kaspersky

Kaspersky Endpoint Security 14.2 for Windows

© 2026 AO Kaspersky Lab

جدول المحتويات

تعليمات Kaspersky Endpoint Security for Windows

ما الجديد

المشكلات التي تم إصلاحها

الأسئلة الأكثر تكرارًا

Kaspersky Endpoint Security for Windows

أوضاع التطبيق: Standard، EDR Agent، Light Agent

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

عمليات Kaspersky Endpoint Security for Windows

تغيير مكونات التطبيق

ترقية إصدار سابق من التطبيق

ترقية التطبيق دون إعادة التشغيل

تحديث SMU 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

إزالة مفتاح الترخيص

عرض معلومات الترخيص

شراء الترخيص

تجديد الاشتراك

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
تحضير التطبيق للاستخدام
إدارة السياسات
إنشاء سياسة
تصدير واستيراد سياسة
مؤشر مستوى الأمان
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
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
فحص البرامج الضارة
فحص الكمبيوتر
فحص محركات الأقراص القابلة للإزالة عند توصيلها بالكمبيوتر
فحص في الخلفية
الفحص من قائمة السياق
التحقق من سلامة التطبيق
تحرير نطاق الفحص
إجراء فحص مجدول
اجراء 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
تحديث الوحدات النمطية للتطبيق
استخدام الخادم الوكيل للتحديثات
استرجاع آخر تحديث

تقنية التنظيف المتقدمة
تنظيف التهديدات النشطة على محطات العمل
تنظيف التهديدات النشطة على الخوادم
القضاء على التهديدات غير المعالجة
حماية الكمبيوتر
حالة الحماية في الوقت الحقيقي
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
فحص الحاوية
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
منع هجمات BadUSB
تمكين "منع هجمات BadUSB" أو تعطيلها
استخدام لوحة المفاتيح على الشاشة للمصادقة على أجهزة USB
إذن الماسح الضوئي للرمز الشريطي
حماية AMSI
تمكين حماية AMSI وتعطيلها
تحسين فحص الملفات عن طريق حماية AMSI
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
فحص رسائل البريد الإلكتروني في Thunderbird وMyOffice وR7-Office
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 من تهديدات الشبكة حسب النوع
جدار الحماية
تمكين أو تعطيل جدار الحماية
تغيير نوع 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 الاستغلال
تمكين وتعطيل منع الاستغلال
حماية ذاكرة عمليات النظام
اكتشاف السلوك
مكافحة التشفير
تمكين وتعطيل حماية المجلدات المشتركة ضد التشفير الخارجي
تكوين فترة الحظر لجهاز كمبيوتر غير موثوق به
تحرير نطاق المراقبة
إضافة أجهزة كمبيوتر موثوقة لتشفير البيانات الخارجية
تصدير واستيراد قائمة استثناءات من حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي
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
إضافة شهادة Kaspersky إلى مخزن الشهادات الخاص
استثناء الاتصالات المشفرة من الفحص
منع الوصول إلى المجالات ذات الشهادات غير الموثوقة
مسح البيانات
التحكم في الكمبيوتر
التحكم في الويب
إضافة قاعدة وصول إلى موارد الويب
التصفية حسب عناوين موارد الويب
التصفية حسب محتوى مورد الويب
اختبار قواعد الوصول إلى موارد الويب
تصدير واستيراد قواعد التحكم في الويب
تصدير واستيراد عناوين موارد الويب لقاعدة التحكم في الويب
مراقبة نشاط إنترنت المستخدم
تحرير قوالب رسائل التحكم في الويب
تحرير أقنعة عناوين مصادر الويب
التحكم في الويب للأجهزة الافتراضية
المتغيرات في قوالب رسالة Web Control
التحكم في الجهاز
حول قواعد الوصول
الحصول على معلومات عن الأجهزة المثبتة
إدارة الوصول إلى الأجهزة حسب النوع
إدارة الوصول إلى الأجهزة عن طريق ناقل الاتصال
تمييز حقوق وصول المستخدمين إلى الأجهزة
إدارة الوصول إلى الأجهزة المحمولة
إدارة الوصول إلى أجهزة Bluetooth
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
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
تدريب مكون 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
عمليات مراقبة عيوب التكيف
التحكم في التطبيقات
قيود وظيفة التحكم في التطبيق
الحصول على معلومات عن التطبيقات المثبتة
كيفية تمكين وضع التطبيقات الممنوعة
التحكم في التطبيق بناءً على كمبيوتر أساسي
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
المتغيرات في قوالب رسائل التحكم في التطبيقات
أفضل الممارسات لإجراء جرد للملفات القابلة للتنفيذ
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 النظام
حول قواعد مراقبة سلامة النظام
مراقبة سلامة النظام في الوقت الحقيقي
التحقق من سلامة النظام عند الحاجة
تصدير واستيراد قواعد مراقبة سلامة النظام
عرض تقارير مراقبة سلامة النظام
إعادة تعيين حالة سلامة النظام
Cloud Discovery

منطقة موثوقة
إنشاء استثناء من الفحص
إنشاء استثناء حسب نوع الكائنات المكتشفة
تحرير قائمة التطبيقات الموثوقة
إنشاء منطقة موثوقة محلية
تصدير واستيراد المنطقة الموثوقة
التعامل مع التطبيقات بتوقيع رقمي موثوق
الملحق: استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة
Microsoft SQL Server
Microsoft Exchange Server
Microsoft System Center Configuration Manager
Citrix
VMware
إلغاء البيانات المكررة في Microsoft Windows Server
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
الحماية بكلمة مرور
تمكين الحماية بكلمة مرور
منح أذونات للمستخدمين الأفراد أو المجموعات
استخدام كلمة مرور مؤقتة لمنح الأذونات
إلغاء كلمة المرور المؤقتة
الجوانب الخاصة لأذونات الحماية بكلمة المرور
إعادة تعيين كلمة مرور KLAdmin
حماية اتصال خادم الإدارة
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
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
ترخيص MDR و EDR Optimum
التوافق مع حلول EDR للجهات الخارجية
Kaspersky Endpoint Agent
ترحيل تكوين [KEA+KES] إلى تكوين [KES+العامل المضمن]
ترحيل السياسة والمهام لـ Kaspersky Endpoint Agent
Endpoint Detection and Response Agent (EDR Agent)
تثبيت EDR Agent
دمج EDR Agent مع MDR
دمج EDR Agent مع EDR (KATA)
دمج EDR Agent مع NDR (KATA)
دمج EDR Agent مع EDR Expert (on-premises)
التوافق مع تطبيقات EPP للجهات الخارجية
Managed Detection and Response
تكامل العميل المدمج مع MDR
دليل الترحيل من KEA إلى KES لحل MDR
Endpoint Detection and Response
تكامل العميل المدمج مع EDR Optimum / EDR Expert
الفحص للبحث عن مؤشرات الاختراق (مهمة قياسية)
القياس عن بُعد الموسع لفحص مؤشر الاختراق
نقل الملف إلى العزل
الحصول على الملف
حذف الملف
بدء العملية
إنهاء العملية
منع التنفيذ
عزل شبكة الاتصال
Cloud Sandbox
دليل الترحيل من KEA إلى KES لحل EDR Optimum
Kaspersky Sandbox
تكامل العميل المدمج مع Kaspersky Sandbox
الفحص للبحث عن مؤشرات الاختراق (مهمة مستقلة)
دليل الترحيل من KEA إلى KES لحل Kaspersky Sandbox
Kaspersky Anti Targeted Attack Platform
تكامل العميل المدمج مع EDR / NDR (KATA)
تكوين القياس عن بعد لحل EDR (KATA)
استثناءات القياس عن بُعد لحل EDR (KATA)
المثال 1. العمليات المستثناة
المثال 2. اتصالات الشبكة المستثناة
المثال 3. عمليات الملف المستثناة
المثال 4. تعديلات التسجيل المستثناة
KATA Sandbox
تكامل العميل المدمج مع KATA Sandbox
تكوين إجراءات الاستجابة للتهديدات
دليل الترحيل من KEA إلى KES لحل EDR (KATA)

Endpoint Detection and Response Expert (on-premises)
تكامل العميل المدمج مع EDR Expert (on-premises)
تكوين إعدادات القياس عن بُعد لحل EDR Expert (on-premises)
استثناءات القياس عن بُعد لحل EDR Expert (on-premises)
تصدير واستيراد عوامل تصفية حدث EDR Expert (on-premises)
اعتبارات خاصة عند استخدام ملفات تعريف السياسة لتكوين التكامل مع EDR Expert (on-premises) و EDR (KATA)
Endpoint Detection and Response Expert (cloud)
تكامل العميل المدمج مع EDR Expert (cloud)
تكوين إعدادات القياس عن بُعد لحل EDR Expert (cloud)
استثناءات القياس عن بُعد لحل EDR Expert (cloud)
كيفية تصدير أو استيراد عوامل تصفية أحداث EDR Expert (cloud).
إدارة العزل
تكوين الحد الأقصى لحجم العزل
إرسال بيانات عن الملفات المعزولة إلى Kaspersky Security Center
استعادة الملفات من العزل
مراقبة إجراءات EDR
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
تكامل Kaspersky Endpoint Security مع KUMA
التحضير لدمج KES مع KUMA
ربط KES مع KUMA
يتم إرسال أحداث التصفية إلى KUMA
تصدير واستيراد عوامل تصفية حدث KUMA
دليل الترحيل من KSWS إلى KES
مطابقة مكونات KSWS و KES
مطابقة إعدادات KSWS و KES
ترحيل مكونات KSWS
ترحيل مهام وسياسات KSWS
ترحيل المنطقة الموثوقة في KSWS
ترحيل قواعد التحكم في تشغيل تطبيقات 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
إدارة التطبيق على خادم في وضع Server Core
الترحيل من [KSWS+KEA] إلى [KES+العميل المدمج]
وضع Light Agent لحماية الأجهزة الافتراضية
اعتبارات خاصة لوضع Light Agent
التكوين الأولي للجهاز الافتراضي
التوافق مع تقنية Citrix App Layering
التوافق مع تقنية Citrix Provisioning (Citrix Provisioning Services)
التوافق مع تقنية Omnissa App Volumes
تثبيت Light Agent
ربط Light Agent بجهاز SVM
اكتشاف SVM
تكوين خوارزمية اختيار SVM لوضع Light Agent

توزيع اتصالات Light Agent على أجهزة SVM (العلامات)
حماية الاتصال بين Light Agent و SVM
تفعيل Light Agent
دليل ترحيل KSVLA Light Agent إلى KES Light Agent
تثبيت KES Light Agent بدلاً من KSVLA Light Agent
التطابق بين مكونات KSVLA Light Agent و KES Light Agent
ترحيل مهام وسياسات KSVLA Light Agent
ترحيل تكوين [KSVLA Light Agent+KEA] إلى تكوين [KES Light Agent+العامل المُضمن]
لإدارة التطبيق من سطر الأوامر
Setup. تثبيت التطبيق
Setup /x. إزالة التطبيق
msiexec /i. استعادة التطبيق
أوامر AVP
SCAN. فحص البرامج الضارة
UPDATE. تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق
ROLLBACK. استرجاع آخر تحديث
TRACES. التتبع
START. بدء ملف تعريف
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
RENEW. شراء الترخيص
PBATESTRESET. إعادة تعيين 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
SERVERBINDINGDISABLE. تعطيل حماية الاتصال بالخادم
أوامر KESCLI
Scan. 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 تاريخ ووقت آخر تحديث لقواعد البيانات
EnableRTP. تمكين الحماية
GetRealTimeProtectionState. حالة الحماية من تهديدات الملفات
GetEncryptionState. حالة تشفير القرص
Version. تحديد إصدار التطبيق

أوامر إدارة Detection and Response
SANDBOX. إدارة Sandbox
PREVENTION. إدارة منع التنفيذ
ISOLATION. إدارة عزل شبكة الاتصال
RESTORE. استعادة الملفات من العزل
IOCSCAN. فحص مؤشرات الاختراق (IOC)
MDRLICENSE. تفعيل MDR
EDRKATA. تكامل EDR (KATA)
EDRExpertOnPrem. تكامل EDR Expert (on-premises)
KUMA. تكامل KUMA
YARA. تشغيل فحص YARA
عوامل تصفية القياس عن بُعد. يتم إرسال أحداث التصفية إلى KUMA
أوامر إدارة Light Agent
KSVLAINFO. تحديد وضع Light Agent
VIISINFO. حالة اتصال Light Agent بخادم التكامل
SVMINFO. حالة اتصال Light Agent بخادم الحماية
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
الحصول على بيانات نظام التشغيل (الحصول على معلومات النظام من Kaspersky)
القيود والتحذيرات
المصطلحات
Cloud Discovery
IOC
Light Agent
OpenIOC
SVM
إدارة الملفات المحمولة
إنذار خاطئ
الأرشيف
القناع
الملف القابل للإصابة
المهمة
الوحدة النمطية للنظام الأساسي الموثوق به
تنظيف
جهة إصدار الشهادة
خادم التكامل
شهادة الترخيص

عميل الشبكة
قاعدة بيانات عناوين الويب الاحتيالية
قاعدة بيانات عناوين الويب الضارة
قواعد بيانات مكافحة الفيروسات
كائن OLE
مجموعة الإدارة
مصادقة Kerberos
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
مكافحة التشفير
التحكم في الويب
التحكم في الجهاز
التحكم في التطبيقات
مراقبة عيوب التكيف
مراقبة سلامة النظام
أداة استشعار نقطة النهاية
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert (on-premises)
Network Detection and Response (KATA)
تكامل KUMA
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 (RegistryItem)
الملحق رقم 10. متطلبات ملف IOC
الملحق رقم 11. واجهة برمجة التطبيقات للاستجابة لتهديدات EDR
الملحق رقم 12. حسابات المستخدمين في قواعد مكونات التطبيق
المعلومات القانونية
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 Endpoint Detection and Response Expert (on-premises)
Kaspersky Network Detection and Response (KATA)
التكامل مع Kaspersky Unified Monitoring and Analysis Platform (KUMA)
الامتثال لتشريعات الاتحاد الأوروبي (GDPR)
إشعارات العلامة التجارية
معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

تعليمات Kaspersky Endpoint Security for Windows

ما الجديد في الإصدار 14.2

تمت إضافة دعم المصادقة المستندة إلى الرمز المميز لميزة حماية كلمة المرور.

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

توفير البيانات

تحن اتفاقية ترخيص المستخدم النهائي

عند استخدام KSN

اللائحة العامة لحماية البيانات

القضاء على التهديدات

على محطات العمل

على الخوادم

التفاعل مع اكتشاف مؤشر التسوية (عزل شبكة الاتصال ← العزل ← منع التنفيذ)

أفضل الممارسات

تحسين أداء التطبيق

تنفيذ وضع الرفض الافتراضي في التحكم في التطبيقات

ترحيل KEA إلى KES مع العميل المدمج

استخدام KES كجزء من حلول أخرى

Kaspersky EDR

Kaspersky Sandbox

Kaspersky MDR

ما الجديد

التحديث 14.2

يقدم برنامج Kaspersky Endpoint Security 14.2 for Windows الميزات والتحسينات التالية:

1. تم تغيير مجموعة المكونات المثبتة بشكل افتراضي. ويتضمن تكوين التطبيق الافتراضي الآن BadUSB Attack Prevention وإدارة BitLocker والعميل المدمج في EDR Optimum.

2. الدعم الإضافي للمصادقة القائمة على الرمز المميز (الحماية بكلمة مرور). الآن، للوصول إلى التطبيق، يمكنك استخدام إما اسم المستخدم وكلمة مرورك، أو كلمة مرور مؤقتة صادرة بواسطة المسؤول، أو رمز مميز. ويمكن استخدام المصادقة القائمة على رمز مميز، على سبيل المثال، لحسابات مستخدمي الخدمة التي لا تتطلب كلمة مرور.

3. تمت إضافة معيار قوة كلمة المرور الجديد لـ BitLocker - التحقق من سجل كلمة المرور. ويمنع التطبيق المستخدمين من تعيين كلمة مرور سبق لهم استخدامها.

4. تمت إضافة الدعم لتغيير لغة واجهة Kaspersky Endpoint Security عند تحديث التطبيق باستخدام مهمة تثبيت التطبيق عن بعد. ولن تحتاج الآن إلى إعادة تثبيت التطبيق إذا اخترت لغة الواجهة الخطأ.

5. تمت إضافة أحداث جديدة للقياس عن بُعد لمستخدمي حلول Kaspersky Endpoint Detection and Response: SCCM GPO Change، Smb Connection Open، SCCM Deployment Task، SCCM Config Change، Local Config Mismatch. وتعزز هذه الأحداث الجديدة قدرات اكتشاف التهديدات لحلول EDR.

6. تمت إضافة دعم لإجراء استجابة للتهديدات الجديدة، وضع الملف، لمستخدمي Kaspersky Endpoint Detection and Response Expert (on-premises). وتتيح لك هذه المهمة تسليم ملفات التكوين والبرامج النصية للاستجابة للتهديدات والأدوات المساعدة للتخفيف من آثار الهجمات وما إلى ذلك، إلى أجهزة الكمبيوتر. تتوفر مهمة وضع الملف في وحدة تحكم OSMP عند نشر حل Kaspersky EDR Expert (on-premises) الإصدار 9.0.

7. تم تحسين سلوك إجراءات الاستجابة للتهديدات لمستخدمي Kaspersky Endpoint Detection and Response Optimum. الآن قبل تنفيذ الإجراء (حذف الملف أو نقل الملف إلى العزل أو منع التنفيذ)، يتحقق التطبيق مما إذا كان الكائن مهمًا للنظام (System Critical Object، SCO) ويحذر من التأثير المحتمل على استقرار النظام. ولا يُوصى بتطبيق هذه الإجراءات على ملفات العناصر الحيوية للنظام (SCO).

8. تمت إضافة الدعم لمستخدمي Kaspersky Security for Virtualization Light Agent لتشغيل التطبيق كجزء من مجموعة خوادم تكامل عالية التوافر. توفر مجموعة خوادم التكامل عالية التوفر حماية دون انقطاع للبيئة الافتراضية بفضل تجاوز فشل أجهزة SVM وعملاء Light Agent إلى خادم تكامل احتياطي كلما تعطل خادم التكامل الأساسي.

9. عند تطوير هذا الإصدار من Kaspersky Endpoint Security، دمجنا التغييرات المتضمنة في التصحيحات الخاصة التالية: PF15054، PF15056، PF15058، PF15062، PF15063، PF15064، PF16052، PF16053، PF16055، PF16056، PF16057، PF16060، PF16061، PF16062، PF17027، PF17029، PF17039، PF17041، PF17043، PF17048، PF17050، PF17051، PF17053، PF17054، PF17060، PF18010، PF18011، PF18014، PF18015، PF18020، PF18021، PF18022، PF18023، PF18024، PF18028، PF18031، PF18032، PF18043، PF18050، PF18051، PF18053، PF18057، PF19003، PF19016، PF19018، PF19017، PF19032، PF19034، PF19036، PF19037، PF19041، PF19043، PF19049، PF19051، PF19055، PF19056، PF19065، PF20011، PF20016، PF20017، PF20020، PF20021، PF20033، PF20036، PF20038، PF20039، PF20049، PF20052، PF20055، PF20060، PF20065، PF20078، PF20080، PF20081، PF21007، PF21010، PF21019، PF21021، PF21024، PF21026، PF21040، PF21058، PF21062، PF21063، PF22004، PF22008، PF22014، PF22027، PF22036، PF22049، PF22053، PF22056، PF22059، PF22065، PF23022، PF23026، PF23029، PF23031، PF23039، PF23049، PF23063، PF23095، PF24005، PF24011، PF24013، PF24014، PF24017، PF24019، PF24037، PF24043، PF24048، PF25013، PF25016، PF25019، PF25030.

التحديث 14.1

يقدم برنامج Kaspersky Endpoint Security 14.1 for Windows الميزات والتحسينات التالية:

1. تمت إضافة دعم نظام التشغيل Windows Server 2025.

2. تم زيادة الحد الأقصى لعدد قواعد تصفية أحداث القياس عن بعد لحلي Endpoint Detection and Response Expert (on-premises) و Kaspersky Endpoint Detection and Response Expert (cloud). يدعم Kaspersky Endpoint Security الآن ما يصل إلى 10000 قاعدة تصفية شاملة وحصرية في المجمل.

3. يمكنك الآن تكوين المهام لتعمل فقط في أيام محددة من الأسبوع، في فترات زمنية محددة بالأسابيع. ويتوفر الجدول الزمني في Kaspersky Security Center 16.1 أو أحدث.

4. بالنسبة لمهمة فحص البرامج الضارة، يمكنك الآن تحديد فاصل زمني سيتم خلاله إيقاف المهمة مؤقتًا، على سبيل المثال، لتقليل التأثير على أداء الكمبيوتر أثناء فترات التحميل المتزايد.

5. تم تحسين أداء النظام الفرعي لمحرك الأقراص الثابت الموجود على الكمبيوتر المحمي عن طريق تقليل عدد عمليات الإدخال/الإخراج.

6. عند تطوير هذا الإصدار من Kaspersky Endpoint Security، دمجنا التغييرات المضمنة في التصحيحات الخاصة التالية: PF14061 وPF14062 وPF14064 وPF14065 وPF14069 وPF14070 وPF14071 وPF15054 وPF15056 وPF15058 وPF15062 وPF15063 وPF16058 وPF15062 وPF15063 وPF16058 وPF16053 وPF16055 وPF16056 وPF16057 وPF16060 وPF16061 وPF16062 وPF17027 وPF17029 وPF17039 وPF17041 وPF17043 وPF17048 وPF17050 وPF17051 وPF17053 وPF17054 وPF17060 وPF18010 وPF18011 وPF18014 وPF18015 وPF18020 وPF18021 وPF18022 وPF18023 وPF18024 وPF18028 وPF18031 وPF18032 وPF18043 وPF18050 وPF18051 وPF18053 وPF18057 وPF19003 وPF19016 وPF19018 وPF19017 وPF19032 وPF19034 وPF19036 وPF19037 وPF19041 وPF19043 وPF19049 وPF19051 وPF19055 وPF19056 وPF19065 وPF20011 وPF20016 وPF20017 وPF20020 وPF20021 وPF20033 وPF20036 وPF20038 وPF20039 وPF20049 وPF20052 وPF20055 وPF20060 وPF20065 وPF20078 وPF20080 وPF20081 وPF21007 وPF21062 PF1021021958 وPF21063 وPF22004 وPF22008 وPF22014 وPF22027 وPF22036 وPF22049 وPF22053 وPF22056 وPF22059 وPF23022 وPF23026 وPF23029 وPF23031 وPF23039 وPF23049 وPF23063 وPF24005 وPF24011 وPF24013 وPF21940.

التحديث 14.0

يقدم برنامج Kaspersky Endpoint Security 14.0 for Windows الميزات والتحسينات التالية:

1. يتم الآن دعم أجهزة الكمبيوتر القائمة على بنية Arm. يمكنك تثبيت التطبيق في الوضع القياسي أو وضع EDR Agent. ومع ذلك، يتضمن التطبيق العديد من القيود (على سبيل المثال، من بين تقنيات تشفير البيانات ، يتم دعم BitLocker فقط).

2. يتم دعم عملية مراجعة السياسات الموسعة في إصدار Kaspersky Security Center Web Console رقم 15.0 أو أحدث. ويمكنك الآن الاطلاع على مراجعات السياسة وحفظها في ملف. المراجعة هي مجموعة من المعلمات المعدلة المحفوظة بواسطة المستخدم. وتسمح لك المراجعات بمقارنة التغييرات وإعادتها إلى معلمات السياسة.

3. تتوفر الآن أحداث قياس عن بُعد جديدة لمستخدمي Kaspersky Endpoint Detection and Response. وتعزز هذه الأحداث الجديدة قدرات اكتشاف التهديدات باستخدام حلول Kaspersky EDR.

4. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows، دمجنا التغييرات المضمنة في التصحيحات الخاصة التالية: PF13115، PF13118، PF13119، PF13120، PF13123، PF13124، PF14061، PF14062، PF14064، PF14065، PF14069، PF14070، PF15054، PF15056، PF15058، PF15062، PF15063، PF15064، PF16052، PF16053، PF16055، PF16056، PF16057، PF16060، PF16061، PF16062، PF17027، PF17029، PF17039، PF17041، PF17043، PF17048، PF17050، PF17051، PF17053، PF17054، PF17060، PF18010، PF18011، PF18014، PF18015، PF18020، PF18021، PF18022، PF18023، PF18024، PF18028، PF18031، PF18032، PF18043، PF18050، PF18051، PF18053، PF19003، PF19016، PF19018، PF19017، PF19032، PF19034، PF19036، PF19037، PF19041، PF19043، PF19049، PF19051 ، PF19055، PF19056، PF19065، PF20011، PF20016، PF20017، PF20020، PF20021، PF20033، PF20036، PF20038، PF20039، PF20049، PF20052، PF20055، PF20060، PF20065، PF20078، PF20080، PF21007، PF21010، PF21019، PF21021، PF21024، PF21026، PF21040، PF21058، PF22004، PF22008، PF22014، PF22027، PF22036، PF22049، PF22053، PF22056، PF22022، PF23026، PF23029، PF23031، PF23039، PF23049، PF24005، PF24011.

التحديث 12.12

يقدم برنامج Kaspersky Endpoint Security 12.12 for Windows الميزات والتحسينات التالية:

1. أصبحت حماية المجلدات المشتركة من التشفير الخارجي التي كانت جزءًا من مكون اكتشاف السلوك الآن مكونًا منفصلاً ، باسم مكافحة التشفير.

2. تمت إضافة دعم بروتوكول Kerberos لمصادقة التطبيق عبر خادم وكيل للوصول إلى الإنترنت.

3. يمكنك الآن تحديد تجزئة ملف لتطبيق موثوق به وليس مجرد مسار كامل.

4. يتوافر المزيد من ميزات مهمة فحص مؤشر الاختراق لمستخدمي حلول Endpoint Detection and Response (EDR). تتوفر الآن وظيفة فحص مؤشر الاختراق بأثر رجعي. فحص مؤشر الاختراق بأثر رجعي هو وضع لمهمة فحص IOC يفحص فيها Kaspersky Endpoint Security مؤشرات الاختراق باستخدام البيانات لفترة زمنية معينة. وهذا الوضع مخصص لاكتشاف مؤشرات الاختراق في بيانات نشاط شبكة الكمبيوتر. ويحلل Kaspersky Endpoint Security البيانات في سجلات نظام التشغيل وسجلات المستعرض على الكمبيوتر.

5. يمكن لمستخدمي Kaspersky Endpoint Detection and Response (EDR) إزالة حد حجم العزل. وقد يكون هذا ضروريًا لفحص YARA لأن التطبيق يمكنه حفظ ملف تفريغ ذاكرة كبير. ويمكنك الآن استخدام كل مساحة القرص الخالية لديك للعزل.

6. يتم الآن دعم ضغط HTTPS لتحسين تصدير الأحداث إلى Kaspersky Unified Monitoring and Analysis Platform. ويساعد هذا على تقليل حركة المرور الصادرة.

7. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows، دمجنا التغييرات المضمنة في التصحيحات الخاصة التالية: PF13115، PF13118، PF13119، PF13120، PF13123، PF13124، PF14061، PF14062، PF14064، PF14065، PF14069، PF14070، PF15054، PF15056، PF15058، PF15062، PF15063، PF15064، PF16052، PF16053، PF16055، PF16056، PF16057، PF16060، PF16061، PF16062، PF17027، PF17029، PF17039، PF17041، PF17043، PF17048، PF17050، PF17051، PF17053، PF17054، PF17060، PF18010، PF18011، PF18014، PF18015، PF18020، PF18021، PF18022، PF18023، PF18024، PF18028، PF18031، PF18032، PF18043، PF18050، PF18051، PF18053، PF19003، PF19016، PF19018، PF19017، PF19032، PF19034، PF19036، PF19037، PF19041، PF19043، PF19049، PF19051 ، PF19055، PF19056، PF19065، PF20011، PF20016، PF20017، PF20020، PF20021، PF20033، PF20036، PF20038، PF20039، PF20049، PF20052، PF20055، PF20060، PF20065، PF20078، PF20080، PF21007، PF21010، PF21019، PF21021، PF21024، PF21026، PF21040، PF21058، PF22004، PF22008، PF22014، PF22027، PF22036، PF22049، PF22053، PF22056، PF22022، PF23026، PF23029، PF23031، PF23039، PF23049، PF24005، PF24011.

التحديث 12.11

يوفر برنامج Kaspersky Endpoint Security 12.11 for Windows الميزات والتحسينات التالية:

1. يتحقق التطبيق من تكوين مكونات التحكم قبل حفظ الإعدادات. وتمت إضافة الفحص لمكونات التحكم في التطبيق والتحكم في الأجهزة ومراقبة سلامة النظام. ويعرض التطبيق الآن تحذيرًا إذا كانت الإعدادات الحالية لمكون التحكم قد تؤدي إلى زيادة الحمل على الكمبيوتر أو التسبب في فشل النظام. على سبيل المثال، في حالة التحكم بالتطبيقات، إذا اخترتَ وضع حظر جميع التطبيقات باستثناء المسموح بها، ولم تُضِف أي قاعدة سماح، فسيعرض التطبيق تحذيرًا لأن هذا التكوين قد يُسبب أعطالًا في النظام.

2. تمت إضافة دعم لإرسال الملفات تلقائيًا إلى KATA Sandbox للمراجعة. KATA Sandbox هو أحد مكونات Kaspersky Anti Targeted Attack Platform الذي يقوم بتشغيل الملفات على الصور الافتراضية لأنظمة التشغيل. ويحلل Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Sandbox). لكي يعمل KATA Sandbox تلقائيًا، يجب تثبيت Kaspersky Anti Targeted Attack Platform 8.0 أو أحدث.

3. تم تحسين إرسال بيانات قياس EDR عن بُعد. ويمكنك الآن تحديد الحد الأقصى لطول الحزمة.

4. تم تحسين تشخيص الاتصال بشبكة Kaspersky Security Network. وتم توسيع تفاصيل أخطاء الاتصال الخاصة بشبكة Kaspersky Security Network لحل المشكلات المحتملة.

5. تمت إضافة الدعم لتكوين قوائم الأحداث لإرسالها إلى Kaspersky Unified Monitoring and Analysis Platform (KUMA). الآن، بالإضافة إلى قوائم الأحداث المحددة مسبقًا في KUMA، يمكنك يدويًا إضافة أحداث إلى بيانات القياس عن بُعد أو استبعادها حسب معرّفها في سجل أحداث Windows.

6. تم تحديث واجهة السياسات في Web Console. تم تغيير تخطيط أقسام السياسات للوصول بشكل أسرع إلى الميزات الأساسية.

7. دعم نظام التشغيل Windows 11 25H2.

8. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows، دمجنا التغييرات المضمنة في التصحيحات الخاصة التالية: PF13115 وPF13118 وPF13119 وPF13120 وPF13123 وPF13124 وPF14061 وPF14062 وPF14064 وPF14065 وPF14069 وPF14070 وPF15054 وPF15056 وPF15058 وPF15062 وPF15063 وPF15064 وPF16052 وPF16053 وPF16055 وPF16056 وPF16057 وPF16060 وPF16061 وPF16062 وPF17027 وPF17029 وPF17039 وPF17041 وPF17043 وPF17048 وPF17050 وPF17051 وPF17053 وPF17054 وPF18010 وPF18011 وPF18014 وPF18015 وPF18020 وPF18021 وPF18022 وPF18023 وPF18024 وPF18028 وPF18031 وPF18032 وPF18043 وPF18050 وPF18051 وPF18053 وPF19003 وPF19016 وPF19018 وPF19017 وPF19032 وPF19034 وPF19036 وPF19037 وPF19041 وPF19043 وPF19049 وPF19051 وPF19055 وPF19056 وPF20011 وPF20016 وPF20017 وPF20020 وPF20021 وPF20033 وPF20036 وPF20038 وPF20039 وPF20049 وPF20052 وPF20055 وPF20060 وPF20065 وPF21007 وPF21010 وPF21019 وPF21021 وPF21024 وPF21026 وPF22004 وPF22008 وPF22014.

التحديث 12.10

يوفر برنامج Kaspersky Endpoint Security 12.10 for Windows الميزات والتحسينات التالية:

1. بالنسبة لمكون منع هجمات BadUSB، تمت إضافة الخيار للسماح بأجهزة فحص الرموز الشريطية من خلال قراءة رمز شريطي من الشاشة. ولن تحتاج الآن إلى إدخال رمز باستخدام لوحة المفاتيح على الشاشة للسماح بالماسحات الضوئية للرموز الشريطية.

2. تتوفر الميزات والتحسينات التالية لمستخدمي حلول Endpoint Detection and Response (EDR) بواسطة Kaspersky.

- يمكنك الآن إدارة عزل شبكة الاتصال الخاصة بالكمبيوتر في تفاصيل التنبيه. بالإضافة إلى ذلك، في تفاصيل التنبيه يمكنك تحديد الفترة الزمنية لعزل شبكة الاتصال الخاصة الكمبيوتر وإضافة استثناءات.

- تعبئة تفاصيل التنبيه ببيانات جديدة. الآن أصبحت تفاصيل التنبيه تحتوي على معلومات أكثر عن التهديد، بما في ذلك كيفية تصرف التطبيق عند الاستجابة لتهديدات EDR.

- تم تحسين معالجة ملفات مؤشرات الاختراق. ويمكنك الآن عرض وتحرير محتويات ملفات مؤشرات الاختراق في واجهة Kaspersky Security Center Web Console. وبعد تحميل ملف مؤشرات الاختراق، يعرض التطبيق تقريرًا عن تطبيق شروط مؤشرات الاختراق.

- استجابة محسنة لمؤشرات الاختراق المكتشفة. يمكنك الآن عزل الملفات التي تم اكتشافها بواسطة مهمة فحص مؤشرات الاختراق مباشرة في نتائج اكتشاف مؤشرات الاختراق في خصائص المهمة. ويمكنك أيضًا عزل أجهزة الكمبيوتر عن الشبكة في خصائص المهمة.

- الآن، يمكنك إنشاء ملفات مؤشرات الاختراق (IOC) مباشرةً في خصائص مهمة فحص مؤشرات الاختراق بالاعتماد على قوائم تجزئات الملفات، أو عناوين IP، أو أسماء DNS التي يتم إنشاؤها في ملف TXT.

- توسيع نطاق الفحص لمهمة فحص مؤشرات الاختراق. ويمكنك الآن تحديد نطاق فحص مؤشرات الاختراق للتسجيل (**تسجيل Windows - Registryltem**). وفي الإصدارات السابقة من التطبيق، كان بإمكانك فقط استخدام نطاق فحص مؤشرات الاختراق المحدد مسبقًا في التسجيل.

3. تمت إضافة إذن حماية جديد بكلمة مرور، تصدير الإعدادات. وبشكل افتراضي، يستطيع مستخدم KLAdmin فقط إنشاء ملف تكوين باستخدام إعدادات Kaspersky Endpoint Security في واجهة التطبيق. ولمنح حق الوصول إلى مستخدمين آخرين، تحتاج إلى منحهم الإذن المقابل.

4. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows، قمنا بتضمين التغييرات المدرجة في التصحيحات الخاصة التالية: PF12120، PF12121، PF12122، PF13115، PF13118، PF13119، PF13120، PF13123، PF14061، PF14062، PF14064، PF14065، PF15054، PF15056، PF15058، PF15062، PF16052، PF16053، PF16055، PF16056، PF16057، PF17027، PF17029، PF17039، PF17041، PF17043، PF17048، PF17050، PF18010، PF18011، PF18014، PF18015، PF18020، PF18021، PF18022، PF18023، PF18024، PF18028، PF18031، PF18032، PF18043، PF19003، PF19016، PF19018، PF19017، PF19032، PF19034، PF19036، PF19037، PF19041، PF19043، PF19049، PF20011، PF20016، PF20017، PF20020، PF20021، PF20033، PF20036، PF20038، PF20039، PF20049، PF21007.

التحديث 12.9

يوفر برنامج Kaspersky Endpoint Security 12.9 for Windows الميزات والتحسينات التالية:

1. تم إضافة وظائف جديدة لإدارة كلمات المرور المؤقتة. وتتيح لك كلمة المرور المؤقتة توفير الوصول إلى Kaspersky Endpoint Security مع تمكين حماية كلمة المرور لجهاز كمبيوتر منفصل. تسمح إدارة كلمات المرور المؤقتة بحفظ سجل كلمات المرور (حتى 30 يومًا)، ومراقبة حالة كلمة المرور المؤقتة (فعال ومنتهي الصلاحية وتم الإبطال) وإلغاء كلمات المرور المؤقتة.

2. تمت إضافة خيار إنهاء الاتصال بموارد الويب المحظورة بواسطة Web Control مباشرة بعد تطبيق السياسة. وفي الإصدارات السابقة من التطبيق، كان مكون Web Control يقيد الاتصالات الجديدة فقط بموارد الويب المحظورة.

3. بالنسبة لمستخدمي Kaspersky Anti Targeted Attack Platform، تمت إضافة خيار لتشغيل فحص YARA محليًا على الكمبيوتر. ولفعل ذلك، تحتاج إلى تنزيل ملف بقواعد YARA وتنفيذ الأمر في CMD.

4. تم إصلاح سلوك التطبيق عند تمكين BitLocker على أجهزة الكمبيوتر التي تكون محركات الأقراص عليها محمية بالفعل بواسطة BitLocker باستخدام أدوات طرف خارجي. ويبدأ Kaspersky Endpoint Security إجراء الاسترداد لإرسال مفتاح الاسترداد إلى Kaspersky Security Center. وبالتالي، يتم نقل إدارة BitLocker إلى وحدة تحكم Kaspersky Security Center.

5. يتوافر قسم جديد، **Response history**، لمستخدمي حلول Detection and Response من قبل Kaspersky. ويحتوي هذا القسم على معلومات عن إجراءات الاستجابة للتهديد التي يتم تنفيذها على الكمبيوتر. وتتضمن هذه الإجراءات، على سبيل المثال ، تشغيل مهمة إنهاء العملية أو عزل الكمبيوتر عن الشبكة. ويتوفر سجل الاستجابة فقط لمستخدمي حلول Kaspersky التالية: MDR وEDR وKATA.

6. بالنسبة لمستخدمي Kaspersky Unified Monitoring and Analysis Platform، فإن دعم إجراءات الاستجابة للتهديدات لحل EDR متاح الآن. وعند الاستجابة للتهديدات، يدير KUMA البرامج النصية التي تنشئ مهام EDR المقابلة. ولتنفيذ مهام EDR، تحتاج إلى إنشاء قاعدة استجابة للبرنامج النصي المخصص في وحدة تحكم KUMA وتحديد الأحداث.

7. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows، قمنا بتضمين التغييرات المدرجة في التصحيحات الخاصة التالية: PF10360، PF10362، PF10363، PF12120، PF12121، PF12122، PF13115، PF13118، PF13119، PF14061، PF14062، PF14064، PF14065، PF15054، PF15056، PF15058، PF16052، PF16053، PF16055، PF16056، PF17027، PF17029، PF17039، PF17041، PF17043، PF18010، PF18011، PF18014، PF18015، PF18020، PF18021، PF18022، PF18023، PF18024، PF18028، PF19003، PF19016، PF19018، PF19017، PF19032، PF19034، PF19036، PF19037، PF19041، PF20011، PF20016، PF20017، PF20020، PF20021.

التحديث 12.8

يوفر برنامج Kaspersky Endpoint Security 12.8 for Windows الميزات والتحسينات التالية:

1. يدعم التطبيق الآن وضع Light Agent لحماية البيئات الافتراضية. ويمكنك الآن نشر التطبيق في شكل Light Agent كجزء من حل Kaspersky Security for Virtualization Light Agent 6.2.

2. اعتراض عمليات الملفات في حاويات Docker على الخادم مدعوم الآن. الحاوية هي بيئة معزولة حيث يمكن تشغيل أحد التطبيقات دون التفاعل المباشر مع نظام التشغيل. يفحص Kaspersky Endpoint Security الملفات الموجودة داخل الحاويات التي يمكن للمستخدم الوصول إليها. وعند اكتشاف تهديد، تمنع التطبيقات هذا النشاط الضار وتحاول تنظيف الملف داخل الحاوية. وإذا تعذر تنظيف الملف، يوقف التطبيق الحاوية.

3. يمكنك الآن تحديد نطاق حماية لحماية المجلدات المشتركة ضد التشفير الخارجي (مكون اكتشاف السلوك). ويمكنك الآن تحديد المجلدات المشتركة التي يجب على التطبيق مراقبتها لمتابعة نشاط الملف. ويمكنك أيضًا استثناء الملفات من نطاق الحماية. وفي الإصدارات السابقة من التطبيق، كان مكون اكتشاف السلوك يراقب جميع المجلدات المشتركة لمتابعة نشاط الملفات.

4. يمكنك الآن تكوين مجموعات مختلفة من المكونات لأنواع مختلفة من أنظمة التشغيل في حزمة التثبيت. ويعني هذا أنه يمكنك نشر التطبيق على محطات العمل والخوادم باستخدام حزمة التثبيت نفسها. ويتم استثناء المكونات غير المتوفرة لنوع معين من أنظمة التشغيل تلقائيًا في خصائص حزمة التثبيت.

5. تمت إضافة خيار تحديد استثناءات الفحص المحددة مسبقاً والتطبيقات الموثوق بها. وتسمح استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة بتكوين المنطقة الموثوقة بسرعة للتطبيق في بيئة افتراضية (Citrix وVMware). وتشمل هذه الاستثناءات، على سبيل المثال، ملفات الجهاز الافتراضي VHD وLDF. ويمكن إضافة الاستثناءات عند إنشاء حزمة تثبيت التطبيق أو إنشاء سياسة أو عند تثبيت Kaspersky Endpoint Security.

6. يتضمن القياس عن بُعد في EDR الآن أحداثًا للعمليات مع الأجهزة المتصلة عن طريق USB. ويمكنك أيضًا إضافة هذه الأحداث إلى الاستثناءات من القياس عن بُعد في EDR.

7. تمت إضافة خيار منع اتصالات الشبكة عبر بروتوكول TLS 1.0 القديم. ويتمتع بروتوكول TLS 1.0 بمستوى أمان منخفض، لذا يوصى بتعطيل هذا البروتوكول واستخدام إصداري TLS 1.2 أو TLS 1.3 الأحدث. وبشكل افتراضي، يمنع Kaspersky Endpoint Security اتصالات بروتوكول TLS 1.0. وبعد تحديث إصدار التطبيق، قد يفشل تشغيل خدمات الجهات الخارجية التي تستخدم بروتوكول TLS 1.0. ولتجنب المشاكل في تشغيل خدمات الجهات الخارجية، يمكنك السماح باستخدام بروتوكول TLS 1.0 في سياسة المجموعة قبل تحديث إصدار التطبيق.

8. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows، دمجنا التغييرات المضمنة في التصحيحات الخاصة التالية: PF10053 وPF10054 وPF10360 وPF10362 وPF10363 وPF12120 وPF12121 وPF12122 وPF13115 وPF13118 وPF13119 وPF14061 وPF14062 وPF14064 وPF14065 وPF15054 وPF15056 وPF15058 وPF16052 وPF16053 وPF16055 وPF16056 وPF17027 وPF17029 وPF17039 وPF17041 وPF17043 وPF18010 وPF18011 وPF18014 وPF18015 وPF18020 وPF18021 وPF18022 وPF18023 وPF18024 وPF18028 وPF19003 وPF19016 وPF19018.

التحديث 12.7

يوفر برنامج Kaspersky Endpoint Security 12.7 for Windows الميزات والتحسينات التالية:

1. يمكنك الآن تقييد استخدام موارد وحدة المعالجة المركزية لمهام فحص البرامج الضارة. ولفعل ذلك، في إعدادات التطبيق، حدد الحد الأقصى لنسبة تحميل وحدة المعالجة المركزية لجميع النوى التي يمكن استخدامها أثناء فحص الكمبيوتر.

2. يمكنك الآن يدويًا إرسال الملفات لفحصها في KATA Sandbox. KATA Sandbox هو أحد مكونات Kaspersky Anti Targeted Attack Platform الذي يقوم بتشغيل الملفات على الصور الافتراضية لأنظمة التشغيل. ويحلل Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Sandbox). لإرسال ملف للفحص إلى KATA Sandbox، حدد الأمر ذي الصلة في قائمة السياق للملف.

3. يمكنك الآن إعداد التكامل مع الحل الذي يحمي شبكة الاتصال المحلية الخاصة بالشركة، Kaspersky Network Detection and Response. Kaspersky Network Detection and Response (NDR) جزء من Kaspersky Anti Targeted Attack Platform. ويمكنك تكوين التفاعل مع NDR في الوضع القياسي وكذلك في وضع عميل EDR.

4. تمت إضافة دعم إصدار عميل البريد Microsoft Office Outlook 2021 إلى ملحق الحماية من تهديدات البريد. يسمح الملحق بفحص الرسائل على مستوى عميل البريد بدلاً من مستوى البروتوكول. وبالإضافة إلى الرسائل، يتيح لك الملحق فحص الكائنات المستلمة عبر واجهة MAPI من مستودعات Microsoft Exchange (على سبيل المثال، الكائنات الموجودة في التقويم). ويجري هذا الفحص في عميل البريد.

5. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows، دمجنا التغييرات المضمنة في التصحيحات الخاصة التالية: PF10049 وPF10355 وPF12114 وPF13109 وPF14056 وPF15038 وPF15045 وPF16037 وPF16042 وPF16047 وPF17014 وPF17018 وPF17021 وPF17024 وPF18006 وPF18007.

التحديث 12.6

يوفر برنامج Kaspersky Endpoint Security 12.6 for Windows الميزات والتحسينات التالية:

1. تمت إضافة وظيفة التكامل مع حل Kaspersky SIEM – Kaspersky Unified Monitoring and Analysis Platform (KUMA). وأصبح من الممكن الآن إرسال الأحداث من سجلات أحداث Windows إلى أداة تجميع KUMA. ويتيح ذلك لحل KUMA بتلقي أحداث Windows (يتم دعم مجموعة محدودة من معرفات الأحداث) من جميع أجهزة الكمبيوتر المثبت عليها Kaspersky Endpoint Security، دون تثبيت عملاء KUMA على أجهزة الكمبيوتر هذه.

2. تمت إضافة مكون مراقبة سلامة النظام جديد ليحل محل مكون مراقبة سلامة الملفات. يتضمن مكون مراقبة سلامة النظام كل وظائف مراقبة سلامة الملفات ويسمح بالإضافة إلى ذلك بمراقبة تغييرات السجل واتصال الأجهزة الخارجية. يراقب مكون مراقبة سلامة النظام التغييرات في نظام التشغيل التي قد تشير إلى خروقات أمان الكمبيوتر. وعند اكتشاف هذه التغييرات، ينشئ Kaspersky Endpoint Security الأحداث المقابلة وينبه المسؤول. لم تعد مراقبة سلامة الملفات جزءًا من التطبيق. ويتم ترحيل إعدادات مراقبة سلامة الملفات تلقائيًا إلى مراقبة سلامة النظام عند تحديث التطبيق. لضمان التشغيل الصحيح لنظام مراقبة سلامة النظام، يجب تحديث كل من تطبيق Kaspersky Endpoint Security والمكوّن الإضافي للإدارة إلى الإصدار 12.6.

3. تمت إضافة حالة EDR Agent المُضمن المثبت (KATA) إلى خصائص الكمبيوتر في وحدة تحكم Kaspersky Security Center. والآن، إذا كان لديك EDR Agent مضمن (KATA) مُثبتًا، سيعرض عمود **حالة Endpoint Sensor** الحالة الحالية للمكون (على سبيل المثال، قيد التشغيل ومتوقف وغير مدعوم من الترخيص، وما إلى ذلك).

4. تمت إضافة خيار تحديد استثناءات الفحص المحددة مسبقاً والتطبيقات الموثوق بها. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوق بها على تكوين المنطقة الموثوق بها بسرعة عند استخدام التطبيق على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager. وتشمل هذه الاستثناءات، على سبيل المثال، ملفات قاعدة البيانات MDF وLDF. ويمكن إضافة الاستثناءات عند إنشاء سياسة جديدة أو تعديل سياسة موجودة أو عند تثبيت Kaspersky Endpoint Security.

5. تم نقل عرض تفاصيل التنبيه لحل Kaspersky Endpoint Detection and Response Optimum من المكون الإضافي لإدارة Kaspersky Endpoint Security إلى مكون إضافي منفصل لإدارة Kaspersky Endpoint Detection and Response. والمكون الإضافي لإدارة EDR هو مكون إضافي واحد للعمل مع العملاء على أنظمة تشغيل Windows وMac وLinux. والآن، عند العمل مع EDR Optimum، ستحتاج إلى مكون إدارة Kaspersky Endpoint Security الإضافي لإنشاء مهام الاستجابة للتهديدات والمكوّن الإضافي لإدارة EDR لعرض تفاصيل التنبيه.

6. دعم نظام التشغيل Windows 11 24H2.

7. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows ، قمنا بدمج التغييرات المضمنة في التصحيحات الخاصة التالية: pf10048، pf10353، pf12106، pf12107، pf12108، pf13090، pf13100، pf15031، pf15034، pf15036، pf16021، pf16023، pf16029، pf17002.

التحديث 12.5

يوفر برنامج Kaspersky Endpoint Security 12.5 for Windows الميزات والتحسينات التالية:

1. تمت إضافة خيار تكوين استثناءات القياس عن بُعد. القياس عن بعد عبارة عن قائمة الأحداث التي وقعت على الكمبيوتر المحمي. يتم استخدام بيانات القياس عن بُعد بواسطة Kaspersky Anti Targeted Attack Platform (EDR) لمراقبة وحماية البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويساعد تكوين استثناءات القياس عن بُعد بتحسين أداء الكمبيوتر وتحسين إرسال البيانات إلى خادم جمع القياس عن بُعد.

2. تم تحسين واجهة المنطقة الموثوقة للتطبيق. ويخفي Kaspersky Endpoint Security الآن كائنات المنطقة الموثوقة عن المستخدم إذا منع المسؤول المستخدم من إضافة استثناءات الفحص (المحلية) الخاصة به والتطبيقات الموثوقة. ويمنع هذا الوصول غير المصرح به إلى المنطقة الموثوقة بواسطة المتسلل، مما يزيد من مستوى أمان الكمبيوتر.

3. تمت إضافة خيار فحص حركة المرور لعملاء بريد MyOffice Mail وR7-Office Organizer. ولا يفحص مكون الحماية من تهديدات البريد الآن مرفقات الرسائل عند التنزيل فحسب، بل يفحص أيضًا الرسائل المرسلة والمستلمة.

4. تمت إضافة فئة جديدة من موارد الويب أدوات الذكاء الاصطناعي التوليدية. ويمكنك تكوين الوصول إلى مواقع الويب من الفئة الجديدة باستخدام التحكم في الويب.

5. يمكنك الآن تحديد موقع قاعدة حزمة شبكة في قائمة جدار الحماية. ويحدد موقع قاعدة حزمة الشبكة في القائمة أولويتها. وفي الإصدارات السابقة من التطبيق، كان من الممكن إضافة قاعدة جديدة فقط إلى نهاية القائمة، وبعد ذلك كان يتعين عليك نقل القاعدة يدويًا عبر القائمة لتحديد أولوياتها. والآن، عند إضافة قاعدة، يمكنك اختيار ما إذا كان ينبغي وضع القاعدة في بداية القائمة أو في نهايتها أو بجوارها.

6. في قواعد مكونات Kaspersky Endpoint Security، يمكنك الآن تحديد المستخدمين ليس فقط من Active Directory، لكن أيضًا من قائمة المستخدمين في Kaspersky Security Center. ويمكنك أيضًا إدخال بيانات حساب المستخدم المحلي يدويًا. وتمت إضافة هذا الاحتمال لقواعد المكونات التالية: التحكم في التطبيقات، والتحكم في الجهاز، والتحكم في الويب، ومراقبة عيوب التكيف، وفحص السجل.

7. يتضمن تقرير اكتشاف هجوم شبكة الاتصال الآن عمودًا عن عنوان MAC للكمبيوتر المهاجم (مكون الحماية من تهديدات الشبكة). ويمكنك الآن رؤية عنوان MAC للكمبيوتر المهاجم في التقرير بالإضافة إلى عنوان IP الخاص به. وهذا مفيد للتحقيق في الحادث. وستكون التقارير، التي تحتوي على عنوان MAC للكمبيوتر المهاجم، متاحة أيضًا في الإصدار 15.1 وأحدث من وحدة تحكم Kaspersky Security Center Linux.

8. تم زيادة مستوى متطلبات حماية الكمبيوتر. يتطلب مستوى الحماية العالي الآن تمكين حماية خدمات التطبيقات من الإدارة الخارجية. تحقق من مؤشر مستوى الأمان في الجزء العلوي من نافذة السياسة. وإذا كان لديك مستوى أمان متوسط أو منخفض، يمكنك تمكين حماية خدمات التطبيقات من الإدارة الخارجية في نافذة توصية مؤشر مستوى الأمان.

9. تمت إضافة دعم للأحداث الجديدة لاكتشاف الكائنات عند تشغيل التطبيق في تكوين Endpoint Detection and Response Agent (EDR Agent). ويتم دعم هذه الأحداث بالفعل في تكوين [KES+العميل المدمج].

10. عند تطوير هذا الإصدار من Kaspersky Endpoint Security for Windows ، قمنا بدمج التغييرات المضمنة في التصحيحات الخاصة التالية: pf9640، pf9830، pf9831، pf10047، pf10351، pf12102، pf12105، pf13084، pf13089، pf14040، pf14047، pf15026، pf15028، pf16013.

التحديث 12.4

يوفر برنامج Kaspersky Endpoint Security 12.4 for Windows الميزات والتحسينات التالية:

1. تمت إضافة وظائف جديدة لحماية اتصال الكمبيوتر بحل Kaspersky Security Center. تتيح مهمة حماية الاتصال بخادم الإدارة الجديدة تعيين كلمة مرور للاتصال بخادم موثوق به. ويعني هذا أنه من غير الممكن إعادة توصيل الكمبيوتر وتشغيل الأوامر من خادم آخر بدون كلمة المرور هذه.

2. بالنسبة لمكون الحماية بكلمة المرور، تمت إضافة القدرة على تحديد المستخدمين ليس فقط من Active Directory. أي أنه يمكنك تحديد اسم مستخدم وكلمة مرور يدويًا وتعيين حقوق الوصول إلى Kaspersky Endpoint Security لهذا الحساب. وبهذه الطريقة، لن تحتاج إلى مشاركة كلمة مرور KLAdmin الخاصة بك مع مستخدمين آخرين أو إنشاء حسابات Active Directory جديدة للتحكم في الوصول إلى التطبيق.

3. دعم نظام التشغيل Windows 11 23H2.

التحديث 12.3

يوفر برنامج Kaspersky Endpoint Security 12.3 for Windows الميزات والتحسينات التالية:

1. الآن يمكنك تثبيت التطبيق في تكوين Endpoint Detection and Response Agent. ويسمح هذا التكوين بتثبيت التطبيق مع مجموعة من المكونات التي تتطلبها حلول Kaspersky Detection and Response من Kaspersky: Kaspersky Managed Detection and Response، وKaspersky Anti Targeted Attack Platform (EDR). ويمكنك تثبيت التطبيق بهذا التكوين إلى جانب حلول الجهات الخارجية (على سبيل المثال، Dr.Web وDallas Lock وESET). ويتيح لك ذلك استخدام أدوات أمان البنية التحتية التابعة لجهات خارجية إلى جانب Kaspersky Detection and Response بواسطة Kaspersky.

2. تم تحسين تشغيل Kaspersky Endpoint Security مع أجهزة Bluetooth. ويمكنك الآن تكوين الاستثناءات وتقييد الوصول إلى جميع أجهزة Bluetooth باستثناء أجهزة الإدخال (لوحات المفاتيح وأجهزة الماوس اللاسلكية وما إلى ذلك).

3. تم تحسين تشغيل مكون التحكم في التطبيقات مع قاعدة بيانات الملفات القابلة للتنفيذ. ويزيل Kaspersky Endpoint Security الآن تلقائيًا معلومات الملف من قاعدة البيانات في حالة حذف الملف من الكمبيوتر. ويسمح ذلك بالحفاظ على قاعدة البيانات مُحدثة وحفظ موارد Kaspersky Security Center.

4. تم زيادة مستوى متطلبات حماية الكمبيوتر. يتطلب مستوى الحماية العالي الآن تمكين الحماية بكلمة المرور. تحقق من مؤشر مستوى الأمان في الجزء العلوي من نافذة السياسة. وإذا كان لديك مستوى حماية متوسط أو منخفض، يمكنك تمكين الحماية بكلمة مرور في نافذة توصيات مؤشر مستوى الأمان.

5. تمت إضافة دعم بروتوكول HTTPS لتمكين التطبيق من العمل مع Kaspersky Security Network. قم بتمكين استخدام بروتوكول HTTPS في خصائص خادم الإدارة في إعدادات خادم وكيل KSN.

التحديث 12.2

يوفر برنامج Kaspersky Endpoint Security 12.2 for Windows الميزات والتحسينات التالية:

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

2. يمكنك الآن اختيار بروتوكول ومنافذ لاستثناءات الحماية من تهديدات الشبكة. والآن بالإضافة إلى تحديد عناوين IP للأجهزة الموثوقة، يمكنك أيضًا تحديد منفذ وبروتوكول. ويتيح لك هذا استبعاد تدفقات البيانات الفردية ومنع هجمات الشبكة من عناوين IP الموثوقة.

3. ترتيب مختلف لمصادر التحديث لمهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق المحلية إذا تم تطبيق سياسة على الكمبيوتر. ويتم الآن استخدام خادم Kaspersky Security Center افتراضيًا كمصدر التحديث الأول بدلاً من خوادم Kaspersky. ويساعد هذا على حفظ حركة المرور عندما يقوم المستخدم بتشغيل مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق المحلية.

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. تضمن هذه الميزة العرض الصحيح لحالة الجهاز الافتراضي في Azure في وحدة تحكم 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.

المشكلات التي تم إصلاحها

يسرد الجدول أدناه جميع المشكلات المكتشفة في الإصدارات السابقة من Kaspersky Endpoint Security والتي تم إصلاحها في الإصدار الحالي.

قائمة المشكلات التي تم إصلاحها في الإصدار 14.2

المعرف	الوصف
10110351	يسمح مكون التحكم في الجهاز بالوصول إلى جهاز MTD (بطاقة SD) عند تحديد الإجراء **منع** لنوع الجهاز **محركات الأقراص القابلة للإزالة**.
10068496	على جهاز محمي، يمكن تغيير وضع الحماية من انتحال عنوان MAC عندما تكون إعدادات الحماية من تهديدات الشبكة قفلة في السياسة الرئيسية.
10095087	عند تمكين فحص الاتصالات المشفرة، يؤدي الوصول إلى أي موقع ويب من خلال جدار حماية من الجيل التالي (NGFW) بشهادة ملغاة إلى تشغيل إخطار يفيد بإعادة التوجيه إلى مجال بشهادة غير موثوقة.
10140912	عند تثبيت التطبيق، لا يتعرف الكمبيوتر على جهاز المساعد الرقمي الشخصي BHT1100B الذي يعمل بنظام Windows Mobile.
10141009	إذا كان مكون تشفير الملفات مُثبتًا، فقد يتعذر تشغيل تطبيق Anthropic Claude.
10610853	بعد الترقية إلى الإصدار الجديد، يتعذر فتح السياسة لأن إعدادات التحكم في الجهاز في الإصدار الجديد تتضمن أجهزة غير مدعومة في الإصدار السابق.
10720516	قد يتعذر فتح المرفقات الموجودة في ملفات بتنسيقات Office باستخدام التطبيق المثبّت.
10421967	يفشل تسجيل الدخول إلى صندوق بريد مشترك إذا تمت إضافة صندوق البريد هذا كحساب منفصل.

قائمة المشكلات التي تم إصلاحها في المكون الإضافي للويب، الإصدار 14.2.0.8289

المعرف	الوصف
9946286	عند إضافة عنوان موقع ويب إلى إحدى قواعد التحكم في الويب، يتعذر استخدام قناع لا يتضمن نقطة بين المجال ومنطقة المجال.
10054657 10507166	بعد الترحيل إلى الإصدار الجديد، لا يمكن إدارة بعض المكونات (مثل التحكم في الجهاز وApplication Control) عبر السياسة.
10084390	في إعدادات مكون التحكم في الجهاز، يتكرر نوع الجهاز **محرك الأقراص الثابت**، مما يؤدي إلى حظر محركات الأقراص الثابتة الخاصة بالمستخدم.
10113718	في بعض الحالات، لا يتم عرض قواعد جدار الحماية المخصصة.
10311613	في إعدادات مكون Host Intrusion Prevention، ليس من الممكن إضافة مورد محمي بواسطة القناع باستخدام حرف `*`.
10391923	في مكون التحكم في التطبيق، عند إنشاء فئة تطبيق بناءً على تجزئة MD5 لملف، لا يظهر أي تحذير يفيد بأن هذه الفئة غير صالحة ولن تعمل.
10571790	بالنسبة لمكون Application Control، تم تصحيح عنوان قائمة قواعد الحظر في وضع **Allow all except the rules list**.
10592891 10689065	في المنطقة الموثوقة، لا يتم عرض حقل **Comment** الحقل للاستثناءات في قسم **Malware Scan exclusions**.
10613015 10689049 10592534	في مكون التحكم في الجهاز، لا يتم عرض حقل **Comment** للأجهزة الموثوقة.
10645068 10689057	لا تعمل مهمة Remove key في حالة تحديد ملف مفتاح ترخيص بتنسيق KEY.
10685370 10685422	في مكون التحكم في الجهاز، تتعذر إضافة جهاز جديد إلى قائمة الأجهزة الموثوقة إذا كان هناك جهاز يحمل هذا الاسم بالفعل في القائمة.
10721136	لا يمكن حفظ المهام الجماعية إذا لم يتم تحديد تاريخ إكمال في إعدادات الجدول.
10753509	قد يؤدي تعديل قائمة المستخدمين والمجموعات للأجهزة الموثوقة في مكون التحكم في الجهاز إلى تغيير أنواع السجلات، مما يتسبب في عدم تطبيق الإعدادات على الجهاز بعد ذلك.
10773402	في بعض الحالات، قد لا يتم حفظ التغييرات على إعدادات السياسة بسبب ملفات التعريف التالفة.
10822620	لا يتم عرض إعدادات مكون مكافحة أداة التشفير في السياسة، ولا يتم حفظ التغييرات التي تم إجراؤها على إعدادات الإخطارات.
10817035	في السياسة الفرعية، يُسمح بإضافة جهاز موثوق حتى إذا كان هذا الإعداد معطلاً في السياسة الأصلية (رمز "القفل" مغلق). ومع ذلك، لا يتم حفظ الجهاز المضاف.
10678009	في المكون الإضافي للويب لبرنامج Kaspersky Endpoint Security، تفشل إضافة قاعدة جدار حماية جديدة إلى السياسة إذا تم إنشاء قاعدة مسبقًا باستخدام نطاق عناوين IP.

