئ معالج الترحيل تقريرًا لترحيل السياسة. ويحتوي تقرير ترحيل السياسة على تاريخ ووقت تحويل السياسات، واسم سياسة KSWS الأصلية، واسم سياسة KES المستهدفة، واسم ملف تعريف السياسة الجديد.

الخطوة 4. تحويل المهام

ينشئ معالج الترحيل مهام جديدة لبرنامج Kaspersky Endpoint Security for Windows. في قائمة المهام، حدد مهام KSWS التي تريد إنشاءها لتطبيق Kaspersky Endpoint Security. وسيتم تسمية المهام الجديدة (converted) <KSWS task name>. انتقل إلى الخطوة التالية.

الخطوة 5. اكتمال المعالج

أغلق المعالج. نتيجة لذلك، ينفذ المعالج ما يلي:

- تتم إضافة ملفات تعريف السياسة الجديدة إلى سياسة Kaspersky Endpoint Security.

  تتضمن السياسة ملفات تعريف تحتوي على إعدادات Kaspersky Security for Windows Server. وتكون حالة السياسة الجديدة فعال. ويترك المعالج سياسات KSWS دون تغيير.

- ينشئ مهام Kaspersky Endpoint Security جديدة.

  تكون المهام الجديدة عبارة عن نسخ من مهام KSWS. ويترك المعالج مهام KSWS دون تغيير.

سيتم تسمية ملف تعريف السياسة الجديد الذي يتضمن إعدادات KSWS UpgradedFromKSWS <اسم سياسة Kaspersky Security for Windows Server>. وفي خصائص ملف التعريف، يحدد معالج الترحيل تلقائيًا علامة الجهاز `UpgradedFromKSWS` كمعيار تشغيل. وبالتالي يتم تطبيق الإعدادات من ملف تعريف السياسة على الخوادم تلقائيًا.

معالج لإنشاء سياسة تستند إلى سياسة KSWS

عند إنشاء سياسة KES بناءً على سياسة KSWS، ينقل المعالج الإعدادات إلى السياسة الجديدة وفقًا لذلك. أي أن سياسة KES واحدة تتوافق مع سياسة KSWS واحدة. ولا يقوم المعالج بتحويل السياسة إلى ملف تعريف.

كيفية استخدام معالج السياسة الجديدة لترحيل إعدادات سياسة KSWS

1. افتح Kaspersky Security Center Administration Console.
2. في مجلد **الأجهزة المدارة** الخاص بشجرة وحدة تحكم الإدارة، حدد المجلد الذي يحتوي على اسم مجموعة الإدارة التي تنتمي إليها أجهزة الكمبيوتر العميلة ذات الصلة.
3. في مساحة العمل، حدد علامة التبويب **سياسات**.
4. انقر فوق الزر **سياسة جديدة**.

   بدء تشغيل معالج السياسة.
5. اتبع تعليمات "معالج السياسات".
6. لإنشاء سياسة، حدد Kaspersky Endpoint Security. انتقل إلى الخطوة التالية.
7. في خطوة إدخال اسم جديد لسياسة المجموعة، حدد خانة الاختيار **استخدام إعدادات السياسة لإصدار سابق للتطبيق**.
8. انقر فوق **استعراض** وحدد سياسة KSWS. انتقل إلى الخطوة التالية.
9. اتبع تعليمات معالج السياسة الجديدة حتى يكتمل.

عند الانتهاء، سينشئ المعالج سياسة جديدة لتطبيق Kaspersky Endpoint Security for Windows تتضمن الإعدادات من سياسة KSWS.

التكوين الإضافي للسياسات والمهام بعد الترحيل

يحتوي KSWS وKES على مجموعات مختلفة من المكونات وإعدادات السياسة، لذا بعد الترحيل، يجب عليك التحقق من أن إعدادات السياسة تفي بمتطلبات الأمان الخاصة بشركتك.

تحقق من إعدادات السياسة الأساسية التالية:

- الحماية بكلمة مرور. لم يتم ترحيل إعدادات حماية كلمة مرور KSWS. ويحتوي Kaspersky Endpoint Security على ميزة حماية كلمة المرور المضمنة. واذا لزم الأمر، قم بتشغيل الحماية بكلمة مرور وتعيين كلمة مرور.
- المنطقة الموثوقة. تختلف الطرق المستخدمة بواسطة KSWS وKES لتحديد الكائنات. وعند الترحيل، يدعم KES الاستثناءات المحددة كملفات فردية أو مسارات إلى ملف / مجلد. وإذا كان KSWS يحتوي على استثناءات تم تكوينها كمنطقة محددة مسبقًا أو عنوان URL لبرنامج نصي، فلن يتم ترحيل هذه الاستثناءات. وبعد الترحيل، يجب إضافة هذه الاستثناءات يدويًا.

للتأكد من عمل Kaspersky Endpoint Security بشكل صحيح على الخوادم، يوصى بإضافة الملفات المهمة لعمل الخادم إلى المنطقة الموثوقة. وبالنسبة لخوادم SQL، يجب إضافة ملفات قاعدة بيانات MDF وLDF. وبالنسبة لخوادم Microsoft Exchange، يجب إضافة ملفات CHK وEDB وJRS وLOG وJSL. ويمكنك استخدام الأقنعة، على سبيل المثال، `C:\Program Files (x86)\Microsoft SQL Server\*.mdf`.

- جدار الحماية. يتم تنفيذ وظائف جدار حماية KSWS بواسطة جدار الحماية على مستوى النظام. وفي KES يكون مكون منفصل مسؤولاً عن وظيفة جدار الحماية. وبعد الترحيل، يمكنك تكوين جدار حماية Kaspersky Endpoint Security.
- Kaspersky Security Network. لا يدعم Kaspersky Endpoint Security تكوين KSN للمكونات الفردية. يستخدم Kaspersky Endpoint Security شبكة KSN لكل مكونات التطبيق. ولاستخدام KSN، يجب عليك قبول الشروط والأحكام الجديدة لبيان Kaspersky Security

.Network

- التحكم في الويب. يتم ترحيل قواعد الحظر الخاصة بالتحكم في فئة حركة المرور على الويب إلى قاعدة حظر واحدة في Kaspersky Endpoint Security. ويتجاهل Kaspersky Endpoint Security السماح بقواعد التحكم في الفئة. لا يدعم Kaspersky Endpoint Security كل فئات Kaspersky Security for Windows Server. ولا يتم ترحيل الفئات غير الموجودة في Kaspersky Endpoint Security. لذلك، لا يتم ترحيل قواعد تصنيف مورد الويب التي تتضمن فئات غير مدعومة. وإذا لزم الأمر، أضف قواعد التحكم في الويب.

- الخادم الوكيل. لا يتم ترحيل كلمة مرور الاتصال بالخادم الوكيل. أدخل كلمة المرور المراد استخدامها للاتصال بالخادم الوكيل يدويًا.

- جداول المكونات الفردية. لا يدعم Kaspersky Endpoint Security تكوين الجداول للمكونات الفردية. ويكون المكون قيد التشغيل دائمًا أثناء تشغيل Kaspersky Endpoint Security.

- مجموعة المكونات. تعتمد مجموعة المزايا المتاحة بتطبيقKaspersky Endpoint Security على نوع نظام التشغيل: محطة عمل أو خادم. على سبيل المثال، من أدوات التشفير، يتوفر فقط تشفير محرك BitLocker على الخوادم.

- سمة . لا يتم ترحيل حالة سمة . وسوف تتضمن سمة الإعدادات الافتراضية. وبشكل افتراضي، تتضمن جميع الإعدادات في السياسة الجديدة تقريبًا حظرًا مطبقًا على تعديل الإعدادات في السياسات الفرعية وفي واجهة التطبيق المحلية. وتتضمن السمة قيمة لإعدادات السياسة في القسم **Managed Detection and Response** وفي مجموعة الإعدادات **دعم المستخدم** (القسم **الواجهة**). وإذا لزم الأمر، قم بتكوين توريث الإعدادات من السياسة الأصلية.

- التعامل مع التهديدات النشطة. ويعمل التنظيف المتقدم بشكل مختلف لمحطات العمل والخوادم. ويمكنك تكوين التنظيف المتقدم في إعدادات مهمة فحص البرامج الضارة وفي إعدادات التطبيق.

- ترقية التطبيق. لتثبيت التحديثات والتصحيحات الرئيسية دون إعادة التشغيل، يجب عليك تغيير وضع ترقية التطبيق. وبشكل افتراضي، يتم تعطيل ميزة تثبيت تحديثات التطبيق بدون إعادة التشغيل.

- Kaspersky Endpoint Agent. يقدم Kaspersky Endpoint Security عاملاً مدمجًا للعمل مع حلول Detection and Response. وإذا لزم الأمر، انقل إعدادات سياسة Kaspersky Endpoint Agent إلى سياسة Kaspersky Endpoint Security.

- مهام تحديث. تأكد أن إعدادات مهمة تحديث تم ترحيلها بشكل صحيح. وبدلاً من مهام KSWS الثلاث، تستخدم KES مهمة KES واحدة. ويمكنك تحسين مهام تحديث وإزالة المهام الزائدة.

- مهام اخرى. تعمل مكونات التحكم في التطبيق والتحكم في الجهاز ومراقبة سلامة الملفات بشكل مختلف في KSWS وKES. ولا يستخدم KES مهام Baseline File Integrity Monitor وApplications Launch Control Generator وRule Generator for Device Control. لذلك لا يتم ترحيل هذه المهام. وبعد الترحيل، يمكنك تكوين مكونات مراقبة سلامة الملفات والتحكم في التطبيقات والتحكم في الجهاز.

تثبيت KES بدلاً من KSWS

يمكنك تثبيت Kaspersky Endpoint Security بالطرق التالية:

- تثبيت KES بعد إزالة KSWS (موصى به).

- تثبيت KES فوق KSWS.

إزالة Kaspersky Security for Windows Server

يمكنك إزالة التطبيق عن بعد باستخدام مهمة إلغاء تثبيت التطبيق عن بعد أو محليًا على الخادم. وقد تحتاج إلى إعادة تشغيل الخادم بعد إزالة KSWS. إذا كنت تريد تثبيت Kaspersky Endpoint Security دون إعادة التشغيل، يرجى التأكد من إزالة Kaspersky Security for Windows Server بالكامل. وإذا لم تتم إزالة التطبيق بالكامل، فقد يتسبب تثبيت Kaspersky Endpoint Security في تشغيل الخادم بشكل خاطئ. ويُوصى أيضًا بالتأكد من إزالة التطبيق بالكامل إذا كنت قد استخدمت الأداة المساعدة kavremover. لا تدعم الأداة المساعدة kavremover إدارة KSWS.

بعد إزالة KSWS، قم بتثبيت Kaspersky Endpoint Security for Windows باستخدام أي طريقة متاحة.

يقوم المسؤولون عادةً بتمكين الحماية بكلمة مرور لتقييد الوصول إلى KSWS. وهذا يعني أنك ستحتاج إلى إدخال كلمة المرور لإزالة KSWS. لا يدعم Kaspersky Endpoint Security نقل كلمة المرور لإزالة Kaspersky Security for Windows Server عند تثبيت KES أعلى KSWS. ويمكنك نقل كلمة المرور فقط إذا كنت تقوم بتثبيت KES في سطر الأوامر. لذلك، قبل إزالة KSWS، يجب عليك إيقاف تشغيل حماية كلمة المرور في إعدادات التطبيق وأعد تشغيل الحماية بكلمة مرور في إعدادات التطبيق بعد إكمال الترحيل من KSWS إلى KES.

عندما تقوم بتثبيت KES عن بعد، فإن المكونات التي حددتها في خصائص حزمة التثبيت يتم تثبيتها على الخادم. ونوصي بتحديد المكونات الافتراضية في خصائص حزمة التثبيت. وليس من الضروري إعادة التشغيل عند تثبيت KES فوق KSWS.

قبل التثبيت المحلي، يتحقق تطبيق Kaspersky Endpoint Security من جهاز الكمبيوتر بحثًا عن وجود تطبيقات Kaspersky. وفي حالة تثبيت Kaspersky Security for Windows Server على جهاز الكمبيوتر، يكتشف KES مجموعة مكونات KSWS المثبتة ويحدد المكونات نفسها لتثبيتها. وليس من الضروري إعادة التشغيل عند تثبيت KES فوق KSWS.

إذا فشل تثبيت KES فوق KSWS، يمكنك التراجع عن التثبيت. وبعد التراجع عن التثبيت، يوصى بإعادة تشغيل الخادم والمحاولة مرة أخرى.

ولا يتم ترحيل إعدادات ومهام KSWS عند تثبيت Kaspersky Endpoint Security for Windows. ولترحيل الإعدادات والمهام، قم بتشغيل معالج تحويل تصحيح المهام والسياسات.

يمكنك التحقق من قائمة المكونات المثبتة في القسم **الأمان** في واجهة التطبيق، باستخدام الأمر `status`، أو في وحدة تحكم Kaspersky Security Center في خصائص الكمبيوتر. ويمكنك تغيير مجموعة المكونات بعد التثبيت باستخدام تغيير مكونات التطبيق.

ترحيل تكوين [KSWS+KEA] إلى تكوين [KES+العامل المضمن]

لدعم استخدام Kaspersky Endpoint Security for Windows كجزء من EDR (KATA) وEDR Optimum وEDR Expert وKaspersky Sandbox وMDR، تمت إضافة عامل مُضمن إلى التطبيق. ولم تعد بحاجة إلى تطبيق Kaspersky Endpoint Agent منفصل للعمل مع هذين الحلين.

عند الترحيل من KSWS إلى KES، تستمر حلول EDR (KATA) وEDR Optimum وEDR Expert وKaspersky Sandbox وMDR في العمل مع Kaspersky Endpoint Security. بالإضافة إلى ذلك، تتم إزالة Kaspersky Endpoint Agent من الكمبيوتر.

يتضمن ترحيل تكوين [KSWS+KEA] إلى [KES+العامل المضمن] الخطوات التالية:

1. **الترحيل من KSWS إلى KES**

   يتضمن الترحيل من KSWS إلى KES تثبيت Kaspersky Endpoint Security بدلاً من Kaspersky Security for Windows Server.

   للترحيل، يجب عليك تحديد المكونات اللازمة لدعم حلول Detection and Response كجزء من Kaspersky Endpoint Security. وبعد تثبيت التطبيق، يتحول Kaspersky Endpoint Security إلى استخدام العامل المضمن ويزيل Kaspersky Endpoint Agent.

2. **ترحيل السياسة والمهام**

   يتضمن ترحيل سياسات ومهام [KSWS+KEA] إلى [KES+العامل المضمن] الخطوات التالية:

   1. ترحيل السياسات والمهام من KSWS إلى KES باستخدام معالج تحويل تصحيح المهام والسياسات (متاح فقط في وحدة تحكم الإدارة (MMC)).

      نتيجة لذلك، تتم إضافة ملف تعريف السياسة مع اسم سياسة UpgradedFromKSWS <Kaspersky Security for Windows Server> إلى سياسة KES. ويتم أيضًا إنشاء مهام KES الجديدة مع أسماء <اسم مهمة KSWS > (تم التحويل).

   2. ترحيل السياسات والمهام من KEA إلى KES باستخدام المعالج للترحيل من Kaspersky Endpoint Agent (متاح فقط على Web Console وCloud Console).

نتيجة لذلك، يتم إنشاء سياسة جديدة بالاسم <اسم سياسة Kaspersky Endpoint Security> و<اسم سياسة Kaspersky Endpoint Agent>. ويتم أيضًا إنشاء مهام جديدة ومهام KES.

3. **وظيفة الترخيص**

إذا كنت تستخدم ترخيص Kaspersky Endpoint Detection and Response Optimum أو Kaspersky Optimum Security لتفعيل Kaspersky Endpoint Security لنظام التشغيل Windows و Kaspersky Endpoint Agent، فسيتم تفعيل وظيفة EDR Optimum تلقائيًا بعد ترقية التطبيق إلى الإصدار 11.7.0. ولست بحاجة إلى فعل أي شيء آخر.

إذا كنت تستخدم ترخيص المكون الإضافي Kaspersky Endpoint Detection and Response Optimum مستقلاً لتفعيل وظيفة EDR Optimum، فيجب عليك التأكد من إضافة مفتاح EDR Optimum إلى مستودع Kaspersky Security Center و تمكين وظيفة توزيع مفتاح الترخيص التلقائي. وبعد ترقية التطبيق إلى الإصدار 11.7.0، يتم تفعيل وظيفة EDR Optimum تلقائيًا.

إذا كنت تستخدم ترخيص Kaspersky Endpoint Detection and Response Optimum أو Kaspersky Optimum Security لتفعيل Kaspersky Endpoint Agent، وترخيصًا مختلفًا لتفعيل Kaspersky Endpoint Security for Windows، فيجب عليك استبدال مفتاح Kaspersky Endpoint Security for Windows ليحل محله مفتاح Kaspersky Endpoint Detection المشترك ومفتاح Response Optimum أو Kaspersky Optimum Security. يمكنك استبدال المفتاح باستخدام مهمة Add key.

لا تحتاج إلى تفعيل وظيفة Kaspersky Sandbox. وستتوفر وظيفة Kaspersky Sandbox فور ترقية وتفعيل Kaspersky Endpoint Security for Windows.

يمكن استخدام ترخيص Kaspersky Anti Targeted Attack Platform فقط لتفعيل Kaspersky Endpoint Security كجزء من حل Kaspersky Anti Targeted Attack Platform. وبعد ترقية التطبيق إلى الإصدار 12.1، يتم تفعيل وظيفة EDR (KATA) تلقائيًا. ولست بحاجة إلى فعل أي شيء آخر.

4. **التحقق من صحة Kaspersky Endpoint Detection and Response Optimum وKaspersky Sandbox**

إذا كانت حالة الكمبيوتر بعد الترقية هي Critical في Kaspersky Security Center console:

- تأكد من تثبيت عامل الإدارة الإصدار 13.2 أو أحدث.
- تحقق من حالة تشغيل العامل المُضمن عن طريق عرض Application components status report. إذا كانت حالة أحد المكونات Not installed ، فقم بتثبيت المكونات باستخدام مهمة Change application components.
- تأكد من قبولك لبيان Kaspersky Security Network في السياسة الجديدة لتطبيق Kaspersky Endpoint Security for Windows.

تأكد من تفعيل وظيفة EDR Optimum باستخدام Application components status report. وإذا كانت حالة مكون ما غير مشمول بالترخيص ، فتأكد من تشغيل وظيفة توزيع مفتاح الترخيص التلقائي لمكون EDR Optimum.

التأكد من إزالة Kaspersky Security for Windows Server بنجاح

تأكد من إزالة Kaspersky Security for Windows Server بشكل كامل:

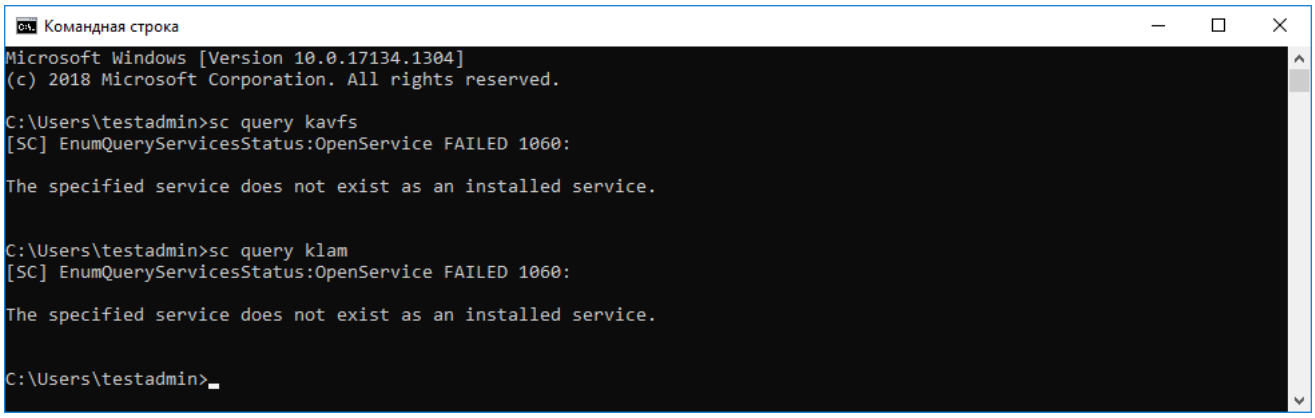
- المجلد `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` غير موجود.
- تكون الخدمات التالية غير موجودة:
  - (Kaspersky Security Service (KAVFS
  - (Kaspersky Security Management (KAVFSGT
  - (Kaspersky Security Exploit Prevention (KAVFSSLP
  - (Kaspersky Security Script Checker (KAVFSSCS

يمكنك التحقق من الخدمات قيد التشغيل في Task Manager (إدارة المهام) أو عن طريق إصدار أمر `sc query` (انظر الشكل أدناه).

- تكون برامج التشغيل التالية غير موجودة:

- klam.sys
- klflt.sys
- klramdisk.sys
- klelaml.sys
- klfltdev.sys
- klips.sys
- klids.sys
- klwtpee

يمكنك التحقق من برامج التشغيل المثبتة في المجلد `C:\Windows\System32\drivers` أو عن طريق إصدار الأمر `sc query`. وإذا كانت هناك خدمة أو برنامج تشغيل مفقود، فستتلقى الاستجابة التالية:



التأكد من إزالة Kaspersky Security for Windows Server وبرامج التشغيل بنجاح

إذا ظل التطبيق أو ملفات برنامج التشغيل على الخادم، فاحذف الملفات ذات الصلة يدويًا. وإذا استمرت خدمات Kaspersky Security for Windows Server قيد التشغيل على الخادم، أوقف خدمات (`sc stop`) واحذف (`sc delete`) يدويًا. لإيقاف برنامج التشغيل klam.sys، استخدم الأمر `fltmc unload klam`.

تفعيل KES بمفتاح KSWS

بعد تثبيت التطبيق، يمكنك تفعيل Kaspersky Endpoint Security for Windows (KES) باستخدام مفتاح ترخيص Kaspersky Security for Windows Server (KSWS). وتعتمد عملية التفعيل بعد الترحيل على طريقة تفعيل KSWS (انظر الجدول أدناه).

لا يدعم Kaspersky Endpoint Security ترخيص Kaspersky Security for Storage. وللعمل مع هذا الترخيص، تحتاج إلى استخدام Kaspersky Security for Windows Server.

لتفعيل KES باستخدام مفتاح KSWS، يمكنك استخدام رمز التفعيل. وإذا كنت تستخدم ملف مفتاح لتفعيل التطبيق، تحتاج إلى الاتصال بالدعم الفني لطلب ملف مفتاح Kaspersky Endpoint Security.

تفعيل Kaspersky Endpoint Security for Windows باستخدام مفتاح Kaspersky Security for Windows Server

طريقة تفعيل Kaspersky Security for Windows Server	ترحيل المفتاح إلى Kaspersky Endpoint Security for Windows.

التوزيع التلقائي لمفتاح ترخيص KSWS على أجهزة الكمبيوتر.	في حالة تمكين التوزيع التلقائي للمفاتيح في خصائص مفتاح ترخيص KSWS، يتم تفعيل KES تلقائيًا باستخدام مفتاح KSWS.
تمت إضافة مفتاح KSWS بواسطة مهمة.	في حالة تفعيل KSWS باستخدام المهمة، سيتم حذف مفتاح ترخيص KSWS أثناء الترحيل من KSWS. ويجب عليك تفعيل التطبيق مرة أخرى. على سبيل المثال، يمكنك إضافة مفتاح ترخيص إلى حزمة تثبيت Kaspersky Endpoint Security for Windows.
يتم إضافة مفتاح KSWS محليًا في واجهة التطبيق.	في حالة تفعيل KSWS محليًا باستخدام معالج تفعيل التطبيق، سيتم حذف مفتاح ترخيص KSWS أثناء الترحيل من KSWS. ويجب عليك تفعيل التطبيق مرة أخرى. على سبيل المثال، يمكنك إضافة مفتاح ترخيص إلى حزمة تثبيت Kaspersky Endpoint Security for Windows.
يُضاف مفتاح KSWS إلى حزمة التثبيت.	في حالة تفعيل KSWS باستخدام المفتاح من حزمة التثبيت، سيتم حذف مفتاح ترخيص KSWS أثناء الترحيل من KSWS. ويجب عليك تفعيل التطبيق مرة أخرى. على سبيل المثال، يمكنك إضافة مفتاح ترخيص إلى حزمة تثبيت Kaspersky Endpoint Security for Windows.
صورة جهاز افتراضي مدفوع Amazon Machine Image - AMI) في Amazon Web Services (AWS).	إذا اشتريت Kaspersky Security Center كصورة جهاز افتراضي مدفوع (Amazon Machine Image - AMI) في Amazon Web Services (AWS) ، فإن تفعيل KES ليس مطلوبًا. وفي هذه الحالة، يستخدم Kaspersky Security Center اشتراك AWS الذي تمت إضافته بالفعل إلى التطبيق.
صورة Kaspersky Security Center جاهزة ومجانية مع ترخيصك الخاص (نموذج أحضر ترخيصك - BYOL).	إذا كنت تستخدم صورة Kaspersky Security Center مجانية جاهزة للاستخدام مع ترخيصك الخاص في بيئة سحابية (نموذج أحضر ترخيصك - BYOL) ، يجب عليك تفعيل التطبيق باستخدام أي طريقة متاحة. وستحتاج إلى ترخيص Kaspersky Hybrid Cloud Security.

اعتبارات خاصة لترحيل الخوادم عالية التحميل

على الخوادم عالية التحميل، من المهم مراقبة الأداء وتجنب الأخطاء. وبعد الترحيل إلى Kaspersky Endpoint Security for Windows، نوصي بالتعطيل المؤقت لمكونات التطبيق التي تستخدم موارد خادم كبيرة مقارنة بالمكونات الأخرى. وبعد التأكد من أن الخادم يعمل كالمعتاد، يمكنك إعادة تشغيل مكونات التطبيق.

نوصي بترحيل الخوادم عالية التحميل على النحو التالي:

1. أنشئ سياسة Kaspersky Endpoint Security بالإعدادات الافتراضية.

   تعتبر الإعدادات الافتراضية هي الأمثل. ويوصي خبراء Kaspersky بهذه الإعدادات. وتوفر الإعدادات الافتراضية مستوى الحماية الموصى به والاستخدام الأمثل للموارد.

2. في إعدادات السياسة، قم بإيقاف تشغيل المكونات التالية: الحماية من تهديدات الشبكة واكتشاف السلوك ومنع الاستغلال ومحرك المعالجة والتحكم في التطبيقات.

   إذا قامت مؤسستك بنشر حل Kaspersky Managed Detection and Response (MDR)، قم بتحميل ملف تكوين BLOB إلى سياسة Kaspersky Endpoint Security.

3. قم بإزالة Kaspersky Security for Windows Server من الخادم.

4. قم بتثبيت Kaspersky Endpoint Security for Windows باستخدام مجموعة المكونات الافتراضية.

   إذا نشرت مؤسستك حلول Detection and Response، حدد المكونات ذات الصلة في خصائص حزمة التثبيت.

5. التحقق من إعدادات التطبيق:

   - يتم تفعيل التطبيق باستخدام مفتاح ترخيص KSWS.
   - يتم تطبيق السياسة الجديدة. يتم تعطيل المكونات المحددة مسبقًا.

6. تأكد أن الخادم يعمل. تأكد أن Kaspersky Endpoint Security for Windows لا يستخدم أكثر من 1% من موارد الخادم.

7. إذا لزم الأمر، أنشئ استثناءات الفحص وأضف التطبيقات الموثوقة وأنشئ قائمة بعناوين الويب الموثوقة.

8. قم بتشغيل مكونات اكتشاف السلوك ومنع الاستغلال ومحرك المعالجة. تأكد أن Kaspersky Endpoint Security for Windows لا يستخدم أكثر من 1% من موارد الخادم.

9. قم بتشغيل مكون الحماية من تهديدات الشبكة. تأكد أن Kaspersky Endpoint Security for Windows لا يستخدم أكثر من 2% من موارد الخادم.

10. قم بتشغيل مكون التحكم في التطبيقات في وضع اختبار القاعدة.

11. تأكد من عمل التحكم في التطبيقات. إذا لزم الأمر، أضف تحكم في التطبيقات جديدة وأوقف تشغيل وضع اختبار القاعدة بعد التأكد من أن مكون التحكم في التطبيقات يعمل.

بعد الترحيل من KSWS إلى KES، تأكد أن التطبيق يعمل بشكل صحيح. تحقق من حالة الخادم في وحدة التحكم (يجب أن تكون جيدة). تأكد من عدم الإبلاغ عن أي أخطاء في التطبيق، وتحقق أيضًا من وقت آخر اتصال بخادم الإدارة ووقت آخر تحديث لقاعدة البيانات وحالة حماية الخادم.

مثال على الترحيل من [KSWS + KEA] إلى KES

عند الترحيل من Kaspersky Security for Windows Server (KSWS) إلى Kaspersky Endpoint Security (KES)، يمكنك استخدام التوصيات التالية لتكوين حماية الخادم وتحسين الأداء. وهنا سنلقي نظرة على مثال للترحيل لمؤسسة واحدة.

البنية التحتية للمؤسسة

قامت الشركة بتركيب المعدات التالية:

- Kaspersky Security Center 14.2

  يدير المسؤول حلول Kaspersky باستخدام وحدة تحكم الإدارة (MMC). يتم نشر Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) أيضًا

  في Kaspersky Security Center، يتم إنشاء ثلاث مجموعات إدارة تحتوي على خوادم المؤسسة: مجموعتا إدارة لخوادم SQL ومجموعة إدارة لخوادم Microsoft Exchange. وتتم إدارة كل مجموعة إدارة من خلال سياستها الخاصة. ويتم إنشاء مهام Database Update وOn-demand scan لجميع الخوادم في المؤسسة.

  تتم إضافة مفتاح تفعيل KSWS إلى Kaspersky Security Center. ويتم تمكين التوزيع التلقائي للمفاتيح.

- خوادم SQL التي تم تثبيت Kaspersky Security for Windows Server 11.0.1 وKaspersky Endpoint Agent 3.11 عليها. يتم دمج خوادم SQL في مجموعتين.

  تتم إدارة KSWS بواسطة سياسات (SQL_Policy(1 وSQL_Policy(2) . يتم أيضًا إنشاء مهام Database Update, On-demand scan.

- خادم Microsoft Exchange server مُثبت عليه Kaspersky Security for Windows Server 11.0.1 وKaspersky Endpoint Agent 3.11.

  تتم إدارة KSWS بواسطة سياسة Exchange_Policy. يتم أيضًا إنشاء مهام Database Update, On-demand scan.

التخطيط للترحيل

يتضمن الترحيل الخطوات التالية:

1. ترحيل مهام وسياسات KSWS باستخدام معالج تحويل مجموعة السياسات والمهام.

2. ترحيل سياسة Kaspersky Endpoint Agent باستخدام معالج تحويل مجموعة السياسات والمهام.

3. استخدام العلامات لتفعيل ملفات تعريف السياسة في خصائص السياسة الجديدة.

4. تثبيت KES بدلاً من KSWS.

5. تفعيل EDR Optimum.

6. تأكيد عمل KES.

يتم تنفيذ سيناريو الترحيل مبدئيًا على إحدى مجموعات خوادم SQL. ثم يتم تنفيذ سيناريو الترحيل على المجموعة الأخرى من خوادم SQL. ثم يتم تنفيذ سيناريو الترحيل على Microsoft Exchange.

ترحيل مهام وسياسات KSWS باستخدام معالج تحويل مجموعة السياسات والمهام.

لترحيل مهام KSWS، يمكنك استخدام معالج تحويل مجموعة السياسات والمهام (معالج الترحيل). ونتيجة لذلك، بدلاً من سياسات 1)SQL_Policy) و2)SQL_Policy) وExchange_Policy، ستحصل على سياسة واحدة مع ثلاثة ملفات تعريف لخوادم SQL وMicrosoft Exchange على التوالي. سيتم تسمية ملف تعريف السياسة الجديد الذي يتضمن إعدادات KSWS UpgradedFromKSWS <اسم سياسة Kaspersky Security for Windows Server>. وفي خصائص ملف التعريف، يحدد معالج الترحيل تلقائيًا علامة الجهاز `UpgradedFromKSWS` كمعيار تشغيل. وبالتالي يتم تطبيق الإعدادات من ملف تعريف السياسة على الخوادم تلقائيًا.

ترحيل سياسة Kaspersky Endpoint Agent باستخدام معالج تحويل مجموعة السياسات والمهام

لترحيل سياسات Kaspersky Endpoint Agent، يمكنك استخدام معالج تحويل مجموعة السياسات والمهام. ولا يتوفر معالج ترحيل السياسة والمهام لتطبيق Kaspersky Endpoint Agent إلا في Web Console.

استخدام العلامات لتفعيل ملفات تعريف السياسة في خصائص السياسة الجديدة

حدد علامة الجهاز التي قمت بتعيينها مسبقًا كحالة تفعيل لملف التعريف. افتح خصائص السياسة وحدد القواعد العامة لتفعيل ملف تعريف السياسة كشرط لتفعيل ملف التعريف.

تثبيت KES بدلاً من KSWS

قبل تثبيت KES، يجب عليك تعطيل حماية كلمة المرور في خصائص سياسة KSWS.

يتضمن تثبيت KES الخطوات التالية:

1. تحضير حزمة التثبيت. في خصائص حزمة التثبيت، حدد مجموعة توزيع Kaspersky Endpoint Security for Windows 12.0 وحدد مجموعة المكونات الافتراضية.

2. أنشئ مهمة تثبيت التطبيق عن بعد لإحدى مجموعات إدارة خادم SQL.

3. في خصائص المهمة، حدد حزمة التثبيت وملف مفتاح الترخيص.

4. انتظر حتى تكتمل المهمة بنجاح.

5. كرر تثبيت KES لمجموعات الإدارة المتبقية.

يضيف Kaspersky Security Center تلقائيًا علامة `UpgradedFromKSWS` إلى أسماء أجهزة الكمبيوتر على وحدة التحكم بعد اكتمال تثبيت KES.

للتحقق من تثبيت KES، يمكنك استخدام التقرير عن نشر الحماية. ويمكنك أيضًا التحقق من حالة الجهاز. لتأكيد تفعيل التطبيق، يمكنك استخدام التقرير عن استخدام مفاتيح الترخيص.

تفعيل EDR Optimum

يمكنك تفعيل وظيفة EDR Optimum باستخدام ترخيص Kaspersky Endpoint Detection and Response Optimum Add-on الإضافي المستقل. ويجب عليك تأكيد إضافة مفتاح EDR Optimum إلى مستودع Kaspersky Security Center وتمكين وظيفة توزيع مفتاح الترخيص التلقائي.

للتحقق من تفعيل EDR Optimum، يمكنك استخدام التقرير عن حالة مكونات التطبيق.

تأكيد عمل KES

لتأكيد عمل KES، يمكنك التحقق ورؤية عدم الإبلاغ عن أي أخطاء. يجب أن تكون حالة الجهاز جيدة. اكتملت بنجاح مهام فحص التحديث والبرامج الضارة.

إدارة التطبيق على خادم Core Mode

لا يحتوي خادم في Core Mode على واجهة مستخدم رسومية. لذلك يمكنك فقط إدارة التطبيق عن بُعد باستخدام وحدة تحكم Kaspersky Security Center أو محليًا في سطر الأوامر.

إدارة التطبيق باستخدام وحدة تحكم Kaspersky Security Center

لا يختلف تثبيت التطبيق باستخدام وحدة تحكم Kaspersky Security Center عن تثبيته بالطريقة العادية. وعند إنشاء حزمة تثبيت، يمكنك إضافة مفتاح ترخيص لتفعيل التطبيق. ويمكنك استخدام مفتاح Kaspersky Endpoint Security for Windows أو مفتاح Kaspersky Security for Windows Server.

على خادم Core Mode، لا تتوفر مكونات التطبيق التالية: الحماية من تهديدات الويب، والحماية من تهديدات البريد، والتحكم في الويب، ومنع هجمات USB الخبيثة ، والتشفير على مستوى الملف (FLE)، وتشفير القرص من Kaspersky (FDE).

إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. إعادة التشغيل مطلوبة فقط إذا كان يجب عليك إزالة التطبيقات غير المتوافقة قبل التثبيت. قد تكون إعادة التشغيل مطلوبة أيضًا عند تحديث إصدار التطبيق. لا يستطيع التطبيق عرض نافذة لمطالبة المستخدم بإعادة تشغيل الخادم. ويمكنك التعرف على الحاجة إلى إعادة تشغيل الخادم من التقارير الموجودة في وحدة تحكم Kaspersky Security Center.

لا تختلف إدارة التطبيق على خادم Core Mode عن إدارة جهاز كمبيوتر. ويمكنك استخدام السياسات والمهام لتكوين التطبيق.

تتضمن إدارة التطبيق على خوادم Core Mode الاعتبارات الخاصة التالية:

- لا يحتوي خادم Core Mode على واجهة مستخدم رسومية، لذلك لا يعرض Kaspersky Endpoint Security تحذيرًا يخبر المستخدم بضرورة التنظيف المتقدم. ولتنظيف تهديد، تحتاج إلى enable Advanced Disinfection technology في إعدادات التطبيق و enable immediate Advanced Disinfection في إعدادات مهمة فحص البرامج الضارة. بعد ذلك يتعين عليك بدء مهمة فحص البرامج الضارة.
- لا يتوفر تشفير محرك الأقراص من BitLocker إلا مع الوحدة النمطية للنظام الأساسي الموثوق بها (TPM). ولا يمكن استخدام رمز PIN / كلمة مرور للتشفير لأن التطبيق لا يستطيع عرض نافذة المطالبة بكلمة المرور للمصادقة على التمهيد المسبق. وفي حالة تمكين وضع التوافق مع معيار معالجة المعلومات الفيدرالي (FIPS) في نظام التشغيل، فيرجى توصيل محرك أقراص قابل للإزالة لحفظ مفتاح التشفير قبل أن تبدأ في تشفير محرك الأقراص.

لإدارة التطبيق من سطر الأوامر

عندما لا يمكنك استخدام واجهة مستخدم رسومية، يمكنك إدارة Kaspersky Endpoint Security من سطر الأوامر.

لتثبيت التطبيق على خادم Core Mode، قم بتشغيل الأمر التالي:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

لتفعيل التطبيق، قم بتشغيل الأمر التالي:

```
avp.com license /add <activation code or key file>
```

للتحقق من حالات ملف تعريف التطبيق، قم بتشغيل الأمر التالي:

```
avp.com status
```

لعرض قائمة أوامر إدارة التطبيق، قم بتشغيل الأمر التالي:

```
avp.com help
```

لإدارة التطبيق من سطر الأوامر

يمكنك إدارة Kaspersky Endpoint Security من سطر الأوامر. يمكنك استعراض قائمة الأوامر لإدارة التطبيق من خلال تنفيذ الأمر HELP. للقراءة عن بناء الأمر لأمر محدد، قم بإدخال HELP <command>.

يجب تخطي الأحرف الخاصة في الأمر. ولتخطي الأحرف & و | و (و) و < و > و ^، استخدم حرف ^ (على سبيل المثال، لاستخدام حرف &، أدخل ^&). لتخطي الحرف %، أدخل %%.

تثبيت التطبيق

يمكن تثبيت برنامج Kaspersky Endpoint Security من سطر الأوامر في واحدة من الأوضاع التالية:

- في الوضع التفاعلي باستخدام معالج إعداد التطبيق.
- في الوضع الصامت. بعد بدء عملية التثبيت في الوضع الصامت، لا يلزم تدخلك في عملية التثبيت. لتثبيت التطبيق في الوضع الصامت، استخدم المفاتيح /s و /qn.

قبل تثبيت التطبيق في الوضع الصامت، يُرجى فتح وقراءة اتفاقية ترخيص المستخدم النهائي ونص سياسة الخصوصية. تم تضمين اتفاقية ترخيص المستخدم النهائي ونص سياسة الخصوصية في حزمة توزيع برنامج Kaspersky Endpoint Security. لا يجوز لك متابعة تثبيت التطبيق إلا إذا كنت قد قرأت، وفهمت، وقبلت أحكام وشروط اتفاقية ترخيص المستخدم النهائي بالكامل، أنك تفهم وتوافق على أن بياناتك ستتم معالجتها ونقلها (بما في ذلك إلى البلدان الخارجية) وفقًا لسياسة الخصوصية، وأنك قد قرأت وفهمت سياسة الخصوصية بالكامل. إذا كنت لا توافق على أحكام وشروط اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية، يُرجى عدم تثبيت برنامج Kaspersky Endpoint Security أو استخدامه.

يمكنك استعراض قائمة الأوامر لتثبيت التطبيق من خلال تنفيذ الأمر /h. وللحصول على تعليمات حول بناء جملة أمر التثبيت، اكتب setup_kes.exe /h. ونتيجة لذلك، يعرض المُثبت نافذة تحتوي على وصف لخيارات الأمر (انظر الشكل أدناه).

لتثبيت التطبيق أو ترقية إصدار سابق للتطبيق:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.

2. انتقل إلى المجلد الذي يحتوي على حزمة التوزيع الخاصة بـ Kaspersky Endpoint Security.

3. قم بتشغيل الأمر التالي:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1]
[/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing
level>] [/s]
```

أو

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0]
[ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password>
KLPASSWDAREA=<password scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [/qn]
```

نتيجة لذلك، يتم تثبيت التطبيق على الكمبيوتر. ويمكنك التأكد من تثبيت التطبيق والتحقق من إعدادات التطبيق عن طريق إصدار أمر `status`.

إعدادات تثبيت التطبيق

`EULA=1`	قبول شروط اتفاقية ترخيص المستخدم النهائي. يتم تضمين نص اتفاقية الترخيص في حزمة توزيع Kaspersky Endpoint Security. يعد قبول شروط اتفاقية ترخيص المستخدم النهائي أمرًا ضروريًا لتثبيت التطبيق أو ترقية إصداره.
`PRIVACYPOLICY=1`	قبول سياسة الخصوصية. ويتم تضمين نص سياسة الخصوصية في حزمة توزيع Kaspersky Endpoint Security. لتثبيت التطبيق أو ترقية إصدار التطبيق، يجب عليك قبول سياسة الخصوصية.
`KSN`	قبول أو رفض المشاركة في Kaspersky Security Network (KSN). إذا لم يتم تعيين قيمة لهذه المعلمة، فسوف يطالب Kaspersky Endpoint Security بتأكيد موافقتك أو رفضك المشاركة في KSN عند بدء تشغيل Kaspersky Endpoint Security لأول مرة. القيم المتاحة: • `1` – قبول المشاركة في KSN. • `0` – رفض المشاركة في KSN (القيمة الافتراضية). يتم تحسين حزمة توزيع Kaspersky Endpoint Security للاستخدام مع Kaspersky Security Network. وإذا اخترت عدم المشاركة في Kaspersky Security Network، فينبغي عليك تحديث Kaspersky Endpoint Security على الفور بعد اكتمال التثبيت.
`ALLOWREBOOT=1`	إعادة التشغيل التلقائي للكمبيوتر، إذا لزم الامر بعد تثبيت التطبيق أو ترقيته. إذا كان لا يوجد قيمة محددة لهذا المعامل، فإن إعادة التشغيل التلقائي للكمبيوتر غير مدعومة. إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. إعادة التشغيل مطلوبة فقط إذا كان يجب عليك إزالة التطبيقات غير المتوافقة قبل التثبيت. قد تكون إعادة التشغيل مطلوبة أيضًا عند تحديث إصدار التطبيق.
`SKIPPRODUCTCHECK=1`	تعطيل التحقق من البرامج غير المتوافقة. تتوفر قائمة البرامج غير المتوافقة في ملف incompatible.txt المضمن في حزمة التوزيع. في حال عدم تحديد قيمة هذه المعلمة وتم اكتشاف برنامج غير متوافق، فسوف يتم

	إلغاء تثبيت Kaspersky Endpoint Security.
SKIPPRODUCTUNINSTALL=1	تعطيل الإزالة التلقائية للبرامج غير المتوافقة التي تم اكتشافها. في حال عدم تحديد قيمة لهذه المعلمة، فإن Kaspersky Endpoint Security سوف يحاول إزالة البرنامج غير المتوافق. لا يمكن تمكين الإزالة التلقائية للبرامج غير المتوافقة عند تثبيت Kaspersky Endpoint Security باستخدام مُثبت msiexec. استخدم setup_kes.exe لتمكين الإزالة التلقائية للبرامج غير المتوافقة.
CLEANERSIGNCHECK=0|1	التحقق من التوقيعات الرقمية لملفات البرامج غير المتوافقة المكتشفة. لإزالة البرامج غير المتوافقة، يقوم Kaspersky Endpoint Security بتشغيل ملف مُثبت البرنامج. وإذا لم يكن لملف المثبت توقيع رقمي، فإن Kaspersky Endpoint Security يعتبر الملف غير موثوق به ويوقف إزالة البرامج غير المتوافقة لتجنب تشغيل التعليمات البرمجية التي يحتمل أن تكون ضارة. وإذا لم يتمكن التطبيق من التحقق من التوقيع الرقمي لملف البرنامج غير المتوافق الذي تم اكتشافه، فسيتم إيقاف تثبيت Kaspersky Endpoint Security مع ظهور خطأ. تختلف القيمة الافتراضية وفقًا لطريقة تثبيت البرنامج: • يعني 0 أن التحقق من التوقيع الرقمي معطل (القيمة الافتراضية في حالة نشرها من خلال Kaspersky Security Center). • يعني 1 أن التحقق من التوقيع الرقمي تم تمكينه (القيمة الافتراضية إذا كان التطبيق قيد التثبيت محليًا).
KLLOGIN	قم بتعيين اسم المستخدم للوصول إلى ميزات وإعدادات Kaspersky Endpoint Security (مكون حماية كلمة المرور). يتم تعيين اسم المستخدم بالإضافة إلى المعلمتين KLPASSWD و KLPASSWDAREA. تم استخدام اسم المستخدم KLAdmin بشكل افتراضي.
KLPASSWD	حدد كلمة مرور للوصول إلى ميزات وإعدادات Kaspersky Endpoint Security (يتم تحديد كلمة المرور بالإضافة إلى المعلمتين KLLOGIN و KLPASSWDAREA). إذا قمت بتحديد كلمة مرور ولم تحدد اسم مستخدم بمعلمة KLLOGIN، فسيتم استخدام KLAdmin كاسم مستخدم افتراضيًا.
KLPASSWDAREA	حدد نطاق كلمة المرور للوصول إلى Kaspersky Endpoint Security. عندما يحاول مستخدم تنفيذ إجراء تم تضمينه في هذا النطاق، فسيطالب Kaspersky Endpoint Security بإدخال بيانات اعتماد حساب المستخدم (المعلمتان KLLOGIN و KLPASSWD). استخدم الحرف " ; " لتحديد قيم متعددة. القيم المتاحة: • SET – تعديل إعدادات التطبيق. • EXIT – الخروج من التطبيق. • DISPROTECT – تعطيل مكونات الحماية وإيقاف مهام الفحص. • DISPOLICY – تعطيل سياسة Kaspersky Security Center. • UNINST – إزالة التطبيق من الكمبيوتر. • DISCTRL – تعطيل مكونات المراقبة. • REMOVELIC – إزالة المفتاح. • REPORTS – عرض تقارير. • على سبيل المثال، KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT.

ENABLETRACES	تمكين أو تعطيل تتبع التطبيق. بعد بدء تشغيل Kaspersky Endpoint Security، فإنه يحفظ ملفات التتبع في المجلد %ProgramData%\Kaspersky Lab\KES.21.13\Traces. القيم المتاحة: • 1 – تم تمكين التتبع. • 0 – تم تعطيل التتبع (القيمة الافتراضية).
TRACESLEVEL	مستوى تفاصيل عمليات التتبع. القيم المتاحة: • 100 (حرجة). فقط رسائل حول الأخطاء الفادحة. • 200 (عالي). رسائل حول جميع الأخطاء، بما في ذلك الأخطاء الفادحة. • 300 (تشخيصية). رسائل حول جميع الأخطاء، وكذلك التحذيرات. • 400 (هامة). رسائل حول جميع الأخطاء، والتحذيرات، وكذلك المعلومات الإضافية. • 500 (عادية). رسائل حول جميع الأخطاء، والتحذيرات، وكذلك المعلومات المفصلة حول تشغيل التطبيق في الوضع العادي (الافتراضي). • 600 (قليلة). جميع الرسائل.
ENABLEAZURESUPPORT	تمكين أو تعطيل وضع التوافق مع Azure WVD. القيم المتاحة: • 1 - تم تمكين وضع التوافق مع Azure WVD. • 0 - تم تعطيل وضع التوافق مع Azure WVD (القيمة الافتراضية). تتيح هذه الميزة عرض حالة جهاز Azure الظاهري بشكل صحيح في وحدة التحكم لتطبيق Kaspersky Anti Targeted Attack Platform. ولمراقبة أداء الكمبيوتر، يرسل Kaspersky Endpoint Security بيانات القياس عن بُعد إلى خوادم KATA. ويتضمن القياس عن بعد معرف الكمبيوتر (معرف المستشعر). ويسمح وضع التوافق مع Azure WVD بتعيين معرف مستشعر فريد دائم لهذه الأجهزة الظاهرية. وفي حالة إيقاف تشغيل وضع التوافق، يمكن أن يتغير معرف المستشعر بعد إعادة تشغيل الكمبيوتر بسبب كيفية عمل أجهزة Azure الظاهرية. ومن الممكن أن يتسبب هذا في ظهور نسخ مكررة من الأجهزة الظاهرية على وحدة التحكم.
AMPPL	يؤدي إلى تمكين أو تعطيل إجراءات الحماية الخاصة Kaspersky Endpoint Security باستخدام تقنية AM-PPL (Antimalware Protected Process Light). للحصول على المزيد من التفاصيل حول تقنية AM-PPL، يُرجى زيارة موقع ويب Microsoft. إن تقنية AM-PPL متاحة للإصدار 1703 من نظام التشغيل Windows 10 (RS2) أو إصدار أحدث، ونظام التشغيل Windows Server 2019. القيم المتاحة: • 1 – تم تمكين إجراءات الحماية الخاصة بـ Kaspersky Endpoint Security باستخدام تقنية AM-PPL. • 0 – تم تعطيل إجراءات الحماية الخاصة بـ Kaspersky Endpoint Security باستخدام تقنية AM-PPL.
UPGRADEMODE	وضع ترقية التطبيق: • سلس يعني ترقية التطبيق مع إعادة تشغيل الكمبيوتر (القيمة الافتراضية). • إجباري يعني ترقية التطبيق دون إعادة التشغيل. يمكنك ترقية التطبيق دون إعادة التشغيل بدءًا من الإصدار 11.10.0. ولترقية إصدار سابق من التطبيق، يجب إعادة تشغيل الكمبيوتر. يمكنك أيضًا تثبيت التصحيحات دون إعادة التشغيل بدءًا من الإصدار 11.11.0.

	إعادة التشغيل ليست مطلوبة عند تثبيت برنامج Kaspersky Endpoint Security. لذلك، سيتم تحديد وضع الترقية للتطبيق في إعدادات التطبيق. ويمكنك تغيير هذه المعلمة في إعدادات التطبيق أو في السياسة. عند ترقية التطبيق المُثبت بالفعل، تكون أولوية معلمة سطر الأوامر أقل من تلك الخاصة بالمعلمة المحددة في application settings أو في ملف setup.ini. على سبيل المثال، في حالة تحديد وضع الترقية Force في سطر الأوامر وتحديد وضع Seamless في إعدادات التطبيق، سيتم تثبيت الترقية مع إعادة تشغيل الكمبيوتر (د Seamless).
RESTAPI	إدارة التطبيق من خلال REST API. لإدارة التطبيق من خلال REST API، يجب عليك تحديد اسم المستخدم (RESTAPI_User). القيم المتاحة: • 1 – الإدارة عبر REST API مسموح بها. • 0 - تم حظر الإدارة عبر REST API (القيمة الافتراضية). لإدارة التطبيق من خلال REST API، يجب السماح بالإدارة باستخدام الأنظمة الإدارية. للقيام بذلك، قم بتعيين المعلمة AdminKitConnector=1. إذا كنت تدير التطبيق من خلال REST API، فمن المستحيل إدارة التطبيق باستخدام أنظمة الإدارة الخاصة بـ Kaspersky.
RESTAPI_User	اسم المستخدم الخاص بحساب المجال المستخدم لإدارة التطبيق من خلال REST API. إن إدارة التطبيق من خلال REST API متاحة فقط لهذا المستخدم. أدخل اسم المستخدم <DOMAIN>\<UserName> (على سبيل المثال، RESTAPI_User=COMPANY\Administrator). يمكنك تحديد مستخدم واحد فقط للعمل باستخدام REST API. إن إضافة اسم مستخدم شرط للتمكن من إدارة التطبيق من خلال REST API.
RESTAPI_Port	المنفذ المستخدم لإدارة التطبيق من خلال REST API. يُستخدم المنفذ 6782 بشكل افتراضي. تأكد أن المنفذ خالٍ.
RESTAPI_Certificate	شهادة لتحديد الطلبات (على سبيل المثال، RESTAPI_Certificate=C:\cert.pem). يتطلب التفاعل الآمن لبرنامج Kaspersky Endpoint Security مع عميل REST تكوين تعريف الطلب. ولفعل ذلك، يجب عليك تثبيت شهادة ثم بعد ذلك التوقيع على حمولة كل طلب.
ADMINKITCONNECTOR	إدارة التطبيقات باستخدام نظم الإدارة. تشمل أنظمة الإدارة، على سبيل المثال، Kaspersky Security Center. بالإضافة إلى أنظمة إدارة Kaspersky، يمكنك استخدام حلول مقدمة من جهات خارجية. يوفر Kaspersky Endpoint Security واجهة برمجة تطبيقات (API) لهذا الغرض. القيم المتاحة: • 1 – مسموح بإدارة التطبيقات بمساعدة أنظمة الإدارة (القيمة الافتراضية). • 0 – مسموح بإدارة التطبيقات من خلال الواجهة المحلية فقط.

مثال:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

بعد تثبيت برنامج Kaspersky Endpoint Security، يتم تفعيل الترخيص التجريبي ما لم تكن قد قمت بتقدم رمز تفعيل في ملف setup.ini. يحتوي الترخيص التجريبي عادة على فترة قصيرة. بمجرد انتهاء الترخيص التجريبي، فسيتم تعطيل كل ميزات برنامج Kaspersky Endpoint Security. لمتابعة استخدام التطبيق، تحتاج إلى تفعيل التطبيق بواسطة ترخيص تجاري وذلك باستخدام معالج تفعيل التطبيق أو أمر خاص.

عند تثبيت التطبيق أو ترقية إصداره في الوضع الصامت، يتم دعم استخدام الملفات التالية:

- setup.ini - إعدادات عامة لتثبيت التطبيق
- install.cfg - إعدادات عملية Kaspersky Endpoint Security
- setup.reg - مفاتيح التسجيل

تتم كتابة مفاتيح السجل من ملف setup.reg في السجل فقط في حالة تعيين قيمة `setup.reg` لمعلمة `SetupReg` في ملف setup.ini. يتم إنشاء ملف setup.reg بواسطة خبراء Kaspersky. لا يوصى بتعديل محتويات هذا الملف.

لتطبيق الإعدادات من ملفات setup.ini و install.cfg و setup.reg، ضع هذه الملفات في المجلد الذي يحتوي على حزمة توزيع Kaspersky Endpoint Security. يمكنك أيضًا وضع ملف setup.reg في مجلد مختلف. إذا فعلت ذلك، فأنت بحاجة إلى تحديد مسار الملف في أمر تثبيت التطبيق التالي: `SETUPREG=<path to the setup.reg file>`.

تفعيل التطبيق

لتفعيل التطبيق من خلال سطر الأوامر

اكتب السلسلة التالية في سطر الأوامر:

```
avp.com license /add <activation code or key file> [/login=<user name> /password=<password>]
```

تحتاج إلى إدخال بيانات اعتماد حساب المستخدم (`/login=<user name> /password=<password>`) في حالة تمكين الحماية باستخدام كلمة مرور.

إزالة التطبيق

يمكن إلغاء تثبيت برنامج Kaspersky Endpoint Security من سطر الأوامر بالطرق التالية:

- في الوضع التفاعلي باستخدام معالج إعداد التطبيق.
- في الوضع الصامت. بعد بدء عملية إلغاء التثبيت في الوضع الصامت، لا يلزم تدخلك في عملية الإزالة. لإلغاء تثبيت التطبيق في الوضع الصامت، استخدم المفاتيح `/s` و `/qn`.

لإلغاء تثبيت التطبيق في الوضع الصامت:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.
2. انتقل إلى المجلد الذي يحتوي على حزمة التوزيع الخاصة بـ Kaspersky Endpoint Security.
3. قم بتشغيل الأمر التالي:

- إذا كانت عملية الإزالة ليست محمية بكلمة المرور:

```
setup_kes.exe /s /x
```

أو

```
msiexec.exe /x <GUID> /qn
```

`<GUID>` هو المعرف الفريد للتطبيق. يمكنك معرفة GUID لأي تطبيق باستخدام الأمر التالي:

```
wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name,
IdentifyingNumber
```

- إذا كانت عملية الإزالة محمية بكلمة المرور:

```
setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

أو

```
msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
```

مثال:

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin
KLPASSWD=!Password1 /qn
```

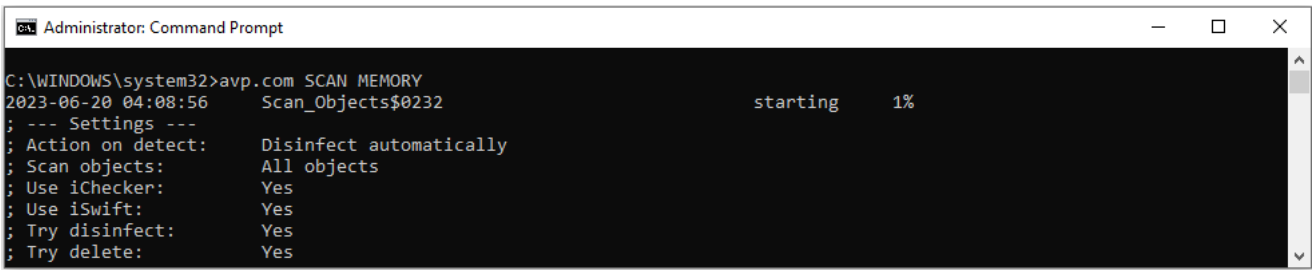
أوامر AVP

لإدارة برنامج Kaspersky Endpoint Security من سطر الأوامر:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.
2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.
3. لتنفيذ الامر، أدخل:

```
avp.com <command> [options]
```

وكنتيجة لذلك، سيقوم برنامج Kaspersky Endpoint Security بتنفيذ الأمر (اطلع على الشكل أدناه).



لإدارة التطبيق من سطر الأوامر

SCAN. فحص البرامج الضارة

قم بتشغيل المهمة فحص البرامج الضارة.

بناء جملة الأمر

```
avp.com SCAN [<نطاق الفحص>] [<الإجراء المطلوب اتخاذه عند اكتشاف تهديد>] [<أنواع
الملفات>] [<استثناءات الفحص>] [/R[A/]:<ملفات التقرير>] [<تقنيات الفحص>] [/C:<الملف
الذي يتضمن إعدادات الفحص>]
```

نطاق الفحص	
<files to scan>	قائمة مفصولة بمسافة من الملفات والمجلدات. يجب أن يتم وضع المسارات الطويلة بين علامات اقتباس. لا تحتاج المسارات القصيرة (تنسيق MS-DOS) إلى أن توضع بين علامات اقتباس. على سبيل المثال: • "C:\Program Files (x86)\Example Folder" – مسار طويل. • C:\PROGRA~2\EXAMPL~1 – مسار قصير.
/ALL	قم بتشغيل المهمة فحص البرامج الضارة. يقوم برنامج Kaspersky Endpoint Security بفحص الكائنات التالية: • ذاكرة Kernel؛ • الكائنات التي يتم تحميلها عند بدء تشغيل نظام التشغيل • قطاعات التمهيد؛ • النسخ الاحتياطي لنظام التشغيل • جميع المحركات الثابتة ومحركات الأقراص القابلة للإزالة
/MEMORY	فحص ذاكرة Kernel
/STARTUP	فحص الكائنات التي يتم تحميلها عند بدء تشغيل نظام التشغيل
/MAIL	فحص صندوق بريد Outlook
/REMDRIVES	فحص محركات الأقراص القابلة للإزالة.
/FIXDRIVES	فحص محركات الأقراص الصلبة.
/NETDRIVES	فحص محركات أقراص الشبكة.
/QUARANTINE	فحص الملفات في النسخ الاحتياطي لبرنامج Kaspersky Endpoint Security.
/@:<file list.lst>	فحص الملفات والمجلدات من القائمة. يجب أن يكون كل ملف في القائمة في صف جديد. يجب أن يتم وضع المسارات الطويلة بين علامات اقتباس. لا تحتاج المسارات القصيرة (تنسيق MS-DOS) إلى أن توضع بين علامات اقتباس. على سبيل المثال: • "C:\Program Files (x86)\Example Folder" – مسار طويل. • C:\PROGRA~2\EXAMPL~1 – مسار قصير.

الإجراء المطلوب اتخاذه عند اكتشاف تهديد	
/i0	**إخطار**. في حالة تحديد هذا الخيار، يضيف Kaspersky Endpoint Security المعلومات حول الملفات المصابة إلى قائمة التهديدات النشطة عند اكتشاف هذه الملفات.
/i1	**تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا تعذر التنظيف، يضيف Kaspersky Endpoint Security معلومات حول الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة.
/i2	**تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات.

	ويتم تحديد هذا الإجراء بصورة افتراضية.
/i3	تنظيف الملفات المصابة المكتشفة. في حالة فشل التنظيف، قم بحذف الملفات المصابة. وأيضًا قم بحذف الملفات المركبة (على سبيل، الأرشيفات) إذا تعذر تنظيف الملف المصاب أو حذفه.
/i4	حذف الملفات المصابة. وأيضًا قم بحذف الملفات المركبة (على سبيل، الأرشيفات) إذا تعذر حذف الملف المصاب.

أنواع الملفات	
/fe	**الملفات التي تم فحصها حسب الامتداد**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. ويتم تحديد تنسيق الملف عندئذٍ استنادًا إلى امتداد الملف.
/fi	**الملفات التي تم فحصها حسب التنسيق**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. قبل فحص أحد الملفات بحثًا عن التعليمات البرمجية الضارة، يتم تحليل العنوان الداخلي للملف لتحديد تنسيق الملف (على سبيل المثال، .txt أو .doc أو .exe). ويبحث الفحص أيضًا عن الملفات بملحقات ملف معينة.
/fa	**كل الملفات**. في حالة تمكين هذا الإعداد، يفحص التطبيق كل الملفات دون استثناء (كل التنسيقات والملحقات). وهذا هو الإعداد الافتراضي.

استثناءات الفحص	
-e:a	يتم استثناء أرشيفات RAR، وARJ، وZIP، وCAB، وLHA، وJAR، وICE من نطاق الفحص.
-e:b	يتم استثناء قواعد بيانات البريد، ورسائل البريد الإلكتروني الواردة والصادرة من نطاق الفحص.
-e:<file mask>	يتم استثناء الملفات التي تتطابق قناع الملف من نطاق الفحص. على سبيل المثال: • سيشمل القناع `exe.*` كافة المسارات إلي الملفات التي لها امتداد exe. • سيشمل `*example` القناع كل المسارات إلى الملفات المسماة EXAMPLE.
-e:<seconds>	يتم استثناء الملفات التي تستغرق وقت أكبر في عملية الفحص من المدة الزمنية المحددة (بالثواني) من نطاق الفحص.
-es:<megabytes>	يتم استثناء الملفات التي يزيد حجمها عن الحجم المحدد (بالميجابايت) من نطاق الفحص.

حفظ الأحداث في وضع ملف التقرير (لأوضاع الفحص وبرنامج التحديث والتراجع فقط)	
/R:<report file>	حفظ الأحداث الهامة فقط في ملف التقرير.
/RA:<report file>	حفظ جميع الأحداث في ملف التقرير.

تقنيات الفحص	
/iChecker=on|off	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).
/iSwift=on|off	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ

	لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.

إعدادات متقدمة	
/C:<الملف الذي يتضمن إعدادات الفحص>	الملف الذي يحتوي على إعدادات مهمة فحص البرامج الضارة. يجب أن يتم إنشاء الملف يدويًا وحفظه بتنسيق TXT. يمكن أن يحتوي الملف على المحتويات التالية: [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>].

مثال:

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE. تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق

قم بتشغيل المهمة تحديث.

بناء جملة الأمر

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

إعدادات مهمة التحديث	
local	ابدأ مهمة تحديث التي تم إنشاؤها تلقائيًا بعد تثبيت التطبيق. يمكنك تغيير إعدادات مهمة تحديث في واجهة التطبيق المحلية أو في وحدة التحكم على Kaspersky Security Center. إذا لم يتم تكوين هذا الإعداد، يبدأ Kaspersky Endpoint Security مهمة تحديث بالإعدادات الافتراضية أو بالإعدادات المحددة في الأمر. يمكنك تكوين إعدادات مهمة تحديث على النحو التالي: • يبدأ UPDATE مهمة تحديث بالإعدادات الافتراضية: مصدر التحديث هو خوادم تحديث Kaspersky والحساب هو النظام والإعدادات الافتراضية الأخرى. • يبدأ UPDATE local مهمة تحديث الذي تم إنشاؤه تلقائيًا بعد التثبيت (مهمة محددة مسبقًا). • يبدأ UPDATE <update settings> مهمة تحديث بالإعدادات المحددة يدويًا (انظر أدناه).

مصدر التحديث	
"<update	عنوان خادم HTTP أو FTP أو للمجلد المشترك الذي يحتوي على حزمة التحديث. يمكنك تحديد مصدر تحديث واحد فقط. إذا لم يتم تحديد مصدر التحديث، يستخدم Kaspersky Endpoint Security المصدر الافتراضي: خوادم تحديث Kaspersky.

source>"	

حفظ الأحداث في وضع ملف التقرير (لأوضاع الفحص وبرنامج التحديث والتراجع فقط)	
/R:<report file>	حفظ الأحداث الهامة فقط في ملف التقرير.
/RA:<report file>	حفظ جميع الأحداث في ملف التقرير.

إعدادات متقدمة	
/C:<file with update settings>	الملف الذي يحتوي على إعدادات مهمة تحديث. يجب أن يتم إنشاء الملف يدويًا وحفظه بتنسيق TXT. يمكن أن يحتوي الملف على المحتويات التالية: [<update source>"] [/R[A]:<report file>].