قائمة المشكلات التي تم إصلاحها في الإصدار 14.1

المعرف	الوصف
10140523	قد يؤدي تمكين خيار Native NVMe في نظام التشغيل Windows 11 إلى عدم استقرار سلوك التطبيقات.
9340076	على الجهاز المُثبّت عليه التطبيق وتم تمكين ميزة تشفير الملفات عليها، لا يقوم Windows Explorer بتحديث محتويات مجلد الشبكة تلقائيًا بعد تعديله من جهاز آخر.
9722863	لا يتضمن تقرير التحكم في الأجهزة حدث قطع اتصال رمز USB المميز.
10006481	بعد تطبيق قاعدة ترفض حركة المرور الواردة، قد يتم إنهاء اتصالات TCP النشطة بالخدمات الخارجية قبل الأوان بسبب حساب المهلة غير الصحيح.
10140912	لا يكتشف التطبيق جهاز المساعد الرقمي الشخصي BHT1100B.
10157563	قد لا يعمل خيار Folder Redirection بعد إعادة تشغيل محطات عمل VDI.
10158494	يسجل التحكم في الأجهزة أحداث الاتصال وقطع الاتصال المتعددة لجهاز قابل للإزالة دون إعادة توصيله فعليًا.

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؟

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؟

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؟

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.



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 حل Endpoint Detection and Response، 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.

القسم	المكون
الحماية من التهديدات الأساسية	**الحماية من تهديدات الملفات** يتيح لك مكون الحماية من تهديدات الملفات منع إصابة نظام ملفات الكمبيوتر. وبشكل افتراضي، يوجد مكون الحماية من تهديدات الملفات بشكل دائم في ذاكرة الوصول العشوائي للكمبيوتر ويفحص جميع الملفات التي يتم فتحها وحفظها وبدء تشغيلها، في الوقت الحقيقي. ويفحص هذا المكون الملفات الموجودة على جميع محركات أقراص الكمبيوتر، بما في ذلك 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 الاتصال بمواقع الويب الضارة والخاصة بالتصيد الاحتيالي. 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. 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 • MyOffice Mail • R7-Office Organizer لفحص حركة البيانات في عملاء بريد Mozilla Thunderbird وMyOffice Mail وR7-Office Organizer، فإنك تحتاج إلى إضافة شهادة Kaspersky إلى مخزن الشهادات وتحديد مخزن الشهادات الخاص. 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 إصدارات 32 بت و64 بت من Outlook 2010 و2013 و2016 و2019 و2021 و2024 و365. وعلى أجهزة الكمبيوتر المستندة إلى بنية Arm، يدعم ملحق الحماية من تهديدات البريد إصدارات 32 بت و64 بت من Outlook 2016 وOutlook 2021 وOutlook 2024 وOutlook 365 for Arm64. **الحماية من تهديدات الشبكة** يراقب مكون الحماية من تهديدات الشبكة (يسمى أيضًا Intrusion Detection System، IDS) حركة شبكة الاتصال الواردة للبحث عن خاصية النشاط لهجمات الشبكة. عندما يكتشف التطبيق محاولة هجوم على الشبكة على كمبيوتر مستخدم، فإنه يحظر اتصال الشبكة مع الكمبيوتر المهاجم. وتتوفر أوصاف لأنواع هجمات الشبكة المعروفة حاليًا وطرق إبطالها في قواعد بيانات التطبيق. يتم تحديث قائمة هجمات الشبكة التي يكتشفها مكون الحماية من تهديدات الشبكة أثناء تحديثات قاعدة البيانات والوحدة النمطية للتطبيق. **جدار الحماية** يمنع مكون جدار الحماية الاتصالات غير المصرح بها لجهاز كمبيوتر 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.

القسم	المكون
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. في حال مشاركتك في Kaspersky Security Network (KSN)، فإن خدمات KSN تزود Kaspersky Endpoint Security بمعلومات عن سمعة عناوين الويب المفحوصة، بالإضافة إلى معلومات عن فئة وسمعة الملفات التي يتم 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. وتعتمد وظيفة Kaspersky Endpoint Security على توقيعات تدفق السلوك وتوفر دفاعًا استباقيًا للكمبيوتر. بالإضافة إلى ذلك، يراقب مكون اكتشاف السلوك منافذ الشبكة لعمليات التطبيق التي قد تهدد أمان الكمبيوتر. ويحصل التطبيق على معلومات عن هذه العمليات مع قواعد بيانات مكافحة الفيروسات. **مكافحة أداة التشفير** يحلل مكون مكافحة التشفير النشاط في المجلدات المشتركة. إذا توافق هذا النشاط مع توقيع تدفق السلوك المشابه للتشفير الخارجي، فإن Kaspersky Endpoint Security يقوم باتخاذ الإجراء المحدد. **منع الاستغلال** يكتشف مكون منع الاستغلال 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. بالإضافة إلى ذلك، يراقب مكون منع الاستغلال منافذ الشبكة لعمليات التطبيق التي قد تهدد أمان الكمبيوتر. ويحصل التطبيق على معلومات عن هذه العمليات مع قواعد بيانات مكافحة الفيروسات. **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 مكون 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 كمبيوتر (على سبيل المثال، الأقراص الصلبة أو الكاميرات أو وحدات شبكة Wi-Fi). ويتيح لك هذا حماية جهاز الكمبيوتر من الإصابة بالفيروسات عند اتصال مثل هذه الأجهزة به، ومنع فقدان البيانات أو تسريباتها. **التحكم في الويب** يقوم المكون التحكم في الويب بإدارة وصول المستخدم 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** 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. **مراقبة سلامة النظام** يراقب مكون مراقبة سلامة النظام التغييرات في نظام التشغيل التي قد تشير إلى خروقات أمان الكمبيوتر. وعند اكتشاف هذه التغييرات، ينشئ Kaspersky Endpoint Security الأحداث المقابلة وينبه المسؤول.

القسم	المكون
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 قواعد البيانات والوحدات النمطية للتطبيق** 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 سلامة التطبيق** 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 	**التشفير على مستوى الملف** 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. **تشفير محركات الأقراص القابلة للإزالة** 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. **Endpoint Detection and Response Expert (on-premises) و Network Detection and Response (KATA)** العملاء المدمجون لإدارة مكوني Endpoint Detection and Response و Network Detection and Response التي تعد جزءًا من حل Kaspersky Anti Targeted Attack Platform. Kaspersky Anti Targeted Attack Platform عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. تتضمن Kaspersky Anti Targeted Attack Platform ثلاث وحدات وظيفية: • Kaspersky Anti Targeted Attack Platform (KATA) • Kaspersky Endpoint Detection and Response (EDR (KATA)) • Network Detection and Response (NDR (KATA)) يمكنك شراء جميع الوحدات الوظيفية أو الوحدات الوظيفية الفردية بشكل منفصل. وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform. **Sandbox** عميل مدمج لأجل Sandbox. ويكتشف مكون Sandbox ويمنع تلقائيًا التهديدات المتقدمة على أجهزة الكمبيوتر. ويحلل Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Sandbox). وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Sandbox وتعليمات Kaspersky Anti Targeted Attack Platform. **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.

أوضاع التطبيق: Standard، EDR Agent، Light Agent

يمثل Kaspersky Endpoint Security for Windows جزءًا من العديد من حلول Kaspersky. واعتمادًا على الحل، تحتاج إلى تحديد وضع للتطبيق.



الوضع القياسي

هذا هو الوضع الرئيسي والافتراضي للتطبيق. ويمكنك تثبيت التطبيق في هذا الوضع كجزء من حلول Kaspersky EPP (Endpoint Protection Platform. على سبيل المثال، يعد Kaspersky Endpoint Security في الوضع القياسي جزءًا من Kaspersky Endpoint Security for Business. ويوفر Kaspersky Endpoint Security حماية شاملة لمحطات العمل والخوادم من التهديدات وهجمات الشبكة وعمليات الاحتيال المختلفة. وفي الوضع القياسي، يتوفر أيضًا العملاء المدمجون للتكامل مع حلول Kaspersky Detection and Response، بما في ذلك EDR وMDR وKUMA وغيرها.



EDR Agent

يتيح هذا الوضع نشر حلول Kaspersky Detection and Response إلى جانب حلول منصة حماية نقطة النهاية (EPP) من جهات خارجية. وتتضمن حلول الاكتشاف والاستجابة Kaspersky Managed Detection and Response (MDR) وKaspersky Anti Targeted Attack Platform (KATA). ويدعم Kaspersky EDR Agent حل SIEM نظام Kaspersky Unified Monitoring and Analysis Platform (KUMA).

في هذا الوضع، لا تتوفر مكونات الحماية القياسية مثل الحماية من تهديدات الملفات أو الحماية من تهديدات الويب. ويتم توفير الحماية القياسية للكمبيوتر بواسطة حل EPP من جهة خارجية. ويراقب EDR Agent باستمرار العمليات التي تعمل على أجهزة الكمبيوتر هذه، ويفتح اتصالات الشبكة والملفات التي يتم تعديلها ويتفاعل مع حلول الاكتشاف والاستجابة.



Light Agent

يُستخدم هذا الوضع لحماية البيئات الافتراضية. ويعد Kaspersky Endpoint Security في وضع Light Agent جزءًا من حل Kaspersky Hybrid Cloud Security. ويحمي Light Agent الأجهزة الافتراضية بأنظمة تشغيل الضيف لمحطات العمل والخوادم. وتتوفر مكونات الحماية والتحكم نفسها في هذا الوضع كما في الوضع القياسي. ويتمثل الفرق في أنه يتم فحص الكائنات للبحث عن الفيروسات والبرامج الضارة الأخرى بواسطة مكون حل خاص مثبت على جهاز افتراضي منفصل، SVM (Secure Virtual Machine). وبالتالي يستخدم Light Agent موارد SVM لضمان أمان البنية التحتية بدلاً من موارد الجهاز الافتراضي.

حزمة التوزيع

تتضمن مجموعة التوزيع حزم التوزيع التالية:

- **AES256**

حزمة التوزيع هذه مخصصة للتثبيت على أجهزة الكمبيوتر ذات بنية x86/x64. تحتوي حزمة التوزيع هذه على أدوات التشفير التي تنفذ خوارزمية التشفير AES (Advanced Encryption Standard) باستخدام طول مفتاح فعال 256 بت.

- **AES56**

  حزمة التوزيع هذه مخصصة للتثبيت على أجهزة الكمبيوتر ذات بنية x86/x64. تحتوي حزمة التوزيع هذه على أدوات التشفير التي تقوم بتنفيذ خوارزمية التشفير AES باستخدام طول مفتاح فعال 56 بت.

- **Arm64**

  حزمة التوزيع هذه مخصصة للتثبيت على أجهزة الكمبيوتر القائمة على Arm. حزمة التوزيع هذه غير مخصصة للتثبيت على الخوادم.

قبل التثبيت، تأكد من تطابق حزمة التوزيع مع بنية المعالج الخاص بك. وإذا لم تتطابق حزمة التوزيع مع بنية المعالج، فسيقوم المثبت بإنهاء التثبيت مع ظهور خطأ.

حزمة التوزيع هي أرشيف ذاتي الاستخراج بتنسيق EXE. ولعرض محتويات حزمة التوزيع، تحتاج إلى استخراج الأرشيف إلى مجلد منفصل. 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 التثبيت للمكوّن الإضافي لإدارة التطبيق في وحدة تحكم إدارة Kaspersky Security Center.
`bases.cab`	تحديث ملفات الحزمة التي تستخدم في أثناء عملية التثبيت.
`cleaner_v2.cab` `cleanerapi_v2.cab`	ملفات لإزالة البرامج غير المتوافقة.
`incompatible.txt`	ملف يحتوي على قائمة البرامج التي قد تسبب مشكلات في التوافق مع Kaspersky Endpoint Security. لا يضمن Kaspersky توافق Kaspersky Endpoint Security مع البرامج من القائمة.
`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.
`kes.cab`	ملفات للواجهة الرسومية للتطبيق.
`aes256.cab` / `aes56.cab`	ملفات خوارزمية تشفير AES (غير مضمنة في حزمة توزيع Arm64).
`package.kcat`	ملف مع توقيعات حزمة توزيع التطبيق. يضمن التوقيع الرقمي أصالة مجموعة توزيع التطبيق وسلامتها.

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

متطلبات الأجهزة والبرامج

تسرد هذه المقالة إصدارات البرامج التي تم اختبار التطبيق عليها والتي يتم ضمان عمله بالنسبة لها بشكل صحيح. وقد يعمل التطبيق أيضًا مع إصدارات برامج أخرى، لكن هذه التكوينات لم تخضع لدورة اختبار كاملة ولم يتم تضمينها في قائمة الإصدارات المدعومة المضمونة.

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

لتثبيت التطبيق، تحتاج إلى حقوق المسؤول على الكمبيوتر.

الحد الأدنى للمتطلبات	محطة العمل (x86/x64)	الخادم (x86/x64)	Arm
التخزين	2 جيجابايت	2 جيجابايت	2 جيجابايت
وحدة المعالجة المركزية	1 جيجاهرتز، دعم تعليمات SSE2	1.4 جيجاهرتز، دعم تعليمات SSE2	1 جيجاهرتز، بنية Armv8.1
ذاكرة الوصول العشوائي (RAM)	محطة العمل (x86): 1 جيجابايت محطة العمل (x64): 2 جيجابايت	2 جيجابايت ملاحظة: يتطلب الخادم ذاكرة 8 جيجابايت لتثبيت التطبيق باستخدام العميل المدمج للتكامل مع Kaspersky Anti Targeted Attack Platform.	4 جيجا بايت
Microsoft .NET Framework	4 أو أحدث	4 أو أحدث	4.8 أو أحدث

محطات العمل

أنظمة التشغيل المدعومة لمحطات العمل:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- 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 / Enterprise متعدد الجلسات؛
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

تدعم أنظمة تشغيل Windows، بدءًا من الإصدار 11 و24H2، تقنية UDP Receive Segment Coalescing Offload (URO). ويتم تمكين التقنية بشكل افتراضي في حالة تثبيت بطاقة شبكة وبرامج تشغيل متوافقة على الكمبيوتر. ويمكن أن يؤدي تعطيل استلام تفريغ اندماج القسم (URO) على كمبيوتر المستخدم إلى تقليل أداء التطبيق بشكل كبير.

للتأكد من عمل Kaspersky Endpoint Security بشكل صحيح، يجب تشغيل خدمة Windows Security Center (wscsvc) على كمبيوتر المستخدم.

لا يمكن تثبيت Kaspersky Endpoint Security على نظام التشغيل Microsoft Windows 7 بدون تثبيت تحديثات نظام التشغيل: KB4490628 (12 مارس 2019) وKB4474419 (23 سبتمبر 2019). وللحصول على معلومات مفصلة، ارجع إلى قاعدة معارف الدعم الفني.

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 (Cluster Mode). ويدعم التطبيق أيضا Server Core Mode (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
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)
- Windows Server 2016 Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)
- Windows Server 2019 Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (بما في ذلك وضع Server Core)
- Windows Server 2025 Standard / Datacenter

لا يمكن تثبيت Kaspersky Endpoint Security على نظام التشغيل Microsoft Windows Server 2008 R2 بدون تثبيت تحديثات نظام التشغيل: KB4490628 (12 مارس 2019) وKB4474419 (23 سبتمبر 2019).

للحصول على تفاصيل حول الدعم لأنظمة تشغيل Windows Server 2016 وMicrosoft 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 Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2

- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

الأنظمة الأساسية الافتراضية

الأنظمة الأساسية الافتراضية المدعومة لتشغيل التطبيق في الوضع القياسي:

- VMware Workstation Pro 15.5.2
- VMware ESXi 7.0 Patch Release ESXi 7.0b
- Windows Hyper-V Server 2019
- Citrix Virtual Apps and Desktops 7 2009
- Citrix Provisioning 2009
- Citrix Hypervisor 8.2 LTSR

يدعم التطبيق الأجهزة الافتراضية التي تعمل بنظام التشغيل Windows 11 Pro Arm64 التي تم إنشاؤها باستخدام Hyper-V.

الأجهزة الافتراضية لتثبيت Light Agent

لا يتم دعم تثبيت Kaspersky Endpoint Security في وضع Light Agent على الأجهزة الافتراضية القائمة على Arm.

يجب أن يدعم BIOS على الأجهزة الافتراضية الإصدار 2.1 أو أحدث من مواصفات SMBIOS.

يجب تثبيت الحزم والأدوات المساعدة التالية على الأجهزة الافتراضية:

- عند استخدام Microsoft Hyper-V - حزمة خدمات التكامل.
- عند استخدام حزمة VMware vSphere - VMware Tools.
- عند استخدام حزمة XenServer - XenTools.
- عند استخدام HUAWEI FusionSphere - حزمة أدوات HUAWEI.
- عند استخدام برامج الإدارة الافتراضية المستندة إلى KVM – عميل ضيف QEMU.

انظر تعليمات Kaspersky Security for Virtualization Light Agent للحصول على متطلبات البنية التحتية الافتراضية لتشغيل التطبيق في وضع Light Agent.

لكي يعمل التطبيق بشكل صحيح، استخدم واجهة شبكة افتراضية بعرض نطاق ترددي لا يقل عن 100 ميجابت/ثانية.

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
- Microsoft Remote Desktop Services المعتمد على Windows Server 2025
- Citrix RDSH from Citrix Virtual Apps and Desktops 7 2507 LTSR

دعم Kaspersky Security Center

يدعم Kaspersky Endpoint Security الإصدارات التالية من Kaspersky Security Center:

- Kaspersky Security Center 14.2
- Kaspersky Security Center Linux 14.2
- Kaspersky Security Center Linux 15
- Kaspersky Security Center Windows 15.1
- Kaspersky Security Center Linux 15.1
- Kaspersky Security Center Linux 15.2
- Kaspersky Security Center Linux 15.3
- Kaspersky Security Center Linux 15.4
- Kaspersky Security Center Linux 16
- Kaspersky Security Center Linux 16.1
- Kaspersky Security Center Linux 16.2
- Kaspersky Security Center Linux 16.3
- Kaspersky Security Center Linux 17

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).

بدءًا من Kaspersky Endpoint Security 12.8 for Windows، يمكنك تكوين مجموعات مختلفة من المكونات لأنواع أنظمة تشغيل مختلفة في حزمة التثبيت. ويعني هذا أنه يمكنك نشر التطبيق على محطات العمل والخوادم باستخدام حزمة التثبيت نفسها.

لا يتم دعم تثبيت Kaspersky Endpoint Security في وضع Light Agent على الأجهزة الافتراضية القائمة على Arm.

مقارنة بين مزايا برنامج Kaspersky Endpoint Security

المزايا	محطة عمل	محطة عمل قائمة على Arm	خادم	وضع Server Core
الحماية من التهديدات المتقدمة				
Kaspersky Security Network	✓	✓	✓	✓
اكتشاف السلوك	✓	✓	✓	✓
مكافحة أداة التشفير	✓	✓	✓	✓
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 النظام	–	–	✓	–
Cloud Discovery	✓	✓	–	–
تشفير البيانات				
تشفير القرص من Kaspersky	✓	–	–	–
تشفير محرك الأقراص من BitLocker	✓	✓	✓	✓
التشفير على مستوى الملف	✓	–	–	–
تشفير محركات الأقراص القابلة للإزالة	✓	–	–	–
Detection and Response				

المزايا	محطة عمل	محطة عمل قائمة على Arm	خادم	وضع Server Core
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	✓	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
تكامل KUMA	✓	✓	✓	✓

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.
- Web Console. تم تثبيت مكون Kaspersky Security Center في خادم الإدارة. يمكنك العمل في Web Console باستخدام مستعرض على أي كمبيوتر.

يمكنك 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.

Kaspersky Endpoint Security جزء من حل Kaspersky Next Pro View. وللمزيد من المعلومات عن ميزات التطبيق المتاحة عندما يعمل كجزء من هذا الحل، راجع تعليمات Kaspersky Next.

مقارنة بين مزايا برنامج Kaspersky Endpoint Security

المزايا	Kaspersky Security Center		Kaspersky Security Center
	وحدة تحكم الإدارة	Web Console	وحدة تحكم السحابة
الحماية من التهديدات المتقدمة			
Kaspersky Security Network	✓	✓	✓
Kaspersky Private Security Network	✓	✓	–
اكتشاف السلوك	✓	✓	✓
مكافحة أداة التشفير			
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	✓	✓	✓

المزايا	Kaspersky Security Center		Kaspersky Security Center
	وحدة تحكم الإدارة	Web Console	وحدة تحكم السحابة
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 النظام	✓	✓	✓
Cloud Discovery	–	–	✓
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 (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
تكامل KUMA	✓	✓	✓
المهام			
إضافة مفتاح	✓	✓	✓
تغيير مكونات التطبيق	✓	✓	✓
المخزون	✓	✓	✓
تحديث	✓	✓	✓
تراجع عن التحديث	✓	✓	✓
فحص البرامج الضارة	✓	✓	✓
التحقق من سلامة التطبيق	✓	✓	–
مسح البيانات	✓	✓	✓
إدارة حسابات وكيل المصادقة (تشفير القرص من Kaspersky)	✓	✓	–
فحص IOC (EDR)	–	✓	✓
نقل الملف إلى العزل (EDR)	–	✓	✓
الحصول على الملف (EDR)	–	✓	✓
حذف الملف (EDR)	–	✓	✓
بدء العملية (EDR)	–	✓	✓
إنهاء العملية (EDR)	–	✓	✓

التوافق مع التطبيقات الأخرى

لا يتوافق Kaspersky Endpoint Security مع بعض تطبيقات Kaspersky بالإضافة إلى بعض تطبيقات الجهات الخارجية. لذلك، قبل التثبيت، وتحديث إصدار التطبيق وتغيير مكونات التطبيق، يفحص Kaspersky Endpoint Security الكمبيوتر لمعرفة ما إذا كان هناك أي من هذه التطبيقات.

التوافق مع تطبيقات الجهات الخارجية

لا يتوافق Kaspersky Endpoint Security مع التطبيقات التي تعد جزءًا من أنظمة حماية نقطة النهاية التابعة لجهات خارجية (Endpoint Protection Platform، EPP). ويمكن أن يواجه Kaspersky Endpoint Security أيضًا مشكلات توافق مع تطبيقات أخرى. ولتحديد التوافق، يتحقق Kaspersky Endpoint Security من قائمة تضم البرامج التي أعدتها Kaspersky. وتوجد هذه القائمة في ملف incompatible.txt. ويتم تضمين الملف في حزمة التوزيع.

لا يضمن Kaspersky توافق Kaspersky Endpoint Security مع البرامج من القائمة. إذا تم اكتشاف تطبيق من القائمة، فسيقوم المُثبت بإيقاف نشر Kaspersky Endpoint Security. قد يحذف برنامج التثبيت تلقائيًا بعض التطبيقات من القائمة. وإذا كنت على استعداد لتجاهل المخاطر وتريد تثبيت Kaspersky Endpoint Security وجزء من البرنامج من القائمة على جهاز الكمبيوتر نفسه، فيمكنك تخطي فحص الكمبيوتر (انظر التعليمات أدناه).

تنزيل ملف INCOMPATIBLE.TXT

التوافق مع تطبيقات Kaspersky

لا يتوافق برنامج Kaspersky Endpoint Security مع تطبيقات Kaspersky التالية:

- Kaspersky Standard | Plus | Premium.
- 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.
- Endpoint Sensor كجزء من حلي Kaspersky Anti Targeted Attack Platform وKaspersky Endpoint Detection and Response solutions.

- Kaspersky Endpoint Agent كجزء من حلول Detection and Response من Kaspersky.

تحوّل Kaspersky كل مهام Detection and Response للعمل مع عامل Kaspersky Endpoint Security المضمن بدلاً من Kaspersky Endpoint Agent. وبدءًا من الإصدار 12.1، يدعم التطبيق جميع حلول Detection and Response.

- تطبيق Kaspersky Security for Virtualization Light Agent.
- تطبيق Kaspersky Fraud Prevention for Endpoint.
- Kaspersky Security for Windows Server

بدءًا من Kaspersky Endpoint Security 12.0، يمكنك الترحيل من Kaspersky Security for Windows Server إلى Kaspersky Endpoint Security for Windows واستخدام الحل نفسه لحماية محطات العمل والخوادم.

- 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 التحقق من البرامج التي قد تسبب مشكلات في التوافق

إذا اكتشف Kaspersky Endpoint Security وجود برنامج من قائمة incompatible.txt، فسيتم إنهاء تثبيت التطبيق. ولمتابعة التثبيت، يجب عليك إزالة هذا التطبيق. ومع ذلك، إذا أشار مورد برنامج خارجي في وثائقه إلى أن برامجه متوافقة مع Endpoint Protection Platform (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 المُثبتة. ولفعل ذلك، قم بتمرير المعلمات التالية إلى المُثبت:

- `SKIPPRODUCTCHECK=1` قم بتعطيل التحقق من البرامج المُثبتة. تتوفر قائمة البرامج التي قد تسبب مشكلات في التوافق في ملف incompatible.txt المضمن في حزمة التوزيع. إذا لم يتم تعيين قيمة لهذه المعلمة وتم اكتشاف برنامج من القائمة، فسيتم إنهاء تثبيت Kaspersky Endpoint Security.
- `SKIPPRODUCTUNINSTALL=1` قم بتعطيل الإزالة التلقائية للبرامج المكتشفة من قائمة incompatible.txt. إذا لم يتم تعيين قيمة لهذه المعلمة، فسيحاول Kaspersky Endpoint Security إزالة البرنامج الذي قد يسبب مشكلات في التوافق.
- `CLEANERSIGNCHECK=0` قم بتعطيل التحقق من التوقيع الرقمي للتطبيقات التي يتم العثور عليها بواسطة الفحص. 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.

إذا تخطيت أثناء عملية التثبيت الفحص الخاص بالبحث عن البرامج التي قد تسبب مشكلات في التوافق، فيمكن لتطبيق Kaspersky Endpoint Security إجراء هذا الفحص مرة أخرى عندما تتغير مكونات التطبيق. ولتخطي الفحص الخاص بالبحث عن البرامج المثبتة، تحتاج إلى تكوين مهمة تغيير مكونات التطبيق.

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.
4. الإعدادات الواردة من ملف التكوين (install.cfg).

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

عند تثبيت Kaspersky Endpoint Security، قد يعرض نظام التشغيل الرسائل الخاصة به. وقد يتم أيضًا قطع اتصالات الشبكة والإنترنت أثناء تثبيت التطبيق.

قد تحدث أخطاء عند تثبيت Kaspersky Endpoint Security أو تحديثه أو إلغاء تثبيته. وللحصول على المزيد من المعلومات عن حل هذه الأخطاء، يُرجى الرجوع إلى قاعدة معارف الدعم الفني.

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. قبل تثبيت التطبيق، يجب التأكد من تثبيت Kaspersky Security Center Network Agent على الكمبيوتر. يسهل عميل الشبكة التفاعل بين خادم الإدارة وجهاز العميل.

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.

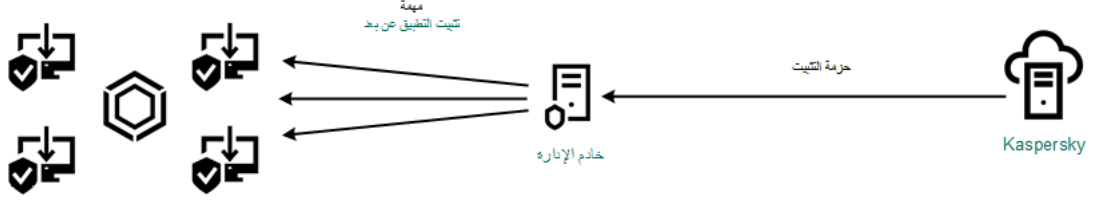
التثبيت القياسي للتطبيق

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 Install application remotely الخاصة بخادم الإدارة Kaspersky Security Center.



نشر Kaspersky Endpoint Security

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

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم ، حدد **Remote installation** ← **Advanced**.

3. انقر فوق الرابط **Deploy installation package on managed devices (workstations)**.

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. على 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 2. تحديد مصدر حزمة التثبيت

حدد المصدر **Deploy Kaspersky Security Center package**.

الخطوة 3: 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 4. تحديد إعدادات مهمة التثبيت عن بُعد

قم بتكوين إعدادات التطبيق الإضافية التالية:

- **Force installation package download**. حدد طريقة تثبيت التطبيق:

- **Using Network Agent**. عميل الشبكة مسؤول عن تسليم حزمة تثبيت Kaspersky Endpoint Security إلى أجهزة الكمبيوتر العميلة. وإذا لم يتم تثبيت Network Agent، فسيتم إنهاء المهمة مع ظهور خطأ. وفي هذه الحالة، أضف حزمة تثبيت عميل الشبكة إلى مهمة Install application remotely وتمكين تسليم الملف عبر موارد نظام التشغيل. وبعد ذلك، سيتم تثبيت عميل الشبكة باستخدام موارد نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.

- **Using operating system resources through distribution points**. 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.

- **Using operating system resources through Administration Server**. 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.

- **Do not re-install application if it is already installed**. 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 5. 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 Add key.

الخطوة 6: 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 7: 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.

الخطوة 8: 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 9. بدء التثبيت

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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. علي 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 Add key.

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 4: 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**. حدد طريقة تثبيت التطبيق:
  - **Using Network Agent**. عميل الشبكة مسؤول عن تسليم حزمة تثبيت Kaspersky Endpoint Security إلى أجهزة الكمبيوتر العميلة. وإذا لم يتم تثبيت Network Agent، فسيتم إنهاء المهمة مع ظهور خطأ. وفي هذه الحالة، أضف حزمة تثبيت عميل الشبكة إلى مهمة Install application remotely وتمكين تسليم الملف عبر موارد نظام التشغيل. وبعد ذلك، سيتم تثبيت عميل الشبكة باستخدام موارد نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.
  - **Using operating system resources through distribution points**. 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.
  - **Using operating system resources through Administration Server**. 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.
- **Do not re-install application if it is already installed**. 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 6: 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 7: 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.

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 **Unassigned devices**.

الخطوة 9: 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

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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 مجلد **Administration Server ← Advanced ← Remote installation ← Installation packages**.

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

2. انقر فوق **Create installation package**.

   يبدأ معالج الحزمة الجديدة. اتبع تعليمات المعالج.

الخطوة 1. تحديد نوع حزمة التثبيت

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

الخطوة الثانية: تحديد اسم نوع حزمة التثبيت

أدخل اسم حزمة التثبيت، مثل Kaspersky Endpoint Security for Windows 14.2.

الخطوة الثالثة: حدد حزمة التوزيع للتثبيت

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

إذا لزم الأمر، قم بتحديث قواعد بيانات مكافحة الفيروسات في حزمة التثبيت باستخدام خانة الاختيار **Copy updates from repository to installation package**.

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 تحديد مكونات التطبيق لأنواع مختلفة من أنظمة التشغيل. أي أن حزمة التثبيت تتضمن مجموعتين من المكونات: لمحطات العمل والخوادم. وقبل نشر حزمة التثبيت، يكتشف المثبت نوع نظام التشغيل ويثبت فقط مكونات التطبيق التي حددتها لنوع نظام التشغيل هذا. وبهذه الطريقة، يمكنك استخدام حزمة التثبيت نفسها لمحطات العمل والخوادم.

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.

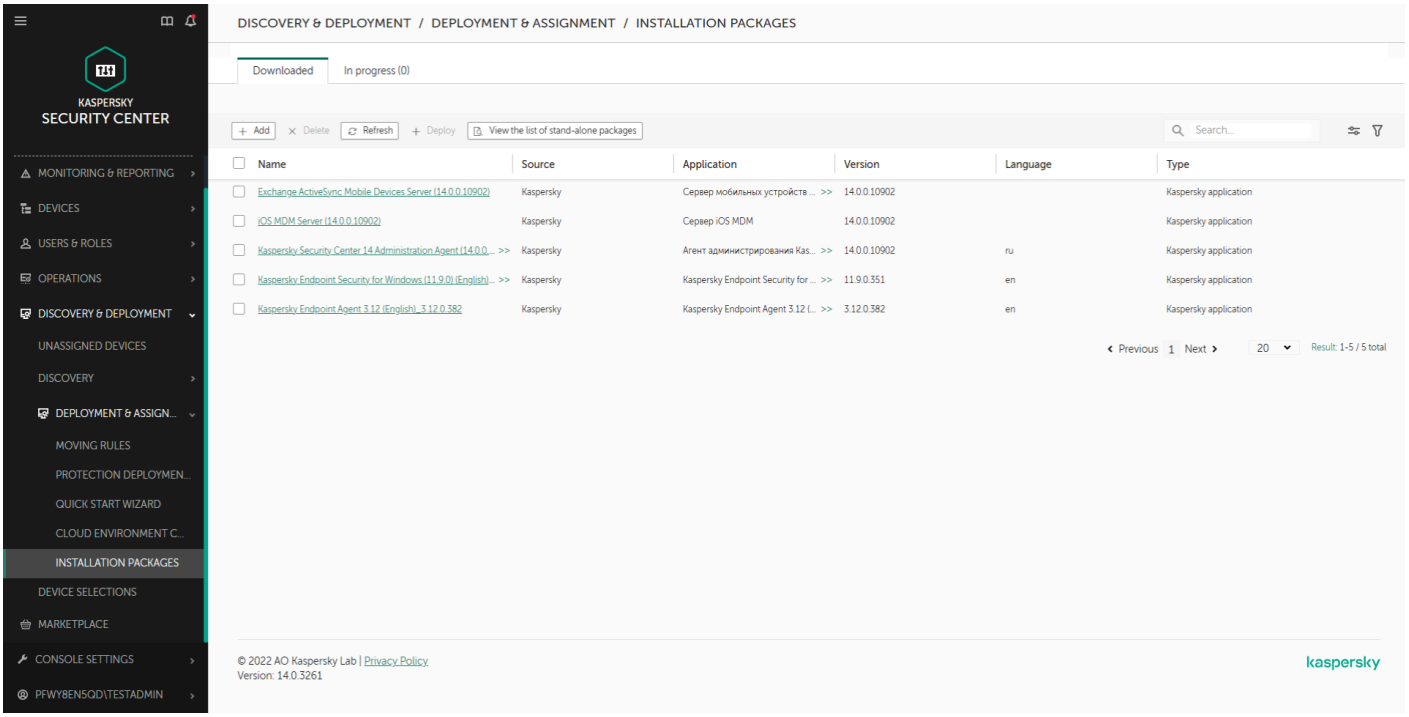
كيفية إنشاء حزمة تثبيت في Web Console

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

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

2. انقر على **Add**.

يبدأ معالج الحزمة الجديدة. اتبع تعليمات المعالج.



قائمة حزم التثبيت

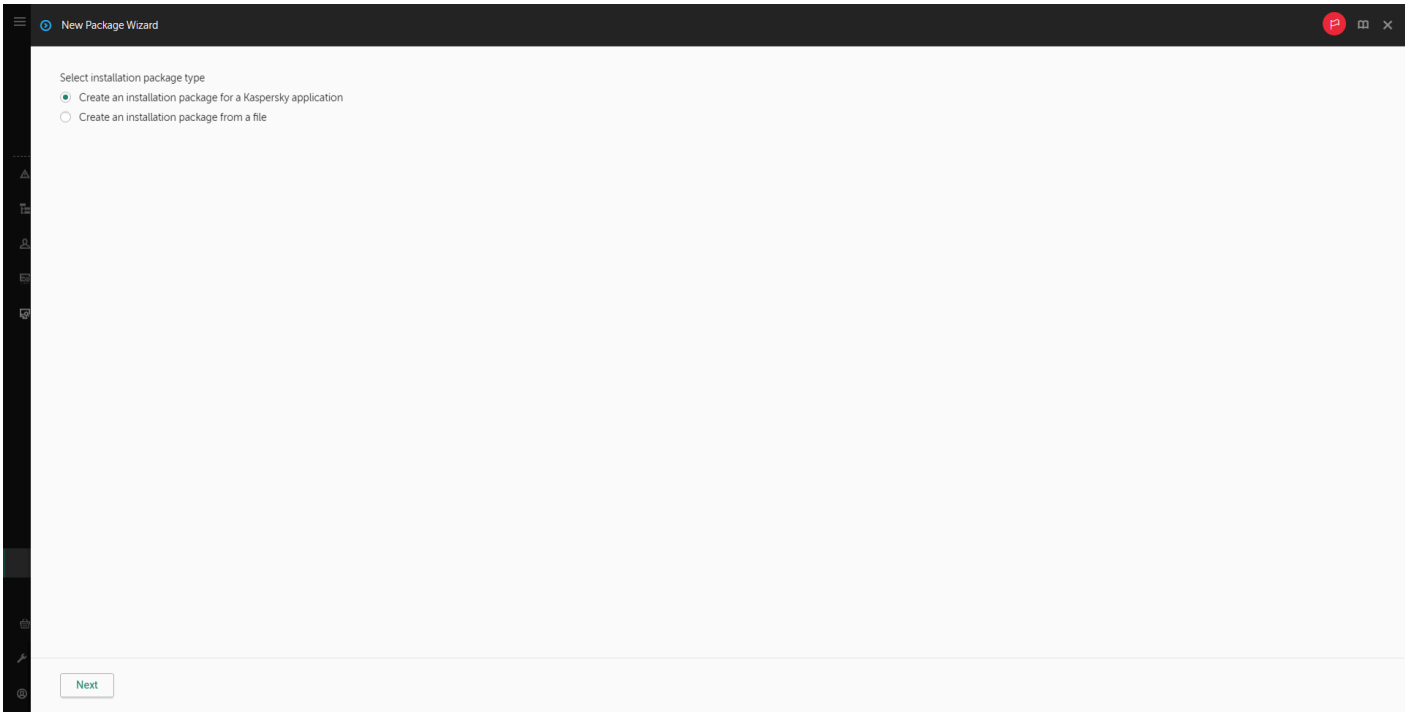
الخطوة 1. تحديد نوع حزمة التثبيت

حدد 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.

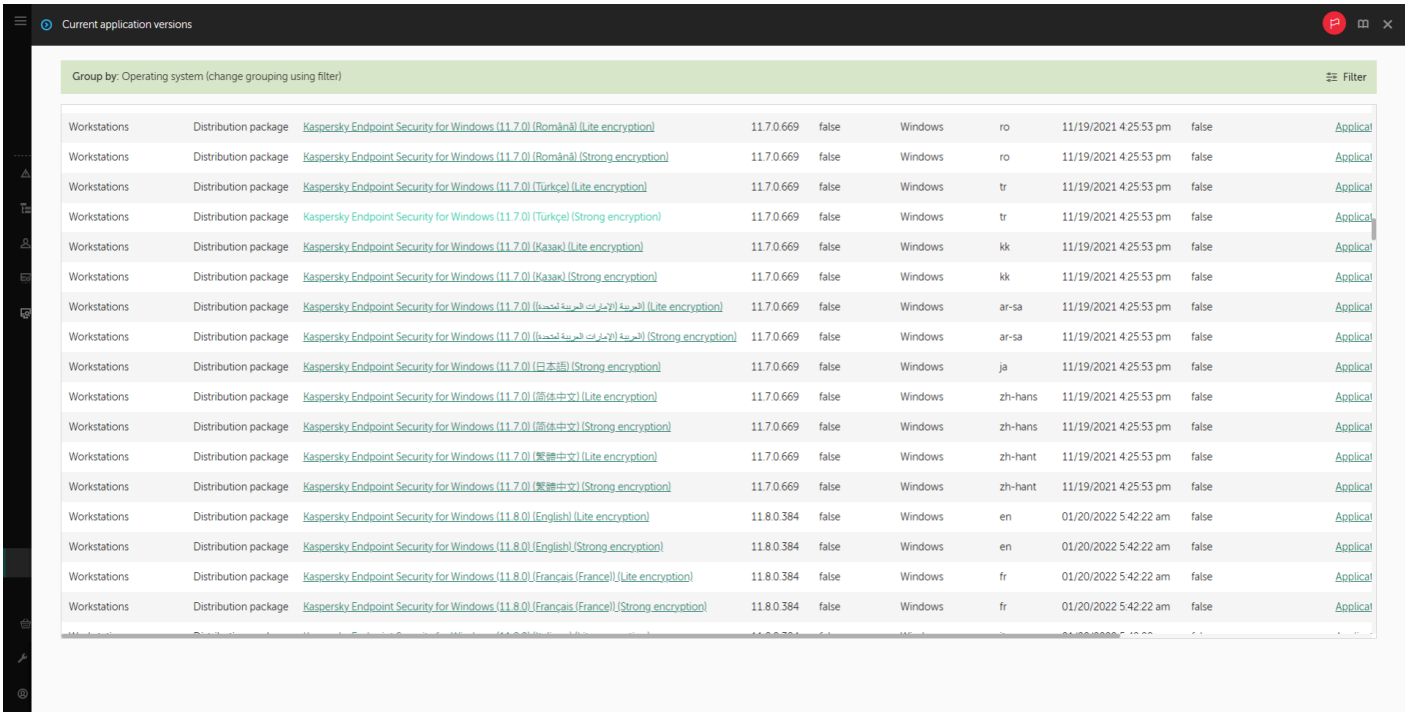
لا يتوفر إنشاء حزمة تثبيت لتطبيق Kaspersky Endpoint Security من ملف إلا في Kaspersky Security Center Web Console.



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.

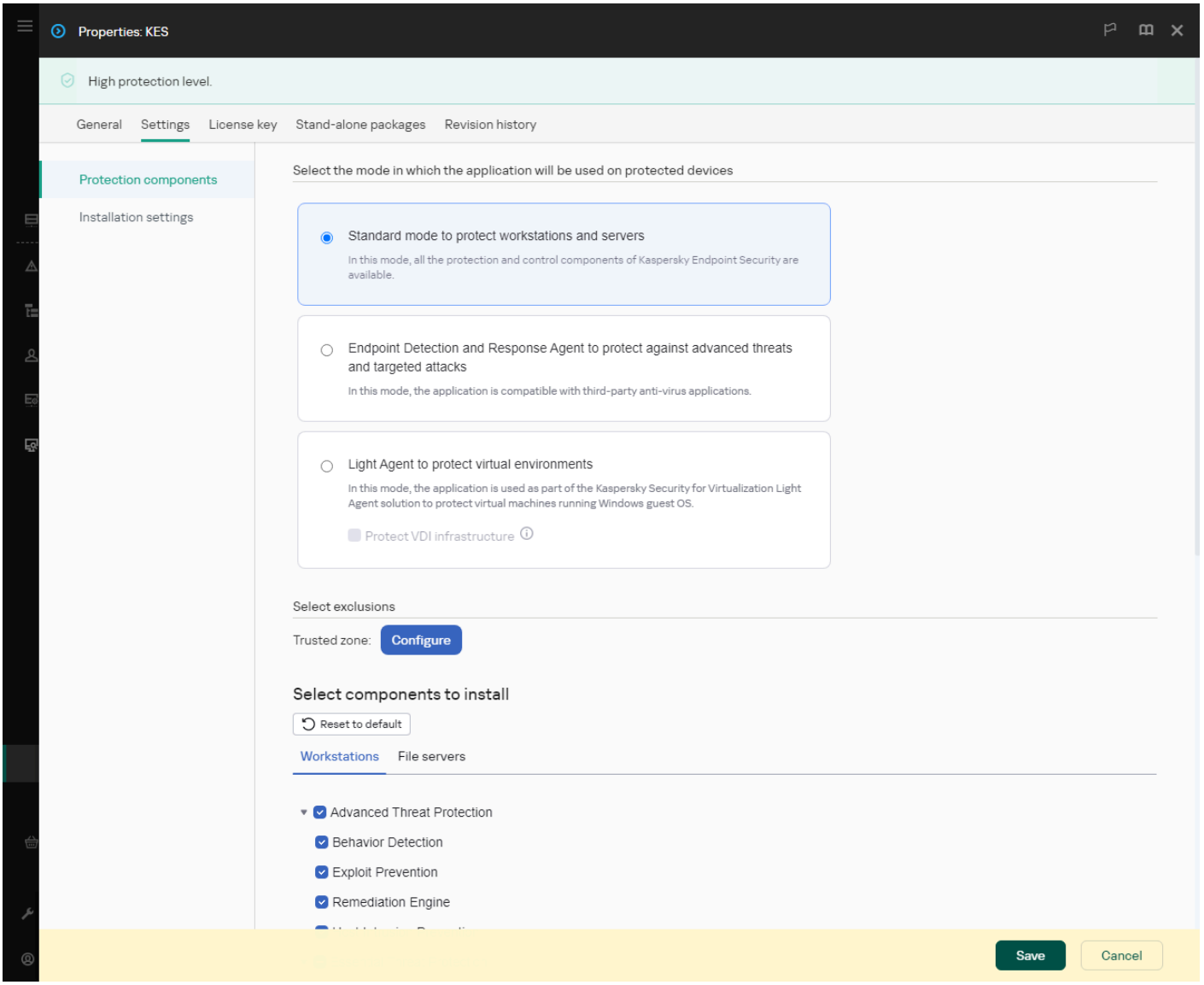


قائمة حزم التثبيت على خوادم Kaspersky

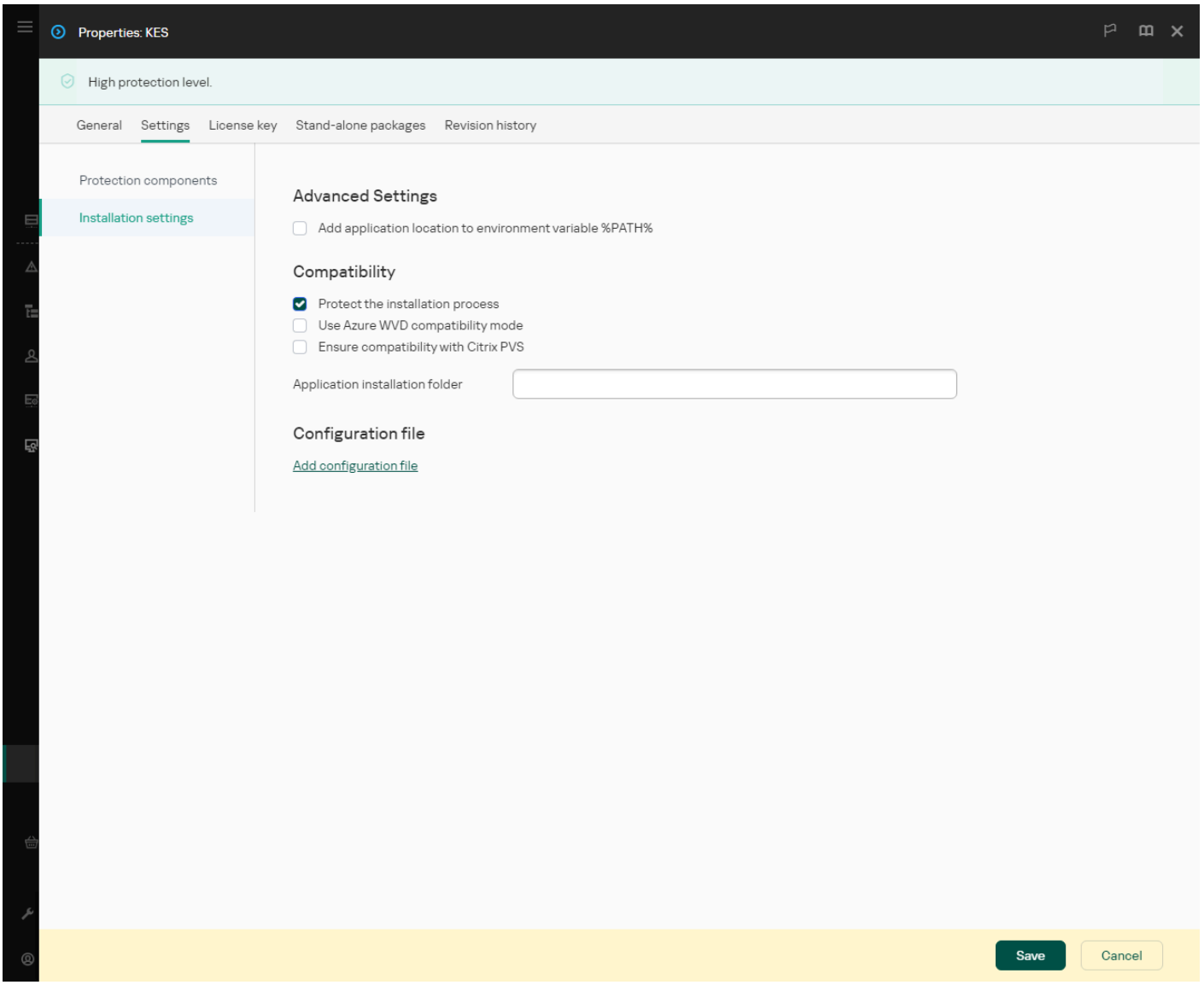
سيتم إنشاء حزمة التثبيت وإضافتها إلى Kaspersky Security Center. باستخدام حزمة التثبيت، يمكنك تثبيت برنامج Kaspersky Endpoint Security على أجهزة الكمبيوتر الخاصة بشبكة الشركة أو تحديث إصدار التطبيق.

في إعدادات حزمة التثبيت، يمكنك تحديد مكونات التطبيق لأنواع مختلفة من أنظمة التشغيل. أي أن حزمة التثبيت تتضمن مجموعتين من المكونات: لمحطات العمل والخوادم. وقبل نشر حزمة التثبيت، يكتشف المثبت نوع نظام التشغيل ويثبت فقط مكونات التطبيق التي حددتها لنوع نظام التشغيل هذا. وبهذه الطريقة، يمكنك استخدام حزمة التثبيت نفسها لمحطات العمل والخوادم.

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
مكونات الحماية	**الوضع القياسي**. التكوين الافتراضي. يتيح لك هذا التكوين استخدام كل مكونات التطبيق، بما في ذلك المكونات التي توفر الدعم لحلول Detection and Response. ويُستخدم هذا التكوين لتوفير الحماية الشاملة للكمبيوتر من مجموعة متنوعة من التهديدات وهجمات الشبكة والاحتيال. **Endpoint Detection and Response Agent**. في هذا التكوين ، يمكنك فقط تثبيت المكونات التي توفر الدعم لحلول الاكتشاف والاستجابة: MDR و EDR (KATA) و NDR (KATA) و EDR Expert (on-premises)، وكذلك KUMA. ويعد هذا التكوين ضروريًا إذا تم نشر Endpoint Protection Platform (EPP) تابع لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية. **Light Agent لحماية البيئات الافتراضية**. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. وفي هذا التكوين، لا يمكنك استخدام مكونات تشفير البيانات أو مراقبة عيوب التكيف. وإذا كنت تقوم بتثبيت Light Agent على قالب جهاز افتراضي سيتم استخدامه لإنشاء أجهزة افتراضية غير ثابتة، حدد خانة الاختيار **حماية البنية التحتية لسطح المكتب الافتراضي** (VDI يعني Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية.
الاستثناءات	بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم. بدءًا من الإصدار Kaspersky Endpoint Security 12.8 for Windows، يمكنك تثبيت التطبيق في وضع Light Agent لحماية البيئات الافتراضية. ويمكن أن تساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في البيئات الافتراضية في Citrix و VMware يمكنك أيضًا تكوين المنطقة الموثوقة لاحقًا في خصائص السياسة: استثناءات الفحص و التطبيقات الموثوقة.

القسم	الوصف
حدد المكونات المراد تثبيتها	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. يمكنك إنشاء مجموعات منفصلة من المكونات لمحطات العمل والخوادم. وقبل نشر حزمة التثبيت، يكتشف المثبت نوع نظام التشغيل ويثبت فقط مكونات التطبيق التي حددتها لنوع نظام التشغيل هذا. وبهذه الطريقة، يمكنك استخدام حزمة التثبيت نفسها لمحطات العمل والخوادم. تعتمد مجموعة المكونات المتوفرة على تكوين التطبيق: **الوضع القياسي** لا يتم تثبيت Kaspersky Data Encryption وFile Level Encryption وكل العوامل المضمنة باستثناء EDR Optimum بشكل افتراضي. ويمكن إضافة هذه المكونات في إعدادات حزمة التثبيت. **Endpoint Detection and Response Agent** في هذا التكوين، لا تتوفر سوى العوامل المدمجة لحلول Kaspersky Detection and Response. **Light Agent لحماية البيئات الافتراضية** في هذا التكوين، يمكنك استخدام جميع مكونات التطبيق المتوفرة في تكوين **الوضع القياسي**، باستثناء مكونات تشفير البيانات ومراقبة عيوب التكيف.
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. **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**. يمكنك تمكين دعم Citrix Provisioning Services لتثبيت برنامج Kaspersky Endpoint Security إلى جهاز افتراضي. **استخدم وضع التوافق مع Azure WVD**. تضمن هذه الميزة العرض الصحيح لحالة الجهاز الافتراضي في Azure في وحدة تحكم 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 (Sensor ID). ويسمح وضع التوافق مع Azure WVD بتعيين Sensor ID 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. **Application installation folder**. يمكنك تغيير مسار تثبيت برنامج Kaspersky Endpoint Security على كمبيوتر العميل. وبشكل افتراضي، يتم تثبيت التطبيق في المجلد `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`. **Configuration file**. تثبيت التطبيق بإعدادات محددة مسبقًا. ولفعل هذا، تحتاج إلى تحميل ملف يحدد إعدادات برنامج Kaspersky Endpoint Security. يمكنك إنشاء ملف تكويني في الواجهة المحلية للتطبيق. لا يدعم معالج الحزمة الجديدة ملفات التكوين المشفرة. وعند تصدير ملف التكوين، تخط خطوة تشفير الملف.

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 Download updates to the Administration Server repository 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. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Remote installation** ← **Advanced** ← مجلد **Installation packages**.

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

3. افتح خصائص حزمة التثبيت.

4. في القسم **General**، انقر فوق الزر **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.

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 Install application remotely مصممة لتثبيت تطبيق Kaspersky Endpoint Security عن بُعد. تسمح لك مهمة Install application remotely 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. افتح Kaspersky Security Center Administration Console.

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

تفتح قائمة المهام.

3. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Install application remotely** ← **Kaspersky Security Center Administration Server**.

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:

- **Force installation package download**. حدد طريقة تثبيت التطبيق:
  - **Using Network Agent**. عميل الشبكة مسؤول عن تسليم حزمة تثبيت Kaspersky Endpoint Security إلى أجهزة الكمبيوتر العميلة. وإذا لم يتم تثبيت Network Agent، فسيتم إنهاء المهمة مع ظهور خطأ. وفي هذه الحالة، أضف حزمة تثبيت عميل الشبكة إلى مهمة Install application remotely وتمكين تسليم الملف عبر موارد نظام التشغيل. وبعد ذلك، سيتم تثبيت عميل الشبكة باستخدام موارد نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.
  - **Using operating system resources through distribution points**. 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.
  - **Using operating system resources through Administration Server**. 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.
- **Behavior for devices managed through other Administration Servers**. 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.
- **Do not re-install application if it is already installed**. 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 14.2.

الخطوة 10. الانتهاء من إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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 نافذة Web Console الرئيسية، حدد **Tasks** ← **Asset management**.

   تفتح قائمة المهام.

2. انقر على **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، مثل تثبيت Kaspersky Endpoint Security for Managers.

4. في القسم **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 (14.2).

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:

- **Using Network Agent**. عميل الشبكة مسؤول عن تسليم حزمة تثبيت Kaspersky Endpoint Security إلى أجهزة الكمبيوتر العميلة. وإذا لم يتم تثبيت Network Agent، فسيتم إنهاء المهمة مع ظهور خطأ. وفي هذه الحالة، أضف حزمة تثبيت عميل الشبكة إلى مهمة Install application remotely وتمكين تسليم الملف عبر موارد نظام التشغيل. وبعد ذلك، سيتم تثبيت عميل الشبكة باستخدام موارد نظام التشغيل. ثم يتم تثبيت Kaspersky Endpoint Security بواسطة أدوات عميل الشبكة.

- **Using operating system resources through distribution points**. 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.

- **Using operating system resources through Administration Server**. 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 حزمة التثبيت التي يتم 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. إذا 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. إذا 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 مهمة، حدد خانة الاختيار المقابلة للمهمة 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. تأكد أن حساب المستخدم الذي تقوم بتشغيل معالج الإعداد به ينتمي إلى مجموعة المسؤولين.

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:

- ما إذا كان هناك أي برنامج مثبت قد يواجه مشكلات توافق مع Kaspersky Endpoint Security (قائمة البرامج متوفرة في ملف incompatible.txt المرفق في حزمة التوزيع).
- ما إذا تم الوفاء بمتطلبات الأجهزة والبرامج أم لا.
- ما إذا كان Microsoft .NET Framework موجودًا أم لا.
- ما إذا 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 14.2 for Windows، وتتم إزالة الإصدار السابق من التطبيق تلقائيًا. وهذا ينطبق على إصدارات التطبيق التالية:

- Kaspersky Endpoint Security 12.3 for Windows (الإصدار 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (الإصدار 12.4.0.467)
- Kaspersky Endpoint Security 12.5 for Windows (الإصدار 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (الإصدار 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (الإصدار 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (الإصدار 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (الإصدار 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (الإصدار 12.10.0.466)

- Kaspersky Endpoint Security 12.11 for Windows (الإصدار 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (الإصدار 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (الإصدار 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (الإصدار 14.1.0.423)

تكوين Kaspersky Endpoint Security



اختيار تكوين التطبيق

الوضع القياسي. التكوين الافتراضي. يتيح لك هذا التكوين استخدام كل مكونات التطبيق، بما في ذلك المكونات التي توفر الدعم لحلول Detection and Response. ويُستخدم هذا التكوين لتوفير الحماية الشاملة للكمبيوتر من مجموعة متنوعة من التهديدات وهجمات الشبكة والاحتيال.

Endpoint Detection and Response Agent. في هذا التكوين ، يمكنك فقط تثبيت المكونات التي توفر الدعم لحلول الاكتشاف والاستجابة: MDR و EDR (KATA) و NDR (KATA) و EDR Expert (on-premises)، وكذلك KUMA. ويعد هذا التكوين ضروريًا إذا تم نشر Endpoint Protection Platform (EPP) تابع لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.

Light Agent لحماية البيئات الافتراضية. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. وفي هذا التكوين، لا يمكنك استخدام مكونات تشفير البيانات أو مراقبة عيوب التكيف. وإذا كنت تقوم بتثبيت Light Agent على قالب جهاز افتراضي سيتم استخدامه لإنشاء أجهزة افتراضية غير ثابتة، حدد خانة الاختيار **حماية البنية التحتية لسطح المكتب الافتراضي** (VDI يعني Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية.

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

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

- تشفير القرص من Kaspersky
- التشفير على مستوى الملف
- Endpoint Detection and Response Expert (on-premises)
- Endpoint Detection and Response Expert (cloud)
- Sandbox
- Managed Detection and Response
- Network Detection and Response (KATA)
- التكامل مع KUMA

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 (cloud) فقط
- Endpoint Detection and Response Expert (on-premises) فقط
- Network Detection and Response (KATA) فقط
- Sandbox فقط

- Endpoint Detection and Response Optimum وSandbox
- Endpoint Detection and Response Expert (cloud) وSandbox
- Endpoint Detection and Response Expert (on-premises) وSandbox
- Network Detection and Response (KATA) وEndpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) وManaged Detection and Response

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.

تحديد المجلد لتثبيت التطبيق

يمكنك تغيير مسار تثبيت برنامج Kaspersky Endpoint Security على كمبيوتر العميل. وبشكل افتراضي، يتم تثبيت التطبيق في المجلد `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.2`.

تكوين المنطقة الموثوقة

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم.

بدءًا من الإصدار Kaspersky Endpoint Security 12.8 for Windows، يمكنك تثبيت التطبيق في وضع Light Agent لحماية البيئات الافتراضية. ويمكن أن تساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في البيئات الافتراضية في Citrix وVMware.

يمكنك أيضًا تكوين المنطقة الموثوقة لاحقًا في خصائص السياسة: استثناءات الفحص والتطبيقات الموثوقة.

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. يمكنك تمكين دعم Citrix Provisioning Services لتثبيت برنامج Kaspersky Endpoint Security إلى جهاز افتراضي.

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.

استخدم ملف setup.ini فقط عند تثبيت التطبيق في الوضع الصامت.

لا يمكنك إضافة مسار إلى ملف install.cfg ملف التكوين في ملف setup.ini. ويتخطى التطبيق أيضًا ملف التكوين install.cfg في حالة وضعه في المجلد نفسه مثل مجموعة توزيع Kaspersky Endpoint Security. لتطبيق الإعدادات من ملف التكوين install.cfg، تحتاج إلى تحديد المسار إلى الملف في أمر تثبيت التطبيق التالي: `CONFIGPATH=<path to the configuration file>`.

تنزيل ملف SETUP.INI

يتكون ملف setup.ini من الأقسام التالية:

- `[Setup]` - إعدادات عامة لتثبيت التطبيق.
- `[Components]` – اختيار مكونات التطبيق المراد تثبيتها في الوضع القياسي. 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.
- `[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.

بدائل القيمة `1` هي القيم `yes` و`on` و`enable` و`enabled` و`true`. بدائل القيمة `0` هي القيم `no` و`off` و`disable` و`disabled` و`false`.