مثال:

```
avp.com UPDATE local
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK. استرجاع آخر تحديث

استرجاع آخر تحديث لقاعدة بيانات مكافحة الفيروسات. يتيح لك هذا الأمر إرجاع قواعد البيانات والوحدات النمطية للتطبيق إلى إصداراتها السابقة عند اللزوم، على سبيل المثال، عند احتواء إصدار قاعدة البيانات الجديد على توقيع غير صالح يتسبب في أن يقوم برنامج Kaspersky Endpoint Security بمنع تشغيل تطبيق آمن.

بناء جملة الأمر

```
[<avp.com ROLLBACK [/R[A]:<report file
```

حفظ الأحداث في وضع ملف التقرير (لأوضاع الفحص وبرنامج التحديث والتراجع فقط)	
/R:<report file>	حفظ الأحداث الهامة فقط في ملف التقرير.
/RA:<report file>	حفظ جميع الأحداث في ملف التقرير.

مثال:

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES. التتبع

تمكين / تعطيل عملية التتبع. يتم تخزين ملفات التتبع على الكمبيوتر طالما أن التطبيق قيد الاستخدام ويتم خذفها نهائيًا عند إزالة التطبيق. يتم حفظ ملفات التتبع، باستثناء تلك الخاصة بوكيل المصادقة، في المجلد %ProgramData%\Kaspersky Lab\KES.21.13\Traces. وبشكل افتراضي، يتم تعطيل عملية التتبع.

بناء جملة الأمر

```
[<avp.com TRACES on|off [<tracing level>] [<advanced settings
```

مستوى التتبع	
<tracing level>	مستوى تفاصيل عمليات التتبع. القيم المتاحة: • 100 (حرجة). فقط رسائل حول الأخطاء الفادحة. • 200 (عالي). رسائل حول جميع الأخطاء، بما في ذلك الأخطاء الفادحة. • 300 (تشخيصية). رسائل حول جميع الأخطاء، وكذلك التحذيرات. • 400 (هامة). رسائل حول جميع الأخطاء، والتحذيرات، وكذلك المعلومات الإضافية. • 500 (عادية). رسائل حول جميع الأخطاء، والتحذيرات، وكذلك المعلومات المفصلة حول تشغيل التطبيق في الوضع العادي (الافتراضي). • 600 (قليلة). جميع الرسائل.

إعدادات متقدمة	
all	تشغيل أمر باستخدام معلمات dbg، و file، و mem.
dbg	استخدم وظيفة OutputDebugString وقم بحفظ ملف التتبع. تقوم وظيفة OutputDebugString بإرسال سلسلة أحرف إلى مصحح أخطاء التطبيق لتعرض على الشاشة. للحصول على التفاصيل، قم بزيارة موقع ويب MSDN.
file	احفظ ملف تتبع واحد (لا يوجد حد للحجم).
rot	احفظ عمليات التتبع لعدد محدود من الملفات التي لها حجم محدود واستبدل الملفات الأقدم عند الوصول إلى الحد الأقصى للحجم.
mem	احفظ عمليات التتبع في ملفات التفريغ.

أمثلة:

```
avp.com TRACES on 500
avp.com TRACES on 500 dbg
avp.com TRACES off
avp.com TRACES on 500 dbg mem
avp.com TRACES off file
```

START. بدء ملف التعريف

بدء تشغيل ملف التعريف (على سبيل المثال، لتحديث قاعدة البيانات أو لتمكين مكون الحماية).

بـنـاء جملة الأمـر

```
[<avp.com START <profile> [/R[A]:<report file
```

ملف التعريف	
<profile>	اسم ملف التعريف. إن ملف التعريف عبارة عن مكون أو مهمة أو ميزة لبرنامج Kaspersky Endpoint Security. يمكنك استعراض قائمة ملفات التعريف المتاحة من خلال تنفيذ الأمر HELP START.

حفظ الأحداث في وضع ملف التقرير (لأوضاع الفحص وبرنامج التحديث والتراجع فقط)	
/R:<report file>	حفظ الأحداث الهامة فقط في ملف التقرير.
/RA:<report file>	حفظ جميع الأحداث في ملف التقرير.

مثال:

```
avp.com START Scan_Objects
```

STOP. إيقاف ملف التعريف

إيقاف ملف التعريف قيد التشغيل (على سبيل المثال، إيقاف عملية الفحص، أو إيقاف فحص محركات الأقراص القابلة للإزالة، أو تعطيل مكون الحماية).

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم أذونات **تعطيل مكونات الحماية** و**تعطيل مكونات التحكم**.

بـنـاء جملة الأمـر

```
<avp.com STOP <profile> /login=<user name> /password=<password
```

ملف التعريف	
<profile>	اسم ملف التعريف. إن ملف التعريف عبارة عن مكون أو مهمة أو ميزة لبرنامج Kaspersky Endpoint Security. يمكنك استعراض قائمة ملفات التعريف المتاحة من خلال تنفيذ الأمر HELP STOP.

المصادقة	
/login=<user name> /password=<password>	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

STATUS. حالة ملف التعريف

عرض حالة المعلومات حول ملفات تعريف التطبيق (على سبيل المثال، `قيد التشغيل` أو `مكتملة`). يمكنك عرض قائمة ملفات التعريف المتاحة من خلال تنفيذ الأمر `HELP STATUS`.

وكذلك يقوم برنامج Kaspersky Endpoint Security بعرض معلومات حول حالة ملفات تعريف الخدمة. قد تكون المعلومات حول ملفات تعريف الخدمة مطلوبة عند تواصلك مع خدمة الدعم الفني لـKaspersky.

بناء جملة الأمر

```
avp.com STATUS [<profile>]
```

إذا أدخلت الأمر بدون ملف تعريف، فسيعرض Kaspersky Endpoint Security حالة جميع ملفات تعريف التطبيق.

STATISTICS. إحصائيات عملية تشغيل ملف التعريف

عرض المعلومات الإحصائية حول ملف تعريف التطبيق (على سبيل المثال، مدة عملية الفحص أو عدد التهديدات التي تم اكتشافها.) يمكنك عرض قائمة ملفات التعريف المتاحة عن طريق تشغيل الأمر `HELP STATISTICS`.

بناء جملة الأمر

```
avp.com STATISTICS <profile>
```

RESTORE. استعادة الملفات من النسخ الاحتياطي

يمكنك استعادة الملف من النسخ الاحتياطي إلى مجلده الأصلي. وإذا كان هناك ملف بالاسم نفسه موجود بالفعل في المسار المحدد، فسيطلب التطبيق تأكيدًا لاستبدال الملف. يتم نسخ الملف الذي تمت استعادته مع الاحتفاظ باسمه الاصلي.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **الاستعادة من نسخة احتياطية**.

يخزن النسخ الاحتياطي نسخًا احتياطية من الملفات التي تم حذفها أو تعديلها أثناء التنظيف. ويتم تعريف النسخة الاحتياطية بأنها نسخة ملف يتم إنشاؤها قبل تنظيف الملف أو حذفه. ويتم تخزين ملفات النسخ الاحتياطي بتنسيق خاص ولا تُمثل تهديدًا.

يتم تخزين النسخ الاحتياطية للملفات في المجلد `C:\ProgramData\Kaspersky Lab\KES.21.13\QB`.

يتم منح المستخدمين في مجموعة المسؤولين الإذن الكامل للوصول إلى هذا المجلد. ويتم منح حقوق الوصول المحدود إلى هذا المجلد للمستخدم الذي تم استخدام حسابه لتثبيت Kaspersky Endpoint Security.

لا يوفر Kaspersky Endpoint Security القدرة على تكوين أذونات وصول المستخدم إلى النسخ الاحتياطية من الملفات.

بناء جملة الأمر

```
<avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password
```

إعدادات متقدمة	
/REPLACE	استبدال الملف الحالي.
<file name>	اسم الملف الذي ستتم استعادته.

المصادقة	
/login=<user name> /password=<password>	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

EXPORT. تصدير إعدادات التطبيق

تصدير إعدادات Kaspersky Endpoint Security في ملف. سيتم وضع الملف في المجلد C:\Windows\SysWOW64.

بناء جملة الأمر

```
<avp.com EXPORT <profile> <file name
```

ملف التعريف	
<profile>	اسم ملف التعريف. إن ملف التعريف عبارة عن مكون أو مهمة أو ميزة لبرنامج Kaspersky Endpoint Security. يمكنك استعراض قائمة ملفات التعريف المتاحة من خلال تنفيذ الأمر HELP EXPORT.

ملف للتصدير	
<file name>	اسم الملف الذي سيتم تصدير إعدادات التطبيق إليه. يمكنك تصدير إعدادات برنامج Kaspersky Endpoint Security إلى ملف تكوين DAT أو CFG أو ملف النص TXT أو إلى مستند XML.

أمثلة:

```
avp.com EXPORT ids ids_config.dat
avp.com EXPORT fm fm_config.txt
```

IMPORT. استيراد إعدادات التطبيق

يستورد الإعدادات لبرنامج Kaspersky Endpoint Security من الملف الذي تم إنشاؤه باستخدام الأمر `EXPORT`.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **تكوين إعدادات التطبيق**.

بناء جملة الأمر

```
<avp.com IMPORT <file name> /login=<user name> /password=<password
```

ملف للاستيراد	
`<file name>`	اسم الملف الذي سيتم استيراد إعدادات التطبيق منه. يمكنك استيراد إعدادات برنامج Kaspersky Endpoint Security من ملف تكوين DAT أو DAT أو من ملف النص TXT أو من مستند XML.

المصادقة	
`/login=<user name> /password=<password>`	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال:

```
avp.com IMPORT config.dat /login=KLAdmin /password=!Password1
```

ADDKEY. تطبيق ملف المفتاح

تطبيق ملف المفتاح لتفعيل Kaspersky Endpoint Security. إذا كان التطبيق مفعلًا بالفعل، فستتم إضافة المفتاح كمفتاح احتياطي.

بناء جملة الأمر

```
[<avp.com ADDKEY <file name> [/login=<user name> /password=<password
```

ملف المفتاح	
`<file name>`	اسم ملف المفتاح.

المصادقة	
`/login=<user name> /password=`	بيانات اعتماد حساب المستخدم. يجب إدخال بيانات الاعتماد هذه فقط إذا تم تمكين الحماية

<password>	بكلمة المرور.

مثال:

```
avp.com ADDKEY file.key
```

LICENSE. الترخيص

نفذ العمليات باستخدام مفاتيح ترخيص Kaspersky Endpoint Security أو باستخدام مفاتيح EDR Optimum أو EDR Expert (الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response).

لتنفيذ هذا الأمر وإزالة مفتاح الترخيص، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **إزالة المفتاح**.

بناء جملة الأمر

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

العملية	
/ADD <file name>	تطبيق ملف المفتاح لتفعيل Kaspersky Endpoint Security. إذا كان التطبيق مفعلًا بالفعل، فستتم إضافة المفتاح كمفتاح احتياطي.
/ADD <activation code>	تفعيل Kaspersky Endpoint Security باستخدام رمز التفعيل. إذا كان التطبيق مفعلًا بالفعل، فستتم إضافة المفتاح كمفتاح احتياطي.
REFRESH/	تحديث حالة ترخيص Kaspersky Endpoint Security. ونتيجة لذلك، يتلقى التطبيق معلومات محدثة عن حالة الترخيص من خوادم تنشيط Kaspersky.
REFRESH EDR/	تحديث حالة ترخيص الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response. ونتيجة لذلك، يتلقى التطبيق معلومات محدثة عن حالة الترخيص من خوادم تنشيط Kaspersky.
/DEL /login=<user name> /password=<password>	إزالة مفتاح الترخيص الخاص بالتطبيق. وكذلك ستتم إزالة المفتاح الاحتياطي.
DEL EDR /login=<user/ name> /password= <password>	إزالة مفتاح الترخيص من الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response. وكذلك ستتم إزالة المفتاح الاحتياطي.

المصادقة	
/login=<user name> /password=<password>	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال:

```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL EDR /login=KLAdmin /password=!Password1
```

التجديد. شراء الترخيص

افتح موقع ويب Kaspersky للقيام بشراء الترخيص أو لتجديد الترخيص الخاص بك.

PBATESTRESET. إعادة ضبط نتائج التحقق من القرص قبل تشفير القرص

إعادة ضبط نتائج التحقق من التوافق لتشفير القرص بالكامل (FDE)، بما في ذلك تقنية تشفير القرص من Kaspersky وكذلك تقنية تشفير محرك الأقراص من BitLocker.

قبل تشغيل تشفير القرص بالكامل، يقوم التطبيق بإجراء عدد من عمليات التحقق للتأكد من إمكانية تشفير جهاز الكمبيوتر. إذا كان جهاز الكمبيوتر لا يدعم تشفير القرص بالكامل، يقوم برنامج Kaspersky Endpoint Security بتسجيل المعلومات حول عدم التوافق. في المرة القادمة التي تحاول فيها القيام بالتشفير، لا يقوم التطبيق بإجراء عملية التحقق هذه ويحذرك من استحالة إجراء عملية التشفير. في حالة تغيير تكوين جهاز الكمبيوتر، يجب القيام بإعادة تعيين نتائج عملية التحقق من التوافق التي تم تسجيلها مسبقًا بواسطة التطبيق، لإعادة التحقق من توافق محرك القرص الصلب الخاص بالنظام مع تقنيات تشفير القرص من Kaspersky أو تشفير محرك الأقراص من BitLocker.

EXIT. إنهاء التطبيق

الخروج من Kaspersky Endpoint Security. لن يتم تحميل التطبيق من ذاكرة الوصول العشوائي لجهاز الكمبيوتر.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **إنهاء التطبيق**.

بناء جملة الأمر

```
<avp.com EXIT /login=<user name> /password=<password
```

EXITPOLICY. تعطيل السياسة

تعطيل سياسة Kaspersky Security Center على جهاز الكمبيوتر. تتوافر جميع إعدادات برنامج Kaspersky Endpoint Security للتكوين، بما في ذلك الإعدادات التي تحتوي على قفل مغلق في السياسة. (🔒).

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **تعطيل سياسة مركز Kaspersky Security Center**.

بناء جملة الأمر

```
<avp.com EXITPOLICY /login=<user name> /password=<password
```

STARTPOLICY. تمكين السياسة

تمكين سياسة Kaspersky Security Center على جهاز الكمبيوتر. سيتم تكوين سياسة إعدادات التطبيق وفقًا للسياسة.

DISABLE. تعطيل الحماية

تعطيل الحماية من تهديدات الملفات على جهاز كمبيوتر باستخدام ترخيص Kaspersky Endpoint Security منتهي. ومن المستحيل تشغيل هذا الأمر على جهاز كمبيوتر يحتوي على التطبيق الذي لم يتم تفعيله أو لديه ترخيص صالح.

SPYWARE. الكشف عن برامج التجسس

تمكين / تعطيل الكشف عن برامج التجسس. افتراضيًا، يتم تمكين الكشف عن برامج التجسس.

بناء جملة الأمر

```
avp.com SPYWARE on|off
```

KSN. التبديل بين KSN / KPSN

تحديد حل Kaspersky لتحديد سمعة الملفات أو مواقع الويب. يدعم Kaspersky Endpoint Security حلول البنية التحتية التالية للعمل مع قواعد بيانات السمعة من Kaspersky:

- Kaspersky Security Network هي المنتج الذي يتم استخدامه من قِبل أغلب تطبيقات Kaspersky. يتسلم المشتركين في شبكة KSN معلومات من Kaspersky ويرسلوا معلومات إلى Kaspersky حول الكائنات التي تم اكتشافها على جهاز كمبيوتر المستخدم ليتم تحليلها بشكل إضافي من قِبل محللي Kaspersky وليتم إدراجها في قواعد بيانات الإحصائية والخاصة بالسمعة.
- Kaspersky Private Security Network عبارة عن حل يتيح لمستخدمي أجهزة الكمبيوتر التي تستضيف Kaspersky Endpoint Security أو غيره من تطبيقات Kaspersky الحصول على حق الوصول إلى قواعد بيانات السمعة من Kaspersky، وإلى البيانات الإحصائية الأخرى دون إرسال بيانات إلى Kaspersky من أجهزة الكمبيوتر الخاصة بهم. وصُممت شبكة KPSN لعملاء الشركات الذين لا يستطيعون المشاركة في شبكة Kaspersky Security Network لأي من الأسباب التالية:
  - محطات العمل المحلية غير متصلة بالإنترنت.
  - يُعتبر نقل أي بيانات خارج البلد أو خارج الشبكة المحلية (LAN) الخاصة بالشركة ممنوعًا بواسطة القانون أو مُقيدًا بواسطة سياسات الأمن الخاصة بالشركة.

بناء جملة الأمر

```
<avp.com KSN /global | /private <file name
```

ملف تكوين Kaspersky Security Network		
`<file name>`	اسم ملف التكوين الذي يحتوي على إعدادات Kaspersky Private Security Network. يكون امتداد هذا الملف PKCS7 أو PEM.	

مثال:

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

أوامر KESCLI

تتيح لك أوامر KESCLI تلقي معلومات حول حالة حماية الكمبيوتر باستخدام مكون OPSWAT، والسماح لك بتنفيذ المهام القياسية مثل فحص البرامج الضارة وتحديث.

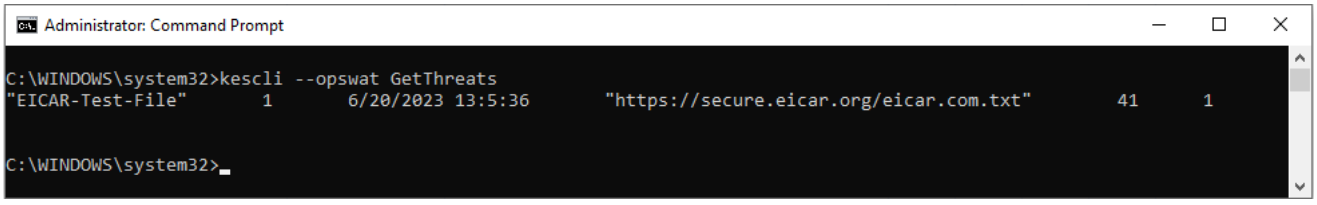
يمكنك عرض قائمة أوامر KESCLI باستخدام أمر `--help` أو باستخدام الأمر المختصر `-h`.

لإدارة برنامج Kaspersky Endpoint Security من سطر الأوامر:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.
2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.
3. لتنفيذ الامر، أدخل:

```
kescli <command> [options]
```

وكنتيجة لذلك، سيقوم برنامج Kaspersky Endpoint Security بتنفيذ الأمر (اطلع على الشكل أدناه).



لإدارة التطبيق من سطر الأوامر

فحص. فحص البرامج الضارة

قم بتشغيل المهمة فحص البرامج الضارة (فحص كامل).

لتشغيل المهمة، يجب على المسؤول السماح باستخدام المهام المحلية في السياسة.

بناء جملة الأمر

```
kescli --opswat Scan "<نطاق الفحص>" <الإجراء المطلوب اتخاذه عند اكتشاف تهديد>
```

يمكنك التحقق من اكتمال حالة مهمة فحص البرامج الضارة باستخدام الأمر `GetScanState` وعرض التاريخ والوقت عند اكتمال الفحص الأخير باستخدام الأمر `GetLastScanTime`.

نطاق الفحص	
<files to scan>	قائمة مفصولة بمسافة من الملفات والمجلدات. على سبيل المثال، "C:\Program Files (x86)\Example" ;-"Folder".

الإجراء المطلوب اتخاذه عند اكتشاف تهديد	
0	**إخطار**. في حالة تحديد هذا الخيار، يضيف Kaspersky Endpoint Security المعلومات حول الملفات المصابة إلى قائمة التهديدات النشطة عند اكتشاف هذه الملفات.
1	**تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات. ويتم تحديد هذا الإجراء بصورة افتراضية.

مثال:

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState. حالة اكتمال الفحص

تلقي معلومات عن حالة اكتمال مهمة فحص البرامج الضارة (فحص كامل):

- 1 – الفحص قيد التقدم.
- 0 – الفحص لا يعمل.

بناء جملة الأمر

```
kescli --opswat GetScanState
```

GetLastScanTime. تحديد وقت إكمال الفحص

تلقي معلومات عن تاريخ ووقت اكتمال مهمة فحص البرامج الضارة (فحص كامل) الأخيرة.

بناء جملة الأمر

```
kescli --opswat GetLastScanTime
```

GetThreats. الحصول على بيانات عن التهديدات المكتشفة

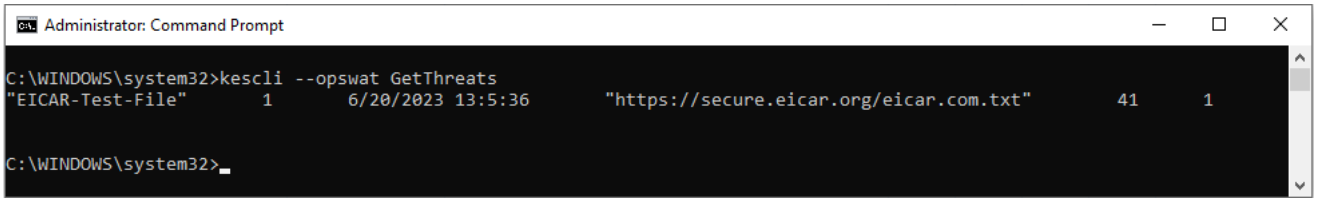
تلقي قائمة بالتهديدات المكتشفة (تقرير التهديدات). يحتوي هذا التقرير على معلومات عن التهديدات ونشاط الفيروسات خلال 30 يومًا الماضية قبل إنشاء التقرير.

بناء جملة الأمر

```
kescli --opswat GetThreats
```

عند تنفيذ هذا الأمر، سوف يرسل Kaspersky Endpoint Security استجابة بالتنسيق التالي:

```
name of detected object> <type of object> <detection date and time> <path to file>>
<action on threat detection> <threat danger level>
```



لإدارة التطبيق من سطر الأوامر

نوع الكائن	
0	غير معروف (Unknown).
1	الفيروسات (Virware).
2	برامج فيروس حصان طروادة (Trojware).
3	البرامج الضارة (Malware).
4	برامج الإعلانات (Adware).
5	برامج الاتصال التلقائي (Pornware).
6	التطبيقات التي يستطيع مجرم إلكتروني استخدامها للإضرار بجهاز الكمبيوتر الخاص بالمستخدم أو البيانات (Riskware).
7	كائنات مضغوطة قد تُستخدم طريقة ضغطها لحماية التعليمات البرمجية الضارة (Packed).
20	كائنات غير معروفة (Xfiles).
21	تطبيقات معروفة (Software).
22	ملفات مخفية (Hidden).
23	تطبيقات تتطلب الاهتمام (Pupware).
24	سلوك شاذ (Anomaly).
30	غير محدد (Undetect).
40	شعارات إعلانية (Banner).
50	هجوم شبكة الاتصال (Attack).
51	الوصول إلى التسجيل (Registry).
52	نشاط مشكوك فيه (Suspicion).

60	ثغرات أمنية (Vulnerability).
70	Phishing.
80	مرفق بريد إلكتروني غير مرغوب فيه (Attachment).
90	برنامج ضار تم اكتشافه بواسطة Kaspersky Security Network (Urgent).
100	رابط غير معروف (Suspic URL).
110	برنامج ضار آخر (Behavioral).

الإجراء المطلوب اتخاذه عند اكتشاف تهديد	
0	غير معروف (unknown).
1	تم إصلاح التهديد (ok).
2	أصيب الكائن ولم يتم تنظيفه (infected).
5	الكائن موجود في الأرشيف ولم يتم تنظيفه (archive).
9	تم تنظيف الكائن (disinfected).
10	لم يتم تنظيف الكائن (not disinfected).
11	تم حذف الكائن (deleted).
13	تم إنشاء نسخة احتياطية من الكائن (backupped).
15	تم نقل الكائن إلى النسخ الاحتياطي (quarantined).
23	تم حذف الكائن عند إعادة تشغيل الكمبيوتر (delete on reboot).
25	تم تنظيف الكائن عند إعادة تشغيل الكمبيوتر (disinfect on reboot).
29	تم نقل الكائن إلى النسخ الاحتياطي بواسطة مستخدم (added by user).
30	تمت إضافة الكائن إلى الاستثناءات (added to exclude).
31	تم نقل الكائن إلى النسخ الاحتياطي عند إعادة تشغيل الكمبيوتر (quarantine on reboot).
36	حالة إيجابية زائفة (false alarm).
38	تم إنهاء العملية (terminated).
40	لم يتم اكتشاف الكائن (not found).
41	لا يمكن حل التهديد (untreatable).
42	تم استعادة الكائن (rolled back).
43	تم إنشاء الكائن نتيجة لنشاط تهديد (produced by threat).
44	تمت استعادة الكائن عند إعادة تشغيل الكمبيوتر (roll back on reboot).
0xffffffff	لم تتم معالجة الكائن (discarded).

مستوى خطر التهديد	
0	غير معروف
1	مرتفع

2	فحص متوسط
4	منخفض
8	معلومات (أقل من منخفض)

UpdateDefinitions. تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق

قم بتشغيل المهمة تحديث. يستخدم Kaspersky Endpoint Security المصدر الافتراضي: خوادم تحديث Kaspersky.

لتشغيل المهمة، يجب على المسؤول السماح باستخدام المهام المحلية في السياسة.

بناء جملة الأمر

```
kescli --opswat UpdateDefinitions
```

يمكنك عرض تاريخ ووقت إصدار قواعد بيانات مكافحة الفيروسات الحالية باستخدام الأمر `GetDefinitionsetState`.

GetDefinitionState. تحديد وقت إكمال التحديث

تلقي معلومات عن تاريخ ووقت إصدار قواعد بيانات مكافحة الفيروسات المستخدمة.

بناء جملة الأمر

```
kescli --opswat GetDefinitionState
```

EnableRTP. تمكين الحماية

قم بتمكين مكونات حماية Kaspersky Endpoint Security على الكمبيوتر: الحماية من تهديدات الملفات، والحماية من تهديدات الويب، والحماية من تهديدات البريد، والحماية من تهديدات الشبكة، ومنع اختراق المضيف.

لتمكين مكونات الحماية، يجب على المسؤول التأكد من إمكانية تعديل إعدادات السياسة ذات الصلة (السمات مفتوحة).

بناء جملة الأمر

```
kescli --opswat EnableRTP
```

نتيجة لذلك، يتم تمكين مكونات الحماية حتى إذا كنت قد حظرت تعديل إعدادات التطبيق باستخدام الحماية بكلمة مرور.

يمكنك التحقق من حالة تشغيل الحماية من تهديدات الملفات باستخدام الأمر `GetRealTimeProtectionState`.

GetRealTimeProtectionState. حالة الحماية من تهديدات الملفات

تلقي معلومات عن حالة تشغيل مكون الحماية من تهديدات الملفات:

- `1` – تم تمكين المكون.
- `0` – تم تعطيل المكون.

بناء جملة الأمر

```
kescli --opswat GetRealTimeProtectionState
```

الإصدار. تحديد إصدار التطبيق

حدد إصدار Kaspersky Endpoint Security for Windows.

بناء جملة الأمر

```
kescli --Version
```

يمكنك أيضًا استخدام الأمر المختصر `-v`.

أوامر إدارة Detection and Response

يمكنك استخدام سطر الأوامر لإدارة الوظائف المضمنة لحلول Detection and Response (على سبيل المثال، Kaspersky Sandbox أو Kaspersky Endpoint Detection and Response Optimum). ويمكنك إدارة حلول Managed Detection and Response إذا كانت الإدارة باستخدام وحدة تحكم Kaspersky Security Center غير ممكنة. يمكنك استعراض قائمة الأوامر لإدارة التطبيق من خلال تنفيذ الأمر `HELP`. للقراءة عن بناء الأمر لأمر محدد، قم بإدخال `HELP <command>`.

لإدارة الميزات المضمنة في حلول Detection and Response باستخدام سطر الأوامر:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.
2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.
3. لتنفيذ الامر، أدخل:

```
avp.com <command> [options]
```

كنتيجة لذلك، سوف ينفذ برنامج Kaspersky Endpoint Security الأمر.

SANDBOX. إدارة Kaspersky Sandbox

الأوامر لإدارة مكون Kaspersky Sandbox:

- تمكين أو تعطيل مكون Kaspersky Sandbox.

يتيح مكون Kaspersky Sandbox إمكانية التشغيل التفاعلي مع حل Kaspersky Sandbox.

- تكوين مكون Kaspersky Sandbox:

  - قم بتوصيل الكمبيوتر بخوادم Kaspersky Sandbox.

    تستخدم الخوادم الصور الافتراضية المنشورة لأنظمة تشغيل Microsoft Windows لتشغيل الكائنات التي تحتاج إلى فحصها. ويمكنك إدخال عنوان IP (IPv4 أو IPv6) أو اسم مجال مؤهل بالكامل. وللحصول على التفاصيل حول نشر الصور الافتراضية وتكوين خوادم Kaspersky Sandbox، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

  - قم بتكوين مهلة الاتصال لخادم Kaspersky Sandbox.

    مهلة تلقي رد على طلب فحص كائن من خادم Kaspersky Sandbox. بعد انقضاء المهلة، يعيد Kaspersky Sandbox توجيه الطلب إلى الخادم التالي. تعتمد قيمة المهلة على سرعة الاتصال واستقراره. القيمة الافتراضية هي 5 ثانية.

  - قم بتكوين اتصال موثوق بين الكمبيوتر وخوادم Kaspersky Sandbox.

    لتكوين اتصال موثوق به مع خوادم Kaspersky Sandbox، يجب عليك إعداد شهادة TLS. وبعد ذلك، يجب إضافة الشهادة إلى خوادم Kaspersky Sandbox وسياسة Kaspersky Endpoint Security. وللحصول على تفاصيل عن إعداد الشهادة وإضافة الشهادة إلى الخوادم، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

  - عرض الإعدادات الحالية للمكون.

بناء جملة الأمر

```
[<avp.com stop sandbox [/login=<user name> /password=<password
                                                    avp.com start sandbox
   avp.com sandbox /set [--tls=yes|no] [--servers=<server address>:<port>] [--timeout=
<Kaspersky Sandbox server connection timeout (ms)>] [--pinned-certificate=<path to the
                                [<TLS certificate>][/login=<user name> /password=<password
                                                    avp.com sandbox /show
```

العملية	
`stop`	تعطيل مكون Kaspersky Sandbox.
`start`	تمكين مكون Kaspersky Sandbox.
`set`	تكوين مكون Kaspersky Sandbox. يمكنك تعديل البيانات التالية: • استخدام اتصال موثوق به (`--tls`)؛ • إضافة شهادة TLS (`--pinned-certificate`)؛ • ضبط مهلة اتصال خادم Kaspersky Sandbox (`--timeout`)؛ • إضافة خوادم Kaspersky Sandbox (`--servers`).

`show`	عرض الإعدادات الحالية للمكون. تحصل على الرد التالي:
	`sandbox.timeout=<Kaspersky Sandbox server connection timeout (ms)>`
	`sandbox.tls=<trusted connection status>`
	`sandbox.servers=<list of Kaspersky Sandbox servers>`

المصادقة	
`/login=<user name> /password=<password>`	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال:

```
avp.com start sandbox
"avp.com sandbox /set --tls=yes --pinned-certificate="C:\Users\Admin\certificate.pem
avp.com sandbox /set --servers=10.10.111.0:147
```

المنع. إدارة منع التنفيذ

تعطيل منع التنفيذ أو إظهار إعدادات المكون الحالي، بما في ذلك قائمة قواعد منع التنفيذ.

بناء جملة الأمر

```
avp.com prevention disable
avp.com prevention /show
```

بعد تنفيذ أمر `prevention /show`، ستتلقى الرد التالي:

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

قيم إرجاع الأمر:

- `-1` يعني أن الأمر غير مدعوم من إصدار التطبيق المُثبت على الكمبيوتر.
- `0` يعني أن الأمر تم تنفيذه بنجاح.
- `1` يعني أنه لم يتم تمرير وسيطة إلزامية إلى الأمر.
- `2` يعني حدوث خطأ عام.
- `4` يعني أنه كان هناك خطأ في بناء الجملة.
- `9` – عملية خاطئة (على سبيل المثال، محاولة لتعطيل المكون عندما يكون معطلاً بالفعل).

العزل. إدارة عزل شبكة الاتصال

أوقف تشغيل عزل شبكة الاتصال للكمبيوتر أو عرض الإعدادات الحالية للمكون. وتتضمن إعدادات المكونات أيضًا قائمة باتصالات الشبكة المضافة إلى الاستثناءات.

بناء جملة الأمر:

```
<avp.com isolation /OFF /login=<user name> /password=<password
avp.com isolation /STAT
```

نتيجة لتشغيل الأمر `stat`، تتلقى الرد التالي: `Network isolation on|off`.

RESTORE. استعادة الملفات من العزل

يمكنك استعادة الملف من العزل إلى مجلده الأصلي. العزل هو مخزن محلي خاص على الكمبيوتر. ويستطيع المستخدم عزل الملفات التي يعتبرها المستخدم خطرة على جهاز الكمبيوتر. ويتم تخزين الملفات المعزولة في حالة مشفرة ولا تهدد أمن الجهاز. ولا يستخدم Kaspersky Endpoint Security العزل إلا عند العمل مع حلول Detection and Response: EDR Optimum وEDR Expert وKATA (EDR) وKaspersky Sandbox. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل حول إدارة العزل كجزء من الحلول، يرجى الرجوع إلى تعليمات Kaspersky Sandbox وتعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert وتعليمات Kaspersky Anti Targeted Attack Platform.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **الاستعادة من نسخة احتياطية**.

يتم عزل الكائن تحت حساب النظام (SYSTEM).

تتضمن استعادة الملفات من العزل الاعتبارات الخاصة التالية:

- في حالة حذف المجلد الوجهة أو لم يكن لدى المستخدم حقوق الوصول إلى هذا المجلد، يضع التطبيق الملف في المجلد `%DataRoot%\QB\Restored`. ويجب عليك بعد ذلك نقل الملف يدويًا إلى المجلد الوجهة.
- يعامل التطبيق اسم الملف الذي تتم استعادته على أنه حساس لحالة الأحرف. وإذا لم تلاحظ الحالة عند إدخال اسم الملف، فلن يستعيد التطبيق الملف.
- إذا كان المجلد الوجهة يحتوي بالفعل على ملف بالاسم نفسه، فسوف يلغي التطبيق استعادة الملف.
- إذا كنت تستخدم حل EDR (KATA)، فإن التطبيق يحفظ نسخة من الملف في العزل بعد استعادة الملف. ويمكنك مسح العزل يدويًا. بالنسبة لحلي EDR Optimum وEDR Expert، يحذف التطبيق الملف بعد الاستعادة.

بناء جملة الأمر

```
<avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password
```

إعدادات متقدمة	
`/REPLACE`	استبدال الملف الحالي.
`<file name>`	اسم الملف الذي ستتم استعادته.

المصادقة	
`/login=<user name> /password=<password>`	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال:

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=!Password1
```

قيم إرجاع الأمر:

- -1 يعني أن الأمر غير مدعوم من إصدار التطبيق المُثبت على الكمبيوتر.
- 0 يعني أن الأمر تم تنفيذه بنجاح.
- 1 يعني أنه لم يتم تمرير وسيطة إلزامية إلى الأمر.
- 2 يعني حدوث خطأ عام.
- 4 يعني أنه كان هناك خطأ في بناء الجملة.

IOCSCAN. فحص مؤشرات الاختراق (IOC)

تشغيل مهمة الفحص للبحث عن مؤشرات الاختراق (IOC). مؤشر الاختراق (IOC) عبارة عن مجموعة من البيانات حول كائن أو نشاط يشير إلى وصول غير مصرح به إلى الكمبيوتر (اختراق البيانات). على سبيل المثال، من الممكن أن تشكل العديد من المحاولات الفاشلة لتسجيل الدخول إلى النظام مؤشرًا على الاختراق. تتيح مهمة فحص IOC العثور على مؤشرات الاختراق على الكمبيوتر واتخاذ إجراءات الاستجابة للتهديدات.

بناء جملة الأمر

```
avp.com IOCSCAN <المسار الكامل إلى ملف مؤشر الاختراق>|/path=<المسار إلى مجلد ملفات مؤشر الاختراق> [/hint/] [/process=on|off=<المسار الكامل إلى الملف القابل للتنفيذ لعملية|مسار الملف الكامل>] [/arpentry=on|off]/] [/dnsentry=on|off] [/registry=on|off] [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/channels=<قائمة القنوات>] [/datetime=<event publication date>] [/eventlog=on|off] [/files=on|off] [/drives=<all|system|critical|custom>] [/excludes=<list of exclusions>=<قائمة المجلدات المراد فحصها>][/scope
```

ملفات IOC	
<full path to the IOC file>	المسار الكامل إلى ملف IOC الذي تريد استخدامه للفحص. يمكنك تحديد ملفات IOC متعددة مفصولة بمسافات. يجب إدخال المسار الكامل لملف IOC بدون وسيطة /path. على سبيل المثال، C:\Users\Admin\Desktop\IOC\file1.ioc
/path=<path to the folder with IOC files>	المسار إلى المجلد الذي يحتوي على ملفات IOC التي تريد استخدامها للفحص. ملفات IOC هي ملفات تحتوي على مجموعات المؤشرات التي يحاول التطبيق مطابقتها لإحصاء الاكتشاف. ويجب أن تتوافق ملفات IOC مع معيار OpenIOC. على سبيل المثال، C:\Users\Admin\Desktop\IOC

نوع البيانات لفحص IOC	
/process=on|off	تحليل بيانات العملية عند إجراء فحص IOC (شرط ProcessItem). إذا كانت قيمة الوسيط off، فلا يحلل Kaspersky Endpoint Security العمليات التي تعمل على الكمبيوتر عند إجراء الفحص. وإذا كان ملف IOC يحتوي على شروط IOC لمستند ProcessItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير مطابقة).

	إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security بيانات العملية فقط إذا كان مستند IOC ProcessItem موصوفًا في ملف IOC المتاح للفحص.
`/hint=<full path to the executable file of the process|full path to the file>`	تحليل بيانات الملف عند إجراء فحص IOC (شروط ProcessItem وFileItem). يمكنك تحديد ملف بإحدى الطرق التالية: • `<full path to the executable file of the process>` – ProcessItem term؛ • `<full path to the file>` – FileItem term.
`/registry=on|off`	تحليل بيانات تسجيل Windows عند إجراء فحص IOC (شرط RegistryItem). إذا كانت قيمة الوسيطة `off`، لا يفحص Kaspersky Endpoint Security تسجيل Windows. إذا كان ملف IOC يحتوي على شروط مستند IOC RegistryItem، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security تسجيل Windows فقط إذا كان مستند IOC RegistryItem موصوفًا في ملف IOC المتوفر المقدم للفحص. لنوع البيانات RegistryItem، يفحص Kaspersky Endpoint Security مجموعة من مفاتيح التسجيل.
`/dnsentry=on|off`	تحليل البيانات حول السجلات في ذاكرة التخزين المؤقت لـ DNS المحلي عند إجراء فحص IOC (شرط DnsEntryItem). إذا كانت قيمة الوسيطة `off`، لا يفحص Kaspersky Endpoint Security ذاكرة التخزين المؤقت لـ DNS المحلي. وإذا كان ملف IOC يحتوي على شروط مستند DnsEntryItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security ذاكرة التخزين المؤقت لـ DNS المحلي فقط إذا كان مستند IOC DnsEntryItem موصوفًا في ملف IOC المقدم للفحص.
`/arpentry=on|off`	تحليل البيانات حول السجلات في جدول ARP عند إجراء فحص IOC (شرط ArpEntryItem). إذا كانت قيمة الوسيطة `off`، لا يفحص Kaspersky Endpoint Security جدول ARP. إذا كان ملف IOC يحتوي على شروط مستند IOC ArpEntryItem، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security جدول ARP فقط إذا كان مستند IOC ArpEntryItem موصوفًا في ملف IOC المقدم للفحص.
`/ports=on|off`	تحليل البيانات حول المنافذ المفتوحة للاستماع عند إجراء فحص IOC (شرط PortItem). إذا كانت قيمة الوسيطة `off`، لا يفحص Kaspersky Endpoint Security جدول الاتصالات النشطة على الجهاز. إذا كان ملف IOC يحتوي على شروط مستند PortItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security جدول الاتصالات النشطة فقط إذا كان مستند IOC PortItem موصوفًا في ملف IOC المقدم للفحص.
`/services=on|off`	تحليل البيانات حول الخدمات المثبتة على الجهاز عند إجراء فحص IOC (شرط ServiceItem). إذا كانت قيمة الوسيطة `off`، لا يفحص Kaspersky Endpoint Security البيانات حول الخدمات المثبتة على الجهاز. إذا كان ملف IOC يحتوي على شروط مستند ServiceItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة).

	إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security بيانات الخدمة فقط إذا كان مستند ServiceItem IOC موصوفًا في ملف IOC المقدم للفحص.
`/system=on|off`	تحليل بيانات البيئة عند إجراء فحص IOC (شرط SystemInfoItem). إذا كانت قيمة الوسيط `off`، لا يحلل Kaspersky Endpoint Security بيانات البيئة. وإذا كان ملف IOC يحتوي على شروط مستند SystemInfoItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security بيانات البيئة فقط إذا كان مستند SystemInfoItem IOC موصوفًا في ملف IOC المقدم للفحص.
`/users=on|off`	تحليل البيانات حول المستخدمين عند إجراء فحص IOC (شرط UserItem). إذا كانت قيمة الوسيط `off`، لا يحلل Kaspersky Endpoint Security البيانات المتعلقة بالمستخدمين الذين تم إنشاؤهم في النظام. إذا كان ملف IOC يحتوي على شروط مستند UserItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security البيانات المتعلقة بالمستخدمين الذين تم إنشاؤهم في النظام فقط إذا كان مستند UserItem IOC موصوفًا في ملف IOC المقدم للفحص.
`/volumes=on|off`	تحليل البيانات حول وحدات التخزين عند إجراء فحص IOC (شرط VolumeItem). إذا كانت قيمة الوسيط `off`، لا يفحص Kaspersky Endpoint Security البيانات حول وحدات التخزين على الجهاز. إذا كان ملف IOC يحتوي على شروط مستند VolumeItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيط، يحلل Kaspersky Endpoint Security بيانات وحدات التخزين فقط إذا كان مستند VolumeItem IOC موصوفًا في ملف IOC المقدم للفحص.
`/eventlog=on|off`	تحليل البيانات حول السجلات في سجل أحداث Windows عند إجراء فحص IOC (شرط EventLogItem). إذا كانت قيمة الوسيطة `off`، لا يفحص Kaspersky Endpoint Security السجلات الموجودة في سجل أحداث Windows. إذا احتوى ملف IOC على شروط مستند EventLogItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security سجل أحداث Windows إذا كان مستند EventLogItem IOC موصوفًا في ملف IOC المقدم للفحص.
`/datetime=<event publication date>`	ضع في الاعتبار تاريخ نشر الحدث في سجل أحداث Windows عند تحديد نطاق فحص IOC لمستند IOC المقابل. عند إجراء فحص IOC، يفحص Kaspersky Endpoint Security إدخالات سجل أحداث Windows المنشورة خلال الفترة من الوقت والتاريخ المحددين إلى لحظة تشغيل المهمة. يسمح Kaspersky Endpoint Security بتحديد تاريخ نشر الحدث كقيمة الوسيطة. ويتم إجراء الفحص فقط للأحداث المنشورة في سجل أحداث Windows بعد التاريخ المحدد وقبل تشغيل الفحص. إذا لم يتم تحديد الوسيطة، يفحص Kaspersky Endpoint Security الأحداث بأي تاريخ نشر. لا يمكن تحرير إعداد TaskSettings::BaseSettings::EventLogItem::datetime. يُستخدم الإعداد فقط في حالة وصف مستند EventLogItem IOC في ملف IOC المقدم للفحص.
`/channel=<list of channels>`	قائمة بأسماء القنوات (السجل) التي تريد إجراء فحص IOC لها. في حالة تحديد الوسيطة، يفحص Kaspersky Endpoint Security السجلات المنشورة في السجلات المحددة. ويجب أن يحتوي مستند IOC على شرط EventLogItem الموضح. يتم تحديد اسم السجل كسلسلة وفقًا لاسم السجل (القناة) المحدد في خصائص السجل (معلمة الاسم الكامل) أو في خصائص الحدث (المعلمة <Channel></Channel> في مخطط xml للحدث). يمكنك تحديد قنوات متعددة مفصولة بمسافات.

	إذا لم يتم تحديد الوسيطة، يفحص Kaspersky Endpoint Security السجلات بحثًا عن القنوات `Application` و`System` و`Security`.
`/files=on|off`	تحليل بيانات الملف عند إجراء فحص IOC (شرط FileItem). إذا كانت قيمة الوسيط `off`، لا يحلل Kaspersky Endpoint Security بيانات الملف. إذا كان ملف IOC يحتوي على شروط مستند FileItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security بيانات الملف فقط إذا كان مستند FileItem IOC موصوفًا في ملف IOC المقدم للفحص.
`/drives=<all|system|critical|custom>`	ضبط نطاق فحص IOC عند تحليل البيانات لمستند FileItem IOC. يمكنك تعيين القيم التالية لنطاق الفحص: • `<all>` لجميع نطاقات الملفات المتاحة. • `<system>` للملفات الموجودة في المجلدات حيث تم تثبيت نظام التشغيل. • `<critical>` للملفات المؤقتة في مجلدات المستخدم والنظام. • `<custom>` للملفات في النطاقات المعرفة بواسطة المستخدم (`/scope=<list of folders to scan>`). إذا لم يتم تحديد الوسيطة، يتم إجراء الفحص للمناطق الحرجة.
`/excludes=<list of exclusions>`	تعيين نطاق الاستثناء عند تحليل البيانات لمستند FileItem IOC. يمكنك تحديد مسارات متعددة مفصولة بمسافات.
`/scope=<list of folders to scan>`	نطاق فحص IOC المحدد بواسطة المستخدم عند تحليل البيانات لمستند FileItem IOC (`/drives=custom`). يمكنك تحديد مسارات متعددة مفصولة بمسافات.

قيم إرجاع الأمر:

- `-1` يعني أن الأمر غير مدعوم من إصدار التطبيق المُثبت على الكمبيوتر.
- `0` يعني أن الأمر تم تنفيذه بنجاح.
- `1` يعني أنه لم يتم تمرير وسيطة إلزامية إلى الأمر.
- `2` يعني حدوث خطأ عام.
- `4` يعني أنه كان هناك خطأ في بناء الجملة.

في حالة تنفيذ الأمر بنجاح (قيمة الإرجاع `0`) وتم اكشاف مؤشرات اختراق على طول الطريق، يُخرج Kaspersky Endpoint Security معلومات نتائج المهمة التالية إلى سطر الأوامر:

`Uuid`	معرف ملف IOC من رأس بنية ملف IOC (علامة `<ioc id="">`)
`Name`	وصف ملف IOC من رأس بنية ملف IOC (علامة `<description></description>`)
`Matched Indicator Items`	قائمة معرفات جميع المؤشرات المطابقة.
`Matched objects`	البيانات الخاصة بكل مستند IOC التي تم العثور على تطابق لها.

MDRLICENSE. تفعيل MDR

نفذ العمليات باستخدام ملف تكوين BLOB لتفعيل Managed Detection and Response. ويحتوي ملف BLOB على معرّف العميل ومعلومات حول ترخيص Kaspersky Managed Detection and Response. ويوجد ملف BLOB داخل أرشيف ZIP الخاص بملف تكوين MDR. ويمكنك الحصول على أرشيف ZIP في لوحة تحكم Kaspersky Managed Detection and Response. وللحصول على معلومات تفصيلية عن ملف BLOB، يرجى الرجوع إلى تعليمات Kaspersky Managed Detection and Response.

امتيازات المسؤول مطلوبة لتنفيذ العمليات باستخدام ملف BLOB. ويجب أن تكون إعدادات Managed Detection and Response في السياسة متاحة أيضًا للتحرير ().

بناء جملة الأمر

```
[<avp.com MDRLICENSE <operation> [/login=<user name> /password=<password
```

العملية	
/ADD <file name>	طبق ملف تكوين BLOB للتكامل مع Kaspersky Managed Detection and Response (تنسيق الملف P7). ويمكنك تطبيق ملف BLOB واحد فقط. وفي حالة إضافة ملف BLOB بالفعل إلى الكمبيوتر، فسيتم استبدال الملف.
/DEL	احذف ملف تكوين BLOB.

المصادقة	
/login=<user name> /password=<password>	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال:

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=!Password1
```

EDRKATA. التكامل مع KATA) EDR)

أوامر إدارة مكون Endpoint Detection and Response (KATA):

- تمكين أو تعطيل مكون EDR (KATA).

  يوفر مكون EDR (KATA) إمكانية التشغيل التفاعلي مع حل Kaspersky Anti Targeted Attack Platform.

- تكوين الاتصال بخوادم Kaspersky Anti Targeted Attack Platform.

- عرض الإعدادات الحالية للمكون.

بناء جملة الأمر

```
avp.com START EDRKATA
avp.com STOP EDRKATA
avp.com edrkata /set /servers=<عنوان الخادم>:<المنفذ> /server-certificate=<المسار
إلى شهادة /timeout=TLS> [<مهلة اتصال خادم Central Node (ث)>] [/sync-period=<فترة
مزامنة خادم Central Node (دقيقة)>]
avp.com edrkata /show
```

العملية	
stop	تعطيل مكون EDR (KATA).
start	تمكين مكون EDR (KATA).
set	تكوين مكون EDR (KATA). يمكنك تعديل البيانات التالية: • إضافة خوادم العقدة المركزية (servers=<عنوان الخادم>:<المنفذ>). • إضافة شهادة TLS (server-certificate=<المسار إلى شهادة TLS>). • تعيين مهلة اتصال خادم العقدة المركزية (timeout/=<مهلة الاتصال بخادم العقدة المركزية (بالثواني)>). • تعيين فترة التزامن مع خادم العقدة المركزية (sync-period/=<فترة مزامنة خادم العقدة المركزية (بالدقائق)>).
show	عرض الإعدادات الحالية للمكون.

رموز الخطأ

قد تحدث أخطاء عند العمل مع التطبيق من خلال سطر الأوامر. عند حدوث أخطاء، يعرض Kaspersky Endpoint Security رسالة خطأ على سبيل المثال، `خطأ: لا يمكن بدء المهمة 'EntAppControl'`. يمكن أن يعرض Kaspersky Endpoint Security معلومات إضافية في شكل رمز، على سبيل المثال، `error = 8947906D` (انظر الجدول أدناه).

رموز الخطأ

رمز الخطأ	الوصف
09479001	هذا المفتاح مستخدم بالفعل
0947901D	انتهت صلاحية الترخيص. تحديثات قاعدة البيانات غير متاحة
89479002	لم يتم العثور على المفتاح
89479003	التوقيع الرقمي إما مفقود أو تالف
89479004	البيانات تالفة
89479005	ملف المفتاح تالف
89479006	انتهت صلاحية الترخيص
89479007	لم يتم تحديد ملف المفتاح
89479008	ملف المفتاح غير صحيح
89479009	فشل حفظ البيانات
8947900A	فشل قراءة البيانات
8947900B	خطأ في الإدخال/الإخراج
8947900C	لم يتم العثور على قواعد البيانات
8947900E	لم يتم تحميل مكتبة التراخيص
8947900F	قواعد البيانات تالفة أو تم تحديثها يدويًا

89479010	قواعد البيانات تالفة
89479011	لا يمكن استخدام ملف مفتاح غير صالح لإضافة مفتاح احتياطي
89479012	خطأ في النظام
89479013	قائمة الرفض الخاصة بالمفاتيح تالفة
89479014	توقيع الملف لا يطابق التوقيع الرقمي لـ Kaspersky
89479015	لا يمكن استخدام مفتاح لترخيص تجريبي كمفتاح لترخيص تجاري
89479016	يلزم ترخيص لاختبار بيتا لاستخدام إصدار بيتا من التطبيق
89479017	ملف المفتاح غير متوافق مع هذا التطبيق. لا يمكن تفعيل Kaspersky Endpoint Security for Windows باستخدام ملف مفتاح خاص بتطبيق آخر. يرجى التحقق من التطبيق المُثبّت
89479018	تم منع مفتاح الترخيص بواسطة Kaspersky
89479019	تم استخدام التطبيق بالفعل تحت الترخيص التجريبي. تعذر إضافة مفتاح للترخيص التجريبي مرة أخرى
8947901A	ملف المفتاح تالف
8947901B	التوقيع الرقمي مفقود أو تالف أو لا يطابق التوقيع الرقمي من Kaspersky
8947901C	لا يمكن إضافة مفتاح إذا انتهت صلاحية الترخيص غير التجاري المناظر له
8947901E	تاريخ إنشاء ملف المفتاح أو استخدامه غير صالح. يرجى التحقق من تاريخ النظام
8947901F	لا يمكن إضافة مفتاح للترخيص التجريبي: يوجد مفتاح آخر فعال للترخيص التجريبي
89479020	قائمة الرفض الخاصة بالمفاتيح تالفة أو مفقودة
89479021	وصف التحديث مفقود أو تالف
89479022	البيانات الداخلية غير متوافقة مع هذا التطبيق
89479023	لا يمكن استخدام ملف مفتاح غير صالح لإضافة مفتاح احتياطي
89479025	خطأ في إرسال طلب خادم التفعيل. الأسباب المحتملة: وجود خطأ في الاتصال بالإنترنت أو مشكلات مؤقتة في خادم التفعيل. حاول تفعيل التطبيق لاحقًا (خلال ساعة إلى ساعتين) باستخدام رمز التفعيل. إذا تكرر هذا الخطأ مرة أخرى، فاتصل بموفر خدمة الإنترنت
89479026	يحتوي الطلب على رمز تفعيل غير صحيح
89479027	لا يمكن الحصول على حالة الاستجابة
89479028	حدث خطأ عند حفظ ملف مؤقت
89479029	تم إدخال رمز تفعيل خاطئ أو تم إعداد تاريخ نظام غير صالح على الكمبيوتر. يرجى التحقق من تاريخ النظام على الكمبيوتر
8947902A	المفتاح لا يتوافق مع هذا التطبيق، أو انتهت صلاحية الترخيص
8947902B	فشل استلام ملف مفتاح. تم إدخال رمز تفعيل غير صحيح
8947902C	أعاد خادم التفعيل الخطأ 400
8947902D	أعاد خادم التفعيل الخطأ 401
8947902E	أعاد خادم التفعيل الخطأ 403
8947902F	هناك مورد ضروري غير متاح على خادم التفعيل. أعاد خادم التفعيل الخطأ 404. يرجى التحقق من إعدادات اتصال الإنترنت
89479030	أعاد خادم التفعيل الخطأ 405
89479031	أعاد خادم التفعيل الخطأ 406
89479032	يلزم مصادقة الخادم الوكيل. الرجاء التحقق من إعدادات الشبكة
89479033	انتهت مهلة الطلب

89479034	أعاد خادم التفعيل الخطأ 409
89479035	هناك مورد ضروري غير متاح على خادم التفعيل. أعاد خادم التفعيل الخطأ 410. يرجى التحقق من إعدادات اتصال الإنترنت
89479036	أعاد خادم التفعيل الخطأ 411
89479037	أعاد خادم التفعيل الخطأ 412
89479038	أعاد خادم التفعيل الخطأ 413
89479039	أعاد خادم التفعيل الخطأ 414
8947903A	أعاد خادم التفعيل الخطأ 415
8947903C	خطأ داخلي بالخادم
8947903D	الوظيفة غير مدعومة
8947903E	استجابة غير صالحة من البوابة. الرجاء التحقق من إعدادات الشبكة
8947903F	المورد غير متاح مؤقتًا
89479040	انتهت مهلة استجابة البوابة. الرجاء التحقق من إعدادات الشبكة لديك
89479041	البروتوكول غير مدعوم من قبل الخادم
89479043	خطأ http غير معروف
89479044	معرف مورد غير صالح
89479046	عنوان URL غير صالح
89479047	مجلد الوجهة غير صالح
89479048	خطأ في تخصيص الذاكرة
89479049	حدث خطأ عند تحويل المعلّمات إلى سلسلة ANSI (عنوان URL، مجلد، وكيل)
8947904A	حدث خطأ عند إنشاء مؤشر ترابط عامل
8947904B	مؤشر ترابط العامل يعمل بالفعل
8947904C	مؤشر ترابط العامل لا يعمل
8947904D	لم يتم العثور على ملف المفتاح على خادم التفعيل
8947904E	تم منع المفتاح
8947904F	خطأ داخلي في خادم التفعيل
89479050	لا تتوافر بيانات كافية في طلب التفعيل
89479053	لقد انتهت بالفعل صلاحية الترخيص الخاص بالمفتاح المضاف
89479054	تم ضبط تاريخ نظام غير صالح على الكمبيوتر. يرجى التحقق من قيمة تاريخ النظام
89479055	انتهت صلاحية الترخيص التجريبي
89479056	انتهت صلاحية فترة تفعيل التطبيق
89479057	تم تجاوز حد عمليات تفعيل التطبيق للرمز المحدد
89479058	اكتمل إجراء التفعيل مع وجود خطأ في النظام
89479059	لا يمكن استخدام مفتاح لترخيص تجريبي كمفتاح لترخيص تجاري
8947905C	رمز التفعيل مطلوب
89479062	لا يمكن الاتصال بخادم التفعيل
89479064	خادم التفعيل غير متاح. يرجى التحقق من إعدادات الاتصال بالإنترنت لديك وإعادة محاولة التفعيل

89479065	انتهت صلاحية الترخيص
89479066	لا يمكن استبدال المفتاح الفعال بمفتاح منتهي الصلاحية
89479067	لا يمكن إضافة مفتاح احتياطي إذا انتهت صلاحية الترخيص المرتبط به قبل الترخيص الحالي
89479068	مفتاح الاشتراك المحدّث مفقود
8947906A	رمز التفعيل غير صالح
8947906B	المفتاح فعال بالفعل
8947906C	إن أنواع التراخيص المرتبطة بالمفاتيح النشطة والمفاتيح الاحتياطية لا تتطابق
8947906D	الترخيص لا يدعم المكون
8947906E	تتعذر إضافة مفتاح اشتراك كمفتاح احتياطي
89479213	خطأ عام في طبقة النقل
89479214	فشل الاتصال بخادم التفعيل
89479215	تنسيق عنوان ويب غير صالح
89479216	فشل تحويل عنوان خادم الوكيل
89479217	فشل تحويل عنوان الخادم. يرجى التحقق من إعدادات الاتصال بالإنترنت
89479218	فشلت محاولة الاتصال بالخادم
89479219	تم رفض الوصول عن بعد
8947921A	انتهت مهلة العملية
8947921B	خطأ في إرسال طلب HTTP
8947921C	خطأ في اتصال SSL
8947921D	تمت مقاطعة العملية بالرد
8947921E	توجد حالات إعادة توجيه أكثر من اللازم
8947921F	فشل فحص المستلم
89479220	استجابة فارغة من الخادم
89479221	خطأ في إرسال البيانات
89479222	خطأ في استلام البيانات
89479223	مشكلة مرتبطة بشهادة SSL
89479224	مشكلة مرتبطة بتشفير SSL
89479225	مشكلة مرتبطة بمركز شهادات SSL
89479226	محتويات غير صالحة لحزمة الشبكة
89479227	تم رفض الوصول إلى الحساب
89479228	ملف شهادة SSL غير صالح
89479229	يتعذر إيقاف اتصال SSL
8947922A	خطأ متكرر
8947922B	ملف غير صالح مع شهادات ملغاة
8947922C	خطأ في طلب شهادة SSL

89479401	خطأ غير معروف في الخادم
89479402	خطأ في الخادم الداخلي
89479403	لا يتوافر مفتاح لرمز التفعيل الذي تم إدخاله
89479404	تم منع المفتاح الفعال
89479405	المعلمات المطلوبة لطلب التفعيل مفقودة
89479406	كلمة مرور غير صالحة أو رقم غير صالح للوكيل
89479407	رمز التفعيل غير صالح
89479408	رمز التفعيل غير متوافق مع هذا التطبيق. لا يمكن تفعيل Kaspersky Endpoint Security for Windows باستخدام رمز تفعيل خاص بتطبيق آخر. يرجى التحقق من التطبيق المُثبّت
89479409	رمز التفعيل مطلوب
8947940B	انتهاء صلاحية فترة التفعيل
8947940C	تم تجاوز عدد مرات التفعيل المسموح بها لهذا الرمز
8947940D	تنسيق غير صالح لمعرف الطلب
8947940E	رمز التفعيل موجود بالفعل
8947940F	فشل إعادة تجديد رمز التفعيل
89479410	رمز التفعيل غير صالح لهذه المنطقة
89479411	لا يمكن استخدام رمز التفعيل هذا لترجمة هذا التطبيق
89479412	رمز التفعيل خاص بالإصدار الجديد لهذا التطبيق. احصل على رمز تفعيل مختلف لتفعيل الإصدار المثبت لهذا التطبيق
89479413	أرجع خادم التفعيل الخطأ 643
89479414	أرجع خادم التفعيل الخطأ 644
89479415	أرجع خادم التفعيل الخطأ 645
89479416	أرجع خادم التفعيل الخطأ 646
89479417	يتطلب إصدار خادم التفعيل 1.0
89479418	تنسيق رمز تفعيل غير صحيح
89479419	توقيت الكمبيوتر غير متزامن مع توقيت خادم التفعيل
8947941A	إصدار تطبيق غير صحيح
8947941B	انتهت صلاحية الاشتراك
8947941C	تم تجاوز عدد عمليات التفعيل
8947941D	توقيع تذكرة غير صالح
8947941E	البيانات الإضافية مطلوبة
8947941F	فشل التحقق من البيانات
89479420	الاشتراك غير فعال
89479421	خادم التفعيل تحت الصيانة
89479501	خطأ غير متوقع
89479502	تم نقل معلمة غير صالحة. على سبيل المثال، قائمة فارغة بعناوين خادم التفعيل
89479503	رمز تفعيل غير صالح (تجزئة غير صالحة)

89479504	معرف المستخدم غير صالح
89479505	كلمة مرور المستخدم غير صالحة
89479506	استجابة غير صالحة من خادم التفعيل
89479507	تمت مقاطعة طلب التفعيل
89479509	أعاد خادم التفعيل قائمة إعادة توجيه فارغة

الملحق. ملفات تعريف التطبيق

إن ملف التعريف عبارة عن مكون أو مهمة أو ميزة لبرنامج Kaspersky Endpoint Security. تستخدم ملفات التعريف لإدارة التطبيق من سطر الأوامر. يمكنك استخدام ملفات التعريف لتنفيذ الأوامر `START`، و`STOP`، و`STATUS`، و`STATISTICS`، و`EXPORT`، و`IMPORT`. باستخدام ملفات التعريف، يمكنك تكوين إعدادات التطبيق (على سبيل المثال، `STOP DeviceControl`) أو تشغيل المهام (على سبيل المثال، `START Scan_My_Computer`).

تتوافر ملفات التعريف التالية:

- `AdaptiveAnomaliesControl` – مراقبة عيوب التكيف.
- `AMSI` – حماية AMSI.
- `BehaviorDetection` – اكتشاف السلوك.
- `DeviceControl` – التحكم في الجهاز.
- `EntAppControl` – التحكم في التطبيق.
- `File_Monitoring` أو `FM` – الحماية من تهديدات الملفات.
- `Firewall` أو `FW` – جدار الحماية.
- `HIPS` – منع اختراق المضيف.
- `IDS` – الحماية من تهديدات الشبكة.
- `IntegrityCheck` – التحقق من التكامل.
- `LogInspector` – فحص السجل.
- `Mail_Monitoring` أو `EM` – الحماية من تهديدات البريد.
- `Rollback` – تحديث عملية التراجع.
- `Scan_ContextScan` – الفحص من قائمة السياق.
- `Scan_IdleScan` – فحص في الخلفية.
- `Scan_Memory` – فحص ذاكرة Kernel.
- `Scan_My_Computer` – الفحص الكامل.

- `Scan_Objects` – الفحص المخصص.
- `Scan_Qscan` – فحص الكائنات التي تم تحميلها عند بدء تشغيل نظام التشغيل.
- `Scan_Removable_Drive` – فحص محركات الأقراص القابلة للإزالة.
- `Scan_Startup` أو `STARTUP` – فحص المناطق الحرجة.
- `Updater` – تحديث.
- `Web_Monitoring` أو `WM` – الحماية من تهديدات الويب.
- `WebControl` – التحكم في الويب.

وكذلك يدعم برنامج Kaspersky Endpoint Security ملفات تعريف الخدمة. قد تكون ملفات تعريف الخدمة مطلوبة عند تواصلك مع خدمة الدعم الفني لـKaspersky.

إدارة التطبيق من خلال REST API

يتيح لك Kaspersky Endpoint Security تكوين إعدادات التطبيق، وإدارة إجراءات فحص ما، وتحديث قواعد بيانات مكافحة الفيروسات، وأداء مهام أخرى باستخدام حلول مقدمة من جهات خارجية. يوفر Kaspersky Endpoint Security واجهة برمجة تطبيقات (API) لهذا الغرض. إن Kaspersky Endpoint Security REST API تعمل عبر HTTP وتتكون من مجموعة من طرق الطلب/الاستجابة. بعبارةٍ أخرى، يمكنك إدارة Kaspersky Endpoint Security من خلال حل مقدم من جهة خارجية، وليست واجهة التطبيق المحلية أو وحدة تحكم إدارة Kaspersky Security Center.

لبدء استخدام REST API، ستحتاج إلى تثبيت Kaspersky Endpoint Security مع دعم REST API. يجب تثبيت عميل REST وKaspersky Endpoint Security على نفس جهاز الكمبيوتر.

لضمان التفاعل الآمن بين Kaspersky Endpoint Security وعميل REST:

- كوّن حماية عميل REST ضد الوصول غير المصرح به وفقًا لتوصيات مطور عميل REST. كوّن حماية مجلد عميل REST ضد الكتابة بمساعدة قائمة Discretionary Access Control List - DACL.
- لتشغيل عميل REST، استخدم حسابًا منفصلاً يمتلك حقوق المسؤول. وارفض تسجيل الدخول التفاعلي إلى النظام لهذا الحساب.

تتم إدارة التطبيق من خلال REST API على http://127.0.0.1 أو http://localhost. لا يمكن إدارة Kaspersky Endpoint Security عن بُعد من خلال REST API.

فتح المراجع الخاصة بـ REST API

تثبيت التطبيق مع REST API

لإدارة التطبيق من خلال REST API، ستحتاج إلى تثبيت Kaspersky Endpoint Security بدعم لـ REST API. إذا كنت تدير Kaspersky Endpoint Security من خلال REST API، فلن تتمكن من إدارة التطبيق باستخدام Kaspersky Security Center.

التحضير لتثبيت التطبيق مع دعم REST API

يتطلب التفاعل الآمن لبرنامج Kaspersky Endpoint Security مع عميل REST تكوين تعريف الطلب. ولفعل ذلك، يجب عليك تثبيت شهادة ثم بعد ذلك التوقيع على حمولة كل طلب.

لإنشاء شهادة، يمكنك استخدام OpenSSL على سبيل المثال.

مثال:

```
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

استخدم خوارزمية تشفير RSA بطول مفتاح 2048 بت أو أكثر.

نتيجة لذلك، سوف تحصل على شهادة `cert.pem` ومفتاح `key.pem` خاص.

تثبيت التطبيق مع دعم REST API

لتثبيت Kaspersky Endpoint Security الذي يشتمل على دعم REST API:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.
2. انتقل إلى المجلد الذي يحتوى على حزمة التوزيع الخاصة بالإصدار 11.2.0 من Kaspersky Endpoint Security أو إصدار أحدث.
3. قم بتثبيت Kaspersky Endpoint Security باستخدام الإعدادات التالية:

- `RESTAPI=1`
- `RESTAPI_User=<User name>`

اسم المستخدم الخاص بإدارة التطبيق من خلال REST API. أدخل اسم المستخدم `<DOMAIN>\<UserName>` (على سبيل المثال، `RESTAPI_User=COMPANY\Administrator`). يمكنك إدارة التطبيق من خلال REST API من خلال هذا الحساب فقط. يمكنك تحديد مستخدم واحد فقط للعمل باستخدام REST API.

- `RESTAPI_Port=<Port>`

المنفذ المستخدم لإدارة التطبيق من خلال REST API. يُستخدم المنفذ 6782 بشكل افتراضي. تأكد أن المنفذ خالٍ. معلمة اختيارية.

- `RESTAPI_Certificate=<Path to certificate>`

شهادة لتحديد الطلبات (على سبيل المثال، `RESTAPI_Certificate=C:\cert.pem`).

يمكنك تثبيت الشهادة بعد تثبيت التطبيق أو تحديث الشهادة بعد انتهاء صلاحيتها.

كيفية تثبيت شهادة لتعريف طلب REST API

1. تعطيل الدفاع الذاتي لبرنامج Kaspersky Endpoint Security

   تمنع آلية الدفاع الذاتي تغيير أو حذف ملفات التطبيق على محرك الأقراص الصلبة، وكذلك العمليات في الذاكرة والإدخالات في سجل النظام.

2. انتقل إلى مفتاح التسجيل الذي يحتوي على إعدادات REST API:
`Y_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestApi`

3. أدخل مسار الشهادة، على سبيل المثال، `Certificate = C:\Folder\cert.pem`.

   تمكين الدفاع الذاتي لبرنامج Kaspersky Endpoint Security.
4. أعد تشغيل التطبيق.

- `AdminKitConnector=1`

إدارة التطبيقات باستخدام نظم الإدارة. الإدارة مسموح بها بشكل افتراضي.

ويمكنك أيضًا استخدام ملف setup.ini لتحديد إعدادات العمل باستخدام REST API.

مثال:

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
/pAdminKitConnector=1 /pRESTAPI=1 /pRESTAPI_User=COMPANY\Administrator
/pRESTAPI_Certificate=C:\cert.pem /s
```

نتيجةً لذلك، ستتمكن من إدارة التطبيق من خلال REST API. للتحقق من عمله على النحو الصحيح، افتح المراجع الخاصة بـ REST API باستخدام طلب GET.

مثال:

```
GET http://localhost:6782/kes/v1/api-docs
```

إذا قمت بتثبيت التطبيق مع دعم REST API، ينشئ Kaspersky Endpoint Security تلقائيًا قاعدة سماح في إعدادات التحكم في الويب للوصول إلى موارد الويب (قاعدة الخدمة لأجل REST API). وهذه القاعدة ضرورية للسماح لعميل REST بالوصول إلى Kaspersky Endpoint Security في جميع الأوقات. على سبيل المثال، إذا قيدت وصول المستخدم إلى موارد الويب، فلن يؤثر ذلك على إدارة التطبيق من خلال واجهة REST API. نوصي بعدم حذف القاعدة أو تغيير إعدادات قاعدة الخدمة لأجل REST API. وإذا حذفت القاعدة، فسوف يستعيدها Kaspersky Endpoint Security بعد إعادة تشغيل التطبيق.

العمل باستخدام واجهة برمجة التطبيقات (API)

لا يمكن تقييد الوصول إلى التطبيقات من خلال REST API باستخدام الحماية بكلمة مرور. على سبيل المثال، لا يمكن منع مستخدم من تعطيل حماية من خلال REST API. يمكنك تكوين الحماية بكلمة المرور من خلال REST API وتقييد وصول المستخدم إلى التطبيق من خلال الواجهة المحلية.

لإدارة التطبيق من خلال REST API، ستحتاج إلى تشغيل عميل REST في الحساب الذي حددته عند تثبيت التطبيق الذي يشتمل على دعم REST API. يمكنك تحديد مستخدم واحد فقط للعمل باستخدام REST API.

فتح المراجع الخاصة بـ REST API

تتكون إدارة التطبيق من خلال REST API من الخطوات التالية:

1. الحصول على القيم الحالية لإعدادات التطبيق. لتنفيذ ذلك، أرسل طلب GET.

مثال:

```
GET http://localhost:6782/kes/v1/settings/ExploitPrevention
```

2. سيقوم التطبيق بإرسال استجابة تشتمل على بنية الإعدادات وقيمها. يدعم Kaspersky Endpoint Security الصيغ XML و JSON.

مثال:

```
{
"action": 0,
"enableSystemProcessesMemoryProtection": true,
"enabled": true
}
```

3. تحرير إعدادات التطبيق. استخدم بنية الإعدادات التي تم استلامها في سياق الاستجابة لطلب GET.

مثال:

```
{
"action": 0,
"enableSystemProcessesMemoryProtection": false,
"enabled": true
}
```

4. حفظ إعدادات التطبيق (الحمولة) في JSON (payload.json).

5. وقّع JSON بتنسيق PKCS7.

مثال:

```
openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -
binary -outform pem -out signed_payload.pem
```

نتيجة لذلك، تحصل على ملف موقع مع حمولة الطلب (signed_payload.pem).

6. تحرير إعدادات التطبيق. لفعل ذلك، أرسل طلب POST وأرفق الملف الموقع مع حمولة الطلب (signed_payload.pem).

يطبق التطبيق الإعدادات الجديدة ويرسل استجابة تحتوي على نتائج تكوين التطبيق (من الممكن أن تكون الاستجابة فارغة). ويمكنك التحقق من تحديث الإعدادات باستخدام طلب GET.

مصادر المعلومات المتعلقة بالتطبيق

يحتوي هذا القسم على وصف لمصادر المعلومات عن التطبيق.

يمكنك تحديد المصدر الأكثر ملاءمة للمعلومات اعتمادًا على أهمية وإلحاح المشكلة.

الاتصال بالدعم الفني

إذا لم تتمكن من إيجاد حل لمشكلتك في الوثائق أو في مصادر أخرى للمعلومات عن Kaspersky Endpoint Security، فننصحك بالاتصال بالدعم الفني. وسوف يجيب أخصائيو الدعم الفني على تساؤلاتك حول تثبيت Kaspersky Endpoint Security واستخدامه.

توفر Kaspersky دعمًا لتطبيق Kaspersky Endpoint Security أثناء دورة حياة التطبيق (يرجى الرجوع إلى صفحة دورة حياة التطبيق). قبل الاتصال بالدعم الفني، الرجاء قراءة قواعد الدعم.

يمكنك الاتصال بخدمة الدعم الفني بإحدى الطرق التالية:

- عن طريق زيارة موقع ويب الدعم الفني
- عن طريق إرسال طلب إلى الدعم الفني لشركة Kaspersky من خلال بوابة Kaspersky CompanyAccount

بعد أن تخبر اختصاصيي الدعم الفني في Kaspersky بمشكلتك، يمكنك أن تطلب منهم إنشاء ملف تتبع. يسمح لك ملف التتبع بتتبع عملية تنفيذ أوامر التطبيق خطوة بخطوة وتحديد مرحلة من مراحل تشغيل التطبيق التي يحدث فيها الخطأ.

قد يطلب اختصاصيو الدعم الفني معلومات إضافية عن نظام التشغيل والعمليات قيد التشغيل على الكمبيوتر وتقارير مفصلة عن مكونات تشغيل التطبيق.

أثناء تشغيل التشخيصات، قد يطلب منك خبراء الدعم الفني تغيير إعدادات التطبيق عن طريق:

- تفعيل الوظيفة لتلقي معلومات تشخيصية موسعة.
- يمكنك تكوين المكونات الفردية الخاصة بالتطبيق عبر تغيير الإعدادات الخاصة التي لا يمكن الوصول إليها من خلال واجهة المستخدم القياسية.
- تغيير إعدادات تخزين المعلومات التشخيصية.
- تكوين الاعتراض وتسجيل حركة مرور الشبكة.

سيقدم خبراء الدعم الفني جميع المعلومات الضرورية لتنفيذ هذه العمليات (وصف تسلسل الخطوات، والإعدادات التي سيتم تعديلها، وملفات التكوين، والنصوص، ووظائف سطر الأوامر الإضافية، ووحدات تصحيح الأخطاء النمطية، والأدوات المساعدة لأغراض خاصة وما إلى ذلك) وإعلامك بنطاق البيانات التي تم استخدامها لأغراض تصحيح الأخطاء. يتم حفظ المعلومات التشخيصية الموسعة على كمبيوتر المستخدم. لا يتم نقل البيانات تلقائيا إلى Kaspersky.

يجب إجراء العمليات المذكورة أعلاه فقط تحت إشراف متخصصي الدعم الفني من خلال اتباع تعليماتهم. قد يتسبب تغيير إعدادات التطبيق بنفسك على نحو غير الموضح في التعليمات عبر الإنترنت أو في توصيات الدعم الفني، في بطء وتعطل نظام التشغيل، وخفض مستوى حماية الكمبيوتر وإتلاف توافر وسلامة المعلومات التي يجري معالجتها.

محتويات وتخزين ملفات التتبع

أنت تتحمل المسؤولية الشخصية عن أمان البيانات المخزنة على جهاز الكمبيوتر لديك، وبالأخص عن مراقبة وتقييد الوصول إلى البيانات حتى يتم إرسالها إلى Kaspersky.

يتم تخزين ملفات التتبع على الكمبيوتر طالما أن التطبيق قيد الاستخدام ويتم خذفها نهائيًا عند إزالة التطبيق.

يتم حفظ ملفات التتبع، باستثناء تلك الخاصة بوكيل المصادقة، في المجلد `%ProgramData%\Kaspersky Lab\KES.21.13\Traces`.

يتم تسمية ملفات التتبع على النحو التالي: `KES<21.13_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`.

يمكنك عرض البيانات التي تم حفظها في ملفات التتبع.

تحتوي جميع ملفات التتبع على البيانات المشتركة التالية:

- وقت الحدث.
- رقم مؤشر ترابط التنفيذ.

لا يحتوى ملف تتبع وكيل المصادقة على هذه المعلومات.

- مكون التطبيق الذي تسبب في الحدث.
- درجة خطورة الحدث (حدث معلوماتي، تحذير، حدث حرج، خطأ).
- وصف الحدث الذي ينطوي على تنفيذ الأمر بواسطة مكون التطبيق ونتيجة تنفيذ هذا الأمر.

يقوم Kaspersky Endpoint Security بحفظ كلمات المرور الخاصة بالمستخدم في ملف التتبع بصيغة مشفرة فقط.

محتويات ملفات التتبع SRV.log، وGUI.log، وALL.log

قد تُخزِن ملفات التتبع `SRV.log`، و`GUI.log`، و`ALL.log` المعلومات التالية بالإضافة إلى البيانات العامة:

- البيانات الشخصية، بما في ذلك الاسم الأخير، والاسم الأول والاسم الأوسط، وذلك إذا تم تضمين هذه البيانات في المسار إلى الملفات على الكمبيوتر المحلي.
- بيانات عن الجهاز المثبت على الكمبيوتر (مثل بيانات البرنامج الثابت لأي من BIOS/UEFI). يتم كتابة هذه البيانات في ملفات تتبع عند أجراء تشفير القرص من Kaspersky.
- اسم المستخدم وكلمة المرور إذا تم نقلهم بشكل علني. يمكن تسجيل هذه البيانات في ملفات التتبع أثناء فحص حركة الإنترنت.
- اسم المستخدم وكلمة المرور إذا تم تضمينهم في رؤوس HTTP.
- اسم حساب Microsoft Windows إذا تم تضمين اسم الحساب في اسم الملف.
- عنوان بريدك الإلكتروني أو عنوان الويب الذي يحتوى على اسم حسابك وكلمة المرور إذا تم تضمينهم في اسم الكائن الذي تم اكتشافه.
- المواقع التي تقوم بزيارتها وحالات إعادة التوجيه من هذه المواقع. يتم كتابة هذه البيانات إلى ملفات التتبع عند قيام التطبيق بفحص مواقع الويب.
- عنوان الخادم الوكيل، واسم الكمبيوتر، والمنفذ، وعنوان IP، واسم المستخدم الذي يتم استخدامه لتسجيل الدخول إلى الخادم الوكيل. يتم كتابة هذه البيانات إلى ملفات التتبع إذا استخدم التطبيق الخادم الوكيل.
- عناوين IP البعيدة التي يقوم الكمبيوتر الخاص بك بإنشاء اتصالات إليها.
- موضوع الرسالة، المعرف، اسم المرسل ورسالة صفحة ويب المرسل على شبكة التواصل الاجتماعي. يتم كتابة هذه البيانات إلى ملفات التتبع إذا تم تمكين مكون التحكم في الويب.
- بيانات مرور شبكة الاتصال. يتم كتابة هذه البيانات في ملفات تتبع إذا كان المرور يراقب مكونات مفعلة (مثل التحكم في الويب).
- البيانات المستلمة من خوادم Kaspersky (مثل إصدار قواعد بيانات مكافحة الفيروسات).
- حالات مكونات Kaspersky Endpoint Security وبيانات تشغيلها.
- بيانات عن نشاط المستخدم في التطبيق.

- أحداث نظام التشغيل.

محتويات ملفات التتبع HST.log، وBL.log، وDumpwriter.log، وWD.log، وAVPCon.dll.log

بالإضافة إلى البيانات العامة، يحتوي ملف التتبع HST.log على معلومات حول تنفيذ مهمة تحديث الوحدة النمطية للتطبيق وقاعدة البيانات.

بالإضافة إلى البيانات العامة، يحتوي ملف التتبع BL.log على معلومات حول الأحداث التي وقعت أثناء تشغيل التطبيق، وكذلك البيانات المطلوبة لاكتشاف وإصلاح أخطاء التطبيق. يتم إنشاء هذا الملف إذا تم بدء التطبيق مع المعلمة avp.exe –b.l.

بالإضافة إلى البيانات العامة، يحتوي ملف التتبع Dumpwriter.log على معلومات الخدمة المطلوبة لاكتشاف وإصلاح الأخطاء التي تقع عند كتابة ملف تفريغ التطبيق.

بالإضافة إلى البيانات العامة، يحتوي ملف التتبع WD.log على معلومات حول الأحداث التي تقع أثناء تشغيل الخدمة avpsus، بما في ذلك أحداث تحديث الوحدة النمطية للتطبيق.

بالإضافة إلى البيانات العامة، يحتوي ملف التتبع AVPCon.dll.log على معلومات حول الأحداث التي تقع أثناء تشغيل الوحدة النمطية لاتصال Kaspersky Security Center.

محتويات ملفات عمليات تتبع الأداء

يتم تسمية ملفات عمليات تتبع الأداء على النحو التالي: KES<21.13_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl.

بالإضافة إلى البيانات العامة، تحتوي ملفات عمليات تتبع الأداء على معلومات حول التحميل على المعالج، ومعلومات حول وقت التحميل الخاص بنظام التشغيل والتطبيقات، ومعلومات حول العمليات قيد التشغيل.

محتويات ملف التتبع لمكون حماية AMSI

يحتوي ملف التتبع AMSI.log إضافة إلى البيانات العامة، معلومات حول نتائج عمليات الفحص التي تم تنفيذها على الطلبات المقدمة من تطبيقات خارجية.

محتويات ملفات التتبع الخاصة بمكون الحماية من تهديدات البريد

قد يحتوي ملف التتبع mcou.OUTLOOK.EXE.log على أجزاء من رسائل بريد إلكتروني، تتضمن عناوين بريد إلكتروني بالإضافة إلى بيانات عامة.

محتويات ملفات التتبع الخاصة بمكون الفحص من قائمة السياق

يحتوي ملف التتبع shellex.dll.log على معلومات تتعلق بإكمال مهمة الفحص والبيانات المطلوبة لتصحيح أخطاء التطبيق، بالإضافة إلى وجود معلومات عامة.

محتويات ملفات تتبع المكون الإضافي للويب الخاص بالتطبيق

يتم تخزين ملفات التتبع الخاصة بالمكون الإضافي للويب للتطبيق على جهاز الكمبيوتر الذي تم نشر Kaspersky Security Center Web Console عليه، في المجلد Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs.

تم تسمية ملفات التتبع الخاصة بالمكون الإضافي لويب التطبيق على النحو التالي: logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log. تبدأ Web Console في كتابة البيانات بعد عملية التثبيت وتقوم بحذف ملفات التتبع بعد إزالة Web Console.

تحتوي ملفات تتبع المكون الإضافي للويب الخاص بالتطبيق على المعلومات التالية بالإضافة إلى البيانات العامة:

- كلمة مرور مستخدم KLAdmin لفتح واجهة Kaspersky Endpoint Security (حماية كلمة المرور).
- كلمة مرور مؤقتة لفتح واجهة Kaspersky Endpoint Security (حماية كلمة المرور).
- اسم المستخدم وكلمة المرور لخادم بريد SMTP (إشعارات البريد الإلكتروني).
- اسم المستخدم وكلمة المرور لخادم وكيل شبكة الإنترنت (الخادم الوكيل).
- اسم المستخدم وكلمة مرور مهمة تغيير مكونات التطبيق.
- بيانات اعتماد الحساب والمسارات المحددة في خصائص مهام وسياسات برنامج Kaspersky Endpoint Security.

محتويات ملف تتبع وكيل المصادقة

يتم تخزين ملف تتبع وكيل المصادقة في المجلد System Volume Information ويكون له الاسم التالي: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

بالإضافة إلى البيانات العامة، يحتوى ملف تتبع وكيل المصادقة على معلومات حول تشغيل وكيل المصادقة والإجراءات التي تم تنفيذها بواسطة المستخدم مع وكيل المصادقة.

تتبع تشغيل التطبيق

تتبع التطبيق عبارة عن سجل تفصيلي للإجراءات التي ينفذها التطبيق، والرسائل عن الأحداث التي تقع أثناء تشغيل التطبيق.

يجب إجراء تتبع التطبيق تحت إشراف فريق الدعم الفني من Kaspersky.

لإنشاء ملف خاص بعمليات تتبع التطبيق:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر .
2. في النافذة التي تفتح، انقر فوق الزر **أدوات الدعم**.
3. استخدم مفتاح التبديل **تمكين تتبع التطبيق** لتمكين أو تعطيل تتبع تشغيل التطبيق.
4. في القائمة المنسدلة **التتبع**، حدد وضع تتبع التطبيق:
   - **مع التدوير**. احفظ عمليات التتبع لعدد محدود من الملفات التي لها حجم محدود واستبدل الملفات الأقدم عند الوصول إلى الحد الأقصى للحجم. في حالة تحديد هذا الوضع، يمكنك تحديد الحد الأقصى من الملفات للتدوير والحجم الأقصى لكل ملف.
   - **الكتابة إلى ملف واحد**. احفظ ملف تتبع واحد (لا يوجد حد للحجم).
5. في القائمة المنسدلة **المستوى**، حدد مستوى التتبع.
   يُنصح بتوضيح مستوى التتبع المطلوب لاختصاصي الدعم الفني. في غياب توجيه الدعم الفني، حدد مستوى التتبع إلى **عادي (500)**.
6. إعادة تشغيل Kaspersky Endpoint Security.
7. لإيقاف عملية التتبع، ارجع إلى النافذة **أدوات الدعم** وقم بتعطيل التتبع.

يمكنك أيضا إنشاء ملفات عمليات التتبع عند تثبيت التطبيق من سطر الأوامر، بما في ذلك استخدام ملف setup.ini.

نتيجة لذلك، سيتم إنشاء ملف تتبع تشغيل التطبيق في المجلد %ProgramData%\Kaspersky Lab\KES.21.13\\Traces. بعد إنشاء ملف التتبع، أرسل الملف إلى فريق الدعم الفني بشركة Kaspersky.

يحذف Kaspersky Endpoint Security تلقائيًا ملفات التتبع عند إزالة التطبيق. ويمكنك أيضًا حذف الملفات يدويًا. ولفعل ذلك، يجب عليك تعطيل التتبع و إيقاف التطبيق.

تتبع أداء التطبيق

يسمح لك برنامج Kaspersky Endpoint Security باستلام معلومات حول مشاكل تشغيل جهاز الكمبيوتر خلال استخدام التطبيق. على سبيل المثال، يمكنك استلام معلومات حول حدوث تأخير عند تحميل نظام التشغيل بعد تثبيت التطبيق. للقيام بذلك، يقوم برنامج Kaspersky Endpoint Security بإنشاء ملفات تتبع الأداء. ويشير تتبع الأداء إلى تسجيل الإجراءات التي ينفذها التطبيق بغرض تشخيص مشاكل أداء تطبيق Kaspersky Endpoint Security. لاستلام معلومات، يستخدم برنامج Kaspersky Endpoint Security خدمة الأحداث لنظام Windows (ETW). فريق الدعم الفني بشركة Kaspersky يكون مسئول عن تشخيص المشاكل الخاصة ببرنامج Kaspersky Endpoint Security وتحديد أسباب هذه المشاكل.

يجب إجراء تتبع التطبيق تحت إشراف فريق الدعم الفني من Kaspersky.

لإنشاء ملف تتبع الأداء:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر .
2. في النافذة التي تفتح، انقر فوق الزر **أدوات الدعم**.
3. استخدم مفتاح التبديل **تمكين تتبع الأداء** لتمكين تتبع أداء التطبيق أو تعطيله.
4. في القائمة المنسدلة **التتبع**، حدد وضع تتبع التطبيق:
   - **مع التدوير**. احفظ عمليات التتبع لعدد محدود من الملفات التي لها حجم محدود واستبدل الملفات الأقدم عند الوصول إلى الحد الأقصى للحجم. في حالة تحديد هذا الوضع، يمكنك تحديد الحجم الأقصى لكل ملف.
   - **الكتابة إلى ملف واحد**. احفظ ملف تتبع واحد (لا يوجد حد للحجم).
5. في القائمة المنسدلة **المستوى**، حدد مستوى التتبع:
   - **خفيف**. يحلل برنامج Kaspersky Endpoint Security أهم عمليات نظام التشغيل المتعلقة بالأداء.
   - **تفصيلي**. يحلل Kaspersky Endpoint Security جميع عمليات نظام التشغيل الرئيسية المتعلقة بالأداء.
6. في القائمة المنسدلة **نوع التتبع**، حدد نوع التتبع:
   - **معلومات أساسية**. يحلل Kaspersky Endpoint Security العمليات أثناء تشغيل نظام التشغيل. استخدم نوع التتبع هذا إذا استمرت المشكلة بعد تحميل نظام التشغيل، على سبيل المثال مشكلة الوصول إلى الإنترنت في المستعرض.
   - **عند إعادة التشغيل**. لا يحلل Kaspersky Endpoint Security العمليات إلا أثناء تحميل نظام التشغيل. بعد تحميل نظام التشغيل، يتوقف برنامج Kaspersky Endpoint Security عن التتبع. استخدم نوع التتبع هذا إذا كانت المشكلة تتعلق بالتأخير في تحميل نظام التشغيل.
7. أعد تشغيل جهاز الكمبيوتر وحاول إعادة إنشاء المشكلة.
8. لإيقاف عملية التتبع، ارجع إلى النافذة **أدوات الدعم** وقم بتعطيل التتبع.

نتيجة لذلك، سيتم إنشاء ملف تتبع أداء في المجلد %ProgramData%\Kaspersky Lab\KES.21.13\Traces folder. بعد إنشاء ملف التتبع، أرسل الملف إلى فريق الدعم الفني بشركة Kaspersky.

تفريغ الكتابة

ملف تفريغ يحتوي على كل المعلومات حول الذاكرة العاملة لعمليات Kaspersky Endpoint Security في لحظة إنشاء ملف التفريغ.

قد تحتوي ملفات التفريغ المحفوظة على بيانات سرية. للتحكم في الوصول إلى البيانات، يجب عليك ضمان أمان ملفات التفريغ بصورة مستقلة.

يتم تخزين ملفات التفريغ على الكمبيوتر طالما أن التطبيق قيد الاستخدام ويتم خذفها نهائيًا عند إزالة التطبيق. يتم تخزين ملفات التفريغ في المجلد `%ProgramData%\Kaspersky Lab\KES.21.13\Traces`.

لتمكين أو تعطيل كتابة التفريغ:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.
3. في القسم **معلومات تتبع الأخطاء**، استخدم خانة الاختيار **تمكين كتابة التفريغ** لتمكين كتابة تفريغ التطبيق أو تعطيله.
4. احفظ تغييراتك.

حماية ملفات التفريغ وملفات التتبع

تحتوي ملفات التفريغ وملفات التتبع على معلومات حول نظام التشغيل، وقد تحتوي أيضًا على بيانات المستخدم. لمنع الوصول غير المصرح به لهذه البيانات، يمكنك تمكين حماية ملفات التفريغ وملفات التتبع.

إذا تم تمكين حماية ملفات التفريغ وملفات التتبع، يمكن الوصول إلى الملفات بواسطة المستخدمين التاليين:

- يمكن الوصول إلى ملفات التفريغ بواسطة مسؤول النظام والمسؤول المحلي، وبواسطة المستخدم الذي قام بتمكين كتابة ملفات التفريغ وملفات التتبع.
- ويمكن الوصول إلى ملفات التتبع بواسطة مسؤول النظام والمسؤول المحلي فقط.

لتمكين أو تعطيل حماية ملفات التفريغ وملفات التتبع:

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة** ← **إعدادات التطبيق**.
3. في القسم **معلومات تتبع الأخطاء**، استخدم خانة الاختيار **تمكين حماية ملفات التفريغ والتتبع** لتمكين حماية الملفات أو تعطيلها.
4. احفظ تغييراتك.

تظل ملفات التفريغ وملفات التتبع التي تمت كتابتها أثناء تفعيل الحماية محمية حتى بعد تعطيل هذه الوظيفة.

القيود والتحذيرات

ينطوي Kaspersky Endpoint Security على عدد من القيود غير المهمة لتشغيل التطبيق.

تثبيت التطبيق

- للحصول على تفاصيل حول الدعم لأنظمة تشغيل Microsoft Windows 10 وMicrosoft Windows Server 2016 وMicrosoft Windows Server 2019، يرجى الرجوع إلى قاعدة معارف الدعم الفني.
- للحصول على تفاصيل حول الدعم لأنظمة تشغيل Windows 11 وMicrosoft Windows Server 2022، الرجاء الرجوع إلى قاعدة معارف الدعم الفني.
- بعد التثبيت على جهاز كمبيوتر مصاب، لا يخبر التطبيق المستخدم بالحاجة إلى إجراء فحص للكمبيوتر. وقد تواجه مشاكل في تفعيل التطبيق. لحل هذه المشكلات، ابدأ فحص المناطق الحرجة.
- في حالة استخدام أحرف غير ASCII (على سبيل المثال، الأحرف الروسية) في ملفي setup.ini وsetup.reg، يُنصح بتحرير الملف باستخدام notepad.exe وحفظ الملف بترميز UTF-16LE. لا يتم دعم أنواع الترميز الأخرى.
- لا يدعم التطبيق استخدام أحرف غير ASCII عند تحديد مسار تثبيت التطبيق في إعدادات حزمة التثبيت.
- عند استيراد إعدادات التطبيق من ملف CFG، لا يتم تطبيق قيمة الإعداد الذي يحدد المشاركة في Kaspersky Security Network. بعد استيراد الإعدادات، يرجى قراءة نص بيان Kaspersky Security Network وتأكيد موافقتك على المشاركة في Kaspersky Security Network. يمكنك قراءة نص البيان في واجهة التطبيق أو في ملف ksn_*.txt الموجود في المجلد الذي يحتوي على مجموعة توزيع التطبيق.
- إذا كنت تريد إزالة التشفير (FLE أو FDE) أو مكون التحكم في الجهاز ثم إعادة تثبيته، فيجب إعادة تشغيل النظام قبل إعادة التثبيت.
- عند استخدام نظام التشغيل Microsoft Windows 10، يجب إعادة تشغيل النظام بعد إزالة مكون التشفير على مستوى الملف (FLE).
- عند إزالة مكونات التطبيق الفردية (على سبيل المثال، باستخدام مهمة تغيير مكونات التطبيق)، قد يلزم إعادة تشغيل الكمبيوتر.
- قد ينتهي تثبيت التطبيق بخطأ يفيد بأنه تم تثبيت تطبيق اسمه مفقود أو غير قابل للقراءة على جهاز الكمبيوتر الخاص بك. وهذا يعني أن التطبيقات غير المتوافقة أو أجزاء منها تظل على جهاز الكمبيوتر الخاص بك. لإزالة عيوب التطبيقات غير المتوافقة، أرسل طلبًا بوصف مفصل للموقف إلى فريق الدعم الفني في Kaspersky عبر حساب شركة Kaspersky.
- إذا ألغيت إزالة التطبيق، فابدأ في استرداده بعد إعادة تشغيل الكمبيوتر.
- يتطلب التطبيق Microsoft .NET Framework 4.0 أو أحدث. يحتوي Microsoft .NET Framework 4.6.1 على ثغرات أمنية. وإذا كنت تستخدم Microsoft .NET Framework 4.6.1، فيجب عليك تثبيت تحديثات الأمان. وللحصول على تفاصيل حول تحديثات أمان Microsoft .NET Framework، يرجى الرجوع إلى موقع ويب الدعم الفني لشركة Microsoft.
- إذا لم ينجح تثبيت التطبيق باستخدام مكون Kaspersky Endpoint Agent المحدد في نظام تشغيل الخادم وظهرت نافذة Windows Installer Coordinator Error، فيرجى الرجوع إلى التعليمات الموجودة على موقع ويب الدعم من Microsoft.
- إذا تم تثبيت التطبيق محليًا في الوضع غير التفاعلي، فاستخدم ملف setup.ini المتوفر لاستبدال المكونات المثبتة.
- بعد تثبيت Kaspersky Endpoint Security for Windows في بعض تكوينات Windows 7، يواصل Windows Defender العمل. ويُنصح بتعطيل Windows Defender يدويًا لمنع تدهور أداء النظام.
- عند تثبيت Kaspersky Endpoint Security for Windows على خادم مُثبت عليه Kaspersky Security for Windows Server (KSWS) وتطبيقات Windows Defender، يجب عليك إعادة تشغيل النظام. ومن الضروري إعادة تشغيل النظام حتى إذا قمت بتمكين تثبيت التطبيق بدون إعادة تشغيل النظام. ويتم تضمين Windows Defender for Windows Server في قائمة البرامج غير المتوافقة مع Kaspersky Endpoint Security for Windows. وقبل تثبيت التطبيق، يقوم المُثبت بإزالة Windows Defender for Windows Server. وتؤدي إزالة البرامج غير المتوافقة إلى ضرورة إعادة تشغيل النظام.
- قبل تثبيت Kaspersky Security for Windows (KES) على خادم مُثبت عليه Kaspersky Endpoint Security for Windows Server (KSWS)، يجب عليك إيقاف تشغيل KSWS Password Protection. وبعد الترحيل من KSWS إلى KES، قم بتمكين الحماية بكلمة مرور في إعدادات التطبيق.
- لتثبيت التطبيق على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 7 أو Windows Server 2008 R2 مع نشر برنامج Veeam Backup & Replication، قد تحتاج إلى إعادة تشغيل الكمبيوتر وتشغيل التثبيت مرة أخرى.

ترقية التطبيق

- بدءًا من إصدار التطبيق 11.0.0، يمكنك تثبيت المكون الإضافي Kaspersky Endpoint Security for Windows MMC فوق إصدار المكون الإضافي السابق. وللعودة إلى إصدار مكون إضافي سابق، احذف المكون الإضافي الحالي وقم بتثبيت إصدار سابق من المكون الإضافي.
- عند ترقية Kaspersky Endpoint Security 11.0.0 for Windows أو 11.0.1، لا يتم حفظ إعدادات جدولة المهام المحلية لمهام التحديث وفحص المناطق الحرجة والفحص المخصص والتحقق السلامة.
- على أجهزة الكمبيوتر التي تعمل بنظام Windows 10 الإصدار 1903 و1909، قد تنتهي الترقيات من Kaspersky Endpoint Security 10 Service Pack 2 Maintenance Release 3 for Windows (الإصدار 10.3.3.275) و Service Pack 2 Maintenance Release 4 (الإصدار 10.3.3.304) و11.0.0 و11.0.1 مع تثبيت مكون التشفير على مستوى الملفات (FLE) بخطأ. وهذا لأن تشفير الملفات غير مدعوم لهذه الإصدارات من Kaspersky Endpoint Security for Windows في الإصدارين 1903 و1909 من Windows 10. قبل تثبيت هذه الترقية، يُنصح بإزالة مكون تشفير الملف.
- يتطلب التطبيق Microsoft .NET Framework 4.0 أو أحدث. يحتوي Microsoft .NET Framework 4.6.1 على ثغرات أمنية. وإذا كنت تستخدم Microsoft .NET Framework 4.6.1، فيجب عليك تثبيت تحديثات الأمان. وللحصول على تفاصيل حول تحديثات أمان Microsoft .NET Framework، يرجى الرجوع إلى موقع ويب الدعم الفني لشركة Microsoft.
- إذا كنت تقوم بترقية إصدار سابق من التطبيق إلى الإصدار 12.1، لتثبيت Kaspersky Endpoint Agent، فأعد تشغيل الكمبيوتر وسجل الدخول إلى النظام باستخدام حساب يمتلك حقوق المسؤول المحلي. وبخلاف ذلك، لن يتم تثبيت Kaspersky Endpoint Agent أثناء إجراء الترقية.
- عند ترقية Kaspersky Endpoint Security، يعطل التطبيق استخدام KSN إلى أن يتم قبول بيان Kaspersky Security Network. وبالإضافة إلى ذلك، يمكن تغيير حالة الكمبيوتر إلى حرجة في Kaspersky Security Center؛ ويتم استلام الحدث خوادم KSN servers غير متاحة. وإذا كنت تستخدم Kaspersky Managed Detection and Response، فستتلقى أحداثًا حول الانتهاكات في تشغيل الحل. ويلزم استخدام KSN لتشغيل Kaspersky Managed Detection and Response. ويتيح Kaspersky Endpoint Security استخدام KSN بعد تطبيق السياسة التي يقبل فيها المسؤول شروط استخدام KSN. وبمجرد قبول بيان Kaspersky Security Network، يستأنف Kaspersky Endpoint Security عمله.
- بعد ترقية Kaspersky Endpoint Security إلى الإصدار 11.10.0 أو أحدث دون إعادة التشغيل، سيحتوي الكمبيوتر على تطبيقين مُثبتين من Kaspersky Endpoint Security. لا تقم بإزالة الإصدار السابق من التطبيق يدويًا. وستتم إزالة الإصدار السابق تلقائيًا عند إعادة تشغيل الكمبيوتر.
- بعد ترقية التطبيق من إصدارات أقدم من Kaspersky Endpoint Security 11 for Windows، يجب إعادة تشغيل الكمبيوتر.

الدعم للأنظمة الأساسية للخادم

- نظام الملفات ReFS مدعوم بقيود:

- قد يعالج Kaspersky Endpoint Security أحداث تنظيف التهديدات بشكل غير صحيح. على سبيل المثال، إذا حذف التطبيق ملفًا خبيثًا، فقد يحتوي التقرير على إدخال كائن لم تتم معالجته. وفي الوقت نفسه، ينظف Kaspersky Endpoint Security التهديدات وفقًا لإعدادات التطبيق. يستطيع Kaspersky Endpoint Security أيضًا إنشاء نسخة مكررة من حدث سيتم تنظيف الكائن عند إعادة التشغيل للكائن نفسه.

- قد تتخطى الحماية من تهديدات الملفات بعض التهديدات. وفي الوقت نفسه، يعمل فحص البرامج الضارة بشكل صحيح.

- بعد بدء مهمة فحص البرامج الضارة، تتم إعادة تعيين الاستثناءات التي تمت إضافتها باستخدام iChecker عند إعادة تشغيل الخادم.

- لا يتم دعم تقنية iSwift. لا يضع Kaspersky Endpoint Security في الاعتبار استثناءات الفحص المضافة باستخدام تقنية iSwift.

- لا يكتشف Kaspersky Endpoint Security ملفات eicar.com وsusp-eicar.com إذا كان ملف meicar.exe موجودًا على الكمبيوتر قبل تثبيت Kaspersky Endpoint Security.

- قد يعرض Kaspersky Endpoint Security إخطارات تنظيف التهديدات بشكل غير صحيح. على سبيل المثال، قد يعرض التطبيق إخطار تهديد لتهديد سبق تنظيفه.

- لا يتم دعم تقنيات التشفير على مستوى الملف (FLE) وتشفير القرص من Kaspersky (FDE) على الأنظمة الأساسية للخادم. وفي الوقت نفسه، قد يعالج Kaspersky Endpoint Security أحداث تشفير البيانات بشكل غير صحيح.

- في أنظمة تشغيل الخادم، لا يتم عرض أي تحذير بخصوص الحاجة إلى التنظيف المتقدم.

- تم استبعاد نظام التشغيل Microsoft Windows Server 2008 من الدعم. - لا يتم دعم تثبيت التطبيق على جهاز كمبيوتر يعمل بنظام التشغيل Microsoft Windows Server 2008.

- من الممكن أن يتسبب تثبيت Kaspersky Endpoint Security على خادم يتضمن (Microsoft Data Protection Manager (DPM في حدوث خلل في DPM. ويتعلق بالقيود في تشغيل DPM. وللقضاء على الأعطال، يجب عليك إضافة محركات الخادم المحلي إلى الاستثناءات لمكون الحماية من تهديدات الملفات ومهام فحص البرامج الضارة .

- الوضع الأساسي مدعوم مع قيود:

- لا تتوافر واجهة المستخدم الرسومية المحلية، بما في ذلك الإشعارات والإشعارات المنبثقة وعناصر التحكم الأخرى الخاصة بالواجهة. ولا يستطيع التطبيق عرض نوافذ المطالبة، بما في ذلك النوافذ التالية:

  - مطالبة تأكيد إصدار التطبيق وترقية الوحدة النمطية؛

  - مطالبة إعادة تشغيل الكمبيوتر؛

  - المطالبة الخاصة ببيانات اعتماد مصادقة الخادم الوكيل.

  - مطالبة للوصول إلى جهاز (التحكم في الجهاز).

- المكونات التالية غير متوفرة: الحماية من تهديدات الويب، والحماية من تهديدات البريد، والتحكم في الويب، ومنع هجمات USB الخبيثة.

- منع تعدد الاتصال غير متاح.

- يمكنك فقط قبول بيان Kaspersky Security Network في سياسة التطبيق في وحدة تحكم Kaspersky Security Center.

- لا يتوفر تشفير محرك الأقراص من BitLocker إلا مع الوحدة النمطية للنظام الأساسي الموثوق بها (TPM). ولا يمكن استخدام رمز PIN / كلمة مرور للتشفير لأن التطبيق لا يستطيع عرض نافذة المطالبة بكلمة المرور للمصادقة على التمهيد المسبق. وفي حالة تمكين وضع التوافق مع معيار معالجة المعلومات الفيدرالي (FIPS) في نظام التشغيل، فيرجى توصيل محرك أقراص قابل للإزالة لحفظ مفتاح التشفير قبل أن تبدأ في تشفير محرك الأقراص.

الدعم للأنظمة الأساسية الافتراضية

- لا يتم دعم تشفير القرص بالكامل (FDE) على أجهزة Hyper-V الافتراضية.
- لا يتم دعم تشفير القرص بالكامل (FDE) على الأنظمة الأساسية الافتراضية من Citrix.
- يتم دعم جلسات Windows 10 Enterprise المتعددة مع قيود:
  - يُنظف Kaspersky Endpoint Security التهديدات النشطة دون إخطار المستخدم، تمامًا كما يفعل عند تنظيف التهديدات النشطة على الخوادم. نظرًا لاستمرار عمل نظام التشغيل في وضع الجلسات المتعددة، قد يفقد المستخدمون النشطون الآخرون بياناتهم إذا لم يتم حل التهديد على الفور.
  - لا يتم دعم تشفير القرص الكامل (FDE).
  - لا يتم دعم إدارة BitLocker.
  - لا يتم دعم استخدام Kaspersky Endpoint Security مع محركات الأقراص القابلة للإزالة. تُعرف البنية التحتية لمنصة Microsoft Azure محركات الأقراص القابلة للإزالة كمحركات أقراص شبكة.
- لا يتم دعم التثبيت واستخدام التشفير على مستوى الملفات (FLE) على الأنظمة الأساسية الافتراضية من Citrix.
- لدعم توافق Kaspersky Endpoint Security for Windows مع Citrix PVS، نفذ التثبيت من خلال تمكين خيار **تأكيد التوافق مع Citrix PVS**. ويمكن تمكين هذا الخيار في معالج الإعداد أو باستخدام معلمة سطر الأوامر `/pCITRIXCOMPATIBILITY=1`. في حالة التثبيت عن بُعد، يجب تحرير ملف KUD عن طريق إضافة المعلمة التالية: `/pCITRIXCOMPATIBILITY=1`.
- Citrix XenDesktop. قبل بدء الاستنساخ، يجب عليك تعطيل الدفاع الذاتي لاستنساخ الأجهزة الافتراضية التي تستخدم vDisk.
- عند إعداد آلة قالب للصورة الرئيسية لتطبيق Citrix XenDesktop مع Kaspersky Endpoint Security for Windows وKaspersky Security Center Network Agent المُثبت مسبقًا، أضف الأنواع التالية من الاستثناءات إلى ملف التكوين:

```
[Rule-Begin]
Type=File-Catalog-Construction
Action=Catalog-Location-Guest-Modifiable
name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
[Rule-End]
```

للحصول على تفاصيل حول Citrix XenDesktop، يرجى زيارة موقع ويب دعم Citrix.

- في بعض الحالات، قد تفشل محاولة فصل محرك أقراص قابل للإزالة بأمان على جهاز افتراضي يتم نشره على Hypervisor VMware ESXi. حاول فصل الجهاز بأمان مرة أخرى.

التوافق مع Kaspersky Security Center

- لا يمكنك إدارة مكون التحكم غير الطبيعي التكيفي إلا في الإصدار 11 من Kaspersky Security Center أو أحدث.
- قد لا يعرض تقرير تهديد Kaspersky Security Center 11 معلومات حول الإجراء المتخذ بشأن التهديدات التي تم اكتشافها بواسطة حماية AMSI.
- في الإصدار 14.1 من Kaspersky Security Center Web Console والإصدارات الأقدم، لا يتم عرض أسماء المناطق الوظيفية لمكونات فحص السجل ومراقب سلامة الملف بشكل صحيح في قسم إعدادات أذونات وصول المستخدم في خصائص خادم الإدارة.
- يوفر Kaspersky Security Center Linux دعمًا محدودًا لبرنامج Kaspersky Endpoint Security. وللمزيد من التفاصيل عن قيود الدعم، راجع تعليمات Kaspersky Security Center Linux 14.2 أو تعليمات Kaspersky Security Center Linux 15.

الترخيص

- في حالة عرض رسالة النظام خطأ في استلام البيانات، فتحقق من أن الكمبيوتر الذي تنفذ عليه التفعيل لديه وصول إلى شبكة الاتصال، أو كوّن إعدادات التفعيل عبر الخادم الوكيل للتفعيل على Kaspersky Security Center.
- لا يمكن تفعيل التطبيق بواسطة اشتراك عبر Kaspersky Security Center إذا انتهت صلاحية الترخيص أو إذا كان الترخيص التجريبي فعالاً على الكمبيوتر. ولاستبدال ترخيص تجريبي أو ترخيص على وشك انتهاء صلاحيته بترخيص اشتراك آخر، استخدم مهمة توزيع الترخيص.
- في واجهة التطبيق، يتم عرض تاريخ انتهاء صلاحية الترخيص بالتوقيت المحلي للكمبيوتر.
- قد يؤدي تثبيت التطبيق بملف مفتاح مضمن على جهاز كمبيوتر به وصول غير مستقر إلى الإنترنت إلى العرض المؤقت للأحداث الذي يشير إلى أن التطبيق لم يتم تفعيله أو أن الترخيص لا يسمح بتشغيل المكون. وذلك لأن التطبيق يقوم أولاً بتثبيت ومحاولة تفعيل الترخيص التجريبي المضمن، الذي يتطلب الوصول إلى الإنترنت للتفعيل أثناء إجراء التثبيت.
- أثناء الفترة التجريبية، قد يؤدي تثبيت أي ترقية أو تصحيح للتطبيق على جهاز كمبيوتر به وصول غير مستقر إلى الإنترنت إلى عرض مؤقت للأحداث يفيد بأن التطبيق لم يتم تفعيله. وذلك لأن التطبيق يقوم مرة أخرى بتثبيت ومحاولة تفعيل الترخيص التجريبي المضمن، الذي يتطلب الوصول إلى الإنترنت للتفعيل عند تثبيت الترقية.
- في حالة تفعيل الترخيص التجريبي تلقائيًا أثناء تثبيت التطبيق ثم تمت إزالة التطبيق دون حفظ معلومات الترخيص، فلن يتم تفعيل التطبيق تلقائيًا باستخدام الترخيص التجريبي عند إعادة تثبيته. وفي هذه الحالة، قم بتفعيل التطبيق يدويًا.
- إذا كنت تستخدم الإصدار 11 من Kaspersky Security Center والإصدار 12.1 من Kaspersky Endpoint Security، فقد تعمل تقارير أداء المكونات بشكل غير صحيح. وإذا قمت بتثبيت مكونات Kaspersky Endpoint Security غير المضمنة في ترخيصك، فقد يرسل وكيل الشبكة أخطاء حالة المكون إلى سجل أحداث Windows. ولتجنب الأخطاء، قم بإزالة المكونات غير المضمنة في ترخيصك.

الحماية من تهديدات البريد

- عند فحص البريد باستخدام ملحق الحماية من تهديدات البريد لبرنامج Microsoft Outlook، يُنصح باستخدام وضع Exchange المخزن مؤقتًا (خيار استخدام وضع Exchange المخزن مؤقتًا).
- لا يدعم Kaspersky Endpoint Security إصدار 64 بت من عميل البريد MS Outlook. وهذا يعني أن Kaspersky Endpoint Security لا يفحص ملفات MS Outlook (ملفات PST وOST) في حالة تثبيت إصدار 64 بت من MS Outlook على الكمبيوتر، حتى إذا كان البريد مضمنًا في نطاق الفحص.

محرك المعالجة

- يقوم التطبيق باستعادة الملفات في الأجهزة التي تحتوي على نظام الملف NTFS أو FAT32 فقط.
- يمكن للتطبيق استعادة الملفات التي تحمل الملحقات التالية: odt أو ods أو odp أو odm أو odc أو odb أو doc أو docx أو docm أو wps أو xls أو xlsx أو xlsm أو xlsb أو xlk أو ppt أو pptx أو pptm أو mdb أو accdb أو pst أو dwg أو dxf أو dxg أو wpd أو rtf أو wb2 أو pdf أو mdf أو dbf أو psd أو pdd أو eps أو ai أو indd أو cdr أو jpg أو jpe أو dng أو 3fr أو arw أو srf أو sr2 أو bay أو crw أو cr2 أو dcr أو kdc أو erf أو mef أو mrw أو nef أو nrw أو orf أو raf أو raw أو rwl أو rw2 أو r3d أو ptx أو pef أو srw أو x3f أو der أو cer أو crt أو pem أو pfx أو p12 أو p7b أو p7c أو 1cd.
- من غير الممكن استعادة الملفات الموجودة على محركات الشبكة أو على محركات الأقراص / أقراص DVD القابلة لإعادة الكتابة.
- من غير الممكن استعادة الملفات التي تم تشفيرها باستخدام نظام تشفير الملفات (EFS). للحصول على المزيد من المعلومات حول نظام تشفير الملفات (EFS)، يُرجى زيارة Microsoft website.
- لا يراقب التطبيق عمليات التعديل على الملفات التي تم إجراؤها من قبل العمليات على مستوى نظام تشغيل kernel.
- لا يراقب التطبيق عمليات التعديل التي تم إجراؤها على الملفات عبر واجهة الشبكة (على سبيل المثال، إذا تم تخزين ملف ما في مجلد مشترك وتم بدء تشغيل عملية عن بُعد من جهاز كمبيوتر آخر).

جدار الحماية

- يتم دعم تصفيه الحزم أو الاتصالات حسب العنوان المحلي والواجهة الفعلية ومدة بقاء الحزمة (TTL) في الحالات التالية:
  - حسب العنوان المحلي للحزم الصادرة أو الاتصالات في قواعد التطبيق لقواعد TCP وUDP والحزم.
  - حسب العنوان المحلي للحزم أو الاتصالات الواردة (باستثناء UDP) في قواعد منع التطبيق وقواعد الحزمة.
  - حسب مدة بقاء (TTL) الحزمة في منع قواعد الحزمة للحزم الواردة أو الصادرة.
  - حسب واجهة الشبكة للحزم الواردة والصادرة أو الاتصالات في قواعد الحزمة.
- في إصدارات التطبيق 11.0.0 و11.0.1، يتم تطبيق عناوين MAC المحددة بشكل غير صحيح. إعدادات عنوان MAC للإصدارات 11.0.0 و11.0.1 و11.1.0 أو أحدث غير متوافقة. بعد ترقية التطبيق أو المكون الإضافي من هذه الإصدارات إلى الإصدار 11.1.0 أو أحدث، يجب عليك التحقق من عناوين MAC المحددة وإعادة تكوينها في قواعد جدار الحماية.
- عند ترقية التطبيق من الإصدارين 11.1.1 و11.2.0 إلى الإصدار 12.1، لا يتم ترحيل حالات الأذونات لقواعد جدار الحماية التالية:
  - طلبات لخادم DSN عبر TCP.
  - طلبات لخادم DSN عبر UDP.
  - أي نشاط للشبكة.
  - الاستجابات الواردة لوجهات ICMP التي يتعذر الوصول إليها.
  - تدفق ICMP الوارد.
- إذا كوّنت محول شبكة أو مدة بقاء الحزمة (TTL) لقاعدة حزمة سماح، فإن أولوية هذه القاعدة أقل من قاعدة تطبيق الحظر. بمعنى آخر، في حالة حظر نشاط الشبكة لأحد التطبيقات (على سبيل المثال، التطبيق موجود في مجموعة الثقة مقيد بشكل عالٍ)، فلا يمكنك السماح بنشاط الشبكة للتطبيق باستخدام قاعدة الحزمة مع هذه الإعدادات. وفي جميع الحالات الأخرى، تكون أولوية قاعدة الحزمة أعلى من قاعدة شبكة التطبيق.
- عند استيراد قواعد حزمة جدار الحماية، قد يجري Kaspersky Endpoint Security تعديلاً على أسماء القواعد. ويحدد التطبيق القواعد بمجموعات متطابقة من المعلمات العامة: البروتوكول والاتجاه والمنافذ البعيدة والمحلية ومدة بقاء الحزمة (TTL). وإذا كانت هذه المجموعة من المعلمات الرئيسية مطابقة لقواعد متعددة، فسيعين التطبيق الاسم نفسه لهذه القواعد أو يضيف علامة معلمة إلى الاسم. بهذه الطريقة، يستورد Kaspersky Endpoint Security جميع قواعد الحزمة، لكن يمكن تعديل اسم القواعد التي تتضمن إعدادات عامة متطابقة.
- إذا قمت بتمكين الإبلاغ عن حدث التطبيق في قاعدة الشبكة، عند نقل التطبيق إلى مجموعة ثقة مختلفة، فلن يتم تطبيق قيود مجموعة الثقة هذه. وبالتالي، إذا كان التطبيق في مجموعة ثقة موثوقة، فلن يكون له أي قيود على الشبكة. ثم قمت بتمكين الإبلاغ عن الأحداث لهذا التطبيق ونقلته إلى مجموعة الثقة غير الموثوق بها. ولن يفرض جدار الحماية قيود الشبكة لهذا التطبيق. ونوصي أولاً بنقل التطبيق إلى مجموعة الثقة المناسبة ثم تمكين الإبلاغ عن الأحداث. وإذا لم تكن هذه الطريقة مناسبة، فيمكنك تكوين قيود التطبيق يدويًا في إعدادات قاعدة الشبكة. وينطبق التقييد فقط على الواجهة المحلية للتطبيق. ويعمل نقل التطبيق بين مجموعات الثقة في السياسة بشكل صحيح.
- يحتوي مكونا جدار الحماية ومنع الاختراق على إعدادات مشتركة: حقوق التطبيق والموارد المحمية. وإذا أجريت تغييرات على إعدادات جدار الحماية، فسوف يطبق Kaspersky Endpoint Security تلقائيًا الإعدادات الجديدة على منع الاختراق. على سبيل المثال، إذا سمحت بإجراء تغييرات على الإعدادات العامة لسياسة جدار الحماية (القفل مفتوح)، فستصبح إعدادات منع الاختراق قابلة للتحرير أيضًا.
- عند تشغيل قاعدة حزمة شبكة في Kaspersky Endpoint Security 11.6.0 أو إصدار أقدم، سيعرض العمود **اسم التطبيق** في تقرير جدار الحماية دائمًا قيمة Kaspersky Endpoint Security. بالإضافة إلى ذلك، سيحظر جدار الحماية الاتصال على مستوى الحزمة لجميع التطبيقات. وتم تعديل هذا السلوك لبرنامج Kaspersky Endpoint Security 11.7.0 أو أحدث. تمت إضافة العمود **نوع القاعدة** إلى تقرير جدار الحماية. عند تشغيل قاعدة حزمة الشبكة، تظل القيمة الموجودة في عمود **اسم التطبيق** فارغة.

منع هجمات BadUSB

- يعيد Kaspersky Endpoint Security تعيين مهلة قفل جهاز USB عند قفل الكمبيوتر (على سبيل المثال، انقضاء مهلة قفل الشاشة). أي، إذا أدخلت رمزًا خاطئًا لمصادقة جهاز USB عدة مرات وأغلق التطبيق جهاز USB، فإن Kaspersky Endpoint Security يسمح لك بتكرار محاولة المصادقة بعد إلغاء قفل الكمبيوتر. وفي هذه الحالة، لا يقفل Kaspersky Endpoint Security جهاز USB لفترة محددة في إعدادات مكون منع هجمات BadUSB.

- ويعيد Kaspersky Endpoint Security تعيين مهلة قفل جهاز USBعند إيقاف حماية الكمبيوتر مؤقتًا. أي، إذا أدخلت رمزًا خاطئًا لمصادقة جهاز USB عدة مرات وأغلق التطبيق جهاز USB، فإن Kaspersky Endpoint Security يسمح لك بتكرار محاولة المصادقة بعد استئناف حماية الكمبيوتر. وفي هذه الحالة، لا يقفل Kaspersky Endpoint Security جهاز USB لفترة محددة في إعدادات مكون منع هجمات BadUSB.

التحكم في التطبيقات

- يتم دعم أرشيفات ZIP التي يقل حجمها عن 104 ميجا بايت فقط عند إدارة قواعد التحكم في التطبيقات في Kaspersky Security Center Web Console. ولا يتم دعم الأرشيفات بتنسيقات أخرى، مثل RAR أو 7z. ولا يوجد مثل هذا التقييد إذا كنت تعمل مع قواعد التحكم في التطبيقات في وحدة تحكم الإدارة (MMC).

- عند العمل في Microsoft Windows 10 في وضع قائمة الرفض للتطبيق، قد يتم تطبيق قواعد المنع بشكل غير صحيح، مما قد يتسبب في منع التطبيقات غير المحددة في القواعد.

- عندما يتم حظر تطبيقات الويب التقدمية (PWA) بواسطة مكون التحكم في التطبيقات، يُشار إلى appManifest.xml على أنه التطبيق الممنوع في التقرير.

- عند إضافة تطبيق Notepad القياسي إلى قاعدة التحكم في التطبيقات لنظام التشغيل Windows 11، لا يوصى بتحديد المسار إلى التطبيق. وعلى أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 11، يستخدم نظام التشغيل برنامج Metro Notepad الموجود في المجلد C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe. وفي الإصدارات السابقة من نظام التشغيل، يوجد برنامج Notepad في المجلدات التالية:

  - C:\Windows\notepad.exe

C:\Windows\System32\notepad.exeC:\Windows\SysWOW64\notepad.exe

عند إضافة برنامج Notepad إلى قاعدة التحكم في التطبيقات، يمكنك تحديد اسم التطبيق وتجزئة الملف من خصائص التطبيق قيد التشغيل، على سبيل المثال.

التحكم في الجهاز

- تم حظر الوصول إلى أجهزة الطابعة التي تمت إضافتها إلى القائمة الموثوقة بواسطة قواعد منع الجهاز والناقل.
- لأجهزة MTP، يتم دعم التحكم في عمليات القراءة والكتابة والاتصال إذا كنت تستخدم برامج تشغيل Microsoft في نظام التشغيل. إذا قام المستخدم بتثبيت برنامج تشغيل مخصص للعمل مع جهاز (على سبيل المثال، كجزء من iTunes أو Android Debug Bridge)، فقد لا يعمل التحكم في عمليات القراءة والكتابة.
- عند العمل مع أجهزة MTP، يتم تغيير قواعد الوصول بعد إعادة توصيل الجهاز.
- يسجل مكون التحكم في الجهاز الأحداث المتعلقة بالأجهزة التي يتم مراقبتها، مثل توصيل الجهاز وفصله وقراءة ملف من الجهاز وكتابة ملف إلى الجهاز والأحداث الأخرى. يسجل Kaspersky Endpoint Security أحداث انقطاع الاتصال لأنواع الأجهزة التالية فقط: أجهزة محمولة (MTP) ومحركات الأقراص القابلة للإزالة والأقراص المرنة ومحركات أقراص CD/DVD. وبالنسبة لأنواع الأجهزة الأخرى ، لا يسجل التطبيق أحداث انقطاع الاتصال. ويسجل التطبيق عملية توصيل الجهاز بالكمبيوتر لجميع أنواع الأجهزة.
- إذا كنت تضيف جهازًا إلى القائمة الموثوقة استنادًا إلى قناع طراز وتستخدم الأحرف المضمنة في المعرّف لكن ليس في اسم الطراز، فلن تتم إضافة هذه الأجهزة. على محطة عمل، ستتم إضافة هذه الأجهزة إلى القائمة الموثوقة بناءً على قناع معرّف.
- على أجهزة الكمبيوتر المُثبت عليها الإصدار 12.0 من Kaspersky Endpoint Security، فإن وضع الوصول إلى الطابعة **السماح وعدم التسجيل** لنوع الجهاز **طابعات الشبكة** يسمى **يعتمد على ناقل الاتصال**، إذا تم تطبيق سياسة الإصدار 12.1 من Kaspersky Endpoint Security على الكمبيوتر. وفي هذه الأوضاع، ينفذ التطبيق الإجراءات نفسها. وفي الإصدار 12.1 من Kaspersky Endpoint Security، تمت تسمية وضع الوصول لطابعات الشبكة بشكل صحيح **السماح وعدم التسجيل**.
- بدءًا من Kaspersky Endpoint Security 12.0 لنظام التشغيل Windows، يسمح التطبيق بتكوين قواعد الطباعة للطابعات (التحكم في الطباعة). وبعد تثبيت التطبيق مع التحكم في الطباعة أو ترقية التطبيق إلى إصدار مع التحكم في الطباعة، يجب إعادة تشغيل الكمبيوتر. وإلى أن تتم إعادة تشغيل الكمبيوتر، لا يطبق Kaspersky Endpoint Security قواعد الطباعة ويمكنه فقط التحكم في الوصول إلى الطابعات. وإذا كانت إعادة تشغيل الكمبيوتر تؤثر سلبًا على سير العمل في مؤسستك، فيمكنك إعادة تشغيل خدمة التخزين المؤقت فقط (التخزين المؤقت للطباعة).
- تُصنف أجهزة Apple كأجهزة محمولة (MTP) وأجهزة iTunes. من الممكن أن يتعرف نظام التشغيل على توصيل جهاز Apple بشكل غير صحيح وعدم تحديد جهاز Apple كجهاز محمول (MTP). لذلك لن يكون جهاز Apple متاحًا في مدير الملفات، لكن يمكن الوصول إليه في تطبيق iTunes. ونتيجة لذلك، سيتحكم Kaspersky Endpoint Security في الوصول إلى جهاز Apple في تطبيق iTunes فقط. للوصول إلى جهاز Apple كجهاز محمول (MTP)، تحتاج إلى الانتقال إلى Device Manager (إدارة الأجهزة) وإزالة برنامج تشغيل Apple Mobile Device USB من قائمة USB Controllers (وحدات تحكم USB). بعد إعادة تشغيل الكمبيوتر، سيحدد نظام التشغيل جهاز Apple كجهاز محمول (MTP) وجهاز iTunes. سيتحكم Kaspersky Endpoint Security في الوصول إلى الجهاز في كل من تطبيق iTunes ومدير الملفات.

التحكم في الويب

- لا يتم دعم تنسيقات OGV وWEBM.
- لا يتم دعم بروتوكول RTMP.

مراقبة عيوب التكيف

- يوصى بإنشاء استثناءات تلقائيًا بناءً على الحدث. عند إضافة استثناءً يدويًا، أضف الحرف * إلى بداية المسار عند تحديد الكائن الهدف.
- لا يمكن إنشاء تقرير قواعد التحكم غير الطبيعي التكيفي إذا تضمن النموذج حتى حدثًا واحدًا يحتوي اسمه على أكثر من 260 حرفًا.
- لا يتم دعم إضافة استثناءات من مستودع تشغيل قواعد التحكم غير الطبيعي التكيفي إذا كانت خصائص كائن أو عملية تحتوي على قيمة تتكون من أكثر من 256 حرفًا (على سبيل المثال، المسار إلى الكائن الهدف). ويمكنك إضافة استثناء يدويًا في إعدادات السياسة. ويمكنك أيضًا إضافة استثناء في التقرير حول قواعد التحكم غير الطبيعي التكيفي التي تم تشغيلها.

تشفير محرك الأقراص (FDE)

- بعد تثبيت التطبيق، يجب إعادة تشغيل نظام التشغيل حتى يعمل تشفير محرك الأقراص الصلبة بشكل صحيح.
- لا يدعم وكيل المصادقة الهيروغليفية أو الحرفين الخاصين | و\.
- للحصول على أفضل أداء للكمبيوتر بعد التشفير، من الضروري أن يدعم المعالج مجموعة تعليمات AES-NI (التعليمات الجديدة لمعيار التشفير المتقدم من Intel). وإذا كان المعالج لا يدعم AES-NI، فقد ينخفض أداء الكمبيوتر.
- عند وجود عمليات تحاول الوصول إلى الأجهزة المشفرة قبل أن يمنح التطبيق الوصول إلى هذه الأجهزة، يعرض التطبيق تحذيرًا يفيد بوجوب إنهاء هذه العمليات. إذا تعذر إنهاء العمليات، فأعد توصيل الأجهزة المشفرة.
- يتم عرض المعرفات الفريدة لمحركات الأقراص الصلبة في إحصاءات تشفير الجهاز بتنسيق معكوس.
- لا يوصى بتهيئة الأجهزة أثناء تشفيرها.
- عندما يتم توصيل عدة محركات أقراص قابلة للإزالة في وقت واحد بجهاز كمبيوتر، يمكن تطبيق سياسة التشفير على محرك أقراص واحد فقط قابل للإزالة. عند إعادة توصيل الأجهزة القابلة للإزالة، يتم تطبيق سياسة التشفير بشكل صحيح.
- قد يفشل بدء التشفير على محرك قرص صلب مجزأ بدرجة كبيرة. وقم بإلغاء تجزئة القرص الصلب.
- عندما يتم تشفير محركات الأقراص الصلبة، يتم حظر الإسبات من الوقت الذي تبدأ فيه مهمة التشفير حتى إعادة التشغيل الأولى لجهاز كمبيوتر يعمل بنظام التشغيل Microsoft Windows 7/8/8.1/10، وبعد تثبيت تشفير محرك الأقراص الصلبة حتى عملية إعادة التشغيل الأولى لأنظمة التشغيل Microsoft Windows 8/8.1/10. عندما يتم فك تشفير محركات الأقراص الصلبة، يتم منع الإسبات من وقت فك تشفير محرك أقراص التمهيد بالكامل حتى عملية إعادة التشغيل الأولى لنظام التشغيل. عند تمكين خيار **البدء السريع** في Microsoft Windows 8/8.1/10، يمنعك حظر الإسبات من إيقاف تشغيل النظام.
- لا تسمح أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 7 بتغيير كلمة المرور أثناء الاسترداد عندما يتم تشفير القرص بتقنية BitLocker. وبعد إدخال مفتاح الاسترداد وتحميل نظام التشغيل، لن يطالب Kaspersky Endpoint Security المستخدم بتغيير كلمة المرور أو رمز PIN. وبالتالي، من المستحيل تعيين كلمة مرور جديدة أو رمز PIN جديد. وتنشأ هذه المشكلة من خصوصيات نظام التشغيل. وللمتابعة، تحتاج إلى إعادة تشفير محرك الأقراص الصلبة.
- لا يوصى باستخدام أداة xbootmgr.exe عند تمكين موفري خدمة إضافيين. على سبيل المثال، المرسل أو الشبكة أو محركات الأقراص.
- لا يتم دعم تهيئة محرك أقراص قابل للإزالة مشفر على جهاز كمبيوتر مُثبت عليه Kaspersky Endpoint Security for Windows.
- لا يتم دعم تهيئة محرك أقراص قابل للإزالة مشفر باستخدام نظام الملفات FAT32 (يتم عرض محرك الأقراص على أنه مشفر). لتهيئة محرك أقراص، قم بإعادة تهيئته إلى نظام ملفات NTFS.
- للحصول على تفاصيل حول استعادة نظام تشغيل من نسخة احتياطية إلى جهاز GPT مشفر، يرجى بزيارة قاعدة معارف الدعم الفني.
- لا يمكن أن تتواجد عوامل تنزيل متعددة على جهاز كمبيوتر مشفر واحد.
- من المستحيل الوصول إلى محرك أقراص قابل للإزالة مشفر مسبقًا على جهاز كمبيوتر مختلف عندما يتم استيفاء جميع الشروط التالية في وقت واحد:
  - لا يوجد اتصال بخادم Kaspersky Security Center.
  - يحاول المستخدم المصادقة برمز مميز جديد أو كلمة مرور جديدة.

  في حالة حدوث موقف مشابه، أعد تشغيل الكمبيوتر. بعد إعادة تشغيل التطبيق، سيتم منح الوصول إلى محرك الأقراص القابل للإزالة المشفر.
- قد يكون اكتشاف أجهزة USB بواسطة وكيل المصادقة غير مدعوم عند تمكين وضع xHCI لمنفذ USB في إعدادات BIOS.
- لا يتم دعم تشفير القرص من Kaspersky (FDE) لجزء SSD من الجهاز المستخدم للتخزين المؤقت للبيانات الأكثر استخدامًا لأجهزة SSHD.
- لا يتم دعم تشفير محركات الأقراص الصلبة في أنظمة تشغيل Microsoft Windows 8/8.1/10 بنظام 32 بت التي تعمل في وضع UEFI.

- أعد تشغيل الكمبيوتر قبل إعادة تشفير محرك الأقراص الصلبة الذي تم فك تشفيره مرة أخرى.
- لا يتوافق تشفير محرك الأقراص الصلبة مع Kaspersky Anti-Virus for UEFI. لا يوصى باستخدام تشفير محرك الأقراص الصلبة على أجهزة الكمبيوتر المثبت عليها تطبيق Kaspersky Anti-Virus for UEFI.
- يتم دعم إنشاء حسابات وكيل المصادقة استنادًا إلى حسابات Microsoft مع القيود التالية:
  - لا يتم دعم تقنية تسجيل الدخول الأحادي.
  - لا يتم دعم الإنشاء التلقائي لحسابات وكيل المصادقة في حالة تحديد خيار إنشاء حسابات للمستخدمين الذين سجلوا الدخول إلى النظام في آخر N يومًا (أيام).
- إذا كان اسم حساب وكيل المصادقة بتنسيق <Windows اسم حساب/المجال>، بعد تغيير اسم الكمبيوتر، تحتاج أيضًا إلى تغيير أسماء الحسابات التي تم إنشاؤها للمستخدمين المحليين لهذا الكمبيوتر. على سبيل المثال، تخيل وجود مستخدم محلي باسم Ivanov على كمبيوتر Ivanov، وتم إنشاء حساب وكيل مصادقة باسم Ivanov/Ivanov لهذا المستخدم. وفي حالة تغيير اسم الكمبيوتر Ivanov إلى Ivanov-PC، فأنت بحاجة إلى تغيير اسم حساب وكيل المصادقة للمستخدم Ivanov من Ivanov/Ivanov إلى Ivanov-PC/Ivanov. ويمكنك تغيير اسم الحساب باستخدام مهمة إدارة الحساب المحلي لوكيل المصادقة. وقبل تغيير اسم الحساب، يمكن المصادقة في بيئة ما قبل التمهيد باستخدام الاسم القديم (على سبيل المثال، Ivanov/Ivanov).
- في حالة السماح لمستخدم بالوصول إلى جهاز كمبيوتر تم تشفيره باستخدام تقنية تشفير القرص من Kaspersky فقط باستخدام رمز مميز ويحتاج هذا المستخدم لإكمال إجراء استرداد الوصول، فتأكد من منح هذا المستخدم حق الوصول المستند إلى كلمة المرور إلى هذا الكمبيوتر بعد استعادة الوصول إلى الكمبيوتر المشفر. وقد لا يتم حفظ كلمة المرور التي عينها المستخدم عند استعادة الوصول. وفي هذه الحالة، سيتعين على المستخدم إكمال إجراء استعادة الوصول إلى الكمبيوتر المشفر مجددًا في المرة التالية التي يتم فيها إعادة تشغيل الكمبيوتر.
- عند فك تشفير محرك أقراص صلبة باستخدام أداة استرداد FDE، قد تنتهي عملية فك التشفير بخطأ في حالة الكتابة فوق البيانات الموجودة على الجهاز المصدر بالبيانات التي تم فك تشفيرها. وسيظل جزء من البيانات الموجودة على محرك الأقراص الصلبة مشفرًا. ويوصى بتحديد خيار حفظ البيانات التي تم فك تشفيرها في ملف في إعدادات فك تشفير الجهاز عند استخدام أداة استرداد FDE.
- في حالة تغيير كلمة مرور وكيل المصادقة، ستظهر رسالة تحتوي على نص تم تغيير كلمة المرور الخاصة بك بنجاح.تظهر انقر فوق موافق، ثم يعيد المستخدم تشغيل جهاز الكمبيوتر، ولا يتم حفظ كلمة المرور الجديدة. ويجب استخدام كلمة المرور القديمة للمصادقة اللاحقة في بيئة ما قبل التمهيد.
- لا يتوافق تشفير القرص مع تقنية Intel Rapid Start.
- لا يتوافق تشفير القرص مع تقنية ExpressCache.
- في بعض الحالات، عند محاولة فك تشفير محرك أقراص مشفر باستخدام أداة استرداد FDE، تكتشف الأداة عن طريق الخطأ حالة الجهاز على أنها "غير مشفرة" بعد اكتمال إجراء "استجابة الطلب". ويعرض سجل الأداة حدثًا يفيد بأنه تم فك تشفير الجهاز بنجاح. وفي هذه الحالة، يجب إعادة تشغيل إجراء استعادة البيانات لفك تشفير الجهاز.
- بعد تحديث المكون الإضافي Kaspersky Endpoint Security for Windows في وحدة تحكم الويب، لا تعرض خصائص الكمبيوتر العميل مفتاح استرداد BitLocker حتى يتم إعادة تشغيل خدمة وحدة تحكم الويب.
- للاطلاع على القيود الأخرى لدعم تشفير القرص بالكامل وقائمة بالأجهزة التي يتم دعم تشفير محركات الأقراص الصلبة لها مع وجود قيود، يرجى الرجوع إلى قاعدة معارف الدعم الفني.

التشفير على مستوى الملفات (FLE)

- لا يتم دعم تشفير الملفات والمجلدات في أنظمة تشغيل عائلة Microsoft Windows Embedded.
- بمجرد تثبيت التطبيق، يجب إعادة تشغيل نظام التشغيل لكي يعمل تشفير الملفات والمجلدات بشكل صحيح.
- في حالة تخزين ملف مشفر على جهاز كمبيوتر يتوافر عليه وظيفة تشفير وقمت بالوصول إلى الملف من جهاز كمبيوتر لا يتوافر عليه التشفير، فسيتم توفير الوصول المباشر إلى هذا الملف. ويتم نسخ الملف المشفر الذي تم تخزينه في مجلد شبكة على جهاز كمبيوتر تتوافر عليه وظيفة تشفير في شكل غير مشفر إلى جهاز كمبيوتر لا تتوافر عليه وظيفة تشفير.
- يُنصح بفك تشفير الملفات التي تم تشفيرها باستخدام نظام تشفير الملفات قبل تشفير الملفات باستخدام Kaspersky Endpoint Security for Windows.
- بعد تشفير ملف، يزيد حجمه 4 كيلو بايت.
- بعد تشفير ملف، يتم تعيين سمة الأرشيف في خصائص الملف.
- إذا كان ملف غير مضغوط من أرشيف مشفر يحمل الاسم نفسه لملف موجود بالفعل على جهاز الكمبيوتر الخاص بك، فسيتم استبدال الأخير ليحل محله الملف الجديد الذي تم فك ضغطه من أرشيف مشفر. ولا يتم إعلام المستخدم بعملية الاستبدال.
- قبل فك حزمة أرشيف مشفر، تأكد أنك تمتلك مساحة خالية كافية على القرص لاستيعاب الملفات غير المضغوطة. وإذا لم تكن لديك مساحة كافية على القرص، قد يكتمل فك حزمة الأرشيف لكن الملفات قد تتلف. وفي هذه الحالة، من المحتمل ألا يعرض Kaspersky Endpoint Security أي رسائل خطأ.
- لا تعرض واجهة إدارة الملفات المحمولة رسائل حول الأخطاء التي تحدث أثناء تشغيلها.
- لا يبدأ Kaspersky Endpoint Security for Windows تشغيل إدارة الملفات المحمولة على جهاز كمبيوتر مثبت عليه مكون التشفير على مستوى الملفات.
- لا يمكنك استخدام إدارة الملفات المحمولة للوصول إلى محرك أقراص قابل للإزالة إذا تحققت الشروط التالية في وقت واحد:
  - لا يوجد اتصال بـ Kaspersky Security Center؛
  - يتم تثبيت Kaspersky Endpoint Security for Windows على الكمبيوتر؛
  - لم يتم تنفيذ تشفير البيانات (FDE أو FILE) على الكمبيوتر.

  لا يكون الوصول ممكنًا حتى إذا كنت تعرف كلمة المرور الخاصة بإدارة الملفات المحمولة.
- عند استخدام تشفير الملفات، يكون التطبيق غير متوافق مع عميل بريد Sylpheed.
- لا يدعم Kaspersky Endpoint Security for Windows قواعد تقييد الوصول إلى الملفات المشفرة لبعض التطبيقات. وهذا يرجع إلى حقيقة أن بعض عمليات الملفات يتم تنفيذها بواسطة تطبيق تابع لجهة خارجية. على سبيل المثال، يتم إجراء نسخ الملف بواسطة برنامج إدارة الملفات، وليس بواسطة التطبيق نفسه. وبهذه الطريقة، إذا تم رفض وصول عميل بريد Outlook إلى الملفات المشفرة، سيسمح Kaspersky Endpoint Security لعميل البريد بالوصول إلى الملف المشفر، وإذا نسخ المستخدم الملفات إلى رسالة البريد الإلكتروني عبر الحافظة أو وظيفة باستخدام السحب والإفلات. تم تنفيذ عملية النسخ بواسطة مدير الملفات، والتي لم يتم تحديد قواعد تقييد وصول إلى الملفات المشفرة لها، أي أن الوصول مسموح به.
- عندما يتم تشفير محركات الأقراص القابلة للإزالة مع دعم الوضع المحمول، لا يمكن تعطيل التحكم في عمر كلمة المرور.
- لا يتم دعم تغيير إعدادات ملف الصفحة. يستخدم نظام التشغيل القيم الافتراضية بدلاً من قيم المعلمات المحددة.
- استخدم الإزالة الآمنة عند العمل مع محركات الأقراص القابلة للإزالة المشفرة. لا يمكننا ضمان سلامة البيانات إذا لم يتم إزالة محرك الأقراص القابلة للإزالة بأمان.
- بعد تشفير الملفات، يتم حذف أصولها غير المشفرة بأمان.

- لا يتم دعم مزامنة الملفات غير المتصلة بالإنترنت باستخدام التخزين المؤقت في جانب العميل (CSC). من المستحسن حظر إدارة الموارد المشتركة غير المتصلة بالإنترنت على مستوى سياسة المجموعة. ويمكن تحرير الملفات الموجودة في وضع عدم الاتصال بالإنترنت. وبعد المزامنة، قد يتم فقد التغييرات التي تم إجراؤها على ملف غير متصل بالإنترنت. وللحصول على تفاصيل بشأن دعم التخزين المؤقت على جانب العميل (CSC) عند استخدام التشفير، يرجى الرجوع إلى قاعدة معارف الدعم الفني.

- لا يتم دعم إنشاء أرشيف مشفر في جذر نظام محرك الأقراص الصلبة.

- قد تواجه مشاكل عند الوصول إلى الملفات المشفرة عبر الشبكة. يُنصح بنقل الملفات إلى مصدر مختلف أو التأكد من أن الكمبيوتر المستخدم كخادم ملفات تتم إدارته بواسطة خادم إدارة Kaspersky Security Center ذاته.

- قد يؤدي تغيير تخطيط لوحة المفاتيح إلى تعليق نافذة إدخال كلمة المرور لأرشيف استخراج ذاتي مشفر. ولحل هذه المشكلة، أغلق نافذة إدخال كلمة المرور وقم بتبديل تخطيط لوحة المفاتيح في نظام التشغيل وأعد إدخال كلمة المرور للأرشيف المشفر.

- عند استخدام تشفير الملفات على الأنظمة التي تحتوي على أقسام متعددة على قرص واحد، يُنصح باستخدام الخيار الذي يحدد حجم ملف pagefile.sys تلقائيًا. وبعد إعادة تشغيل جهاز الكمبيوتر، قد ينتقل ملف pagefile.sys بين أقسام القرص.

- بعد تطبيق قواعد تشفير الملفات، بما في ذلك الملفات الموجودة في مجلد My Documents، تأكد أن المستخدمين الذين تم تطبيق التشفير لهم يمكنهم الوصول إلى الملفات المشفرة بنجاح. ولفعل ذلك، اطلب من كل مستخدم تسجيل الدخول إلى النظام عند توفر اتصال بـ Kaspersky Security Center. وإذا حاول مستخدم الوصول إلى الملفات المشفرة دون الاتصال بـ Kaspersky Security Center، فقد يتعطل النظام.

- في حالة تضمين ملفات النظام بطريقة ما في نطاق التشفير على مستوى الملفات، فقد تظهر الأحداث المتعلقة بالأخطاء عند تشفير هذه الملفات في التقارير. وتكون الملفات المحددة في هذه الأحداث غير مشفرة بالفعل.

- لا يتم دعم عد عمليات Pico.

- لا يتم دعم المسارات الحساسة لحالة الأحرف. عند تطبيق قواعد التشفير أو قواعد فك التشفير، يتم عرض المسارات في أحداث المنتج بأحرف صغيرة.

- لا يوصى بتشفير الملفات التي يستخدمها النظام عند بدء التشغيل. وإذا كانت هذه الملفات مشفرة، فقد تؤدي محاولة الوصول إلى الملفات المشفرة دون الاتصال بـ Kaspersky Security Center إلى تعطل النظام أو تؤدي إلى مطالبات للوصول إلى الملفات غير المشفرة.

- وإذا عمل المستخدمون بشكل مشترك مع ملف عبر الشبكة بموجب قواعد التشفير على مستوى الملفات عبر التطبيقات التي تستخدم طريقة تعيين الملفات إلى الذاكرة (مثل WordPad أو FAR) والتطبيقات المصممة للعمل مع الملفات الكبيرة (مثل Notepad ++)، فقد يتم حظر الملف في الشكل غير المشفر إلى أجل غير مسمى دون القدرة على الوصول إليه من جهاز الكمبيوتر الموجود عليه.

- لا يشفر Kaspersky Endpoint Security الملفات الموجودة في التخزين السحابي في OneDrive أو في مجلدات أخرى يكون اسمها OneDrive. ويحظر Kaspersky Endpoint Security أيضًا نسخ الملفات المشفرة إلى مجلدات OneDrive إذا لم تتم إضافة هذه الملفات إلى قاعدة فك التشفير.

- عند تثبيت مكون التشفير على مستوى الملفات، لا تعمل إدارة المستخدمين والمجموعات في وضع WSL (نظام Windows الفرعي لنظام Linux).

- عند تثبيت مكون التشفير على مستوى الملفات، لا يتم دعم POSIX (واجهة نظام التشغيل المحمولة) لإعادة تسمية الملفات وحذفها.

- لا يوصى بتشفير الملفات المؤقتة، لأن ذلك قد يؤدي إلى فقدان البيانات. على سبيل المثال، ينشئ Microsoft Word ملفات مؤقتة عند معالجة مستند. وفي حالة تشفير الملفات المؤقتة، لكن لم يتم تشفير الملف الأصلي، فقد يتلقى المستخدم خطأ تم رفض الوصول عند محاولة حفظ المستند. بالإضافة إلى ذلك، قد يحفظ Microsoft Word الملف، لكن لن يكون من الممكن فتح المستند في المرة القادمة، أي ستفقد البيانات. لمنع فقدان البيانات، تحتاج إلى استثناء مجلد الملفات المؤقتة من قواعد التشفير.

- بعد تحديث Kaspersky Endpoint Security for Windows الإصدار 11.0.1 أو أقدم، للوصول إلى الملفات المشفرة بعد إعادة تشغيل الكمبيوتر، تأكد من تشغيل عميل الشبكة. ويتضمن عميل الشبكة بدء تشغيل متأخر، لذا لا يمكنك الوصول إلى الملفات المشفرة فور تحميل نظام التشغيل. وليست هناك حاجة لانتظار بدء عميل الشبكة بعد بدء تشغيل الكمبيوتر التالي.

Detection and Response (EDR وMDR وKaspersky Sandbox)

- لا يمكنك فحص كائن تم عزله نتيجة مهمة نقل الملف إلى العزل.
- لا يمكن عزل تدفق بيانات بديل (ADS) أكبر من 4 ميجا بايت. ويتخطى Kaspersky Endpoint Security عزل تدفق البيانات البديل (ADS) بهذا الحجم دون إخطار المستخدم.
- لا يقوم Kaspersky Endpoint Security بتشغيل مهام فحص IOC على محركات أقراص الشبكة إذا كان مسار المجلد في خصائص المهمة يبدأ بحرف محرك أقراص. ويدعم Kaspersky Endpoint Security تنسيق مسار UNC فقط لمهام فحص IOC على محركات أقراص الشبكة. على سبيل المثال، `\\server\shared_folder`.
- ينتهي استيراد ملف تكوين التطبيق بخطأ في حالة تمكين التكامل مع إعداد Kaspersky Sandbox في ملف التكوين. وقبل تصدير إعدادات التطبيق، قم بتعطيل Kaspersky Sandbox. ثم نفذ إجراء التصدير/الاستيراد. وبعد استيراد ملف التكوين، قم بتمكين Kaspersky Sandbox.
- عند اكتشاف مؤشر على حدوث اختراق أثناء مهمة فحص IOC، يعزل التطبيق ملفًا فقط لشرط FileItem. لا يتم دعم عزل ملف للشروط الأخرى.
- يلزم وجود المكوّن الإضافي للويب لتطبيق Kaspersky Endpoint Security for Windows 11.7.0 أو أحدث لإدارة تفاصيل التنبيه. ويلزم وجود تفاصيل التنبيه عند العمل مع حلول Endpoint Detection and Response (EDR Optimum وEDR Expert). وتتوافر تفاصيل الاكتشاف فقط في Kaspersky Security Center Web Console وKaspersky Security Center Cloud Console.
- قد يكتمل ترحيل تكوين [KES+KEA] إلى تكوين [KES + العامل المضمن] مع حدوث خطأ في إزالة تطبيق Kaspersky Endpoint Agent. وتم إصلاح خطأ إزالة التطبيق في أحدث إصدار من Kaspersky Endpoint Agent. ولإزالة Kaspersky Endpoint Agent، أعد تشغيل الكمبيوتر وأنشئ مهمة إزالة تطبيق.
- لا يتم دعم تكوين [KES+KEA+العامل المضمن]. ويؤدي هذا التكوين إلى تعطيل التفاعل بين التطبيقات وحل Detection and Response الذي يتم نشره في مؤسستك. بالإضافة إلى ذلك، يمكن أن يؤدي استخدام Kaspersky Endpoint Agent والعامل المضمن على الكمبيوتر نفسه إلى تكرار القياس عن بُعد وزيادة الحمل على الكمبيوتر والشبكة. وبعد الترحيل إلى تكوين [KES + العامل المضمن]، تأكد من إزالة Kaspersky Endpoint Agent من الكمبيوتر. وإذا استمر Kaspersky Endpoint Agent في العمل بعد الترحيل، فقم بإلغاء تثبيت التطبيق يدويًا (على سبيل المثال، باستخدام مهمة إلغاء تثبيت التطبيق عن بعد).

  يتيح لك المُثبت نشر Kaspersky Endpoint Agent على جهاز كمبيوتر باستخدام Kaspersky Endpoint Security والعامل المضمن المُثبت. ويمكن أيضًا تثبيت Kaspersky Endpoint Agent والعامل المضمن على جهاز كمبيوتر واحد نتيجة لمهمة تغيير مكونات التطبيق. يعتمد السلوك على إصدارات Kaspersky Endpoint Security وKaspersky Endpoint Agent.
- يلزم وجود المكوّن الإضافي للويب لتطبيق Kaspersky Endpoint Security for Windows 11.7.0 أو أحدث لإدارة مكوني EDR Optimum وKaspersky Sandbox. يلزم وجود المكوّن الإضافي للويب لتطبيق Kaspersky Endpoint Security for Windows 11.8.0 أو أحدث لإدارة مكون EDR Expert. إذا أنشأت مهمة تغيير مكونات التطبيق باستخدام مكون إضافي للويب لا يدعم العمل مع هذه المكونات، سيقوم المُثبت بحذف هذه المكونات على أجهزة الكمبيوتر المُثبت عليها EDR Optimum أو EDR Expert أو Kaspersky Sandbox.
- يستأنف العامل المضمن، EDR (KATA)، عزل الشبكة للكمبيوتر بعد إعادة تشغيل الكمبيوتر، حتى إذا انتهت فترة العزل. ولمنع تكرار عزل الكمبيوتر، تحتاج إلى إيقاف تشغيل عزل الشبكة في وحدة تحكم Kaspersky Anti Targeted Attack Platform.
- نوصي بترقية التطبيق بعد انتهاء عزل شبكة الاتصال. وبعد ترقية Kaspersky Endpoint Security، يمكن إيقاف عزل شبكة الاتصال.
- لا يتوافق العمال المضمنون لحل EDR (KATA) وEDR Optimum وEDR Expert مع بعضهم البعض. لذلك، يمكن تخطي تفعيل العامل المُضمن في EDR مع ترخيص الوظيفة الإضافية لحل Kaspersky Endpoint Detection and Response on Kaspersky Endpoint Security بوظائف EDR مختلفة. على سبيل المثال، يتم تخطي تفعيل العامل المضمن في EDR (KATA) بترخيص مستقل إذا قمت بتفعيل Kaspersky Endpoint Security باستخدام ترخيص [KES EDR Optimum].
- في الإصدار 12.1 من Kaspersky Endpoint Security، لا يدعم عميل EDR (KATA) المدمج ملفات التعريف التالية لمهمة الحصول على ملفات تعريف NTFS: $Secure:$SDH:$INDEX_ROOT; $Secure:$SDH:$INDEX_ALLOCATION; $Secure:$SDH:$BITMAP; $Secure:$SII:$INDEX_ROOT; $Secure:$SII:$INDEX_ALLOCATION; $Secure:$SII:$BITMAP; $Extend\$UsnJrnl:$J:$DATA; $Extend\$UsnJrnl:$Max:$DATA.
- عند الترحيل من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security لحل Kaspersky Anti Targeted Attack Platform (EDR)، قد تواجه أخطاء عند توصيل الكمبيوتر بخوادم Central Node. ويرجع السبب في ذلك إلى أن معالج الترحيل في وحدة تحكم الويب يتخطى إعدادات السياسة التالية ولا يقوم بترحيلها:
  - حظر تعديل الإعدادات **Settings for connecting to KATA servers** ("قفل").

بشكل افتراضي، يمكن تعديل الإعدادات ("القفل" مفتوح). لذلك لا يتم تطبيق الإعدادات على الكمبيوتر. ويجب حظر تعديل الإعدادات وإغلاق "القفل".

- حاوية التشفير.

إذا كنت تستخدم المصادقة ثنائية الاتجاه للاتصال بخوادم Central Node، فيجب إعادة إضافة حاوية التشفير. ويقوم معالج الترحيل بترحيل شهادة TLS الخاصة بالخادم بشكل صحيح.

يقوم معالج ترحيل السياسة والمهام في وحدة تحكم الإدارة (MMC) بترحيل جميع الإعدادات الخاصة بحل Kaspersky Anti Targeted Attack Platform (EDR).

قيود أخرى

- إذا أظهر التطبيق خطأ أو تعطل خلال التشغيل، فإنه يمكن إعادة تشغيله تلقائيًا. إذا واجه التطبيق أخطاء متكررة تسببت في تعطل التطبيق، يقوم التطبيق بإجراء العمليات التالية:

  1. تعطيل وظائف التحكم والحماية (لا تزال وظيفة التشفير ممكنة).

  2. إخطار المستخدم بتعطيل الوظائف.

  3. محاولة استعادة التطبيق إلى الحالة الوظيفية عقب تحديث قواعد بيانات مكافحة الفيروسات أو تطبيق تحديثات الوحدة النمطية للتطبيق.

- قد تتم معالجة عناوين الويب التي تمت إضافتها إلى القائمة الموثوقة بشكل غير صحيح.

- في وحدة تحكم Kaspersky Security Center لا يمكنك حفظ ملف على القرص من **متقدم** ← **المستودعات** ← مجلد **التهديدات النشطة**. ولحفظ الملف، يجب عليك تنظيف الملف المصاب. وعند التنظيف، يحفظ التطبيق نسخة من الملف في النسخة الاحتياطية. ويمكنك الآن حفظ الملف على القرص من المجلد **متقدم** ← **المستودعات** ← مجلد **النسخ الاحتياطي**.

- تختلف وراثة إعدادات نقل البيانات إلى خادم الإدارة (**الإعدادات العامة** ← **التقارير والمخزن** ← **نقل البيانات إلى خادم الإدارة**) عن وراثة الإعدادات الأخرى. وإذا سمحت بتغيير إعدادات إرسال البيانات في السياسة ("القفل" مفتوح)، فستتم إعادة تعيين هذه الإعدادات إلى القيم الافتراضية في خصائص الكمبيوتر المحلي في وحدة التحكم إذا لم يتم تحديدها مسبقًا. وإذا تم تحديد هذه الإعدادات مسبقًا، فستتم استعادة قيمها. وعند حذف سياسة، يتم توريث الإعدادات بالطريقة نفسها. وفي هذه الحالات، يتم توريث الإعدادات الأخرى في خصائص الكمبيوتر المحلي من السياسة.

- يراقب Kaspersky Endpoint Security حركة HTTP التي تتوافق مع معايير RFC 2616 وRFC 7540 وRFC 7541 وRFC 7301. وإذا اكتشف Kaspersky Endpoint Security تنسيق تبادل بيانات آخر في حركة HTTP، فإن التطبيق يحظر هذا الاتصال لمنع تنزيل الملفات الضارة من الإنترنت.

- يمنع Kaspersky Endpoint Security الاتصال عبر بروتوكول QUIC. وتستخدم المستعرضات بروتوكول النقل القياسي (TLS أو SSL) بغض النظر عما إذا كان دعم QUIC ممكنًا في المستعرض أم لا.

- مراقب النظام. لا يتم عرض المعلومات الكاملة حول العمليات.

- عند بدء تشغيل Kaspersky Endpoint Security for Windows لأول مرة، قد يتم وضع تطبيق موقّع رقميًا بشكل مؤقت في المجموعة الخطأ. وسيتم لاحقًا وضع التطبيق الموقع رقميًا في المجموعة الصحيحة.

- في Kaspersky Security Center، عند التبديل من استخدام شبكة Kaspersky Security Network العالمية إلى استخدام شبكة Kaspersky Security Network خاصة، أو العكس، يتم تعطيل خيار المشاركة في شبكة Kaspersky Security Network في سياسة المنتج المحدد. وبعد التبديل، اقرأ بعناية نص بيان Kaspersky Security Network وأكد موافقتك على المشاركة في KSN. ويمكنك قراءة نص البيان في واجهة التطبيق أو عند تحرير سياسة المنتج.

- أثناء إعادة فحص كائن خبيث تم منعه بواسطة برنامج خاص بطرف خارجي، لا يتم إخطار المستخدم عند اكتشاف التهديد مرة أخرى. ويتم عرض حدث إعادة اكتشاف التهديد في تقرير التطبيق وفي تقرير Kaspersky Security Center.

- لا يمكن تثبيت مكون أداة استشعار نقطة النهاية في Microsoft Windows Server 2008.

- لن يتضمن تقرير Kaspersky Security Center حول تشفير الجهاز معلومات حول الأجهزة التي تم تشفيرها باستخدام Microsoft BitLocker على الأنظمة الأساسية للخوادم أو على محطات العمل التي لم يتم تثبيت مكون التحكم في الجهاز عليها.

- لا يمكن تمكين عرض كل إدخالات التقرير في Kaspersky Security Center Web Console. وفي Web Console، يمكنك فقط تغيير عدد الإدخالات المعروضة في التقارير. وبشكل افتراضي، يعرض Kaspersky Security Center Web Console ألف إدخال تقرير. ويمكنك تمكين عرض كل إدخالات التقرير في وحدة تحكم الإدارة (MMC).

- لا يمكن تعيين عرض أكثر من 1000 إدخال تقرير في Kaspersky Security Center Console. وإذا قمت بتعيين قيمة أعلى من 1000، فسيعرض Kaspersky Security Center Console ألف إدخال تقرير فقط.

- عند استخدام التسلسل الهرمي للسياسة، يمكن الوصول إلى إعدادات قسم تشفير محركات الأقراص القابلة للإزالة في السياسة الفرعية للتحرير إذا كانت السياسة الأصلية تمنع تعديل هذه الإعدادات.

- يجب تمكين Audit Logon (التدقيق في تسجيل الدخول) في إعدادات نظام التشغيل لضمان حسن عمل الاستثناءات لحماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي.

- في حالة تمكين حماية المجلد المشترك، يراقب Kaspersky Endpoint Security for Windows محاولات تشفير المجلدات المشتركة لكل جلسة وصول عن بُعد بدأت قبل بدء تشغيل Kaspersky Endpoint Security for Windows، بما في ذلك ما إذا كان الكمبيوتر الذي بدأت منه جلسة الوصول عن بُعد قد تمت إضافته إلى الاستثناءات. إذا كنت لا تريد أن يراقب Kaspersky Endpoint Security for Windows محاولات تشفير المجلدات المشتركة لجلسات الوصول عن بُعد التي بدأت من جهاز كمبيوتر تمت إضافته إلى الاستثناءات والتي بدأت قبل بدء تشغيل Kaspersky Endpoint Security for Windows، فقم بإنهاء جلسة الوصول عن بُعد وأعد إنشاءها أو أعد تشغيل الكمبيوتر المثبت عليه تطبيق Kaspersky Endpoint Security for Windows.

- في حالة تشغيل مهمة التحديث بأذونات حساب مستخدم معين، فلن يتم تنزيل تصحيحات المنتج عند التحديث من مصدر يتطلب مصادقة.

- قد يفشل التطبيق في بدء التشغيل بسبب عدم كفاية أداء النظام. ولإصلاح هذه المشكلة، استخدم خيار التمهيد الجاهز أو قم بزيادة مهلة نظام التشغيل لبدء الخدمات.

- لا يستطيع التطبيق العمل في الوضع الآمن.

- للتأكد من إمكانية عمل الإصدارين 11.5.0 و11.6.0 من Kaspersky Endpoint Security لنظام تشغيل Windows بشكل صحيح مع برنامج Cisco AnyConnect، يجب عليك تثبيت الإصدار 4.3.183.2048 من الوحدة النمطية للتوافق أو إصدار أحدث. تعرف على المزيد حول التوافق مع Cisco Identity Services Engine في وثائق Cisco.

- لا يمكننا ضمان عمل التحكم في الصوت إلا بعد إعادة التشغيل الأولى بعد تثبيت التطبيق.

- في وحدة تحكم الإدارة (MMC)، في إعدادات منع الاختراق في نافذة تكوين أذونات التطبيق، لا يتوفر الزر **إزالة**. ويمكنك إزالة تطبيق من مجموعة الثقة عبر قائمة السياق الخاصة بالتطبيق.

- في الواجهة المحلية للتطبيق، في إعدادات منع الاختراق، لا تتوفر أذونات التطبيق والموارد المحمية للعرض إذا كان الكمبيوتر يُدار بواسطة سياسة. ولا تتوافر عناصر التمرير والبحث والتصفية وعناصر التحكم الأخرى في النافذة. ويمكنك عرض أذونات التطبيق في خصائص السياسة في Kaspersky Security Center Console.

- عند تمكين ملفات التتبع التي تم تدويرها، لا يتم إنشاء أي تتبعات لمكون AMSI ومكون Outlook الإضافي.

- لا يمكن جمع عمليات تتبع الأداء يدويًا في Windows Server 2008.

- لا يتم دعم عمليات تتبع الأداء لنوع التتبع "إعادة التشغيل".

- لا يتم دعم تسجيل التفريغ لعمليات PICO.

- لم تعد مهمة التحقق من توفر KSN مدعومة.

- لن يسمح لك إيقاف تشغيل خيار "تعطيل الإدارة الخارجية لخدمات النظام" بإيقاف خدمة التطبيق الذي تم تثبيته باستخدام المعلمة `AMPPL=1` (افتراضيًا، يتم تعيين قيمة المعلمة على 1 بدءًا من إصدار نظام التشغيل Windows 10RS2). تتيح المعلمة `AMPPL` بقيمة `1` استخدام تقنية عمليات الحماية لخدمة المنتج.

- لإجراء فحص مخصص لمجلد، يجب أن يمتلك المستخدم الذي يبدأ الفحص المخصص الأذونات لقراءة سمات هذا المجلد. وإلا سيكون فحص المجلد المخصص مستحيلاً وسينتهي بخطأ.

- عندما تتضمن قاعدة فحص محددة في سياسة ما مسارًا بدون الحرف `\` في النهاية، على سبيل المثال، `C:\folder1\folder2`، سيتم تشغيل الفحص للمسار C:\folder1\.

- عند ترقية التطبيق من الإصدار 11.1.0 إلى 12.1، ستتم إعادة تعيين إعدادات حماية AMSI إلى قيمها الافتراضية.

- إذا كنت تستخدم سياسات تقييد البرامج (SRP)، فقد يفشل الكمبيوتر في التحميل (شاشة سوداء). لمنع الأعطال، تحتاج إلى السماح باستخدام مكتبات التطبيقات في خصائص SRP. في خصائص SRP أضف القاعدة بمستوى أمان **غير مقيد** لملف khkum.dll (عنصر القائمة **قاعدة تجزئة جديدة**). ويوجد الملف في المجلد `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.<version>\klhk\klhk_x64\`. إذا حددت هذه الطريقة، ستحتاج أيضًا إلى مسح خانة الاختيار **تنزيل تحديثات وحدات التطبيق** في إعدادات

مهمة تحديث لتطبيق Kaspersky Endpoint Security. وللتفاصيل عن استخدام سياسات تقييد البرامج، يُرجى الرجوع إلى مستندات Microsoft.

يمكنك أيضًا تعطيل SRP واستخدام مكون التحكم في التطبيقات من Kaspersky Endpoint Security للتحكم في استخدام التطبيقات.

- إذا كان الكمبيوتر ينتمي إلى مجال تحت كائن نهج المجموعة (GPO) لنظام التشغيل Windows مع تعيين معلمة DriverLoadPolicy على 8 (جيد فقط)، فإن إعادة تشغيل الكمبيوتر المثبت عليه Kaspersky Endpoint Security تؤدي إلى ظهور شاشة الموت الزرقاء. ولمنع الفشل، يجب تعيين معلمة التشغيل المبكر لمكافحة البرامج الضارة (ELAM) في "نهج المجموعة" على 1 (جيد وغير معروف). توجد إعدادات ELAM في السياسة تحت: **تكوين الكمبيوتر ← القوالب الإدارية ← النظام ← التشغيل المبكر لمكافحة البرامج الضارة**.

- لا يتم دعم إدارة إعدادات المكون الإضافي في Outlook عبر Rest API.

- لا يمكن نقل إعدادات تشغيل المهمة لمستخدم معين بين الأجهزة عبر ملف تكوين. بعد تطبيق الإعدادات من ملف تكوين، حدد اسم المستخدم وكلمة المرور يدويًا.

- بعد تثبيت تحديث، لا تعمل مهمة التحقق من السلامة حتى يتم إعادة تشغيل النظام لتطبيق التحديث.

- عندما يتم تغيير مستوى التتبع الذي تم تدويره من خلال أداة عمليات التشخيص عن بُعد، يعرض Kaspersky Endpoint Security for Windows بشكل غير صحيح قيمة فارغة لمستوى التتبع. ومع ذلك، تتم كتابة ملفات التتبع وفقًا لمستوى التتبع الصحيح. وعندما يتم تغيير مستوى التتبع الذي تم تدويره من خلال الواجهة المحلية للتطبيق، يتم تعديل مستوى التتبع بشكل صحيح، لكن الأداة المساعدة للتشخيص عن بُعد تعرض بشكل غير صحيح مستوى التتبع الذي تم تحديده مؤخرًا بواسطة الأداة المساعدة. وقد يتسبب هذا في عدم حصول المسؤول على معلومات محدثة حول مستوى التتبع الحالي، وقد تكون المعلومات ذات الصلة غائبة عن عمليات التتبع إذا غير المستخدم يدويًا مستوى التتبع في الواجهة المحلية للتطبيق.

- في الواجهة المحلية، لا تسمح إعدادات حماية كلمة المرور بتغيير اسم حساب المسؤول (KLAdmin بشكل افتراضي). ولتغيير اسم حساب المسؤول، تحتاج إلى تعطيل الحماية بكلمة مرور، ثم تمكين الحماية بكلمة مرور وتحديد اسم جديد لحساب المسؤول.

- لا يتوافق تطبيق Kaspersky Endpoint Security عند تثبيته على Windows Server 2019 مع Docker. ويؤدي نشر حاويات Docker على جهاز كمبيوتر باستخدام Kaspersky Endpoint Security إلى حدوث عطل (شاشة الموت الزرقاء).

- توافق Kaspersky Endpoint Security وSecret Net Studio محدود:

  - لا يتوافق تطبيق Kaspersky Endpoint Security مع مكون مكافحة الفيروسات في برنامج Secret Net Studio.

    ولا يمكن تثبيت التطبيق على جهاز كمبيوتر حيث يتم نشر Secret Net Studio مع مكون مكافحة الفيروسات. ولجعل التشغيل البيني ممكنًا، يجب إزالة مكون مكافحة الفيروسات من Secret Net Studio.

  - لا يتوافق تطبيق Kaspersky Endpoint Security مع مكون تشفير القرص بالكامل في برنامج Secret Net Studio.

    ولا يمكن تثبيت التطبيق على جهاز كمبيوتر حيث يتم نشر Secret Net Studio مع مكون تشفير القرص بالكامل. ولجعل التشغيل البيني ممكنًا، يجب إزالة مكون تشفير القرص بالكامل من Secret Net Studio.

  - لا يتوافق Secret Net Studio مع مكون التشفير على مستوى الملف (FLE) في Kaspersky Endpoint Security.

    عند تثبيت Kaspersky Endpoint Security باستخدام مكون التشفير على مستوى الملف (FLE)، يمكن أن يعمل Secret Net Studio مع وجود أخطاء. ولضمان إمكانية التشغيل البيني، يجب عليك إزالة مكون التشفير على مستوى الملف (FLE) من Kaspersky Endpoint Security.

المصطلحات

IOC

مؤشر الاختراق. مجموعة من البيانات حول كائن أو نشاط خبيث.

OpenIOC

المعيار المفتوح لوصف مؤشر الاختراق (IOC) المستند إلى XML ويتضمن أكثر من 500 مؤشر مختلف للاختراق.

إدارة الملفات المحمولة

هذا تطبيق يوفر واجهة للعمل على الملفات المشفرة على محركات أقراص قابلة للإزالة، عندما لا تتوفر وظيفة التشفير على جهاز الكمبيوتر.

إنذار خاطئ

يصدر إنذار زائف عندما يبلغ تطبيق Kaspersky عن ملف غير مصاب نظرًا لتشابه توقيع الملف مع توقيع خاص بأحد الفيروسات.

الأرشيف

ملف واحد أو ملفات عديدة تم حزمها في ملف واحد مضغوط. يلزم تطبيق مخصص يسمى "الأرشيف" لحزم البيانات وفك حزمها.

القناع

تمثيل لاسم وامتداد ملف باستخدام أحرف البدل.

قد تشتمل أقنعة الملفات على أية حروف مسموح بها في أسماء الملفات، بما في ذلك أحرف البدل:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.

- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح. يتوفر القناع ** فقط لإنشاء استثناءات الفحص.

- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

المفتاح الإضافي

مفتاح يصدق على حق استخدام التطبيق لكن لا يُستخدم حاليًا.

الملف القابل للإصابة

هو ملف، بالنظر لهيكله أو تنسيقه، يمكن للدخلاء استخدامه كـ "وعاء" لتخزين تعليمات برمجية ضارة وتوزيعه. وكقاعدة، تكون هذه ملفات تنفيذية تحمل ملحقات ملفات مثل com. وexe. وdll.. ويكون هناك خطر عالٍ لاقتحام رمز خبيث في تلك الملفات.

المهمة

الوظائف التي يتم تنفيذها بواسطة تطبيق Kaspersky كمهام، على سبيل المثال: حماية الملف في الوقت الحقيقي والفحص الكامل للجهاز وتحديث قاعدة البيانات.

الوحدة النمطية للنظام الأساسي الموثوق به

وهي رقاقة إلكترونية تم تصميمها لتوفير الوظائف الأساسية المرتبطة بالأمن (على سبيل المثال، لتخزين مفاتيح التشفير). عادة يتم تركيب الوحدة النمطية للنظام الأساسي الموثوق به على اللوحة الأم في جهاز الكمبيوتر وتتفاعل مع كل مكونات النظام الأخرى عبر ناقل الأجهزة.

تنظيف

طريقة معالجة الكائنات المصابة الناتجة عن الاستعادة الكاملة أو الجزئية للبيانات. لا يمكن تنظيف جميع الكائنات المصابة.

جهة إصدار الشهادة

مركز الشهادات الذي أصدر الشهادة.

شهادة الترخيص

مستند تمنحه Kaspersky للمستخدم مع ملف المفتاح أو رمز التفعيل. وهو يتضمن معلومات حول الترخيص الممنوح للمستخدم.

عميل الشبكة

هو مكون Kaspersky Security Center يتيح التفاعل بين خادم الإدارة وتطبيقات Kaspersky التي تم تثبيتها على عقدة شبكة اتصال معينة (محطة العمل أو الخادم). هذا المكون شائع لجميع تطبيقات Kaspersky التي يتم تشغيلها بنظام Windows. تكون الإصدارات الخاصة بعميل الشبكة مخصصة للتطبيقات التي يتم تشغيلها في أنظمة التشغيل الأخرى.

قاعدة بيانات عناوين الويب الاحتيالية

قائمة تضم عناوين الويب التي حدد أخصائيو Kaspersky وجود علاقة لها بالبرامج الاحتيالية. يتم تحديث قاعدة البيانات بانتظام بالإضافة لكونها جزءًا من حزمة توزيع تطبيق Kaspersky.

قاعدة بيانات عناوين الويب الضارة

قائمة بعناوين ويب التي تشتمل على محتوى يمكن اعتباره خطرًا. ويتم إنشاء هذه القائمة بواسطة أخصائيي Kaspersky. ويتم تحديثها بصفة منتظمة كما يتم تضمينها في حزمة توزيع تطبيق Kaspersky.

قواعد بيانات مكافحة الفيروسات

قواعد البيانات التي تحتوي على معلومات حول تهديدات أمن الكمبيوتر المعروفة لـ Kaspersky اعتبارًا من تاريخ إصدار قاعدة بيانات مكافحة الفيروسات. تساعد تواقيع قاعدة بيانات مكافحة الفيروسات على اكتشاف الرمز الضار في الكائنات التي تم فحصها. ويتم إنشاء قواعد بيانات مكافحة الفيروسات بواسطة أخصائي Kaspersky ويتم تحديثها على كل الساعة.

كائن OLE

ملف مرفق أو ملف مضمن في ملف آخر. تتيح تطبيقات Kaspersky فحص كائنات OLE للتأكد من عدم وجود فيروسات. على سبيل المثال، إذا قمت بإدخال جدول Microsoft Office Excel® إلى مستند Microsoft Office Word، يتم فحص الجدول بوصفه كائن OLE.

مجموعة الإدارة

مجموعة من الأجهزة التي تشترك في الوظائف العامة ومجموعة من تطبيقات Kaspersky المثبتة عليها. يتم تجميع الأجهزة حتى يمكن إدارتها بشكل مناسب كوحدة واحدة. قد تشتمل المجموعة على مجموعات أخرى. ومن الممكن إنشاء نُهج مجموعات ومهام مجموعات لكل تطبيق تم تثبيته في المجموعة.

مفتاح نشط

مفتاح يُستخدم حاليًا بواسطة التطبيق.

ملف IOC

ملف يحتوي على مجموعة من مؤشرات الاختراق (IOCs) التي يحاول التطبيق مطابقتها لحساب الاكتشاف. ويمكن أن تكون احتمالية الاكتشاف أعلى في حالة العثور على تطابقات تامة مع ملفات IOC متعددة للكائن نتيجة الفحص.

ملف مصاب

ملف يحتوي على تعليمات برمجية ضارة (تم اكتشاف تعليمات برمجيات ضارة معروفة عند فحص الملف). ولا يوصي Kaspersky باستخدام مثل هذه الملفات، حيث إنها قد تؤدي إلى إصابة جهاز الكمبيوتر.

نطاق الحماية

الكائنات التي يتم فحصها باستمرار بواسطة مكون الحماية من التهديدات الأساسية عند تشغيلها. تتمتع نطاقات الحماية للمكونات المختلفة بخصائص مختلفة.

نطاق الفحص

الكائنات التي يقوم Kaspersky Endpoint Security بفحصها أثناء تنفيذ مهمة الفحص.

نموذج تمت معايرته من عنوان مصدر ويب

يعد النموذج الذي تمت معايرته من عنوان مصدر ويب عبارة عن تمثيل نصي لعنوان مصدر ويب تم الحصول عليه من خلال المعايرة. وتعد المعايرة عملية يتغير فيها التمثيل النصي لعنوان مصدر ويب وفقًا لقواعد معينة (على سبيل المثال، استثناء منفذ اتصال وكلمة مرور وتسجيل دخول المستخدم من التمثيل النصي لعنوان مصدر الويب؛ بالإضافة إلى ذلك، يتم تغيير عنوان مصدر الويب من الأحرف الكبيرة إلى الصغيرة).

بخصوص تشغيل مكونات الحماية، يكون الغرض من معايرة عنوان مصدر الويب هو تجنب فحص عناوين مواقع الويب، وهو الأمر الذي قد يختلف في بناء الجملة بينما يكون مكافئًا من الناحية المادية، أكثر من مرة.

مثال:

صيغة غير معيارية للعنوان: \www.Example.com.

صيغة معيارية للعنوان: www.example.com.

وكيل المصادقة

واجهة تتيح لك إكمال المصادقة للوصول إلى محركات الأقراص الصلبة المشفرة وتحميل نظام التشغيل بعد تشفير محرك الأقراص الصلبة القابل لبدء تشغيله.

الملحقات

يحتوي هذا القسم على معلومات تكمل المستند الرئيسي.

الملحق رقم 1. إعدادات التطبيق

يمكنك استخدام السياسة أو المهام أو واجهة التطبيق لتكوين Kaspersky Endpoint Security. يتم توفير معلومات تفصيلية حول مكونات التطبيق في الأقسام الموافقة.

الحماية من تهديدات الملفات

يتيح لك مكون الحماية من تهديدات الملفات منع إصابة نظام الملفات في جهاز الكمبيوتر. بشكل افتراضي، يوجد مكون الحماية من تهديدات الملفات بشكل دائم في ذاكرة الوصول العشوائي للكمبيوتر. يقوم المكون بفحص الملفات على كافة محركات الأقراص للكمبيوتر وكذلك على محركات الأقراص المتصلة. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

يقوم المكون بفحص الملفات التي تم الوصول إليها بواسطة المستخدم أو التطبيق. إذا تم الكشف عن ملف ضار، يقوم Kaspersky Endpoint Security بحظر عمل الملف. يقوم التطبيق بعد ذلك بتطهير أو حذف الملف الضار، وذلك اعتمادًا على إعدادات مكون الحماية من تهديدات الملفات.

عند محاولة الوصول إلى ملف تم حفظ محتوياته في خدمة التخزين عبر الإنترنت OneDrive، يقوم Kaspersky Endpoint Security بتنزيل وفحص محتويات الملف.

إعدادات مكون الحماية من تهديدات الملفات

المعلمة	الوصف
مستوى الأمان (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	للحماية من تهديدات الملفات، يستطيع Kaspersky Endpoint Security تطبيق مجموعات مختلفة من الإعدادات. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان: • **مرتفع**. عندما يتم تحديد مستوى أمان الملف هذا، يتحكم مكون الحماية من تهديدات الملفات بأقصى صرامة في كل الملفات التي يتم فتحها وحفظها وبدء تشغيلها. ويفحص مكون الحماية من تهديدات الملفات كل أنواع الملفات على كل محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة من الكمبيوتر. يقوم أيضًا بفحص الأرشيفات وحزم التثبيت وكائنات OLE المضمنة. • **مستحسن**. يوصي خبراء Kaspersky Lab بمستوى أمان الملف هذا. ويفحص مكون الحماية من تهديدات الملفات فقط تنسيقات الملفات المحددة على جميع محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة على الكمبيوتر وكائنات OLE المضمنة. لا يفحص مكون الحماية من تهديدات الملفات الأرشيفات وحزم التثبيت. • **منخفض**. تضمن إعدادات مستوى أمان الملف هذه الوصول لسعة الفحص القصوى. ولا يفحص مكون الحماية من تهديدات الملفات إلا الملفات ذات الامتدادات المحددة على كل محركات الأقراص الصلبة ومحركات الأقراص القابلة للإزالة ومحركات أقراص الشبكة من الكمبيوتر. ولا يقوم مكون الحماية من تهديدات الملفات بفحص الملفات المركبة.
أنواع الملفات (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	**كل الملفات**. إذا تم تمكين هذا الإعداد، فإن Kaspersky Endpoint Security يفحص كل الملفات دون استثناء (كل التنسيقات والامتدادات). **الملفات التي تم فحصها حسب التنسيق**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. قبل فحص أحد الملفات بحثًا عن التعليمات البرمجية الضارة، يتم تحليل العنوان الداخلي للملف لتحديد تنسيق الملف (على سبيل المثال، txt. أو doc. أو exe.). ويبحث الفحص أيضًا عن الملفات بملحقات ملف معينة. **الملفات التي تم فحصها حسب الامتداد**. إذا تم تمكين هذا الإعداد، فإن التطبيق يفحص الملفات المصابة فقط. ويتم تحديد تنسيق الملف عندئذٍ استنادًا إلى امتداد الملف.
نطاق الفحص	

	تحتوي على الكائنات التي يفحصها مكون الحماية من تهديدات الملفات. قد يكون كائن الفحص محرك أقراص قابل للإزالة أو محرك أقراص شبكة اتصال أو مجلدًا أو ملفًا أو ملفات متعددة محددة بواسطة قناع. بشكل افتراضي يقوم مكون الحماية من تهديدات الملفات بفحص الملفات التي يتم بدء تشغيلها على أي محركات أقراص صلبة أو محركات الأقراص القابلة للإزالة أو محركات أقراص الشبكة. لا يمكن تغيير نطاق الحماية لهذه الكائنات أو حذفها. يمكنك أيضًا استبعاد كائن من عمليات الفحص (مثل محرك الأقراص القابلة للإزالة).
التعلّم الآلي وتحليل التوقيع (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تستخدم طريقة التعلّم الآلي وتحليل التوقيع قواعد بيانات Kaspersky Endpoint Security التي تحتوي على وصف للتهديدات المعروفة وطرق إبطالها. وتوفر الحماية التي تستخدم هذه الطريقة الحد الأدنى المقبول لمستوى الأمان. بناءً على توصيات خبراء Kaspersky، يتم تمكين التعلّم الآلي وتحليل التوقيع دائمًا.
التحليل المساعد على الاكتشاف (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف. عند فحص الملفات للبحث عن تعليمات برمجية ضارة، ينفذ المحلل المساعد على الاكتشاف الإرشادات الواردة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف كل الملفات المصابة المكتشفة. في حالة فشل التنظيف، يحذف التطبيق الملفات. **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا تعذر التنظيف، يضيف Kaspersky Endpoint Security معلومات حول الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة. **منع**. في حالة تحديد هذا الخيار، فإن مكون الحماية من تهديدات الملفات يمنع تلقائيًا كل الملفات المصابة دون محاولة تنظيفها. قبل محاولة تنظيف ملف مصاب أو حذفه، ينشئ التطبيق نسخة احتياطية من الملف في حال احتجت إلى استعادة الملف أو إذا كان من الممكن تنظيفه في المستقبل.
فحص الملفات الجديدة والتي تم تغييرها فقط	يفحص فقط الملفات الجديدة والملفات التي تم تعديلها منذ آخر مرة لفحصها. هذا يساعد على تقليل فترة الفحص. ينطبق هذا الوضع على كل من الملفات البسيطة والمركبة.
فحص الأرشيفات	فحص تنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE وتنسيقات الأرشيفات الأخرى. يفحص التطبيق الأرشيفات ليس فقط حسب الملحق، لكن أيضًا حسب التنسيق. عند التحقق من الأرشيفات، ينفذ التطبيق عملية تفريغ متكررة. ويسمح هذا باكتشاف التهديدات داخل أرشيفات متعددة المستويات (أرشيف داخل أرشيف).
فحص حزم التوزيع	تقوم خانة الاختيار هذه بتمكين/تعطيل فحص حزم التوزيع التابعة لجهة خارجية.
Scan files in Microsoft Office formats	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
عدم فك ضغط الملفات المركبة كبيرة الحجم	في حالة تحديد هذا المربع، لا يفحص التطبيق الملفات المركبة إذا كان حجمها يتجاوز القيمة المحددة. في حالة عدم تحديد خانة الاختيار هذه، يفحص التطبيق الملفات المركبة من جميع الأحجام. يفحص التطبيق الملفات الكبيرة التي يتم استخراجها من الأرشيفات بغض النظر عما إذا كانت خانة الاختيار محددة أو لا.

فك حزمة الملفات المركبة في الخلفية	في حالة تحديد خانة الاختيار، يوفر التطبيق الوصول إلى الملفات المركبة الأكبر من القيمة المحددة قبل فحص هذه الملفات. في هذه الحالة، فإن Kaspersky Endpoint Security يفك حزمة الملفات المركبة ويفحصها في الخلفية. يوفر التطبيق الوصول إلى الملفات المركبة الأصغر من هذه القيمة فقط بعد فك هذه الملفات وفحصها. في حالة عدم تحديد خانة الاختيار، لا يوفر التطبيق الوصول إلى الملفات المركبة إلا بعد فك الحزمة الملفات وفحصها، أيًا كان حجمها.
وضع الفحص (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	يفحص Kaspersky Endpoint Security الملفات التي يصل إليها المستخدم أو نظام التشغيل أو أحد التطبيقات التي تعمل تحت حساب المستخدم. **الوضع الذكي**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائن بناءً على تحليل الإجراءات المتخذة على الكائن. على سبيل المثال، عند العمل على مستند Microsoft Office، يفحص Kaspersky Endpoint Security الملف عند فتحه لأول مرة وإغلاقه لآخر مرة. أما العمليات التي تجرى أثناء فتح الملف والتي يتم فيها استبدال الملف فلا تتسبب في فحصه. **عند الوصول والتعديل**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائنات عند وجود محاولة لفتحها أو تعديلها. **عند الوصول**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائنات عند محاولة فتحها فقط. **عند التنفيذ**. في هذا الوضع، يفحص مكون الحماية من تهديدات الملفات الكائنات عند محاولة تشغيلها فقط.
استخدام تقنية iSwift (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء ملفات من الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. وتعتبر تقنية iSwift تقدمًا لتقنية iChecker لنظام الملفات NTFS.
استخدام تقنية iChecker (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تسمح هذه التقنية بزيادة سرعة الفحص من خلال استثناء ملفات معينة من الفحص. يتم استثناء الملفات من عمليات الفحص باستخدام خوارزمية خاصة تراعي تاريخ إصدار قواعد بيانات Kaspersky Endpoint Security وآخر تاريخ لفحص الكائن وأي تعديلات على إعدادات الفحص. توجد قيود على تقنية iChecker: لا تعمل هذه التقنية مع الملفات الكبيرة ولا تنطبق إلا على الملفات التي يمكن للتطبيق التعرف على بنيتها (على سبيل المثال، EXE وDLL وLNK وTTF وINF وSYS وCOM وCHM وZIP وRAR).
إيقاف الحماية من تهديد الملفات مؤقتًا (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	يؤدي هذا إلى إيقاف تشغيل الحماية من تهديدات الملفات مؤقتًا وتلقائيًا في الوقت المحدد أو عند العمل مع التطبيقات المحددة.

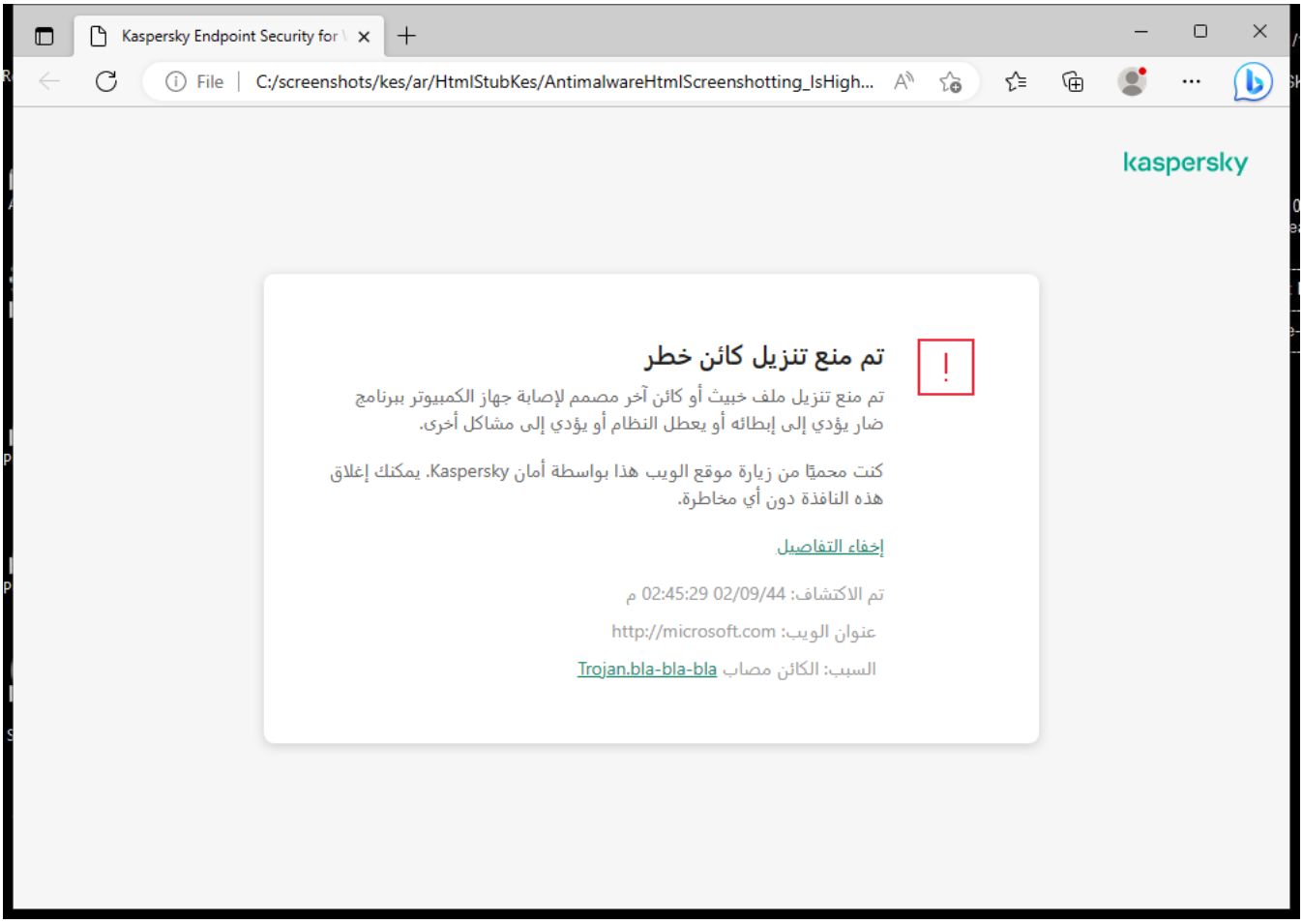
الحماية من تهديدات الويب

يمنع مكون الحماية من تهديدات الويب تنزيلات الملفات الضارة عبر الإنترنت، ويحظر أيضًا مواقع الويب الضارة والاحتيالية. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

يفحص برنامج Kaspersky Endpoint Security حركة مرور HTTP، وHTTPS، وFTP. إن Kaspersky Endpoint Security يفحص عناوين URL وعناوين IP. يمكنك تحديد المنافذ التي يراقبها Kaspersky Endpoint Security، أو تحديد كل المنافذ.

لمراقبة حركة مرور HTTPS، تحتاج إلى تمكين عمليات فحص الاتصالات المشفرة.

عندما يحاول مستخدم فتح موقع إلكتروني ضار أو احتيالي، فإن Kaspersky Endpoint Security سوف يحجب الوصول إلى ذلك الموقع ويعرض تحذيرًا (راجع الشكل أدناه).



رسالة رفض الوصول الخاص بموقع الويب

إعدادات مكون الحماية من تهديدات الويب

المعلمة	الوصف
مستوى الأمان (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	للحماية من تهديدات الويب، فإن التطبيق باستطاعته تطبيق مجموعات مختلفة من الإعدادات. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان: • **مرتفع**. مستوى الأمان الذي ينفذ مكون الحماية من تهديدات الويب من خلاله الحد الأقصى من الفحص لحركة المرور على الويب التي يتلقاها الكمبيوتر عبر بروتوكولات HTTP وFTP. ينفذ مكون الحماية من تهديدات الويب فحصًا مفصلاً لجميع كائنات حركة المرور على الويب باستخدام المجموعة الكاملة من قواعد بيانات التطبيق وينفذ أعمق تحليل مساعد على الاكتشاف ممكن. • **مستحسن**. مستوى الأمان الذي يوفر التوازن المثالي بين أداء Kaspersky Endpoint Security وأمان حركة المرور على الويب. وينفذ مكون الحماية من تهديدات الويب التحليل المساعد على الاكتشاف وفقًا لمستوى فحص متوسط. ويوصي الخبراء في Kaspersky بهذا المستوى من أمان حركة المرور على الويب. • **منخفض**. تضمن إعدادات هذا المستوى من أمان حركة الويب أقصى سرعة فحص لحركة الويب. وينفذ مكون الحماية من تهديدات الويب التحليل المساعد على الاكتشاف وفقًا لمستوى فحص خفيف.
الإجراء المطلوب	**منع**. إذا تم تحديد هذ الاختيار واكتشاف كائن مصاب في حركة المرور على الويب، يمنع مكون الحماية من تهديدات الويب

اتخاذه عند اكتشاف تهديد	الوصول إلى الكائن ويعرض رسالةً في المستعرض. **إعلام**. إذا تم تحديد هذا الخيار وتم اكتشاف كائن مصاب في حركة المرور على الويب، فإن Kaspersky Endpoint Security يسمح بتنزيل هذا الكائن إلى الكمبيوتر ولكنه يضيف معلومات حول الكائن المصاب إلى قائمة التهديدات النشطة.
التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الخبيثة (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	يسمح لك فحص الروابط لتحديد ما إذا كانت مدرجة في قاعدة بيانات عناوين الويب الضارة بتتبع مواقع الويب التي تم إضافتها إلى قائمة الرفض. يتم الاحتفاظ بقاعدة بيانات عناوين الويب الضارة بواسطة Kaspersky وتضمينها في حزمة تثبيت التطبيق وإكمال تحديثات قاعدة بيانات Kaspersky Endpoint Security.
استخدام التحليل المساعد على الاكتشاف (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف. عند فحص حركة الويب للبحث عن الفيروسات والتطبيقات الأخرى التي تشكل تهديدًا، ينفذ المحلل المساعد على الاكتشاف التعليمات المدرجة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
التحقق من عنوان الويب مقابل قاعدة بيانات عناوين الويب الاحتيالية (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تتضمن قاعدة بيانات مواقع الويب الاحتيالية عناوين الويب الخاصة بمواقع الويب المعروف حاليًا أنها تُستخدم في بدء الهجمات الاحتيالية. وتستكمل Kaspersky قاعدة بيانات الروابط الاحتيالية هذه بالعناوين التي يتم الحصول عليها من المنظمة الدولية المعروفة باسم "مجموعة عمل مكافحة الاحتيال". يتم تضمين قاعدة بيانات العناوين الاحتيالية في حزمة تثبيت التطبيق وإكمال تحديثات قاعدة بيانات Kaspersky Endpoint Security.
عدم فحص حركة المرور على الويب من عناوين الويب الموثوقة	في حالة تحديد خانة الاختيار هذه، لا يفحص مكون الحماية من تهديدات الويب محتوى صفحات الويب أو مواقع الويب التي تم تضمين عناوينها في قائمة عناوين الويب الموثوقة. يمكنك إضافة كلاً من العنوان المحدد وقناع عنوان صفحة الويب / موقع الويب إلى قائمة عناوين الويب الموثوقة. يمكنك أيضا إنشاء قائمة عامة باستثناءات الاتصالات المشفرة. وفي هذه الحالة، لا يفحص Kaspersky Endpoint Security حركة مرور HTTPS لعناوين الويب الموثوقة عندما يؤدي مكونات الحماية من تهديدات الويب والحماية من تهديدات البريد والتحكم في الويب عملها.

الحماية من تهديدات البريد

يفحص مكون الحماية من تهديدات البريد مرفقات رسائل البريد الإلكتروني الصادرة والواردة للحماية من الفيروسات والتهديدات الأخرى. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

تستطيع الحماية من تهديدات البريد فحص كل من الرسائل الواردة والصادرة. ويدعم التطبيق بروتوكولات POP3 وSMTP وIMAP وNNTP في عملاء البريد التاليين:

- Microsoft Office Outlook
- Mozilla Thunderbird

- Windows Mail

لا تدعم الحماية من تهديدات البريد البروتوكولات وعملاء البريد الآخرين.

قد لا تتمكن الحماية من تهديدات البريد دائمًا من الحصول على الوصول إلى الرسائل على مستوى البروتوكول (على سبيل المثال، عند استخدام حل Microsoft Exchange). ولهذا السبب، تتضمن الحماية من تهديدات البريد ملحقًا لبرنامج Microsoft Office Outlook. ويسمح الملحق بفحص الرسائل على مستوى عميل البريد. يدعم ملحق الحماية من تهديدات البريد العمليات باستخدام Outlook 2010 و2013 و2016 و2019.

لا يقوم مكون الحماية من تهديدات البريد بفحص الرسائل إذا كان عميل البريد مفتوحًا في مستعرض.

عند اكتشاف ملف ضار في مرفق، يضيف Kaspersky Endpoint Security معلومات عن الإجراء المتخذ إلى موضوع الرسالة، على سبيل المثال: [تمت معالجة الرسالة] <موضوع الرسالة>.

إعدادات مكون الحماية من تهديدات البريد

المعلمة	الوصف
مستوى الأمان (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	وللحماية من تهديدات البريد، يطبق Kaspersky Endpoint Security مجموعات مختلفة من الإعدادات. تُسمى مجموعات الإعدادات المخزنة في التطبيق مستويات الأمان: • **مرتفع**. عند تحديد مستوى أمان البريد الإلكتروني هذا، يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني بشكل أكثر شمولاً. يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني الواردة والصادرة ويقوم بإجراء تحليل مساعد على الاكتشاف عميق. ويُوصى بمستوى أمان البريد "مرتفع" للبيئات عالية المخاطر. ومن الأمثلة على هذه البيئات، الاتصال بخدمة بريد إلكتروني مجانية من شبكة اتصال منزلية ليست محمية بواسطة حماية البريد الإلكتروني المركزية. • **مستحسن**. مستوى أمان البريد الإلكتروني الذي يوفر التوازن الأمثل بين أداء Kaspersky Endpoint Security وأمان البريد الإلكتروني. يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني الواردة والصادرة ويقوم بإجراء تحليل مساعد على الاكتشاف متوسط المستوى. يوصى بمستوى أمان حركة البريد هذا بواسطة مختصي Kaspersky. • **منخفض**. عندما يتم تحديد مستوى أمان البريد الإلكتروني هذا، يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني الواردة فقط، وينفذ تحليلاً مساعدًا على الاكتشاف خفيفًا، ولا يفحص الأرشيفات الملحقة برسائل البريد الإلكتروني. في مستوى أمان البريد هذا، يفحص مكون الحماية من تهديدات البريد رسائل البريد الإلكتروني بأقصى سرعة ويستخدم الحد الأدنى من موارد نظام التشغيل. ويُوصى باستخدام مستوى أمان البريد "منخفض" في بيئة محمية جيدًا. وقد يكون أحد الأمثلة على هذه البيئة شبكة المنطقة المحلية (LAN) للمؤسسة مع أمان مركزي للبريد الإلكتروني.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**تنظيف؛ حذف إذا فشل التنظيف**. عند اكتشاف كائن مصاب في رسالة واردة أو صادرة، يحاول Kaspersky Endpoint Security تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف Kaspersky Endpoint Security الكائن المصاب. ويضيف Kaspersky Endpoint Security معلومات عن الإجراء المتخذ إلى موضوع الرسالة، على سبيل المثال: [تمت معالجة الرسالة] <موضوع الرسالة>. **تنظيف؛ منع إذا فشل التنظيف**. عند اكتشاف كائن مصاب في رسالة واردة، يحاول Kaspersky Endpoint Security تنظيف الكائن المحدد. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يضيف Kaspersky Endpoint Security تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. عندما يتم اكتشاف كائن مصاب في رسالة صادرة، يحاول Kaspersky Endpoint Security تنظيف الكائن الذي تم اكتشافه. إذا تعذّر تنظيف الكائن، يقوم Kaspersky Endpoint Security بحظر إرسال الرسالة ويظهر عميل البريد خطأ. **منع**. في حالة اكتشاف كائن مصاب في رسالة واردة، يضيف Kaspersky Endpoint Security تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. إذا تم اكتشاف كائن مصاب في رسالة صادرة، يقوم Kaspersky Endpoint Security بحظر إرسال الرسالة، ويظهر عميل البريد خطأ.
نطاق الحماية (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint Security)	يتضمن نطاق الحماية الكائنات التي يتحقق منها المكون عند تشغيله: الرسائل الواردة والصادرة أو الرسائل الواردة فقط. لحماية أجهزة الكمبيوتر الخاصة بك، ما عليك سوى فحص الرسائل الواردة. ويمكنك تشغيل الفحص للبحث عن الرسائل الصادرة لمنع إرسال الملفات المصابة في الأرشيفات. ويمكنك أيضًا تشغيل فحص الرسائل الصادرة إذا كنت تريد منع إرسال ملفات ذات تنسيقات محددة، مثل ملفات الصوت والفيديو، على سبيل المثال.

فحص حركة POP3 وSMTP وNNTP وIMAP	تؤدي خانة الاختيار إلى تمكين / تعطيل الفحص حسب مكون الحماية من تهديدات البريد للحركة التي يتم نقلها عبر بروتوكولات POP3 وSMTP وNNTP وIMAP.
توصيل ملحق Microsoft Outlook	إذا تم تحديد خانة الخيار يتم تمكين فحص رسائل البريد الإلكتروني التي يتم بثها عبر البروتوكولات POP3 وSMTP وNNTP وIMAP على جانب الملحق المدمج في Microsoft Outlook. في حالة فحص البريد باستخدام ملحق برنامج Microsoft Outlook، فمن المستحسن استخدام وضع Exchange المُخَزَّن مؤقتًا. للمزيد من المعلومات التفصيلية حول وضع التبادل المخزن مؤقتًا والتوصيات حول استخدامه، يُرجى الرجوع إلى قاعدة معارف Microsoft.
التحليل المساعد على الاكتشاف (متوفر فقط في وحدة تحكم الإدارة (MMC) وواجهة Kaspersky Endpoint (Security	تقنية تم تصميمها لاكتشاف التهديدات التي لا يمكن اكتشافها باستخدام الإصدار الحالي لقواعد بيانات تطبيق Kaspersky. يكتشف الملفات المشتبه في كونها مصابة بفيروس غير معروف أو نوع جديد من فيروس معروف. عند فحص الملفات للبحث عن تعليمات برمجية ضارة، ينفذ المحلل المساعد على الاكتشاف الإرشادات الواردة في الملفات القابلة للتنفيذ. ويعتمد عدد الإرشادات التي يتم تنفيذها بواسطة المحلل المساعد على الاكتشاف على المستوى المحدد للمحلل المساعد على الاكتشاف. يضمن مستوى للتحليل المساعد على الاكتشاف التوازن بين شمولية البحث عن تهديدات جديدة، والتحميل على موارد نظام التشغيل، ومدة التحليل المساعد على الاكتشاف.
فحص الأرشيفات المرفقة	فحص تنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE وتنسيقات الأرشيفات الأخرى. يفحص التطبيق الأرشيفات ليس فقط حسب الملحق، لكن أيضًا حسب التنسيق. عند التحقق من الأرشيفات، ينفذ التطبيق عملية تفريغ متكررة. ويسمح هذا باكتشاف التهديدات داخل أرشيفات متعددة المستويات (أرشيف داخل أرشيف). إذا اكتشف Kaspersky Endpoint Security أثناء الفحص كلمة مرور لأرشيف في نص الرسالة، فسيتم استخدام كلمة المرور هذه لفحص محتوى الأرشيف للبحث عن التطبيقات الضارة. وفي هذه الحالة، لا يتم حفظ كلمة المرور. ويتم فك الأرشيف أثناء الفحص. وفي حالة حدوث خطأ في التطبيق أثناء عملية الفك، يمكنك يدويًا حذف الملفات غير المضغوطة المحفوظة في المسار التالي: %systemroot%\temp. تتضمن الملفات بادئة PR.
فحص الملفات المرفقة بتنسيقات Microsoft Office	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
عدم فحص الأرشيفات الأكبر من N ميجابايت	في حالة تحديد خانة الاختيار هذه، فإن مكون الحماية من تهديدات البريد يستثني الأرشيفات المرفقة برسائل البريد الإلكتروني من الفحص إذا تجاوز حجمها القيمة المحددة. في حالة إلغاء تحديد خانة الاختيار، يفحص مكون الحماية من تهديدات البريد الأرشيفات المرفقة بالبريد الإلكتروني أيًا كان حجمها.
تقييد الوقت للتحقق من الأرشيفات إلى N ثانية	إذا تم تحديد خانة الاختيار، فإن الوقت المخصص لفحص الأرشيفات المرفقة في رسائل البريد الإلكتروني يكون مقصورًا على المدة المحددة.
عامل تصفية المرفقات	لا يتم تطبيق عامل تصفية المرفقات على رسائل البريد الإلكتروني الصادرة. **تعطيل التصفية**. في حالة تحديد هذا الخيار، لا يقوم مكون الحماية من تهديدات البريد بتصفية الملفات المرفقة مع رسائل البريد الإلكتروني.

	إعادة تسمية المرفقات من الأنواع المحددة. في حالة تحديد هذا الخيار، يستبدل مكون الحماية من تهديدات البريد آخر حرف في الملفات المرفقة من الأنواع المحددة برمز تسطير أسفل السطر (على سبيل المثال، _). وبالتالي، لفتح الملف، يجب على المستخدم إعادة تسميته. **حذف المرفقات من الأنواع المحددة**. في حالة تحديد هذا الخيار، يقوم مكون الحماية من تهديدات البريد بحذف الملفات المرفقة من الأنواع المحددة من رسائل البريد الإلكتروني. في القائمة التي تحتوي على أقنعة الملفات يمكنك تحديد أنواع الملفات المرفقة لإعادة تسميتها أو حذفها من رسائل البريد الإلكتروني.

الحماية من تهديدات الشبكة

يراقب مكون الحماية من تهديدات الشبكة (يسمى أيضًا نظام اكتشاف التطفل) حركة شبكة الاتصال\ الواردة للبحث عن خاصية النشاط لهجمات الشبكة. عندما يكتشف Kaspersky Endpoint Security محاولة هجوم على الشبكة على كمبيوتر المستخدم، فإنه يحظر اتصال الشبكة مع الكمبيوتر المهاجم. تتوفر أوصاف لأنواع هجمات الشبكة المعروفة حاليًا وطرق إبطالها في قواعد بيانات Kaspersky Endpoint Security. يتم تحديث قائمة هجمات الشبكة التي يكتشفها مكون الحماية من تهديدات الشبكة أثناء تحديثات قاعدة البيانات والوحدة النمطية للتطبيق.

إعدادات مكون الحماية من تهديدات الشبكة

المعلمة	الوصف
التعامل مع فحص المنافذ وإغراق الشبكة كهجمات	إغراق الشبكة هو هجوم على موارد شبكة الاتصال لمؤسسة ما (مثل خوادم الويب). يتكون هذا الهجوم من إرسال عدد كبير من الطلبات لزيادة الحمل على النطاق الترددي لموارد شبكة الاتصال. وعند حدوث ذلك، يتعذر على المستخدمين الوصول إلى موارد شبكة الاتصال الخاصة بالمؤسسة. يتكون هجوم فحص المنفذ من فحص منافذ UDP ومنافذ TCP وخدمات الشبكة على الكمبيوتر. ويسمح هذا الهجوم للمهاجم بتحديد درجة الثغرات الأمنية للكمبيوتر قبل تنفيذ أنواع أكثر خطورة من هجمات شبكة الاتصال. ويتيح فحص المنفذ أيضًا للمهاجم التعرف على نظام التشغيل على الكمبيوتر وتحديد هجمات شبكة الاتصال المناسبة لنظام التشغيل هذا. في حالة تحديد خانة الاختيار هذه، يراقب Kaspersky Endpoint Security حركة شبكة الاتصال لاكتشاف هذه الهجمات. في حالة اكتشاف هجوم، يخطر التطبيق المستخدم ويرسل الحدث المقابل إلى Kaspersky Security Center. ويوفر التطبيق معلومات عن الكمبيوتر المهاجم، وهو أمر مطلوب لاتخاذ إجراءات الاستجابة للتهديد في الوقت المناسب. يمكنك تعطيل اكتشاف هذه الأنواع من الهجمات في حالة إجراء بعض التطبيقات المسموح بها عمليات نموذجية لهذه الأنواع من الهجمات. وسوف يساعد هذا في تجنب الإنذارات الكاذبة.
حظر الأجهزة التي تنفذ الهجوم لمدة N دقيقة	في حالة تحديد خانة الاختيار، يضيف مكون الحماية من تهديدات الشبكة الكمبيوتر المهاجم إلى قائمة المنع. وهذا يعني أن مكون الحماية من تهديدات الشبكة يمنع اتصال الشبكة بالكمبيوتر المهاجم بعد أول محاولة لهجوم الشبكة لمدة محددة من الوقت. ويؤدي هذا المنع إلى وجود حماية تلقائية لكمبيوتر المستخدم ضد هجمات الشبكة المستقبلية المحتملة من نفس العنوان. الحد الأدنى للوقت الذي يجب أن يقضيه الكمبيوتر المهاجم في قائمة الحظر هو دقيقة واحدة. ويبلغ الحد الأقصى للوقت 999 دقيقة. يمكنك عرض قائمة المنع في النافذة أداة مراقبة شبكة الاتصال. يمسح Kaspersky Endpoint Security قائمة المنع عند إعادة تشغيل التطبيق وعندما تتغير إعدادات الحماية من تهديدات الشبكة.
الاستثناءات	تحتوي القائمة على عناوين IP التي لا يمنع مكون الحماية من تهديدات الشبكة هجمات الشبكة منها. لا يسجل التطبيق معلومات عن هجمات الشبكة من خلال عناوين IP الواردة في قائمة الاستثناءات.
الحماية ضد انتحال عنوان MAC	يتألف هجوم انتحال عنوان MAC من تغيير عنوان MAC الخاص بجهاز شبكة (بطاقة الشبكة). ونتيجة لذلك، يمكن للمهاجم إعادة توجيه البيانات المرسلة إلى جهاز إلى جهاز آخر والوصول إلى هذه البيانات. يتيح لك Kaspersky Endpoint Security حظر هجمات انتحال عنوان MAC وتلقي إشعارات حول الهجمات.

جدار الحماية

يقوم جدار الحماية بحظر الاتصالات غير المصرح بها للكمبيوتر أثناء العمل على الإنترنت أو الشبكة المحلية. يتحكم جدار الحماية كذلك في نشاط الشبكة للتطبيقات على الكمبيوتر. يسمح لك هذا بحماية الشبكة المحلية الخاصة بشركتك من سرقة الهوية والهجمات الأخرى. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك قواعد الشبكة المحددة مسبقًا.

يتم استخدام وكيل الشبكة للتفاعل مع Kaspersky Security Center. ينشئ جدار الحماية تلقائيًا قواعد الشبكة المطلوبة لكي يعمل التطبيق ووكيل الشبكة. ونتيجة لذلك، يفتح جدار الحماية عدة منافذ على الكمبيوتر. وتعتمد المنافذ المفتوحة على دور الكمبيوتر (على سبيل المثال، نقطة توزيع). ولمعرفة المزيد حول المنافذ التي سيتم فتحها على الكمبيوتر، يرجى الرجوع إلى تعليمات Kaspersky Security Center .

قواعد الشبكة

يمكنك تكوين قواعد الشبكة على المستويات التالية:

- قواعد حزمة الشبكة. تفرض قواعد حزمة الشبكة قيودًا على حزمة الشبكة، بغض النظر عن التطبيق. وتُقيد هذه القواعد من حركة مرور الشبكة الصادرة والواردة من خلال منافذ معينة لبروتوكول البيانات المحدد. قام Kaspersky Endpoint Security بتعريف قواعد حزم الشبكة مسبقًا مع الأذونات التي أوصى بها خبراء Kaspersky.
- قواعد الشبكة للتطبيق. تفرض قواعد الشبكة للتطبيق قيودًا على نشاط الشبكة الخاص بتطبيق معين. لا يعتبر العامل بمثابة خصائص لحزمة الشبكة فقط، لكنه أيضًا تطبيقًا معينًا يقوم بمخاطبة حزمة الشبكة هذه أو أنه أصدر هذه الحزمة.

يتم توفير الوصول المحكوم للتطبيقات إلى موارد نظام التشغيل والعمليات والبيانات الشخصية من خلال مكون منع اختراق المضيف باستخدام حقوق التطبيق.

أثناء بدء التشغيل الأول للتطبيق، يقوم جدار الحماية بتنفيذ الإجراءات التالية:

1. يتحقق من أمان التطبيق باستخدام قواعد بيانات مكافحة الفيروسات التي تم تنزيلها.
2. سيتحقق من درجة أمان التطبيق في شبكة Kaspersky Security Network.

   ننصحك بالمشاركة في شبكة Kaspersky Security Network لمساعدة جدار الحماية على العمل بفعالية أكثر.
3. يضع التطبيق في إحدى مجموعات الثقة: موثوق، مقيد بشكل منخفض، مقيد بشكل عالٍ، غير موثوق.

   تحدد مجموعة ثقة الحقوق التي يشير إليها Kaspersky Endpoint Security عند التحكم في نشاط التطبيق. يضع Kaspersky Endpoint Security تطبيقًا في مجموعة ثقة بناءً على مستوى الخطر الذي قد يشكله هذا التطبيق على الكمبيوتر.

يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة لمكونات جدار الحماية ومنع اختراق المضيف. لا يمكنك تغيير مجموعة الثقة فقط لجدار الحماية أو منع اختراق المضيف.

إذا رفضت المشاركة في KSN أو لم تكن هناك شبكة، يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة اعتمادًا على إعدادات مكون منع اختراق المضيف. بعد استلام سمعة التطبيق من KSN، يمكن تغيير مجموعة الثقة تلقائيًا.

4. هذا يحظر نشاط الشبكة للتطبيق، اعتمادًا على مجموعة الثقة. على سبيل المثال: لا يُسمح للتطبيقات الموجودة في مجموعة الثقة مقيد بشكل عالٍ باستخدام أي اتصالات شبكة.

في المرة التالية التي يعمل فيها التطبيق، يتحقق Kaspersky Endpoint Security من سلامة التطبيق. في حالة عدم تغير التطبيق، يستخدم المكون قواعد الشبكة الحالية عليه. في حالة تعديل التطبيق، فإن Kaspersky Endpoint Security يحلل التطبيق كما لو كان يجرى تشغيله لأول مرة.

أولويات قاعدة الشبكة

لكل قاعدة أولوية. كلما كانت القاعدة تحتل مرتبة أعلى في القائمة، فإنها تكون ذات أولوية أعلى. إذا تمت إضافة نشاط شبكة إلى عدة قواعد، ينظم جدار الحماية نشاط الشبكة وفقًا للقاعدة ذات أعلى أولوية.

قواعد حزمة الشبكة لها أولوية أعلى من قواعد الشبكة الخاصة بالتطبيقات. إذا تم تحديد كل من قواعد حزمة الشبكة وقواعد الشبكة الخاصة بالتطبيقات لنفس نوع نشاط الشبكة، فسيتم معالجة نشاط هذه الشبكة وفقًا لقواعد حزمة الشبكة.

تعمل قواعد الشبكة للتطبيقات بطريقة معينة. وتتضمن قاعدة الشبكة للتطبيقات قواعد الوصول بناءً على حالة الشبكة: الشبكة العامة والشبكة المحلية والشبكة الموثوقة. على سبيل المثال: التطبيقات في مجموعة الثقة مقيد بشكل عالٍ غير مسموح لها بأي نشاط على الشبكة في الشبكات بجميع الحالات، وذلك في الوضع الافتراضي. إذا كانت قاعدة شبكة محددة لتطبيق معين (تطبيق أصلي) فإن العمليات الفرعية للتطبيقات الأخرى سوف تسير وفق قاعدة الشبكة للتطبيق الأصلي. في حالة عدم وجود قاعدة شبكة للتطبيق، فإن العمليات الفرعية سوف تسري وفق قاعدة وصول الشبكة لمجموعة ثقة التطبيق.

على سبيل المثال: لقد منعت أي نشاط على الشبكة في جميع الشبكات بجميع الحالات لجميع التطبيقات باستثناء المستعرض س. بالتالي إذا بدأت تثبيت المستعرض ص (عملية فرعية) من المستعرض س (التطبيق الأصل)، فإن مثبت المستعرض ص سيتمكن من الوصول للشبكة وتنزيل الملفات الضرورية. بعد التثبيت لن يقدر المستعرض ص على الاتصال بأي شبكة، وذلك وفق إعدادات جدار الحماية. لمنع نشاط الشبكة لمثبت المستعرض ص كعملية فرعية، يجب أن تضيف قاعدة شبكة لمثبت المستعرض ص.

حالات اتصال الشبكة

يسمح لك جدار الحماية بالتحكم في نشاط الشبكة اعتمادًا على حالة اتصال الشبكة. يتلقى Kaspersky Endpoint Security حالة اتصال الشبكة من نظام تشغيل الكمبيوتر. يقوم المستخدم بتعيين حالة اتصال الشبكة في نظام التشغيل عند إعداد الاتصال. يمكنك تغيير حالة اتصال الشبكة في إعدادات Kaspersky Endpoint Security. سيراقب جدار الحماية نشاط الشبكة اعتمادًا على حالة الشبكة في إعدادات Kaspersky Endpoint Security وليس في نظام التشغيل.

يمكن أن يشتمل اتصال الشبكة على أنواع الحالة التالية:

- **الشبكة العامة**. الشبكة غير محمية بتطبيقات مكافحة الفيروسات أو جدران الحماية أو المرشحات (مثل Wi-Fi في مقهى). عندما يقوم المستخدم بتشغيل كمبيوتر متصل بشبكة كهذه، فإن جدار الحماية يحجب الوصول إلى الملفات والطابعات على هذا الكمبيوتر. ويتعذر أيضًا على المستخدمين الخارجين الوصول إلى البيانات من خلال مجلدات المشاركة والوصول عن بُعد إلى سطح مكتب هذا الكمبيوتر. يقوم جدار الحماية بتصفية نشاط الشبكة لكل تطبيق حسب قواعد الشبكة التي تم تعيينها له.

  ويقوم جدار الحماية بتعيين حالة الشبكة العامة إلى الإنترنت بشكل افتراضي. لا يمكنك تغيير حالة الإنترنت.

- **الشبكة المحلية**. شبكة للمستخدمين الذين لديهم وصول مقيد إلى الملفات والطابعات على هذا الكمبيوتر (مثل الشبكة المحلية للشركات أو الشبكة المنزلية).

- **الشبكة الموثوقة**. شبكة آمنة لا يتعرض فيها الكمبيوتر للهجمات أو محاولات الوصول للبيانات غير المسموح بها. ويسمح جدار الحماية بأي نشاط للشبكة ضمن الشبكات التي تتمتع بهذه الحالة.

إعدادات مكون جدار الحماية

المعلمة	الوصف
قواعد الحزمة	جدول يحتوي على قواعد حزمة الشبكة. تفرض قواعد حزمة الشبكة قيودًا على حزم الشبكة، بغض النظر عن التطبيق. وتُقيد هذه القواعد من حركة مرور الشبكة الصادرة والواردة من خلال منافذ معينة لبروتوكول البيانات المحدد. ويتضمن الجدول قواعد حزم الشبكة التي تم تكوينها مسبقًا والتي يُنصح بها من قبل Kaspersky للحصول على الحماية المثلى لحركة مرور شبكة اتصال أجهزة الكمبيوتر التي تعمل بنظم التشغيل Microsoft Windows. ويقوم جدار الحماية بتعيين أولوية التنفيذ لكل قاعدة حزمة شبكة اتصال. ويقوم جدار الحماية بمعالجة قواعد حزم شبكة الاتصال بنفس الترتيب الذي تظهر به في قائمة قواعد حزم شبكة الاتصال، من أعلى إلى الأسفل. يقوم جدار الحماية بتحديد أفضل قاعدة لحزمة الشبكة المناسبة لاتصال الشبكة وتطبيقها إما عن طريق السماح أو حظر نشاط الشبكة. وبعد ذلك يتجاهل جدار الحماية جميع قواعد حزم الشبكة اللاحقة لاتصال الشبكة المحدد. قواعد حزمة الشبكة لها أولوية أعلى من قواعد الشبكة الخاصة بالتطبيقات.
الشبكات	يحتوي هذا الجدول على معلومات حول اتصالات الشبكة التي يكتشفها جدار الحماية على الكمبيوتر.

المتاحة	ويتم تخصيص حالة الشبكة العامة للإنترنت بشكل افتراضي. لا يمكنك تغيير حالة الإنترنت.
قواعد التطبيقات	**التطبيق** قائمة بالتطبيقات التي يتحكم فيها مكون جدار الحماية. يتم تعيين التطبيقات إلى مجموعات موثوقة. تحدد مجموعة الثقة الحقوق التي يستخدمها Kaspersky Endpoint Security عند التحكم في نشاط الشبكة للتطبيقات. يمكنك تحديد تطبيق من قائمة واحدة لجميع التطبيقات المثبتة على أجهزة الكمبيوتر تحت تأثير سياسة وإضافة التطبيق إلى مجموعة ثقة. **قواعد شبكة الاتصال** جدول قواعد الشبكة للتطبيقات التي تشكل جزءًا من مجموعة ثقة. وفقًا لهذه القواعد، يقوم جدار الحماية بتنظيم نشاط الشبكة للتطبيق. يعرض الجدول قواعد الشبكة المحددة مسبقًا التي يوصي بها خبراء Kaspersky. تم إضافة قواعد الشبكة هذه لحماية حركة مرور الشبكة لأجهزة الكمبيوتر التي تعمل بأنظمة تشغيل Windows على النحو الأمثل. لا يمكن حذف قواعد الشبكة المحددة مسبقًا.

منع هجمات BadUSB

تقوم بعض الفيروسات بتعديل البرامج الثابتة لأجهزة USB، بهدف خداع نظام التشغيل ليكتشف جهاز USB على أنه لوحة مفاتيح. نتيجة لذلك، قد ينفذ الفيروس أوامر من حساب المستخدم الخاص بك لتنزيل البرامج الضارة، على سبيل المثال.

يمنع المكون "منع هجمات BadUSB" أجهزة USB المصابة من محاكاة لوحة المفاتيح للاتصال بالكمبيوتر.

عند توصيل جهاز USB بالكمبيوتر وتم التعرف عليه كلوحة مفاتيح بواسطة نظام التشغيل، يطلب التطبيق من المستخدم إدخال رمز رقمي يتم إنشاؤه بواسطة التطبيق من لوحة المفاتيح هذه أو باستخدام لوحة المفاتيح على الشاشة إذا كانت متاحة (انظر الشكل أدناه). يُعرف هذا الإجراء باسم مصادقة لوحة المفاتيح.

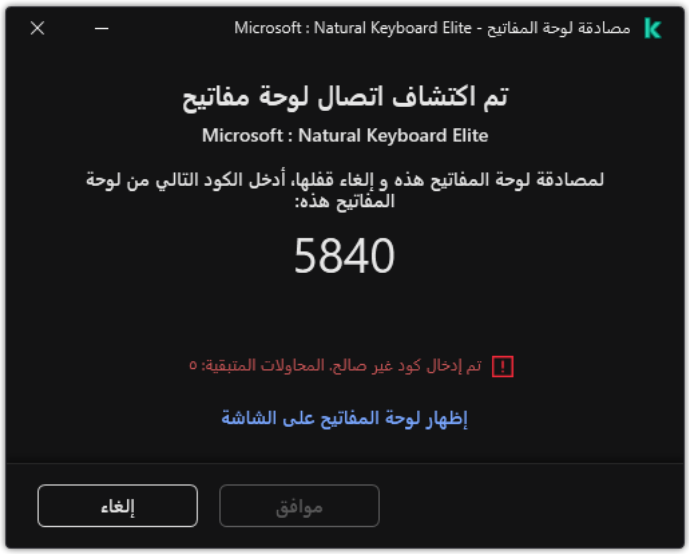
إذا تم إدخال الرمز بشكل صحيح، فيقوم التطبيق بحفظ معلمات التعريف – VID/PID للوحة المفاتيح ورقم المنفذ الذي تم توصيلها به – في قائمة لوحات المفاتيح المصرح لها. لا يلزم تكرار مصادقة لوحة المفاتيح عند إعادة توصيل لوحة المفاتيح أو بعد إعادة تشغيل نظام التشغيل.

عندما يتم توصيل لوحة المفاتيح المصرح لها بمنفذ مختلف في الكمبيوتر، يقوم التطبيق بإظهار مطالبة بالحصول على تصريح للوحة المفاتيح هذه مرة أخرى.

إذا تم إدخال الرمز الرقمي بطريقة غير صحيحة، فيقوم التطبيق بإنشاء رمز جديد. يمكنك تكوين عدد محاولات إدخال الرمز العددي. وفي حالة إدخال الرمز العددي بشكل غير صحيح عدة مرات أو إغلاق نافذة مصادقة لوحة المفاتيح (انظر الشكل أدناه)، فإن التطبيق يحظر الإدخال من لوحة المفاتيح هذه. وعند انقضاء وقت منع جهاز USB أو إعادة تشغيل نظام التشغيل، يطالب التطبيق المستخدم بإجراء مصادقة للوحة المفاتيح مرة أخرى.

يتيح التطبيق استخدام لوحة مفاتيح مصرح لها، ويمنع لوحة المفاتيح التي لم يتم التصريح لها.

لا يتم تثبيت مكون الوقاية من هجمات USB الخبيثة بشكل افتراضي. إذا كنت بحاجة إلى مكون الوقاية من هجمات USB الخبيثة، يمكنك إضافة المكون في خصائص حزمة التثبيت قبل تثبيت التطبيق أو تغيير مكونات التطبيق المتاحة بعد تثبيت التطبيق.



مصادقة لوحة المفاتيح

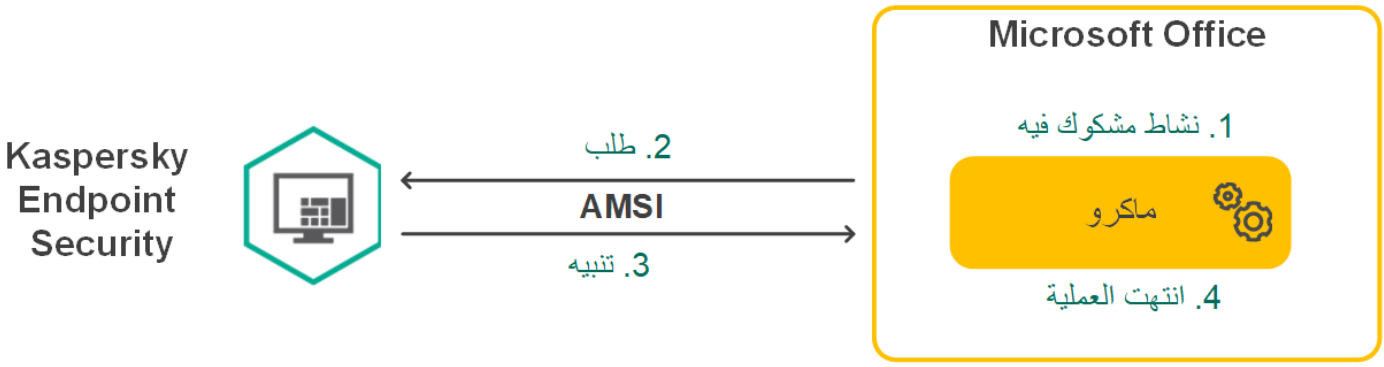
إعدادات مكون منع هجمات BadUSB

المعلمة	الوصف
منع استخدام لوحة المفاتيح على الشاشة لمصادقة أجهزة USB	إذا تم تحديد خانة الاختيار، فيقوم التطبيق بمنع استخدام لوحة المفاتيح على الشاشة للحصول على تصريح لجهاز USB الذي يتعذر إدخال رمز تصريح من خلاله.
الحد الأقصى لعدد محاولات مصادقة جهاز USB	حظر جهاز USB تلقائيًا في حالة إدخال رمز المصادقة بشكل غير صحيح لعدد المرات المحدد. القيم الصالحة من 1 إلى 10. على سبيل المثال، إذا سمحت بخمس محاولات لإدخال رمز المصادقة، فسيتم حظر جهاز USB بعد المحاولة الفاشلة الخامسة. ويعرض Kaspersky Endpoint Security مدة الحظر لجهاز USB. وبعد انقضاء هذا الوقت، يكون لديك 5 محاولات لإدخال رمز المصادقة.
المهلة عند الوصول إلى الحد الأقصى لعدد المحاولات	مدة حظر جهاز USB بعد العدد المحدد من المحاولات الفاشلة لإدخال رمز المصادقة. القيم الصالحة من 1 إلى 180 (دقيقة).

حماية AMSI

يكون مكون حماية AMSI مخصصًا لدعم واجهة فحص البرمجيات الضارة من Microsoft. تتيح واجهة فحص البرمجيات الضارة (AMSI) للتطبيقات الخارجية التي تتمتع بدعم AMSI إرسال الكائنات (على سبيل المثال، البرامج النصية PowerShell) إلى برنامج Kaspersky Endpoint Security لإجراء عملية فحص إضافية واستقبال نتائج الفحص لهذه الكائنات. قد تتضمن التطبيقات الخارجية، على سبيل المثال، تطبيقات Microsoft Office (انظر الشكل أدناه). ولمعرفة التفاصيل حول AMSI، يُرجى الرجوع إلى وثائق Microsoft.

لا يستطيع مكون حماية AMSI سوى اكتشاف التهديدات وإخطار تطبيق خارجي بالتهديد المكتشف. لا يتيح التطبيق الخارجي بعد استلام الإخطار بوجود تهديد تنفيذ إجراءات مشكوك فيها (على سبيل المثال، عمليات الإنهاء).



مثال عملية AMSI

قد يرفض مكون حماية AMSI طلبًا من تطبيق خارجي، على سبيل المثال، إذا تجاوز هذا التطبيق الحد الأقصى لعدد الطلبات في خلال فترة زمنية محددة. يرسل Kaspersky Endpoint Security معلومات بشأن طلب مرفوض من تطبيق تابع لجهة خارجية إلى خادم الإدارة. لا يرفض مكون حماية AMSI الطلبات الواردة من تطبيقات الطرف الثالث التي يتم تمكين التكامل المستمر مع مكون حماية AMSI لأجلها.

تتوفر وظائف مكون حماية AMSI لأنظمة التشغيل التالية المخصصة لمحطات العمل والخوادم:

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise؛
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise؛
- Windows Server 2016 Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2019 Essentials / Standard / Datacenter (بما في ذلك Core Mode)؛
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (بما في ذلك Core Mode).

إعدادات حماية AMSI

المعلمة	الوصف
فحص الأرشيفات	فحص تنسيقات ZIP وGZIP وBZIP وRAR وTAR وARJ وCAB وLHA وJAR وICE وتنسيقات الأرشيفات الأخرى. يفحص التطبيق الأرشيفات ليس فقط حسب الملحق، لكن أيضًا حسب التنسيق. عند التحقق من الأرشيفات، ينفذ التطبيق عملية تفريغ متكررة. ويسمح هذا باكتشاف التهديدات داخل أرشيفات متعددة المستويات (أرشيف داخل أرشيف).
فحص حزم التوزيع	تقوم خانة الاختيار هذه بتمكين/تعطيل فحص حزم التوزيع التابعة لجهة خارجية.
فحص الملفات بتنسيقات Microsoft Office	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. يفحص تطبيق Kaspersky Endpoint Security الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
عدم فك ضغط الملفات المركبة كبيرة الحجم	في حالة تحديد هذا المربع، لا يفحص التطبيق الملفات المركبة إذا كان حجمها يتجاوز القيمة المحددة. في حالة عدم تحديد خانة الاختيار هذه، يفحص التطبيق الملفات المركبة من جميع الأحجام. يفحص التطبيق الملفات الكبيرة التي يتم استخراجها من الأرشيفات بغض النظر عما إذا كانت خانة الاختيار محددة أو لا.

منع الاستغلال

مكون منع الاستغلال يكتشف رمز البرنامج الذي يستفيد من الثغرات الأمنية الموجودة على جهاز الكمبيوتر لاستغلال امتيازات المسؤول أو لتنفيذ أنشطة ضارة. على سبيل المثال، يمكن أن يستخدم المستغلون هجوم تجاوز سعة المخزن المؤقت للقيام بذلك، يُرسل المستغل كمية كبيرة من البيانات إلى تطبيق معرض للاختراق. عند معالجة هذه البيانات، ينفذ التطبيق المعرض للاختراق تعليمات برمجية ضارة. كنتيجة لهذا الهجوم، يمكن أن يبدأ المستغل عملية تثبيت مُصرح بها للبرمجيات الضارة. عند اكتشاف محاولة لتشغيل الملف التنفيذي من تطبيق قابل للاختراق والتي لم يتم تنفيذها من قِبل المستخدم، يحظر برنامج Kaspersky Endpoint Security تشغيل هذا الملف ويقوم بإخطار المستخدم.

إعدادات مكون منع الاستغلال

المعلمة	الوصف
عند اكتشاف استغلال	**منع التشغيل**. في حالة تحديد هذا العنصر، عند اكتشاف استغلال، يمنع Kaspersky Endpoint Security عمليات هذا الاستغلال ويدون إدخال سجل بالمعلومات حول هذا الاستغلال. **إخطار**. في حالة تحديد هذا العنصر، عندما يكتشف Kaspersky Endpoint Security استغلالاً فإنه يسجل إدخالاً يحتوي على معلومات حول الاستغلال ويضيف معلومات حول هذا الاستغلال إلى قائمة التهديدات النشطة.
تمكين حماية ذاكرة عملية النظام	إذا تم تشغيل زر التبديل، يمنع Kaspersky Endpoint Security العمليات الخارجية التي تحاول الوصول إلى ذاكرة عملية النظام.

اكتشاف السلوك

يتلقى مكون اكتشاف السلوك بيانات حول إجراءات التطبيقات على جهاز الكمبيوتر الخاص بك ويقدم هذه المعلومات إلى مكونات الحماية الأخرى لتحسين أدائها. يستخدم مكون اكتشاف السلوك توقيعات تدفق السلوك (BSS) للتطبيقات. إذا كان نشاط تطبيق متطابقًا مع توقيع تدفق سلوك، ينفذ Kaspersky Endpoint Security إجراء الاستجابة المحدد. ويوفر الأداء الوظيفي لبرنامج Kaspersky Endpoint Security المستند إلى توقيعات تدفق السلوك دفاعًا وقائيًا للكمبيوتر.

إعدادات مكون اكتشاف السلوك

المعلمة	الوصف
عند اكتشاف نشاط برنامج ضار	**حذف الملف**. في حالة تحديد هذا الخيار، عند اكتشاف نشاط ضار، يحذف Kaspersky Endpoint Security الملف التنفيذي للتطبيقات الضارة وينشئ نسخة احتياطية من الملف في النسخ الاحتياطي. **إنهاء التطبيق**. في حالة تحديد هذا الخيار، فإنKaspersky Endpoint Security يقوم بإنهاء هذا التطبيق عند اكتشاف وجود أي نشاط ضار. **إخطار**. في حالة تحديد هذا الخيار وتم اكتشاف نشاط ضار لتطبيق ما، فلا يقوم Kaspersky Endpoint Security بإنهاء التطبيق ولكن يضيف معلومات حول نشاط البرمجيات الضارة للتطبيق إلى قائمة التهديدات النشطة.
تمكين حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي	إذا تم تشغيل زر التبديل, يقوم Kaspersky Endpoint Security بتحليل النشاط في المجلدات المشتركة. إذا توافق هذا النشاط مع توقيع تدفق السلوك المشابه للتشفير الخارجي، فإن Kaspersky Endpoint Security يقوم باتخاذ الإجراء المحدد. يمنع Kaspersky Endpoint Security التشفير الخارجي فقط للملفات الموجودة على وسائط ذات نظام ملفات NTFS وليست مشفرة بنظام EFS. • **إخطار**. في حالة تحديد هذا الخيار، عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة، فإن Kaspersky Endpoint Security يضيف معلومات حول هذه المحاولة لتعديل الملفات في المجلدات المشتركة إلى قائمة التهديدات النشطة. • **منع الاتصال لمدة N min**. في حالة تحديد هذا الخيار، عندما يكتشف Kaspersky Endpoint Security محاولة لتعديل الملفات في المجلدات المشتركة، فإنه يمنع الوصول إلى تعديل الملف (القراءة فقط) للجلسة التي بدأت النشاط الضار وينشئ نسخًا احتياطية من الملفات المعدلة.

	في حالة تمكين مكون محرك المعالجة وتحديد الخيار **منع الاتصال لمدة N min**، سيتم استعادة الملفات المعدلة من النسخ الاحتياطية.
الاستثناءات	قائمة أجهزة الكمبيوتر التي يتم مراقبة محاولات تشفير المجلدات المشتركة منها. لتطبيق قائمة استثناءات أجهزة الكمبيوتر من حماية المجلدات المشتركة ضد التشفير الخارجي، يجب عليك تمكين تسجيل الدخول للتدقيق في سياسة تدقيق أمان Windows. تم تعطيل تسجيل الدخول للتدقيق بشكل افتراضي. وللمزيد من التفاصيل حول سياسة التدقيق الأمني Windows، يُرجى زيارة موقع ويب Microsoft.

منع اختراق المضيف

يمنع مكون منع اختراق المضيف التطبيقات من تنفيذ الإجراءات التي قد تكون خطرة على نظام التشغيل ويضمن التحكم في الوصول إلى موارد نظام التشغيل والبيانات الشخصية. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network.

يتحكم المكون في تشغيل التطبيقات باستخدام حقوق التطبيقات . حقوق التطبيقات تتضمن معلمات الوصول التالية:

- الوصول إلى موارد نظام التشغيل (على سبيل المثال، خيارات بدء التشغيل التلقائي ومفاتيح التسجيل)
- الوصول إلى البيانات الشخصية (مثل الملفات والتطبيقات)

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة جدار الحماية باستخدام قواعد الشبكة.

أثناء بدء التشغيل الأول للتطبيق، يقوم مكون منع اختراق المضيف بتنفيذ الإجراءات التالية:

1. يتحقق من أمان التطبيق باستخدام قواعد بيانات مكافحة الفيروسات التي تم تنزيلها.
2. سيتحقق من درجة أمان التطبيق في شبكة Kaspersky Security Network.

ننصحك بالمشاركة في شبكة Kaspersky Security Network لمساعدة مكون منع اختراق المضيف على العمل على نحو أكثر فعالية.

3. يضع التطبيق في إحدى مجموعات الثقة: موثوق، مقيد بشكل منخفض، مقيد بشكل عالٍ، غير موثوق.

تحدد مجموعة ثقة الحقوق التي يشير إليها Kaspersky Endpoint Security عند التحكم في نشاط التطبيق. يضع Kaspersky Endpoint Security تطبيقًا في مجموعة ثقة بناءً على مستوى الخطر الذي قد يشكله هذا التطبيق على الكمبيوتر.

يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة لمكونات جدار الحماية ومنع اختراق المضيف. لا يمكنك تغيير مجموعة الثقة فقط لجدار الحماية أو منع اختراق المضيف.

إذا رفضت المشاركة في KSN أو لم تكن هناك شبكة، يضع Kaspersky Endpoint Security التطبيق في مجموعة ثقة اعتمادًا على إعدادات مكون منع اختراق المضيف. بعد استلام سمعة التطبيق من KSN، يمكن تغيير مجموعة الثقة تلقائيًا.

4. يحظر إجراءات التطبيق بناءً على مجموعة الثقة. على سبيل المثال: يتم رفض وصول التطبيقات من مجموعة الثقة مقيد بشكل عالٍ إلى وحدات نظام التشغيل.

في المرة التالية التي يعمل فيها التطبيق، يتحقق Kaspersky Endpoint Security من سلامة التطبيق. في حالة عدم تغير التطبيق، يستخدم المكون حقوق التطبيق الحالية عليه. في حالة تعديل التطبيق، فإن Kaspersky Endpoint Security يحلل التطبيق كما لو كان يجرى تشغيله لأول مرة.

إعدادات المكون الخاص بمنع اختراق المضيف

المعلمة	الوصف
حقوق التطبيق	جدول التطبيقات التير يراقبها مكون منع اختراق المضيف. يتم تعيين التطبيقات إلى مجموعات موثوقة. تحدد مجموعة الثقة الحقوق التي يشير إليها Kaspersky Endpoint Security عند التحكم في نشاط التطبيق. يمكنك تحديد تطبيق من قائمة واحدة لجميع التطبيقات المثبتة على أجهزة الكمبيوتر تحت تأثير سياسة وإضافة التطبيق إلى مجموعة ثقة. حقوق الوصول إلى التطبيق معروضة في الجداول التالية: • **سجل الملفات والنظام**. يحتوي هذا الجدول على حقوق التطبيقات في مجموعة ثقة للوصل إلى موارد نظام التشغيل والبيانات الشخصية. • **الحقوق**. يحتوي هذا التطبيق على حقوق التطبيقات في مجموعة ثقة في الوصول إلى العمليات والموارد الخاصة بنظام التشغيل. • **قواعد شبكة الاتصال**. جدول قواعد الشبكة للتطبيقات التي تشكل جزءًا من مجموعة ثقة. وفقًا لهذه القواعد، يقوم جدار الحماية بتنظيم نشاط الشبكة للتطبيق. يعرض الجدول قواعد الشبكة المحددة مسبقًا التي يوصي بها خبراء Kaspersky. تم إضافة قواعد الشبكة هذه لحماية حركة مرور الشبكة لأجهزة الكمبيوتر التي تعمل بأنظمة تشغيل Windows على النحو الأمثل. لا يمكن حذف قواعد الشبكة المحددة مسبقًا.
الموارد المحمية	يحتوي الجدول على موارد الكمبيوتر المصنفة. يراقب مكون منع اختراق المضيف المحاولات التي تتم بواسطة التطبيقات الأخرى للوصول إلى الموارد الموجودة في الجدول. وقد يمثل المورد فئة تسجيل أو ملف أو مجلد أو مفتاح تسجيل.
تم إطلاق مجموعة الثقة للتطبيقات قبل بدء عمل Kaspersky Endpoint Security for Windows	مجموعة ثقة سيضع فيها Kaspersky Endpoint Security التطبيقات التي بدأت قبل Kaspersky Endpoint Security.
تحديث القواعد للتطبيقات التي لم تكن معروفة سابقًا من Kaspersky Security Network	في حالة تحديد خانة الاختيار، يقوم مكون منع اختراق المضيف بتحديث الحقوق المخصصة للتطبيقات التي لم تكن معروفة سابقًا عن طريق استخدام قاعدة بيانات Kaspersky Security Network.
الثقة في التطبيقات الموقعة رقميًا	في حالة تحديد خانة الاختيار هذه، فإن مكون منع اختراق المضيف يضع التطبيقات التي تحمل التوقيع الرقمي للبائعين الموثوقين في المجموعة موثوق. البائعون الموثوقون هم بائعو البرامج الموثوقون بواسطة Kaspersky. ويمكنك أيضًا إضافة شهادة البائع إلى مخزن الشهادات الموثوق يدويًا. في حالة إلغاء تحديد خانة الاختيار هذه، فإن مكون منع اختراق المضيف لا يعتبر هذه التطبيقات موثوقة، ويستخدم المعلمات الأخرى لتحديد مجموعة الثقة الخاصة بها.
حذف قواعد التطبيقات التي لم يتم تشغيلها لأكثر من N الأيام (من 1 إلى 90)	في حالة تحديد خانة الاختيار، سوف يقوم Kaspersky Endpoint Security تلقائيًا بحذف معلومات التطبيق (مجموعة الثقة وحقوق الوصول) إذا تم استيفاء الشروط التالية: • قمت يدويًا بوضع التطبيق في مجموعة ثقة أو بتكوين حقوق الوصول الخاصة بها. • لم يبدأ التطبيق في الفترة الزمنية المحددة. إذا كانت مجموعة الثقة والحقوق لتطبيق محددة بشكل تلقائي، سيقوم Kaspersky Endpoint Security تلقائيًا بحذف معلومات هذا التطبيق بعد 30 يومًا. إذا لم يمكن من الممكن تغيير مدة التخزين لمعلومات التطبيق أو إلغاء الحذف. المرة القادمة التي تبدأ فيها هذا التطبيق، سوف يقوم Kaspersky Endpoint Security بتحليل التطبيق كأنه يبدأ للمرة الأولى.

مجموعة الثقة للتطبيقات التي لا يمكن إضافتها إلى المجموعات الموجودة	تحدد العناصر في هذه القائمة المنسدلة مجموعة الثقة التي سيعين لها Kaspersky Endpoint Security تطبيقًا غير معروف. ويمكنك اختيار أحد العناصر التالية: • **مقيد بشكل منخفض**. • **مقيد بشكل عالٍ**. • **غير موثوق**.

محرك المعالجة

يتيح محرك المعالجة لبرنامج Kaspersky Endpoint Security التراجع عن الإجراءات التي تم تنفيذها باستخدام برمجيات ضارة في نظام التشغيل.

عند التراجع عن نشاط ضار في نظام التشغيل، يتعامل Kaspersky Endpoint Security مع الأنواع التالية من أنشطة البرمجيات الضارة:

- **نشاط الملف**

يقوم Kaspersky Endpoint Security بالإجراءات التالية:

- يحذف الملفات القابلة للتنفيذ التي تم إنشاؤها من قبل برمجيات ضارة (في جميع الوسائط ما عدا محركات الشبكات).
- يحذف الملفات القابلة للتنفيذ التي تم إنشاؤها بواسطة البرامج التي تسللت بواسطة البرمجيات الضارة.
- يستعيد الملفات التي تم تعديلها أو حذفها بواسطة البرمجيات الضارة.

لدى ميزة استرداد الملف عدد من القيود.

- **نشاط التسجيل**

يقوم Kaspersky Endpoint Security بالإجراءات التالية:

- يحذف مفاتيح التسجيل التي تم إنشاؤها بواسطة البرمجيات الضارة.
- لا يستعيد مفاتيح التسجيل التي تم تعديلها أو حذفها بواسطة البرمجيات الضارة.

- **نشاط النظام**

يقوم Kaspersky Endpoint Security بالإجراءات التالية:

- ينهي العمليات التي تم بدؤها بواسطة البرمجيات الضارة.
- ينهي العمليات التي اخترقها تطبيق ضار.
- لا يستأنف العمليات التي تم وقفها باستخدام برمجيات ضارة.

- **نشاط الشبكة**

يقوم Kaspersky Endpoint Security بالإجراءات التالية:

- يحظر نشاط شبكة البرمجيات الضارة.
- يحظر نشاط شبكة العمليات التي تسللت بواسطة البرمجيات الضارة.

يمكن بدء التراجع عن إجراءات البرامج الضارة بواسطة مكون الحماية من تهديدات الملفات أو اكتشاف السلوك أو أثناء فحص البرامج الضارة.

يؤثر التراجع عن عمليات البرمجيات الضارة على مجموعة محددة من البيانات. التراجع لا يوجد له تأثيرات سلبية على نظام التشغيل أو على سلامة بيانات جهاز الكمبيوتر.

Kaspersky Security Network

لحماية الكمبيوتر الخاص بك بشكل أكثر فاعلية، يستخدم برنامج Kaspersky Endpoint Security بيانات تم تلقيها من المستخدمين من جميع أنحاء العالم. تم تصميم Kaspersky Security Network للحصول على هذه البيانات.

تعتبر شبكة Kaspersky Security Network (KSN) بنية تحتية من الخدمات السحابية التي توفر الوصول إلى قاعدة معارف Kaspersky على الإنترنت والتي تحتوي على معلومات عن سمعة الملفات وموارد الويب والبرامج. ويعد استخدام البيانات من Kaspersky Security Network ضمانًا لسرعة وقت استجابات Kaspersky Endpoint Security عند مواجهة تهديدات جديدة، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية ويقلل من خطر وقوع الحالات الإيجابية الزائفة. إذا كنت تشارك في شبكة Kaspersky Security Network، فإن خدمات شبكة KSN تقوم بتزويد برنامج Kaspersky Endpoint Security بمعلومات حول فئة وسمعة الملفات التي تم فحصها، بالإضافة إلى معلومات حول سمعة عناوين الويب التي تم فحصها.

استخدام شبكة Kaspersky Security Network اختياري. يطلب منك التطبيق استخدام KSN أثناء التكوين الأولي للتطبيق. يمكن للمستخدمين بدء المشاركة في KSN وعدم المتابعة في أي وقت.

للحصول على مزيد من المعلومات التفصيلية حول إرسال معلومات إحصائية إلى Kaspersky والتي يتم إنشاؤها أثناء المشاركة في شبكة KSN، وكذلك حول تخزين تلك المعلومات وتدميرها، الرجاء الرجوع إلى بيان Kaspersky Security Network وموقع ويب Kaspersky. يتم تضمين الملف ksn_<language ID>.txt مع نص بيان Kaspersky Security Network في حزمة توزيع التطبيق.

البنية التحتية لقواعد بيانات السمعة من Kaspersky

يدعم Kaspersky Endpoint Security حلول البنية التحتية التالية للعمل مع قواعد بيانات السمعة من Kaspersky:

- Kaspersky Security Network هي المنتج الذي يتم استخدامه من قِبل أغلب تطبيقات Kaspersky. يتسلم المشتركين في شبكة KSN معلومات من Kaspersky ويرسلوا معلومات إلى Kaspersky حول الكائنات التي تم اكتشافها على جهاز كمبيوتر المستخدم ليتم تحليلها بشكل إضافي من قِبل محللي Kaspersky وليتم إدراجها في قواعد بيانات الإحصائية والخاصة بالسمعة.
- Kaspersky Private Security Network عبارة عن حل يتيح لمستخدمي أجهزة الكمبيوتر التي تستضيف Kaspersky Endpoint Security أو غيره من تطبيقات Kaspersky الحصول على حق الوصول إلى قواعد بيانات السمعة من Kaspersky، وإلى البيانات الإحصائية الأخرى دون إرسال بيانات إلى Kaspersky من أجهزة الكمبيوتر الخاصة بهم. وصُممت شبكة KPSN لعملاء الشركات الذين لا يستطيعون المشاركة في شبكة Kaspersky Security Network لأي من الأسباب التالية:
  - محطات العمل المحلية غير متصلة بالإنترنت.
  - يُعتبر نقل أي بيانات خارج البلد أو خارج الشبكة المحلية (LAN) الخاصة بالشركة ممنوعًا بواسطة القانون أو مُقيدًا بواسطة سياسات الأمن الخاصة بالشركة.

افتراضيًا، يستخدم Kaspersky Security Center شبكة KSN. ويمكنك تكوين استخدام شبكة KPSN في وحدة تحكم الإدارة (MMC) في Kaspersky Security Center Web Console وفي سطر الأوامر. ولا يمكن تكوين استخدام شبكة KPSN في Kaspersky Security Center Cloud Console.

للمزيد من التفاصيل عن شبكة KPSN، يُرجى الرجوع إلى الوثائق الموجودة على شبكة Kaspersky Private Security Network.

إعدادات Kaspersky Security Network

المعلمة	الوصف
تمكين وضع	إن وضع KSN الموسع هو وضع يقوم فيه Kaspersky Endpoint Security بإرسال بيانات إضافية إلى Kaspersky.

KSN الموسع	Kaspersky Endpoint Security يستخدم KSN في اكتشاف التهديدات بغض النظر عن منطقتها.
تمكين وضع السحابة	الوضع السحابي تُشير إلى وضع تشغيل التطبيق الذي يستخدم فيه برنامج Kaspersky Endpoint Security إصدارًا خفيفًا من قواعد بيانات مكافحة الفيروسات. تدعم Kaspersky Security Network تشغيل التطبيق عند استخدام إصدار خفيف من قواعد بيانات مكافحة الفيروسات. يُتيح لك الإصدار الخفيف من قواعد بيانات مكافحة الفيروسات استخدام نصف ذاكرة الوصول العشوائي الموجودة بجهاز الكمبيوتر تقريبًا والتي يمكن استخدامها مع قواعد البيانات المعتادة بطريقة أخرى. إذا لم تشارك في Kaspersky Security Network أو إذا تم تعطيل الوضع السحابي، يقوم برنامج Kaspersky Endpoint Security بتنزيل الإصدار الكامل من قواعد بيانات مكافحة الفيروسات من خوادم Kaspersky. في حالة تحديد خانة الاختيار، فإن برنامج Kaspersky Endpoint Security يستخدم النسخة الخفيفة من قواعد بيانات مكافحة الفيروسات، مما يقلل من العبء على موارد نظام التشغيل. يقوم Kaspersky Endpoint Security بتنزيل النسخة الخفيفة من قواعد بيانات مكافحة الفيروسات أثناء التحديث التالي بعد تحديد خانة الاختيار. إذا تم إيقاف تشغيل زر التبديل، فإن برنامج Kaspersky Endpoint Security يستخدم النسخة الكاملة من قواعد بيانات مكافحة الفيروسات. يقوم Kaspersky Endpoint Security بتنزيل النسخة الكاملة من قواعد بيانات مكافحة الفيروسات أثناء التحديث التالي بعد إلغاء تحديد خانة الاختيار.
حالة الكمبيوتر عند عدم توفر خوادم شبكة KSN (متوفر فقط في Kaspersky Security Center (Console	تحدد العناصر الموجودة في هذه القائمة المنسدلة حالة جهاز الكمبيوتر في Kaspersky Security Center عندما تكون خوادم KSN غير متوفرة.
استخدام وكيل شبكة KSN (متوفر فقط في Kaspersky Security Center (Console	إذا تم تحديد خانة الاختيار، سيقوم Kaspersky Endpoint Security باستخدام خدمة الوكيل لشبكة KSN. يمكنك تكوين إعدادات خدمة وكيل شبكة KSN في خصائص خادم الإدارة.
استخدام خوادم شبكة KSN عندما يكون وكيل شبكة KSN غير متاح (متوفر فقط في Kaspersky Security Center (Console	إذا تم تحديد خانة الاختيار، سيقوم برنامج Kaspersky Endpoint Security باستخدام خوادم شبكة KSN عند عدم توافر خدمة الوكيل لشبكة KSN. قد يتم وضع خوادم KSN على جانب Kaspersky وعلى جانب أطراف خارجية (عند استخدام Kaspersky Private Security Network).

فحص السجل

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم. ولا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل.

بدءً من الإصدار 11.11.0 يتضمن Kaspersky Endpoint Security for Windows مكون فحص السجل. يراقب فحص السجل سلامة البيئة المحمية استنادًا إلى تحليل سجل أحداث Windows. وعندما يكتشف التطبيق علامات سلوك غير نمطي في النظام، فإنه يُبلغ المسؤول، لأن هذا السلوك قد يشير إلى محاولة هجوم إلكتروني.

يحلل Kaspersky Endpoint Security سجلات أحداث Windows ويكتشف الانتهاك وفقًا للقواعد. ويتضمن المكون predefined rules. ويتم تشغيل القواعد المحددة مسبقًا من خلال التحليل المساعد على الاكتشاف. ويمكنك أيضا إضافة القواعد الخاصة بك (قواعد مخصصة). وعند تشغيل قاعدة، ينشئ التطبيق حدثًا بحالة Critical (انظر الشكل أدناه).

إذا كنت ترغب في استخدام فحص السجل، تأكد من تكوين سياسة التدقيق وأن النظام يسجل الأحداث ذات الصلة (للحصول على التفاصيل، يرجى الرجوع إلى موقع ويب الدعم الفني من Microsoft).

إخطار فحص السجل

إعدادات فحص السجل

المعلمة	الوصف
القواعد المحددة مسبقًا	قائمة قواعد فحص السجل. تتضمن القواعد المحددة مسبقًا قوالب للنشاط غير الطبيعي على الكمبيوتر المحمي. ويمكن أن يشير النشاط غير الطبيعي إلى محاولة هجوم.
قواعد مخصصة	قائمة قواعد فحص السجل التي أضافها المستخدم. يمكنك تعيين معايير تشغيل قاعدة فحص السجل الخاصة بك. ولفعل ذلك، يجب عليك إدخال معرف الحدث وتحديد مصدر حدث. ويمكنك تحديد مصدر حدث من بين السجلات القياسية: Application أو Security أو System. ويمكنك أيضًا تحديد سجل تطبيق جهة خارجية.

التحكم في الويب

يقوم المكون التحكم في الويب بإدارة وصول المستخدمين إلى موارد الويب. هذا يساعد على تقليل حركة المرور والاستخدام غير المناسب لوقت العمل. عندما يحاول مستخدم فتح موقع إلكتروني محجوب من التحكم في الويب، فإن Kaspersky Endpoint Security سوف يحجب الوصول إلى ذلك الموقع أو يعرض تحذيرًا (راجع الشكل أدناه).

يراقب برنامج Kaspersky Endpoint Security حركة مرور HTTP، وHTTPS فقط.

لمراقبة حركة مرور HTTPS، تحتاج إلى تمكين عمليات فحص الاتصالات المشفرة.

طرق لإدارة الوصول إلى مواقع الويب

يُتيح لك المكون التحكم في الويب تكوين الوصول إلى مواقع الويب باستخدام الطرق التالية:

- **فئة موقع الويب**. يتم تصنيف مواقع الويب وفقًا لخدمة سحابة Kaspersky Security Network، والتحليل الموجه، وقاعدة بيانات المواقع المعروفة (المُضمنة في قواعد بيانات التطبيق). على سبيل المثال، يمكنك تقييد وصول المستخدم إلى فئة الشبكات الاجتماعية أو إلى فئات أخرى.
- **نوع البيانات**. يمكنك تقييد وصول المستخدمين إلى البيانات الموجودة على موقع الويب، وإخفاء الصور الرسومية، على سبيل المثال. يحدد برنامج Kaspersky Endpoint Security نوع البيانات بناءً على تنسيق الملف وليس بناءً على ملحقاته.

لا يفحص برنامج Kaspersky Endpoint Security الملفات الموجودة في الأرشيفات. على سبيل المثال، إذا تم وضع ملفات الصور في الأرشيف، فإن برنامج Kaspersky Endpoint Security يحدد نوع البيانات لتكون الأرشيفات وليس الرسومات.

- **العنوان الفردي**. يمكنك إدخال عنوان الويب أو استخدام الأقنعة.

يمكنك في الوقت نفسه استخدام طرق متعددة لتنظيم الوصول إلى مواقع الويب. على سبيل المثال، يمكنك تقييد الوصول إلى نوع البيانات "ملفات Office" وحصره فقط على فئة موقع الويب البريد الإلكتروني على الويب.

قواعد الوصول لموقع الويب

يقوم المكون التحكم في الويب بإدارة وصول المستخدم إلى مواقع الويب باستخدام قواعد الوصول. يمكنك تكوين الإعدادات المتقدمة التالية الخاصة بقاعدة الوصول إلى موقع الويب:

- المستخدمين الذين تنطبق عليهم القاعدة.

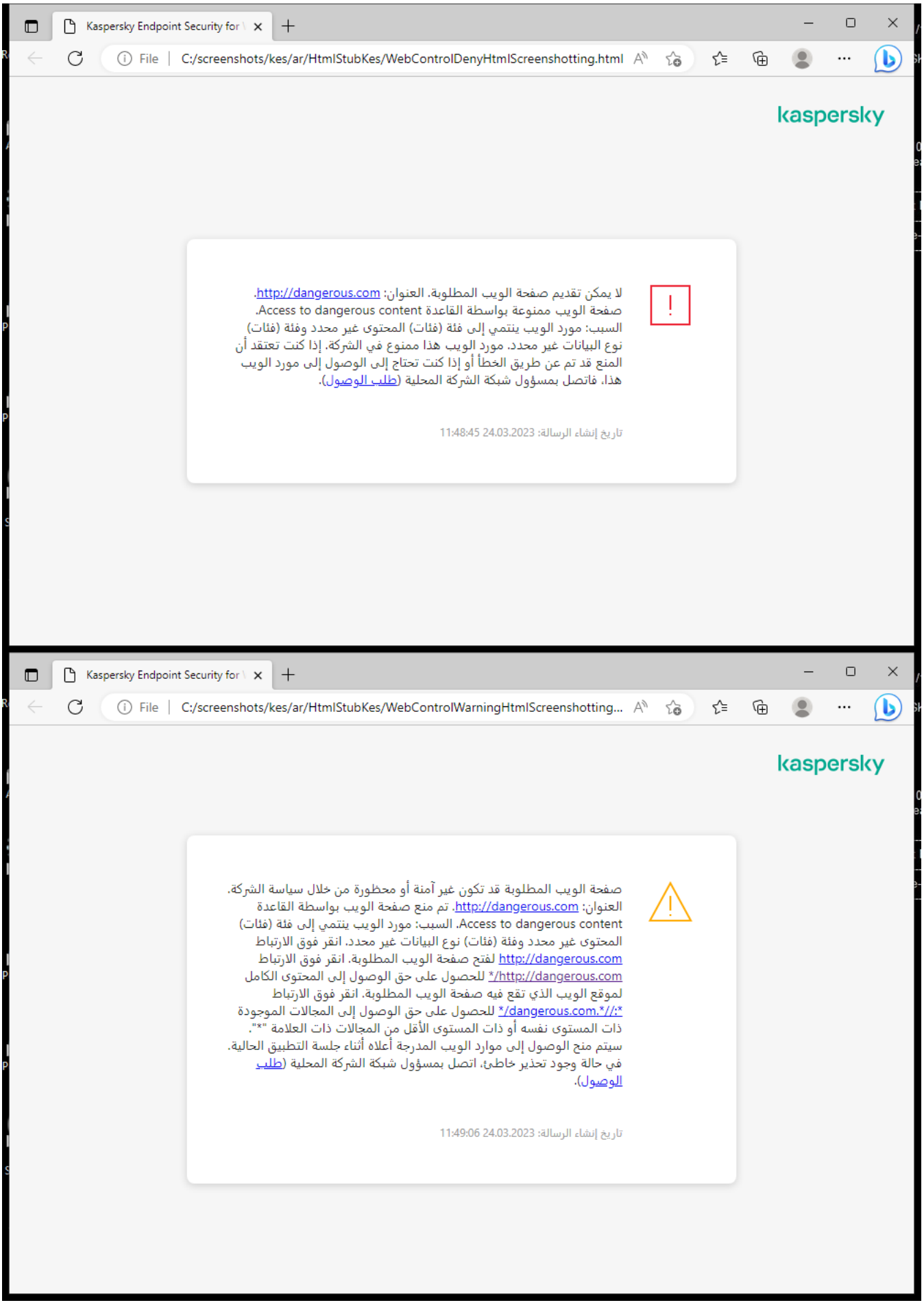
  على سبيل المثال، يمكنك تقييد وصول جميع مستخدمي الشركة إلى الإنترنت من خلال المستعرض باستثناء قسم تكنولوجيا المعلومات.

- جدول القاعدة.

  على سبيل المثال، يمكنك تقييد الوصول إلى الإنترنت من خلال المستعرض خلال ساعات العمل فقط.

أولوية قاعدة الوصول

لكل قاعدة أولوية. كلما كانت القاعدة تحتل مرتبة أعلى في القائمة، فإنها تكون ذات أولوية أعلى. إذا تمت إضافة موقع ويب إلى قواعد متعددة، ينظم المكون التحكم في الويب الوصول إلى موقع الويب بناءً إلى القاعدة ذات أعلى أولوية. على سبيل المثال، قد يحدد برنامج Kaspersky Endpoint Security بوابة شركة لتكون شبكة اجتماعية. لتقييد الوصول إلى الشبكات الاجتماعية وتوفير الوصول إلى بوابة الويب الخاصة بالشركة، قم بإنشاء قاعدتين: قاعدة واحدة لحظر الوصول إلى فئة موقع الويب الشبكات الاجتماعية وقاعدة واحدة للسماح بالوصول إلى بوابة الويب الخاصة بالشركة. يجب أن يكون لقاعدة الوصول لبوابة الويب الخاصة بالشركة أولوية أعلى من قاعدة الوصول إلى الشبكات الاجتماعية.



رسائل التحكم في الويب

إعدادات مكون التحكم في الويب

المعلمة	الوصف

قواعد الوصول إلى موارد الويب	قائمة تضم قواعد الوصول إلى موارد الويب. لكل قاعدة أولوية. كلما كانت القاعدة تحتل مرتبة أعلى في القائمة، فإنها تكون ذات أولوية أعلى. إذا تمت إضافة موقع ويب إلى قواعد متعددة، ينظم المكون التحكم في الويب الوصول إلى موقع الويب بناءً إلى القاعدة ذات أعلى أولوية.
القاعدة الافتراضية	القاعدة الافتراضية هي قاعدة للوصول إلى موارد الويب التي لا تغطيها أي قاعدة أخرى. الخيارات التالية متاحة: • **السماح للكل ما عدا قائمة القواعد**، المعروف أيضًا باسم وضع قائمة الرفض لمواقع الويب المحظورة. • **رفض كل شيء ما عدا قائمة القواعد**، المعروف أيضًا باسم وضع قائمة السماح لمواقع الويب المسموح بها.
القوالب	**تحذير**. يتكون حقل الإدخال من قالب للرسالة التي يتم عرضها إذا تم تشغيل قاعدة للتحذير بشأن محاولات وصول إلى مورد ويب غير مرغوب فيه. **رسالة حول المنع**. يحتوي حقل الإدخال على قالب الرسالة التي تظهر في حالة تشغيل قاعدة تمنع الوصول إلى أحد موارد الويب. **رسالة إلى المسؤول**. قالب الرسالة المقرر إرسالها إلى مسؤول الشبكة المحلية إذا كان المستخدم يعتقد أن المنع تم عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع الوصول لصفحة الويب إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.
تسجيل فتح الصفحات المسموح بها	يقوم برنامج Kaspersky Endpoint Security بتسجيل بيانات عن زيارات لجميع مواقع الويب، بما في ذلك مواقع الويب المسموح بها. يُرسل برنامج Kaspersky Endpoint Security الأحداث إلى Kaspersky Security Center، وإلى السجل المحلي لبرنامج Kaspersky Endpoint Security، وإلى سجل أحداث Windows. لمراقبة نشاط إنترنت المستخدم، تحتاج إلى تكوين الإعدادات لحفظ الأحداث. المستعرضات التي تدعم وظيفة المراقبة: Microsoft Edge وMicrosoft Internet Explorer وGoogle Chrome وYandex Browser وMozilla Firefox. ولا تعمل مراقبة نشاط المستخدم في المستعرضات الأخرى. قد يتطلب مراقبة نشاط إنترنت المستخدم استخدام موارد أجهزة كمبيوتر بصورة أكبر عند فك تشفير حركة مرور HTTPS.

التحكم في الجهاز

يعمل التحكم في الجهاز على إدارة إمكانية وصول المستخدم إلى الأجهزة المثبت عليها أو المتصلة بجهاز الكمبيوتر (على سبيل المثال، الأقراص الصلبة أو الكاميرات أو وحدات شبكة Wi-Fi). يتيح لك هذا حماية جهاز الكمبيوتر من الإصابة بالفيروسات عند اتصال مثل هذه الأجهزة به بالإضافة إلى الوقاية من فقدان البيانات أو تسريبها.

مستويات الوصول إلى الجهاز

يعمل التحكم في الجهاز على التحكم في إمكانية الوصول عند المستويات التالية:

- **نوع الجهاز**. على سبيل المثال، آلات الطباعة ومحركات الأقراص القابلة للإزالة ومحركات الأقراص المضغوطة / أقراص DVD.

يمكنك تكوين إمكانية الوصول إلى الجهاز على النحو التالي:

- سماح – ✓.
- منع – ⊘.

- حسب القواعد (الطابعات والأجهزة المحمولة فقط) –
- يعتمد على ناقل الاتصال (باستثناء Wi-Fi) –
- حظر مع استثناءات (Wi-Fi فقط) –

- **ناقل الاتصال**. ناقل الاتصال عبارة عن واجهة تستخدم لتوصيل الأجهزة بجهاز الكمبيوتر (على سبيل المثال، أجهزة USB أو FireWire). ولذلك، يمكنك تقييد اتصال جميع الأجهزة، على سبيل المثال، ما يزيد عن USB.

  يمكنك تكوين إمكانية الوصول إلى الجهاز على النحو التالي:

  - سماح –
  - منع –

- **الأجهزة الموثوقة**. الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

  يمكنك إضافة الأجهزة الموثوقة وفقًا للبيانات التالية:

  - **الأجهزة حسب المُعرِّف**. كل جهاز له معرف فريد (معرف الأجهزة أو HWID). يمكنك عرض المُعرّف في خصائص الجهاز من خلال استخدام أدوات نظام التشغيل. مثال على معرف الجهاز: `SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`. إضافة الأجهزة حسب المُعرِّف عملية ملائمة إذا كنت ترغب في إضافة مجموعة أجهزة محددة.

  - **الأجهزة حسب الموديل**. كل جهاز له معرف بائع (VID) ومعرف منتج (PID). يمكنك عرض المُعرّفات في خصائص الجهاز من خلال استخدام أدوات نظام التشغيل. قالب إدخال معرف البائع ومعرف المنتج: `VID_1234&PID_5678`. إضافة أجهزة حسب الموديل طريقة ملائمة إذا كنت تستخدم أجهزة ذات موديل معين في مؤسستك. بهذه الطريقة، يمكنك إضافة جميع الأجهزة من هذا الموديل.

  - **الأجهزة حسب قناع المُعرِّف**. إذا كنت تستخدم عدة أجهزة ذات معرفات متشابهة، يمكنك إضافة الأجهزة إلى القائمة الموثوقة باستخدام الأقنعة. الحرف `*` يستبدل أي مجموعة من الرموز. لا يدعم برنامج Kaspersky Endpoint Security الحرف `?` عند إدخال قناع. على سبيل المثال: `WDC_C*`.

  - **الأجهزة حسب قناع الطراز**. إذا كنت تستخدم عدة أجهزة لها معرفات البائعين ومعرفات المنتجين نفسها (مثل أجهزة من الشركة المصنعة ذاتها)، عندها يمكنك إضافة أجهزة إلى القائمة الموثوقة باستخدام الأقنعة. الحرف `*` يستبدل أي مجموعة من الرموز. لا يدعم برنامج Kaspersky Endpoint Security الحرف `?` عند إدخال قناع. على سبيل المثال، `VID_05AC & PID_*`.

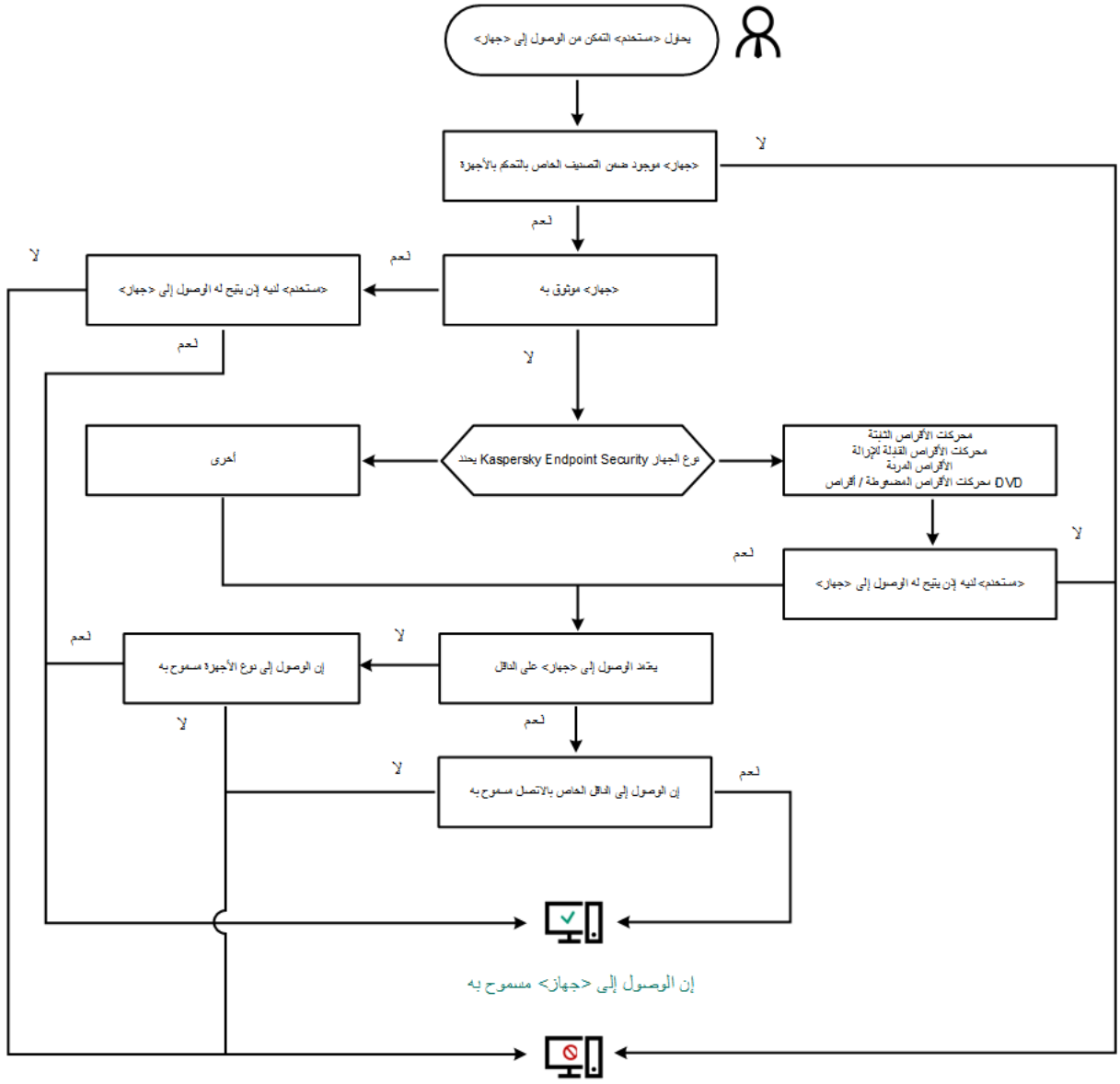
يقوم التحكم في الجهاز بتنظيم وصول المستخدم إلى الأجهزة باستخدام قواعد الوصول. وكذلك يتيح لك التحكم في الجهاز القيام بحفظ أحداث اتصال الجهاز/انقطاع اتصاله. لحفظ الأحداث، تحتاج إلى تكوين تسجيل الأحداث في السياسة.

إذا كان يعتمد الوصول إلى جهاز ما على ناقل الاتصال (الحالة)، لا يقوم برنامج Kaspersky Endpoint Security بحفظ أحداث اتصال الجهاز/انقطاع اتصاله. لتمكين برنامج Kaspersky Endpoint Security من حفظ أحداث اتصال الجهاز/انقطاع اتصاله، قم بالسماح بالوصول إلى نوع الجهاز المتطابق (الحالة) أو قم بإضافة الجهاز إلى القائمة الموثوقة.

عند حظر جهاز متصل بجهاز كومبيوتر بواسطة التحكم في الجهاز، فإن برنامج Kaspersky Endpoint Security سيقوم بحظر الوصول وإظهار إخطار (انظر الشكل أدناه).

إخطار التحكم في الجهاز

يتخذ برنامج Kaspersky Endpoint Security قرارًا بشأن السماح بالوصول إلى الجهاز بعد أن يقوم المستخدم بتوصيل هذا الجهاز بجهاز الكمبيوتر (انظر الشكل أدناه).



خوارزمية تشغيل التحكم في الجهاز

إذا كان الجهاز متصلًا وكان الوصول مسموحًا به، يمكنك تحرير قاعدة الوصول وحظر الوصول. في هذه الحالة، في المرة التالية التي يحاول فيها شخص ما الوصول إلى الجهاز (على سبيل المثال عرض شجرة المجلدات، أو تنفيذ عمليات القراءة أو الكتابة)، سيقوم برنامج Kaspersky Endpoint Security بحظر الوصول. يتم منع أي جهاز لا يحتوي على ملف نظام، ولكن في المرة التالية التي يتم فيها توصيل الجهاز.

إذا كان يجب على مستخدم جهاز كمبيوتر مثبت عليه Kaspersky Endpoint Security طلب الوصول إلى جهاز يعتقد المستخدم أنه تم منعه عن طريق الخطأ، فأرسل للمستخدم تعليمات طلب الوصول.

إعدادات مكون التحكم في الجهاز

المعلمة	الوصف
السماح بطلب للوصول المؤقت	إذا تم تحديد خانة الاختيار هذه، يصبح الزر **طلب الوصول** متوفرًا من خلال الواجهة المحلية لتطبيق Kaspersky Endpoint Security. باستخدام هذا الزر، يمكن للمستخدم طلب إمكانية وصول مؤقت إلى جهاز ممنوع.

(متوفر فقط في Kaspersky Security Center (Console	
الأجهزة وشبكات Wi-Fi	تعرض علامة التبويب جدولاً يضم جميع أنواع الأجهزة المحتملة وفقًا لتصنيف مكون "التحكم في الجهاز"، بما في ذلك حالات الوصول المحددة.
ناقلات الاتصال	قائمة بجميع ناقلات الاتصال المتوفرة وفقًا لتصنيف مكون التحكم في الجهاز، بما في ذلك حالات الوصول المحددة.
الأجهزة الموثوقة	قائمة الأجهزة الموثوقة والمستخدمين الذين تم منحهم حق الوصول إلى هذه الأجهزة.
منع تعدد الاتصال	تمنع مكافحة اتصالات الجسر إنشاء جسور شبكة عن طريق منع التأسيس المتزامن لاتصالات الشبكة المتعددة لجهاز الكمبيوتر. يتيح لك ذلك حماية شبكة الشركة من الهجمات عبر شبكات غير محمية وغير مُصرح بها. تحظر مكافحة اتصالات الجسر إنشاء اتصالات متعددة وفقًا لأولويات الأجهزة. كلما كان الجهاز يحتل مرتبة أعلى في القائمة، فإنه يكون ذا أولوية أعلى. إذا كان الاتصال النشط والاتصال الجديد من نفس النوع (على سبيل المثال، شبكة Wi-Fi)، يحظر برنامج Kaspersky Endpoint Security الاتصال النشط ويسمح بإنشاء اتصالاً جديدًا. إذا كان الاتصال النشط والاتصال الجديد من أنواع مختلفة (على سبيل المثال، محول شبكة وشبكة Wi-Fi)، يحظر برنامجKaspersky Endpoint Security الاتصال صاحب الأولوية الأقل ويسمح بالاتصال صاحب الأولوية الأعلى. تدعم مكافحة اتصالات الجسر التشغيل باستخدام الأنواع التالية من الأجهزة: محول الشبكة، وشبكة Wi-Fi، والمودم.
قوالب الرسائل	**رسالة حول المنع**. قالب الرسالة الذي يظهر عندما يحاول المستخدم الوصول إلى جهاز محظور. تظهر هذه الرسالة أيضًا عندما يحاول المستخدم تنفيذ عملية على محتويات الجهاز الذي تم حظره لهذا المستخدم. **رسالة إلى المسؤول**. قالب الرسالة الذي يتم إرساله إلى مسؤول الشبكة المحلية (LAN) عندما يعتقد المستخدم أنه قد تم حظر وصوله إلى الجهاز أو منعه من إجراء عملية باستخدام محتوى الجهاز عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع الوصول للجهاز إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.

التحكم في التطبيقات

يدير التحكم في التطبيقات بدء تشغيل التطبيقات على أجهزة كمبيوتر المستخدمين. يتيح لك هذا تنفيذ سياسة أمان الشركة عند استخدام التطبيقات. التحكم في التطبيقات يقلل أيضًا من خطر إصابة الكمبيوتر بتقييد الوصول إلى التطبيقات.

يتضمن تكوين نظام مراقبة عيوب التكيف الخطوات التالية:

1. إنشاء فئات التطبيقات.

   يقوم المسؤول بإنشاء فئات التطبيقات التي يريد المسؤول إدارتها. فئات التطبيقات مخصصة لجميع أجهزة الكمبيوتر في شبكة الشركة، بغض النظر عن مجموعات الإدارة. لإنشاء فئة، يمكنك استخدام المعايير التالية: فئة KL (على سبيل المثال المستعرضات) وتجزئة الملف وبائع التطبيق ومعايير أخرى.

2. إنشاء قواعد التحكم في التطبيق.

   يقوم المسؤول بإنشاء قواعد التحكم في التطبيقات في السياسة لمجموعة الإدارة. تتضمن القاعدة فئات التطبيقات وحالة بدء تشغيل التطبيقات من هذه الفئات: محظورة أو مسموح بها.

3. تحديد وضع التحكم في التطبيق.

يختار المسؤول وضع العمل مع التطبيقات غير المدرجة في أي من القواعد (قائمة السماح وقائمة الرفض الخاصة بالتطبيق).

عندما يحاول مستخدم بدء تشغيل تطبيق محظور ، سيحظر Kaspersky Endpoint Security التطبيق من بدء التشغيل وسيعرض إشعارًا (انظر الشكل أدناه).

يتم توفير وضع اختبار للتحقق من تكوين التحكم في التطبيقات. في هذا الوضع، يقوم Kaspersky Endpoint Security بما يلي:

- يسمح ببدء تشغيل التطبيقات، بما في ذلك التطبيقات المحظورة.
- يعرض إشعارًا حول بدء تشغيل تطبيق محظور ويضيف معلومات إلى التقرير على جهاز الكمبيوتر الخاص بالمستخدم.
- يرسل بيانات حول بدء تشغيل التطبيقات المحظورة إلى Kaspersky Security Center.

إشعار التحكم في التطبيقات

أوضاع تشغيل التحكم في التطبيقات

يعمل مكون التحكم في التطبيقات في وضعين:

- **قائمة الرفض**. في هذا الوضع، يتيح التحكم في التطبيقات للمستخدمين بدء تشغيل جميع التطبيقات باستثناء التطبيقات المحظورة في قواعد التحكم في التطبيقات.

  يتم تمكين وضع المنع لإجراءات التحكم في التطبيقات بشكلٍ افتراضي.

- **قائمة السماح**. في هذا الوضع، يمنع التحكم في التطبيقات المستخدمين من بدء أي تطبيقات باستثناء التطبيقات المسموح بها وغير المحظورة في قواعد التحكم في التطبيقات.

  إذا تم تكوين قواعد السماح للتحكم في التطبيقات بالكامل، فسيحظر المكون بدء تشغيل جميع التطبيقات الجديدة التي لم يتم التحقق منها بواسطة مسؤول الشبكة المحلية، وذلك مع السماح بتشغيل نظام التشغيل والتطبيقات الموثوقة التي يعتمد عليها المستخدمون في عملهم.

  يمكنك قراءة التوصيات الخاصة بتكوين قواعد التحكم في التطبيقات في وضع قائمة السماح.

يمكن تكوين التحكم في التطبيقات للعمل في هذه الأوضاع باستخدام واجهة Kaspersky Endpoint Security المحلية واستخدام Kaspersky Security Center.

ومع ذلك، يقدم Kaspersky Security Center أدوات غير متوفرة في واجهة Kaspersky Endpoint Security المحلية، مثل الأدوات اللازمة للمهام التالية:

- إنشاء فئات التطبيقات.

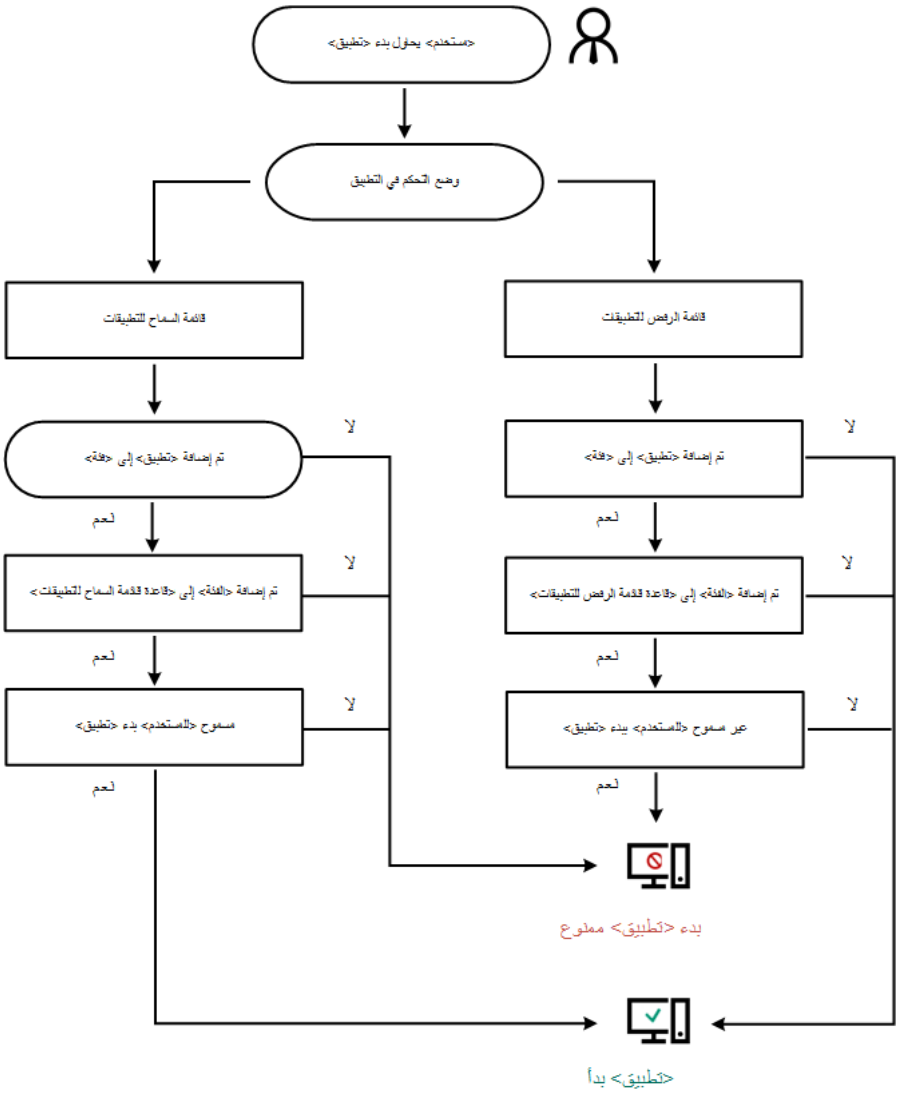
  تستند قواعد التحكم في التطبيقات التي تم إنشاؤها في وحدة تحكم إدارة Kaspersky Security Center إلى فئات التطبيقات المخصصة وليس على شروط التضمين والاستبعاد كما هو الحال في الواجهة المحلية لـ Kaspersky Endpoint Security.

- استلام معلومات حول التطبيقات المثبّتة على أجهزة كمبيوتر الشبكة المحلية للشركة.

ولهذا يوصى باستخدام Kaspersky Security Center لتكوين تشغيل مكون التحكم في التطبيقات.

خوارزمية تشغيل التحكم في التطبيقات

يستخدم Kaspersky Endpoint Security خوارزمية لاتخاذ قرار بشأن تطبيق (انظر الشكل أدناه).



خوارزمية تشغيل التحكم في التطبيقات

إعدادات مكون التحكم في التطبيقات

المعلمة	الوصف
الإجراء عند بدء تشغيل التطبيقات الممنوعة	**تطبيق القواعد**. يدير Kaspersky Endpoint Security بدء تشغيل التطبيقات وفقًا للوضع المحدد. **اختبار القواعد**. يتيح برنامج Kaspersky Endpoint Security بدء تشغيل تطبيق تم منعه في وضع التحكم في التطبيقات الحالي، لكنه يسجل معلومات حول بدء تشغيله في التقرير.
وضع التحكم في بدء تشغيل التطبيق	يمكنك اختيار أحد الخيارات التالية: • **قائمة الرفض**. في حالة تحديد هذا الخيار، يسمح التحكم في التطبيقات لكل المستخدمين بدء تشغيل أي تطبيقات، إلا في الحالات التي تفي بشروط قواعد منع التحكم في التطبيقات. • **قائمة السماح**. في حالة تحديد هذا الخيار، يمنع التحكم في التطبيقات جميع المستخدمين من بدء تشغيل أي تطبيقات، إلا في الحالات التي تفي بشروط قواعد السماح بالتحكم في التطبيقات.

	عند تحديد وضع **قائمة السماح**، يتم إنشاء قاعدتي تحكم في التطبيقات تلقائيًا: • **صورة ذهبية**. • **برامج التحديث الموثوقة**. لا يمكنك تحرير إعدادات القواعد التي تم إنشاؤها تلقائيًا أو حذفها. يمكنك تمكين أو تعطيل هذه القواعد.
التحكم في تحميل وحدات DLL	إذا تم تحديد مربع الاختيار، فيقوم Kaspersky Endpoint Security بالتحكم في تحميل الوحدات النمطية DLL عندما يحاول المستخدمون بدء التطبيقات. ويتم تسجيل المعلومات حول الوحدة النمطية DLL والتطبيق الذي قام بتحميل هذه الوحدة النمطية DLL في التقرير. عند تمكين التحكم في تحميل وحدات DLL وبرامج التشغيل، تأكد من تمكين إحدى القواعد التالية في إعدادات التحكم في التطبيقات: القاعدة الافتراضية **صورة ذهبية** أو قاعدة أخرى تتضمن فئة KL للشهادات الموثوقة وتضمن تحميل وحدات DLL و برامج التشغيل قبل بدء تشغيل Kaspersky Endpoint Security. وقد يتسبب تمكين التحكم في تحميل وحدات DLL وبرامج التشغيل عند تعطيل قاعدة **صورة ذهبية** في عدم استقرار في نظام التشغيل. يراقب Kaspersky Endpoint Security وحدات DLL وبرامج التشغيل التي تم تحميلها منذ تحديد خانة الاختيار. بعد تحديد خانة الاختيار، يوصى بإعادة تشغيل الكمبيوتر للتأكد من أن التطبيق يراقب جميع وحدات DLL وبرامج التشغيل، بما في ذلك تلك التي تم تحميلها قبل بدء تشغيل Kaspersky Endpoint Security.
قوالب رسائل عن منع التطبيق	**رسالة حول المنع**. قالب الرسالة التي يتم عرضها عندما يتم بدء تشغيل قاعدة التحكم في التطبيق التي تمنع بدء تشغيل تطبيق ما. **رسالة إلى المسؤول**. قالب الرسالة التي يمكن للمستخدم إرسالها إلى مسؤول الشبكة المحلية للشركة إذا كان المستخدم يعتقد أنه قد تم حظر التطبيق عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع بدء تشغيل التطبيق إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.

مراقبة عيوب التكيف

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل. لا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم.

يراقب مكون مراقبة عيوب التكيف ويمنع الإجراءات التي لا تعتبر معتادة لأجهزة الكمبيوتر الموجودة في شبكة الشركة. يستخدم نظام مراقبة عيوب التكيف مجموعة من القواعد لتتبع السلوك غير النموذجي (على سبيل المثال، قاعدة بدء تشغيل Windows PowerShell من خلال تطبيق Office). تم إنشاء القواعد من قِبل متخصصي Kaspersky استنادًا إلى سيناريوهات نموذجية للنشاط الضار. تستطيع تكوين كيفية قيام نظام مراقبة عيوب التكيف بمعالجة كل قاعدة، وعلى سبيل المثال، يسمح بتنفيذ نصوص PowerShell التي تقوم بالتشغيل التلقائي لبعض مهام سير العمل. يقوم Kaspersky Endpoint Security بتحديث مجموعة القواعد إلى جانب قواعد بيانات التطبيق. يجب تأكيد إجراء تحديثات لمجموعات القواعد يدويًا.

إعدادات مراقبة عيوب التكيف

يتضمن تكوين نظام مراقبة عيوب التكيف الخطوات التالية:

1. تدريب نظام مراقبة عيوب التكيف.

بعد تمكين نظام مراقبة عيوب التكيف، تعمل قواعده في وضع التدريب. خلال التدريب، يقوم نظام مراقبة عيوب التكيف بمراقبة تشغيل القاعدة وإرسال أحداث التشغيل إلى Kaspersky Security Center. لكل قاعدة المدة الزمنية الخاصة بها لوضع التدريب. يتم تعيين المدة الزمنية لوضع التدريب من جانب خبراء Kaspersky. عادةً، يكون وضع التدريب نشط لمدة أسبوعين.

في حال عدم تشغيل قاعدة ما أبدًا خلال التدريب، سيعتبر نظام مراقبة عيوب التكيف الإجراءات المرتبطة بهذه القاعدة غير نموذجية. سيقوم Kaspersky Endpoint Security بحظر جميع الإجراءات المرتبطة بهذه القاعدة.

في حالة تشغيل قاعدة ما خلال التدريب، سيسجل Kaspersky Endpoint Security أحداث في تقرير تشغيل القاعدة ومستودع **تشغيل القواعد في حالة التدريب الذكي**.

2. تحليل تقرير تشغيل القاعدة.

يحلل المسؤول تقرير تشغيل القاعدة أو محتويات مستودع **تشغيل القواعد في حالة التدريب الذكي**. يمكن أن يحدد المسؤول سلوك مراقبة عيوب التكيف عند تشغيل القاعدة: إما الحظر أو السماح. يمكن أن يستمر المسؤول أيضًا في مراقبة كيفية عمل القاعدة وتمديد المدة الزمنية لوضع التدريب. إذا لم يتخذ المسؤول أي إجراء، سيستمر التطبيق أيضًا في العمل بوضع التدريب. تم إعادة تشغيل فترة وضع التدريب.

يتم تكوين مراقبة عيوب التكيف في الوقت الحقيقي. يتم تكوين مراقبة عيوب التكيف عبر القنوات التالية:

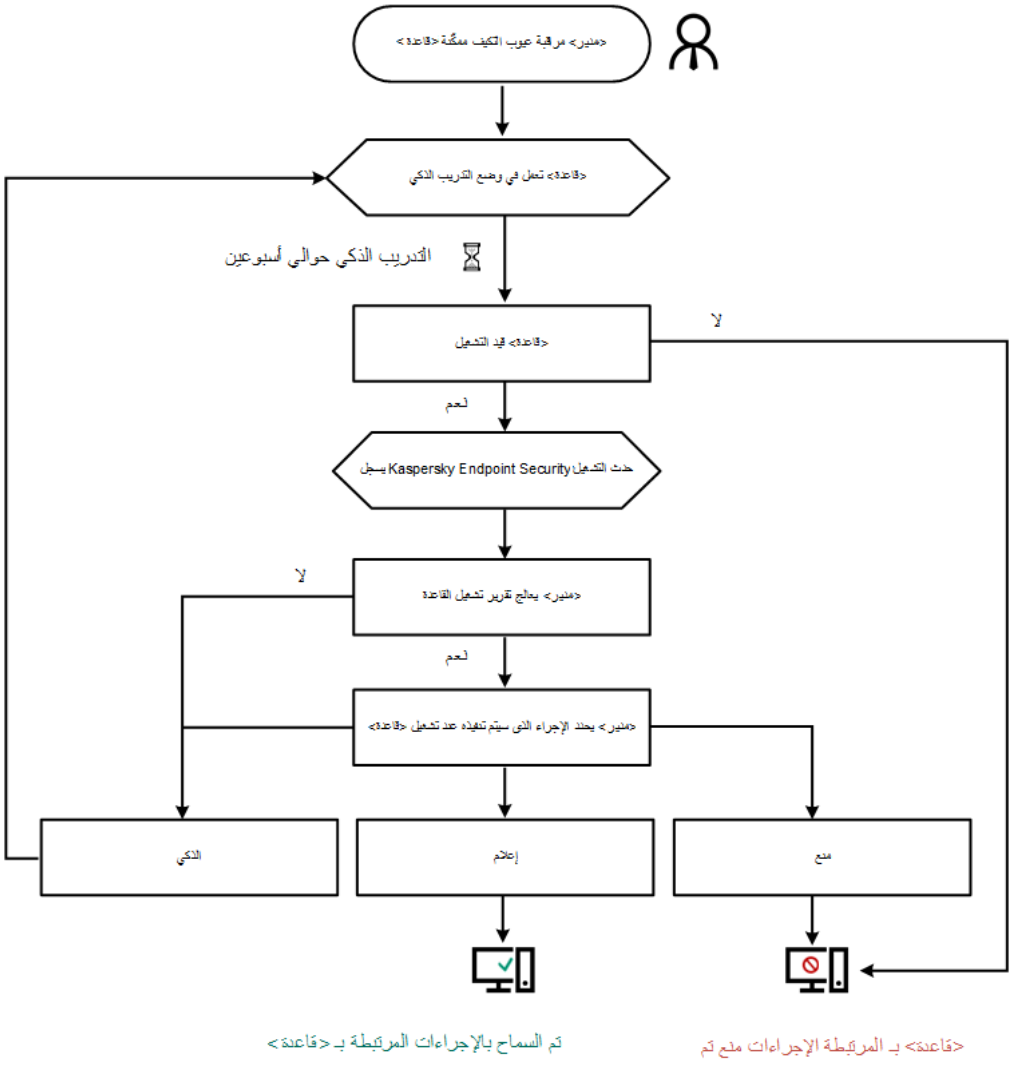
- يتم بدء تشغيل مراقبة عيوب التكيف تلقائيًا لحظر الإجراءات المرتبطة بالقواعد التي لم يتم تشغيلها أبدًا في وضع التدريب.
- يضيف Kaspersky Endpoint Security قواعد جديدة أو يحذف قواعد قديمة.
- يكون المسؤول عملية مراقبة عيوب التكيف بعد مراجعة تقرير تشغيل القاعدة ومحتويات مستودع **تشغيل القواعد في حالة التدريب الذكي**. ويُوصى بالتحقق من تقرير تشغيل القاعدة ومحتويات مستودع **تشغيل القواعد في حالة التدريب الذكي**.

عندما يحاول تطبيق ضار تنفيذ إجراء ما، سيحظر Kaspersky Endpoint Security الإجراء ويعرض إخطارًا (انظر الشكل أدناه).

إخطار مراقبة عيوب التكيف

خوارزمية تشغيل مراقبة عيوب التكيف

يقرر Kaspersky Endpoint Security ما إذا كان يجب السماح بإجراء مرتبط بقاعدة أو حظره استنادًا على الخوارزمية التالية (انظر الشكل أدناه).



خوارزمية تشغيل مراقبة عيوب التكيف

إعدادات مكون مراقبة عيوب التكيف

المعلمة	الوصف
تقرير حول حالة قواعد مراقبة عيوب التكيف (متوفر فقط في Kaspersky Security Center (Console	يحتوي هذا التقرير على معلومات حول حالات قواعد كشف نظام مراقبة عيوب التكيف (على سبيل المثال، تم التعطيل أو منع). يتم إنشاء التقرير لجميع مجموعات الإدارة.
تقرير حول قواعد مراقبة عيوب التكيف التي تم تشغيلها (متوفر فقط في Kaspersky Security Center (Console	يحتوي هذا التقرير على معلومات حول الإجراءات غير النموذجية التي تم اكتشافها باستخدام مراقبة عيوب التكيف. يتم إنشاء التقرير لجميع مجموعات الإدارة.

القواعد	جدول قواعد مراقبة عيوب التكيف. تم إنشاء القواعد من قِبل متخصصي Kaspersky استنادًا إلى سيناريوهات نموذجية للنشاط الضار المحتمل حدوثه.
القوالب	**رسالة حول المنع**. قالب الرسالة المعروض لمستخدم عند تشغيل قاعدة مراقبة عيوب التكيف والتي تمنع وجود الإجراء غير النموذجي. **رسالة إلى المسؤول**. قالب الرسالة التي يمكن أن يرسلها مستخدم إلى المسؤول عن شبكة المؤسسة المحلية إذا كان المستخدم يعتبر عملية المنع حدثت عن طريق الخطأ. بعد أن يطلب المستخدم توفير الوصول، يرسل Kaspersky Endpoint Security حدثًا إلى Kaspersky Security Center: **رسالة منع نشاط التطبيق إلى المسؤول**. ويحتوي وصف الحدث على رسالة إلى المسؤول بالمتغيرات المستبدلة. ويمكنك عرض هذه الأحداث في وحدة تحكم Kaspersky Security Center باستخدام تحديد الحدث المحدد مسبقًا **طلبات المستخدم**. وإذا لم يتم نشر Kaspersky Security Center في مؤسستك أو لم يكن هناك اتصال بخادم الإدارة، سيرسل التطبيق رسالة إلى المسؤول إلى عنوان البريد الإلكتروني المحدد.

مراقبة سلامة الملف

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم. ولا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل.

يعمل مكون مراقبة سلامة الملف فقط على الخوادم التي تحتوي على نظام ملفات NTFS أو ReFS.

بدءً من الإصدار 11.11.0 يتضمن Kaspersky Endpoint Security for Windows مكون مراقبة سلامة الملف. ويكتشف مكون مراقبة سلامة الملف التغييرات في الكائنات (الملفات والمجلدات) في منطقة مراقبة معينة. وقد تشير هذه التغييرات إلى حدوث خرق لأمان الكمبيوتر. وعند اكتشاف تغييرات الكائن، يُبلغ التطبيق المسؤول.

لاستخدام مكون مراقبة سلامة الملف تحتاج إلى تكوين نطاق المكون، أي تحديد الكائنات التي يجب أن يراقب المكون حالتها.

يمكنك عرض معلومات حول نتائج عملية مراقبة سلامة الملف في Kaspersky Security Center وفي واجهة Kaspersky Endpoint Security for Windows.

إعدادات مكون مراقبة سلامة الملف

المعلمة	الوصف
مستوى خطورة الحدث	يسجل Kaspersky Endpoint Security أحداث تعديل الملف كلما تم تعديل ملف في نطاق المراقبة. وتتوفر مستويات خطورة الحدث التالية: معلوماتي، تحذير، حرج.
نطاق المراقبة	قائمة الملفات والمجلدات التي يراقبها مكون مراقبة سلامة الملف. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع. على سبيل المثال، `C:\Folder\Application\`.
الاستثناءات	قائمة الاستثناءات من نطاق المراقبة. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع. على سبيل المثال، `C:\Folder\Application\*.log`. وتتمتع إدخالات الاستثناء بأولوية أعلى من إدخالات نطاق المراقبة.

أداة استشعار نقطة النهاية

أداة استشعار نقطة النهاية ليست متضمنة في Kaspersky Endpoint Security 11.4.0.

يمكنك إدارة أداة استشعار نقطة النهاية في وحدة التحكم Kaspersky Security Center Web Console وكذلك في Kaspersky Security Center Administration Console. لا يمكن إدارة أداة استشعار نقطة النهاية في وحدة التحكم Kaspersky Security Center Cloud Console.

أداة استشعار نقطة النهاية مصممة للتفاعل مع منصةKaspersky Anti Targeted Attack Platform. منصة Kaspersky Anti Targeted Attack عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. ويتضمن Kaspersky Anti Targeted Attack Platform مكونين وظيفيين: Kaspersky Anti Targeted Attack (ويشار إليه هنا باسم "KATA") والثاني Kaspersky Endpoint Detection and Response (ويشار إليه هنا باسم "EDR (KATA")). ويمكنك شراء EDR (KATA) بشكل منفصل. وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

إدارة أداة استشعار نقطة النهاية عليها القيود التالية:

- يمكنك تكوين إعدادات أداة استشعار نقطة النهاية في سياسة شريطة أن يكون Kaspersky Endpoint Security بالإصدار 11.0.0 إلى 11.3.0 مثبتًا على الكمبيوتر. وللمزيد من المعلومات عن تكوين إعدادات أداة استشعار نقطة النهاية باستخدام السياسة، يرجى الرجوع إلى مقالات الدعم للإصدارات السابقة من Kaspersky Endpoint Security.
- إذا كان الإصدار 11.4.0 أو أحدث من Kaspersky Endpoint Security مثبتًا على جهاز الكمبيوتر، فلن تتمكن من تكوين إعدادات أداة استشعار نقطة النهاية من السياسة.

يتم تثبيت أداة استشعار نقطة النهاية على أجهزة الكمبيوتر العميلة. يقوم المكون بمراقبة العمليات واتصالات الشبكة النشطة والملفات التي تم تعديلها بشكل مستمر على أجهزة الكمبيوتر هذه. تقوم أداة استشعار نقطة النهاية بترحيل المعلومات إلى خادم KATA.

تتوفر وظيفة المكون تحت أنظمة التشغيل التالية:

- Windows 7 Service Pack 1 Home / Professional / Enterprise؛
- Windows 8.1.1 Professional / Enterprise؛
- Windows 10 RS3 Home / Professional / Education / Enterprise؛
- Windows 10 RS4 Home / Professional / Education / Enterprise؛
- Windows 10 RS5 Home / Professional / Education / Enterprise؛
- Windows 10 RS6 Home / Professional / Education / Enterprise؛
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit)؛
- Windows Server 2012 Foundation / Standard / Enterprise (64-bit)؛
- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit)؛
- Windows Server 2016 Essentials / Standard (64-bit).

للحصول على معلومات تفصيلية حول عمل KATA، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

Kaspersky Sandbox

بدءًا من الإصدار 11.7.0، يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا للتكامل مع حل Kaspersky Sandbox. ويكتشف حل Kaspersky Sandbox ويمنع تلقائيًا التهديدات المتقدمة على أجهزة الكمبيوتر. ويحلل Kaspersky Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Kaspersky Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Kaspersky Sandbox). وللحصول على تفاصيل حول الحل، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

يمكن إدارة المكون فقط باستخدام Kaspersky Security Center Web Console. لا يمكنك إدارة هذا المكون باستخدام وحدة تحكم الإدارة (MMC).

إعدادات مكون Kaspersky Sandbox

المعلمة	الوصف
Server TLS certificate	لتكوين اتصال موثوق به مع خوادم Kaspersky Sandbox، يجب عليك إعداد شهادة TLS. وبعد ذلك، يجب إضافة الشهادة إلى خوادم Kaspersky Sandbox وسياسة Kaspersky Endpoint Security. وللحصول على تفاصيل عن إعداد الشهادة وإضافة الشهادة إلى الخوادم، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.
Timeout	انتهت مهلة الاتصال لخادم Kaspersky Sandbox. بعد انقضاء المهلة التي تم تكوينها، يرسل Kaspersky Endpoint Security طلبًا إلى الخادم التالي. ويمكنك زيادة مهلة الاتصال لتطبيق Kaspersky Sandbox إذا كانت سرعة الاتصال لديك منخفضة أو إذا كان الاتصال غير مستقر. مهلة الطلب الموصى بها 0.5 ثانية أو أقل.
Kaspersky Sandbox request queue	حجم مجلد قائمة انتظار الطلبات. عند الوصول إلى كائن على الكمبيوتر (تم تشغيل الملف القابل للتنفيذ أو فتح المستند، على سبيل المثال بتنسيق DOCX أو PDF)، يستطيع برنامج Kaspersky Endpoint Security أيضًا إرسال الكائن لفحصه بواسطة Kaspersky Sandbox. في حالة وجود طلبات متعددة، يُنشئ Kaspersky Endpoint Security قائمة انتظار الطلبات. وافتراضيًا، يقتصر حجم مجلد قائمة انتظار الطلبات على 100 ميجابايت. وبعد الوصول إلى الحد الأقصى للحجم، يتوقف Kaspersky Sandbox عن إضافة طلبات جديدة إلى قائمة الانتظار ويرسل الحدث المقابل إلى Kaspersky Security Center. ويمكنك تكوين حجم مجلد قائمة انتظار الطلبات بناءً على تكوين خادمك.
Kaspersky Sandbox servers	إعدادات اتصال خادم Kaspersky Sandbox. تستخدم الخوادم الصور الافتراضية المنشورة لأنظمة تشغيل Microsoft Windows لتشغيل الكائنات التي تحتاج إلى فحصها. ويمكنك إدخال عنوان IP (IPv4 أو IPv6) أو اسم مجال مؤهل بالكامل.
Action on threat detection	**Move copy to Quarantine, delete object**. في حالة تحديد هذا الخيار، يحذف Kaspersky Endpoint Security الكائن الضار الموجود على الكمبيوتر. قبل حذف الكائن، يُنشئ Kaspersky Endpoint Security نسخة احتياطية في حالة الحاجة إلى استعادة الكائن لاحقًا. ينقل Kaspersky Endpoint Security النسخة الاحتياطية إلى العزل. **Run scan of critical areas**. في حالة تحديد هذا الخيار، يُشغل Kaspersky Endpoint Security مهمة فحص المناطق الحرجة بشكلٍ افتراضي، يفحص Kaspersky Endpoint Security ذاكرة kernel والعمليات قيد التشغيل وقطاعات تمهيد القرص. **Create IOC scan task**. في حالة تحديد هذا الخيار، ينشئ Kaspersky Endpoint Security تلقائيًا مهمة فحص مؤشر الاختراق (مهمة فحص مؤشر الاختراق مستقلة). ولهذه المهمة، يمكنك تكوين وضع التشغيل ونطاق الفحص والإجراء عند اكتشاف IOC: حذف الكائن وتشغيل مهمة فحص المناطق الحرجة. ولتعديل الإعدادات الأخرى لمهمة فحص IOC، انتقل إلى إعدادات المهمة.