إعدادات ملف setup.ini

القسم	المعلمة	الوصف
`[Setup]`	`InstallDir`	المسار المؤدي لمجلد تثبيت التطبيق.
	`ActivationCode`	رمز تفعيل Kaspersky Endpoint Security.
	`Eula`	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`	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.
	`CLEANERSIGNCHECK`	التحقق من التوقيعات الرقمية لملفات البرامج المكتشفة من قائمة incompatible.txt. لإزالة البرنامج، يقوم Kaspersky Endpoint Security بتشغيل ملف مُثبت البرنامج. وإذا لم يكن ملف التثبيت يحتوي على توقيع رقمي، فإن Kaspersky Endpoint Security يعتبر الملف غير موثوق به ويوقف عملية إزالة البرنامج لتجنب تشغيل تعليمات برمجية ضارة محتملة. وإذا لم يتمكن التطبيق من التحقق من التوقيع الرقمي لملف البرنامج المكتشف، فسيتم إيقاف تثبيت Kaspersky Endpoint Security بسبب حدوث 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).
	`Login`	قم بتعيين اسم المستخدم للوصول إلى ميزات وإعدادات Kaspersky Endpoint Security (مكون حماية كلمة المرور). يتم تعيين اسم المستخدم بالإضافة إلى المعلمتين `Password` و `PasswordArea`. تم استخدام اسم المستخدم KLAdmin بشكل افتراضي.
	`Password`	حدد كلمة مرور للوصول إلى ميزات وإعدادات Kaspersky Endpoint Security (يتم تحديد كلمة المرور بالإضافة إلى المعلمتين `Login` و `PasswordArea`). إذا قمت بتحديد كلمة مرور ولم تحدد اسم مستخدم بمعلمة `Login`، فسيتم استخدام KLAdmin كاسم مستخدم افتراضيًا.

القسم	المعلمة	الوصف
	`PasswordArea`	حدد نطاق كلمة المرور للوصول إلى Kaspersky Endpoint Security. عندما يحاول مستخدم تنفيذ إجراء تم تضمينه في هذا النطاق، فسيطالب Kaspersky Endpoint Security ببيانات اعتماد حساب المستخدم (معلمتا `Login` و`Password`). 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. • `EXPORT` – تصدير إعدادات التطبيق. على سبيل المثال، `PasswordArea=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 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.
	`PROTECTOSSERVICES`	حماية وظائف خدمات نظام التشغيل. تمنع حماية خدمات نظام التشغيل تطبيقات الطرف الثالث من التدخل في تشغيل خدمات نظام التشغيل. وتشمل هذه الخدمات، على سبيل المثال، خدمة التشغيل التلقائي للتطبيق. • `1` يعني أنه تم تمكين حماية خدمات نظام التشغيل (القيمة الافتراضية). • `0` يعني أن حماية خدمات نظام التشغيل معطلة.
	`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). تضمن هذه الميزة العرض الصحيح لحالة الجهاز الافتراضي في Azure في وحدة تحكم 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 (Sensor ID). ويسمح وضع التوافق مع Azure WVD بتعيين Sensor ID فريد دائم لهذه الأجهزة الظاهرية. وفي حالة إيقاف تشغيل وضع التوافق، Sensor ID 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.
	`Reboot`	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.
	`AddEnvironment`	في متغير النظام %PATH%، أضف المسار إلى الملفات القابلة للتنفيذ الموجودة في مجلد إعداد Kaspersky Endpoint Security. القيم المتاحة: • `1` – يتم تزويد متغير النظام %PATH% بمسار الملفات القابلة للتنفيذ الموجودة في مجلد إعداد Kaspersky Endpoint Security. • `0` – لن يتم تزويد متغير النظام %PATH% بمسار الملفات القابلة للتنفيذ الموجودة في مجلد إعداد Kaspersky Endpoint Security.
	`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.

القسم	المعلمة	الوصف
	UPGRADEMODE	وضع ترقية التطبيق: • Seamless يعني ترقية التطبيق مع إعادة تشغيل الكمبيوتر (القيمة الافتراضية). • Force 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 المعلمة المحددة في ملف setup.ini أعلى من تلك الخاصة بالمعلمة المحددة في application settings أو في سطر الأوامر. على سبيل المثال، في حالة تحديد وضع الترقية Force في ملف setup.ini وتحديد وضع Seamless في إعدادات التطبيق، سيتم تثبيت الترقية دون إعادة تشغيل(Force). وإذا كنت تستخدم ملف setup.ini، حيث لم يتم تحديد المعلمة UPGRADEMODE، سيستخدم المُثبت قيمة افتراضية (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، فإنه يحفظ ملفات التتبع في المجلد %ProgramData%\Kaspersky Lab\KES.14.2\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.
	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.
	StandaloneMode	تثبيت التطبيق في وضع Endpoint Detection and Response Agent (EDR Agent). ويعد EDR Agent تطبيقًا يتم تثبيته على محطات العمل والخوادم الفردية في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة لدعم حلي Kaspersky Managed Detection and Response و Kaspersky Anti Targeted Attack Platform. يتوافق EDR Agent مع تطبيقات EPP التابعة لجهات خارجية. ويتيح لك ذلك استخدام أدوات أمان البنية التحتية التابعة لجهات خارجية إلى جانب Kaspersky Endpoint Detection and Response. لتثبيت عميل EDR، في القسم [Components]، حدد المكونين StandaloneKATA و StandaloneNDR أو StandaloneMDR. ولا يدعم EDR Agent مكونات التطبيق الأخرى. القيم المتاحة: • 1 لتثبيت التطبيق في وضع EDR Agent. • 0 لتثبيت التطبيق في الوضع القياسي (الافتراضي).
	KSVLAMode	تثبيت التطبيق في وضع Light Agent. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. القيم المتاحة: • 1 لتثبيت التطبيق في وضع Light Agent. • 0 لتثبيت التطبيق في الوضع القياسي (الافتراضي).

القسم	المعلمة	الوصف
	`InstallOnVDI`	تمكين وضع حماية VDI عند تثبيت التطبيق في وضع (`KSVLAMode=1`) Light Agent. يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي. وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية. القيم المتاحة: • `1` لتمكين وضع حماية VDI. • `0` لتعطيل وضع حماية VDI (الافتراضي).
	`KESExclusions`	إضافة استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة عند تثبيت التطبيق على الخادم. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. على سبيل المثال، تتضمن استثناءات الفحص المحددة مسبقًا لخوادم SQL ملفات قاعدة بيانات MDF وLDF. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم. القيم المتاحة: • `1` إضافة استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة. • `0` تعطيل استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة (الافتراضي).
	`LAExclusions`	إضافة استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة عند تثبيت التطبيق على جهاز افتراضي (وضع Light Agent). ويمكن أن تساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في البيئات الافتراضية في Citrix وVMware القيم المتاحة: • `1` إضافة استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة. • `0` تعطيل استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة (الافتراضي).
	`EnableUniqueSensorID`	إنشاء معرف كمبيوتر فريد (Sensor ID) أثناء تثبيت أو تحديث التطبيق. يتم استخدام Sensor ID في حل Kaspersky Anti Targeted Attack Platform لتحديد أجهزة الكمبيوتر التي ترسل القياس عن بُعد إلى الخادم. وعند إنشاء Sensor ID، يستخدم التطبيق خوارزمية تضع في الاعتبار تكوين الكمبيوتر، مثل الرقم التسلسلي للوحة الأم. وفي بعض الحالات، على سبيل المثال، عند استخدام التطبيق في بيئة افتراضية، قد يتم تكرار Sensor ID. ونتيجة لذلك، يتعذر على Kaspersky Anti Targeted Attack Platform تحديد الكمبيوتر الذي يتم إرسال القياس عن بُعد منه. ولإنشاء Sensor ID فريد، تحتاج إلى ضبط المعلمة `EnableUniqueSensorID=1`. ونتيجة لذلك، سيستخدم التطبيق خوارزمية مختلفة لإنشاء Sensor ID، والذي يضع في الاعتبار البيانات الأخرى حول الكمبيوتر. ويضمن هذا وجود Sensor ID فريد. بشكل افتراضي، لا يتم تعيين المعلمة. ويرث التطبيق Sensor ID في الحالات التالية: • تحديث إصدار التطبيق؛ • ترحيل تكوين [KES+KEA] إلى تكوين [KES+العامل المضمن] كجزء من إصلاح التطبيق، يحاول المثبت وراثة Sensor ID. إذا كان من غير الممكن استعادة Sensor ID، فإن التطبيق ينشئ Sensor ID.
	`CitrixCompatibility`	تمكين دعم Citrix Provisioning Services لتثبيت Kaspersky Endpoint Security إلى جهاز افتراضي.
`[Components]`	`ALL`	تثبيت جميع المكونات. إذا تم تحديد قيمة المعلمة `1`، فسيتم تثبيت كل المكونات بغض النظر عن إعدادات تثبيت المكونات الفردية. نظرًا للطريقة التي يتم بها دعم حلول Detection and Response، يتم تثبيت مكوني Endpoint Detection and Response Optimum وSandbox على الكمبيوتر. ولا يتوافق مكون Endpoint Detection and Response Expert (cloud) 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.

القسم	المعلمة	الوصف
	`CloudDiscovery`	Cloud Discovery.
	`LogInspector`	فحص السجل
	`AntiCryptor`	مكافحة التشفير
	`FileThreatProtection`	الحماية من تهديدات الملفات.
	`SystemIntegrityMonitor`	مراقبة سلامة النظام.
	`FileEncryption`	أقسام التشفير على مستوى الملف.
	`DiskEncryption`	مكتبات تشفير القرص بالكامل.
	`MSBitLocker`	مكتبات إدارة تشفير BitLocker.
	`BadUSBAttackPrevention`	منع هجمات BadUSB.
	`EDR`	Endpoint Detection and Response Optimum لا يتوافق المكون مع مكوني (`EDRCloud`) Endpoint Detection and Response Expert (cloud) و(`AntiAPT`) Endpoint Detection and Response Expert (on-premises).
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) لا يتوافق المكون مع مكوني (`EDR`) Endpoint Detection and Response Optimum وEndpoint Detection and Response Expert (on-premises) (`AntiAPT`).
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) لا يتوافق المكون مع مكوني (`EDRCloud`) Endpoint Detection and Response Expert (cloud) و(`EDR`) Endpoint Detection and Response Optimum.
	`SB`	Kaspersky Sandbox أو KATA Sandbox. Kaspersky Sandbox هو حل اكتشاف واستجابة مستقل بواسطة Kaspersky. KATA Sandbox هو مكون في حل Kaspersky Anti Targeted Attack Platform.
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) لا يتوافق المكون مع مكوني (`EDRCloud`) Endpoint Detection and Response Expert (cloud) و(`EDR`) Endpoint Detection and Response Optimum.
	`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.
	`KUMAIntegration`	التكامل مع KUMA.
	`StandaloneKATA`	تثبيت التطبيق في وضع Endpoint Detection and Response Agent (EDR Agent) للتكامل مع Kaspersky Anti Targeted Attack Platform (EDR).
	`StandaloneMDR`	تثبيت التطبيق في وضع Endpoint Detection and Response Agent (EDR Agent) للتكامل مع Kaspersky Managed Detection and Response.
	`StandaloneNDR`	تثبيت التطبيق في وضع Endpoint Detection and Response Agent (EDR Agent) للتكامل مع Kaspersky Anti Targeted Attack Platform (NDR).
	`StandaloneSiemTelemetry`	تثبيت التطبيق في وضع Endpoint Detection and Response Agent (EDR Agent) للتكامل مع KUMA.

القسم	المعلمة	الوصف
[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.

عمليات Kaspersky Endpoint Security for Windows

يبدأ Kaspersky Endpoint Security for Windows العمليات الموضحة في الجدول أدناه.

عمليات Kaspersky Endpoint Security for Windows

اسم الملف	الغرض
avp.exe	عملية تشغيل Kaspersky Endpoint Security for Windows.
avpsus.exe	تتيح هذه العملية تثبيت تحديثات وحدات التطبيق الهامة والمعتمدة والتراجع عنها.

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.

لا تتوفر هذه الطريقة إذا تم تثبيت التطبيق عبر Kaspersky Security Center. ولا يمكنك تغيير اختيار مكونات التطبيق في لوحة التحكم إلا بعد تثبيت التطبيق محليًا.

- 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.

- إذا كان التطبيق مثبت في وضع Light Agent في البنية التحتية VDI، فإن تغيير مكونات المجموعة غير مدعوم.

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

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.

   تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **حدد المكونات المراد تثبيتها**.

الخطوة الثانية: إعدادات المهمة لتغيير مكونات التطبيق

تحديد تكوين التطبيق:

- **الوضع القياسي لحماية المضيفين**. التكوين الافتراضي. يتيح لك هذا التكوين استخدام كل مكونات التطبيق، بما في ذلك المكونات التي توفر الدعم لحلول Detection and Response. ويُستخدم هذا التكوين لتوفير الحماية الشاملة للكمبيوتر من مجموعة متنوعة من التهديدات وهجمات الشبكة والاحتيال.

- **Endpoint Detection and Response Agent للحماية من التهديدات المتقدمة والهجمات المستهدفة**. في هذا التكوين ، يمكنك فقط تثبيت المكونات التي توفر الدعم لحلول الاكتشاف والاستجابة: MDR و EDR (KATA) و NDR (KATA) و EDR Expert (on-premises)، وكذلك KUMA. ويعد هذا التكوين ضروريًا إذا تم نشر Endpoint Protection Platform (EPP) تابع لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.

عند تغيير تكوين التطبيق لأجل EDR Agent للعمل مع MDR، تأكد من تمكين المكونات المسؤولة عن استلام القياس عن بُعد.

- **Light Agent لحماية البيئات الافتراضية**. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. وفي هذا التكوين، لا يمكنك استخدام مكونات تشفير البيانات أو مراقبة عيوب التكيف. وإذا كنت تقوم بتثبيت Light Agent على قالب جهاز افتراضي سيتم استخدامه لإنشاء أجهزة افتراضية غير ثابتة، حدد خانة الاختيار **حماية البنية التحتية لسطح المكتب الافتراضي** (VDI يعني Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية.

حدد مكونات التطبيق التي ستكون متاحة على كمبيوتر المستخدم.

الخطوة 3. الإعدادات المتقدمة

قم بتكوين الإعدادات المتقدمة للمهمة (انظر الجدول أدناه).

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: تكوين جدول بدء المهمة

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

الخطوة السادسة: تحديد اسم المهمة

أدخل اسم المهمة، مثل إضافة مكون التحكم في التطبيقات.

الخطوة 7 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية إضافة أو إزالة مكونات التطبيقات في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر على **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 14.2.0**.
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 **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.

من خصائص الكمبيوتر، حدد علامة التبويب **Application settings**. بعد ذلك، حدد تكوين التطبيق:

- **Standard mode to protect workstations and servers**. التكوين الافتراضي. يتيح لك هذا التكوين استخدام كل مكونات التطبيق، بما في ذلك المكونات التي توفر الدعم لحلول Detection and Response. ويُستخدم هذا التكوين لتوفير الحماية الشاملة للكمبيوتر من مجموعة متنوعة من التهديدات وهجمات الشبكة والاحتيال.
- **Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks**. في هذا التكوين ، يمكنك فقط تثبيت المكونات التي توفر الدعم لحلول الاكتشاف والاستجابة: MDR و EDR (KATA) و NDR (KATA) و EDR Expert (on-premises)، وكذلك KUMA. ويعد هذا التكوين ضروريًا إذا تم نشر Endpoint Protection Platform (EPP) تابع لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.

عند تغيير تكوين التطبيق لأجل EDR Agent للعمل مع MDR، تأكد من تمكين المكونات المسؤولة عن استلام القياس عن بُعد.

- **Light Agent to protect virtual environments**. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. وفي هذا التكوين، لا يمكنك استخدام مكونات تشفير البيانات أو مراقبة عيوب التكيف. وإذا كنت تقوم بتثبيت Light Agent على قالب جهاز افتراضي سيتم استخدامه لإنشاء أجهزة افتراضية غير ثابتة، حدد خانة الاختيار **Protect VDI infrastructure** (VDI يعني Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية.

حدد مكونات التطبيق التي ستكون متاحة على كمبيوتر المستخدم. قم بتكوين الإعدادات المتقدمة للمهمة (انظر الجدول أدناه).

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.

قد تحدث أخطاء عند تثبيت Kaspersky Endpoint Security أو تحديثه أو إلغاء تثبيته. وللحصول على المزيد من المعلومات عن حل هذه الأخطاء، يُرجى الرجوع إلى قاعدة معارف الدعم الفني.

الإعدادات المتقدمة للمهمة

المعلمة	الوصف
إعدادات المهمة	**التحقق من وجود تطبيقات جهات خارجية غير متوافقة**. بشكل افتراضي، يتحقق Kaspersky Endpoint Security من توافق التطبيقات المثبتة. تتوفر قائمة البرامج التي قد تسبب مشكلات في التوافق في ملف incompatible.txt. ويتم تضمين الملف في مجموعة التوزيع. وإذا تم تمكين فحص البرامج المثبتة، فعند اكتشاف تطبيق من القائمة، يوقف Kaspersky Endpoint Security المهمة. ويمكنك تعطيل فحص البرامج المثبتة إذا كانت وثائق البائع الخاصة ببرنامج الجهة الخارجية تزعم التوافق مع Endpoint Protection Platform (EPP). **إزالة تطبيقات الجهات الخارجية غير المتوافقة**. الإزالة التلقائية للتطبيقات المدرجة في ملف incompatible.txt قبل تغيير مجموعة المكونات. إذا تم تمكين هذه الوظيفة، يحاول Kaspersky Endpoint Security إزالة التطبيقات التي قد تسبب مشكلات في التوافق لمواصلة المهمة. **استخدم وضع التوافق مع Azure WVD**. تضمن هذه الميزة العرض الصحيح لحالة الجهاز الافتراضي في Azure في وحدة تحكم 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 (Sensor ID). ويسمح وضع التوافق مع Azure WVD بتعيين Sensor ID فريد دائم لهذه الأجهزة الظاهرية. وفي حالة إيقاف تشغيل وضع التوافق، Sensor ID 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.
الاستثناءات	بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم. بدءًا من الإصدار Kaspersky Endpoint Security 12.8 for Windows، يمكنك تثبيت التطبيق في وضع Light Agent لحماية البيئات الافتراضية. ويمكن أن تساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في البيئات الافتراضية في Citrix وVMware. يمكنك أيضًا تكوين المنطقة الموثوقة لاحقًا في خصائص السياسة: استثناءات الفحص والتطبيقات الموثوقة.
الوضع المنفصل / الوضع المشترك	يمكنك إنشاء مجموعات منفصلة من المكونات لمحطات العمل والخوادم – **الوضع المنفصل**. وقبل نشر حزمة التثبيت، يكتشف المثبت نوع نظام التشغيل ويثبت فقط مكونات التطبيق التي حددتها لنوع نظام التشغيل هذا. وبهذه الطريقة، يمكنك استخدام حزمة التثبيت نفسها لمحطات العمل والخوادم. يقدم **الوضع المشترك** قائمة مشتركة من المكونات لمحطة العمل والخوادم. ويعتمد توفر المكونات الفردية على نوع نظام التشغيل. وفي هذا الوضع، نوصي بإنشاء حزمة تثبيت منفصلة لمحطات العمل وحزمة تثبيت منفصلة للخوادم. ويمكنك تكوين قائمة المكونات العامة في حزمة التثبيت في الوضع القياسي فقط.
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.
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 [KEA+KES] إلى [KES+العامل المدمج]، أو إذا كنت تقوم بالترحيل من KSWS إلى KES، فيجب عليك إدخال كلمة مرور لإزالة هذه التطبيقات.

ترقية إصدار سابق من التطبيق

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

- 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.
- لتغيير لغة التطبيق، في مهمة Install application remotely، حدد حزمة التثبيت مع الترجمة المفضلة لديك وقم بتحديث التطبيق. وقد أصبح تغيير لغة التطبيق متاحًا لأول مرة في Kaspersky Endpoint Security for Windows 14.2.

يدعم Kaspersky Endpoint Security تحديثات الإصدارات التالية من التطبيق:

- Kaspersky Endpoint Security 12.3 for Windows (الإصدار 12.3.0.493)
- Kaspersky Endpoint Security 12.4 for Windows (الإصدار 12.4.0.467)

- Kaspersky Endpoint Security 12.5 for Windows (الإصدار 12.5.0.539)
- Kaspersky Endpoint Security 12.6 for Windows (الإصدار 12.6.0.438)
- Kaspersky Endpoint Security 12.7 for Windows (الإصدار 12.7.0.533)
- Kaspersky Endpoint Security 12.8 for Windows (الإصدار 12.8.0.505)
- Kaspersky Endpoint Security 12.9 for Windows (الإصدار 12.9.0.384)
- Kaspersky Endpoint Security 12.10 for Windows (الإصدار 12.10.0.466)
- Kaspersky Endpoint Security 12.11 for Windows (الإصدار 12.11.0.637)
- Kaspersky Endpoint Security 12.12 for Windows (الإصدار 12.12.0.522)
- Kaspersky Endpoint Security 14.0 for Windows (الإصدار 14.0.0.504)
- Kaspersky Endpoint Security 14.1 for Windows (الإصدار 14.1.0.423)

قد تحدث أخطاء عند تثبيت Kaspersky Endpoint Security أو تحديثه أو إلغاء تثبيته. وللحصول على المزيد من المعلومات عن حل هذه الأخطاء، يُرجى الرجوع إلى قاعدة معارف الدعم الفني.

طرق ترقية التطبيق

يمكن تحديث Kaspersky Endpoint Security على جهاز الكمبيوتر بطرق التالية:

- استخدام خدمة التحديث من Kaspersky (Seamless Update – SMU).
- 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 الذي تم نشره في شبكة الشركة يتضمن مجموعة من المكونات مختلفة عن المجموعة الافتراضية، فإن تحديث التطبيق من خلال وحدة تحكم الإدارة (MMC) يختلف عن تحديث التطبيق من خلال Web Console. فكر فيما يلي عند تحديث Kaspersky Endpoint Security:

- Kaspersky Security Center Web 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. أي أنه إذا كان الإصدار الجديد من التطبيق يحتوي على المجموعة الافتراضية من المكونات، فسيتم، على سبيل المثال، إزالة عميل MDR المدمج من الكمبيوتر، نظرًا لأن هذا المكون مُستثنى 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.
- لا يمكن ترقية التطبيق على جهاز افتراضي بدون إعادة تشغيل. ولترقية التطبيق على جهاز افتراضي، يجب إعادة تشغيل الجهاز الافتراضي.

بعد ترقية التطبيق أو تثبيت تصحيح أو تغيير مجموعة مكونات التطبيق أو الاستعادة، تتم إعادة تشغيل Kaspersky Endpoint Security لبدء استخدام الإصدار الجديد. وقد تستغرق إعادة تشغيل Kaspersky Endpoint Security ما يصل إلى دقيقة واحدة. وأثناء ذلك الوقت، يتم خفض مستوى حماية الكمبيوتر. وبعد إعادة تشغيل التطبيق، سيتم استعادة مستوى حماية الكمبيوتر.

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

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
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. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تحديد وضع ترقية التطبيق في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **User Interaction**.

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

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ 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 **عام**، حدد أو امسح خانة الاختيار **تثبيت التحديثات دون إعادة تشغيل الكمبيوتر** لتكوين وضع ترقية التطبيق.

4. احفظ تغييراتك.

يمكنك أيضًا تحديد وضع ترقية التطبيق عند تثبيت التطبيق من سطر الأوامر (باستخدام الخيار UPGRADEMODE).

بعد إجراء ترقية التطبيق دون انتهاء إعادة التشغيل، سيتم تثبيت الإصدار الجديد من Kaspersky Endpoint Security على الكمبيوتر. ويتم حذف الإصدار السابق من التطبيق تلقائيًا.

لا يمكنك بدء ترقية تطبيق قبل انتهاء الترقية السابقة تمامًا.

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

تحديث SMU للتطبيق

لتحديث التطبيق باستخدام خدمة التحديث من Kaspersky (Seamless Update؛ SMU)، لن تحتاج إلى تشغيل برنامج التثبيت، على عكس طرق التحديث الأخرى. ويحصل Kaspersky Endpoint Security على الإصدار الجديد من التطبيق جنبًا إلى جنب مع قواعد بيانات مكافحة الفيروسات من المصدر نفسه.

يسمح تحديث SMU بتحديث التطبيق على جميع أجهزة الكمبيوتر في مؤسستك إلى أحدث إصدار. وقبل تطبيق تحديث SMU، نوصي باختبار الإصدار الجديد من التطبيق على عدد قليل من أجهزة الكمبيوتر. ولفعل ذلك، يجب عليك تحديث التطبيق على أجهزة الكمبيوتر هذه يدويًا (على سبيل المثال، محليًا باستخدام معالج الإعداد). ولا يمكنك تحديد أجهزة كمبيوتر فردية عند إجراء تحديث SMU.

يتم تحديد جدول تحديث التطبيق بواسطة موظفي Kaspersky. وللتأكد من تشغيل الإصدار الجديد من التطبيق بسلاسة، تتيح Kaspersky التحديثات خطوة بخطوة. ويعني هذا أنك قد تحصل على تحديث SMU الخاص بك بعد شهرين من طرح الإصدار الجديد.

يمكنك إدارة تحديث SMU للتطبيق باستخدام مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق. ولتضمين الإصدار الجديد من التطبيق في الحزمة نفسها مثل قواعد بيانات مكافحة الفيروسات، يجب السماح بتحديث الوحدات النمطية للتطبيق في إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق. أيضًا في إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، يمكنك السماح بتحديث التطبيق دون إعادة تشغيل.

خطوات تحديث SMU للتطبيق

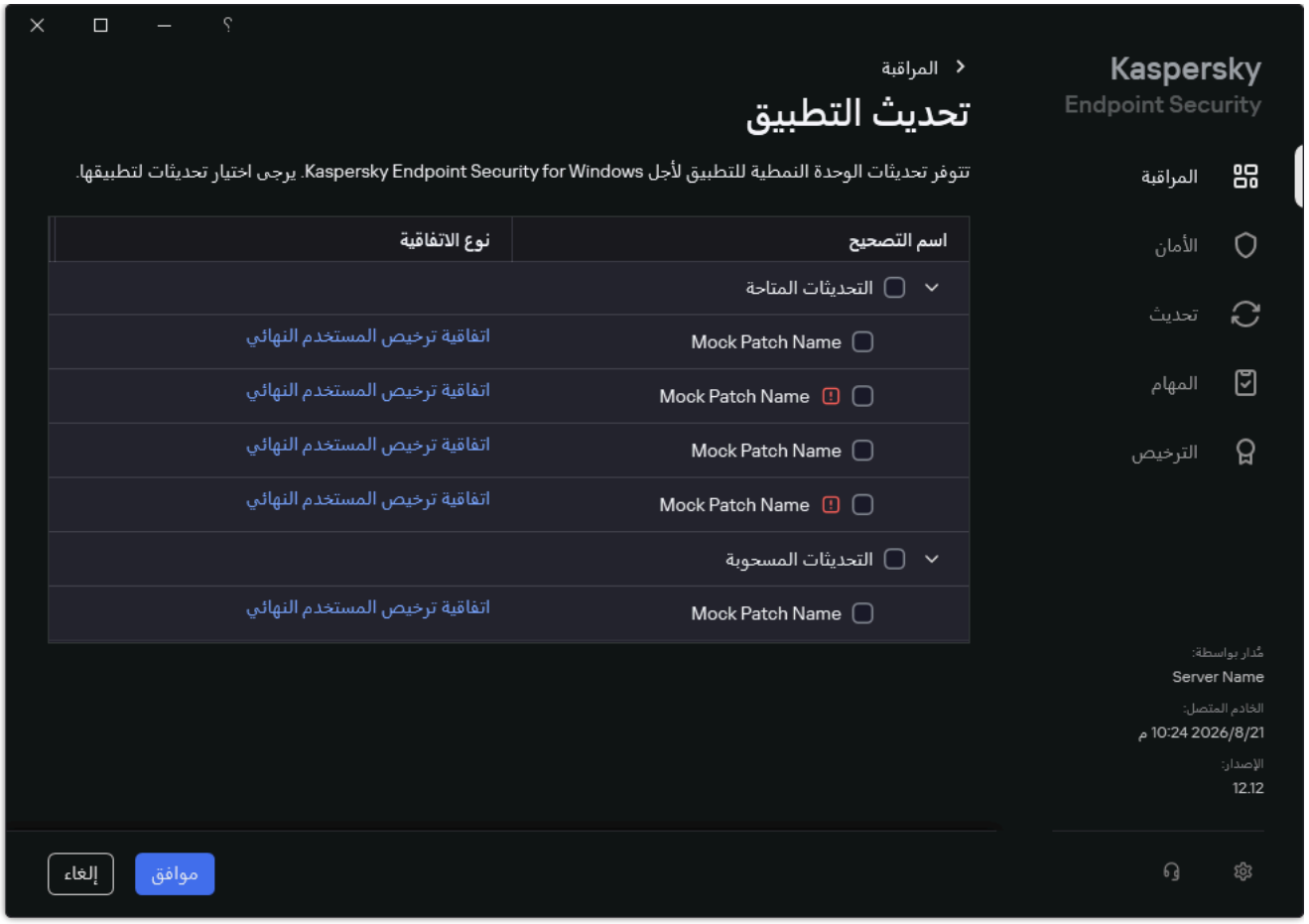
1. **بعد إصدار جديد من التطبيق، توزع Kaspersky التحديث.**
2. **يوافق المستخدم على تحديث التطبيق.**

إذا كان الكمبيوتر متصلاً بـ Kaspersky Security Center، فإن التحديث يكون متاحًا في Kaspersky Security Center، في القسم **تحديث قواعد بيانات Kaspersky والوحدات النمطية للتطبيق**. وللمزيد من التفاصيل عن اعتماد التحديثات، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

إذا لم يكن الكمبيوتر متصلاً بـ Kaspersky Security Center، فإن التحديث يكون متاحًا في قسم الإخطارات في واجهة التطبيق: . وللموافقة على التحديث، حدد إصدارًا من التطبيق واقبل شروط وأحكام الاتفاقيات (انظر الشكل أدناه).

3. **يقوم Kaspersky Endpoint Security بتشغيل مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وفقًا للجدول الزمني الذي تم تكوينه.**

ونتيجة لذلك، يقوم Kaspersky Endpoint Security بتحديث التطبيق في الوضع "الصامت".



تحديثات التطبيق المتاحة

إزالة التطبيق

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

قد تحدث أخطاء عند تثبيت Kaspersky Endpoint Security أو تحديثه أو إلغاء تثبيته. وللحصول على المزيد من المعلومات عن حل هذه الأخطاء، يُرجى الرجوع إلى قاعدة معارف الدعم الفني.

إزالة التطبيق عن بعد باستخدام Kaspersky Security Center

يُمكنك إلغاء تثبيت التطبيق عن بُعد عن طريق استخدام مهمة Uninstall application remotely. 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. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Tasks**.
تفتح قائمة المهام.

3. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Security Center Administration Server ← Advanced ← Uninstall application remotely**.