IOC scan scope	**Critical file areas**. في حالة تحديد هذا الخيار، ينفذ Kaspersky Endpoint Security فحص IOC فقط في مناطق الملفات الحرجة بالكمبيوتر: ذاكرة kernel (قلب نظام التشغيل) ومقاطع التشغيل. **File areas on system drives of the computer**. في حالة تحديد هذا الخيار، ينفذ Kaspersky Endpoint Security فحص IOC على محرك أقراص النظام في الكمبيوتر.
Run IOC scan task	**Manually**. وضع التشغيل الذي يمكنك من خلاله بدء تشغيل مهمة فحص IOC يدويًا في الوقت الذي تختاره. **After threat is detected**. وضع التشغيل الذي يقوم فيه Kaspersky Endpoint Security بتشغيل مهمة فحص IOC تلقائيًا عند اكتشاف تهديد. **Run only when the computer is idle**. وضع التشغيل الذي يقوم فيه Kaspersky Endpoint Security بتشغيل مهمة فحص IOC إذا كانت شاشة التوقف نشطة أو كانت الشاشة مقفلة. وإذا ألغى المستخدم قفل الكمبيوتر، يوقف Kaspersky Endpoint Security المهمة مؤقتًا. وهذا يعني أن المهمة قد تستغرق عدة أيام حتى تكتمل.

Endpoint Detection and Response

بدءًا من الإصدار 11.7.0، يتضمن Kaspersky Endpoint Security for Windows عاملًا مضمنًا لحل Kaspersky Endpoint Detection and Response Optimum (يشار إليه فيما يلي أيضًا باسم "EDR Optimum"). وبدءًا من الإصدار 11.8.0، يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا لحل Kaspersky Endpoint Detection and Response Expert (يشار إليه فيما يلي أيضًا باسم "EDR Expert"). ويعد Kaspersky Endpoint Detection and Response مجموعة حلول لحماية البنية التحتية لتكنولوجيا المعلومات في الشركة من التهديدات الإلكترونية المتقدمة. وتجمع وظائف الحلول بين الاكتشاف التلقائي للتهديدات والقدرة على الرد على هذه التهديدات لمواجهة الهجمات المتقدمة بما في ذلك عمليات الاستغلال الجديدة وبرامج الفدية والهجمات الخالية من الملفات، بالإضافة إلى الأساليب التي تستخدم أدوات النظام المشروعة. ويوفر EDR Expert وظائف أكثر لرصد التهديدات والاستجابة لها من EDR Optimum. وللحصول على التفاصيل عن الحلول، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

يراجع حل Kaspersky Endpoint Detection and Response ويحلل تطور التهديدات ويزود أفراد الأمن أو المسؤول بمعلومات حول الهجوم المحتمل اللازمة للاستجابة في وقت مناسب. يعرض Kaspersky Endpoint Detection and Response تفاصيل الاكتشاف في نافذة منفصلة. تفاصيل الاكتشاف عبارة عن أداة لعرض كامل المعلومات التي تم جمعها حول التهديد المكتشف. وتتضمن تفاصيل الاكتشاف، على سبيل المثال، محفوظات الملفات التي تظهر على الكمبيوتر. وللحصول على التفاصيل عن إدارة تفاصيل الاكتشاف، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

يمكنك تكوين مكون EDR Optimum في Cloud Console وCloud Console. وتتوفر إعدادات المكون لتطبيق EDR Expert فقط في Cloud Console.

إعدادات Endpoint Detection and Response

المعلمة	الوصف
Network isolation	عزل تلقائي للكمبيوتر من شبكة الاتصال استجابة للتهديدات المكتشفة. وعند تشغيل عزل شبكة الاتصال، يقطع التطبيق جميع الاتصالات النشطة ويحظر جميع اتصالات TCP/IP الجديدة على الكمبيوتر. ويترك التطبيق الاتصالات التالية نشطة فقط: • الاتصالات المدرجة في استثناءات عزل شبكة الاتصال. • الاتصالات التي بدأتها خدمات Kaspersky Endpoint Security. • الاتصالات التي بدأها عميل شبكة Kaspersky Security Center.
Automatically unlock isolated computer in N ساعة	فيمكن إيقاف عزل شبكة الاتصال تلقائيًا بعد وقت محدد أو يدويًا. وافتراضيًا، يوقف Kaspersky Endpoint Security تشغيل عزل شبكة الاتصال بعد 5 ساعات من بدء العزل.
Network isolation exclusions	قائمة قواعد الاستثناءات من عزل شبكة الاتصال. لا يتم حظر اتصالات شبكة الاتصال التي تطابق القواعد على أجهزة الكمبيوتر عند تشغيل عزل شبكة الاتصال. لتكوين استثناءات عزل الشبكة، يمكنك استخدام قائمة ملفات تعريف الشبكة القياسية. افتراضيًا، تتضمن الاستثناءات ملفات تعريف الشبكة التي تحتوي على قواعد تضمن التشغيل المتواصل للأجهزة مع خادم DNS/DHCP وأدوار عميل DNS/DHCP. ويمكنك أيضًا تعديل إعدادات ملفات تعريف الشبكة القياسية أو تحديد الاستثناءات يدويًا. يتم تطبيق الاستثناءات المحددة في خصائص السياسة فقط في حالة تشغيل عزل شبكة الاتصال تلقائيًا استجابة لتهديد مكتشف. ويتم تطبيق الاستثناءات المحددة في خصائص الكمبيوتر فقط في حالة تشغيل عزل شبكة الاتصال يدويًا في خصائص الكمبيوتر في وحدة تحكم Kaspersky Security Center أو في تفاصيل التنبيه.
Execution prevention	التحكم في تنفيذ الملفات التنفيذية والبرامج النصية وفتح ملفات تنسيق Office. على سبيل المثال، يمكنك منع تنفيذ التطبيقات التي تعتبر غير آمنة على الكمبيوتر المحدد. ويدعم منع التنفيذ مجموعة من امتدادات ملفات Office ومجموعة من مترجمي البرنامج النصي. لاستخدام مكون منع التنفيذ، تحتاج إلى إضافة قواعد منع التنفيذ. قاعدة منع التنفيذ هي مجموعة من المعايير التي يضعها التطبيق في الاعتبار عند الاستجابة لتنفيذ كائن، على سبيل المثال عند منع تنفيذ الكائن. يتعرف التطبيق على الملفات حسب مساراتها أو المجاميع الاختبارية المحسوبة باستخدام خوارزميات التجزئة MD5 وSHA256.

Action on execution or opening of forbidden object	**Block and write to report**. في هذا الوضع، يحظر التطبيق تنفيذ الكائنات أو فتح المستندات التي تطابق معايير قاعدة المنع. وينشر التطبيق أيضًا حدثًا حول محاولات تنفيذ الكائنات أو فتح المستندات في سجل أحداث Windows وسجل أحداث Kaspersky Security Center. **Log events only**. في هذا الوضع، ينشر Kaspersky Endpoint Security حدثًا حول محاولات تشغيل الكائنات القابلة للتنفيذ أو فتح مستندات تطابق معايير قاعدة المنع مع سجل أحداث Windows وKaspersky Security Center، لكنها لا تمنع محاولة تشغيل أو فتح الكائن أو المستند. ويتحدد هذا الوضع بشكل افتراضي.
Cloud Sandbox	Cloud Sandbox هي تقنية تتيح لك اكتشاف التهديدات المتقدمة على جهاز كمبيوتر. ويعيد Kaspersky Endpoint Security تلقائيًا توجيه الملفات المكتشفة إلى Cloud Sandbox لتحليلها. ويقوم Cloud Sandbox بتشغيل هذه الملفات في بيئة معزولة لتحديد النشاط الضار وتحديد سمعتها. ثم يتم إرسال البيانات الموجودة في هذه الملفات إلى Kaspersky Security Network. لذلك، إذا اكتشف Cloud Sandbox ملفًا ضارًا، فسوف ينفذ Kaspersky Endpoint Security الإجراء المناسب للقضاء على هذا التهديد على جميع أجهزة الكمبيوتر التي تم اكتشاف هذا الملف عليها. يتم تمكين تقنية Cloud Sandbox بشكل دائم وهي متاحة لجميع مستخدمي Kaspersky Security Network بغض النظر عن نوع الترخيص الذي يستخدمونه. في حالة تحديد خانة الاختيار هذه، سيقوم Kaspersky Endpoint Security بتمكين عداد التهديدات المكتشفة باستخدام Cloud Sandbox في نافذة التطبيق الرئيسية تحت **تقنيات اكتشاف التهديدات**. وسيشير Kaspersky Endpoint Security أيضًا إلى تقنية اكتشاف التهديدات في Cloud Sandbox في أحداث التطبيق وفي تقرير التهديدات في وحدة تحكم Kaspersky Security Center.

(Endpoint Detection and Response (KATA

يتضمن الإصدار 12.1 من Kaspersky Endpoint Security الآن عاملاً مضمنًا لإدارة مكون Kaspersky Endpoint Detection and Response كجزء من حل Kaspersky Anti Targeted Attack Platform. منصة Kaspersky Anti Targeted Attack عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدِفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. ويتضمن Kaspersky Anti Targeted Attack Platform مكونين وظيفيين: Kaspersky Anti Targeted Attack (ويشار إليه هنا باسم "KATA") والثاني Kaspersky Endpoint Detection and Response (ويشار إليه هنا باسم "EDR (KATA")). ويمكنك شراء EDR (KATA) بشكل منفصل. وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

يتم تثبيت Kaspersky Endpoint Security على أجهزة كمبيوتر فردية على البنية التحتية لتكنولوجيا المعلومات بالشركة ويراقب باستمرار العمليات واتصالات الشبكة المفتوحة والملفات التي يتم تعديلها. ويتم إرسال معلومات عن الأحداث على الكمبيوتر (بيانات القياس عن بُعد) إلى خادم Kaspersky Anti Targeted Attack Platform. وفي هذه الحالة، يرسل Kaspersky Endpoint Security أيضًا معلومات إلى خادم Kaspersky Anti Targeted Attack Platform حول التهديدات التي اكتشفتها Kaspersky بالإضافة إلى معلومات عن نتائج معالجة هذه التهديدات.

تم تكوين تكامل EDR (KATA) على وحدة تحكم Kaspersky Security Center. وبعد ذلك تتم إدارة العامل المضمن باستخدام وحدة تحكم Kaspersky Anti Targeted Attack Platform، بما في ذلك مهام التشغيل وإدارة الكائنات المعزولة وعرض التقارير والإجراءات الأخرى.

إعدادات (Endpoint Detection and Response (KATA

المعلمة	الوصف
Settings for connecting to KATA servers	**Timeout**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف. **Server TLS certificate**. شهادة TLS لإنشاء اتصال موثوق به مع خادم Central Node. ويمكنك الحصول على شهادة TLS في وحدة تحكم Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform). **Use two-way authentication**. تسمح المصادقة ثنائية الاتجاه بتمكين عملية تحقق إضافية للكمبيوتر على Central Node. ولتمكين هذا التحقق، يجب عليك تشغيل المصادقة ثنائية الاتجاه في إعدادات Central Node وKaspersky Endpoint Security. ولاستخدام المصادقة ثنائية الاتجاه، ستحتاج أيضًا إلى حاوية تشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. ويمكنك الحصول على حاوية تشفير في Kaspersky Anti Targeted Attack Platform (راجع الإرشادات في تعليمات Kaspersky Anti Targeted Attack Platform).

	يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.
KATA servers	إعدادات اتصال خادم العقدة المركزية. يمكنك إدخال عنوان IP (IPv4 أو IPv6).
Send sync request to KATA server (every (min	عدد مرات إرسال طلبات المزامنة إلى خادم العقدة المركزية. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.
إرسال القياس عن بعد إلى KATA	تتيح لك هذه الوظيفة إيقاف تشغيل إرسال القياس عن بُعد إلى الخادم تمامًا. وإذا كنت تستخدم Kaspersky Anti Targeted Attack Platform جنبًا إلى جنب مع حل آخر يستخدم أيضًا القياس عن بُعد، يمكنك إيقاف تشغيل القياس عن بُعد لحل KATA (EDR)). ويتيح لك هذا تحسين حمل الخادم لهذه الحلول. على سبيل المثال، إذا كان لديك حل Managed Detection and Response وتم نشر KATA (EDR)، يمكنك استخدام القياس عن بُعد في MDR وإنشاء مهام الاستجابة للتهديد في KATA (EDR)).
Maximum events transmission (delay (sec	يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
Enable request throttling	تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تحديد خانة الاختيار، فإن التطبيق يُقيد الأحداث المرسلة. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث.
Maximum number of events per hour	يحلل التطبيق تدفق بيانات القياس عن بُعد ويُقيد إرسال الأحداث إذا تجاوز تدفق الحدث حد الأحداث المكون لكل ساعة. ويستأنف Kaspersky Endpoint Security إرسال الأحداث بعد ساعة. الإعداد الافتراضي هو 3000 حدث في الساعة.
Percentage of event limit excess	يفرز التطبيق الأحداث حسب النوع (على سبيل المثال" أحداث "التغييرات في السجل") ويقيد إرسال الأحداث إذا تجاوزت نسبة الأحداث من النوع نفسه إلى العدد الإجمالي للأحداث الحد الذي تم تكوينه بالنسبة المئوية. ويستأنف Kaspersky Endpoint Security إرسال الأحداث عندما تصبح نسبة الأحداث الأخرى إلى العدد الإجمالي للأحداث كبيرة بما يكفي مرة أخرى. الإعداد الافتراضي هو 15%.

تشفير القرص بالكامل

يمكنك تحديد تقنية تشفير: تشفير القرص من Kaspersky أو تشفير محرك الأقراص من BitLocker (المشار إليها فيما بعد بمجرد "BitLocker").

تشفير القرص من Kaspersky

بعد تشفير محركات الأقراص الصلبة للنظام، عند بدء التشغيل التالي للكمبيوتر، يجب أن يكمل المستخدم المصادقة باستخدام وكيل المصادقة قبل إمكانية الوصول إلى محركات الأقراص الصلبة وتحميل نظام التشغيل. ويتطلب ذلك إدخال كلمة المرور للرمز المميز أو البطاقة الذكية الموصلة بالكمبيوتر، أو اسم المستخدم وكلمة مرور حساب وكيل المصادقة الذي تم إنشاؤه بواسطة مسؤول الشبكة المحلية باستخدام مهمة إدارة حسابات وكيل المصادقة. وتعتمد هذه الحسابات على حسابات Microsoft Windows التي يقوم المستخدمون من خلالها بتسجيل الدخول إلى نظام التشغيل. يمكنك كذلك استخدام تقنية تسجيل الدخول الأحادي (SSO) التي تتيح لك الولوج تلقائيًا إلى نظام التشغيل باستخدام اسم المستخدم وكلمة المرور لحساب وكيل المصادقة.

يمكن إجراء مصادقة المستخدم في وكيل المصادقة بطريقتين:

- أدخل اسم وكلمة مرور حساب وكيل المصادقة الذي تم إنشاؤه بواسطة مسؤول الشبكة المحلية باستخدام أدوات Kaspersky Security Center.
- أدخل كلمة مرور الرمز المميز أو البطاقة الذكية المتصلة بالكمبيوتر.

يتوفر استخدام رمز مميز أو بطاقة ذكية فقط إذا تم تشفير محركات الأقراص الصلبة للكمبيوتر باستخدام لوغاريتم التشفير AES256. إذا تم تشفير محركات الأقراص الصلبة في الكمبيوتر باستخدام خوارزمية التشفير AES56، فسيتم رفض إضافة ملف الشهادة الإلكترونية إلى الأمر.

تشفير محرك الأقراص من BitLocker

BitLocker هي تقنية تشفير مدمجة في نظام التشغيل Windows. Kaspersky Endpoint Security يسمح لك بالتحكم في Bitlocker وإدارتها باستخدام Kaspersky Security Center. BitLocker تقوم بتشفير أحجام منطقية. لا يمكن استخدام تقنية BitLocker في تشفير محركات الأقراص القابلة للإزالة. وللحصول على مزيد من التفاصيل عن BitLocker، يُرجى الرجوع إلى مستندات Microsoft.

BitLocker توفر تخزين آمن لمفاتيح الوصول باستخدام وحدة نمطية للنظام الأساسي الموثوق به. الوحدة النمطية للنظام الأساسي الموثوق به (TPM) هي رقاقة إلكترونية تم تصميمها لتوفير الوظائف الأساسية المرتبطة بالأمن (على سبيل المثال، لتخزين مفاتيح التشفير). عادة يتم تركيب الوحدة النمطية للنظام الأساسي الموثوق به على اللوحة الأم في جهاز الكمبيوتر وتتفاعل مع كل مكونات النظام الأخرى عبر ناقل الأجهزة. استخدام TPM هي أكثر طريقة آمنة لتخزين مفاتيح وصول BitLocker حيث إن TPM توفر تحقق من سلامة النظام قبل التشغيل. لا يزال بإمكانك تشفير محركات الأقراص على جهاز كمبيوتر بدون استخدام TPM. في هذه الحالة، سيتم تشفير مفتاح الوصول بكلمة مرور. BitLocker يستخدم أساليب المصادقة التالية:

- TPM.
- TPM ورمز PIN.
- كلمة المرور.

بعد تشفير محرك أقراص، يقوم BitLocker بإنشاء مفتاح رئيسي. يقوم Kaspersky Endpoint Security بإرسال المفتاح الرئيسي إلى Kaspersky Security Center حتى يمكنك استعاد الوصول إلى القرص إذا، مثلًا، نسي المستخدم كلمة المرور.

إذا قام مستخدم بتشفير قرص باستخدام BitLocker، فسوف يرسل Kaspersky Endpoint Security معلومات عن تشفير القرص إلى Kaspersky Security Center. مع ذلك، سوف يقوم Kaspersky Endpoint Security بإرسال المفتاح الرئيسي إلى Kaspersky Security Center حتى يكون من المستحيل استعادة الوصول إلى القرص باستخدام Kaspersky Security Center. كي تعمل تقنية BitLocker بشكل صحيح مع Kaspersky Security Center، قم بفك تشفير محرك الأقراص وأعد تشفيره باستخدام سياسة. يمكنك فك تشفير محرك أقراص محليًا أو باستخدام سياسة.

بعد تشفير محرك أقراص النظام، يحتاج المستخدم إلى تجاوز مصادقة BitLocker لإقلاع نظام التشغيل. وبعد إجراء المصادقة، سوف تسمح تقنية BitLocker للمستخدمين بتسجيل الدخول. ولا تدعم BitLocker تقنية تسجيل الدخول الأحادي (SSO).

إذا كنت تستخدم سياسات مجموعات Windows، أوقف تشغيل إدارة BitLocker في إعدادات السياسة. يمكن أن تتعارض إعدادات السياسة لنظام Windows مع إعدادات سياسة Kaspersky Endpoint Security. عند تشفير محرك أقراص، يمكن أن تحدث أخطاء.

إعدادات مكون تشفير القرص من Kaspersky

المعلمة	الوصف
وضع التشفير	**تشفير جميع محركات الأقراص الصلبة**. إذا تم تحديد هذا العنصر، فيقوم التطبيق بتشفير جميع محركات الأقراص الصلبة عند تطبيق السياسة. في حالة تثبيت العديد من أنظمة التشغيل على الكمبيوتر، فسوف يمكنك بعد التشفير تحميل نظام التشغيل المثبتة عليه التطبيق فقط. **فك تشفير جميع محركات الأقراص الصلبة**. إذا تم تحديد هذا العنصر، فيقوم التطبيق بفك تشفير جميع محركات الأقراص الصلبة المشفرة سابقًا عند تطبيق السياسة. **عدم التغيير**. إذا تم تحديد هذا العنصر، فيقوم التطبيق بترك محركات الأقراص على حالتها السابقة عند تطبيق السياسة. إذا كان قد تم تشفير محرك الأقراص، فسيظل مشفرًا. في حالة فك تشفير محرك الأقراص، فسيظل دون تشفير. ويتم تحديد هذا العنصر افتراضيًا.
أثناء التشفير، أنشئ حسابات	وفي حالة تحديد خانة الاختيار هذه، ينشئ التطبيق حسابات وكيل المصادقة استنادًا إلى قائمة حسابات مستخدمي Windows على الكمبيوتر. بشكل افتراضي، Kaspersky Endpoint Security يستخدم جميع الحسابات المحلية والمجالية التي قام المستخدم من خلالها بتسجيل الدخول إلى نظام التشغيل في آخر 30 يومًا.

وكيل المصادقة تلقائيًا لمستخدمي Windows	
إعدادات إنشاء حساب وكيل المصادقة	**جميع الحسابات على الكمبيوتر**. جميع الحسابات على الكمبيوتر التي كانت نشطة في أي وقت. **جميع حسابات المجال على الكمبيوتر**. جميع الحسابات على الكمبيوتر التي تنتمي إلى مجال ما والتي كانت نشطة في أي وقت. **جميع الحسابات المحلية على الكمبيوتر**. جميع الحسابات المحلية على الكمبيوتر التي كانت نشطة في أي وقت. **حساب الخدمة مع كلمة مرور لمرة واحدة**. ويعد حساب الخدمة ضروريًا للوصول إلى الكمبيوتر، على سبيل المثال، عندما ينسى المستخدم كلمة المرور. ويمكنك أيضًا استخدام حساب الخدمة كحساب احتياطي. يجب عليك إدخال اسم الحساب (افتراضيًا، `ServiceAccount`). يُنشئ Kaspersky Endpoint Security كلمة مرور تلقائيًا. ويمكنك العثور على كلمة المرور في وحدة تحكم Kaspersky Security Center. **المسؤول المحلي**. ينشئ Kaspersky Endpoint Security حساب مستخدم وكيل مصادقة للمسؤول المحلي للكمبيوتر. **إدارة الكمبيوتر**. يُنشئ Kaspersky Endpoint Security حساب مستخدم وكيل مصادقة لحساب إدارة الكمبيوتر. يمكنك معرفة الحساب الذي يتمتع بدور إدارة الكمبيوتر في خصائص الكمبيوتر في Active Directory. وبشكل افتراضي، لم يتم تحديد دور إدارة الكمبيوتر، أي أنه لا يتوافق مع أي حساب. **الحساب النشط**. يُنشئ Kaspersky Endpoint Security تلقائيًا حساب وكيل مصادقة للحساب النشط في وقت تشفير القرص.
أنشئ تلقائيًا حسابات وكيل المصادقة لجميع مستخدمي هذا الكمبيوتر عند تسجيل الدخول	في حالة تحديد خانة الاختيار هذه، يتحقق التطبيق من المعلومات حول حسابات مستخدمي Windows على الكمبيوتر قبل بدء وكيل المصادقة. إذا اكتشف Kaspersky Endpoint Security حساب مستخدم Windows ليس له حساب وكيل مصادقة، فسوف ينشئ التطبيق حسابًا جديدًا للوصول إلى محركات الأقراص المشفرة. وسوف يتضمن حساب وكيل المصادقة الجديد الإعدادات الافتراضية التالية: تسجيل الدخول المحمي بكلمة مرور فقط وتغيير كلمة المرور عند المصادقة الأولى. لذلك، لا تحتاج إلى إضافة حسابات وكيل المصادقة يدويًا باستخدام مهمة إدارة حسابات وكيل المصادقة لأجهزة الكمبيوتر التي تحتوي على محركات أقراص مشفرة بالفعل.
حفظ اسم المستخدم المدخل في وكيل المصادقة	إذا تم تحديد خانة الاختيار، فسيحفظ التطبيق اسم حساب وكيل المصادقة. لن تتم مطالبتك بإدخال اسم الحساب في المحاولة التالية لإكمال المصادقة في وكيل المصادقة بموجب نفس الحساب.
تشفير مساحة القرص المستخدمة فقط (يحد من وقت التشفير)	يؤدي تحديد خانة الاختيار هذه إلى تمكين / تعطيل الخيار الذي يقيد منطقة التشفير لمقاطع محرك الأقراص الصلبة الممتلئة فقط. ويتيح لك هذا الحد تقليل وقت التشفير. لا يؤدي تمكين أو تعطيل ميزة **تشفير مساحة القرص المستخدمة فقط (يحد من وقت التشفير)** بعد بدء التشفير إلى تعديل هذا الإعداد حتى يتم فك تشفير محركات الأقراص الثابتة. يجب تحديد أو إلغاء تحديد خانة الاختيار قبل بدء التشفير. في حالة تحديد خانة الاختيار، يتم تشفير أجزاء محرك القرص الصلب الممتلئة بالملفات فقط. ويقوم Kaspersky Endpoint Security تلقائيًا بتشفير البيانات الجديدة بمجرد إضافتها. في حالة إلغاء تحديد خانة الاختيار، يتم تشفير محرك القرص الصلب بالكامل، بما في ذلك القطاعات المتبقية من الملفات التي تم حذفها وتعديلها سابقًا. هذا الخيار مستحسن لمحركات الأقراص الصلبة الجديدة التي لم يتم تعديل بياناتها أو حذفها. وإذا كنت تقوم بتشفير محرك أقراص صلبة مستخدم بالفعل، فمن المستحسن تشفير محرك الأقراص الصلبة بالكامل. ويضمن هذا حماية كل البيانات، وحتى حذف البيانات التي يحتمل أن تكون قابلة للاسترداد. ويتم إلغاء تحديد خانة الاختيار هذه بشكل افتراضي.
استخدام دعم USB القديم	خانة الاختيار هذه تقوم بتفعيل/تعطيل وظيفة دعم USB القديم. دعم USB القديم **هو** وظيفة في BIOS/UEFI تتيح لك استخدام أجهزة USB (مثل رمز أمان مميز) أثناء مرحلة إقلاع جهاز الكمبيوتر قبل بدء نظام التشغيل (وضع BIOS). دعم USB القديم لا يؤثر على

(غير موصى به)	دعم أجهزة USB بعد بدء تشغيل نظام التشغيل. في حالة تحديد خانة الاختيار، سوف يتم تمكين دعم أجهزة USB أثناء بدء التشغيل المبدئي للكمبيوتر. عند تفعيل وظيفة دعم USB القديم، فإن وكيل المصادقة في وضع BIOS لا يدعم العمل مع الرموز مع USB. ومن المستحسن استخدام هذا الخيار فقط عند وجود مشكلة في توافق الأجهزة وفقط لأجهزة الكمبيوتر التي حدثت عليها المشكلة.
إعدادات كلمة المرور	إعدادات قوة كلمة مرور حساب وكيل المصادقة. عند استخدام تقنية تسجيل الدخول الأحادي فإن وكيل المصادقة يتجاهل متطلبات قوة كلمة المرور المحددة في Kaspersky Security Center. يمكنك وضع متطلبات قوة كلمة المرور في إعدادات نظام التشغيل.
استخدام تقنية تسجيل الدخول الأحادي (SSO)	تتيح تقنية SSO إمكانية استخدام نفس بيانات اعتماد الحساب للوصول إلى محركات الأقراص الصلبة المشفرة لتسجيل الدخول إلى نظام التشغيل. في حالة تحديد خانة الاختيار، يجب عليك إدخال بيانات الاعتماد للوصول إلى محركات الأقراص الصلبة المشفرة ثم تسجيل الدخول تلقائيًا إلى نظام التشغيل. للوصول إلى محركات الأقراص الثابتة المشفرة ثم تسجيل الدخول إلى نظام التشغيل، في حالة إلغاء تحديد خانة الاختيار، يجب إدخال بيانات الاعتماد كل على حدة للوصول إلى محركات الأقراص الثابتة المشفرة وبيانات اعتماد حساب مستخدم نظام التشغيل.
استخدام موفري بيانات الاعتماد الخارجيين	يدعم Kaspersky Endpoint Security موفر بيانات الاعتماد الخارجي ADSelfService Plus. عند العمل مع موفري بيانات اعتماد خارجيين، يعترض عامل المصادقة كلمة المرور قبل تحميل نظام التشغيل. وهذا يعني أن المستخدم يحتاج إلى إدخال كلمة مرور مرة واحدة فقط عند تسجيل الدخول إلى Windows. وبعد تسجيل الدخول إلى Windows، يستطيع المستخدم الاستفادة من إمكانات موفر بيانات اعتماد خارجي للمصادقة على سبيل المثال في خدمات الشركات. ويسمح موفرو بيانات الاعتماد الخارجيون كذلك للمستخدمين بإعادة تعيين كلمات المرور الخاصة بهم بشكل مستقل. وفي هذه الحالة، سيقوم Kaspersky Endpoint Security تلقائيًا بتحديث كلمة المرور لوكيل المصادقة. إذا كنت تستخدم موفر بيانات اعتماد خارجيًا لا يدعمه التطبيق، فقد تواجه بعض القيود في تشغيل تقنية تسجيل الدخول الأحادي.
تعليمات	**المصادقة**. نصوص المساعدة التي تظهر في نافذة وكيل المصادقة عند إدخال بيانات اعتماد الحساب. **تغيير كلمة المرور**. نصوص المساعدة التي تظهر في نافذة وكيل المصادقة عند تغيير كلمة المرور لحساب وكيل المصادقة. **استرداد كلمة المرور**. نصوص المساعدة التي تظهر في نافذة وكيل المصادقة عند استرداد كلمة المرور لحساب وكيل المصادقة.

إعدادات مكون تشفير محرك BitLocker

المعلمة	الوصف
وضع التشفير	**تشفير جميع محركات الأقراص الصلبة**. إذا تم تحديد هذا العنصر، فيقوم التطبيق بتشفير جميع محركات الأقراص الصلبة عند تطبيق السياسة. في حالة تثبيت العديد من أنظمة التشغيل على الكمبيوتر، فسوف يمكنك بعد التشفير تحميل نظام التشغيل المثبتة عليه التطبيق فقط. **فك تشفير جميع محركات الأقراص الصلبة**. إذا تم تحديد هذا العنصر، فيقوم التطبيق بفك تشفير جميع محركات الأقراص الصلبة المشفرة سابقًا عند تطبيق السياسة. **عدم التغيير**. إذا تم تحديد هذا العنصر، فيقوم التطبيق بترك محركات الأقراص على حالتها السابقة عند تطبيق السياسة. إذا كان قد تم تشفير محرك الأقراص، فسيظل مشفرًا. في حالة فك تشفير محرك الأقراص، فسيظل دون تشفير. ويتم تحديد هذا العنصر افتراضيًا.
تمكين استخدام مصادقة BitLocker التي تتطلب إدخال لوحة المفاتيح قبل التشغيل على أجهزة الكمبيوتر اللوحية	تؤدي خانة الاختيار هذه إلى تمكين / تعطيل استخدام المصادقة التي تتطلب إدخال بيانات في بيئة مسبقة التمهيد، حتى وإن كان النظام الأساسي ليس لديه قدرة الإدخال مسبق التمهيد (على سبيل المثال، لوحات المفاتيح التي تعمل باللمس على أجهزة الكمبيوتر اللوحية).

	إن شاشة اللمس الخاصة بأجهزة الكمبيوتر اللوحية غير متاحة في بيئة ما قبل التشغيل. لإكمال مصادقة BitLocker على أجهزة الكمبيوتر اللوحية، يجب على المستخدم، على سبيل المثال، توصيل لوحة مفاتيح USB. إذا تم تحديد خانة الاختيار، يتم السماح باستخدام المصادقة التي تتطلب إدخال مسبق التهيئة. من المستحسن استخدام هذا الإعداد فقط للأجهزة التي لديها أدوات إدخال بيانات بديلة في بيئة مسبقة التهيئة، مثل لوحة مفاتيح USB بالإضافة إلى لوحات المفاتيح التي تعمل باللمس على الشاشة. في حال عدم تحديد خانة الاختيار، فإن تشفير محرك الأقراص من BitLocker يكون غير ممكنًا على الأجهزة اللوحية.
استخدام تشفير الأجهزة (Windows 8 والإصدارات الأحدث)	إذا تم تحديد خانة الاختيار، يقوم التطبيق بتطبيق تشفير الأجهزة. يتيح لك ذلك زيادة سرعة التشفير واستخدام أقل لموارد الكمبيوتر.
تشفير مساحة القرص المستخدمة فقط (Windows 8 والإصدارات الأحدث)	يؤدي تحديد خانة الاختيار هذه إلى تمكين / تعطيل الخيار الذي يقيد منطقة التشفير لمقاطع محرك الأقراص الصلبة الممتلئة فقط. ويتيح لك هذا الحد تقليل وقت التشفير. لا يؤدي تمكين أو تعطيل ميزة **تشفير مساحة القرص المستخدمة فقط (يحد من وقت التشفير)** بعد بدء التشفير إلى تعديل هذا الإعداد حتى يتم فك تشفير محركات الأقراص الثابتة. يجب تحديد أو إلغاء تحديد خانة الاختيار قبل بدء التشفير. في حالة تحديد خانة الاختيار، يتم تشفير أجزاء محرك القرص الصلب الممتلئة بالملفات فقط. ويقوم Kaspersky Endpoint Security تلقائيًا بتشفير البيانات الجديدة بمجرد إضافتها. في حالة إلغاء تحديد خانة الاختيار، يتم تشفير محرك القرص الصلب بالكامل، بما في ذلك القطاعات المتبقية من الملفات التي تم حذفها وتعديلها سابقًا. هذا الخيار مستحسن لمحركات الأقراص الصلبة الجديدة التي لم يتم تعديل بياناتها أو حذفها. وإذا كنت تقوم بتشفير محرك أقراص صلبة مستخدم بالفعل، فمن المستحسن تشفير محرك الأقراص الصلبة بالكامل. ويضمن هذا حماية كل البيانات، وحتى حذف البيانات التي يحتمل أن تكون قابلة للاسترداد. ويتم إلغاء تحديد خانة الاختيار هذه بشكل افتراضي.
طريقة المصادقة	**كلمة المرور فقط (Windows 8 والإصدارات الأحدث)** في حالة تحديد هذا الاختيار، فإن Kaspersky Endpoint Security يطلب من المستخدم إدخال كلمة مرور عندما يحاول المستخدم الوصول إلى محرك مشفر. يمكن تحديد هذا الاختيار في حالة عدم استخدام وحدة نمطية للنظام الأساسي الموثوق به (TPM). **الوحدة النمطية للنظام الأساسي الموثوق بها (TPM)** إذا تم تحديد هذا الخيار، فيستخدم BitLocker الوحدة النمطية للنظام الأساسي الموثوق به (TPM). الوحدة النمطية للنظام الأساسي الموثوق به (TPM) هي رقاقة إلكترونية تم تصميمها لتوفير الوظائف الأساسية المرتبطة بالأمن (على سبيل المثال، لتخزين مفاتيح التشفير). عادة يتم تركيب الوحدة النمطية للنظام الأساسي الموثوق به على اللوحة الأم في جهاز الكمبيوتر وتتفاعل مع كل مكونات النظام الأخرى عبر ناقل الأجهزة. بالنسبة لأجهزة الكمبيوتر التي تعمل بنظام Windows 7 أو Windows Server 2008 R2، يتوفر التشفير باستخدام الوحدة TPM فقط. إذا لم يتم تثبيت وحدة TPM، فلن يكون تشفير BitLocker ممكنًا. استخدام كلمة مرور على أجهزة الكمبيوتر هذه غير مدعوم. يمكن للجهاز المزود بوحدة نمطية لنظام أساسي موثوق به إنشاء مفاتيح تشفير لا يمكن فك تشفيرها إلا باستخدام الجهاز. تقوم الوحدة النمطية للنظام الأساسي الموثوق به بتشفير مفاتيح التشفير باستخدام مفتاح تخزين الجذر الخاص بها. ويتم تخزين مفتاح تخزين الجذر داخل الوحدة النمطية للنظام الأساسي الموثوق به. يوفر ذلك مستوى إضافي من الحماية ضد محاولات اختراق مفاتيح التشفير.

ويتم تحديد هذا الإجراء بصورة افتراضية.

يمكنك تعيين طبقة حماية إضافية للوصول إلى مفتاح التشفير، وتشفير المفتاح بكلمة مرور أو رمز PIN:

- **استخدام رمز PIN لأجل TPM**. إذا كانت خانة الاختيار هذه محددة، يمكن للمستخدم استخدام رمز PIN للحصول على الوصول إلى مفتاح تشفير مخزن في وحدة نمطية للنظام الأساسي الموثوق به (TPM).
إذا كانت خانة الاختيار هذه غير محددة، فإنه لا يجوز للمستخدمين استخدام رموز PIN. للوصول إلى مفتاح التشفير، يجب على المستخدم إدخال كلمة المرور.
يمكنك السماح للمستخدم باستخدام رمز PIN المحسن. ويسمح رمز PIN المحسّن باستخدام أحرف أخرى بالإضافة إلى الأحرف الرقمية: الأحرف اللاتينية الكبيرة والصغيرة والأحرف الخاصة والمسافات.

- **وحدة النظام الأساسي الموثوق بها (TPM) أو كلمة المرور إذا لم تكن وحدة النظام الأساسي الموثوق بها متاحة**. إذا تم تحديد خانة الاختيار، فبإمكان المستخدم استخدام كلمة مرور للحصول على حق الوصول إلى مفاتيح التشفير عند عدم توفر الوحدة النمطية للنظام الأساسي الموثوق به.
في حال عدم تحديد خانة الاختيار وكان TPM غير متوفرًا، فإن تشفير القرص بالكامل لن يبدأ.

التشفير على مستوى الملف

يمكنك تجميع قوائم الملفات حسب الملحق أو مجموعة الملحقات وقوائم المجلدات المخزنة على محركات أقراص الكمبيوتر المحلية، وإنشاء قواعد لتشفير الملفات التي تم إنشاؤها بواسطة تطبيقات محددة. بعد تطبيق سياسة، يقوم Kaspersky Endpoint Security بتشفير الملفات التالية وفك تشفيرها:

- الملفات التي تمت إضافتها بشكل فردي إلى قوائم التشفير وفك التشفير؛
- الملفات المخزنة في المجلدات التي تمت إضافتها إلى قوائم التشفير وفك التشفير؛
- الملفات التي تم إنشاؤها بواسطة تطبيقات منفصلة.

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل. لا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم.

يحتوي تشفير الملف على الميزات الخاصة التالية:

- يقوم Kaspersky Endpoint Security بتشفير / فك تشفير الملفات في المجلدات المحددة مسبقًا فقط لملفات بيانات المستخدمين المحليين لنظام التشغيل. لا يقوم Kaspersky Endpoint Security بتشفير/فك تشفير الملفات في المجلدات المحددة مسبقًا لملفات بيانات مستخدمي التجوال وملفات بيانات المستخدم الإلزامي وملفات بيانات المستخدمين المؤقتين والمجلدات المعاد توجيهها.

- لا يشفر Kaspersky Endpoint Security الملفات التي قد يتسبب تعديلها في الإضرار بنظام التشغيل والتطبيقات المثبتة. على سبيل المثال، توجد الملفات والمجلدات التالية ذات المجلدات المتداخلة في قسم استثناءات التشفير:
  - %WINDIR%؛
  - %PROGRAMFILES% وكذلك %PROGRAMFILES(X86)%؛
  - ملفات تسجيل Windows.

لا يمكن عرض قائمة استثناءات التشفير أو تحريرها. على الرغم من إمكانية إضافة الملفات والمجلدات الموجودة في قائمة استثناءات التشفير إلى قائمة التشفير، فإنه لن يتم تشفيرها أثناء تشفير الملفات.

إعدادات مكون التشفير على مستوى الملف

المعلمة	الوصف
وضع	**عدم التغيير**. إذا تم تحديد هذا العنصر، فيترك Kaspersky Endpoint Security الملفات والمجلدات بدون تغيير دون تشفيرها أو

التشفير	فك تشفيرها. **وفقًا للقواعد**. في حالة اختيار هذا العنصر، يقوم Kaspersky Endpoint Security بتشفير الملفات والمجلدات وفق قواعد التشفير، وكذلك يفك تشفير الملفات والمجلدات وفق قواعد التشفير، وينظم وصول التطبيقات إلى الملفات المشفرة وفق قواعد التطبيق. **فك تشفير الكل**. إذا تم تحديد هذا العنصر، فيقوم Kaspersky Endpoint Security بفك تشفير جميع الملفات والمجلدات المشفرة.
التشفير	تعرض علامة التبويب هذه قواعد التشفير للملفات المخزنة على محركات الأقراص المحلية. يمكنك إضافة ملفات كما يلي: • **المجلدات المحددة مسبقًا**. يتيح Kaspersky Endpoint Security لك إضافة المناطق التالية: **المستندات**. الملفات في مجلد المستندات القياسي لنظام التشغيل والمجلدات الفرعية به. **المفضلات**. الملفات في مجلد المفضلة القياسي لنظام التشغيل والمجلدات الفرعية به. **سطح المكتب**. الملفات في مجلد سطح المكتب القياسي لنظام التشغيل والمجلدات الفرعية به. **ملفات مؤقتة**. الملفات المؤقتة المتعلقة بعمل التطبيقات المثبتة على الكمبيوتر. على سبيل المثال: تطبيقات Microsoft Office تنشئ ملفات مؤقتة تحتوي على نسخ احتياطية من المستندات. **ملفات Outlook**. الملفات المتعلقة بعمل عميل بريد Outlook: ملفات البيانات (PST)، وملفات بيانات عدم الاتصال (OST)، وملفات دفتر العناوين غير المتصل (OAB)، وملفات دفتر العناوين الشخصي (PAB). • **مجلد مخصص**. يمكنك أيضًا كتابة مسار المجلد يدويًا. عند إضافة مسار مجلد، التزم بالقواعد التالية: استخدم متغير بيئة (على سبيل المثال: `%FOLDER%\UserFolder`). يمكنك استخدام متغير بيئة مرة واحدة وفقط في بداية المسار. لا تستخدم المسارات النسبية. لا تستخدم الحروف `*` أو `?`. لا تستخدم مسارات UNC. ستخدم `;` أو `,` كحرف فاصل. • **الملفات حسب الملحق**. يمكنك تحديد مجموعات الامتدادات من القائمة، مثل مجموعة امتداد الأرشيف. يمكنك كذلك إضافة امتداد الملف بشكل يدوي.
فك التشفير	تعرض علامة التبويب هذه قواعد فك التشفير للملفات المخزنة على محركات الأقراص المحلية.
قواعد التطبيقات	تعرض علامة التبويب جدول يحتوي على قواعد الوصول للملفات المشفرة للتطبيقات وقواعد التشفير للملفات التي تم إنشاؤها أو تعديلها بواسطة تطبيقات فردية.
الحزم المشفرة	متطلبات قوة كلمة المرور لتتوافق مع إنشاء حزم مشفرة.

تشفير محركات الأقراص القابلة للإزالة

يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows لمحطات العمل. لا يتوفر هذا المكون في حالة تثبيت برنامج Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام تشغيل Windows للخوادم.

يدعم Kaspersky Endpoint Security تشفير الملفات في أنظمة ملفات FAT32 وNTFS. في حالة توصيل محرك أقراص قابل للإزالة مزود بنظام ملفات غير مدعوم بجهاز الكمبيوتر، تنتهي مهمة التشفير الخاصة بمحرك الأقراص القابل للإزالة هذا بالخطأ ويقوم Kaspersky Endpoint Security بتعيين الحالة للقراءة فقط إلى محرك الأقراص القابل للإزالة.

لحماية البيانات الموجودة على محركات الأقراص القابلة للإزالة، يمكنك استخدام أنواع التشفير التالية:

- تشفير القرص بالكامل (FDE).

  تشفير محرك الأقراص القابل للإزالة بالكامل، بما في ذلك نظام الملفات.

لا يمكن الوصول إلى البيانات المشفرة خارج شبكة الشركة. من المستحيل أيضًا الوصول إلى البيانات المشفرة داخل شبكة الشركة إذا لم يكن الكمبيوتر متصلاً بـ Kaspersky Security Center (مثل على كمبيوتر "الضيف").

- التشفير على مستوى الملف (FLE).

  تشفير الملفات الموجودة على محرك الأقراص القابل للإزالة فقط. نظام الملفات يبقى دون تغيير.

تشفير الملفات الموجودة على محركات الأقراص القابلة للإزالة يوفر القدرة على الوصول إلى البيانات خارج شبكة الشركة باستخدام وضع خاص يسمى الوضع المحمول .

أثناء التشفير، يقوم Kaspersky Endpoint Security بإنشاء مفتاح رئيسي. يحفظ Kaspersky Endpoint Security المفتاح الرئيسي في المستودعات التالية:

- Kaspersky Security Center.
- كمبيوتر المستخدم.

  يتم تشفير المفتاح الرئيسي باستخدام المفتاح السري للمستخدم.
- محرك أقراص قابل للإزالة.

  يتم تشفير المفتاح الرئيسي بالمفتاح العام لـ Kaspersky Security Center.

بعد اكتمال التشفير، يمكن الوصول إلى البيانات الموجودة على محرك الأقراص القابل للإزالة داخل شبكة الشركة كما لو كانت على محرك أقراص قابل للإزالة من النوع التقليدي بدون تشفير.

الوصول إلى البيانات المشفرة

عند توصيل محرك أقراص قابل للإزالة مع بيانات مشفرة، يقوم Kaspersky Endpoint Security باتخاذ الإجراءات التالية:

1. التحقق من وجود مفتاح رئيسي في التخزين المحلي على كمبيوتر المستخدم.

   إذا تم العثور على المفتاح الرئيسي، يحصل المستخدم على حق الوصول إلى البيانات الموجودة على محرك الأقراص القابل للإزالة.

   إذا لم يتم العثور على المفتاح الرئيسي، يقوم Kaspersky Endpoint Security بتنفيذ الإجراءات التالية:

   a. يرسل طلبًا إلى Kaspersky Security Center.

      بعد استلام الطلب، يرسل Kaspersky Security Center ردًا يحتوي على المفتاح الرئيسي.

   b. يحفظ Kaspersky Endpoint Security المفتاح الرئيسي في التخزين المحلي على كمبيوتر المستخدم للعمليات اللاحقة باستخدام محرك الأقراص القابل للإزالة المشفر.

2. يفك تشفير البيانات.

ميزات خاصة لتشفير محرك الأقراص القابل للإزالة

تشفير محركات الأقراص القابلة للإزالة له المزايا الخاصة التالية:

- يتم تشكيل السياسة المزودة بالإعدادات المعدة مسبقًا لتشفير محرك الأقراص القابل للإزالة لمجموعة محددة من أجهزة الكمبيوتر المدارة. لذلك، فإن نتيجة تطبيق سياسة Kaspersky Security Center المكونة لتشفير / فك تشفير الأقراص القابلة للإزالة تعتمد على الكمبيوتر الذي يتم توصيل محرك الأقراص القابلة للإزالة به.
- لا يقوم Kaspersky Endpoint Security بتشفير/فك تشفير ملفات القراءة فقط والمخزنة على محركات الأقراص القابلة للإزالة.

- يتم دعم أنواع الأجهزة التالية كمحركات أقراص قابلة للإزالة:
  - وسائط البيانات المتصلة عبر ناقل USB
  - محركات الأقراص الصلبة المتصلة عبر نواقل USB وFireWire
  - محركات أقراص SSD المتصلة عبر نواقل USB وFireWire

إعدادات مكون تشفير محركات الأقراص القابلة للإزالة

المعلمة	الوصف
وضع التشفير	**تشفير محرك الأقراص القابل للإزالة بالكامل**. إذا تم تحديد هذا العنصر، عند تطبيق السياسة باستخدام إعدادات التشفير المحددة للأقراص القابلة للإزالة، يقوم Kaspersky Endpoint Security بتشفير محركات الأقراص القابلة للإزالة قطاع بعد قطاع، بما في ذلك أنظمة الملفات عليها. **تشفير جميع الملفات**. إذا تم تحديد هذا العنصر، عند تطبيق السياسة باستخدام إعدادات التشفير المحددة للأقراص القابلة للإزالة، فيقوم Kaspersky Endpoint Security بتشفير جميع الملفات المخزنة على محركات الأقراص القابلة للإزالة. لا يقوم Kaspersky Endpoint Security بإعادة تشفير الملفات التي تم تشفيرها بالفعل. لا يتم تشفير محتويات نظام ملفات محرك أقراص قابل للإزالة، بما في ذلك هيكل المجلدات وأسماء الملفات المشفرة، وتظل متاحة للوصول. **تشفير الملفات الجديدة فقط**. إذا تم تحديد هذا العنصر، عند تطبيق السياسة باستخدام إعدادات التشفير المحددة لمحركات الأقراص القابلة للإزالة، فيقوم Kaspersky Endpoint Security بتشفير الملفات التي تم إضافتها أو تعديلها فقط على محركات الأقراص القابلة للإزالة بعد تطبيق سياسة Kaspersky Security Center. يُعد وضع التشفير هذا مناسبًا عند استخدام محرك قرص قابل للإزالة لأغراض شخصية وأغراض العمل. يتيح لك وضع التشفير هذا عدم تغيير جميع الملفات القديمة وتشفير فقط هذه الملفات التي قام المستخدم بإنشائها على كمبيوتر العمل المثبت عليه Kaspersky Endpoint Security والممكن لوظيفة التشفير. كنتيجة لذلك، يكون الوصول إلى الملفات الشخصية متوفر دائمًا، بغض النظر عما إذا كان Kaspersky Endpoint Security مثبتًا على الكمبيوتر مع تمكين وظائف التشفير أم لا. **فك تشفير محرك الأقراص القابل للإزالة بالكامل**. إذا تم تحديد هذا العنصر، عند تطبيق السياسة باستخدام إعدادات التشفير المحددة لمحركات الأقراص القابلة للإزالة، يقوم Kaspersky Endpoint Security بفك تشفير جميع الملفات المشفرة المخزنة على محركات الأقراص القابلة للإزالة بالإضافة إلى نظم ملفات محركات الأقراص القابلة للإزالة إذا تم تشفيرها سابقًا. **عدم التغيير**. إذا تم تحديد هذا العنصر، فيقوم التطبيق بترك محركات الأقراص على حالتها السابقة عند تطبيق السياسة. إذا كان قد تم تشفير محرك الأقراص، فسيظل مشفرًا. في حالة فك تشفير محرك الأقراص، فسيظل دون تشفير. ويتم تحديد هذا العنصر افتراضيًا.
الوضع المحمول	تقوم خانة الاختيار هذه بتمكين / تعطيل إعداد القرص القابل للإزالة مما يسهل من الوصول إلى الملفات المخزنة على|محرك الأقراص القابل للإزالة هذا على أجهزة الكمبيوتر خارج شبكة الشركة. إذا تم تحديد خانة الاختيار هذه، فيُطالب Kaspersky Endpoint Security المستخدم بتحديد كلمة مرور قبل تشفير ملفات على محرك الأقراص القابل للإزالة عند تطبيق السياسة. يلزم كلمة المرور للوصول إلى الملفات المشفرة على محرك أقراص قابل للإزالة على أجهزة الكمبيوتر خارج شبكة الشركة. يمكنك التحكم في قوة كلمة المرور. الوضع المحمول متوفر لوضع **تشفير جميع الملفات** أو **تشفير الملفات الجديدة فقط**.
تشفير مساحة القرص المستخدمة فقط	تؤدي خانة الاختيار هذه إلى تمكين / تعطيل وضع التشفير حيث يتم تشفير قطاعات القرص الممتلئة فقط. هذا الوضع مستحسن لبرامج التشغيل الجديدة التي لم يتم تعديل بياناتها أو حذفها. إذا تم تحديد خانة الاختيار، يتم تشفير أجزاء محرك القرص الممتلئة بالملفات فقط. ويقوم Kaspersky Endpoint Security تلقائيًا بتشفير البيانات الجديدة بمجرد إضافتها. إذا تم إلغاء تحديد خانة الاختيار، فيتم تشفير محرك القرص بالكامل، بما في ذلك القطاعات المتبقية من الملفات التي تم حذفها وتعديلها سابقًا. القدرة على تشفير المساحة المشغولة فقط غير متوفرة إلا في وضع **تشفير محرك الأقراص القابل للإزالة بالكامل**. بعد بدء التشفير، لن يؤدي تمكين / تعطيل الوظيفة **تشفير مساحة القرص المستخدمة فقط** إلى تغيير هذا الإعداد. يجب تحديد أو إلغاء تحديد خانة الاختيار قبل بدء التشفير.
قواعد مخصصة	يحتوي هذا الجدول على الأجهزة التي تم تحديد قواعد تشفير مخصصة لها. يمكنك إنشاء قواعد التشفير لمحركات الأقراص القابلة للإزالة على حدة بالطرق التالية:

	• إضافة محرك أقراص قابل للإزالة من قائمة الأجهزة الموثوقة للتحكم في الجهاز.
	• إضافة محرك أقراص قابل للإزالة يدويًا:
	  • عن طريق معرف الجهاز (Hardware ID أو HWID)
	  • عن طريق طراز الجهاز: معرف البائع (VID) ومعرف المنتج (PID)

السماح بتشفير محركات الأقراص القابلة للإزالة في وضع عدم الاتصال	إذا تم تحديد خانة الاختيار هذه، فيقوم Kaspersky Endpoint Security بتشفير محركات الأقراص القابلة للإزالة حتى في حالة عدم وجود اتصال بـ Kaspersky Security Center. وفي هذه الحالة، يتم تخزين البيانات المطلوبة لفك تشفير محركات الأقراص القابلة للإزالة في محرك الأقراص الصلبة للكمبيوتر الموصل به محرك الأقراص القابلة للإزالة، ولا يتم نقلها إلى Kaspersky Security Center. إذا تم إلغاء تحديد خانة الاختيار، فلا يقوم Kaspersky Endpoint Security بتشفير محركات الأقراص القابلة للإزالة دون الاتصال بـ Kaspersky Security Center.
إعدادات كلمة مرور التشفير / إدارة الملفات المحمولة	إعدادات قوة كلمة المرور لمدير الملفات المحمولة.

قوالب (تشفير البيانات)

بعد تشفير البيانات، من الممكن أن يقيد Kaspersky Endpoint Security الوصول إلى البيانات على سبيل المثال بسبب تغيير في البنية الأساسية للمؤسسة وتغيير في خادم إدارة Kaspersky Security Center. إذا كان لا يمتلك مستخدم الوصول إلى بيانات مشفرة، فإن المستخدم يمكنه أن يطلب من المسؤول الوصول إلى البيانات. هذا يعني أن المستخدم يحتاج إلى إرسال ملف طلب الوصول إلى المسؤول. يحتاج المستخدم بعدها إلى رفع ملف الرد المستلم من المسؤول إلى Kaspersky Endpoint Security. Kaspersky Endpoint Security يتيح لك طلب الوصول إلى البيانات من المسؤول عبر البريد الإلكتروني (راجع الشكل أدناه).

طلب الوصول إلى البيانات المشفرة

يتوفر قالب للإبلاغ عن نقص في الوصول إلى البيانات المشفرة. لراحة المستخدم، يمكن ملء الحقول التالية:

- **إلى**. أدخل عنوان البريد الإلكتروني لمجموعة الإدارة التي تتمتع بحقوق مزايا تشفير البيانات.
- **الموضوع**. أدخل موضوع البريد الإلكتروني بطلبك للوصول إلى الملفات المشفرة. يمكنك مثلًا أن تضيف وسومًا من أجل تصفية الرسائل.
- **رسالة المستخدم**. قم بتغيير محتويات الرسالة إذا رأيت أن ذلك ضروري. يمكنك استخدام متغيرات في الحصول على البيانات المطلوبة (مثل متغير %USER_NAME%).

الاستثناءات

تُعد المنطقة الموثوقة بمثابة قائمة يتم تكوينها بواسطة مسؤول النظام تضم كائنات وتطبيقات لا يقوم Kaspersky Endpoint Security بمراقبتها عندما يكون نشطًا.

يقوم المسؤول بتكوين المنطقة الموثوقة بشكل فردي، مع الأخذ في الاعتبار الميزات المتوفرة بالكائنات التي تمت معالجتها والتطبيقات التي تم تثبيتها على الكمبيوتر. قد يكون من الضروري تضمين الكائنات والتطبيقات في المنطقة الموثوقة عند قيام Kaspersky Endpoint Security بمنع الوصول إلى كائن أو تطبيق معين، إذا كنت على يقين بأن الكائن أو التطبيق غير ضار. يستطيع المسؤول أيضًا السماح لمستخدم بإنشاء منطقته الموثوقة المحلية لجهاز كمبيوتر معين. وبهذه الطريقة، يستطيع المستخدمون إنشاء قوائم محلية من الاستثناءات والتطبيقات الموثوقة الخاصة بهم بالإضافة إلى المنطقة العامة الموثوقة في سياسة ما.

استثناءات الفحص

استثناءات من الفحص هي عبارة عن مجموعة من الشروط التي يجب تنفيذها حتي لا يقوم Kaspersky Endpoint Security بفحص كائن معين للبحث عن الفيروسات والتهديدات الأخرى.

تجعل استثناءات من الفحص من الممكن استخدام البرامج القانونية التي يمكن استغلالها من قِبل المجرمين للإضرار بالكمبيوتر أو بيانات المستخدم. على الرغم من عدم احتوائها على أية وظائف ضارة، يمكن للدخلاء استغلال مثل هذه التطبيقات. وللحصول على تفاصيل حول البرامج الشرعية التي يمكن أن يستخدمها المجرمون للإضرار بجهاز الكمبيوتر أو البيانات الشخصية لمستخدم ما، يرجى الرجوع إلى موقع ويب موسوعة تكنولوجيا معلومات Kaspersky.

قد يتم منع هذه التطبيقات بواسطة Kaspersky Endpoint Security. لمنع أن يتم حظرهم، يمكنك تكوين استثناءات من الفحص للتطبيقات التي يتم استخدامها. للقيام بذلك، قم بإضافة الاسم أو قناع الاسم المدرج في موسوعة تكنولوجيا المعلومات من Kaspersky إلى المنطقة الموثوقة. على سبيل المثال، تستخدم في معظم الأحيان تطبيق Radmin لإدارة أجهزة الكمبيوتر عن بُعد. يعتبر Kaspersky Endpoint Security هذا النشاط نشاطًا مشكوكًا فيه وربما يقوم بمنعه. لمنع التطبيق من الحظر، قم بإنشاء استثناء من الفحص يحمل الاسم أو قناع الاسم المدرج في موسوعة تكنولوجيا المعلومات من Kaspersky.

إذا كان أحد التطبيقات التي تجمع المعلومات وترسلها لكي تتم معالجتها مثبت على الكمبيوتر لديك، فقد يُصنف Kaspersky Endpoint Security هذا التطبيق كبرمجيات ضارة. ولتجنب حدوث ذلك، يمكنك استثناء التطبيق من الفحص عبر تكوين Kaspersky Endpoint Security على النحو الموضح في هذا المستند.

يمكن استخدام استثناءات من الفحص بواسطة مكونات التطبيقات التالية والمهام التي تم تكوينها بواسطة مسؤول النظام:

- اكتشاف السلوك.
- منع الاستغلال.
- منع اختراق المضيف.
- الحماية من تهديدات الملفات.
- الحماية من تهديدات الويب.
- الحماية من تهديدات البريد.
- مهام فحص البرامج الضارة.

قائمة التطبيقات الموثوقة

قائمة التطبيقات الموثوقة عبارة عن قائمة تطبيقات لا يتم مراقبة نشاط الملف والشبكة (بما في ذلك النشاط الخبيث) والوصول إلى سجل النظام بواسطة Kaspersky Endpoint Security. افتراضيًا، يراقب برنامج Kaspersky Endpoint Security الكائنات التي يتم فتحها أو تشغيلها أو حفظها بواسطة أي عملية تطبيق، ويراقب نشاط كل التطبيقات وحركة الشبكة التي تنشئها هذه التطبيقات. بعد إضافة تطبيق إلى قائمة التطبيقات الموثوقة، يتوقف Kaspersky Endpoint Security عن مراقبة نشاط التطبيقات.

يتمثل الاختلاف بين استثناءات الفحص والتطبيقات الموثوقة أنه بالنسبة للاستثناءات لا يفحص Kaspersky Endpoint Security الملفات، بينما بالنسبة للتطبيقات الموثوقة، فإنه لا يتحكم في العمليات التي بدأت. وإذا أنشأ تطبيق موثوق ملفًا ضارًا في مجلد غير مُضمن في استثناءات الفحص، سيكتشف Kaspersky Endpoint Security الملف ويزيل التهديد. وإذا تمت إضافة المجلد إلى الاستثناءات، سيتخطى Kaspersky Endpoint Security هذا الملف.

على سبيل المثال، إذا اعتبرتَ أن الكائنات التي يتم استخدامها بواسطة تطبيق Microsoft Windows Notepad القياسي آمنة، بمعنى أنك تثق في هذا التطبيق، يمكنك إضافة Microsoft Windows Notepad إلى قائمة التطبيقات الموثوقة بحيث لا تتم مراقبة الكائنات المستخدمة بواسطة هذا التطبيق. وسيؤدي ذلك إلى زيادة أداء الكمبيوتر، وهو أمر مهم خاصة عند استخدام تطبيقات الخادم.

بالإضافة إلى ذلك، قد تكون بعض التطبيقات التي تم تصنيفها بواسطة Kaspersky Endpoint Security كتطبيقات ضارة آمنة في سياق الوظائف المتوفرة بعدد من التطبيقات. على سبيل المثال، يكون اعتراض النص الذي تمت كتابته من لوحة المفاتيح عملية روتينية لتطبيقات تبديل تخطيط لوحة المفاتيح تلقائيًا (مثل Punto Switcher). لتقديم تفاصيل هذه البرامج واستثناء نشاطها من المراقبة، نوصي بإضافة هذه التطبيقات إلى قائمة التطبيقات الموثوقة.

تساعد التطبيقات الموثوقة على تجنب مشكلات التوافق بين Kaspersky Endpoint Security والتطبيقات الأخرى (على سبيل المثال، مشكلة الفحص المزدوج لحركة شبكة الاتصال لجهاز كمبيوتر تابع لجهة خارجية بواسطة Kaspersky Endpoint Security وتطبيق آخر لمكافحة الفيروسات).

في نفس الوقت، يستمر فحص الملف التنفيذي وعملية التطبيق الموثوق للبحث عن الفيروسات والبرمجيات الضارة الأخرى. يمكن استثناء تطبيق بالكامل من فحص Kaspersky Endpoint Security عن طريق استثناءات من الفحص.

إعدادات الاستثناءات

المعلمة	الوصف
أنواع الكائنات المكتشفة	بغض النظر عن تكوين إعدادات التطبيقات، يقوم دائمًا Kaspersky Endpoint Security باكتشاف الفيروسات المتنقلة وفيروسات أحصنة طروادة ومنعها. وقد تؤدي تلك الفيروسات إلى حدوث ضرر بالغ بالكمبيوتر. • **الفيروسات وفيروسات الدودة**

الفئة الفرعية: الفيروسات والفيروسات المتنقلة (الفيروسات_و_الفيروسات المتنقلة)

مستوى التهديد: عالي

تقوم الفيروسات التقليدية والفيروسات المتنقلة بإجراءات غير مسموح بها من قِبل المستخدم. فيمكنها إنشاء نسخ من أنفسها كما تتمكن هذه النسخ من نسخ نفسها.

الفيروس التقليدي

عند اختراق فيروس تقليدي للكمبيوتر، فإنه يصيب أحد الملفات، ويقوم بتفعيل نفسه، وينفذ إجراءات ضارة، ويضيف نُسخًا من نفسه إلى ملفات أخرى.

يتضاعف الفيروس التقليدي فقط على الموارد المحلية للكمبيوتر؛ ولا يمكنه اختراق أجهزة الكمبيوتر الأخرى بمفرده. ويمكنه فقط المرور إلى كمبيوتر آخر إذا قام بإضافة نسخة من نفسه على ملف مُخزن في مجلد مشترك أو مُخزن على قرص مدمج، أو إذا قام المستخدم بإعادة توجيه رسالة بريد إلكتروني وكان بها ملف مرفق مصاب.

يتمكن رمز الفيروس التقليدي من اختراق مناطق مختلفة في أجهزة الكمبيوتر وأنظمة التشغيل والتطبيقات. حسب بيئة التشغيل, يتم تقسيم الفيروسات إلى فيروسات الملفات وفيروسات التمهيد وفيروسات البرامج النصية وفيروسات الماكرو.

تتمكن الفيروسات من إصابة الملفات باستخدام مجموعة متنوعة من الأساليب. الكتابة فوق الملفات بكتابة رمزها الخاص فوق الرمز الخاص بالملف المصاب، ومن ثم تمسح محتواه. ولذا، يتوقف ملف مصاب عن العمل ويتعذر استعادته. التطفلية على تعديل الملفات مع تركها تعمل كليًا أو جزئيًا. الفيروسات المصاحبة بتعديل الملفات، ولكنها تنشئ نُسخ متماثلة. عندما يتم فتح ملف مصاب، يبدأ النسخ المتماثل من هذا الملف (والذي يكون في الواقع عبارة عن فيروس). تتم أيضًا مواجهة الأنواع التالية من الفيروسات: فيروسات الروابط وفيروسات OBJ وفيروسات LIB ورمز المصدر والعديد من الفيروسات الأخرى.

Worm

وكما هو الحال مع الفيروس التقليدي، يتم تفعيل رمز الفيروس المتنقل وينفذ هذا الفيروس إجراءات ضارة بعد اختراقه للكمبيوتر. تم تسمية الفيروسات المتنقلة بهذا الاسم نظرًا لقدرتها على "التسلل" من كمبيوتر إلى آخر ونشر نُسخها عبر العديد من قنوات بيانات دون إذن المستخدم.

أما السمة الرئيسية التي تتيح التفريق بين الأنواع المختلفة من الفيروسات المتنقلة هي الطريقة التي تنتشر بها. يوفر الجدول التالي نظرة عامة على الأنواع المختلفة من الفيروسات المتنقلة، والتي يتم تصنيفها حسب طريقة انتشارها.

طرق انتشار الفيروسات المتنقلة

النوع	الاسم	الوصف
Email-Worm	Email-Worm	تنتشر عبر البريد الإلكتروني. تحتوي رسالة البريد الإلكتروني المصابة على ملف مرفق بنسخة من فيروس متنقل أو تحتوي على ارتباط إلى ملف تم إيداعه على أحد مواقع الويب الذي يحتمل تعرضه للقرصنة أو قد يكون تم إنشاؤه خصيصًا لهذا الغرض. عندما تفتح الملف المرفق، يتم تنشيط فيروس متنقل. وعند النقر على الارتباط، تحميل، ثم فتح الملف، يبدأ فيروس الدودة في اتخاذ إجراءاته الضارة. وبعد ذلك، يستمر في نشر نفسه، بحثًا عن عناوين بريد إلكتروني أخرى وإرسال الرسائل المصابة إليها.
IM-Worm	الفيروسات المتنقلة لعميل المراسلة الفورية	تنتشر عبر عملاء المراسلة الفورية. عادةً مل ترسل الفيروسات المتنقلة رسائل تحتوي على ارتباط إلى ملف به نسخة من الفيروس المتنقل على موقع ويب، مما يعني استخدام قوائم اتصال المستخدم. عندما يقوم المستخدم بتحميل ذلك الملف وفتحه، يتم تنشيط الفيروس المتنقل.
IRC-Worm	الفيروسات المتنقلة في المحادثة	تنتشر من خلال المحادثات عبر الإنترنت، والتي تتمثل في أنظمة الخدمة التي تسمح بالاتصال بالآخرين عبر الإنترنت في الوقت الحقيقي.

	عبر الإنترنت	تقوم الفيروسات المتنقلة هذه بنشر ملف به نسخة منها أو ارتباط إلى هذا الملف في المحادثة عبر الإنترنت. عندما يقوم المستخدم بتحميل ذلك الملف وفتحه، يتم تنشيط الفيروس المتنقل.
Net-Worm	فيروسات الشبكة المتنقلة	تنتشر الفيروسات المتنقلة هذه عبر شبكات الكمبيوتر. وعلى عكس الأنواع الأخرى من الفيروسات المتنقلة، فإن فيروس الشبكة النموذجي المتنقل ينتشر دون تدخل المستخدم. فهو يفحص الشبكة المحلية لأجهزة الكمبيوتر التي تحتوي على برامج بها ثغرات أمنية. وللقيام بذلك، فهو يقوم بإرسال حزمة شبكة اتصال مكوّنة خصيصًا (فيروس تعطيل الأمان) وتحتوي على رمز الفيروس المتنقل أو جزء منه. في حالة وجود كمبيوتر "به ثغرات أمنية" على الشبكة، فإنه يتلقى حزمة الشبكة هذه. ويتم تنشيط الفيروس المتنقل بمجرد اختراقه التام للكمبيوتر.
P2P-Worm	فيروسات شبكة مشاركة الملفات المتنقلة	تنتشر عبر شبكات مشاركة الملفات من نظير إلى نظير. للتسلل إلى شبكة P2P، يقوم الفيروس المتنقل بنسخ نفسه في مجلد مشاركة ملفات يوجد عادةً في كمبيوتر المستخدم. تعرض شبكة P2P معلومات حول هذا الملف لهذا بطريقة تجعل المستخدم قد "يجد" ملف مصاب على الشبكة مثل أي ملف آخر، ثم يقوم بتنزيله وفتحه. أما الفيروسات المتنقلة الأكثر تعقيدًا فتقوم بمحاكاة بروتوكول شبكة P2P معينة. وتوفر هذه الفيروسات استجابة إيجابية لاستعلامات البحث وعرض نُسخ من نفسها للتنزيل.
Worm	أنواع أخرى من الفيروسات المتنقلة	تتضمن الأنواع الأخرى من الفيروسات المتنقلة: • الفيروسات المتنقلة تنشر نُسخًا من نفسها عبر موارد الشبكة. باستخدام وظائف نظام التشغيل، تقوم بفحص مجلدات الشبكة المتاحة، والاتصال بأجهزة الكمبيوتر على الإنترنت، ومحاولة الحصول على الوصول الكامل إلى محركات الأقراص الخاصة بها. على عكس الأنواع الموضحة مسبقًا من الفيروسات المتنقلة، لا تقوم الأنواع الأخرى من الفيروسات المتنقلة بتفعيل نفسها، ولكن يتم تنشيطها عندما يقوم المستخدم بفتح ملف يحتوي على نسخة منها. • الفيروسات المتنقلة التي لا تستخدم أي من الوسائل المذكورة في الجدول السابق للانتشار (على سبيل المثال، الفيروسات التي تنتشر عبر الهواتف المحمولة).

- **فيروسات حصان طروادة (بما في ذلك برامج طلب الفدية)**

الفئة الفرعية: فيروسات حصان طروادة

مستوى التهديد: عالي

على عكس الفيروسات التقليدية، لا تقوم برامج حصان طروادة بالنسخ المتماثل لنفسها. على سبيل المثال، فإنها تخترق الكمبيوتر عبر البريد الإلكتروني أو المستعرض عند زيارة المستخدم لصفحة ويب مصابة. يتم بدء برامج حصان طروادة بعد تدخل من المستخدم. تبدأ في اتخاذ إجراءاتها الضارة مباشرة بعد أن يبدأ تشغيلها.

وتعمل برامج حصان طروادة الأخرى بشكل مختلف على أجهزة الكمبيوتر المصابة. تتضمن الوظائف الأساسية لبرامج حصان طروادة منع المعلومات أو تعديلها أو تدميرها، وتعطيل أجهزة الكمبيوتر أو الشبكات. يمكن أيضًا لبرامج حصان طروادة استلام الملفات أو إرسالها، وتشغيلها، وعرض الرسائل على الشاشة، وطلب صفحات الويب، وتنزيل البرامج وتثبيتها، وإعادة تشغيل جهاز الكمبيوتر.

غالبًا ما يستخدم القراصنة "مجموعات" من برامج حصان طروادة.

يوضح الجدول التالي أنواع سلوكيات برامج حصان طروادة.

أنواع سلوكيات برامج حصان طروادة على الكمبيوتر المصاب

النوع	الاسم	الوصف
Trojan-ArcBomb	برامج حصان طروادة – "قنابل الأرشيف"	عند فك حزم الأرشيفات، يزداد حجمها بشكل يؤثر على تشغيل الكمبيوتر. عندما يحاول المستخدم فك حزمة الأرشيف، قد يبدأ الكمبيوتر في العمل ببطء أو يتجمد؛ وقد يتم ملء القرص الثابت ببيانات "فارغة". وتمثل "قنابل الأرشيف" خطورة بالنسبة لخوادم البريد الإلكتروني والملفات على وجه الخصوص. إذا كان الخادم يستخدم نظام تلقائي لمعالجة البيانات الواردة، فإن "قنابل الأرشيف" قد تؤدي إلى توقف عمل الخادم.
Backdoor	برامج حصان طروادة للإدارة عن بُعد	تعتبر أخطر نوع من بين كل أنواع برامج حصان طروادة. ومن حيث وظائفها، فإنها تشبه تطبيقات الإدارة عن بُعد المُثبتة على أجهزة الكمبيوتر. تقوم تلك البرامج بتثبيت نفسها على الكمبيوتر دون أن يلاحظها المستخدم، مما يتيح للدخلاء أن يديروا الكمبيوتر عن بُعد.
Trojan	أحصنة طروادة	تتضمن التطبيقات الضارة التالية: • **برامج حصان طروادة التقليدية**. تقوم تلك البرامج فقط بأداء الوظائف الأساسية لبرامج حصان طروادة: منع المعلومات أو تعديلها أو تدميرها، وتعطيل أجهزة الكمبيوتر أو الشبكات. ولا تتضمن أي ميزات متقدمة على عكس الأنواع الأخرى من برامج حصان طروادة الموضحة في الجدول. • **برامج حصان طروادة متعددة الاستخدامات**. لدى هذه البرامج ميزات متقدمة مطابقة للعديد من أنواع برامج حصان طروادة.
Trojan-Ransom	برامج حصان طروادة للفدية	تقوم هذه البرامج بأخذ معلومات المستخدم "كرهينة" وتقوم بتعديلها أو منعها، أو التأثير على تشغيل الكمبيوتر لكي يفقد المستخدم القدرة على استخدام المعلومات. يطلب الدخيل فدية من المستخدم، مع التعهد بإرسال تطبيق يستعيد أداء الكمبيوتر والبيانات المخزنة عليه.
Trojan-Clicker	الأشخاص الذين ينقرون فوق برامج حصان طروادة	تصل إلى صفحات الويب من كمبيوتر المستخدم، إما بإرسال أوامر إلى المستعرض من تلقاء نفسها أو بتغيير عناوين الويب المحددة في ملفات النظام. باستخدام هذه البرامج، يقوم الدخلاء بهجمات على الشبكة وزيادة زيارات مواقع الويب، مما يزيد من عدد عرض الشعارات الإعلانية.
Trojan-Downloader	برامج حصان طروادة للتنزيل	تصل هذه البرامج إلى صفحة ويب الدخيل، وتقوم بتنزيل تطبيقات ضارة أخرى منها، وتثبيتها على كمبيوتر المستخدم. وقد تتضمن هذه البرامج اسم ملف التطبيق الخبيث لتنزيله أو استلامه من صفحة الويب التي يتم الوصول إليها.

Trojan-Dropper	برامج حصان طروادة للإسقاط	تتضمن برامج حصان طروادة أخرى تقوم بتثبيتها على القرص الثابت. قد يستخدم الدخلاء برامج حصان طروادة للإسقاط من أجل الأهداف التالية: • تثبيت برنامج ضار دور أن يلاحظه المستخدم: لا تعرض تطبيق حصان طروادة للإسقاط أية رسائل، أو أنها تعرض رسائل مزيفة تخبرك على سبيل المثال بوجود خطأ في أرشيف أو في إصدار غير متوافق مع نظام التشغيل. • حماية تطبيق خبيث معروف آخر من الاكتشاف: ليس بإمكان جميع برامج مكافحة الفيروسات اكتشاف تطبيق خبيث موجود داخل برامج حصان طروادة للإسقاط.
Trojan-Notifier	برامج حصان طروادة للإخطار	تقوم هذه البرامج بإخطار الدخيل بإمكانية الوصول إلى الكمبيوتر المصاب، وترسل إليه معلومات عن الكمبيوتر: عنوان IP أو عدد المنافذ المفتوحة أو عنوان البريد الإلكتروني. وهي تتصل بالدخيل عبر البريد الإلكتروني أو عن طريق FTP أو عن طريق الوصول إلى صفحة الويب الخاصة بالدخيل أو بأي طريقة أخرى. عادةً ما يتم استخدام برامج حصان طروادة للإخطار في مجموعات تتكون من برامج حصان طروادة متعددة. وهي تخطر الدخيل بنجاح تثبيت برامج حصان طروادة الأخرى على كمبيوتر المستخدم.
Trojan-Proxy	برامج حصان طروادة لخوادم الوكيل	تسمح للدخيل الوصول إلى صفحات الويب بشكل مجهول من خلال استخدام كمبيوتر المستخدم؛ وعادةً ما يتم استخدامها لإرسال رسائل بريد إلكتروني غير مرغوب فيها.
Trojan-PSW	برمجيات سرقة كلمة المرور	تعتبر برمجيات سرقة كلمة المرور نوعًا من برامج حصان طروادة يسرق حسابات المستخدم، مثل بيانات تسجيل البرامج. تعثر برامج حصان طروادة هذه على بيانات الخصوصية في ملفات النظام وفي السجل وإرسالها إلى "المهاجم" عن طريق البريد الإلكتروني، أو عن طريق FTP أو عن طريق الوصول إلى صفحة ويب الدخيل، أو بأي طريقة أخرى. يتم تصنيف بعض فيروسات حصان طروادة هذه إلى أنواع منفصلة موضحة في هذا الجدول. إنها برامج حصان طروادة التي تسرق حسابات البنوك (Trojan-Banker)، وتسرق البيانات من مستخدمي عملاء المراسلة الفورية (Trojan-IM) (IM)، وتسرق المعلومات من مستخدمي ألعاب الإنترنت (Trojan-GameThief).
Trojan-Spy	برامج حصان طروادة للتجسس	تتجسس هذه البرامج على المستخدم بجمع معلومات عن الإجراءات التي يقوم بها أثناء العمل على الكمبيوتر. ويمكن أن تعترض البيانات التي يدخلها المستخدم عن طريق لوحة المفاتيح أو تأخذ لقطات شاشة أو تجمع قوائم بالتطبيقات النشطة. وبعد استلامها للمعلومات، تقوم هذه البرامج بإرسالها إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة ويب الدخيل أو باستخدام طريقة أخرى.
Trojan-DDoS	برامج حصان طروادة للهجوم على الشبكة	تقوم بإرسال العديد من الطلبات من جهاز كمبيوتر المستخدم إلى خادم بعيد. ويفتقر الخادم إلى الموارد اللازمة لمعالجة جميع الطلبات، بحيث يتوقف عن العمل (رفض الخدمة أو DoS ببساطة). غالبًا ما يصيب القراصنة العديد من أجهزة الكمبيوتر بهذه البرامج بحيث يمكنهم استخدامها للهجوم على خادم واحد في نفس الوقت. تقوم برامج رفض الخدمة (DoS) بارتكاب هجوم من جهاز كمبيوتر واحد بمعرفة المستخدم. وتقوم برامج رفض الخدمة الموزعة (DDoS) بارتكاب هجمات موزعة من العديد من أجهزة الكمبيوتر دون أن تتم ملاحظتها من جانب مستخدم جهاز الكمبيوتر المصاب.
Trojan-IM	برامج حصان طروادة التي تسرق معلومات من مستخدمي عملاء	تسرق أرقام الحسابات وكلمات المرور الخاصة بمستخدمي عملاء المراسلة الفورية (IM). وتقوم هذه البرامج بنقل البيانات إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة ويب الدخيل أو باستخدام طريقة أخرى.

	المراسلة الفورية (IM)	
Rootkit	فيروسات الجذر	تقوم هذه الفيروسات بحجب التطبيقات الضارة الأخرى ونشاطها، وبالتالي تطيل من استمرار التطبيق في نظام التشغيل. ويمكن أيضًا أن تقوم بإلغاء ملفات أو عمليات في ذاكرة جهاز كمبيوتر مصاب أو مفاتيح تسجيل تقوم بتشغيل التطبيقات الضارة. كما يمكن أن تقوم فيروسات الجذر بحجب تبادل البيانات بين التطبيقات في جهاز كمبيوتر المستخدم وأجهزة الكمبيوتر الأخرى على شبكة الاتصال.
Trojan-SMS	برامج حصان طروادة في شكل رسائل SMS	تصيب هذه البرامج الهواتف الخلوية وتقوم بإرسال رسائل SMS إلى أرقام الهواتف ذات الأسعار العالية.
Trojan-GameThief	برامج حصان طروادة التي تسرق معلومات من مستخدمي الألعاب عبر الإنترنت	تسرق هذه البرامج بيانات اعتماد الحساب من مستخدمي الألعاب عبر الإنترنت، ثم تقوم بعد ذلك بإرسال البيانات إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة الويب الخاصة بالدخيل أو باستخدام طريقة أخرى.
Trojan-Banker	برامج حصان طروادة التي تسرق حسابات البنوك	تقوم هذه البرامج بسرقة بيانات حسابات البنوك أو بيانات الأنظمة المالية الإلكترونية ثم بعد ذلك ترسل البيانات إلى المتسلل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة الويب الخاصة بالمتسلل أو باستخدام طريقة أخرى.
Trojan-Mailfinder	برامج حصان طروادة التي تجمع عناوين البريد الإلكتروني	تقوم هذه البرامج بجمع عناوين البريد الإلكتروني المخزنة على جهاز كمبيوتر وبإرسالها إلى الدخيل عن طريق البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى صفحة ويب الدخيل أو باستخدام طريقة أخرى. ويمكن أن يقوم الدخلاء بإرسال بريد إلكتروني غير مرغوب فيه إلى العناوين التي قاوموا بجمعها.

- أدوات خبيثة

الفئة الفرعية: الأدوات الخبيثة

مستوي الخطر: متوسط

على عكس الأنواع الأخرى من البرمجيات الضارة، لا تقوم الأدوات الخبيثة بإجراءاتها فور بدء تشغيلها. فيمكن تخزينها بأمان وبدء تشغلها على كمبيوتر المستخدم. وغالبًا ما يستخدم الدخلاء ميزات هذه البرامج لإنشاء فيروسات وفيروسات دودة وبرامج حصان طروادة أو القيام بهجمات الشبكة على الخوادم البعيدة أو قرصنة أجهزة كمبيوتر أو القيام بأنشطة ضارة أخرى.

يتم تصنيف مختلف ميزات الأدوات الخبيثة وفقًا للأنواع الوارد وصفها في الجدول التالي.

خصائص الأدوات الخبيثة

النوع	الاسم	الوصف
Constructor	دوال إنشائية	تسمح بإنشاء فيروسات وفيروسات دودة وبرامج حصان طروادة جديدة. يتباهى بعض منشئ الفيروسات بأن لديهم واجهة نوافذ قياسية يمكن للمستخدم أن يقوم فيها بتحديد نوع التطبيق الخبيث المطلوب إنشائه وطريقة مقاومة المصححين وغير ذلك من الخصائص.
Dos	هجمات شبكة الاتصال	تقوم بإرسال العديد من الطلبات من جهاز كمبيوتر المستخدم إلى خادم بعيد. ويفتقر الخادم إلى الموارد اللازمة لمعالجة جميع الطلبات، بحيث يتوقف عن العمل (رفض الخدمة أو DoS ببساطة).
Exploit	فيروسات معطلة للأمان	فيروس الاستغلال عبارة عن مجموعة من البيانات أو رمز برنامج يستخدم ثغرات أمنية بالتطبيق الذي تتم معالجته فيه، لأجل القيام بإجراء خبيث على الكمبيوتر. فعلى سبيل المثال، يمكن للفيروس المعطل للأمان كتابة أو قراءة الملفات أو طلب صفحات ويب "مصابة". تستخدم الفيروسات المعطلة للأمان المختلفة ثغرات أمنية في خدمات شبكة اتصال أو تطبيقات مختلفة. ويتم إرسال الفيروسات المعطلة للأمان مخفيةً على هيئة حزمة شبكة اتصال إلى أجهزة كمبيوتر متعددة عبر الشبكة، بحثًا عن أجهزة كمبيوتر بها خدمات شبكة اتصال قابلة للاختراق. ويستخدم الفيروس المعطل للأمان الموجود في ملف DOC ثغرات أمنية لمحرر نصوص. وقد يبدأ هذا الفيروس بتنفيذ إجراءات مبرمجة من قبل أحد القراصنة عند قيام المستخدم بفتح ملف مصاب. ويبحث الفيروس المعطل للأمان المضمن في رسالة بريد إلكتروني عن ثغرات أمنية في أي من عملاء البريد الإلكتروني. وقد يبدأ بتنفيذ إجراء خبيث بمجرد فتح المستخدم للرسالة المصابة في عميل البريد الإلكتروني هذا. تنتشر فيروسات دودة الشبكة عبر الشبكات باستخدام الفيروسات المعطلة للأمان. ففيروسات الاستغلال عبارة عن حزم شبكة تقوم بتعطيل أجهزة الكمبيوتر.
FileCryptor	مشفرون	تقوم بترميز التطبيقات الضارة الأخرى لإخفائها من تطبيق مكافحة الفيروسات.
Flooder	برامج "لتلويث" شبكات الاتصال	تقوم بإرسال العديد من الرسائل عبر قنوات شبكة الاتصال. ويتضمن هذا النوع من الأدوات، على سبيل المثال، برامج تلوث المحادثات عبر الإنترنت. لا تتضمن الأدوات التي من هذا النوع من الفيروسات أي برامج "تلوث" القنوات المستخدمة بواسطة البريد الإلكتروني وعملاء المراسلة الفورية (IM) وأنظمة الاتصالات المتنقلة. ويتم تمييز هذه البرامج على أنها أنواع مستقلة وارد وصفها في هذا الجدول (فيروسات فيضان البريد الإلكتروني وفيروس إرسال كميات ضخمة من المراسلات الفورية المراسلات الفورية وفيروسات فيضان رسائل SMS).
HackTool	أدوات قرصنة	تتيح التسلل إلى الكمبيوتر الذي يتم تثبيتها عليه، أو مهاجمة كمبيوتر آخر (على سبيل المثال، عن طريق إضافة حسابات جديدة بالنظام دون إذن المستخدم، أو عن طريق مسح سجلات النظام لإخفاء ما يدل على وجودها في نظام التشغيل). ويتضمن هذا النوع من الأدوات بعض برامج مراقبة الشبكة التي تتميز بوظائف ضارة، منها على سبيل المثال اعتراض كلمات المرور.

		وبرامج مراقبة الشبكة هي عبارة عن برامج تسمح بإمكانية عرض حركة مرور الشبكة.
Hoax	برامج خداعية	تخطر المستخدم برسائل تشبه الفيروسات: وقد "تكتشف فيروسًا" في ملف غير مصاب وتخطر المستخدم بأنه تم تنسيق القرص على الرغم من عدم حدوث ذلك في الواقع.
Spoofer	أدوات محاكاة	ترسل رسائل وطلبات شبكة اتصال بعنوان مزيف للمرسل. ويستخدم الدخلاء أدوات من نوع محاكي المستخدم المصرح له لإظهار أنفسهم كمرسلين حقيقيين للرسائل على سبيل المثال.
VirTool	أدوات تعدل التطبيقات الضارة	وهي تسمح بتعديل البرمجيات الضارة الأخرى، مع إخفائها من تطبيقات مكافحة الفيروسات.
Email-Flooder	برامج "تلوث" عناوين البريد الإلكتروني	ترسل العديد من الرسائل إلى عناوين بريد إلكتروني مختلفة، وبالتالي يتم "تلويثها". ويمنع وجود قدر كبير من الرسائل الواردة المستخدمين من عرض الرسائل المفيدة في صناديق الوارد الخاصة بهم.
IM-Flooder	برامج تؤدي إلى تلوث حركة عملاء المراسلة الفورية	وهي تغمر مستخدمي عملاء المراسلة الفورية (IM) بالرسائل. ويمنع وجود قدر كبير من الرسائل المستخدمين من عرض الرسائل الواردة المفيدة.
SMS-Flooder	برامج "تلوث" الحركة برسائل SMS	ترسل العديد من رسائل SMS إلى الهواتف الخلوية.

- **برمجيات إعلانية**

الفئة الفرعية: البرامج الإعلانية (Adware)؛

مستوى التهديد: متوسط

البرمجيات الإعلانية هي برمجيات تعرض معلومات إعلانية للمستخدم. وتقوم البرامج الإعلانية بعرض شعارات إعلانية في واجهات برامج أخرى وتعيد توجيه استعلامات البحث إلى مواقع ويب إعلانية. وتقوم بعضها بجمع معلومات تسويقية عن المستخدم وإرسالها إلى المطور: وقد تتضمن هذه المعلومات أسماء مواقع الويب التي تمت زيارتها من جانب المستخدم أو محتوى استعلامات البحث الخاصة به. وعلى عكس برامج حصان طروادة-Spy، ترسل البرامج الإعلانية هذه المعلومات إلى المطور بإذن المستخدم.

- **برامج الاتصال التلقائي**

الفئة الفرعية: البرامج القانونية التي يمكن أن يستخدمها المجرمون لإتلاف الكمبيوتر أو بياناتك الشخصية.

مستوى الخطر: متوسط

معظم هذه التطبيقات مفيدة، ولذلك يقوم الكثير من المستخدمين بتشغيلها. تتضمن هذه التطبيقات عملاء المحادثة عبر الإنترنت (IRC)، وبرامج الاتصال التلقائي، وبرامج تنزيل الملفات، وبرامج مراقبة أنشطة نظام الكمبيوتر، والأدوات المساعدة لكلمات المرور، وخوادم الإنترنت لشبكات FTP وHTTP وTelnet.

ومع ذلك، إذا تمكن الدخلاء من الوصول إلى هذه البرامج أو إذا زرعوها على كمبيوتر المستخدم، قد يتم استخدام هذه ميزات التطبيق لانتهاك الأمان.

تختلف هذه التطبيقات حسب الوظيفة؛ ويتم توضيح أنواعها في الجدول التالي.

النوع	الاسم	الوصف
Client-IRC	عملاء المحادثة عبر الإنترنت	يقوم المستخدمين بتثبيت هذه البرامج للتحدث مع آخرين عبر الإنترنت. ويستخدمها الدخلاء لنشر البرمجيات الضارة.
Dialer	برامج الاتصال التلقائي	يمكنها إجراء اتصالات عبر الهاتف عن طريق مودم في الوضع "مخفي".
Downloader	برامج التنزيل	يتمكنون من تحميل الملفات من صفحات الإنترنت في الوضع "مخفي".
Monitor	برامج للمراقبة	تسمح تلك البرامج بنشاط المراقبة على جهاز الكمبيوتر الذي تم تثبيتها عليه (مما يؤدي إلى معرفة التطبيقات قيد التشغيل وكيف تتبادل البيانات مع التطبيقات المثبتة على أجهزة الكمبيوتر الأخرى).
PSWTool	أدوات استعادة كلمات المرور	تسمح بعرض واستعادة كلمات المرور المنسية. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض.
RemoteAdmin	برامج الإدارة عن بعد	يتم استخدامها على نطاق واسع من قبل مديري النظام. وتسمح هذه البرامج بالوصول إلى واجهة كمبيوتر بعيد لمراقبته وإدارته. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض: لمراقبة أجهزة الكمبيوتر البعيدة وإدارتها. تختلف برامج الإدارة عن بُعد القانونية عن برامج حصان طروادة من نوع الباب الخلفي للإدارة عن بُعد. تتوفر لدى برامج حصان طروادة القدرة على اختراق نظام التشغيل بشكل مستقل وتثبيت نفسها؛ بينما لا يمكن للبرامج القانونية القيام بذلك.
Server-FTP	خوادم FTP	تعمل كخوادم FTP. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول FTP.
Server-Proxy	خوادم الوكيل	تعمل كخوادم وكيلة. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
Server-Telnet	خوادم Telnet	تعمل كخوادم Telnet. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول Telnet.
Server-Web	خوادم الويب	تعمل كخوادم ويب. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول HTTP.
RiskTool	أدوات للعمل على	تزود المستخدم بخيارات إضافية أثناء العمل على الكمبيوتر الخاص به. وتسمح هذه الأدوات للمستخدم بإخفاء الملفات أو نوافذ التطبيقات قيد التشغيل وإنهاء العمليات قيد التشغيل.

	كمبيوتر محلي	
NetTool	أداوت شبكة الاتصال	تزود المستخدم بخيارات إضافية أثناء العمل على أجهزة كمبيوتر أخرى على الشبكة. وتسمح هذه الأدوات بإعادة تشغيلها واكتشاف المنافذ المفتوحة وبدء تشغيل التطبيق المثبتة على أجهزة الكمبيوتر.
Client-P2P	عملاء شبكة اتصال النظراء P2P	تسمح بالعمل على شبكات الاتصال من نظير إلى نظير. ويمكن أن يستخدمها الدخلاء لنشر البرمجيات الضارة.