الخطوة الثانية: اختيار التطبيق الذي ترغب في إزالته

حدد **Uninstall application supported by Kaspersky Security Center**.

الخطوة الثالثة: إعدادات المهمة لإلغاء تثبيت التطبيق

حدد **Kaspersky Endpoint Security for Windows (14.2)**.

الخطوة الرابعة: إلغاء تثبيت إعدادات الأداة المساعدة

قم بتكوين إعدادات التطبيق الإضافية التالية:

- **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.

- **Verify operating system type before downloading**. 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 **Use uninstallation password**.
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 14.2.

الخطوة 10. الانتهاء من إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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 نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

2. انقر على **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 Kaspersky Endpoint Security من أجهزة كمبيوتر الدعم الفني.

4. في القسم **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 نوع **Uninstall managed application**.

2. حدد **Kaspersky Endpoint Security for Windows**.

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 الأداة المساعدة لإلغاء 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 مهمة، حدد خانة الاختيار المقابلة للمهمة 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 نافذة Web Console الرئيسية، حدد **Asset management** ← **Tasks**.
تفتح قائمة المهام.

2. انقر فوق مهمة **Uninstall application remotely** في 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 المعرّف الفريد العام (GUID) للتطبيق في قاعدة معارف الدعم الفني أو 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=samplePassword /qn
```

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

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.

يحفظ Kaspersky Endpoint Security البيانات في المجلد `C:\ProgramData\Kaspersky Lab\KES.14.2\QB`.

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. ولا يمكن تفعيل التطبيق بموجب ترخيص تجريبي بعد تفعيله باستخدام ترخيص تجاري.

- 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:

- معرف 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.
- احصل على ملف مفتاح من خادم إدارة آخر.

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

مقارنة وظائف التطبيق حسب نوع ترخيص Kaspersky Next، راجع تعليمات Kaspersky Next.

مقارنة بين مزايا برنامج Kaspersky Endpoint Security

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	Kaspersky Hybrid Cloud Security Enterprise
الحماية من التهديدات المتقدمة								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
اكتشاف السلوك	✓	✓	✓	✓	✓	✓	✓	✓
مكافحة أداة التشفير	✓	✓	✓	✓	✓	✓	✓	✓
منع الاستغلال	✓	✓	✓	✓	✓	✓	✓	✓
منع اختراق المضيف	✓	✓	✓	✓	✓	✓	✓	✓
محرك المعالجة	✓	✓	✓	✓	✓	✓	✓	✓
الحماية من التهديدات الأساسية								
الحماية من تهديدات الملفات	✓	✓	✓	✓	✓	✓	✓	✓
الحماية من تهديدات الويب	✓	✓	✓	✓	✓	✓	✓	✓
الحماية من تهديدات البريد	✓	✓	✓	✓	✓	✓	✓	✓

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	Kaspersky Hybrid Cloud Security Enterprise
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 النظام	–	–	–	–	–	–	–	–
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)	✓	✓	✓	✓	✓	✓	✓	✓
التكامل مع KUMA (يجب شراء ترخيص تكامل KUMA بشكل منفصل)	✓	✓	✓	✓	✓	✓	✓	✓
وضع Light Agent (لتفعيل التطبيق، يجب عليك إضافة مفتاح ترخيص إلى SVM الذي يتصل به Light Agent)	–	–	–	–	–	–	✓	✓

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 وظائف التطبيق حسب نوع ترخيص Kaspersky Next، راجع تعليمات Kaspersky Next.

مقارنة بين مزايا برنامج Kaspersky Endpoint Security

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	Kaspersky Hybrid Cloud Security Enterprise
الحماية من التهديدات المتقدمة								
Kaspersky Security Network	✓	✓	✓	✓	✓	✓	✓	✓
اكتشاف السلوك	✓	✓	✓	✓	✓	✓	✓	✓
مكافحة أداة التشفير	✓	✓	✓	✓	✓	✓	✓	✓
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 النظام	–	–	–	–	–	–	–	✓

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	Kaspersky Hybrid Cloud Security Enterprise
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)	✓	✓	✓	✓	✓	✓	✓	✓
التكامل مع KUMA (يجب شراء ترخيص تكامل KUMA بشكل منفصل)	✓	✓	✓	✓	✓	✓	✓	✓
وضع Light Agent (لتفعيل التطبيق، يجب عليك إضافة مفتاح ترخيص إلى SVM الذي يتصل به Light Agent)	–	–	–	–	–	–	✓	✓

تفعيل التطبيق

التفعيل هي عملية تفعيل الترخيص 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 بعد باستخدام مجموعة برامج Kaspersky Security Center.
  - استخدام مهمة إضافة مفتاح.

    تتيح لك هذه الطريقة القيام بإضافة مفتاح لجهاز كمبيوتر معين أو لأجهزة الكمبيوتر التي تُعد جزءًا من مجموعة الإدارة. يمكنك إضافة المفتاح النشط والمفتاح الاحتياطي بهذه الطريقة.
  - 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.

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

- 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.
- 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".

> إذا تم استخدام Kaspersky Endpoint Security في وضع Light Agent لحماية البيئات الافتراضية، فلن تحتاج إلى تفعيل التطبيق بشكل منفصل.

تفعيل التطبيق

كيفية تفعيل التطبيق في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.

   تفتح قائمة المهام.
2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **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

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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 نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر على **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 14.2**.

2. في القائمة المنسدلة **Task type**، حدد **Add key**.

3. في الحقل **Task name**، أدخل وصفًا موجزًا، مثل تفعيل Kaspersky Endpoint Security for Windows.

4. في القسم **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 (**Operations** ← **Licensing**) Web Console.

الخطوة 4 إكمال إنشاء المهمة

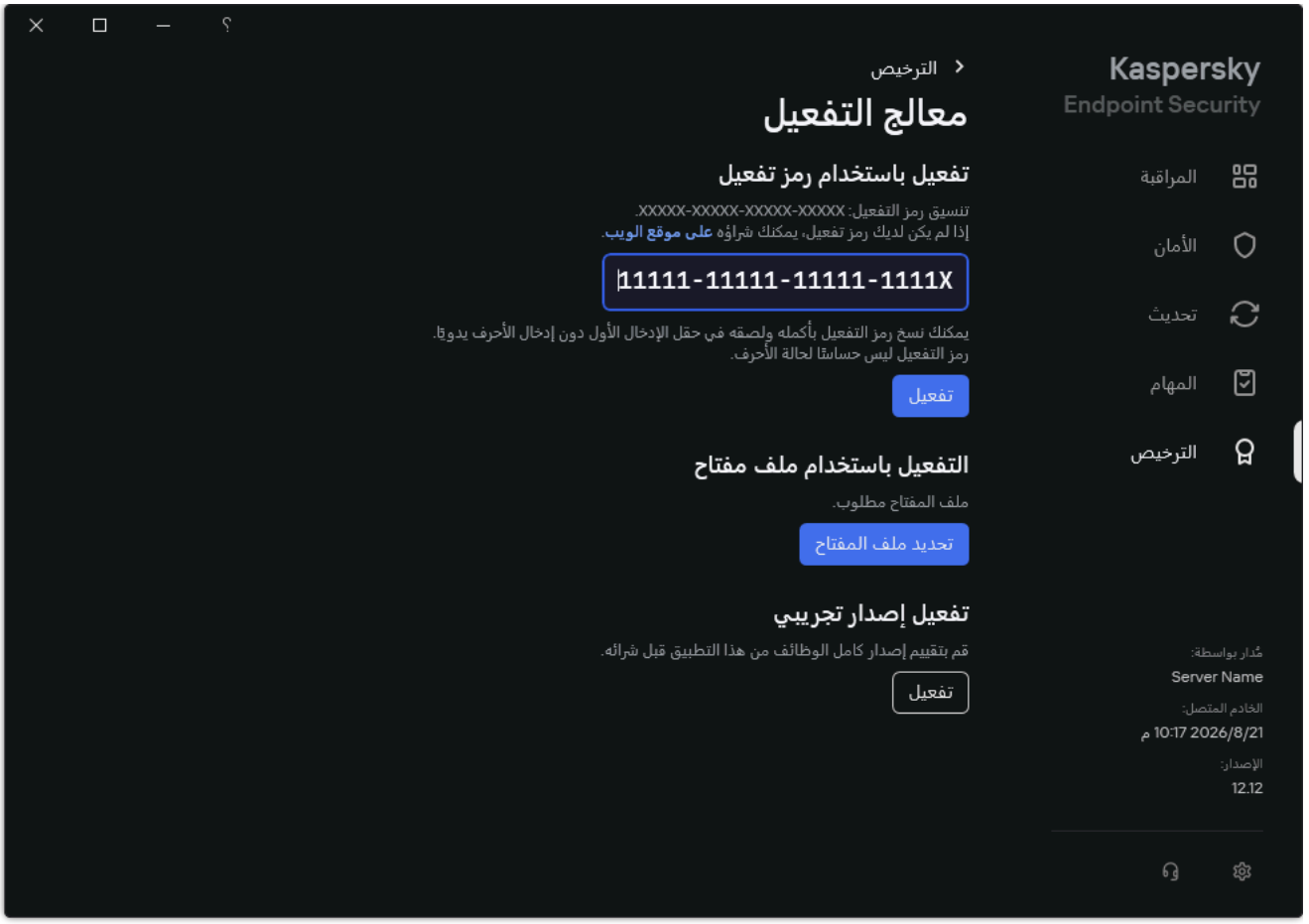
قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**. سيتم عرض مهمة جديدة في قائمة المهام. لتشغيل مهمة، حدد خانة الاختيار المقابلة للمهمة وانقر فوق الزر **Start**. ونتيجة لذلك، سيتم تفعيل Kaspersky Endpoint Security على أجهزة كمبيوتر المستخدمين في الوضع الصامت.

كيفية تفعيل التطبيق في واجهة التطبيق

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

في خصائص مهمة إضافة مفتاح، يمكنك إضافة مفتاح احتياطي إلى الكمبيوتر. يصبح المفتاح الإضافي نشطًا عند انتهاء صلاحية المفتاح النشط. 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 **Kaspersky Licenses**.

   ستفتح قائمة بمفاتيح الترخيص.

2. افتح خصائص مفتاح الترخيص.

3. في القسم **عام**، حدد خانة الاختيار **Automatically distribute license key to managed devices**.

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 **Devices**.

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

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

   ستفتح قائمة بمفاتيح الترخيص.

2. افتح خصائص مفتاح الترخيص.

3. في علامة التبويب **General**، قم بتمكين مفتاح التبديل **Automatically distribute license key to managed devices**.

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. ويمكنك عرض عدد أجهزة الكمبيوتر التي تمت إضافة المفتاح إليها وبيانات أخرى في خصائص المفتاح في علامة التبويب **Devices**.

إذا كنت تقوم بتفعيل التطبيق باستخدام رمز التفعيل، فستحتاج إلى الوصول إلى الإنترنت للاتصال بخوادم التفعيل في Kaspersky. وإذا كنت تقوم بتفعيل التطبيق باستخدام ملف مفتاح، فلن يكون الوصول إلى الإنترنت ضروريًا. وإذا كانت أجهزة الكمبيوتر موجودة في جزء شبكة منعزل بدون اتصال بالإنترنت، فلتفعيل التطبيق برمز، يجب أن تسمح باستخدام خادم إدارة Kaspersky Security Center كخادم وكيل. بمعنى، يستطيع التطبيق الوصول إلى خوادم التفعيل من خلال خادم الإدارة الذي يمتلك الوصول إلى الإنترنت.

كيفية السماح باستخدام خادم الإدارة كخادم وكيل لتفعيل التطبيق في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.

4. حدد خانة الاختيار **استخدام Kaspersky Security Center كالخادم الوكيل للتفعيل**.

5. احفظ تغييراتك.

كيفية السماح باستخدام خادم الإدارة كخادم وكيل لتفعيل التطبيق في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **General Settings** ← **KSC Integration**.

5. حدد خانة الاختيار **Use Kaspersky Security Center as proxy server for activation**.

6. احفظ تغييراتك.

إذا لم تتمكن من تفعيل التطبيق باستخدام رمز التفعيل، يمكنك محاولة الحصول على ملف مفتاح باستخدام حل Kaspersky ومحاولة تفعيل التطبيق مرة أخرى باستخدام طريقة مختلفة.

مراقبة استخدام الترخيص

يمكنك مراقبة استخدام التراخيص بالطرق التالية:

- عرض Report on usage of license keys للبنية التحتية للمؤسسة (**Reports** ← **Monitoring**).
- عرض حالات أجهزة الكمبيوتر في **Managed devices** ← علامة التبويب **Devices**. إذا لم يتم تفعيل التطبيق، فستكون حالة الكمبيوتر ⚠ لم يتم تفعيل التطبيق.

- عرض معلومات الترخيص في خصائص الكمبيوتر.
- عرض الخصائص الرئيسية (**Licensing** ← **Operations**).

تفاصيل تفعيل التطبيق كجزء من Kaspersky Security Center Cloud Console

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.

إزالة مفتاح الترخيص

لإزالة مفتاح ترخيص، تحتاج إلى تشغيل مهمة خاصة على أجهزة الكمبيوتر الخاصة بك. ويمكنك إزالة مفتاح ترخيص، على سبيل المثال، لإعادة ترتيب وحدات الترخيص. وأيضًا، عند انتهاء صلاحية الترخيص، يخطرك Kaspersky Endpoint Security بذلك. وإذا أضفت مفتاح ترخيص لفترة قصيرة لتجربة التطبيق (على سبيل المثال، وظيفة EDR Optimum الإضافية)، فيمكنك إزالة مفتاح الترخيص هذا للتخلص من الإخطارات وإصلاح حالة الكمبيوتر الخاص بك.

تسمح لك المهمة إزالة المفتاح بإزالة أي مفاتيح ترخيص من الكمبيوتر. ويمكنك إزالة مفاتيح الترخيص النشطة وكذلك الاحتفاظ بمفاتيح الترخيص. وبالإضافة إلى مفتاح ترخيص تفعيل Kaspersky Endpoint Security، يمكنك إزالة مفاتيح الترخيص الفردية لحلول Kaspersky Detection and Response (على سبيل المثال، وظيفة EDR Optimum الإضافية).

كيفية إزالة مفتاح ترخيص في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.

   تفتح قائمة المهام.

2. انقر فوق **New task**.

   يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **إزالة المفتاح**.

الخطوة الثانية: اختيار ترخيص

حدد مفتاح الترخيص الذي تريد حذفه. يمكنك تحديد مفتاح ترخيص من مخزن مفاتيح Kaspersky Security Center أو تحديد ملف مفتاح.

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، على سبيل المثال، إزالة مفتاح للإصدار التجريبي.

الخطوة 6 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية إزالة مفتاح ترخيص في وحدة Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر على **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 14.2**.
2. في القائمة المنسدلة **Task type**، حدد **Remove key**.

3. في الحقل **Task name**، أدخل وصفًا مختصرًا، علي سبيل المثال، إزالة مفتاح للإصدار التجريبي.

4. في القسم **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 مفتاح الترخيص الذي تريد حذفه. يمكنك تحديد مفتاح ترخيص من مخزن مفاتيح Kaspersky Security Center أو تحديد ملف مفتاح. انتقل إلى الخطوة التالية.

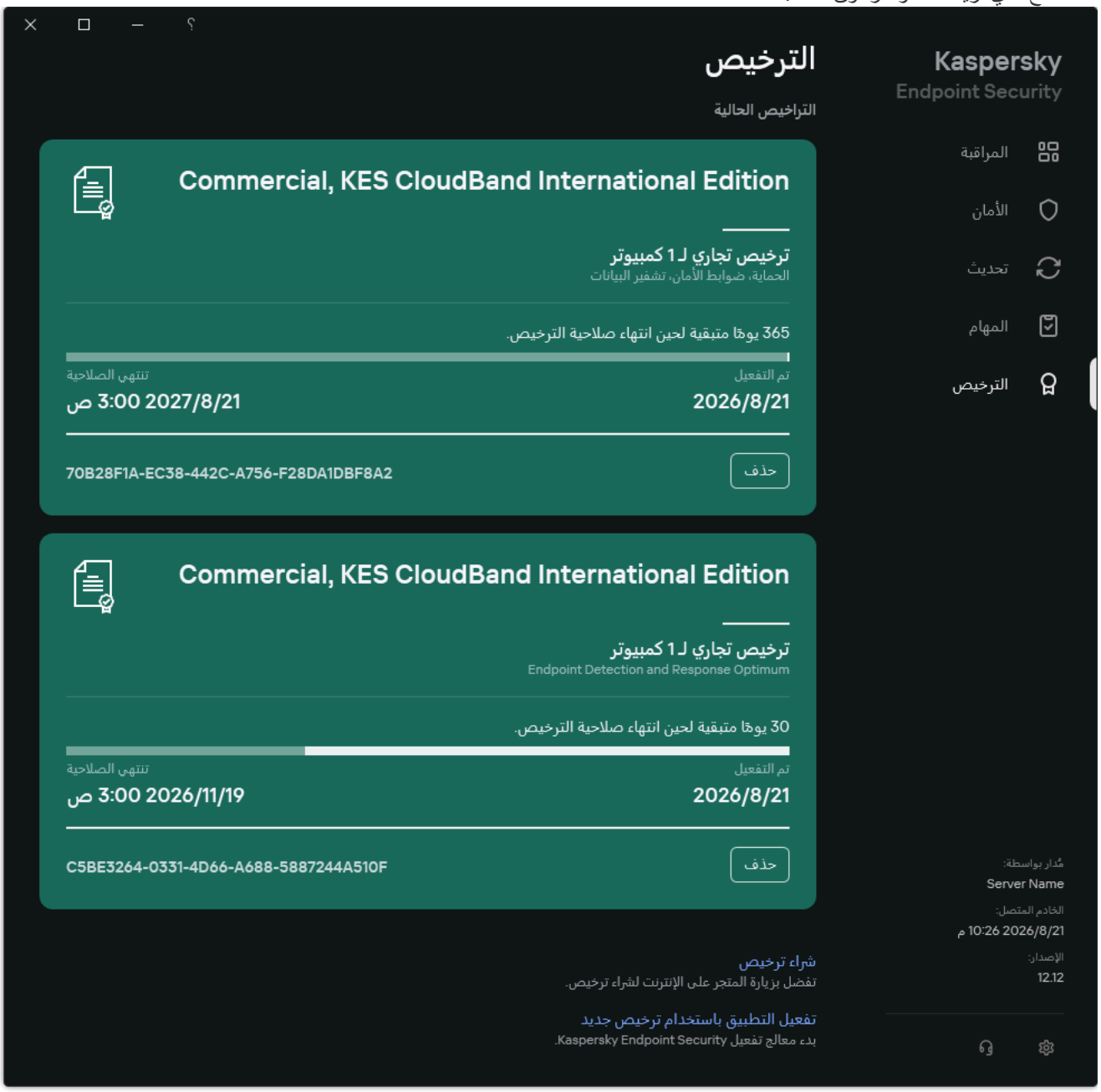
الخطوة 4 إكمال إنشاء المهمة

قم بإنهاء المعالج عن طريق النقر فوق الزر **Finish**. سيتم عرض مهمة جديدة في قائمة المهام. لتشغيل مهمة، حدد خانة الاختيار المقابلة للمهمة وانقر فوق الزر **Start**.

كيفية إزالة مفتاح ترخيص في واجهة التطبيق

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

2. حدد المفتاح الذي تريد حذفه وانقر فوق **حذف**.



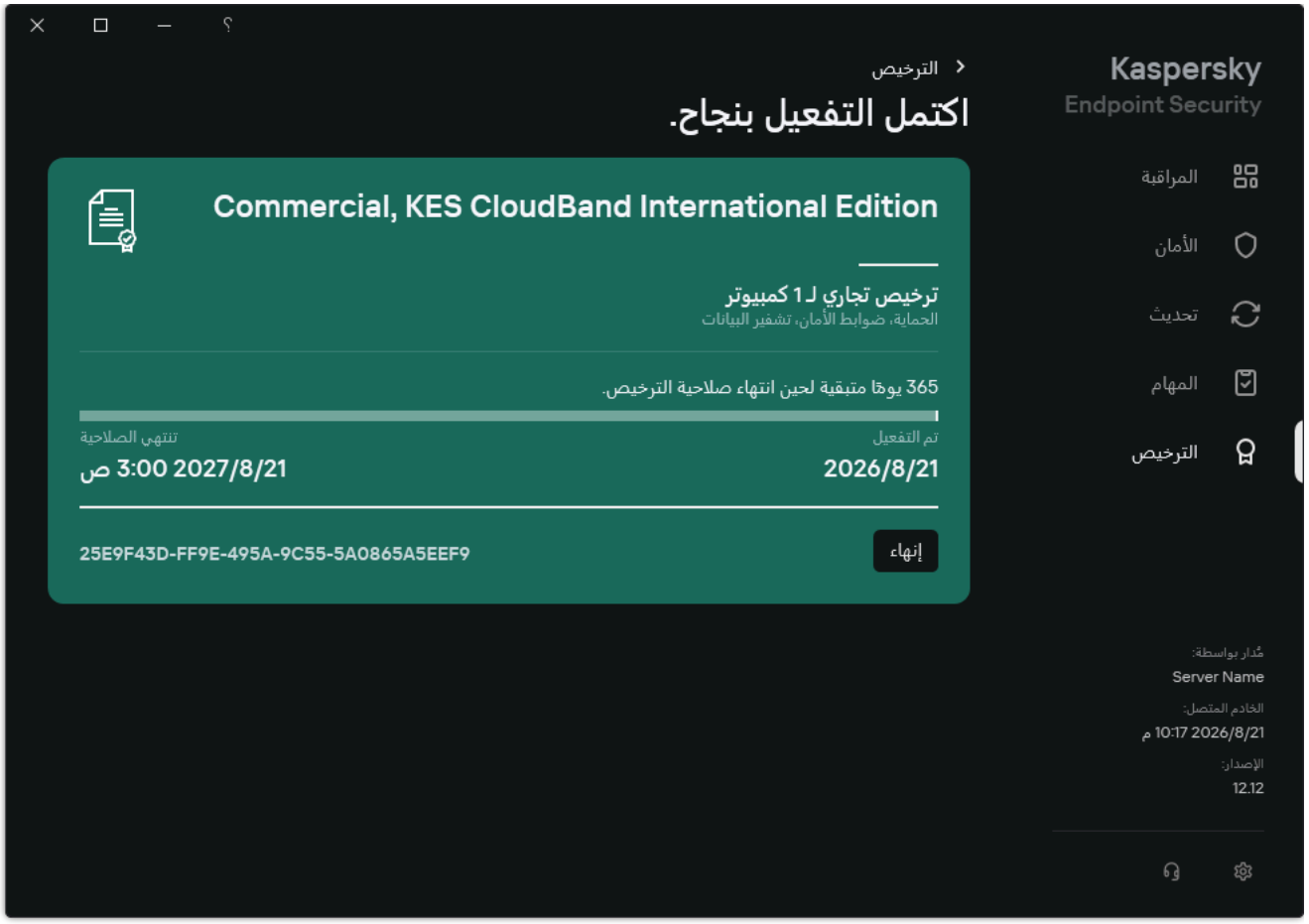
نافذة الترخيص

يمكنك أيضا إزالة مفتاح ترخيص من سطر الأوامر.

عرض معلومات الترخيص

لعرض المعلومات بشأن الترخيص:

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



نافذة الترخيص

يعرض القسم التفاصيل التالية:

- حالة المفتاح. يمكن تخزين عدة مفاتيحعلي 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 تجريبًا 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.

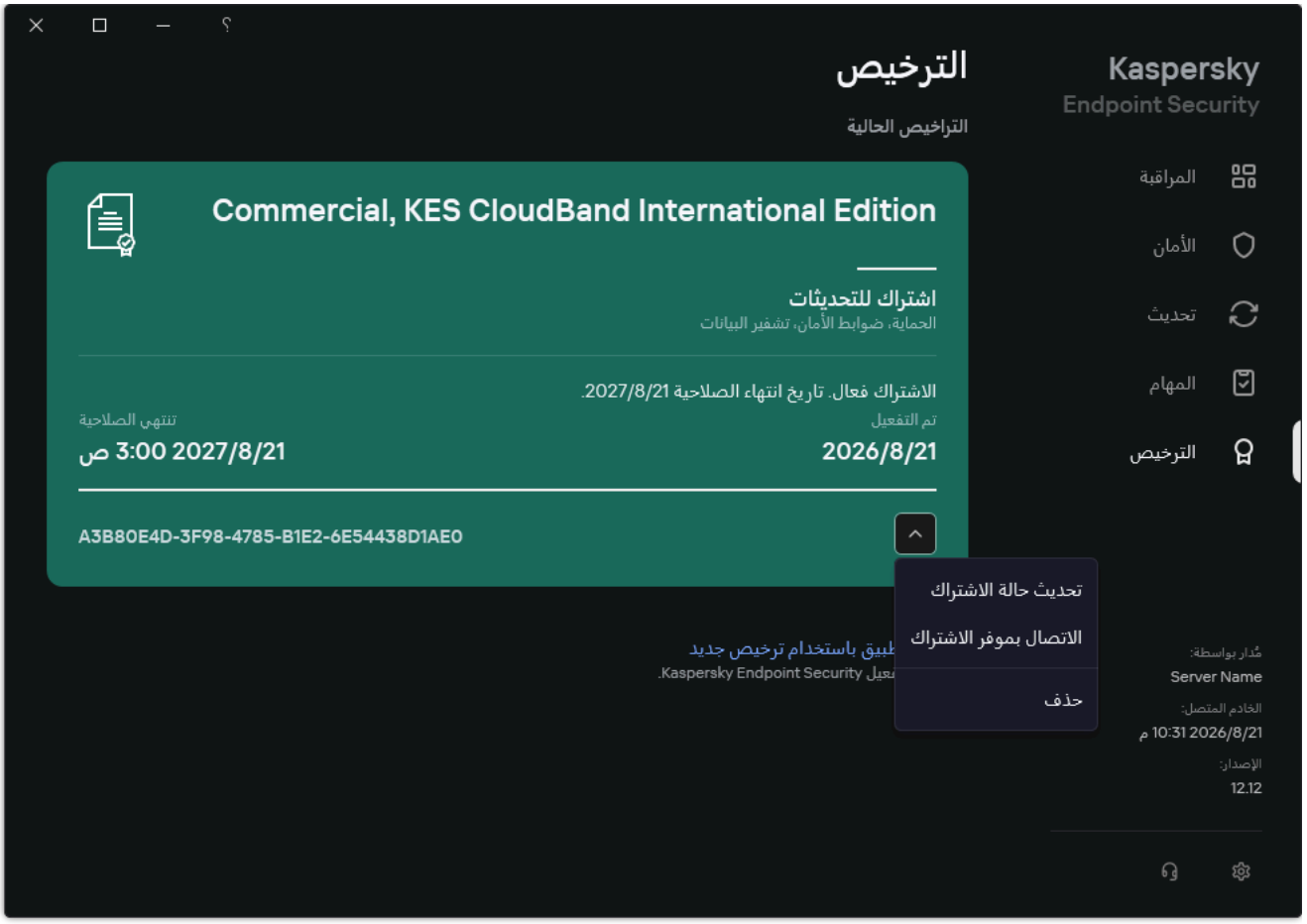
إذا كنت تستخدم التطبيق بموجب اشتراك محدود، فسوف يخطرك Kaspersky Endpoint Security في تاريخ انتهاء الاشتراك (أو في تاريخ انتهاء فترة السماح لتجديد الاشتراك)حول هذا ويتوقف عن محاولة تجديد الاشتراك تلقائيًا. في هذه الحالة، يعمل Kaspersky Endpoint Security بنفس الطريقة كما يحدث عند انتهاء صلاحية الترخيص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

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 (يشار إليه فيما يلي أيضًا باسم Web Console). هذه واجهة ويب لإدارة نظام حماية قائم على تطبيقات Kaspersky. ويمكنك العمل في Kaspersky Security Center Web Console باستخدام مستعرض على أي جهاز. 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 المكون الإضافي للويب.

إصدار مكون الإدارة الإضافي قد يختلف 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. ويجب تثبيت المكون الإضافي للويب على جهاز كمبيوتر مُثبت عليه Kaspersky Security Center Web Console . إن وظيفة المكون الإضافي للويب متوفرة لجميع المسؤولين الذين لديهم إمكانية الوصول إلى Web Console في مستعرض. ويمكنك عرض قائمة المكونات الإضافية للويب المثبتة في واجهة Web Console (**Console settings** ← **Web plug-ins**).

إذا كنت تستخدم Kaspersky Endpoint Security كجزء من حل Kaspersky Endpoint Detection and Response Optimum، فيجب عليك تثبيت المكون الإضافي لإدارة Kaspersky Endpoint Detection and Response. وتحتاج إلى المكون الإضافي للإدارة لعرض تفاصيل التنبيه. 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. وبالتالي، لإنشاء مهام الاستجابة للتهديدات، فأنت بحاجة إلى المكون الإضافي لإدارة Kaspersky Endpoint Security، ولعرض تفاصيل التنبيه، فإنك بحاجة إلى المكون الإضافي لإدارة EDR.

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 الأولي. يمكنك أيضًا 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 في 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، أضف أرشيف ZIP لحزمة التوزيع المخصصة للمكوّن الإضافي للويب في Kaspersky Endpoint Security في واجهة Web Console: **Web plug-ins** ← **Console settings**. ويمكن تنزيل حزمة توزيع المكون الإضافي للويب على موقع ويب Kaspersky على سبيل المثال.

بدءًا من Kaspersky Endpoint Security 12.11 for Windows، تم تغيير إجراء تثبيت المكون الإضافي للويب. وتتضمن حزمة التوزيع الآن مكونين إضافيين للويب: Kaspersky Endpoint Security for Windows 14.2.0 وUnified Protection and Management Plug-in. ويرجع ذلك إلى الانتقال إلى مكون إضافي للويب موحد لإدارة تطبيقات Kaspersky. ويسمح المكون الإضافي للويب الموحد بإنشاء سياسة واحدة لإدارة تطبيقات Kaspersky المتعددة (على سبيل المثال، Kaspersky Endpoint Security for Windows وmacOS وLinux). وقد يستغرق الانتقال إلى المكون الإضافي للويب الموحد عدة إصدارات. وبعد اكتمال النقل، سوف تتضمن حزمة التوزيع فقط Unified Protection and Management Plug-in.

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 (**Console settings** ← **Web plug-ins**). 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: **Console settings** ← **Web plug-ins**). 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 القيام بتحديد أرشيف ZIP لحزمة التوزيع المخصصة للمكوّن الإضافي للويب لبرنامج Kaspersky Endpoint Security في واجهة Web Console (**Console settings** ← **Web plug-ins**). ويمكن تنزيل حزمة توزيع المكون الإضافي للويب على موقع ويب Kaspersky على سبيل المثال. ويمكنك 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 (Transport Layer Security) 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 Public Key Infrastructure (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 Self-Signed Certificate. 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. • **النسخ الاحتياطي**. يمنك 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. في حال مشاركتك في Kaspersky Security Network (KSN)، فإن خدمات KSN تزود Kaspersky Endpoint Security بمعلومات عن سمعة عناوين الويب المفحوصة، بالإضافة إلى معلومات عن فئة وسمعة الملفات التي يتم فحصها. • **مراقبة نشاط التطبيقات**. يمكنك عرض معلومات حول تشغيل التطبيقات المثبتة. ويتتبع مراقب نشاط التطبيقات 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 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.

إذا كانت أيقونة التطبيق في منطقة الإخطار في شريط المهام مخفية، فهذا يعني أن المسؤول قام بتعطيل عرض واجهة التطبيق في السياسة.

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.

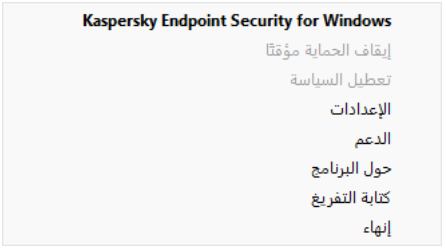
  قبل إيقاف التشغيل المؤقت لمكونات الحماية والمراقبة، يطلب التطبيق كلمة المرور الخاصة بالوصول إلى برنامج Kaspersky Endpoint Security (كلمة المرور الخاصة بالحساب أو كلمة مرور مؤقتة). يمكنك بعد ذلك تحديد فترة الإيقاف المؤقت: لمدة محددة من الوقت، أو حتى إعادة التشغيل، أو بناءً على طلب المستخدم.

  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.

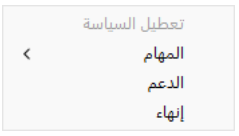


قائمة سياق رمز التطبيق

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 سلامة التطبيق**.
  - **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:

- **Simplified**. 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. ويعرض Kaspersky Endpoint Security أيضًا الإخطارات التي تتطلب إجراءً من المستخدم أعلى أيقونة التطبيق.

- **Full**. 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.

- **Do not display user 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.

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

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

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

4. في القسم **التفاعل مع المستخدم**، قم بتكوين كيفية عرض واجهة 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. إذا لزم الأمر، يمكنك تمكين وظيفة **إخفاء قسم مراقبة نشاط التطبيقات** لإخفاء البيانات عن نشاط التطبيق على الكمبيوتر، وبالتالي تقييد وصول المستخدم إلى أداة مراقبة نشاط التطبيق.

- **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. ويعرض Kaspersky Endpoint Security أيضًا الإخطارات التي تتطلب إجراءً من المستخدم أعلى أيقونة التطبيق.

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

5. احفظ تغييراتك.

كيفية تكوين وضع شاشة واجهة التطبيق في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **General Settings** ← **User Interaction**.

5. في القسم **Visibility for users**، قم بتكوين كيفية عرض واجهة التطبيق:

- **Display user interface**. إذا تم تعطيل هذه الوظيفة، فلن يتم عرض أي علامات على عملية Kaspersky Endpoint Security على كمبيوتر عميل. الرمز الموجود في منطقة إخطار Windows والإخطارات غير متاحين.

- **Simplified**. 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. ويعرض Kaspersky Endpoint Security أيضًا الإخطارات التي تتطلب إجراءً من المستخدم أعلى أيقونة التطبيق.

- **Full**. 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.

- **Hide Application Activity Monitor section**. إذا كنت تريد إخفاء معلومات نشاط التطبيق على كمبيوتر مستخدم، فيمكنك تقييد وصول المستخدم إلى أداة مراقبة نشاط التطبيق.

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

تحضير التطبيق للاستخدام

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 قواعد البيانات والوحدات النمطية للتطبيق وفحص البرامج الضارة.

مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيقمطلوبة 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 قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، 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 شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **تنظيف؛ إبلاغ إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا فشل التنظيف، يضيف Kaspersky Endpoint Security معلومات عن 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.
- **Run only when the computer is idle**. تأجيل بدء مهمة 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. يتيح لك خيار الجدولة هذا الحفاظ على موارد الكمبيوتر عند استخدام 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

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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 نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر على **Add**.
   يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.
   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 **Devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.
5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.
6. قم بإنهاء المعالج.
   سيتم عرض مهمة جديدة في قائمة المهام.

7. لتكوين جدول المهام انتقل إلى خصائص المهمة.

من المستحسن أن تكون جدولة المهمة للتشغيل مرة واحدة على الأقل في الأسبوع.

8. حدد خانة الاختيار المجاورة للمهمة.

9. انقر فوق **Start**.

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.

- تحسين أداء Kaspersky Endpoint Security.

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.

لكل إعداد سياسة سمة (قفل"). وتحدد حالة هذه السمة ما إذا كان الإعداد سيتم تمريره إلى الأجهزة المُدارة في مجموعة الإدارة أم لا:

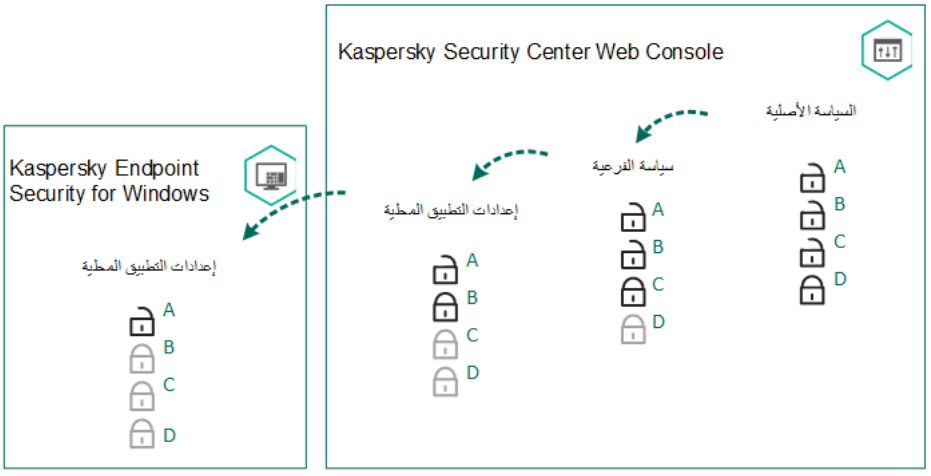
- إذا كان "القفل" مفتوحًا ()، فلن يتم تمرير قيمة هذا الإعداد إلى الأجهزة المدارة. وسيكون الإعداد متاحًا للتعديل في الواجهة المحلية للتطبيق. ويشار إلى هذه الإعدادات على أنها غير مؤمنة.
- إذا كان "القفل" مغلقًا ()، سيتم تمرير قيمة هذا الإعداد وتطبيقها على الأجهزة المدارة. يشار إلى هذه الإعدادات على أنها مؤمنة. الإعدادات الممنوعة غير متاحة للتعديل في الواجهة المحلية للتطبيق.

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.

توريث الإعدادات

السياسات، مثل مجموعات الإدارة، تكون مرتبة في تسلسل هرمي. السياسة الفرعية هي سياسة مخصصة للمستويات الهرمية المتداخلة، أي أنها سياسة مخصصة لمجموعات الإدارة المتداخلة وخوادم الإدارة الثانوية.

الوضع الافتراضي أن إعدادات السياسة الفرعية تورث من السياسة الأصلية. وإذا كان الإعداد في السياسة الرئيسية يحتوي على (قفل" مغلق)، ففي السياسات الفرعية و إعدادات التطبيق المحلي، سيتم تجاوز قيمة هذا الإعداد وفقًا للسياسة الرئيسية، وسيتم قفل الإعداد. وإذا لزم الأمر، يمكنك تعطيل توريث الإعدادات من السياسة الأصلية. 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 **Security** في نافذة خصائص خادم إدارة Kaspersky Security Center (بشكل افتراضي، يكون هذا القسم مخفيًا في واجهة وحدة التحكم).

مراجعات السياسة

يتتبع Kaspersky Security Center تعديلات السياسة وينشئ المراجعات. المراجعة هي مجموعة من المعلمات المعدلة المحفوظة بواسطة المستخدم. وتسمح لك المراجعات بمقارنة التغييرات وإعادتها إلى معلمات السياسة. وبالإضافة إلى مجموعة المعلمات المعدلة، تتضمن المراجعة معلومات عن المستخدم الذي أجرى التغييرات، بالإضافة إلى الوقت وعنوان IP وتعليق المستخدم والبيانات الأخرى ذات الصلة.

لعرض سجل المراجعة، افتح خصائص السياسة وانتقل إلى قسم **Revision history**. وللمزيد من التفاصيل عن العمل مع المراجعات، ارجع إلى تعليمات Kaspersky Security Center.

إنشاء سياسة

وعند إنشاء سياسة، يقترح المعالج الإعدادات ذات الصلة بالوضع المحدد. على سبيل المثال، بالنسبة لوضع Light Agent، يجب إضافة خادم حماية (SVM). وعند استخدام التطبيق لحماية خادم SQL، يجب إضافة استثناءات الفحص المحددة مسبقًا للتأكد من عدم التدخل في تشغيل الخادم. ويقترح المعالج إعدادات السياسة ذات الصلة بعد تحديد الوضع. ويمكنك بعد ذلك تحرير هذه الإعدادات في خصائص السياسة.

كيفية إنشاء سياسة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في مجلد **Managed devices** 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 **Policies**.

4. انقر فوق **New policy**.

بدء تشغيل معالج السياسة.

5. اتبع تعليمات "معالج السياسات".

الخطوة 1. تحديد التطبيق لإنشاء سياسة المجموعة

حدد تطبيق **Kaspersky Endpoint Security for Windows (14.2)**.

الخطوة 2. تسمية سياسة المجموعة

أدخل اسمًا لسياسة المجموعة، على سبيل المثال، السياسة الخاصة بالمكتب.

يمكنك أيضًا إنشاء سياسات جديدة بناءً على السياسات الحالية باستخدام معالج السياسة. ولفعل ذلك عند تحديد اسم سياسة مجموعة، حدد خانة الاختيار **Use policy settings for an earlier version of the application**. ويسمح المعالج أيضًا بإنشاء سياسة Kaspersky Endpoint Security (KES) بناءً على سياسة حل مختلف، على سبيل المثال، Kaspersky Security for Windows Server (KSWS) أو Kaspersky Security for Virtualization Light Agent for Windows

الخطوة 3. المشاركة في شبكة Kaspersky Security Network

يرجى قراءة شروط بيان Kaspersky Security Network (KSN) والموافقة عليها.

الخطوة 4. تحديد وضع استخدام التطبيق على أجهزة الكمبيوتر

اعتمادًا على الغرض من استخدام Kaspersky Endpoint Security، يمكنك تكوين سياسة لأوضاع التطبيق التالية:

- الوضع القياسي لحماية المضيفين

في هذا الوضع، يمكنك تحديد الطريقة التي تريد تكوين السياسة باستخدامها:

- **إنشاء سياسة بالإعدادات الافتراضية**. تعتبر الإعدادات الافتراضية هي الأمثل. ويوصي خبراء Kaspersky بهذه الإعدادات. وتوفر الإعدادات الافتراضية مستوى الحماية الموصى به والاستخدام الأمثل للموارد.
- **تغيير إعدادات السياسة في المعالج**. تتيح هذه الطريقة إدارة إعدادات السياسة خطوة بخطوة باستخدام معالج. ويمكنك أيضًا إدارة إعدادات السياسة باستخدام ملف تكوين للتطبيق (انظر الخطوة التالية).

- Endpoint Detection and Response Agent للحماية من التهديدات المتقدمة والهجمات المستهدفة.

Endpoint Detection and Response Agent هو تطبيق يتم تثبيته على محطات العمل والخوادم الفردية في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة لدعم حلول Detection and Response بواسطة Kaspersky: وفي الخطوة التالية، تحتاج إلى تحديد حل لتكامل EDR Agent.

- Light Agent لحماية البيئات الافتراضية.

لاستخدام التطبيق في وضع Light Agent، تحتاج إلى تكوين اتصال بجهاز افتراضي خاص بـ SVM. وتكون هذه الإعدادات مطلوبة لكي يعمل التطبيق في وضع Light Agent.

يوفر Kaspersky Endpoint Security سياسة مشتركة لجميع أوضاع التطبيقات وأنواع أنظمة التشغيل. وهذا يعني أن السياسة تغطي مجموعة كاملة من الإعدادات. ومع ذلك، قد يتجاهل التطبيق بعض إعدادات السياسة لأنه يتم نشر Kaspersky Endpoint Security في وضع لا تتوفر فيه بعض الوظائف. على سبيل المثال، عند استخدام التطبيق في وضع Endpoint Detection and Response Agent، تتوفر فقط الإعدادات ذات الصلة بالتكامل مع حلول Kaspersky Detection and Response والتكامل مع KUMA.

نوصي باستخدام سياسات مختلفة للأوضاع وأنواع أنظمة التشغيل المختلفة.

الخطوة 5. استيراد الإعدادات

تتوفر هذه الخطوة إذا حددت تكوين السياسة اليدوي في الخطوة 4.

يمكنك إنشاء سياسة بناءً على إعدادات Kaspersky Endpoint Security من ملف تكوين CFG. لا يدعم معالج السياسة الجديد ملفات التكوين المشفرة. وعند تصدير ملف التكوين، تخط خطوة تشفير الملف.

عند استيراد ملف تكوين CFG لتطبيق، لا تتوفر جميع إعدادات السياسة للمعالج. على سبيل المثال، ملفات تعريف السياسة مفقودة من إعدادات التطبيق. وإذا كنت ترغب في نقل جميع الإعدادات وملفات التعريف إلى السياسة، فيمكنك استيراد سياسة أخرى من ملف KLP.

عند استيراد ملف تكوين، لا ينقل Kaspersky Endpoint Security كلمات مرور حاوية التشفير. وإذا كنت تستخدم المصادقة ثنائية الاتجاه عند الاتصال بالخوادم، فستحتاج إلى تحديد كلمات مرور حاوية التشفير من البداية.

الخطوة 6 - 10. تكوين إعدادات السياسة

تتوفر هذه الخطوة إذا حددت تكوين السياسة اليدوي في الخطوة 4.

اتبع الخطوات لإدارة إعدادات السياسة.

الخطوة 11. تكوين المنطقة الموثوقة

تكوين المنطقة الموثوقة. يمكنك إضافة استثناءات الفحص محددة مسبقًا وتطبيقات موثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم. ويمكن أن تساعدك أيضًا استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في وضع Light Agent في البيئات الافتراضية في Citrix وVMware.

الخطوة 12. تحديد حالة السياسة

- **Active**. بعد إجراء المزامنة التالية، سيتم استخدام السياسة باعتبارها السياسة النشطة على جهاز الكمبيوتر.

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.

- **Inactive**. سياسة النسخ الاحتياطي. إذا لزم الأمر يمكن تحويل حالة السياسة من غير نشطة إلى نشطة.

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.

- **Out-of-office**. يتم تفعيل السياسة عندما يترك جهاز الكمبيوتر شبكة المؤسسة المحيطة.

قم بإنهاء المعالج.

كيفية إنشاء سياسة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر على **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) ثم انقر على **Next**.

5. تحديد وضع التطبيق:

- Standard mode to protect workstations and servers
- Endpoint Detection and Response Agent to protect against advanced threats and targeted attacks.

إذا حددت هذا الوضع، يمكنك إنشاء سياسة لدمج الكمبيوتر مع حلول Kaspersky Detection and Response. ويطالبك المعالج بتكوين تكامل Kaspersky Managed Detection and Response ثم Kaspersky Anti Targeted Attack Platform (EDR).

- Light Agent to protect virtual environments.

إذا حددت هذا الوضع، في الخطوة التالية، يجب عليك تكوين الاتصال بخادم الحماية (SVM). وتكون هذه الإعدادات مطلوبة لكي يعمل التطبيق في وضع Light Agent.

يوفر Kaspersky Endpoint Security سياسة مشتركة لجميع أوضاع التطبيقات وأنواع أنظمة التشغيل. وهذا يعني أن السياسة تغطي مجموعة كاملة من الإعدادات. ومع ذلك، قد يتجاهل التطبيق بعض إعدادات السياسة لأنه يتم نشر Kaspersky Endpoint Security في وضع لا تتوفر فيه بعض الوظائف. على سبيل المثال، عند استخدام التطبيق في وضع Endpoint Detection and Response Agent، تتوفر فقط الإعدادات ذات الصلة بالتكامل مع حلول Kaspersky Detection and Response والتكامل مع KUMA.

نوصي باستخدام سياسات مختلفة للأوضاع وأنواع أنظمة التشغيل المختلفة.

6. تكوين المنطقة الموثوقة. يمكنك إضافة استثناءات الفحص محددة مسبقًا وتطبيقات موثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم. ويمكن أن تساعدك أيضًا استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في وضع Light Agent في البيئات الافتراضية في Citrix وVMware.

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

- تغيير اسم السياسة.
- تحديد حالة السياسة:

- **Active**. بعد إجراء المزامنة التالية، سيتم استخدام السياسة باعتبارها السياسة النشطة على جهاز الكمبيوتر.

  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.

- **Inactive**. سياسة النسخ الاحتياطي. إذا لزم الأمر يمكن تحويل حالة السياسة من غير نشطة إلى نشطة.

  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.

- **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.

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

9. قم بإنهاء المعالج.

ونتيجة لذلك سيتم تكوين الإعدادات الخاصة بـ Kaspersky Endpoint Security 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.

تصدير واستيراد سياسة

يسمح Kaspersky Endpoint Security بتصدير سياسة بإعداداتها وملفات تعريفها إلى ملف KLP. ويمكنك بعد ذلك استخدام وظيفة تصدير / استيراد السياسة لإجراء نسخ احتياطي للسياسات أو ترحيل السياسات إلى خادم آخر، على سبيل المثال، لترحيل السياسات من Kaspersky Security Center Windows إلى Kaspersky Security Center Linux. وللتفاصيل عن إدارة السياسات، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

كيفية تصدير واستيراد سياسة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في مجلد **Managed devices** 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 **Policies**.

4. لتصدير سياسة:

a. انقر فوق السياسة التي تريد تصديرها.

b. انقر فوق رابط **Export policy to file** في الجزء الأيسر من النافذة.

c. في النافذة التي تفتح، حدد اسم ملف KLP الذي تريد تصدير السياسة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.

5. لاستيراد سياسة:

a. انقر فوق **Import policy from file**.

b. في النافذة التي تفتح، حدد سياسة KLP التي ترغب في استيرادها.

c. افتح الملف.

يضيف هذا سياسة جديدة بحالة Inactive policy.

كيفية تصدير واستيراد السياسة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

2. لتصدير سياسة:

a. حدد خانة الاختيار المجاورة للسياسة التي ترغب في تصديرها.

b. انقر فوق الزر **Export**.

c. في النافذة التي تفتح، حدد اسم ملف KLP الذي تريد تصدير السياسة إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.

3. لاستيراد سياسة:

a. انقر فوق **Import**.

b. حدد ملف سياسة KLP الذي تريد استيراده.

c. بعد معالجة السياسة بنجاح، حدد مجموعة الإدارة التي تريد تطبيق السياسة عليها.

d. انقر فوق الزر **Complete** لإنهاء استيراد السياسة.

يضيف هذا سياسة جديدة بحالة Inactive.

مؤشر مستوى الأمان

يتم عرض مؤشر مستوى الأمان في أعلى نافذة خصائص 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.
    - حماية خدمات التطبيق من الإدارة الخارجية.
  - **هام**. تتضمن هذه الفئة المكونات التالية:
    - Kaspersky Security Network.
    - الحماية من تهديدات الويب.
    - الحماية من تهديدات البريد.
    - منع اختراق المضيف.
    - الحماية بكلمة مرور.
- **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 **مكونات الحماية الموصى بها** على يسار المؤشر. وفي هذه النافذة، يمكنك تمكين أي من مكونات الحماية الموصى بها.

بعد ترقية التطبيق، قد يشير مؤشر مستوى الحماية إلى مستوى حماية أقل مما كان عليه قبل الترقية. ويحدث هذا لأن الإصدار الأحدث من التطبيق يقدم مكونات أو ميزات جديدة مهمة لأمان الكمبيوتر. وبعد ترقية التطبيق، تحتاج إلى إدارة الإعدادات الجديدة للتأكد من بقاء مستوى الحماية مرتفعًا.



مؤشر مستوى الأمان للسياسة

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 قواعد البيانات والوحدات النمطية للتطبيق**. يقوم برنامج Kaspersky Endpoint Security بتحديث قواعد البيانات والوحدات النمطية الخاصة بالتطبيق. وتعتبر مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق 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 سلامة التطبيق**. 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.

إذا كان التطبيق يعمل كجزء من حل Endpoint Detection and Response بواسطة Kaspersky، يمكنك تشغيل مهام إضافية كإجراءات استجابة للاكتشاف (responses). على سبيل المثال، يمكنك إنهاء العمليات عن بعد باستخدام المهمة إنهاء العملية.

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

إنشاء مهمة

كيفية إنشاء مهمة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. حدد المجلد **Tasks** في شجرة وحدة تحكم الإدارة.

3. انقر فوق **New task**.
   يبدأ معالج المهمة.

4. اتبع تعليمات معالج المهمة.

كيفية إنشاء مهمة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.

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

3. تكوين إعدادات المهمة:

   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

   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 **Devices to which the task will be assigned**، حدد نطاق المهمة.

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

5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

6. قم بإنهاء 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 **Start**. 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. ويمكنك أيضًا إنشاء مجموعة من الأحداث لمراقبة إكمال المهام (**Event selections** ← **Monitoring**). 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.

إدارة الوصول إلى المهام

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

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

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

5. احفظ تغييراتك.

كيفية تكوين وضع إدارة المهام في واجهة Kaspersky Endpoint Security من خلال Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **General Settings** ← **User Interaction**.

5. تحت **Permitted actions**، قم بتكوين وضع إدارة المهام (انظر الجدول أدناه).

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

المعلمة	الوصف
Access to 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. في حالة إلغاء تحديد خانة الاختيار هذه، يتم إخفاء المهام المحلية في واجهة التطبيق. 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.
View group tasks	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.
Manage group tasks	في حالة تحديد خانة الاختيار، يمكن للمستخدمين بدء وإيقاف المهام الجماعية المحددة في وحدة تحكم 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 يبدأ المسؤول المهام يدويًا في وحدة تحكم 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 مجلد **Managed devices** 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 **Devices**.
4. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.
5. من نافذة خصائص الكمبيوتر، حدد القسم **Applications**.
6. في قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر، حدد **Kaspersky Endpoint Security for Windows (14.2)** وانقر نقرًا مزدوجًا لفتح خصائص التطبيق.
7. في القسم **الإعدادات العامة**، كوّن إعدادات Kaspersky Endpoint Security وكذلك التقارير والمخزن.

   تعد الأقسام المتبقية في نافذة خصائص التطبيق قياسية بالنسبة إلى 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**.

8. احفظ تغييراتك.

كيفية تكوين التطبيق المحلي في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.
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 14.2**.
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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.

4. استخدم خانة الاختيار **بدء التطبيق عند بدء تشغيل الكمبيوتر (موصى به)** لتكوين بدء تشغيل التطبيق.

5. احفظ تغييراتك.

كيفية تكوين بدء تشغيل Kaspersky Endpoint Security في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **General Settings** ← **User Interaction**.

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 التطبيق عند بدء تشغيل الكمبيوتر (موصى به)** 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 أداة **Protection status**.

كيفية تكوين بدء أو إيقاف Kaspersky Endpoint Security في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في مجلد **Managed devices** 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 **Devices**.

4. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.

5. من نافذة خصائص الكمبيوتر، حدد القسم **Applications**.

6. في قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر، حدد **Kaspersky Endpoint Security for Windows (14.2)** وانقر نقرًا مزدوجًا لفتح خصائص التطبيق.

7. قم بأحد الإجراءات التالية:

- 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 نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.
2. انقر فوق اسم الكمبيوتر الذي تريد بدء أو إيقاف Kaspersky Endpoint Security عليه.
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 **بدء التشغيل** أو **إيقاف**.

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 حيث يوجد الملف القابل للتنفيذ klpsm.exe.
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.

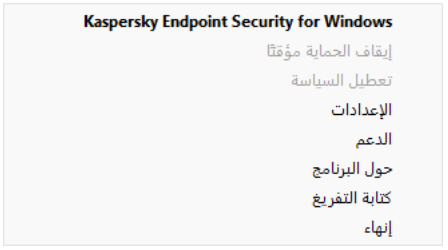
في حالة تأسيس أي من اتصالات الشبكة فعليًا عند الإيقاف المؤقت لمكون الحماية والمراقبة بجهاز الكمبيوتر واستئناف تشغيله، فسوف يظهر إخطار يشير إلى قطع هذه الاتصالات.

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.
- قم بإجراء تثبيت عن بعد لتطبيق Kaspersky Endpoint Security عبر Kaspersky Security Center باستخدام الإعدادات مسبقة التحديد.
- نقل إعدادات التطبيق إلى سياسة.
- قم بترحيل إعدادات Kaspersky Endpoint Security من جهاز كمبيوتر إلى آخر (انظر التعليمات أدناه).

تصدير ملف تكوين

بدءًا من الإصدار 14.2 من Kaspersky Endpoint Security، يمكن تشفير ملف التكوين الذي تم تصديره. ونظرًا لأن ملف التكوين قد يحتوي على بيانات اعتماد، فنحن نوصي بتشفير ملف التكوين. ولا يمكنك تحرير ملف مشفر. وستؤدي أي محاولات لتعديل ملف تكوين إلى تلفه.

يحتوي تشفير ملف التكوين على الميزات الخاصة التالية:

- يسمح Kaspersky Endpoint Security باستيراد الملفات المشفرة فقط في واجهة مستخدم التطبيق أو في سطر الأوامر. ولا يمكنك استخدام ملف مثل هذا في وحدة تحكم Kaspersky Security Center لتكوين سياسة أو تثبيت التطبيق عن بُعد. وإذا كنت تنوي إضافة الملف إلى سياسة أو حزمة تثبيت، فتخط خطوة تشفير الملف.
- لا يمكن استعادة كلمة المرور لملف مشفر.
- لا تدعم إصدارات Kaspersky Endpoint Security الأقدم من 14.1 استيراد ملفات التكوين المشفرة. وإذا كنت تنوي استيراد الملف إلى إصدار سابق من التطبيق، فتخط خطوة تشفير الملف.

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. لحفظ ملف التكوين، يجب تمكين الحماية بكلمة مرور. يجب أن يكون لدى المستخدم إذن **تصدير الإعدادات**.
5. 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.

6. إذا لزم الأمر، قم بتمكين مفتاح **تشفير الملف الذي تم تصديره** وأدخل كلمة مرور التشفير لملف التكوين.

احفظ كلمة المرور في مخزن آمن. ولا يمكن استعادة كلمة المرور هذه.

7. احفظ الملف.

نتيجة لذلك، ينشئ التطبيق ملف تكوين.

استيراد ملف تكوين

عند استيراد ملف تكوين، لا ينقل Kaspersky Endpoint Security كلمات مرور حاوية التشفير. وإذا كنت تستخدم المصادقة ثنائية الاتجاه عند الاتصال بالخوادم، فستحتاج إلى تحديد كلمات مرور حاوية التشفير من البداية.

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. إذا كان ملف التكوين مشفرًا، فأدخل كلمة المرور التي حددتها عند التصدير.

إذا نسيت كلمة مرور تشفير ملف التكوين، فلا يمكنك استرداد كلمة المرور. وفي هذه الحالة، تحتاج إلى تكرار الخطوات لتصدير ملف التكوين.

6. 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

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 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 عند فحص كمبيوتر إلى زيادة الحمل على الأنظمة الفرعية لوحدة المعالجة المركزية. 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 المتقدم. لتنظيف إصابة نشطة لخادم، قم بتمكين تقنية التنظيف المتقدم للخوادم وابدأ مهمة جماعية فحص البرامج الضارة في وقت مناسب لمستخدمي الخادم.

تمكين أو تعطيل وضع توفير الطاقة

وضع توفير الطاقة هو وظيفة تعمل على تقليل الحمل على موارد الكمبيوتر المحمول وإطالة عمر البطارية دون المساس بمستوى الأمان بشكل كبير. وفي وضع توفير الطاقة، يحد التطبيق من بدء تشغيل المهام المجدولة. وبهذه الطريقة، يضمن وضع توفير الطاقة توازنًا بين مستوى الأمان وعمر بطارية الكمبيوتر المحمول.

عند تمكين وضع توفير الطاقة وتشغيل الكمبيوتر باستخدام طاقة البطارية، لا يتم تشغيل المهام التالية حتى وإن كانت مجدولة:

- فحص كامل.
- فحص المناطق الحرجة.

- فحص مخصص.
- التحقق من سلامة التطبيق.
- فحص IOC.
- تحديث قواعد البيانات والوحدات النمطية للتطبيق (الإصلاحات فقط)

يتخطى التطبيق تحديثات قاعدة البيانات المجدولة فقط عندما يعمل الكمبيوتر المحمول على طاقة البطارية ومستوى البطارية أقل من 30% (القيمة الافتراضية). ويمكنك تغيير الحد الأدنى لمستوى شحن البطارية الذي يبدأ عنده التطبيق في تخطي تحديثات قاعدة بيانات مكافحة الفيروسات المجدولة عن طريق تحرير السجل (انظر التعليمات أدناه). وفي جميع الحالات الأخرى، يقوم Kaspersky Endpoint Security بتحديث قواعد البيانات وفقًا للجدول الزمني، بغض النظر عما إذا كان الكمبيوتر المحمول متصلاً بالتيار الكهربائي أو يعمل بطاقة البطارية، أو ما إذا كان التطبيق في وضع توفير الطاقة.

كيفية تمكين أو تعطيل وضع توفير الطاقة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.
5. في القسم **الأداء**، استخدم خانة الاختيار **تأجيل تشغيل المهام المجدولة أثناء التشغيل على طاقة البطارية** لتمكين وضع توفير الطاقة أو تعطيله.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل وضع توفير الطاقة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Performance**.
5. في القسم **Postpone or skip scheduled tasks while running on battery power**، استخدم خانة الاختيار **Postpone or skip scheduled tasks while running on battery power (depends on OS)** لتمكين وضع توفير الطاقة أو تعطيله.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل وضع توفير الطاقة 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 **الأداء**، استخدم خانة الاختيار **تأجيل تشغيل المهام المجدولة أثناء التشغيل على طاقة البطارية** لتمكين وضع توفير الطاقة أو تعطيله.

4. احفظ تغييراتك.

كيفية تغيير الحد الأدنى لمستوى الشحن الذي يبدأ التطبيق عنده بتخطي التحديثات المجدولة لقواعد بيانات مكافحة الفيروسات

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.14.2\environment]`
- لأنظمة تشغيل 32 بت:
`[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\environment]`

3. افتح `UpdaterAccumulatorThreshold` لتحريره.

4. حدد الحد الأدنى لمستوى الشحن الذي يبدأ عنده التطبيق بتخطي التحديثات المجدولة لقاعدة بيانات مكافحة الفيروسات.

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 لمنح الموارد للتطبيقات الأخرى.

كيفية تمكين أو تعطيل التنازل عن الموارد للتطبيقات الأخرى في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.
4. في القسم **الأداء**، استخدم خانة الاختيار **التنازل عن الموارد لتطبيقات أخرى** لتمكين أو تعطيل التنازل عن الموارد للتطبيقات الأخرى.
5. احفظ تغييراتك.

كيفية تمكين أو تعطيل التنازل عن الموارد للتطبيقات الأخرى في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Performance**.
5. في القسم **Yield resources to other applications**، استخدم مفتاح التبديل **Yield resources to other applications** لتمكين أو تعطيل التنازل عن الموارد لتطبيقات أخرى.
6. احفظ تغييراتك.

كيفية تمكين أو تعطيل التنازل عن الموارد للتطبيقات الأخرى 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 **الأداء**، استخدم خانة الاختيار **التنازل عن الموارد 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.
وللحصول على المزيد من المعلومات عن مشاكل أداء الكمبيوتر، يُرجى الرجوع إلى قاعدة معارف الدعم الفني.

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. فحص 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 بتعيين حد لاستهلاك موارد وحدة المعالجة المركزية أثناء فحص الكمبيوتر.

يمكنك الحد من استخدام وحدة المعالجة المركزية عند تشغيل مهمة فحص البرامج الضارة. ولفعل ذلك، في إعدادات التطبيق، حدد الحد الأقصى لنسبة تحميل وحدة المعالجة المركزية لجميع النوى التي يمكن استخدامها أثناء فحص الكمبيوتر. وقد يؤدي هذا إلى زيادة الوقت المستغرق لفحص الكمبيوتر الخاص بك.

2. 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 الكمبيوتر خارج ساعات العمل، فيمكنك تمكين وظيفة التشغيل عن بُعد عبر الشبكة المحلية. وتتيح ميزة Wake-on-LAN تشغيل الكمبيوتر عن بُعد بواسطة إرسال إشارة خاصة عبر الشبكة المحلية. ولاستخدام هذه الميزة، يجب تمكين Wake-on-LAN في إعدادات BIOS. يمكنك أيضًا إيقاف تشغيل الكمبيوتر تلقائيًا بعد انتهاء الفحص.

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.

3. حدد نطاق فحص.

حدد الكائنات التالية للفحص (الحد الأدنى لمجموعة نطاقات الفحص):

- ذاكرة Kernel
- العمليات قيد التشغيل وكائنات بدء التشغيل
- قطاعات التمهيد
- %systemroot% (لا يشمل المجلدات الفرعية)
- %systemroot%\System (لا يشمل المجلدات الفرعية)
- %systemroot%\System32 (لا يشمل المجلدات الفرعية)
- %systemroot%\System32\drivers (لا يشمل المجلدات الفرعية)
- %systemroot%\SysWOW64 (لا يشمل المجلدات الفرعية)
- %systemroot%\SysWOW64\drivers (لا يشمل المجلدات الفرعية)

4. قم بتشغيل تقنيتي iSwift وiChecker.

- تقنية iSwift.

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. 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.

5. 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.

6. قم بتعطيل التشغيل المتزامن لعدة مهام فحص.

وسوف يُدرج Kaspersky Endpoint Security مهام الفحص الجديدة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر.

فحص البرامج الضارة على الخوادم

قم بتكوين مهمة فحص البرامج الضارة وفقًا للتوصيات التالية:

1. قم بتعيين حد لاستهلاك موارد وحدة المعالجة المركزية أثناء فحص الكمبيوتر.

يمكنك الحد من استخدام وحدة المعالجة المركزية عند تشغيل مهمة فحص البرامج الضارة. ولفعل ذلك، في إعدادات التطبيق، حدد الحد الأقصى لنسبة تحميل وحدة المعالجة المركزية لجميع النوى التي يمكن استخدامها أثناء فحص الكمبيوتر. وقد يؤدي هذا إلى زيادة الوقت المستغرق لفحص الكمبيوتر الخاص بك.

2. 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.

3. قم بتشغيل تقنيتي iSwift وiChecker.

- تقنية iSwift.

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. 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.

5. قم بتعطيل التشغيل المتزامن لعدة مهام فحص.

وسوف يُدرج Kaspersky Endpoint Security مهام الفحص الجديدة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على 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. في حال مشاركتك في Kaspersky Security Network (KSN)، فإن خدمات KSN تزود Kaspersky Endpoint Security بمعلومات عن سمعة عناوين الويب المفحوصة، بالإضافة إلى معلومات عن فئة وسمعة الملفات التي يتم 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.

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 فحص كامل.

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
- محركات الأقراص الصلبة والقابلة للإزالة ومحركات الشبكة
- أي ملف محدد

فحص في الخلفية

فحص 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 سلامة التطبيق

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.

كيفية تشغيل مهمة فحص في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Tasks**.
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

1. في النافذة الرئيسية لـ Web Console، حدد **Asset management** ← **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 ⚙.

إذا لم يتم عرض مهمة الفحص، فيعني هذا أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

في واجهة التطبيق، يمكنك تكوين مهام الفحص المحلية فقط: فحص كامل وفحص المناطق الحرجة وفحص مخصص. ولا يمكن تكوين المهام الجماعية المضافة عبر Kaspersky Security Center Console في واجهة التطبيق. ولا يتم عرض الزر ⚙ للمهام الجماعية.

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**.

لتحسين أداء Kaspersky Endpoint Security أثناء فحص الكمبيوتر، يمكنك إدارة الإعدادات المتقدمة لمهمة فحص كامل والحد من استخدام موارد وحدة المعالجة المركزية.

في Kaspersky Security Center، يمكنك أيضًا استخدام مهمة فحص في الخلفية بدلاً من مهمة فحص كامل لتحسين أداء التطبيق. لن يؤثر ذلك على مستوى أمان الكمبيوتر. ولا يمكن تكوين الفحص في الخلفية.