Client-SMTP	عملاء SMTP	يرسلون رسائل بريد إلكترونية دون علم المستخدم. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
WebToolbar	أشرطة أدوات الويب	تضيف أشرطة أدوات إلى واجهات التطبيقات الأخرى لاستخدام محركات البحث.
FraudTool	برامج زائفة	تظهر نفسها في هيئة برامج أخرى. على سبيل المثال، توجد برامج زائفة لحماية ضد الفيروسات تعرض رسائل حول اكتشاف البرمجيات الضارة. برغم ذلك، فإنها لا تكتشف في الواقع أي شيء أو تنظفه.

- **اكتشاف برامج قانونية أخرى يمكن أن يستخدمها المجرمون لإتلاف جهازك أو بياناتك الشخصية**

الفئة الفرعية: البرامج القانونية التي يمكن أن يستخدمها المجرمون لإتلاف الكمبيوتر أو بياناتك الشخصية.

مستوى الخطر: متوسط

معظم هذه التطبيقات مفيدة، ولذلك يقوم الكثير من المستخدمين بتشغيلها. تتضمن هذه التطبيقات عملاء المحادثة عبر الإنترنت (IRC)، وبرامج الاتصال التلقائي، وبرامج تنزيل الملفات، وبرامج مراقبة أنشطة نظام الكمبيوتر، والأدوات المساعدة لكلمات المرور، وخوادم الإنترنت لشبكات FTP وHTTP وTelnet.

ومع ذلك، إذا تمكن الدخلاء من الوصول إلى هذه البرامج أو إذا زرعوها على كمبيوتر المستخدم، قد يتم استخدام هذه ميزات التطبيق لانتهاك الأمان.

تختلف هذه التطبيقات حسب الوظيفة؛ ويتم توضيح أنواعها في الجدول التالي.

النوع	الاسم	الوصف
Client-IRC	عملاء المحادثة عبر الإنترنت	يقوم المستخدمين بتثبيت هذه البرامج للتحدث مع آخرين عبر الإنترنت. ويستخدمها الدخلاء لنشر البرمجيات الضارة.
Dialer	برامج الاتصال التلقائي	يمكنها إجراء اتصالات عبر الهاتف عن طريق مودم في الوضع "مخفي".
Downloader	برامج التنزيل	يتمكنون من تحميل الملفات من صفحات الإنترنت في الوضع "مخفي".
Monitor	برامج للمراقبة	تسمح تلك البرامج بنشاط المراقبة على جهاز الكمبيوتر الذي تم تثبيتها عليه (مما يؤدي إلى معرفة التطبيقات قيد التشغيل وكيف تتبادل البيانات مع التطبيقات المثبتة على أجهزة الكمبيوتر الأخرى).
PSWTool	أدوات استعادة كلمات المرور	تسمح بعرض واستعادة كلمات المرور المنسية. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض.
RemoteAdmin	برامج الإدارة عن بعد	يتم استخدامها على نطاق واسع من قبل مديري النظام. وتسمح هذه البرامج بالوصول إلى واجهة كمبيوتر بعيد لمراقبته وإدارته. ويزرعها الدخلاء سرًا على أجهزة الكمبيوتر الخاصة بالمستخدمين لنفس الغرض: لمراقبة أجهزة الكمبيوتر البعيدة وإدارتها. تختلف برامج الإدارة عن بُعد القانونية عن برامج حصان طروادة من نوع الباب الخلفي للإدارة عن بُعد. تتوفر لدى برامج حصان طروادة القدرة على اختراق نظام التشغيل بشكل مستقل وتثبيت نفسها؛ بينما لا يمكن للبرامج القانونية القيام بذلك.
Server-FTP	خوادم FTP	تعمل كخوادم FTP. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول FTP.
Server-Proxy	خوادم الوكيل	تعمل كخوادم وكيلة. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
Server-Telnet	خوادم Telnet	تعمل كخوادم Telnet. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول Telnet.
Server-Web	خوادم الويب	تعمل كخوادم ويب. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لفتح الوصول عن بُعد إليه عن طريق بروتوكول HTTP.
RiskTool	أدوات للعمل على	تزود المستخدم بخيارات إضافية أثناء العمل على الكمبيوتر الخاص به. وتسمح هذه الأدوات للمستخدم بإخفاء الملفات أو نوافذ التطبيقات قيد التشغيل وإنهاء العمليات قيد التشغيل.

	كمبيوتر محلي	
NetTool	أداوت شبكة الاتصال	تزود المستخدم بخيارات إضافية أثناء العمل على أجهزة كمبيوتر أخرى على الشبكة. وتسمح هذه الأدوات بإعادة تشغيلها واكتشاف المنافذ المفتوحة وبدء تشغيل التطبيق المثبتة على أجهزة الكمبيوتر.
Client-P2P	عملاء شبكة اتصال النظراء P2P	تسمح بالعمل على شبكات الاتصال من نظير إلى نظير. ويمكن أن يستخدمها الدخلاء لنشر البرمجيات الضارة.
Client-SMTP	عملاء SMTP	يرسلون رسائل بريد إلكترونية دون علم المستخدم. ويقوم الدخلاء بزرعها على كمبيوتر المستخدم لإرسال بريد إلكتروني غير مرغوب باسم المستخدم.
WebToolbar	أشرطة أدوات الويب	تضيف أشرطة أدوات إلى واجهات التطبيقات الأخرى لاستخدام محركات البحث.
FraudTool	برامج زائفة	تظهر نفسها في هيئة برامج أخرى. على سبيل المثال، توجد برامج زائفة لحماية ضد الفيروسات تعرض رسائل حول اكتشاف البرمجيات الضارة. برغم ذلك، فإنها لا تكتشف في الواقع أي شيء أو تنظفه.

- **كائنات مضغوطة قد يُستخدم الضغط الخاص بها لحماية التعليمات البرمجية الخبيثة**

يقوم Kaspersky Endpoint Security بمسح الكائنات المضغوطة والوحدة النمطية لفك الحزمة داخل الأرشيفات ذاتية الاستخراج (SFX).

لإخفاء البرامج الخطرة من تطبيقات مكافحة الفيروسات، يقوم الدخلاء بأرشفتها باستخدام منشئي حزم خاصة أو إنشاء الملفات متعددة الحزم.

حدد محللو الفيروسات في Kaspersky برامج الحزم الأكثر شيوعًا بين القراصنة.

إذا اكتشف Kaspersky Endpoint Security وجود أحد برامج الحزم من هذا النوع في ملف، فيكون من الأرجح أن يحتوي هذا الملف على تطبيق ضار أو تطبيق ربما يتم استخدامه بواسطة المجرمين للإضرار بالكمبيوتر أو بياناتك الشخصية.

ينتقي Kaspersky Endpoint Security الأنواع التالية من البرامج:

- الملفات المضغوطة التي قد تسبب ضررًا – يتم استخدامها لحزم البرمجيات الضارة مثل الفيروسات التقليدية والفيروسات المتنقلة وبرامج حصان طروادة.
- الملفات متعددة الحزم (مستوى التهديد المتوسط) – تم حزم الكائن ثلاث مرات بواسطة واحد أو أكثر من برامج الحزم.

- **الكائنات متعددة الضغط**

يقوم Kaspersky Endpoint Security بمسح الكائنات المضغوطة والوحدة النمطية لفك الحزمة داخل الأرشيفات ذاتية الاستخراج (SFX).

لإخفاء البرامج الخطرة من تطبيقات مكافحة الفيروسات، يقوم الدخلاء بأرشفتها باستخدام منشئي حزم خاصة أو إنشاء الملفات متعددة الحزم.

حدد محللو الفيروسات في Kaspersky برامج الحزم الأكثر شيوعًا بين القراصنة.

إذا اكتشف Kaspersky Endpoint Security وجود أحد برامج الحزم من هذا النوع في ملف، فيكون من الأرجح أن يحتوي هذا الملف على تطبيق ضار أو تطبيق ربما يتم استخدامه بواسطة المجرمين للإضرار بالكمبيوتر أو بياناتك الشخصية.

ينتقي Kaspersky Endpoint Security الأنواع التالية من البرامج:

- الملفات المضغوطة التي قد تسبب ضررًا – يتم استخدامها لحزم البرمجيات الضارة مثل الفيروسات التقليدية والفيروسات المتنقلة وبرامج حصان طروادة.
- الملفات متعددة الحزم (مستوى التهديد المتوسط) – تم حزم الكائن ثلاث مرات بواسطة واحد أو أكثر من برامج الحزم.

الاستثناءات

يحتوي هذا الجدول على معلومات حول استثناءات من الفحص.

يمكنك استبعاد الكائنات من عمليات الفحص باستخدام الطرق التالية:

- تحديد المسار إلى الملف أو المجلد.
- أدخل تجزئة الكائن.
- استخدم الأقنعة:

- حرف `*` (العلامة النجمية)، الذي يحل محل أي مجموعة من الأحرف، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\*\*.txt` كل المسارات إلى الملفات ذات الامتداد TXT الموجود في المجلدات على محرك الأقراص :C، ولكنه ليس موجودًا في المجلدات الفرعية.
- تحل علامتان نجميتان متتاليتان `*` محل أي مجموعة من الأحرف (بما في ذلك مجموعة فارغة) في اسم الملف أو المجلد، بما في ذلك حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سوف يتضمن القناع `C:\Folder\**\*.txt` كل المسارات إلى الملفات ذات الملحق TXT الموجودة في المجلدات المتداخلة في `Folder`، باستثناء المجلد `Folder` نفسه. يجب أن يتضمن القناع مستوى تداخل واحد على الأقل. القناع `C:\**\*.txt` هو قناع غير صالح.
- حرف `?` (علامة الاستفهام)، الذي يحل محل أي حرف فردي، باستثناء حرفي `\` و `/` (محددات لأسماء الملفات والمجلدات في مسارات الملفات والمجلدات). على سبيل المثال، سيتضمن القناع `C:\Folder\???.txt` مسارات إلى جميع الملفات الموجودة في المجلد المُسمى `Folder` الذي يحتوي على الامتداد TXT واسم يتكون من ثلاثة أحرف.

يمكنك استخدام الأقنعة في أي مكان في مسار الملف أو المجلد. على سبيل المثال، إذا كنت تريد أن يتضمن نطاق الفحص مجلد Downloads لجميع حسابات المستخدمين على الكمبيوتر، فأدخل القناع `C:\Users\*\Downloads\`.

يدعم Kaspersky Endpoint Security متغيرات البيئة

لا يدعم Kaspersky Endpoint Security متغير البيئة `%userprofile%` عند توليد قائمة الاستثناءات باستخدام وحدة تحكم Kaspersky Security Center. ولتطبيق الإدخال على كل حسابات المستخدمين، يمكنك استخدام الحرف * (على سبيل المثال، `C:\Users\*\Documents\File.exe`). كلما أضفت متغير بيئة جديدًا، فأنت بحاجة إلى إعادة تشغيل التطبيق.

- أدخل اسم الكائن وفقًا لتصنيف موسوعة Kaspersky (على سبيل المثال، `Email-Worm` أو `Rootkit` أو `RemoteAdmin`). يمكنك استخدام الأقنعة مع حرف `?` (يستبدل أي حرف مفرد) و `*` (يحل محل أي عدد من الأحرف). على

	سبيل المثال، في حالة تحديد القناع `*Client`، يستثني التطبيق كائنات `Client-IRC` و`Client-P2P` و`Client-SMTP` من عمليات الفحص.
التطبيقات الموثوقة	يسرد هذا الجدول التطبيقات الموثوقة التي لا يتم مراقبة نشاطها بواسطة Kaspersky Endpoint Security أثناء تشغيله. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع. لا يدعم Kaspersky Endpoint Security متغير البيئة `%userprofile%` عند توليد قائمة بالتطبيقات الموثوقة على وحدة تحكم Kaspersky Security Center. ولتطبيق الإدخال على كل حسابات المستخدمين، يمكنك استخدام الحرف * (على سبيل المثال، `C:\Users\*\Documents\File.exe`). كلما أضفت متغير بيئة جديدًا، فأنت بحاجة إلى إعادة تشغيل التطبيق. ينظم مكون التحكم في التطبيقات بدء تشغيل كل من التطبيقات بغض النظر عن تضمين التطبيق أم لا في جدول التطبيقات الموثوقة.
دمج القيم عند التوريث (متوفر فقط في Kaspersky Security Center (Console	يؤدي هذا إلى دمج قائمة استثناءات الفحص والتطبيقات الموثوقة في السياسات الأصلية والفرعية في Kaspersky Security Center. لدمج القوائم، يجب تكوين السياسة الفرعية لترث إعدادات السياسة الأصلية لتطبيق Kaspersky Security Center. في حالة تحديد خانة الاختيار، سيتم عرض عناصر القائمة من السياسة الأصلية لتطبيق Kaspersky Security Center في السياسات الفرعية. ويمكنك بهذه الطريقة، على سبيل المثال، إنشاء قائمة موحدة بالتطبيقات الموثوقة للمؤسسة بأكملها. لا يمكن حذف عناصر القائمة الموروثة في السياسات الفرعية أو تحريرها. ويمكن حذف العناصر الموجودة في قائمة الاستثناءات من الفحص وقائمة التطبيقات الموثوقة التي يتم دمجها أثناء الوراثة وتحريرها فقط في السياسة الأصلية. ويمكنك إضافة عناصر قائمة أو تحريرها أو حذفها في سياسات المستوى الأدنى. إذا كانت العناصر الموجودة في قوائم السياسة الفرعية والأصلية متطابقة، فيتم عرض هذه العناصر على العنصر نفسه للسياسة الأصلية. في حالة عدم تحديد خانة الاختيار، فإن عناصر لا يتم دمجها عند وراثة إعدادات سياسات Kaspersky Security Center.
السماح باستخدام الاستثناءات المحلية / السماح باستخدام التطبيقات الموثوقة المحلية (متوفر فقط في Kaspersky Security Center (Console	الاستثناءات المحلية والتطبيقات الموثوقة المحلية (المنطقة الموثوقة المحلية) – قائمة بالكائنات والتطبيقات المحددة بواسطة المستخدم في Kaspersky Endpoint Security لجهاز كمبيوتر معين. لا يراقب Kaspersky Endpoint Security الكائنات والتطبيقات من المنطقة الموثوقة المحلية. وبهذه الطريقة، يستطيع المستخدمون إنشاء قوائم الاستثناءات والتطبيقات الموثوقة المحلية الخاصة بهم بالإضافة إلى المنطقة الموثوقة العامة في سياسة ما. في حالة تحديد خانة الاختيار، يستطيع المستخدم إنشاء قائمة محلية لاستثناءات الفحص وقائمة محلية بالتطبيقات الموثوقة. يستطيع المسؤول استخدام Kaspersky Security Center لعرض عناصر القائمة أو إضافتها أو تحريرها أو حذفها في خصائص الكمبيوتر. في حالة إلغاء تحديد خانة الاختيار، يستطيع المستخدم الوصول فقط إلى القوائم العامة للاستثناءات من الفحص والتطبيقات الموثوقة التي تم إنشاؤها في السياسة.
مخزن شهادات النظام الموثوق	في حالة تحديد أحد مخازن شهادات النظام الموثوقة، يستثني Kaspersky Endpoint Security التطبيقات الموقعة بتوقيع رقمي موثوق من عمليات الفحص. ويُعين Kaspersky Endpoint Security تلقائيًا هذه التطبيقات إلى المجموعة **موثوق**. في حالة تحديد **عدم الاستخدام**، يفحص Kaspersky Endpoint Security التطبيقات بغض النظر عما إذا كانت تتضمن توقيعًا رقميًا أم لا. يضع Kaspersky Endpoint Security تطبيقًا في مجموعة ثقة بناءً على مستوى الخطر الذي قد يشكله هذا التطبيق على الكمبيوتر.

إعدادات التطبيق

يمكنك تكوين الإعدادات العامة التالية للتطبيق:

- وضع التشغيل
- الدفاع الذاتي
- الأداء
- معلومات تتبع الأخطاء
- حالة الكمبيوتر عند تطبيق الإعدادات

إعدادات التطبيق

المعلمة	الوصف
بدء Kaspersky Endpoint Security عند بدء تشغيل الكمبيوتر (مستحسن)	عند تحديد خانة الاختيار، يبدأ Kaspersky Endpoint Security بعد تحميل نظام التشغيل، مما يعمل على حماية الكمبيوتر أثناء الجلسة بأكملها. عند إلغاء تحديد خانة الاختيار، لا يبدأ تشغيل Kaspersky Endpoint Security بعد تحميل نظام التشغيل حتى يقوم المستخدم ببدئه يدويًا. يتم تعطيل حماية الكمبيوتر وقد تتعرض بيانات المستخدم للتهديدات.
استخدام تقنية التنظيف المتقدم (تتطلب موارد كمبيوتر كبيرة)	إذا تم تحديد خانة الاختيار، يظهر إخطار منبثق على الشاشة عند اكتشاف نشاط ضار في نظام التشغيل. في الإخطار الخاص به، يعرض Kaspersky Endpoint Security على المستخدم إجراء تطهير متقدم للكمبيوتر. بعد تصديق المستخدم على هذا الإجراء، يقوم Kaspersky Endpoint Security بإبطال التهديد. بعد إكمال إجراء التنظيف المتقدم، يقوم Kaspersky Endpoint Security بإعادة تشغيل الكمبيوتر. تستهلك تقنية التنظيف المتقدمة موارد كبيرة من الكمبيوتر، الأمر الذي قد يؤدي إلى إبطاء التطبيقات الأخرى. عندما يكون التطبيق بصدد اكتشاف إصابة نشطة، قد تكون بعض وظائف نظام التشغيل غير متاحة. وتتم استعادة توفر نظام التشغيل عند اكتمال التنظيف المتقدم وإعادة تشغيل الكمبيوتر. في حالة تثبيت Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام Windows for Servers، فلن يعرض Kaspersky Endpoint Security الإخطار. ولذلك، لا يستطيع المستخدم تحديد إجراء لتنظيف تهديد نشط. ولتنظيف تهديد، تحتاج إلى enable Advanced Disinfection technology في إعدادات التطبيق و enable immediate Advanced Disinfection في إعدادات مهمة فحص البرامج الضارة. بعد ذلك يتعين عليك بدء مهمة فحص البرامج الضارة.
استخدام Kaspersky Security Center كالخادم الوكيل للتفعيل (متوفر فقط في Kaspersky Security Center (Console	إذا تم تحديد خانة الاختيار هذه ، يتم استخدام الخادم الوكيل الخاص بـ Kaspersky Security Center كخادم وكيل عند تفعيل التطبيق.
تمكين الدفاع الذاتي	عند تحديد هذا المربع، يمنع Kaspersky Endpoint Security أي تغيير أو حذف لملفات التطبيق على محرك القرص الثابت وعمليات الذاكرة وإدخالات تسجيل النظام.
تمكين الإدارة الخارجية لخدمات النظام	في حالة تحديد خانة الاختيار، يسمح Kaspersky Endpoint Security بإدارة خدمات التطبيق من جهاز كمبيوتر بعيد. عند محاولة إدارة خدمات التطبيق عن بعد، يتم عرض إخطار على شريط مهام نظام تشغيل Microsoft Windows فوق رمز التطبيق (ما لم يكن المستخدم قد قام بتعطيل خدمة الإخطار).
تأجيل تشغيل المهام المجدولة أثناء	في حالة تحديد المربع، يتم تمكين وضع الحفاظ على الطاقة. يؤجل Kaspersky Endpoint Security المهام المجدولة. يمكن بدء مهام الفحص والتحديث يدويًا، إذا لزم الأمر.

التشغيل على طاقة البطارية	عند تمكين وضع توفير الطاقة وتشغيل الكمبيوتر باستخدام طاقة البطارية، لا يتم تشغيل المهام التالية حتى وإن كانت مجدولة: • تحديث • فحص كامل • فحص المناطق الحرجة • فحص مخصص • التحقق من السلامة • فحص IOC.
التنازل عن موارد لتطبيقات أخرى	قد يؤدي استهلاك موارد الكمبيوتر بواسطة Kaspersky Endpoint Security عند فحص الكمبيوتر إلى زيادة الحمل على الأنظمة الفرعية لوحدة المعالجة المركزية. وقد يؤدي هذا إلى إبطاء التطبيقات الأخرى. ولتحسين الأداء، يوفر Kaspersky Endpoint Security وضعًا لنقل الموارد إلى التطبيقات الأخرى. وفي هذا الوضع، يستطيع نظام التشغيل تقليل أولوية سلاسل مهام فحص Kaspersky Endpoint Security عندما يكون حمل وحدة المعالجة المركزية مرتفعًا. ويسمح هذا بإعادة توزيع موارد نظام التشغيل على التطبيقات الأخرى. وبالتالي، ستتلقى مهام الفحص وقتًا أقل لوحدة المعالجة المركزية. ونتيجة لذلك، سيستغرق Kaspersky Endpoint Security وقتًا أطول لفحص الكمبيوتر. بشكل افتراضي، يتم تكوين التطبيق بحيث يتم السماح بالتنازل عن الموارد للتطبيقات الأخرى.
تمكين كتابة التفريغ	إذا تم تحديد خانة الاختيار، يقوم Kaspersky Endpoint Security بكتابة التفريغات إذا ما تعطل. في حالة إلغاء تحديد خانة الاختيار هذه، لن يقوم Kaspersky Endpoint Security بكتابة التفريغات. يقوم التطبيق أيضًا بحذف ملفات التفريغ الموجودة من محرك القرص الصلب لجهاز الكمبيوتر.
تمكين حماية ملفات التفريغ والتتبع	إذا تم تحديد خانة الاختيار، يتم منح صلاحية الوصول إلى ملفات التفريغ لمسؤول النظام والمسؤولين المحليين وكذلك إلى المستخدم الذي قام بتمكين كتابة التفريغ. يمكن فقط للمسؤولين المحليين ومسؤولي النظام الوصول إلى ملفات التتبع. إذا تم إلغاء تحديد مربع الاختيار، فيمكن لأي مستخدم الوصول إلى ملفات التفريغ وملفات التتبع.
حالة الكمبيوتر عند تطبيق الإعدادات (متوفر فقط في Kaspersky Security Center (Console	إعدادات لعرض حالات أجهزة الكمبيوتر العميلة باستخدام برنامج Kaspersky Endpoint Security المثبت في وحدة Web Console عند حدوث أخطاء أثناء تطبيق سياسة أو تنفيذ مهمة. وتتوافر الحالات التالية موافق وتحذير وحرج.
تثبيت التحديثات دون إعادة تشغيل الكمبيوتر	تسمح لك ترقية التطبيق دون إعادة تشغيل الكمبيوتر بضمان تشغيل الخوادم دون انقطاع. يمكنك ترقية التطبيق دون إعادة التشغيل بدءًا من الإصدار 11.10.0. ولترقية إصدار سابق من التطبيق، يجب إعادة تشغيل الكمبيوتر. بدءًا من الإصدار 11.11.0، يمكنك تنفيذ الإجراءات التالية دون إعادة تشغيل الكمبيوتر: • تثبيت التصحيحات • تغيير مجموعة مكونات التطبيق • تثبيت Kaspersky Endpoint Security فوق Kaspersky Security for Windows Server تختلف القيمة الافتراضية للمعلمة وفقًا لنوع نظام التشغيل. وإذا كان التطبيق مُثبتًا على محطة عمل، فسيتم تعطيل ترقية التطبيق دون خيار إعادة التشغيل. واذا كان التطبيق مُثبتًا على خادم، سيتم تمكين ترقية التطبيق دون خيار إعادة التشغيل.

التقارير والمخزن

التقارير

يتم تسجيل معلومات حول تشغيل كل مكون من مكونات Kaspersky Endpoint Security، وحالات تشفير البيانات، وأداء كل مهمة فحص، ومهمة التحديث، ومهمة التحقق من السلامة، والتشغيل الإجمالي للتطبيق في التقارير.

يتم تخزين التقارير في المجلد `C:\ProgramData\Kaspersky Lab\KES.21.13\Report`.

النسخ الاحتياطي

يخزن النسخ الاحتياطي نسخًا احتياطية من الملفات التي تم حذفها أو تعديلها أثناء التنظيف. ويتم تعريف النسخة الاحتياطية بأنها نسخة ملف يتم إنشاؤها قبل تنظيف الملف أو حذفه. ويتم تخزين ملفات النسخ الاحتياطي بتنسيق خاص ولا تُمثل تهديدًا.

يتم تخزين النسخ الاحتياطية للملفات في المجلد `C:\ProgramData\Kaspersky Lab\KES.21.13\QB`.

يتم منح المستخدمين في مجموعة المسؤولين الإذن الكامل للوصول إلى هذا المجلد. ويتم منح حقوق الوصول المحدود إلى هذا المجلد للمستخدم الذي تم استخدام حسابه لتثبيت Kaspersky Endpoint Security.

لا يوفر Kaspersky Endpoint Security القدرة على تكوين أذونات وصول المستخدم إلى النسخ الاحتياطية من الملفات.

العزل

العزل هو مخزن محلي خاص على الكمبيوتر. ويستطيع المستخدم عزل الملفات التي يعتبرها المستخدم خطرة على جهاز الكمبيوتر. ويتم تخزين الملفات المعزولة في حالة مشفرة ولا تهدد أمن الجهاز. ولا يستخدم Kaspersky Endpoint Security العزل إلا عند العمل مع حلول Detection and Response: EDR Optimum وEDR Expert وKATA (EDR) وKaspersky Sandbox. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل حول إدارة العزل كجزء من الحلول، يرجى الرجوع إلى تعليمات Kaspersky Sandbox وتعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert وتعليمات Kaspersky Anti Targeted Attack Platform.

لا يمكن تكوين العزل إلا باستخدام Web Console. ويمكنك أيضًا استخدام Web Console لإدارة الكائنات المعزولة (استعادة، حذف، إضافة، وما إلى ذلك). ويمكنك استعادة الكائنات محليًا على الكمبيوتر باستخدام سطر الأوامر.

يستخدم Kaspersky Endpoint Security حساب النظام (SYSTEM) لعزل الملفات.

إعدادات التقارير والمخازن

المعلمة	الوصف
تخزين التقارير بحد أقصى N يوم/أيام	إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لفترة تخزين التقرير ليكون بالفاصل الزمني المُحدد. أقصى فترة زمنية افتراضية لتخزين التقارير هي 30 يومًا. وبعد انتهاء هذه الفترة، يقوم برنامج Kaspersky Endpoint Security بشكل تلقائي بحذف الإدخالات القديمة من ملف التقارير.
تقييد حجم ملف التقرير إلى N م ب	إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لحجم ملف التقرير ليكون بالقيمة المُحددة. والحجم الأقصى الافتراضي لهذا الملف هو 1024 ميجابايت. لتجنب تجاوز الحد الأقصى لحجم ملف التقارير، يقوم برنامج Kaspersky Endpoint Security بشكل تلقائي بحذف الإدخالات القديمة من ملف التقارير عندما يتم الوصول إلى الحد الأقصى لحجم ملف التقارير.
تخزين الكائنات بحد أقصى N يوم/أيام	إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لفترة تخزين الملف ليكون بالفاصل الزمني المُحدد. الفترة القصوى الافتراضية لتخزين الملفات هي 30 يومًا. وبعد انتهاء فترة التخزين القصوى، يحذف Kaspersky Endpoint Security أقدم الملفات من النسخ الاحتياطي.

تقييد حجم النسخ الاحتياطي إلى N م ب	إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لحجم التخزين ليكون بالقيمة المُحددة. والإعداد الافتراضي لهذا الخيار هو 1024 ميجا بايت. لتجنب تجاوز الحد الأقصى لحجم التخزين، يقوم برنامج Kaspersky Endpoint Security بشكل تلقائي بحذف الملفات القديمة من المخزن عندما يتم الوصول إلى الحد الأقصى لحجم التخزين.
Limit the size of Quarantine to N MB (متوفر فقط في Web Console)	الحد الأقصى لحجم العزل بالميجابايت. على سبيل المثال، يمكنك ضبط الحد الأقصى لحجم العزل على 200 ميجابايت. عندما يصل العزل إلى الحجم الأقصى، يرسل Kaspersky Endpoint Security الحدث المقابل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يوقف التطبيق عزل الكائنات الجديدة. ويجب إفراغ العزل يدويًا.
Notify when the Quarantine storage reaches N percent (متوفر فقط في Web Console)	قيمة الحد للعزل. على سبيل المثال، يمكنك تعيين حد العزل إلى 50%. عندما يصل العزل إلى الحد، يرسل Kaspersky Endpoint Security الحدث المقابل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يستمر التطبيق في عزل الكائنات الجديدة.
نقل البيانات إلى خادم الإدارة (متوفر فقط في Kaspersky Security Center)	فئات الأحداث على أجهزة الكمبيوتر العميلة التي يجب أن يتم ترحيل معلوماتها إلى خادم الإدارة.

إعدادات الشبكة

يمكنك تكوين الخادم الوكيل الذي يتم استخدامه للاتصال بالإنترنت وتحديث قواعد بيانات مكافحة الفيروسات، قم بتحديد وضع مراقبة منافذ الشبكة وتكوين فحص الاتصالات المشفرة.

خيارات شبكة الاتصال

المعلمة	الوصف
تقييد حركة البيانات للاتصالات المقاسة	في حالة تحديد خانة الاختيار هذه، يقيد التطبيق حركة شبكة الاتصال الخاصة به عندما يكون الاتصال بالإنترنت محدودًا. يحدد Kaspersky Endpoint Security اتصال الإنترنت عبر الهاتف المحمول عالي السرعة كاتصال محدود، ويحدد اتصال Wi-Fi كاتصال غير محدود. تعمل اتصالات الشبكة المراعية للتكلفة على أجهزة الكمبيوتر التي تعمل بنظام Windows 8 أو أحدث.
إدخال البرنامج النصي في حركة مرور الويب للتفاعل مع صفحات الويب	في حالة تحديد خانة الاختيار، يقوم Kaspersky Endpoint Security بإدخال برنامج نصي لتفاعل صفحة الويب في حركة الويب. يضمن هذا البرنامج النصي قدرة مكون التحكم في الويب على العمل بشكل صحيح. يتيح البرنامج النصي تسجيل أحداث التحكم في الويب. وبدون هذا البرنامج النصي، لا يمكنك تمكين مراقبة نشاط المستخدم على الإنترنت. يوصي خبراء Kaspersky بإدخال نص تفاعل صفحة الويب هذا في حركة المرور لضمان التشغيل الصحيح للتحكم في الويب.
الخادم الوكيل	إعدادات الخادم الوكيل المستخدم للوصول إلى الإنترنت لمستخدمي أجهزة الكمبيوتر العميلة. يستخدم Kaspersky Endpoint Security هذه الإعدادات لمكونات حماية معينة تشتمل على تحديث قواعد البيانات والوحدات النمطية للتطبيق. بالنسبة للتهيئة التلقائية للخادم الوكيل يستخدم Kaspersky Endpoint Security بروتوكول WPAD (بروتوكول اكتشاف تلقائي لوكيل الويب). إذا تعذر تحديد عنوان IP الخادم الوكيل باستخدام هذا البروتوكول، فسوف يستخدم التطبيق عنوان الخادم الوكيل الذي تم تحديده في إعدادات مستعرض Microsoft Internet Explorer.
تجاوز الخادم	إذا تم تحديد خانة الاختيار هذه، فلن يستخدم Kaspersky Endpoint Security الخادم الوكيل عند إجراء تحديث من مجلد

الوكيل للعناوين المحلية	مشارك.
المنافذ قيد المراقبة	**مراقبة كل منافذ الشبكة**. في وضع مراقبة منفذ شبكة الاتصال هذا تقوم مكونات الحماية (الحماية من تهديدات الملفات، والحماية من تهديدات الويب، والحماية من تهديدات البريد) بمراقبة تدفقات البيانات التي يتم نقلها عبر أي منافذ شبكة مفتوحة بالكمبيوتر. **مراقبة منافذ الشبكة المحددة فقط**. في وضع مراقبة منفذ شبكة الاتصال هذا، تراقب مكونات الحماية المنافذ المحددة للكمبيوتر ونشاط الشبكة للتطبيقات المحددة. يتم تكوين القائمة الخاصة بمنافذ الشبكة التي تُستخدم عادة في نقل حركة البريد الإلكتروني والشبكة وفقًا لتوصيات خبراء Kaspersky. **مراقبة جميع المنافذ للتطبيقات الموجودة في القائمة التي توصي بها Kaspersky**. يستخدم هذا الخيار قائمة محددة مسبقًا بالتطبيقات التي تتم مراقبة منافذ شبكة الاتصال الخاصة بها بواسطة Kaspersky Endpoint Security. على سبيل المثال، تتضمن هذه القائمة Google Chrome وAdobe Reader وJava وتطبيقات أخرى. **مراقبة جميع منافذ التطبيقات المحددة**. يستخدم هذا قائمة بالتطبيقات التي تتم مراقبة منافذ شبكة الاتصال الخاصة بها بواسطة Kaspersky Endpoint Security.
فحص الاتصالات المشفرة	يفحص Kaspersky Endpoint Security حركة شبكة الاتصال المشفرة المنقولة عبر البروتوكولات التالية: • SSL 3.0. • TLS 1.0، TLS 1.1، TLS 1.2، TLS 1.3. يدعم Kaspersky Endpoint Security أوضاع فحص الاتصال المشفر التالية: • **عدم فحص الاتصالات المشفرة**. لن يتمكن Kaspersky Endpoint Security من الوصول إلى محتويات مواقع الويب التي تبدأ بالحروف `https://`. • **فحص الاتصالات المشفرة عند الطلب من مكونات الحماية**. سوف يفحص Kaspersky Endpoint Security الحركة المشفرة فقط عند طلبها بواسطة مكونات الحماية من تهديدات الويب والحماية من تهديدات البريد والتحكم في الويب. • **فحص الاتصالات المشفرة دائمًا**. سوف يفحص Kaspersky Endpoint Security حركة شبكة الاتصالات المشفرة حتى إذا تم تعطيل مكونات الحماية. لا يفحص Kaspersky Endpoint Security الاتصالات المشفرة التي تم إنشاؤها بواسطة تطبيقات موثوقة تم تعطيل فحص حركة مرورها. لا يفحص Kaspersky Endpoint Security الاتصالات المشفرة من قائمة مواقع الويب الموثوقة المحددة مسبقًا. يتم إنشاء القائمة المحددة مسبقًا لمواقع الويب الموثوقة بواسطة خبراء Kaspersky. يتم تحديث هذه القائمة بقواعد بيانات برنامج مكافحة الفيروسات الخاصة بالتطبيق. ويمكنك عرض القائمة المحددة مسبقًا لمواقع الويب الموثوقة فقط في واجهة Kaspersky Endpoint Security. ولا يمكنك عرض القائمة في وحدة تحكم Kaspersky Security Center.
شهادات الجذر الموثوق بها	قائمة شهادات الجذر الموثوق بها. يتيح لك Kaspersky Endpoint Security تثبيت شهادات الجذر الموثوق بها على أجهزة كمبيوتر المستخدم إذا احتجت، على سبيل المثال، إلى نشر مركز شهادات جديد. ويتيح لك التطبيق إضافة شهادة إلى متجر شهادات Kaspersky Endpoint Security خاص. وفي هذه الحالة، تعتبر الشهادة موثوقة فقط لتطبيق Kaspersky Endpoint Security. بمعنى آخر، يستطيع المستخدم الوصول إلى موقع ويب باستخدام الشهادة الجديدة في المستعرض. وإذا حاول تطبيق آخر الوصول إلى موقع الويب، فيمكنك الحصول على خطأ في الاتصال بسبب مشكلة في الشهادة. ولإضافتها إلى مخزن شهادات النظام، يمكنك استخدام سياسات مجموعة Active Directory.
عند زيارة مجال له شهادة غير موثوق بها	• **سماح**. عند زيارة مجال ذو شهادة غير موثوقة، يسمح برنامج Kaspersky Endpoint Security باتصال الشبكة. عند فتح مجال ذو شهادة غير موثوقة في مستعرض، يعرض Kaspersky Endpoint Security صفحة HTML يظهر بها تحذيرًا وسببًا يفسر عدم التوصية بزيارة ذلك المجال. بإمكان المستخدم النقر على الرابط من صفحة HTML التحذيرية للحصول على إمكانية الوصول إلى مورد الويب المطلوب. إذا أنشأ تطبيق أو خدمة تابعة لجهة خارجية اتصالاً بمجال بشهادة غير موثوقة، فإن Kaspersky Endpoint Security ينشئ شهادته الخاصة لفحص حركة المرور. وتكون الشهادة الجديدة غير موثوق. ويعد ذلك ضروريًا لتحذير تطبيق الجهة الخارجية بشأن الاتصال غير الموثوق به لأنه لا يمكن عرض صفحة HTML في هذه الحالة ويمكن إنشاء الاتصال في وضع الخلفية. • **منع الاتصال**. عند زيارة مجال ذو شهادة غير موثوقة، يمنع برنامج Kaspersky Endpoint Security اتصال الشبكة. عند فتح مجال ذو شهادة غير موثوقة في مستعرض، يعرض Kaspersky Endpoint Security صفحة HTML يظهر بها سببًا يفسر منع زيارة ذلك المجال.

عند حدوث أخطاء في فحص الاتصال المشفر	• **منع الاتصال**. إذا تم تحديد هذا العنصر، فعند ظهور خطأ في فحص الاتصالات المشفرة، يقوم Kaspersky Endpoint Security بحظر اتصال الشبكة. • **إضافة المجال إلى الاستثناءات**. إذا تم تحديد هذا العنصر، فعند ظهور خطأ في فحص الاتصال المشفر، يضيف Kaspersky Endpoint Security المجال الذي نتج عنه الخطأ إلى قائمة المجالات ذات أخطاء الفحص ولا يقوم بمراقبة نسبة استخدام شبكة الاتصال المشفرة عند زيارة هذا المجال. يمكنك عرض قائمة بمجالات أخطاء فحص الاتصالات المشفرة فقط في الواجهة المحلية الخاصة بالتطبيق. لمسح محتويات القائمة، تحتاج إلى تحديد **منع الاتصال**. ينشئ Kaspersky Endpoint Security أيضًا حدثًا لخطأ فحص الاتصال المشفر.
منع اتصالات SSL 2.0 (موصى به)	في حالة تحديد خانة الاختيار، لن يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 2.0. في حالة إلغاء تحديد خانة الاختيار، لا يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 2.0 ولا يراقب حركة شبكة الاتصال التي تم إرسالها عبر هذه الاتصالات.
فك تشفير اتصال مشفر بموقع الويب الذي يستخدم شهادات EV	تؤكد شهادات EV (شهادات التحقق الموسَّع) مصادقة مواقع الويب وتُحسّن تأمين الاتصال. تستخدم المستعرضات رمز قفل في شريط العناوين للإشارة إلى أن موقع الويب لديه شهادة EV. قد تقوم المستعرضات أيضًا بتلوين شريط العناوين باللون الأخضر كليًا أو جزئيًا. في حالة تحديد خانة الاختيار، يفك التطبيق تشفير الاتصالات المشفرة ويراقبها مع مواقع الويب التي تستخدم شهادة EV. في حالة إلغاء تحديد خانة الاختيار، لن يمتلك للتطبيق حق الوصول إلى المحتويات الخاصة بحركة مرور HTTPS. لهذا السبب، يراقب التطبيق حركة مرور HTTPS فقط بناءً على عنوان موقع الويب، على سبيل المثال، `https://bing.com`. إذا فتحت موقع ويب باستخدام شهادة EV للمرة الأولى، فسوف يتم فك تشفير الاتصال المُشفر بغض النظر عما إذا كانت خانة الاختيار مُحددة أم لا.
العناوين الموثوقة	يستخدم هذا قائمة بعناوين الويب التي لا يفحص Kaspersky Endpoint Security اتصالات الشبكة لها. وفي هذه الحالة، لا يفحص Kaspersky Endpoint Security حركة مرور HTTPS لعناوين الويب الموثوقة عندما يؤدي مكونات الحماية من تهديدات الويب والحماية من تهديدات البريد والتحكم في الويب عملها. ويمكنك إدخال اسم مجال أو عنوان IP. يدعم Kaspersky Endpoint Security حرف `*` لإدخال قناع في اسم المجال. لا يدعم Kaspersky Endpoint Security رموز `*` لعناوين IP. ويمكنك تحديد نطاق من عناوين IP باستخدام القناع الشبكة الفرعية (على سبيل المثال، 198.51.100.0/24). أمثلة: • `domain.com` - يتضمن السجل العناوين التالية: `https://domain.com` و`https://www.domain.com` و`https://domain.com/page123`. ولا يتضمن السجل المجالات الفرعية (على سبيل المثال، `subdomain.domain.com`). • `subdomain.domain.com` - يتضمن السجل العناوين التالية: `https://subdomain.domain.com` و`https://subdomain.domain.com/page123`. السجل حصري لمجال `domain.com`. • `*.domain.com` - يتضمن السجل العناوين التالية: `https://movies.domain.com` و`https://images.domain.com/page123`. السجل حصري لمجال `domain.com`.
التطبيقات الموثوقة	قائمة التطبيقات التي لا يتم مراقبة نشاطها بواسطة Kaspersky Endpoint Security أثناء تشغيله. يمكنك تحديد أنواع أنشطة التطبيق التي لن يقوم برنامج Kaspersky Endpoint Security بمراقبتها (على سبيل المثال، عدم فحص حركة مرور الشبكة). يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع.
استخدام مخزن الشهادات المحدد لفحص الاتصالات المشفرة في تطبيقات Mozilla	في حالة تحديد خانة الاختيار هذه، يفحص التطبيق الحركة المشفرة في مستعرض Mozilla Firefox وعميل البريد Thunderbird. وقد يتم منع الوصول إلى بعض مواقع الويب عبر بروتوكول HTTPS. لفحص حركة المرور في مستعرض Mozilla Firefox وعميل البريد Thunderbird، يجب عليك تمكين فحص الاتصالات المشفرة. وفي حالة تعطيل فحص الاتصالات المشفرة، لا يفحص التطبيق حركة المرور في مستعرض Mozilla Firefox وعميل البريد Thunderbird.

(متوفر فقط في واجهة Kaspersky Endpoint Security)	يستخدم التطبيق شهادة جذر Kaspersky لفك تشفير البيانات المشفرة وتحليلها. يمكنك تحديد مخزن الشهادات الذي سيحتوي على شهادة جذر Kaspersky. • **استخدام مخزن شهادات Windows (مستحسن)**. تتم إضافة شهادة جذر Kaspersky إلى هذا المخزن أثناء تثبيت Kaspersky Endpoint Security. • **استخدام مخزن شهادات Mozilla**. يستخدم Mozilla Firefox وThunderbird مخازن الشهادات الخاصة بهما. في حالة تحديد مخزن شهادات Mozilla، ستحتاج إلى إضافة شهادة جذر Kaspersky يدويًا إلى هذا المخزن من خلال خصائص المستعرض.

الواجهة

يمكنك تكوين الإعدادات الخاصة بواجهة التطبيق.

الإعدادات الخاصة بالواجهة

المعلمة	الوصف
التفاعل مع المستخدم (متوفر فقط في Kaspersky Security Center (Console	**عرض واجهة التطبيق المبسطة**. على جهاز كمبيوتر عميل، لا يمكن الوصول إلى نافذة التطبيق الرئيسية، وتكون الأيقونة الموجودة في منطقة إخطار Windows فقط متاحة. في قائمة السياق الخاصة بالرمز، يُمكن للمستخدم تنفيذ عدد محدود من العمليات مع برنامج Kaspersky Endpoint Security. يعرض أيضًا برنامج Kaspersky Endpoint Security إخطارات فوق رمز التطبيق. **عرض واجهة المستخدم**. على جهاز كمبيوتر عميل، النافذة الرئيسية لبرنامج Kaspersky Endpoint Security و الرمز الموجود في منطقة إخطار Windows يكونوا متاحين. في قائمة السياق الخاصة بالرمز، يُمكن للمستخدم تنفيذ العمليات مع برنامج Kaspersky Endpoint Security. يعرض أيضًا برنامج Kaspersky Endpoint Security إخطارات فوق رمز التطبيق. **إخفاء قسم مراقبة نشاط التطبيقات**. على جهاز الكمبيوتر العميل، في النافذة الرئيسية لبرنامج Kaspersky Endpoint Security، لا يتوفر الزر **مراقبة نشاط التطبيقات**. مراقبة نشاط التطبيقات أداة مصممة لعرض معلومات حول نشاط التطبيقات على كمبيوتر المستخدم في الوقت الحقيقي. **عدم العرض**. على جهاز كمبيوتر عميل، لا يتم عرض أي علامات لعملية تشغيل برنامج Kaspersky Endpoint Security. الرمز الموجود في منطقة إخطار Windows والإخطارات غير متاحين.
إعدادات الإخطار	جدول يضم إعدادات الإخطارات بشأن الأحداث ذات مستويات الأهمية المختلفة التي قد تحدث أثناء تشغيل مكون أو مهمة أو التطبيق بأكمله. يعرض Kaspersky Endpoint Security إخطارات حول تلك الأحداث على الشاشة، أو يرسلها عبر البريد الإلكتروني أو يقوم بتسجيلها.
إعدادات إخطارات البريد الإلكتروني	إعدادات خادم SMTP لتسليم الإخطارات الخاصة بالأحداث المسجلة خلال تشغيل التطبيق.
إظهار حالة التطبيق في منطقة الإخطارات	فئات أحداث التطبيق التي تتسبب في تغيير رمز برنامج Kaspersky Endpoint Security في منطقة إخطار شريط مهام Microsoft Windows (أو) وينتج عنه إخطار منبثق.
إخطارات بحالة قاعدة البيانات المحلية لمكافحة البرامج الضارة	إعدادات الإخطارات حول قواعد بيانات مكافحة الفيروسات القديمة والمستخدمة من قبل التطبيق.
الحماية بكلمة مرور	إذا تم تشغيل زر التبديل، يطالب برنامج Kaspersky Endpoint Security المستخدم بكلمة مرور عندما يحاول المستخدم إجراء عملية تكون في نطاق حماية كلمة المرور. يشمل نطاق حماية كلمة المرور العمليات الممنوعة (مثل تعطيل مكونات الحماية) وحسابات المستخدمين التي يتم تطبيق نطاق حماية كلمة المرور عليها. بعد تمكين حماية كلمة المرور، يطالبك برنامج Kaspersky Endpoint Security بتعيين كلمة مرور لإجراء العمليات.
دعم المستخدم / الروابط الخاصة	قائمة بروابط لموارد الويب التي تحتوي على معلومات حول الدعم الفني لتطبيق Kaspersky Endpoint Security. سوف يتم عرض هذه الروابط في النافذة **الدعم** من واجهة Kaspersky Endpoint Security المحلية بدلًا من الروابط القياسية.

بالموارد على الويب (متوفر فقط في Kaspersky Security Center (Console	
دعم المستخدم / الوصف (متوفر فقط في Kaspersky Security Center (Console	الرسالة التي يتم عرضها في نافذة **الدعم** الخاصة بالواجهة المحلية لبرنامج Kaspersky Endpoint Security.

إدارة الإعدادات

يمكنك حفظ إعدادات Kaspersky Endpoint Security الحالية في ملف واستخدامها لتكوين التطبيق بسرعة على جهاز كمبيوتر مختلف. ويمكنك أيضًا استخدام ملف تكوين عند نشر التطبيق من خلال Kaspersky Security Center مع حزمة تثبيت. ويمكنك استعادة الإعدادات الافتراضية في أي وقت.

تتوفر إعدادات إدارة تكوين التطبيق في واجهة Kaspersky Endpoint Security فقط.

إعدادات إدارة تكوين التطبيق

الإعدادات	الوصف
استيراد	استخرج إعدادات التطبيق من ملف بتنسيق CFG وطبقها.
تصدير	احفظ إعدادات التطبيق الحالية في ملف بتنسيق CFG.
استعادة	يمكنك استعادة إعدادات التطبيق التي توصي بها Kaspersky في أي وقت تريد. عند استعادة الإعدادات، يتم تعيين مستوى الأمان **مستحسن** لجميع مكونات الحماية.

تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق

يضمن تحديث قواعد بيانات Kaspersky Endpoint Security والوحدات النمطية للتطبيق الخاصة به توفير أحدث حماية متوفرة على الكمبيوتر الخاص بك. تظهر بصفة يومية فيروسات جديدة وأنواع أخرى من البرمجيات الضارة على مستوى العالم. وتحتوي قواعد بيانات Kaspersky Endpoint Security على معلومات حول التهديدات وطرق تحييدها. ولاكتشاف التهديدات بسرعة، يجب أن تهتم بتحديث قواعد البيانات والوحدات النمطية للتطبيق بانتظام.

تحتاج التحديثات المنتظمة ترخيص ساريًا. في حالة عدم وجود ترخيص موجود، سيكون بإمكانك إجراء تحديث لمرة واحدة فقط.

وتعتبر خوادم تحديث Kaspersky هي المصدر الرئيسي لتحديث Kaspersky Endpoint Security.

يجب توصيل جهاز الكمبيوتر الخاص بك إلى الإنترنت لتتمكن من تنزيل حزمة التحديثات من خوادم تحديث Kaspersky بنجاح. وافتراضيًا، يتم تحديد إعدادات توصيل الإنترنت تلقائيًا. إذا كنت تستخدم خادمًا وكيلاً، فأنت بحاجة إلى تكوين إعدادات الخادم الوكيل.

يتم تنزيل التحديثات عبر بروتوكول HTTPS. قد يتم تنزيلهم أيضًا عبر بروتوكول HTTP عند استحالة تنزيل التحديثات عبر بروتوكول HTTPS.

أثناء تنفيذ التحديث، يتم تنزيل الكائنات التالية وتثبيتها على جهاز الكمبيوتر الخاص بك:

- قواعد بيانات Kaspersky Endpoint Security. يتم توفير حماية الكمبيوتر باستخدام قواعد البيانات التي تحتوي على توقيعات الفيروسات والتهديدات الأخرى ومعلومات حول طرق إبطالها. كما تقوم مكونات الحماية باستخدام هذه المعلومات عند البحث عن الملفات المصابة الموجودة على الكمبيوتر الخاص بك وتحييدها. يتم تحديث قواعد البيانات باستمرار وتزويدها بسجلات التهديدات الجديدة وطرق مواجهتها. لذا، نوصي بتحديث قواعد البيانات بانتظام.

  وبالإضافة إلى قواعد بيانات Kaspersky Endpoint Security، يتم تحديث برامج تشغيل الشبكة التي تقوم بتمكين مكونات التطبيق لاعتراض حركة مرور الاتصال.

- الوحدات النمطية للتطبيق. بالإضافة إلى قواعد بيانات برنامج Kaspersky Endpoint Security، يمكنك أيضًا تحديث الوحدات النمطية للتطبيق. ويؤدي تحديث الوحدات النمطية للتطبيق إلى إصلاح نقاط الضعف الموجودة في برنامج Kaspersky Endpoint Security، مع إضافة وظائف جديدة أو تحسين الوظائف الموجودة بالفعل.

خلال التحديث، تتم مقارنة قواعد البيانات والوحدات النمطية للتطبيق الموجودة على جهاز الكمبيوتر الخاص بك مع الإصدار الحديث الموجود على مصدر التحديث. في حالة وجود اختلاف بين قواعد البيانات والوحدات النمطية للتطبيق الموجودة لديك حاليًا على الكمبيوتر عن الإصدارات الحديثة الموجودة على مصدر التحديث، يتم تثبيت الجزء المفقود من التحديثات على جهاز الكمبيوتر الخاص بك.

يمكن تحديث ملفات تعليمات السياق جنبًا إلى جنب مع تحديثات الوحدة النمطية للتطبيق.

إذا كانت قواعد البيانات قديمة، فقد تكون حزمة التحديثات كبيرة، وهو ما قد يتسبب في زيادة حركة الإنترنت (بما يصل إلى عشرات الميجابايت).

يتم عرض معلومات حول الحالة الحالية لقواعد بيانات Kaspersky Endpoint Security في نافذة التطبيق الرئيسية أو تلميح الأدوات الذي تراه عند تحريك المؤشر فوق أيقونة التطبيق في منطقة الإخطارات.

يتم تسجيل المعلومات الخاصة بنتائج التحديث وجميع الأحداث التي تقع أثناء تنفيذ مهمة التحديث في تقرير Kaspersky Endpoint Security.

إعدادات تحديث الوحدة النمطية للتطبيق وقاعدة البيانات

المعلمة	الوصف
جدولة تحديث قواعد البيانات	**تلقائيًا**. في هذا الوضع يفحص برنامج التطبيق مصدر التحديث للبحث عن وجود حزم تحديثات جديدة بشكل منتظم. يزيد معدل فحص حزمة التحديثات أثناء انتشار الفيروسات وينخفض في حالة عدم وجود فيروسات. وبعد اكتشاف وجود حزمة تحديث جديدة، يقوم برنامج Kaspersky Endpoint Security بتنزيل الحزمة وتثبيت التحديثات على الكمبيوتر الخاص بك. **يدويًا**. يتيح لك وضع تشغيل مهمة التحديث هذا ببدء مهمة التحديث يدويًا. **حسب الجدول**. في وضع تشغيل مهمة التحديث هذا، يقوم برنامج Kaspersky Endpoint Security بتشغيل مهمة التحديث حسب الجدول الذي قمت بتحديده. في حالة تحديد وضع تشغيل مهمة التحديث هذا، يمكنك أيضًا بدء تشغيل مهمة تحديث Kaspersky Endpoint Security يدويًا.
تشغيل المهام الفائتة	في حالة تحديد خانة الاختيار، يبدأ Kaspersky Endpoint Security في تشغيل مهمة التحديث التي تم تخطيها بمجرد أن يكون هذا الأمر ممكنًا. يمكن تخطي مهمة التحديث، على سبيل المثال، إذا تم إيقاف تشغيل الكمبيوتر عند وقت البدء في مهمة التحديث. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل مهام التحديث التي تم تخطيها. كبديل، سيقوم بتشغيل مهمة التحديث التالية بما يتوافق مع الجدول الحالي.
مصادر التحديث	مصدر التحديث عبارة عن مورد يحتوي على تحديثات لقواعد البيانات ووحدات تطبيق برنامج Kaspersky Endpoint Security. تتضمن مصادر التحديث خادم Kaspersky Security Center وخوادم تحديث Kaspersky والشبكة أو المجلدات المحلية. تتضمن القائمة الافتراضية لمصادر التحديث خوادم تحديث Kaspersky Security Center وKaspersky. يمكنك إضافة مصادر تحديث إلى القائمة. ويمكنك تحديد خوادم HTTP/FTP ومجلدات مشتركة كمصادر تحديث.

	لا يدعم Kaspersky Endpoint Security التحديثات من خوادم HTTPS ما لم تكن خوادم تحديث من Kaspersky. إذا تم تحديد موارد متعددة كمصادر للتحديث، يحاول برنامج Kaspersky Endpoint Security الاتصال بتلك الموارد واحدًا تلو الآخر، ابتداءً بأعلى القائمة، ويجري مهمة تحديث من خلال الحصول حزمة التحديثات من المصدر المتاح أولاً.
تشغيل مهام تحديث قاعدة البيانات باسم	في الوضع الافتراضي، يتم بدء مهمة تحديث برنامج Kaspersky Endpoint Security نيابة عن المستخدم الذي قمت باستخدام حسابه لتسجيل الدخول في نظام التشغيل. على الرغم من ذلك، قد يتم تحديث Kaspersky Endpoint Security من مصدر تحديث يتعذّر على المستخدم الوصول إليه لوجود نقص في الحقوق المطلوبة (على سبيل المثال، من مجلد مشترك يحتوي على حزمة تحديث) أو مصدر تحديث لم يتم تكوين مصادقة الخادم الوكيل له. في إعدادات التطبيق، يمكنك تحديد مستخدم يمتلك هذه الحقوق وتقوم ببدء مهمة تحديث برنامج Kaspersky Endpoint Security تحت حساب ذلك المستخدم.
تنزيل تحديثات وحدات التطبيق	تنزيل تحديثات وحدة التطبيق مع تحديثات قاعدة بيانات التطبيق. إذا تم تحديد خانة الاختيار، يقوم Kaspersky Endpoint Security بإخطار المستخدم بشأن تحديثات الوحدة النمطية للتطبيق المتوفرة كما يقوم بتضمين تحديثات الوحدة النمطية للتطبيق في حزمة التحديث أثناء تشغيل مهمة التحديث. يتم تحديد طريقة تطبيق تحديثات الوحدة النمطية للتطبيق بواسطة الإعدادات التالية: • **تثبيت التحديثات المهمة والمصدق عليها**. إذا تم تحديد هذا الخيار، وعند توافر تحديثات الوحدة النمطية للتطبيق يقومKaspersky Endpoint Security بتثبيت التحديثات الهامة تلقائيًا وجميع تحديثات الوحدة النمطية للتطبيق الأخرى فقط بعد أن تتم الموافقة على تثبيتهم محليًا بواسطة واجهة التطبيق أو على جانب Kaspersky Security Center. • **تثبيت التحديثات المصدق عليها فقط**. إذا تم تحديد هذا الخيار، عند توافر تحديثات الوحدة النمطية للتطبيق يقومKaspersky Endpoint Security بتثبيتهم فقط بعد أن يتم الموافقة على تثبيتهم محليًا عبر واجهة التطبيق أو على جانب Kaspersky Security Center. ويتم تحديد هذا الخيار بشكل افتراضي. إذا تم إلغاء خانة الاختيار، لا يقوم Kaspersky Endpoint Security بإخطار المستخدم بشأن تحديثات الوحدة النمطية للتطبيق المتوفرة ولا يقوم بتضمين تحديثات الوحدة النمطية للتطبيق في حزمة التحديث أثناء تشغيل مهمة التحديث. إذا اقتضت تحديثات الوحدة النمطية للتطبيق مراجعة وقبول شروط اتفاقية ترخيص المستخدم النهائي، يقوم التطبيق بتثبيت التحديثات عقب قبول شروط اتفاقية ترخيص المستخدم النهائي. ويتم تحديد خانة الاختيار هذه بشكل افتراضي.
نسخ التحديثات إلى مجلد	إذا تم تحديد مربع الاختيار، يقوم Kaspersky Endpoint Security بنسخ حزم التحديث إلى المجلد المشترك المحدد أسفل مربع الاختيار. وبعد ذلك يكون بمقدور أجهزة الكمبيوتر الأخرى المتصلة بشبكتك المحلية أن تتلقى حزمة التحديث من هذا المجلد المشترك. يقلل هذا من حركة الإنترنت لأن حزمة التحديث يتم تنزيلها مرة واحدة. يتم تحديد المجلد التالي بشكل افتراضي: `C:\ProgramData\Kaspersky Lab\KES.21.13\Update distribution\`.
الخادم الوكيل للتحديثات (متوفر فقط في واجهة Kaspersky Endpoint (Security	إعدادات الخادم الوكيل للوصول للإنترنت لمستخدمي أجهزة الكمبيوتر العميلة لتحديث الوحدات النمطية للتطبيق وقواعد البيانات. بالنسبة للتهيئة التلقائية للخادم الوكيل يستخدم Kaspersky Endpoint Security بروتوكول WPAD (بروتوكول اكتشاف تلقائي لوكيل الويب). إذا تعذر تحديد عنوان IP الخاص بالخادم الوكيل باستخدام هذا البروتوكول، فسوف يستخدم Kaspersky Endpoint Security عنوان الخادم الوكيل الذي تم تحديده في إعدادات المستعرض Microsoft Internet Explorer.
تجاوز الخادم الوكيل للعناوين المحلية (متوفر فقط في واجهة Kaspersky Endpoint (Security	إذا تم تحديد خانة الاختيار هذه، فلن يستخدم Kaspersky Endpoint Security الخادم الوكيل عند إجراء تحديث من مجلد مشارك.

الملحق رقم 2. المجموعات الموثوقة للتطبيقات

يقوم Kaspersky Endpoint Security بتصنيف جميع التطبيقات التي تم بدء تشغيلها على الكمبيوتر في مجموعات موثوقة. يتم تصنيف التطبيقات في مجموعات موثوقة وفقًا لمستوى التهديد الذي تفرضه التطبيقات على نظام التشغيل.

المجموعات الموثوقة هي على النحو التالي:

- **موثوق**. تضم هذه المجموعة تطبيقات تم الوفاء بشرط أو أكثر من الشروط التالية من أجلها:
  - توقيع التطبيقات رقميًا من قبل بائعين موثوقين.
  - تسجيل التطبيقات في قاعدة بيانات التطبيقات الموثوقة الخاصة بشبكة Kaspersky Security Network.
  - وضع المستخدم التطبيق في المجموعة الموثوقة.

  لم يتم حظر أية عمليات لهذه التطبيقات.
- **مقيد بشكل منخفض**. تضم هذه المجموعة تطبيقات تم الوفاء بالشروط التالية من أجلها:
  - لم يتم توقيع التطبيقات رقميًا من قبل بائعين موثوقين.
  - لم يتم تسجيل التطبيقات في قاعدة بيانات التطبيقات الموثوقة من Kaspersky Security Network.
  - ضع المستخدم التطبيق في المجموعة "مقيدة بشكل منخفض".

  تخضع مثل هذه التطبيقات للمستوى الأدنى من التقييدات المتعلقة بالوصول إلى موارد نظام التشغيل.
- **مقيد بشكل عالٍ**. تضم هذه المجموعة تطبيقات تم الوفاء بالشروط التالية من أجلها:
  - لم يتم توقيع التطبيقات رقميًا من قبل بائعين موثوقين.
  - لم يتم تسجيل التطبيقات في قاعدة بيانات التطبيقات الموثوقة من Kaspersky Security Network.
  - وضع المستخدم التطبيق في المجموعة "مقيدة بشكل عال".

  تخضع مثل هذه التطبيقات للتقييدات المرتفعة المتعلقة بالوصول إلى موارد نظام التشغيل.
- **غير موثوق**. تضم هذه المجموعة تطبيقات تم الوفاء بالشروط التالية من أجلها:
  - لم يتم توقيع التطبيقات رقميًا من قبل بائعين موثوقين.
  - لم يتم تسجيل التطبيقات في قاعدة بيانات التطبيقات الموثوقة من Kaspersky Security Network.
  - وضع المستخدم التطبيق في المجموعة غير الموثوقة.

  يتم منع جميع العمليات لهذه التطبيقات.

الملحق رقم 3. امتدادات الملفات لفحص محركات الأقراص القابلة للإزالة

com – ملف تنفيذي لتطبيق لا يزيد حجمه عن 64 كيلو بايت

exe - ملف تنفيذي أو أرشيف ذاتي الاستخراج

sys - ملف نظام Microsoft Windows

prg - نص خاص ببرامج ™dBase أو Clipper أو ®Microsoft Visual FoxPro أو WAVmaker

bin - ملف ثنائي

bat - ملف دفعي

cmd - ملف الأوامر الخاص بنظام التشغيل Microsoft Windows NT (يشبه ملف bat الخاص بنظام DOS)، ونظام التشغيل OS/2

dpl - مكتبة Borland Delphi المضغوطة

dll - مكتبة الرابط الديناميكية

scr - شاشة Microsoft Windows التمهيدية

cpl - وحدة لوحة تحكم Microsoft Windows

ocx - كائن Microsoft OLE (ربط وتضمين الكائن)

tsp - برنامج يعمل في وضع التوقيت المقسم

drv - برنامج تشغيل الأجهزة

vxd - برنامج تشغيل جهاز افتراضي لنظام التشغيل Microsoft Windows

pif - ملف معلومات البرنامج

lnk - ملف ارتباط نظام التشغيل Microsoft Windows

reg - ملف مفتاح تسجيل نظام Microsoft Windows

ini - ملف تكوين يحتوي على بيانات تكوين لنظام تشغيل Microsoft Windows وWindows NT وبعض التطبيقات الأخرى

cla - فئة جافا

vbs - البرنامج ®النصي للغة Visual Basic

vbe - امتداد فيديو BIOS

js، jse – نص مصدر لغة JavaScript

htm - وثيقة ارتباط تشعبي

htt - رأس ارتباط تشعبي لنظام Microsoft Windows

hta - برنامج ارتباط تشعبي لبرنامج ®Microsoft Internet Explorer

asp - برنامج نصي فعال لصفحات الخادم

chm - ملف HTML مجمع

pht – ملف HTML به برامج PHP نصية

php - برنامج نصي مدمج في ملفات HTML

wsh - ملف استضافة البرنامج النصي لنظام Microsoft Windows

wsf - برنامج نصي لنظام Microsoft Windows

the - ملف صورة خلفية نظام التشغيل Microsoft Windows 95

hlp - ملف Win Help

msg – رسالة بريد إلكتروني Microsoft Mail

plg - رسالة بريد إلكتروني

mbx – رسالة بريد إلكتروني Microsoft Office Outlook المحفوظة

*doc - مستندات Microsoft Office Word، مثل: doc لمستند Microsoft Office Word، وdocx - لمستند Microsoft Office Word 2007 مع دعم XML، وdocm - لمستند Microsoft Office Word 2007 مع دعم الماكرو

*dot - قوالب مستندات Microsoft Office Word، مثل: dot لقوالب مستندات Microsoft Office Word، وdotx لقوالب مستندات Microsoft Office Word 2007، وdotm لقوالب مستندات Microsoft Office Word 2007 مع دعم الماكرو

fpm - برنامج قاعدة بيانات وملف بدء لبرنامج Microsoft Visual FoxPro

rtf - مستند بتنسيق Rich Text Format

shs - جزء معالج كائنات الملفات المؤقتة الخاصة بـ Windows

dwg - قاعدة بيانات رسم AutoCAD®

msi - حزمة مثبت Microsoft Windows

otm - مشروع VBA الخاص بتطبيق Microsoft Office Outlook

pdf - مستند Adobe Acrobat

swf - كائن حزمة Shockwave® Flash

jpg، jpeg – تنسيق رسومات الصورة المضغوط

emf – ملف تنسيق Enhanced Metafile

ico - ملف رمز الكائن

ov? – ملفات Microsoft Office Word التنفيذية

*xl - مستندات وملفات Microsoft Office Excel، مثل: xla – امتداد Microsoft Office Excel، xlc – وxlc للمخططات – وxlt لقوالب المستندات، وxlsx لمصنف Microsoft Office Excel 2007 – وxltm -لمصنف Microsoft Office Excel 2007 مع دعم الماكرو، xlsb – مصنف Microsoft Office Excel 2007 بتنسيق ثنائي (ليس xltx، (XML – قالب Microsoft Office Excel 2007، xlsm – قالب Microsoft Office Excel 2007 مع دعم الماكرو، xlam – للمكونات إضافية الخاصة بتطبيق Microsoft Office Excel 2007 مع دعم الماكرو

*pp - مستندات وملفات ®Microsoft Office PowerPoint، مثل: pps – لشرائح Microsoft Office PowerPoint – وppt للعروض التقديمية وpptx – للعرض التقديمي لتطبيق Microsoft Office PowerPoint 2007 وpptm – للعروض التقديمية لتطبيقMicrosoft Office PowerPoint 2007 مع دعم الماكرو، وpotx – لقوالب العروض التقديمية لتطبيق Microsoft Office PowerPoint 2007، وpotm – لقوالب العروض التقديمية Microsoft Office PowerPoint 2007 مع دعم الماكرو، ppsx – لعرض شرائح Microsoft Office PowerPoint 2007، وpotm – لعرض شرائح Microsoft Office PowerPoint 2007 مع دعم الماكرو، ppam – للمكونات الإضافيةMicrosoft Office PowerPoint 2007 مع دعم الماكرو

*md – مستندات وملفات ®Microsoft Office Access، مثل: mda لمجموعات عمل Microsoft Office Access وmdb لقواعد البيانات

sldx – عرض شرائح Microsoft PowerPoint 2007

sldm – عرض شرائح Microsoft PowerPoint 2007 مع دعم الماكرو

thmx – سمة تطبيق Microsoft Office 2007

الملحق رقم 4. نوع الملف لعامل تهديدات للحماية من تهديدات البريد

لاحظ أن التنسيق الفعلي للملف قد لا يتوافق مع ملحق اسم الملف.

إذا قمت بتمكين تصفية مرفقات البريد الإلكتروني، فإن مكون الحماية من تهديدات البريد قد يعيد تسمية الملفات أو حذفها بالملحقات التالية:

com - ملف تنفيذي لتطبيق لا يزيد حجمه عن 64 كيلو بايت

exe - ملف تنفيذي أو أرشيف ذاتي الاستخراج

sys - ملف نظام Microsoft Windows

prg - نص خاص ببرامج ™dBase أو Clipper أو ®Microsoft Visual FoxPro أو WAVmaker

bin - ملف ثنائي

bat - ملف دفعي

cmd - ملف الأوامر الخاص بنظام التشغيل Microsoft Windows NT (يشبه ملف bat الخاص بنظام DOS)، ونظام التشغيل OS/2

dpl - مكتبة Borland Delphi المضغوطة

dll - مكتبة الرابط الديناميكية

scr - شاشة Microsoft Windows التمهيدية

cpl - وحدة لوحة تحكم Microsoft Windows

ocx - كائن Microsoft OLE (ربط وتضمين الكائن)

tsp - برنامج يعمل في وضع التوقيت المقسم

drv - برنامج تشغيل الأجهزة

vxd - برنامج تشغيل جهاز افتراضي لنظام التشغيل Microsoft Windows

pif - ملف معلومات البرنامج

lnk - ملف ارتباط نظام التشغيل Microsoft Windows

reg - ملف مفتاح تسجيل نظام Microsoft Windows

ini - ملف تكوين يحتوي على بيانات تكوين لنظام تشغيل Microsoft Windows وWindows NT وبعض التطبيقات الأخرى

cla - فئة جافا

vbs - البرنامج ®النصي للغة Visual Basic

vbe - امتداد فيديو BIOS

js، jse – نص مصدر لغة JavaScript

htm - وثيقة ارتباط تشعبي

htt - رأس ارتباط تشعبي لنظام Microsoft Windows

hta - برنامج ارتباط تشعبي لبرنامج ®Microsoft Internet Explorer

asp - برنامج نصي فعال لصفحات الخادم

chm - ملف HTML مجمع

pht – ملف HTML به برامج PHP نصية

php - برنامج نصي مدمج في ملفات HTML

wsh - ملف استضافة البرنامج النصي لنظام Microsoft Windows

wsf - برنامج نصي لنظام Microsoft Windows

the - ملف صورة خلفية نظام التشغيل Microsoft Windows 95

hlp - ملف Win Help

msg – رسالة بريد إلكتروني Microsoft Mail

plg - رسالة بريد إلكتروني

mbx – رسالة بريد إلكتروني Microsoft Office Outlook المحفوظة

*doc - مستندات Microsoft Office Word، مثل: doc لمستند Microsoft Office Word، وdocx - لمستند Microsoft Office Word 2007 مع دعم XML، وdocm - لمستند Microsoft Office Word 2007 مع دعم الماكرو

*dot - قوالب مستندات Microsoft Office Word، مثل: dot لقوالب مستندات Microsoft Office Word، وdotx لقوالب مستندات Microsoft Office Word 2007، وdotm لقوالب مستندات Microsoft Office Word 2007 مع دعم الماكرو

fpm - برنامج قاعدة بيانات وملف بدء لبرنامج Microsoft Visual FoxPro

rtf - مستند بتنسيق Rich Text Format

shs - جزء معالج كائنات الملفات المؤقتة الخاصة بـ Windows

dwg - قاعدة بيانات رسم AutoCAD®

msi - حزمة مثبت Microsoft Windows

otm - مشروع VBA الخاص بتطبيق Microsoft Office Outlook

pdf - مستند Adobe Acrobat

swf - كائن حزمة Shockwave® Flash

jpg، jpeg – تنسيق رسومات الصورة المضغوط

emf – ملف تنسيق Enhanced Metafile

ico - ملف رمز الكائن

ov? – ملفات Microsoft Office Word التنفيذية

*xl - مستندات وملفات Microsoft Office Excel، مثل: xla – امتداد Microsoft Office Excel، xlc – وxlc للمخططات – وxlt لقوالب المستندات، وxlsx لمصنف Microsoft Office Excel 2007 – وxltm -لمصنف Microsoft Office Excel 2007 مع دعم الماكرو، xlsb – مصنف Microsoft Office Excel 2007 بتنسيق ثنائي (ليس xltx، (XML – قالب Microsoft Office Excel 2007، xlsm – قالب Microsoft Office Excel 2007 مع دعم الماكرو، xlam – للمكونات إضافية الخاصة بتطبيق Microsoft Office Excel 2007 مع دعم الماكرو

*pp - مستندات وملفات ®Microsoft Office PowerPoint، مثل: pps – لشرائح Microsoft Office PowerPoint – وppt للعروض التقديمية وpptx – للعرض التقديمي لتطبيق Microsoft Office PowerPoint 2007 وpptm – للعروض التقديمية لتطبيقMicrosoft Office PowerPoint 2007 مع دعم الماكرو، وpotx – لقوالب العروض التقديمية لتطبيق Microsoft Office PowerPoint 2007، وpotm – لقوالب العروض التقديمية Microsoft Office PowerPoint 2007 مع دعم الماكرو، ppsx – لعرض شرائح Microsoft Office PowerPoint 2007، وpotm – لعرض شرائح Microsoft Office PowerPoint 2007 مع دعم الماكرو، ppam – للمكونات الإضافيةMicrosoft Office PowerPoint 2007 مع دعم الماكرو

*md – مستندات وملفات ®Microsoft Office Access، مثل: mda لمجموعات عمل Microsoft Office Access وmdb لقواعد البيانات

sldx – عرض شرائح Microsoft PowerPoint 2007

sldm – عرض شرائح Microsoft PowerPoint 2007 مع دعم الماكرو

thmx – سمة تطبيق Microsoft Office 2007

الملحق رقم 5. إعدادات الشبكة للتفاعل مع الخدمات الخارجية

يستخدم Kaspersky Endpoint Security إعدادات الشبكة التالية للتفاعل مع الخدمات الخارجية.

إعدادات الشبكة

العنوان	الوصف
`activation-v2.kaspersky.com/activationservice/activationservice.svc` البروتوكول: `HTTPS` المنفذ: `443`	تفعيل التطبيق.

s00.upd.kaspersky.com s01.upd.kaspersky.com s02.upd.kaspersky.com s03.upd.kaspersky.com s04.upd.kaspersky.com s05.upd.kaspersky.com s06.upd.kaspersky.com s07.upd.kaspersky.com s08.upd.kaspersky.com s09.upd.kaspersky.com s10.upd.kaspersky.com s11.upd.kaspersky.com s12.upd.kaspersky.com s13.upd.kaspersky.com s14.upd.kaspersky.com s15.upd.kaspersky.com s16.upd.kaspersky.com s17.upd.kaspersky.com s18.upd.kaspersky.com s19.upd.kaspersky.com cm.k.kaspersky-labs.com البروتوكول: HTTPS المنفذ: 443	تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق.
downloads.upd.kaspersky.com البروتوكول: HTTPS المنفذ: 443	• تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق. • التحقق من الوصول إلى خوادم Kaspersky. وإذا لم يكن الوصول إلى الخوادم باستخدام DNS النظام ممكنًا، فسوف يستخدم التطبيق DNS العام. وهذا ضروري للتأكد من تحديث قواعد بيانات مكافحة الفيروسات والحفاظ على مستوى الأمان للكمبيوتر. ويستخدم Kaspersky Endpoint Security قائمة خوادم DNS العامة التالية بالترتيب التالي: 1. Google Public DNS (8.8.8.8). 2. Cloudflare DNS (1.1.1.1). 3. Alibaba Cloud DNS (223.6.6.6). 4. Quad9 DNS (9.9.9.9). 5. CleanBrowsing (185.228.168.168).

	قد تحتوي الطلبات الصادرة عن التطبيق على عناوين المجالات وعنوان IP العام للمستخدم لأن التطبيق ينشئ اتصال TCP/UDP مع خادم DNS. وتكون هذه المعلومات مطلوبة، على سبيل المثال، للتحقق من صحة شهادة مورد ويب عند استخدام HTTPS. وإذا كان Kaspersky Endpoint Security يستخدم خادم DNS عام، فإن معالجة البيانات تخضع لسياسة الخصوصية الخاصة بالخدمة ذات الصلة. وإذا كنت تريد منع Kaspersky Endpoint Security من استخدام خادم DNS عام، اتصل بالدعم الفني للحصول على تصحيح خاص.
touch.kaspersky.com البروتوكول: HTTP	• تلقي الوقت الموثوق به للتحقق من فترة صلاحية الشهادة (اتصال TLS). • تحذير بشأن رفض الوصول إلى مورد ويب في المستعرض عند تشغيل الحماية من تهديدات الويب.
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com	تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق.

cm.k.kaspersky-labs.com البروتوكول: HTTP المنفذ: 80	
ds.kaspersky.com البروتوكول: HTTPS المنفذ: 443	استخدام Kaspersky Security Network.
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com البروتوكول: أي المنفذ: 443، 1443	استخدام Kaspersky Security Network.
click.kaspersky.com redirect.kaspersky.com البروتوكول: HTTPS	اتباع الروابط من الواجهة.

الإعدادات، المستخدمة للتشفير

العنوان	الوصف
crl.kaspersky.com ocsp.kaspersky.com البروتوكول: HTTP المنفذ: 80	البنية التحتية للمفتاح العام (PKI).

الملحق رقم 6. أحداث التطبيق

يتم تسجيل معلومات حول تشغيل كل مكون من مكونات Kaspersky Endpoint Security، وحالات تشفير البيانات، وإكمال كل مهمة فحص للبرامج الضارة، ومهمة التحديث، ومهمة التحقق من السلامة، والتشغيل الإجمالي للتطبيق في سجل أحداث Kaspersky Security Center وسجل أحداث Windows.

يُنشئ Kaspersky Endpoint Security أحداثًا من الأنواع التالية: أحداث عامة وأحداث محددة. يتم إنشاء أحداث معينة فقط بواسطة Kaspersky Endpoint Security for Windows. وتحتوي الأحداث المحددة على معرّف بسيط، مثل 000000cb. تحتوي الأحداث المحددة على المعلمات التالية:

- GNRL_EA_DESCRIPTION هو محتوى الحدث.
- GNRL_EA_ID هو معرف خدمة الحدث.
- GNRL_EA_SEVERITY هو حالة الحدث. 1 – رسالة إعلامية، 2 – تحذير، 3 – خلل وظيفي، 4 – حرج.
- EVENT_TYPE_DISPLAY_NAME هو عنوان الحدث.

- `TASK_DISPLAY_NAME` هو اسم مكون التطبيق الذي بدأ الحدث.

يمكن إنشاء الأحداث العامة بواسطة Kaspersky Endpoint Security for Windows بالإضافة إلى تطبيقات Kaspersky الأخرى (على سبيل المثال، Kaspersky Security for Windows Server). وتحتوي الأحداث العامة على معرّف أكثر تعقيدًا، مثل `GNRL_EV_VIRUS_FOUND`. وبالإضافة إلى الإعدادات المطلوبة، تحتوي الأحداث العامة على إعدادات متقدمة.

حرج

End User License Agreement violated

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	201
معرف حدث Kaspersky Security Center	GNRL_EV_LICENSE_EXPIRATION
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

License has almost expired

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	203
معرف حدث Kaspersky Security Center	000000cb
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Databases are missing or corrupted

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	206
معرف حدث Kaspersky Security Center	000000ce
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Databases are extremely out of date

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	207
معرف حدث Kaspersky Security Center	000000cf
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application autorun is disabled

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	209
معرف حدث Kaspersky Security Center	000000d1
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Activation error

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	229
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Active threat detected. Advanced Disinfection should be started

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	231
معرف حدث Kaspersky Security Center	000000e7
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

KSN servers unavailable

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	2023
معرف حدث Kaspersky Security Center	000007e7
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Not enough space in Quarantine storage

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	343
معرف حدث Kaspersky Security Center	00000157
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object not restored from Quarantine

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	346
معرف حدث Kaspersky Security Center	0000015a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object not deleted from Quarantine

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	348
معرف حدث Kaspersky Security Center	0000015c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The application established a connection to a website with an untrusted certificate

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	57
معرف حدث Kaspersky Security Center	00000039
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The domain is added to the list of exclusions .Failed to verify an encrypted connection

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	60
معرف حدث Kaspersky Security Center	0000003c
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Malicious object detected (local bases)

الحالة	!
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI منع اختراق المضيف اكتشاف السلوك منع الاستغلال فحص البرامج الضارة
معرف حدث Windows	302
معرف حدث Kaspersky Security Center	GNRL_EV_VIRUS_FOUND
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. عند اكتشاف تشفير خارجي للمجلدات المشتركة، يعرض التطبيق المسار إلى الملف الهدف. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Malicious object detected (KSN)

الحالة	!
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI منع اختراق المضيف اكتشاف السلوك منع الاستغلال فحص البرامج الضارة
معرف حدث Windows	302
معرف حدث Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_BY_KSN
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Disinfection impossible

الحالة	⚠
المكون	الحماية من تهديدات الملفات الحماية من تهديدات البريد منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	312
معرف حدث Kaspersky Security Center	GNRL_EV_OBJECT_NOTCURED
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Cannot be deleted

الحالة	⚠
المكون	الحماية من تهديدات الملفات منع اختراق المضيف اكتشاف السلوك فحص البرامج الضارة
معرف حدث Windows	313
معرف حدث Kaspersky Security Center	00000139
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Processing error

الحالة	!
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد منع اختراق المضيف حماية AMSI فحص البرامج الضارة
معرف حدث Windows	317
معرف حدث Kaspersky Security Center	0000013d
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Process terminated

الحالة	!
المكون	الحماية من تهديدات الملفات منع اختراق المضيف اكتشاف السلوك فحص البرامج الضارة
معرف حدث Windows	452
معرف حدث Kaspersky Security Center	000001c4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Unable to terminate process

الحالة	!
المكون	الحماية من تهديدات الملفات منع اختراق المضيف اكتشاف السلوك فحص البرامج الضارة
معرف حدث Windows	453
معرف حدث Kaspersky Security Center	000001c5
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Dangerous link blocked

الحالة	!
المكون	الحماية من تهديدات الويب
معرف حدث Windows	362
معرف حدث Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
معلمات الحدث	• GNRL_EA_PARAM_2 هو المسار إلى الكائن. • GNRL_EA_PARAM_5 هو اسم الكائن وفقًا لتصنيف Kaspersky. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة KSN الخاصة (true: أو denylist) false.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Dangerous link opened

الحالة	!
المكون	الحماية من تهديدات الويب
معرف حدث Windows	363
معرف حدث Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_REPORTED
معلمات الحدث	• GNRL_EA_PARAM_2 هو المسار إلى الكائن. • GNRL_EA_PARAM_5 هو اسم الكائن وفقًا لتصنيف Kaspersky. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة KSN الخاصة (true: أو denylist): false.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Previously opened dangerous link detected

الحالة	❗
المكون	الحماية من تهديدات الويب
معرف حدث Windows	1201
معرف حدث Kaspersky Security Center	GNRL_EV_VIRUS_FOUND_AND_PASSED
معلمات الحدث	• GNRL_EA_PARAM_2 هو المسار إلى الكائن. • GNRL_EA_PARAM_5 هو اسم الكائن وفقًا لتصنيف Kaspersky. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة KSN الخاصة (true: أو denylist): false.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Process action blocked

الحالة	!
المكون	مراقبة عيوب التكيف
معرف حدث Windows	2200
معرف حدث Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
معلمات الحدث	• GNRL_EA_PARAM_1 هو اسم قاعدة مراقبة عيوب التكيف. • GNRL_EA_PARAM_2 هو معرف القاعدة المساعدة على الاكتشاف. • GNRL_EA_PARAM_3 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_4 هو اسم العملية المصدر. • GNRL_EA_PARAM_5 هو الكائن المصدر. • GNRL_EA_PARAM_6 هو العملية الهدف. • GNRL_EA_PARAM_7 هو الكائن الهدف. • GNRL_EA_PARAM_8 هي معلومات إضافية حول الكائن المكتشف: تجزئات العملية المصدر / عملية الكائن والهدف / الكائن. تم منع العملية (verdict_type: true أو false. معرف أمان المستخدم (SID).
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Keyboard not authorized

الحالة	!
المكون	منع هجمات BadUSB
معرف حدث Windows	2051
معرف حدث Kaspersky Security Center	00000803
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

AMSI request was blocked

الحالة	!
المكون	حماية AMSI
معرف حدث Windows	2200
معرف حدث Kaspersky Security Center	00000898
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network activity blocked

الحالة	!
المكون	جدار الحماية
معرف حدث Windows	602
معرف حدث Kaspersky Security Center	00000329
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network attack detected

الحالة	!
المكون	الحماية من تهديدات الشبكة
معرف حدث Windows	651
معرف حدث Kaspersky Security Center	GNRL_EV_ATTACK_DETECTED
معلمات الحدث	• GNRL_EA_PARAM_1 هو اسم الهجوم. • GNRL_EA_PARAM_2 هو البروتوكول. • GNRL_EA_PARAM_3 هو عنوان IP الكمبيوتر الذي يعمل كمصدر لهجوم الشبكة. ويشار إلى عنوان IP بترتيب بايت المضيف. على سبيل المثال، 2886729929 لأجل 172.16.0.201. • GNRL_EA_PARAM_4 هو رقم المنفذ. • GNRL_EA_PARAM_5 هو عنوان IPv6، على سبيل المثال، 12B012B012B012B012B012B012B012B0. • GNRL_EA_PARAM_6 هو عنوان IP الكمبيوتر المستهدف بهجوم الشبكة. ويشار إلى عنوان IP بترتيب بايت المضيف. على سبيل المثال، 2886729929 لأجل 172.16.0.201.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application startup prohibited

الحالة	❗
المكون	التحكم في التطبيقات
معرف حدث Windows	702
معرف حدث Kaspersky Security Center	GNRL_EV_APPLICATION_LAUNCH_DENIED
معلمات الحدث	• GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو معرف الفئة الذي تم إنشاؤه يدويًا. • GNRL_EA_PARAM_4 هو معرف فئة التطبيق. • GNRL_EA_PARAM_5 هو معلومات عن التوقيع الرقمي للتطبيق. • GNRL_EA_PARAM_6 هو اسم الملف القابل للتنفيذ للتطبيق (على سبيل المثال، chrome.exe). • GNRL_EA_PARAM_7 هو المسار إلى الملف القابل للتنفيذ. • GNRL_EA_PARAM_8 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_9 هو إصدار التطبيق الذي يحاول المستخدم تشغيله.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Prohibited process was started before Kaspersky Endpoint Security startup

الحالة	❗
المكون	التحكم في التطبيقات
معرف حدث Windows	710
معرف حدث Kaspersky Security Center	000002c6
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Access denied (local bases)

الحالة	⚠
المكون	التحكم في الويب
معرف حدث Windows	752
معرف حدث Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED
معلمات الحدث	• GNRL_EA_PARAM_1 هو عنوان موقع الويب. • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو اسم قاعدة التحكم في الويب.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Access denied (KSN)

الحالة	⚠
المكون	التحكم في الويب
معرف حدث Windows	752
معرف حدث Kaspersky Security Center	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
معلمات الحدث	• GNRL_EA_PARAM_1 هو عنوان موقع الويب. • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو اسم قاعدة التحكم في الويب.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Operation with the device prohibited

الحالة	!
المكون	التحكم في الجهاز
معرف حدث Windows	802
معرف حدث Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
معلمات الحدث	• GNRL_EA_PARAM_1 هو معرف الجهاز (HWID). • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network connection blocked

الحالة	!
المكون	التحكم في الجهاز
معرف حدث Windows	809
معرف حدث Kaspersky Security Center	00000329
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error updating component

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1011
معرف حدث Kaspersky Security Center	000003f3
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error distributing component updates

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1012
معرف حدث Kaspersky Security Center	000003f4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Local update error

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1014
معرف حدث Kaspersky Security Center	000003f6
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Network update error

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1015
معرف حدث Kaspersky Security Center	000003f7
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Cannot start two tasks at the same time

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1017
معرف حدث Kaspersky Security Center	000003f9
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error verifying application databases and modules

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1018
معرف حدث Kaspersky Security Center	000003fa
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error in interaction with Kaspersky Security Center

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1019
معرف حدث Kaspersky Security Center	000003fb
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Not all components were updated

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1021
معرف حدث Kaspersky Security Center	000003fd
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Update completed successfully, update distribution failed

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1023
معرف حدث Kaspersky Security Center	000003ff
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Internal task error

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	101
معرف حدث Kaspersky Security Center	00000065
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Patch installation failed

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	2153
معرف حدث Kaspersky Security Center	00000869
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Patch rollback failed

الحالة	!
المكون	تحديث قاعدة البيانات
معرف حدث Windows	2156
معرف حدث Kaspersky Security Center	0000086c
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error applying file encryption / decryption rules

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	904
معرف حدث Kaspersky Security Center	00000388
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File encryption / decryption error

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	912
معرف حدث Kaspersky Security Center	GNRL_EV_ENCRYPTION_ERROR
معلمات الحدث	• GNRL_EA_PARAM_1 هو المسار إلى الملف. • GNRL_EA_PARAM_2 هو سبب الخطأ. • GNRL_EA_PARAM_3 هو نوع الجهاز.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File access blocked

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	940
معرف حدث Kaspersky Security Center	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
معلمات الحدث	• GNRL_EA_PARAM_1 هو الكائن الهدف. • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو اسم الملف القابل للتنفيذ للتطبيق (على سبيل المثال، chrome.exe)، الذي يحاول اكتساب الوصول إلى الملف.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Error enabling portable mode

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	951
معرف حدث Kaspersky Security Center	000003b7
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error disabling portable mode

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	953
معرف حدث Kaspersky Security Center	000003b9
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error creating encrypted package

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	931
معرف حدث Kaspersky Security Center	000003a3
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error encrypting / decrypting device

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	1305
معرف حدث Kaspersky Security Center	00000519
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Could not load encryption module

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	1311
معرف حدث Kaspersky Security Center	0000051f
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The task for managing Authentication Agent accounts ended with an error

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	1340
معرف حدث Kaspersky Security Center	0000053c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Policy cannot be applied

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	1312
معرف حدث Kaspersky Security Center	00000520
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

FDE upgrade failed

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	1342
معرف حدث Kaspersky Security Center	0000053e
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

FDE upgrade rollback failed (for more information, please refer to the Kaspersky Endpoint Security for Windows Online Help)

الحالة	!
المكون	تشفير البيانات
معرف حدث Windows	1344
معرف حدث Kaspersky Security Center	00000540
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Kaspersky Anti Targeted Attack Platform server unavailable

الحالة	!
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2100
معرف حدث Kaspersky Security Center	00000834
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Failed to delete object

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2252
معرف حدث Kaspersky Security Center	000008cc
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object not quarantined (Kaspersky Sandbox)

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2603
معرف حدث Kaspersky Security Center	00000a2b
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

An internal error occurred

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2607
معرف حدث Kaspersky Security Center	00000a2f
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid Kaspersky Sandbox server certificate

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2613
معرف حدث Kaspersky Security Center	00000a35
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The Kaspersky Sandbox node is unavailable

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2614
معرف حدث Kaspersky Security Center	00000a36
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

An error occurred while processing the object in Kaspersky Sandbox

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2617
معرف حدث Kaspersky Security Center	00000a39
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Maximum load to Kaspersky Sandbox is exceeded

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2618
معرف حدث Kaspersky Security Center	00000a3a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

IOC found

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2651
معرف حدث Kaspersky Security Center	00000a5b
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Kaspersky Sandbox license verification failed

الحالة	!
المكون	Kaspersky Sandbox
معرف حدث Windows	2620
معرف حدث Kaspersky Security Center	00000a3c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object startup blocked

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2553
معرف حدث Kaspersky Security Center	000009f9
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Process startup blocked

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2551
معرف حدث Kaspersky Security Center	000009f7
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Script execution blocked

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2559
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object not quarantined (Endpoint Detection and Response)

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2556
معرف حدث Kaspersky Security Center	000009fc
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Process startup is not blocked

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2561
معرف حدث Kaspersky Security Center	00000a01
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object is not blocked

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2562
معرف حدث Kaspersky Security Center	00000a02
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Script execution is not blocked

الحالة	!
المكون	Endpoint Detection and Response
معرف حدث Windows	2563
معرف حدث Kaspersky Security Center	00000a03
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error changing application components

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	1401
معرف حدث Kaspersky Security Center	00000579
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

There are patterns of a possible brute-force attack in the system

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2800
معرف حدث Kaspersky Security Center	00000af0
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

There are patterns of a possible Windows Event Log abuse

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2801
معرف حدث Kaspersky Security Center	00000af1
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Atypical actions detected on behalf of a new service installed

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2802
معرف حدث Kaspersky Security Center	00000af2
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Atypical logon that uses explicit credentials detected

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2803
معرف حدث Kaspersky Security Center	00000af3
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

There are patterns of a possible Kerberos forged PAC (MS14-068) attack in the system

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2804
معرف حدث Kaspersky Security Center	00000af4
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Suspicious changes detected in the privileged built-in Administrators group

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2805
معرف حدث Kaspersky Security Center	00000af5
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

There is an atypical activity detected during a network logon session

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2806
معرف حدث Kaspersky Security Center	00000af6
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Log Inspection rule triggered

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2807
معرف حدث Kaspersky Security Center	00000af7
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Event aggregation started .Atypical event occurs too often

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2808
معرف حدث Kaspersky Security Center	00000af8
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Report on an atypical event for the aggregation period

الحالة	!
المكون	فحص السجل
معرف حدث Windows	2809
معرف حدث Kaspersky Security Center	00000af9
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error connecting to the Kaspersky Anti Targeted Attack Platform server

الحالة	!
المكون	(EDR (KATA
معرف حدث Windows	2850
معرف حدث Kaspersky Security Center	00000b22
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid Kaspersky Anti Targeted Attack Platform server certificate

الحالة	!
المكون	(EDR (KATA
معرف حدث Windows	2851
معرف حدث Kaspersky Security Center	00000b23
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid certificate of the agent on the Kaspersky Anti Targeted Attack Platform server

الحالة	!
المكون	(EDR (KATA
معرف حدث Windows	2852
معرف حدث Kaspersky Security Center	00000b24
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

خلل وظيفي

Task cannot be performed

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	212
معرف حدث Kaspersky Security Center	000000d4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid task settings. Settings not applied

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	707
معرف حدث Kaspersky Security Center	000002c3
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تحذير

Application crashed during previous session

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	237
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

License expires soon

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	204
معرف حدث Kaspersky Security Center	000000cc
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Databases are out of date

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	208
معرف حدث Kaspersky Security Center	000000d0
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Automatic updates are disabled

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	210
معرف حدث Kaspersky Security Center	000000d2
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Self-Defense is disabled

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	211
معرف حدث Kaspersky Security Center	000000d3
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Protection components are disabled

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	214
معرف حدث Kaspersky Security Center	000000d6
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Computer is running in safe mode

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	215
معرف حدث Kaspersky Security Center	000000d7
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

There are unprocessed files

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	216
معرف حدث Kaspersky Security Center	000000d8
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Group policy applied

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	219
معرف حدث Kaspersky Security Center	000000db
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Task stopped

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	222
معرف حدث Kaspersky Security Center	000000de
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Quit and reopen the application to complete updating

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	224
معرف حدث Kaspersky Security Center	0000057b
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Computer restart required

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	225
معرف حدث Kaspersky Security Center	000000e1
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The license allows the use of components that have not been installed

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	226
معرف حدث Kaspersky Security Center	000000e2
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Advanced Disinfection started

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	232
معرف حدث Kaspersky Security Center	000000e8
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Advanced Disinfection completed

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	233
معرف حدث Kaspersky Security Center	000000e9
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Incorrect reserve key

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	230
معرف حدث Kaspersky Security Center	000000e6
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Subscription expires soon

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	240
معرف حدث Kaspersky Security Center	000000f0
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

ممنوع

الحالة	⚠
المكون	اكتشاف السلوك منع الاستغلال الحماية من تهديدات الويب
معرف حدث Windows	331
معرف حدث Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. عند اكتشاف تشفير خارجي للمجلدات المشتركة، يعرض التطبيق المسار إلى الملف الهدف. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Cannot restore object from Backup

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	336
معرف حدث Kaspersky Security Center	00000150
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Suspicious network activity detected

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	2001
معرف حدث Kaspersky Security Center	000007d1
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Encrypted connection terminated

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	250
معرف حدث Kaspersky Security Center	000007d3
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Participation in KSN disabled

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	2021
معرف حدث Kaspersky Security Center	000007e5
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Processing of some OS functions is disabled

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	245
معرف حدث Kaspersky Security Center	000000f5
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Quarantine storage is almost out of space

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	344
معرف حدث Kaspersky Security Center	00000158
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network connection blocked

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	809
معرف حدث Kaspersky Security Center	00000abe
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Cannot create a backup copy

الحالة	⚠
المكون	الحماية من تهديدات الملفات اكتشاف السلوك منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	310
معرف حدث Kaspersky Security Center	00000136
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object not processed

الحالة	⚠
المكون	الحماية من تهديدات الملفات الحماية من تهديدات البريد منع اختراق المضيف حماية AMSI فحص البرامج الضارة
معرف حدث Windows	314
معرف حدث Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object encrypted

الحالة	⚠
المكون	منع اختراق المضيف
معرف حدث Windows	320
معرف حدث Kaspersky Security Center	00000140
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Object corrupted

الحالة	⚠
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	321
معرف حدث Kaspersky Security Center	00000141
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Legitimate software that can be used by intruders to damage your computer or personal data was detected (local bases)

الحالة	⚠
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد منع اختراق المضيف حماية AMSI اكتشاف السلوك فحص البرامج الضارة
معرف حدث Windows	303
معرف حدث Kaspersky Security Center	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Legitimate software that can be used by intruders to damage your computer or personal data was detected (KSN)

الحالة	⚠
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد منع اختراق المضيف حماية AMSI اكتشاف السلوك فحص البرامج الضارة
معرف حدث Windows	303
معرف حدث Kaspersky Security Center	GNRL_EV_SUSPICIOUS_OBJECT_FOUND
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object deleted

الحالة	⚠
المكون	الحماية من تهديدات الملفات الحماية من تهديدات البريد منع اختراق المضيف منع الاستغلال اكتشاف السلوك فحص البرامج الضارة
معرف حدث Windows	307
معرف حدث Kaspersky Security Center	GNRL_EV_OBJECT_DELETED
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object disinfected

الحالة	⚠
المكون	الحماية من تهديدات الملفات الحماية من تهديدات البريد منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	306
معرف حدث Kaspersky Security Center	GNRL_EV_OBJECT_CURED
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال، Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network true (denylist): أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object will be disinfected on restart

الحالة	⚠
المكون	منع اختراق المضيف الحماية من تهديدات الملفات فحص البرامج الضارة
معرف حدث Windows	324
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Object will be deleted on restart

الحالة	⚠
المكون	اكتشاف السلوك منع الاستغلال منع اختراق المضيف الحماية من تهديدات الملفات فحص البرامج الضارة
معرف حدث Windows	323
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Object deleted according to settings

الحالة	⚠
المكون	الحماية من تهديدات البريد
معرف حدث Windows	342
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Rollback completed

الحالة	⚠
المكون	الحماية من تهديدات الملفات اكتشاف السلوك منع الاستغلال فحص البرامج الضارة
معرف حدث Windows	455
معرف حدث Kaspersky Security Center	000001c7
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object download was blocked

الحالة	⚠
المكون	الحماية من تهديدات الويب
معرف حدث Windows	341
معرف حدث Kaspersky Security Center	GNRL_EV_OBJECT_BLOCKED
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Keyboard authorization error

الحالة	⚠
المكون	منع هجمات BadUSB
معرف حدث Windows	2052
معرف حدث Kaspersky Security Center	00000804
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The object scan result has been sent to a third-party application

الحالة	⚠
المكون	حماية AMSI
معرف حدث Windows	1512
معرف حدث Kaspersky Security Center	GNRL_EV_OBJECT_REPORTED
معلمات الحدث	• GNRL_EA_PARAM_1 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_5 هو اسم التهديد وفقًا لتصنيف Kaspersky، على سبيل المثال EICAR-Test-File. • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_8 هو نوع التهديد، على سبيل المثال Trojware. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة Kaspersky Private Security Network (denylist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Task settings applied successfully

الحالة	⚠
المكون	التحكم في التطبيقات
معرف حدث Windows	708
معرف حدث Kaspersky Security Center	000002c4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Warning about undesirable content (local bases)

الحالة	⚠
المكون	التحكم في الويب
معرف حدث Windows	708
معرف حدث Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
معلمات الحدث	• GNRL_EA_PARAM_1 هو عنوان موقع الويب. • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو اسم قاعدة التحكم في الويب.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Warning about undesirable content (KSN)

الحالة	⚠
المكون	التحكم في الويب
معرف حدث Windows	708
معرف حدث Kaspersky Security Center	GNRL_EV_WEB_URL_WARNING
معلمات الحدث	• GNRL_EA_PARAM_1 هو عنوان موقع الويب. • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو اسم قاعدة التحكم في الويب.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Undesirable content was accessed after a warning

الحالة	⚠
المكون	التحكم في الويب
معرف حدث Windows	754
معرف حدث Kaspersky Security Center	000002f2
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Temporary access to the device activated

الحالة	⚠
المكون	التحكم في الجهاز
معرف حدث Windows	803
معرف حدث Kaspersky Security Center	000002f2
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Operation cancelled by the user

الحالة	⚠
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1016
معرف حدث Kaspersky Security Center	000003f8
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

User has opted out of the encryption policy

الحالة	⚠
المكون	تشفير البيانات
معرف حدث Windows	1306
معرف حدث Kaspersky Security Center	0000051a
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Interrupted applying file encryption / decryption rules

الحالة	⚠
المكون	تشفير البيانات
معرف حدث Windows	903
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File encryption / decryption interrupted

الحالة	⚠
المكون	تشفير البيانات
معرف حدث Windows	914
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Device encryption / decryption interrupted

الحالة	⚠
المكون	تشفير البيانات
معرف حدث Windows	1303
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Failed to install or upgrade Kaspersky Disk Encryption drivers in the WinRE image

الحالة	⚠
المكون	تشفير البيانات
معرف حدث Windows	1345
معرف حدث Kaspersky Security Center	00000541
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Module signature check failed

الحالة	⚠
المكون	التحقق من السلامة
معرف حدث Windows	2002
معرف حدث Kaspersky Security Center	000007d2
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application startup was blocked

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2105
معرف حدث Kaspersky Security Center	00000839
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Document opening was blocked

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2106
معرف حدث Kaspersky Security Center	0000083a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Process was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2112
معرف حدث Kaspersky Security Center	00000840
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The application was terminated by the Kaspersky Anti Targeted Attack Platform server administrator

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2113
معرف حدث Kaspersky Security Center	00000841
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File or stream was deleted by the Kaspersky Anti Targeted Attack Platform server administrator

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2111
معرف حدث Kaspersky Security Center	0000083f
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File was restored from quarantine on the Kaspersky Anti Targeted Attack Platform server by the administrator

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2110
معرف حدث Kaspersky Security Center	0000083e
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File was quarantined on the Kaspersky Anti Targeted Attack Platform server by administrator

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2109
معرف حدث Kaspersky Security Center	0000083d
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network activity of all third-party applications is blocked

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2107
معرف حدث Kaspersky Security Center	0000083b
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network activity of all third-party applications is unblocked

الحالة	⚠
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2108
معرف حدث Kaspersky Security Center	0000083c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object will be deleted after restart (Kaspersky Sandbox)

الحالة	⚠
المكون	Kaspersky Sandbox
معرف حدث Windows	2605
معرف حدث Kaspersky Security Center	00000a2d
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Total size of scan tasks exceeded the limit

الحالة	⚠
المكون	Kaspersky Sandbox
معرف حدث Windows	2612
معرف حدث Kaspersky Security Center	00000a34
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object startup allowed, event logged

الحالة	⚠
المكون	Endpoint Detection and Response
معرف حدث Windows	2553
معرف حدث Kaspersky Security Center	000009fa
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Process startup allowed, event logged

الحالة	⚠
المكون	Endpoint Detection and Response
معرف حدث Windows	2554
معرف حدث Kaspersky Security Center	000009f8
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object will be deleted after restart (Endpoint Detection and Response)

الحالة	⚠
المكون	Endpoint Detection and Response
معرف حدث Windows	2558
معرف حدث Kaspersky Security Center	000009fe
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network isolation

الحالة	⚠
المكون	Endpoint Detection and Response
معرف حدث Windows	2700
معرف حدث Kaspersky Security Center	00000a8c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Termination of network isolation

الحالة	⚠
المكون	Endpoint Detection and Response
معرف حدث Windows	2701
معرف حدث Kaspersky Security Center	00000a8d
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Restart required to complete the task

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	225
معرف حدث Kaspersky Security Center	0000057b
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application startup blockage message to administrator

الحالة	⚠
المكون	التحكم في التطبيقات
معرف حدث Windows	503
معرف حدث Kaspersky Security Center	GNRL_EV_AC_USER_REQUEST
معلمات الحدث	• GNRL_EA_DESCRIPTION هي الرسالة إلى المستخدم. • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_6 هو اسم الملف القابل للتنفيذ للتطبيق (على سبيل المثال، chrome.exe). • GNRL_EA_PARAM_7 هو المسار إلى الملف القابل للتنفيذ. • GNRL_EA_PARAM_8 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_9 هو إصدار التطبيق الذي يحاول المستخدم تشغيله.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Device access blockage message to administrator

الحالة	⚠
المكون	التحكم في الجهاز
معرف حدث Windows	804
معرف حدث Kaspersky Security Center	GNRL_EV_DC_USER_REQUEST
معلمات الحدث	• c_er_descr هي الرسالة إلى المستخدم. • GNRL_EA_PARAM_1 هو معرف الجهاز (HWID). • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Web page access blockage message to administrator

الحالة	⚠
المكون	التحكم في الويب
معرف حدث Windows	755
معرف حدث Kaspersky Security Center	GNRL_EV_WC_USER_REQUEST
معلمات الحدث	• GNRL_EA_DESCRIPTION هي الرسالة إلى المستخدم. • GNRL_EA_PARAM_1 هو عنوان موقع الويب. • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Device connection blocked

الحالة	⚠
المكون	التحكم في الجهاز
معرف حدث Windows	807
معرف حدث Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
معلمات الحدث	• GNRL_EA_PARAM_1 هو معرف الجهاز (HWID). • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application activity blockage message to administrator

الحالة	⚠
المكون	مراقبة عيوب التكيف
معرف حدث Windows	503
معرف حدث Kaspersky Security Center	GNRL_EV_ADSEC_USER_REQUEST
معلمات الحدث	• GNRL_EA_DESCRIPTION هي الرسالة إلى المستخدم. • GNRL_EA_PARAM_1 هو اسم قاعدة مراقبة عيوب التكيف. • GNRL_EA_PARAM_2 هو معرف القاعدة المساعدة على الاكتشاف. • GNRL_EA_PARAM_3 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_4 هو اسم العملية المصدر. • GNRL_EA_PARAM_5 هو الكائن المصدر. • GNRL_EA_PARAM_6 هو العملية الهدف. • GNRL_EA_PARAM_7 هو الكائن الهدف. • GNRL_EA_PARAM_8 هي معلومات إضافية حول الكائن المكتشف: تجزئات العملية المصدر / عملية الكائن والهدف / الكائن. تم منع العملية (verdict_type: true أو false. معرف أمان المستخدم (SID).
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File modified

الحالة	⚠
المكون	مراقبة سلامة الملف
معرف حدث Windows	2900
معرف حدث Kaspersky Security Center	00000b54
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Event aggregation started .Object changes too often

الحالة	⚠
المكون	مراقبة سلامة الملف
معرف حدث Windows	2901
معرف حدث Kaspersky Security Center	00000b55
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Report on object modification for the aggregation period

الحالة	⚠
المكون	مراقبة سلامة الملف
معرف حدث Windows	2902
معرف حدث Kaspersky Security Center	00000b56
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Monitoring scope includes incorrect objects

الحالة	⚠
المكون	مراقبة سلامة الملف
معرف حدث Windows	2903
معرف حدث Kaspersky Security Center	00000b57
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

رسائل معلوماتية

Application started

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	235
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Application stopped

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	236
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Self-Defense restricted access to the protected resource

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	213
معرف حدث Kaspersky Security Center	000000d5
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Report cleared

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	217
معرف حدث Kaspersky Security Center	000000d9
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Group policy disabled

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	220
معرف حدث Kaspersky Security Center	000000dc
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application settings changed

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	218
معرف حدث Kaspersky Security Center	000000da
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Task started

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	221
معرف حدث Kaspersky Security Center	000000dd
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Task completed

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	223
معرف حدث Kaspersky Security Center	000000df
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

All application components that are defined by the license have been installed and run in normal mode

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	227
معرف حدث Kaspersky Security Center	000000e3
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Subscription settings have changed

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	238
معرف حدث Kaspersky Security Center	000000ee
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Subscription has been renewed

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	239
معرف حدث Kaspersky Security Center	000000ef
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object restored from Backup

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	335
معرف حدث Kaspersky Security Center	0000014f
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

User name and password input

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	2000
معرف حدث Kaspersky Security Center	000007d0
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Participation in KSN enabled

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	2020
معرف حدث Kaspersky Security Center	000007e4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

KSN servers available

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	2022
معرف حدث Kaspersky Security Center	000007e6
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The application works and processes data under relevant laws and uses the appropriate infrastructure

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	2024
معرف حدث Kaspersky Security Center	000007e8
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object restored from Quarantine

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	345
معرف حدث Kaspersky Security Center	00000159
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object deleted from Quarantine

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	347
معرف حدث Kaspersky Security Center	0000015b
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

A backup copy of the object was created

الحالة	ⓘ
المكون	الحماية من تهديدات الملفات الحماية من تهديدات البريد اكتشاف السلوك منع اختراق المضيف Kaspersky Sandbox فحص البرامج الضارة
معرف حدث Windows	308
معرف حدث Kaspersky Security Center	00000134
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Overwritten by a copy that was disinfected earlier

الحالة	ⓘ
المكون	الحماية من تهديدات الملفات منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	327
معرف حدث Kaspersky Security Center	00000147
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Password-protected archive detected

الحالة	ⓘ
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	322
معرف حدث Kaspersky Security Center	GNRL_EV_PASSWD_ARCHIVE_FOUND
معلمات الحدث	• GNRL_EA_PARAM_2 هو اسم الكائن. • GNRL_EA_PARAM_3 هو تاريخ إنشاء الكائن (اختياري). • GNRL_EA_PARAM_7 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). التهديد المكتشف بواسطة KSN الخاصة (قائمة الرفض): true أو false.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Information about detected object

الحالة	ⓘ
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	332
معرف حدث Kaspersky Security Center	0000014c
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The object is in the Kaspersky Private Security Network allowlist

الحالة	ⓘ
المكون	الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI منع اختراق المضيف فحص البرامج الضارة
معرف حدث Windows	340
معرف حدث Kaspersky Security Center	00000154
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object renamed

الحالة	ⓘ
المكون	الحماية من تهديدات البريد منع الاستغلال اكتشاف السلوك فحص البرامج الضارة
معرف حدث Windows	329
معرف حدث Kaspersky Security Center	00000149
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object processed

الحالة	ⓘ
المكون	منع اختراق المضيف الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد فحص البرامج الضارة
معرف حدث Windows	301
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Object skipped

الحالة	ⓘ
المكون	منع اختراق المضيف الحماية من تهديدات الملفات حماية AMSI فحص البرامج الضارة
معرف حدث Windows	315
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Archive detected

الحالة	ⓘ
المكون	منع اختراق المضيف الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI فحص البرامج الضارة
معرف حدث Windows	318
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Packed object detected

الحالة	ⓘ
المكون	منع اختراق المضيف الحماية من تهديدات الملفات الحماية من تهديدات الويب الحماية من تهديدات البريد حماية AMSI فحص البرامج الضارة
معرف حدث Windows	319
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Link processed

الحالة	ⓘ
المكون	الحماية من تهديدات الويب
معرف حدث Windows	361
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Application startup allowed

الحالة	ⓘ
المكون	التحكم في التطبيقات
معرف حدث Windows	701
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Update source is selected

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1001
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

تم تحديد الخادم الوكيل

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1002
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

The link is in the Kaspersky Private Security Network allowlist

الحالة	ⓘ
المكون	الحماية من تهديدات الويب
معرف حدث Windows	370
معرف حدث Kaspersky Security Center	00000172
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application placed in the trusted group

الحالة	ⓘ
المكون	منع اختراق المضيف
معرف حدث Windows	401
معرف حدث Kaspersky Security Center	00000191
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application placed in restricted group

الحالة	ⓘ
المكون	منع اختراق المضيف
معرف حدث Windows	402
معرف حدث Kaspersky Security Center	00000192
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Host Intrusion Prevention was triggered

الحالة	ⓘ
المكون	منع اختراق المضيف
معرف حدث Windows	403
معرف حدث Kaspersky Security Center	00000193
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File restored

الحالة	ⓘ
المكون	اكتشاف السلوك منع الاستغلال منع اختراق المضيف
معرف حدث Windows	457
معرف حدث Kaspersky Security Center	000001c9
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Registry value restored

الحالة	ⓘ
المكون	اكتشاف السلوك منع الاستغلال
معرف حدث Windows	458
معرف حدث Kaspersky Security Center	000001ca
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Registry value deleted

الحالة	ⓘ
المكون	اكتشاف السلوك منع الاستغلال
معرف حدث Windows	459
معرف حدث Kaspersky Security Center	000001cb
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Process action skipped

الحالة	ⓘ
المكون	مراقبة عيوب التكيف
معرف حدث Windows	2201
معرف حدث Kaspersky Security Center	GNRL_EV_ADSEC_DETECT
معلمات الحدث	• GNRL_EA_PARAM_1 هو اسم قاعدة مراقبة عيوب التكيف. • GNRL_EA_PARAM_2 هو معرف القاعدة المساعدة على الاكتشاف. • GNRL_EA_PARAM_3 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_4 هو اسم العملية المصدر. • GNRL_EA_PARAM_5 هو الكائن المصدر. • GNRL_EA_PARAM_6 هو العملية الهدف. • GNRL_EA_PARAM_7 هو الكائن الهدف. • GNRL_EA_PARAM_8 هي معلومات إضافية حول الكائن المكتشف: تجزئات العملية المصدر / عملية الكائن والهدف / الكائن. تم منع العملية (verdict_type): true أو false. معرف أمان المستخدم (SID).
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Keyboard authorized

الحالة	ⓘ
المكون	منع هجمات BadUSB
معرف حدث Windows	2050
معرف حدث Kaspersky Security Center	00000802
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Network activity allowed

الحالة	ⓘ
المكون	جدار الحماية
معرف حدث Windows	601
معرف حدث Kaspersky Security Center	00000259
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Application startup prohibited in test mode

الحالة	ⓘ
المكون	التحكم في التطبيقات
معرف حدث Windows	703
معرف حدث Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_DENIED
معلمات الحدث	• GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو معرف الفئة الذي تم إنشاؤه يدويًا. • GNRL_EA_PARAM_4 هو معرف أمان الحساب (SID). • GNRL_EA_PARAM_5 هو معلومات عن التوقيع الرقمي للتطبيق. • GNRL_EA_PARAM_6 هو اسم الملف القابل للتنفيذ للتطبيق (على سبيل المثال، chrome.exe). • GNRL_EA_PARAM_7 هو المسار إلى الملف القابل للتنفيذ. • GNRL_EA_PARAM_8 هي تجزئة الكائن (SHA256). • GNRL_EA_PARAM_9 هو إصدار التطبيق الذي يحاول المستخدم تشغيله.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application startup allowed in test mode

الحالة	ⓘ
المكون	التحكم في التطبيقات
معرف حدث Windows	704
معرف حدث Kaspersky Security Center	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
معلمات الحدث	• GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_3 هو معرف الفئة الذي تم إنشاؤه يدويًا. • GNRL_EA_PARAM_4 هو معرف أمان الحساب (SID). • GNRL_EA_PARAM_5 هو معلومات عن التوقيع الرقمي للتطبيق.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

A page that is allowed was opened

الحالة	ⓘ
المكون	التحكم في الويب
معرف حدث Windows	751
معرف حدث Kaspersky Security Center	000002f4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Operation with the device allowed

الحالة	ⓘ
المكون	التحكم في الجهاز
معرف حدث Windows	801
معرف حدث Kaspersky Security Center	00000321
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

File operation performed

الحالة	ⓘ
المكون	التحكم في الجهاز
معرف حدث Windows	808
معرف حدث Kaspersky Security Center	GNRL_EV_USB_FILE_OPERATION
معلمات الحدث	• GNRL_EA_PARAM_1 هو عملية الملف (كتابة أو حذف). • GNRL_EA_PARAM_2 هو المسار إلى الملف. • GNRL_EA_PARAM_3 هو اسم الجهاز. • GNRL_EA_PARAM_4 هو اسم مستخدم الجلسة. • GNRL_EA_PARAM_5 هو معرف الجهاز (HWID).
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

No available updates

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1020
معرف حدث Kaspersky Security Center	000003fc
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Update distribution completed successfully

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1022
معرف حدث Kaspersky Security Center	000003fe
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Downloading files

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1003
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File downloaded

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1004
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File installed

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1005
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File updated

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1006
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File rolled back due to update error

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1007
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Updating files

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1008
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Distributing updates

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1009
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Rolling back files

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1010
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Creating the list of files to download

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	1013
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Downloading patches

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	2150
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Installing patch

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	2151
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Patch installed

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	2152
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Rolling back patch

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	2154
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Patch rolled back

الحالة	ⓘ
المكون	تحديث قاعدة البيانات
معرف حدث Windows	2155
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Started applying file encryption / decryption rules

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	901
معرف حدث Kaspersky Security Center	00000385
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Finished applying file encryption / decryption rules

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	902
معرف حدث Kaspersky Security Center	00000386
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Resumed applying file encryption / decryption rules

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	905
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File encryption / decryption started

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	910
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File encryption / decryption completed

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	911
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File has not been encrypted because it is an exclusion

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	913
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Portable mode enabled

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	950
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Portable mode disabled

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	952
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Device encryption / decryption started

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1301
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Device encryption / decryption completed

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1302
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Device encryption / decryption resumed

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1304
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Device is not encrypted

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1307
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Device encryption / decryption process has been switched to active mode

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1308
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Device encryption / decryption process has been switched to passive mode

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1309
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Encryption module loaded

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1310
معرف حدث Kaspersky Security Center	0000051e
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

New Authentication Agent account created

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1330
معرف حدث Kaspersky Security Center	00000532
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Authentication Agent account deleted

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1331
معرف حدث Kaspersky Security Center	00000533
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Authentication Agent account password changed

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1332
معرف حدث Kaspersky Security Center	00000534
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Successful Authentication Agent login

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1333
معرف حدث Kaspersky Security Center	00000535
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Failed Authentication Agent login attempt

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1334
معرف حدث Kaspersky Security Center	00000536
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Hard drive accessed using the procedure of requesting access to encrypted devices

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1335
معرف حدث Kaspersky Security Center	00000537
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Failed attempt to access the hard drive using the procedure of requesting access to encrypted devices

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1336
معرف حدث Kaspersky Security Center	00000538
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

This account already exists .Account was not added

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1337
معرف حدث Kaspersky Security Center	00000539
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

This account does not exist .Account was not modified

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1338
معرف حدث Kaspersky Security Center	0000053a
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

This account does not exist. Account was not deleted

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1339
معرف حدث Kaspersky Security Center	0000053b
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

FDE upgrade successful

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1341
معرف حدث Kaspersky Security Center	0000053d
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

FDE upgrade rollback successful

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1343
معرف حدث Kaspersky Security Center	0000053f
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Failed to uninstall Kaspersky Disk Encryption drivers from the WinRE image

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1346
معرف حدث Kaspersky Security Center	00000542
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

BitLocker recovery key was changed

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1370
معرف حدث Kaspersky Security Center	0000055a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

BitLocker password / PIN was changed

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1371
معرف حدث Kaspersky Security Center	0000055b
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

BitLocker recovery key was saved to a removable drive

الحالة	ⓘ
المكون	تشفير البيانات
معرف حدث Windows	1372
معرف حدث Kaspersky Security Center	0000055c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Processing of tasks from the Kaspersky Anti Targeted Attack Platform server is inactive

الحالة	ⓘ
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2103
معرف حدث Kaspersky Security Center	00000837
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Endpoint Sensor connected to server

الحالة	ⓘ
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2101
معرف حدث Kaspersky Security Center	00000835
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Connection to the Kaspersky Anti Targeted Attack Platform server restored

الحالة	ⓘ
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2102
معرف حدث Kaspersky Security Center	00000836
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Tasks from the Kaspersky Anti Targeted Attack Platform server are being processed

الحالة	ⓘ
المكون	أداة استشعار نقطة النهاية
معرف حدث Windows	2104
معرف حدث Kaspersky Security Center	00000838
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object deleted

الحالة	ⓘ
المكون	مسح البيانات
معرف حدث Windows	2251
معرف حدث Kaspersky Security Center	000008cb
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

Wipe task statistics

الحالة	ⓘ
المكون	(EDR (KATA
معرف حدث Windows	2853
معرف حدث Kaspersky Security Center	00000b25
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

الحالة	ⓘ
المكون	مسح البيانات
معرف حدث Windows	2253
معرف حدث Kaspersky Security Center	000008cd
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object quarantined (Kaspersky Sandbox)

الحالة	ⓘ
المكون	Kaspersky Sandbox
معرف حدث Windows	2602
معرف حدث Kaspersky Security Center	00000a2a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object deleted (Kaspersky Sandbox)

الحالة	ⓘ
المكون	Kaspersky Sandbox
معرف حدث Windows	2604
معرف حدث Kaspersky Security Center	00000a2c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

IOC Scan started

الحالة	ⓘ
المكون	Endpoint Detection and Response
معرف حدث Windows	2652
معرف حدث Kaspersky Security Center	00000a5c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

IOC Scan completed

الحالة	ⓘ
المكون	Endpoint Detection and Response
معرف حدث Windows	2653
معرف حدث Kaspersky Security Center	00000a5d
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object quarantined (Endpoint Detection and Response)

الحالة	ⓘ
المكون	Endpoint Detection and Response
معرف حدث Windows	2555
معرف حدث Kaspersky Security Center	000009fb
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object deleted (Endpoint Detection and Response)

الحالة	ⓘ
المكون	Endpoint Detection and Response
معرف حدث Windows	2557
معرف حدث Kaspersky Security Center	000009fd
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application components successfully changed

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	1402
معرف حدث Kaspersky Security Center	0000057a
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

الحالة	ⓘ
المكون	Kaspersky Sandbox
معرف حدث Windows	2606
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

الحالة	ⓘ
المكون	Kaspersky Sandbox
معرف حدث Windows	2609
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

الحالة	ⓘ
المكون	Kaspersky Sandbox
معرف حدث Windows	2610
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

الحالة	ⓘ
المكون	Kaspersky Sandbox
معرف حدث Windows	2616
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Asynchronous Kaspersky Sandbox detection

الحالة	ⓘ
المكون	Kaspersky Sandbox
معرف حدث Windows	2619
معرف حدث Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
معلمات الحدث	• GNRL_EA_PARAM_1 هو إعدادات مكون Kaspersky Sandbox • GNRL_EA_PARAM_2 هو المسار إلى الكائن. • GNRL_EA_PARAM_3 هو معرف الحادث. • GNRL_EA_PARAM_4 هي تجزئة الكائن (SHA256).
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Device is connected

الحالة	ⓘ
المكون	التحكم في الجهاز
معرف حدث Windows	805
معرف حدث Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_PLUGGED
معلمات الحدث	• GNRL_EA_PARAM_1 هو معرف الجهاز (HWID). • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Device is disconnected

الحالة	ⓘ
المكون	التحكم في الجهاز
معرف حدث Windows	806
معرف حدث Kaspersky Security Center	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
معلمات الحدث	• GNRL_EA_PARAM_1 هو معرف الجهاز (HWID). • GNRL_EA_PARAM_2 هو اسم مستخدم الجلسة.
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error removing the previous version of the application

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	246
معرف حدث Kaspersky Security Center	000000f6
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Successful connection to the Kaspersky Anti Targeted Attack Platform server

الحالة	ⓘ
المكون	(EDR (KATA
معرف حدث Windows	2853
معرف حدث Kaspersky Security Center	00000b25
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

الملحق رقم 7. امتدادات الملفات المدعومة لمنع التنفيذ

يدعم Kaspersky Endpoint Security منع فتح الملفات بتنسيق Office في تطبيقات معينة. ويتم سرد المعلومات الخاصة بامتدادات الملفات والتطبيقات المدعومة في الجدول التالي.

اسم التطبيق	الملف القابل للتنفيذ	ملحق الملف
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe	pdf

مستعرض Yandex	browser.exe	
Tor Browser	tor.exe	

الملحق رقم 8. مترجمو النصوص المدعومون لمنع التنفيذ

يدعم منع التنفيذ مترجمي البرامج النصية التالية:

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe

- regsvr32.exe
- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

يدعم منع التنفيذ العمل مع تطبيقات Java في بيئة وقت تشغيل Java (عمليات java.exe وjavaw.exe).

الملحق رقم 9. نطاق فحص IOC في التسجيل (Registryltem)

عندما تضيف نوع البيانات Registryltem إلى نطاق فحص IOC، يفحص Kaspersky Endpoint Security مفاتيح التسجيل التالية:

HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile

HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

الملحق رقم 10. متطلبات ملف IOC

عند إنشاء مهام فحص IOC، ضع في اعتبارك متطلبات وقيود ملف IOC التالية:

- يدعم التطبيق ملفات IOC بامتدادات IOC و XML في إصدارات OpenIOC القياسية المفتوحة 1.0 و1.1 لوصف مؤشرات الاختراق.
- إذا قمت أثناء إنشاء مهمة فحص IOC في سطر الأوامر بتحميل ملفات IOC (مؤشر الاختراق) بعضها غير مدعوم، فعند تشغيل المهمة، لا يستخدم التطبيق سوى ملفات IOC المدعومة. إذا اتضح أثناء إنشاء مهمة فحص IOC في سطر الأوامر أن جميع ملفات IOC التي قمت بتحميلها غير مدعومة، فمن الممكن مواصلة تشغيل المهمة، لكنها لن تكتشف أي مؤشرات على الاختراق. ولا يمكن تحميل ملفات IOC غير المدعومة باستخدام Web Console أو Cloud Console.
- لا تتسبب الأخطاء الدلالية وشروط وعلامات IOC غير المدعومة في ملفات IOC في فشل تنفيذ المهمة. وفي هذه الأقسام من ملفات IOC، يكتشف التطبيق عدم وجود تطابق.
- يجب أن تكون معرفات كل ملفات IOC المستخدمة في مهمة فحص IOC معرفات فريدة. وإذا كانت هناك ملفات IOC بالمعرف نفسه، فقد تؤثر على نتائج تنفيذ المهمة.
- يجب ألا يتجاوز حجم ملف IOC واحد 2 ميجا بايت. وسيؤدي استخدام ملفات أكبر إلى إيقاف مهام فحص IOC بخطأ. ويجب ألا يتجاوز الحجم الإجمالي لجميع الملفات المضافة إلى مجموعة مؤشر الاختراق 10 ميجا بايت. وإذا تجاوز الحجم الإجمالي لجميع الملفات 10 ميجا بايت، فستحتاج إلى تقسيم مجموعة مؤشر الاختراق وإنشاء مهام IOC Scan عديدة.
- يوصى بإنشاء ملف IOC واحد لكل تهديد. ويسهل هذا تحليل نتائج مهمة فحص IOC.

يحتوي الملف الذي يمكنك تنزيله بالنقر فوق الارتباط أدناه على جدول يحتوي على قائمة كاملة بشروط IOC لمعيار OpenIOC.

تنزيل ملف DOWNLOAD THE IOC_TERMS.XLSX

يوضح الجدول التالي ميزات وقيود دعم التطبيق لمعيار OpenIOC.

ميزات وقيود دعم OpenIOC الإصدارين 1.0 و1.1.

الشروط المدعومة	OpenIOC 1.0:
	
	`is`
	`isnot` (كاستثناء من المجموعة)
	`contains`
	`containsnot` (كاستثناء من المجموعة)
	OpenIOC 1.1:
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`

سمات الشروط المدعومة	OpenIOC 1.1:
	
	`preserve-case`
	`negate`

المشغلون المدعومون	`AND` `OR`
أنواع البيانات المدعومة	`"date"`: التاريخ (الشروط القابلة للتطبيق: `is`، `greater-than`، `less-than`) `"int"`: عدد صحيح (الشروط القابلة للتطبيق: `is`، `greater-than`، `less-than`) `"string"`: السلسلة (الشروط القابلة للتطبيق: `is`، `contains`، `matches`، `starts-with`، `ends-with`) `"duration"`: المدة بالثواني (الشروط المطبقة (الشروط القابلة للتطبيق: `is, greater-than, less-than`)

ميزات تفسير نوع البيانات	تُفسر أنواع البيانات `"boolean string"` و`"restricted string"` و`"md5"` و`"IP"` و`"sha256"` و`"base64Binary"` كسلسلة.
	
	يدعم التطبيق تفسير إعداد المحتوى لنوعي البيانات `int` و`date` عند تعيينهما في شكل فترات زمنية:
	
	OpenIOC 1.0:
	استخدام المشغل `TO` في الحقل `Content` :
	`<Content type="int">49600 TO 50700</Content>`
	`<Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content>`
	`<Content type="int">[154192 TO 154192]</Content>`
	OpenIOC 1.1:
	استخدام شرطي `greater-than` و`less-than`
	استخدام المشغل `TO` في الحقل `Content`
	يدعم التطبيق تفسير نوعي بيانات `date` و`duration` في حالة تعيين المؤشرات بتنسيق `ISO 8601`، `Zulu Time Zone`، `UTC`.

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

يحتوي الملف legal_notices.txt، الموجود في مجلد تثبيت التطبيق، على معلومات عن التعليمات البرمجية الخاصة بطرف ثالث.

إشعارات العلامة التجارية

.العلامات التجارية وعلامات الخدمة المسجلة تعود ملكيتها لمالكيها المعنيين.

Adobe وAcrobat وFlash وReader وShockwave علامات تجارية مسجلة مملوكة لشركة Adobe في الولايات المتحدة الأمريكية و/أو بلدان أخرى.

Amazon Web Services وAWS علامتان تجاريتان لشركة .Amazon.com, Inc أو الشركات التابعة لها.

Apple وFireWire وiTunes وSafari علامات تجارية مملوكة لشركة Apple Inc.

AutoCAD هي علامة تجارية أو علامة تجارية مسجلة مملوكة لشركة Autodesk, Inc. و/أو شركاتها الفرعية و/أو الشركات التابعة لها في الولايات المتحدة و/أو بلاد أخرى.

كلمة Bluetooth وعلامتها وشعاراتها مملوكة لشركة Bluetooth SIG, Inc.

Borland هي علامة تجارية أو علامة تجارية مسجلة لشركة Borland Software Corporation.

Android وGoogle Public DNS وGoogle Chrome وChrome علامات تجارية لشركة Google, LLC.

Citrix وCitrix Provisioning Services وXenDesktop علامات تجارية مملوكة لشركة .Citrix Systems, Inc و/أو واحدة أو أكثر من الشركات التابعة لها، ويمكن أن تكون مسجلة في مكتب براءات الاختراع والعلامات التجارية للولايات المتحدة وفي بلدان أخرى.

Cloudflare وCloudflare Workers وشعار Cloudflare علامات تجارية و/أو علامات تجارية مسجلة لشركة .Cloudflare، Inc في الولايات المتحدة وولايات قضائية أخرى.

Dell والعلامات التجارية الأخرى علامات تجارية لشركة .Dell Inc أو الشركات التابعة لها.

dBase هي علامة تجارية مملوكة لمؤسسة dataBased Intelligence, Inc.

Docker وشعار Docker علامتان تجاريتان و/أو علامتان تجاريتان مسجلتان لشركة .Docker، Inc في الولايات المتحدة وبلدان أخرى. قد تمتلك شركة .Docker, Inc والأطراف الأخرى أيضًا حقوق علامة تجارية بمصطلحات أخرى مستخدمة هنا.

EMC علامة تجارية أو علامة تجارية مسجلة مملوكة لشركة EMC Corporation في الولايات المتحدة و/أو بلدان أخرى.

Foxit علامة تجارية مسجلة لشركة Foxit Corporation.

Radmin هي علامة تجارية مسجلة لشركة Famatech.

IBM علامة تجارية مملوكة لشركة International Business Machines Corporation مسجلة في العديد من المناطق حول العالم.

Intel هي علامة تجارية مملوكة لشركة Intel Corporation في الولايات المتحدة و/أو بلاد أخرى.

Cisco وCisco AnyConnect علامتان تجاريتان مسجلتان أو علامتان تجاريتان لشركة .Cisco Systems, Inc و/أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

Lenovo وLenovo ThinkPad علامتان تجاريتان لشركة Lenovo في الولايات المتحدة و/أو في أماكن أخرى.

Linux هي العلامة التجارية المسجلة لشركة Linus Torvalds في الولايات المتحدة وبلاد أخرى.

Logitech علامة تجارية مسجلة أو علامة تجارية مملوكة لشركة Logitech في الولايات المتحدة و/أو بلاد أخرى.

LogMeIn Pro وRemotely Anywhere علامتان تجاريتان لشركة LogMeIn, Inc.

Mail.ru علامة تجارية مسجلة لشركة Mail.Ru, LLC.

McAfee علامة تجارية أو علامة تجارية مسجلة لشركة McAfee LLC أو الشركات التابعة لها في الولايات المتحدة و/أو بلدان أخرى.

Microsoft وMicrosoft Edge وAccess وActive Directory وActiveSync وBing وBitLocker وExcel وInternet Explorer وLifeCam Cinema وMSDN وMultiPoint وOutlook وPowerPoint وPowerShell وVisual Basic وVisual FoxPro وWindows وWindows PowerShell وWindows Server وWindows Store وMS-DOS وSkype وSurface وHyper-V وSQL Server علامات تجارية لمجموعة شركات Microsoft.

Mozilla وFirefox وThunderbird علامات تجارية مملوكة لشركة Mozilla Foundation في الولايات المتحدة وبلدان أخرى.

NetApp علامة تجارية أو علامة تجارية مسجلة لشركة NetApp, Inc. في الولايات المتحدة و/أو بلدان أخرى.

Python علامة تجارية أو علامة تجارية مسجلة لشركة Python Software Foundation.

Java وJavaScript علامتان تجاريتان مسجلتان مملوكتان لشركة Oracle و/أو الشركات التابعة لها.

VERISIGN علامة تجارية مسجلة في الولايات المتحدة وأماكن أخرى أو علامة تجارية غير مسجلة لشركة VeriSign, Inc. والشركات التابعة لها.

VMware وVMware ESXi وVMware Workstation علامات تجارية مسجلة لشركة VMware, Inc. في الولايات المتحدة و/أو بلدان أخرى.

Tor علامة تجارية مسجلة لمشروع Tor ، برقم تسجيل في الولايات المتحدة 3,465,432.

Thawte علامة تجارية أو علامة تجارية مسجلة لشركة Symantec Corporation أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

SAMSUNG علامة تجارية لشركة SAMSUNG في الولايات المتحدة وبلدان أخرى.