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. وعند فحص الملفات المركبة، يفحص التطبيق الأرشيفات وحزم التوزيع والملفات بتنسيقات Office، لكنه لا يفحص الأرشيفات المحمية بكلمة مرور. وعند تعيين مستوى الأمان هذا، يستخدم التطبيق التحليل المساعد على الاكتشاف مع مستوى تفاصيل **فحص عميق**. • **مستحسن**. يفحص Kaspersky Endpoint Security كل أنواع الملفات. وعند فحص الملفات المركبة، يفحص التطبيق الأرشيفات وحزم التوزيع والملفات بتنسيقات Office، لكنه لا يفحص الأرشيفات المحمية بكلمة مرور. وعند تعيين مستوى الأمان هذا، يستخدم التطبيق التحليل المساعد على الاكتشاف مع مستوى تفاصيل **فحص متوسط**. • **منخفض**. يفحص Kaspersky Endpoint Security تنسيقات الملفات المحددة فقط. وعند فحص الملفات المركبة، يفحص التطبيق الأرشيفات وحزم التوزيع والملفات بتنسيقات Office، لكنه لا يفحص الأرشيفات المحمية بكلمة مرور. وعند تعيين مستوى الأمان هذا، يستخدم التطبيق التحليل المساعد على الاكتشاف مع مستوى تفاصيل **فحص خفيف**. 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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف. **تنظيف؛ إبلاغ إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا فشل التنظيف، يضيف Kaspersky Endpoint Security معلومات عن 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. 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.

المعلمة	الوصف
نطاق الفحص	قائمة الكائنات التي يفحصها Kaspersky Endpoint Security أثناء تنفيذ مهمة فحص. وقد تشتمل الكائنات في نطاق الفحص على ذاكرة قلب نظام التشغيل، أو العمليات قيد التشغيل، أو قطاعات التمهيد، أو مخزن النسخ الاحتياطي للنظام، أو محركات الأقراص الصلبة، أو محركات الأقراص القابلة للإزالة، أو محركات أقراص الشبكة، أو مجلد أو ملف. في Kaspersky Endpoint Security for Windows 12.12، يتم استثناء البريد الإلكتروني من نطاق فحص التطبيق. ويتم فحص رسائل البريد الإلكتروني الواردة والصادرة بواسطة مكون الحماية من تهديدات البريد. وإذا كنت تستخدم إصدارًا سابقًا من المكون الإضافي للإدارة، فإن التطبيق يستثني البريد الإلكتروني من نطاق الفحص، حتى إذا كانت السياسة تتضمنه.
جدولة الفحص	**Manually**. وضع التشغيل الذي يمكنك فيه بدء الفحص يدويًا في الوقت الذي يناسبك. **By schedule**. 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 المهمة التي تم تخطيها بمجرد أن يكون هذا ممكنًا. ويمكن تخطي المهمة، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء المهمة المجدولة. وعندما يحصل التطبيق على فرصة لتنفيذ المهام الفائتة، يقوم بتشغيل المهام بشكل عشوائي خلال فترة زمنية معينة لتوزيع الحمل على الكمبيوتر. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل المهام التي تم تخطيها. وكبديل، سيقوم بتشغيل المهمة التالية بما يتوافق مع الجدول الحالي.
التشغيل فقط عندما يكون الكمبيوتر خاملاً	تأجيل بدء مهمة 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. يتيح لك خيار الجدولة هذا الحفاظ على موارد الكمبيوتر عند استخدام الكمبيوتر.
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 الملف الذي يتم فحصه لأكثر من N من الثواني	تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.
عدم تشغيل مهام فحص متعددة في الوقت نفسه	وقم بتأجيل مهام الفحص المجدولة إذا كان هناك فحص مجدول قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص المجدولة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، قمتَ بجدولة مهام فحص لتعمل في الساعة 6:00 مساءً والساعة 8:00 مساءً. سيؤجل Kaspersky Endpoint Security مهمة الفحص الجارية في الساعة 8:00 مساءً إذا كانت مهمة الفحص المجدولة في الساعة 6:00 مساءً لا تزال قيد التشغيل. وسيقوم التطبيق بتشغيل فحص بعد اكتمال المهمة التي بدأت في الساعة 6:00 مساءً. 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 التوزيع	فحص حزم توزيع تطبيقات الجهات الخارجية.
فحص الملفات بتنسيقات Microsoft Office	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. ويفحص التطبيق الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.

المعلمة	الوصف
فحص ملفات تنسيق 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 Microsoft Outlook. وهذا يعني أن Kaspersky Endpoint Security لا يفحص ملفات Microsoft Outlook (ملفات PST وOST) في حالة تثبيت إصدار 64 بت من Microsoft 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. عند اكتشاف كائن ضار في ملفات PST أو OST، يجعله Kaspersky Endpoint Security غير ضار وفقًا للإجراء المحدد (على سبيل المثال، تنظيف الملف أو حذفه). في حال اكتشاف كائنات ضارة في ملفات عملاء بريد إلكتروني آخرين (مثل Mozilla Thunderbird) ، فلن يُنظف Kaspersky Endpoint Security أو يحذف هذه الملفات لتجنب الحذف غير المرغوب فيه لرسائل البريد الإلكتروني الخاصة بك. ويضيف Kaspersky Endpoint Security فقط معلومات عن الكائنات المكتشفة إلى قائمة التهديدات النشطة. وتحتاج إلى اتخاذ خطوات لحذف رسائل البريد الإلكتروني التي تحتوي على ملفات ضارة في المرفقات في واجهة مستخدم عميل البريد الخاص بك. إذا لم يكن حذف الرسائل التي تحتوي على كائنات خبيثة متاحًا في الوقت الحالي لأي سبب من الأسباب، يمكنك معالجة هذه التهديدات في واجهة مستخدم Kaspersky Endpoint Security عن طريق إضافة الكائنات المكتشفة إلى قائمة الاستثناءات من الفحص.
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 الملفات من عمليات 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **المهام المحلية** ← **فحص محركات الأقراص القابلة للإزالة**.

4. في القائمة المنسدلة **الإجراء عند توصيل محرك أقراص قابل للإزالة**، حدد **فحص مفصل** أو **فحص سريع**.

5. كوّن الخيارات المتقدمة لفحص محركات الأقراص القابلة للإزالة (انظر الجدول أدناه).

6. احفظ تغييراتك.

كيفية تكوين فحص محركات الأقراص القابلة للإزالة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **Host Threat Protection** ← **Removable Drives Scan**.

5. استخدم مفتاح تبديل **Removable Drives Scan ENABLED** لتمكين المكون أو تعطيله.

6. تحت القسم **Scan type**، حدد **Detailed Scan** أو **Quick Scan**.

7. كوّن الخيارات المتقدمة لفحص محركات الأقراص القابلة للإزالة (انظر الجدول أدناه).

8. 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 مهمة فحص محركات الأقراص القابلة للإزالة، فهذا يعني أن المسؤول قد حظر استخدام المهام المحلية في السياسة.

المعلمة	الوصف
Scan type	**Detailed Scan**. في حالة تحديد هذا الخيار، سيفحص Kaspersky Endpoint Security جميع الملفات عند توصيل محرك أقراص قابل 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. **Quick Scan**. في حالة تحديد هذا الخيار، بعد توصيل محرك الأقراص القابل للإزالة، يفحص Kaspersky Endpoint Securityالملفات من تنسيقات محددة فقط التي تكون أكثر عرضة للإصابة، ولا يفك ضغط الكائنات المركبة.
Maximum drive size (MB)	في حالة تحديد خانة الاختيار هذه، ينفذ Kaspersky Endpoint Security الإجراء المحدد على محركات الأقراص القابلة للإزالة ذات حجم لا يزيد عن الحد الأقصى لحجم محرك الأقراص المحدد. وإذا تجاوز حجم محرك الأقراص القابل للإزالة القيمة المكونة، يتخطى Kaspersky Endpoint Security الفحص. إذا تم إلغاء تحديد خانة الاختيار، فسوف ينفذ Kaspersky Endpoint Security الإجراء المحدد على محركات الأقراص القابلة للإزالة من أي حجم.
Hide scan progress bar	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.
Prevent users from stopping the scan	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

فحص 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **المهام المحلية** ← **فحص في الخلفية**.
4. استخدم خانة الاختيار **تمكين الفحص في الخلفية** لتمكين عمليات الفحص في الخلفية أو تعطيله.
5. احفظ تغييراتك.

كيفية تمكين الفحص في الخلفية في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Host Threat Protection** ← **File Threat Protection**.
5. تحت **Background Scan**، استخدم مفتاح التبديل **Background Scan ENABLED** لتمكين 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **المهام المحلية** ← **الفحص من قائمة السياق**.
4. تكوين الفحص من قائمة السياق (انظر الجدول أدناه).
5. احفظ تغييراتك.

كيفية تكوين الفحص من قائمة السياق في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Host Threat Protection** ← **File Threat Protection**.
5. تحت **Scan from Context Menu**، كوّن 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 قد 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. وعند فحص الملفات المركبة، يفحص التطبيق الأرشيفات وحزم التوزيع والملفات بتنسيقات Office، لكنه لا يفحص الأرشيفات المحمية بكلمة مرور. وعند تعيين مستوى الأمان هذا، يستخدم التطبيق التحليل المساعد على الاكتشاف مع مستوى تفاصيل **فحص عميق**. • **مستحسن**. يفحص Kaspersky Endpoint Security كل أنواع الملفات. وعند فحص الملفات المركبة، يفحص التطبيق الأرشيفات وحزم التوزيع والملفات بتنسيقات Office، لكنه لا يفحص الأرشيفات المحمية بكلمة مرور. وعند تعيين مستوى الأمان هذا، يستخدم التطبيق التحليل المساعد على الاكتشاف مع مستوى تفاصيل **فحص متوسط**. • **منخفض**. يفحص Kaspersky Endpoint Security تنسيقات الملفات المحددة فقط. وعند فحص الملفات المركبة، يفحص التطبيق الأرشيفات وحزم التوزيع والملفات بتنسيقات Office، لكنه لا يفحص الأرشيفات المحمية بكلمة مرور. وعند تعيين مستوى الأمان هذا، يستخدم التطبيق التحليل المساعد على الاكتشاف مع مستوى تفاصيل **فحص خفيف**.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	**تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف. **تنظيف؛ إبلاغ إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا فشل التنظيف، يضيف Kaspersky Endpoint Security معلومات عن 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.
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 الملف الذي يتم فحصه لأكثر من N من الثواني	تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.
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. ويفحص التطبيق الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
فحص ملفات تنسيق 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 Microsoft Outlook. وهذا يعني أن Kaspersky Endpoint Security لا يفحص ملفات Microsoft Outlook (ملفات PST وOST) في حالة تثبيت إصدار 64 بت من Microsoft 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. عند اكتشاف كائن ضار في ملفات PST أو OST، يجعله Kaspersky Endpoint Security غير ضار وفقًا للإجراء المحدد (على سبيل المثال، تنظيف الملف أو حذفه). في حال اكتشاف كائنات ضارة في ملفات عملاء بريد إلكتروني آخرين (مثل Mozilla Thunderbird) ، فلن يُنظف Kaspersky Endpoint Security أو يحذف هذه الملفات لتجنب الحذف غير المرغوب فيه لرسائل البريد الإلكتروني الخاصة بك. ويضيف Kaspersky Endpoint Security فقط معلومات عن الكائنات المكتشفة إلى قائمة التهديدات النشطة. وتحتاج إلى اتخاذ خطوات لحذف رسائل البريد الإلكتروني التي تحتوي على ملفات ضارة في المرفقات في واجهة مستخدم عميل البريد الخاص بك. إذا لم يكن حذف الرسائل التي تحتوي على كائنات خبيثة متاحًا في الوقت الحالي لأي سبب من الأسباب، يمكنك معالجة هذه التهديدات في واجهة مستخدم Kaspersky Endpoint Security عن طريق إضافة الكائنات المكتشفة إلى قائمة الاستثناءات من الفحص.

المعلمة	الوصف
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	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. 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).

التحقق من سلامة 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 سلامة التطبيق مُخصصة للتحقق من ملفات التطبيق. قم بتشغيل مهمة التحقق من سلامة التطبيق إذا اكتشف برنامج Kaspersky Endpoint Security كائن ضار ولكنه لم يقوم بإبطال مفعوله.

يمكنك إنشاء التحقق من سلامة التطبيق 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 شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **التحقق من سلامة التطبيق**.

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

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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 نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر على **Add**.
   يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Application Integrity Check**.

c. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، التحقق من سلامة التطبيق بعد إصابة الكمبيوتر.

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

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

5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

6. قم بإنهاء المعالج.
سيتم عرض مهمة جديدة في قائمة المهام.

7. 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 التحقق من سلامة التطبيق 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). إذا لم يتم عرض مهمة التحقق من سلامة التطبيق، فهذا يعني أن المسؤول قد 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 المهمة التي تم تخطيها بمجرد أن يكون هذا ممكنًا. ويمكن تخطي المهمة، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء المهمة المجدولة. وعندما يحصل التطبيق على فرصة لتنفيذ المهام الفائتة، يقوم بتشغيل المهام بشكل عشوائي خلال فترة زمنية معينة لتوزيع الحمل على الكمبيوتر. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل المهام التي تم تخطيها. وكبديل، سيقوم بتشغيل المهمة التالية بما يتوافق مع الجدول الحالي.
التشغيل فقط عندما يكون الكمبيوتر خاملاً	تأجيل بدء مهمة 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. يتيح لك خيار الجدولة هذا الحفاظ على موارد الكمبيوتر عند استخدام الكمبيوتر.

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:

- **ذاكرة النظام**.
- **العمليات قيد التشغيل وكائنات 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**.

في Kaspersky Endpoint Security for Windows 12.12، يتم استثناء البريد الإلكتروني من نطاق فحص التطبيق. ويتم فحص رسائل البريد الإلكتروني الواردة والصادرة بواسطة مكون الحماية من تهديدات البريد. وإذا كنت تستخدم إصدارًا سابقًا من المكون الإضافي للإدارة، فإن التطبيق يستثني البريد الإلكتروني من نطاق الفحص، حتى إذا كانت السياسة تتضمنه.

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 **Tasks**.
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\`.

يتضمن كائن **هذا الكمبيوتر** في قائمة موارد الملفات الخاصة بالكمبيوتر الكائنات التالية: **كل محركات الأقراص الثابتة** و**كل محركات أقراص الشبكة** و**جميع محركات الأقراص القابلة للإزالة**.

يمكنك استثناء كائن من عمليات الفحص دون حذفه من قائمة الكائنات في نطاق الفحص. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إنشاء نطاق الفحص في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Tasks**.

تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.

نافذة خصائص المهمة. إذا لزم الأمر، أنشئ مهمة Malware Scan.

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 على **Add**.

b. أدخل المسار إلى الملف أو المجلد.

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

قد يستغرق الفحص بحثًا عن البرامج الضارة باستخدام مهمة فحص البرامج الضارة وقتًا طويلاً وقد تزيد من استخدام Kaspersky Endpoint Security لموارد الكمبيوتر. ولذلك، يوصى بتحديد الوقت الأمثل لتشغيل المهمة بحيث يتم تقليل التأثير على أداء التطبيقات الأخرى.

على سبيل المثال، إذا كان الموظفون في مؤسستك يعملون وفقًا لجدول زمني ثابت، يمكنك تكوين فحص الكمبيوتر بحيث يعمل ليلاً أو في عطلات نهاية الأسبوع. إذا استحال تشغيل مهمة لأي سبب (على سبيل المثال: عدم تشغيل الكمبيوتر في ذلك الوقت)، يمكنك تكوين المهمة التي تم تخطيها لتبدأ تلقائيًا في أقرب وقت ممكن. ويجب استخدام هذه الوظيفة بحذر، حيث إنها قد تبطئ التطبيقات على كمبيوتر المستخدم عند تشغيل الكمبيوتر في الصباح.

إذا لم تتمكن من تحديد جدول فحص مثالي يناسب احتياجاتك، فيمكنك تكوين الفحص ليتم تشغيله عند استيفاء أحد 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 بعد انقضاء فترة زمنية محددة تلي 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.

- ميزة Wake-on-LAN.

يُجري Kaspersky Endpoint Security فحصًا للكمبيوتر وفقًا للجدولة حتى في حالة إيقاف تشغيل الكمبيوتر. ولفعل ذلك، يستخدم التطبيق ميزة Wake-on-LAN في نظام التشغيل. وتتيح ميزة Wake-on-LAN تشغيل الكمبيوتر عن بُعد بواسطة إرسال إشارة خاصة عبر الشبكة المحلية. ولاستخدام هذه الميزة، يجب تمكين Wake-on-LAN في إعدادات BIOS.

يمكنك تكوين تشغيل الفحص باستخدام Wake-on-LAN فقط لمهمة فحص البرامج الضارة في Kaspersky Security Center. ولا يمكنك تمكين Wake-on-LAN 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. وفي هذه الحالة، قد يستغرق الفحص الكامل عدة أيام حتى يكتمل.

- عندما تم تخطي المهمة.

يقوم Kaspersky Endpoint Security بتشغيل المهمة التي تم تخطيها في أقرب وقت ممكن. ويمكن تخطي المهمة، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء المهمة المجدولة. وعندما يحصل التطبيق على فرصة لتنفيذ المهام الفائتة، يقوم بتشغيل المهام بشكل عشوائي خلال فترة زمنية معينة لتوزيع الحمل على الكمبيوتر.

كيفية تكوين جدولة الفحص في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.

نافذة خصائص المهمة.

3. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

4. تكوين جدول مهمة الفحص.

5. بناءً على التكرار الذي تم تحديده، كوّن 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، كوّن الإعدادات المتقدمة التي تحدد جدول تشغيل المهمة (انظر الجدول أدناه).

6. احفظ تغييراتك.

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 المهمة التي تم تخطيها بمجرد أن يكون هذا ممكنًا. ويمكن تخطي المهمة، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء المهمة المجدولة. وعندما يحصل التطبيق على فرصة لتنفيذ المهام الفائتة، يقوم بتشغيل المهام بشكل عشوائي خلال فترة زمنية معينة لتوزيع الحمل على الكمبيوتر. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل المهام التي تم تخطيها. وكبديل، سيقوم بتشغيل المهمة التالية بما يتوافق مع الجدول الحالي.
التشغيل فقط عندما يكون الكمبيوتر خاملاً	تأجيل بدء مهمة 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. يتيح لك خيار الجدولة هذا الحفاظ على موارد الكمبيوتر عند استخدام الكمبيوتر.
Use automatically randomized delay for task starts (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.
Use randomized delay for task starts within an interval of (min)	في حالة تحديد خانة الاختيار هذه، يتم تشغيل المهمة على أجهزة الكمبيوتر في وقت عشوائي ضمن إطار زمني معين. وتساعد أوقات البدء العشوائية في تجنب وصول عدد كبير من أجهزة الكمبيوتر إلى خادم الإدارة في الوقت نفسه عند تشغيل المهمة في الموعد المحدد. في حالة إلغاء تحديد خانة الاختيار، يتم تشغيل المهمة بالضبط في الوقت المجدول.
Stop the task if it runs longer than (min) (متوفر فقط في Kaspersky Security Center Console)	تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.
Turn on devices by using the Wake-on-LAN function before starting the task (min) (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.
Shut down the devices after completing the task (متوفر فقط في Kaspersky Security Center Console)	في حالة تحديد خانة الاختيار هذه، سيتم إيقاف تشغيل الكمبيوتر بعد اكتمال المهمة. على سبيل المثال، يمكنك تمكين هذه الوظيفة لفحص الكمبيوتر في أيام الجمعة بعد ساعات العمل. وعند انتهاء المهمة، يوقف التطبيق تشغيل الكمبيوتر لعطلة نهاية الأسبوع.
إيقاف المهمة مؤقتًا	يمكنك تحديد فترة زمنية سيتم خلالها إيقاف تنفيذ مهمة مجدولة مسبقًا مؤقتًا. وبمجرد انتهاء الفترة الزمنية المحددة، سيتم استئناف المهمة. وقد يكون ذلك ضروريًا، على سبيل المثال ، لتقليل تأثير Kaspersky Endpoint Security على أداء الكمبيوتر أثناء فترات ذروة الاستخدام.
تعطيل الجدولة من	إذا تم تحديد خانة الاختيار، فسيتوقف Kaspersky Endpoint Security عن تشغيل المهمة المجدولة بدءًا من التاريخ المحدد. وسيتم تعيين المهمة على وضع **يدويًا**.

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 **Managed devices** 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 **Tasks**.
4. حدد مهمة الفحص وانقر نقرًا مزدوجًا لفتح خصائص المهمة.
5. من نافذة خصائص المهمة، حدد القسم **Account**.
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 نافذة Web Console الرئيسية، حدد **Tasks** ← **Asset management**.
   تفتح قائمة المهام.
2. انقر فوق مهمة الفحص.
   نافذة خصائص المهمة.
3. حدد علامة التبويب **Settings**.
4. في القسم **Account**، انقر فوق الزر **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

الحد من استخدام وحدة المعالجة المركزية أثناء فحص الكمبيوتر

يمكنك الحد من استخدام وحدة المعالجة المركزية عند تشغيل مهمة فحص البرامج الضارة. وقد يؤدي هذا إلى زيادة الوقت المستغرق لفحص الكمبيوتر الخاص بك.

كيفية الحد من استخدام وحدة المعالجة المركزية عند فحص الكمبيوتر في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.
4. تحت **الأداء**، حدد خانة الاختيار **تقييد استخدام وحدة المعالجة المركزية لمهام الفحص** وأدخل متوسط قيمة استهلاك موارد وحدة المعالجة المركزية بالنسبة المئوية.
5. احفظ تغييراتك.

كيفية الحد من استخدام وحدة المعالجة المركزية عند فحص الكمبيوتر في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Performance**.
5. تحت **Limit CPU usage for scan tasks**، اضبط مفتاح التبديل على **Limit CPU usage for scan tasks** وأدخل متوسط قيمة استهلاك موارد وحدة المعالجة المركزية بالنسبة المئوية.
6. احفظ تغييراتك.

كيفية الحد من استخدام وحدة المعالجة المركزية عند فحص الكمبيوتر 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. تحت **الأداء**، حدد خانة الاختيار **تقييد استخدام وحدة المعالجة المركزية لمهام الفحص** وأدخل متوسط قيمة استهلاك موارد وحدة المعالجة المركزية بالنسبة المئوية.

4. احفظ تغييراتك.

تكوين إعدادات المهام المتقدمة لمهمة فحص البرامج الضارة

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 وiSwift 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 **Tasks**.

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 **التحسين**، 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**. تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.

- **عدم تشغيل مهام فحص متعددة في الوقت نفسه**. وقم بتأجيل مهام الفحص المجدولة إذا كان هناك فحص مجدول قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص المجدولة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، قمتَ بجدولة مهام فحص لتعمل في الساعة 6:00 مساءً والساعة 8:00 مساءً. سيؤجل Kaspersky Endpoint Security مهمة الفحص الجارية في الساعة 8:00 مساءً إذا كانت مهمة الفحص المجدولة في الساعة 6:00 مساءً لا تزال قيد التشغيل. وسيقوم التطبيق بتشغيل فحص بعد اكتمال المهمة التي بدأت في الساعة 6:00 مساءً.

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**. تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.

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. انتقل إلى 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 الملفات من عمليات 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

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

   تفتح قائمة المهام.

2. انقر فوق مهمة الفحص.

   نافذة خصائص المهمة. إذا لزم الأمر، أنشئ مهمة Malware Scan.

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**. تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.

   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**. وقم بتأجيل مهام الفحص المجدولة إذا كان هناك فحص مجدول قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص المجدولة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، قمتَ بجدولة مهام فحص لتعمل في الساعة 6:00 مساءً والساعة 8:00 مساءً. سيؤجل Kaspersky Endpoint Security مهمة الفحص الجارية في الساعة 8:00 مساءً إذا كانت مهمة الفحص المجدولة في الساعة 6:00 مساءً لا تزال قيد التشغيل. وسيقوم التطبيق بتشغيل فحص بعد اكتمال المهمة التي بدأت في الساعة 6:00 مساءً.

7. في القسم **Advanced settings**، حدد خانة الاختيار **Skip file that is scanned for longer than (sec)**. تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.

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 **التحسين**، 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 الملف الذي يتم فحصه لأكثر من N من الثواني**. تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.

- **عدم تشغيل مهام فحص متعددة في الوقت نفسه**. وقم بتأجيل مهام الفحص المجدولة إذا كان هناك فحص مجدول قيد التشغيل بالفعل. وسوف يُدرج Kaspersky Endpoint Security مهام الفحص المجدولة في قائمة الانتظار إذا استمر الفحص الحالي. ويساعد هذا في تحسين الحمل على الكمبيوتر. على سبيل المثال، قمتَ بجدولة مهام فحص لتعمل في الساعة 6:00 مساءً والساعة 8:00 مساءً. سيؤجل Kaspersky Endpoint Security مهمة الفحص الجارية في الساعة 8:00 مساءً إذا كانت مهمة الفحص المجدولة في الساعة 6:00 مساءً لا تزال قيد التشغيل. وسيقوم التطبيق بتشغيل فحص بعد اكتمال المهمة التي بدأت في الساعة 6:00 مساءً.

5. في القسم **حد الحجم**، حدد خانة الاختيار **عدم فك ضغط الملفات المركبة كبيرة الحجم**. تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.

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 الملفات من عمليات 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.

قد لا تكون وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية) متاحة في التطبيق في الولايات المتحدة.

تحتاج التحديثات المنتظمة ترخيص ساريًا. في حالة عدم وجود ترخيص موجود، سيكون بإمكانك إجراء تحديث لمرة واحدة فقط.

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.

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.

إذا كان التطبيق يعمل في وضع Light Agent، يتم تضمين اعتبارات خاصة في تحديث قواعد بيانات التطبيق والوحدات النمطية.

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.

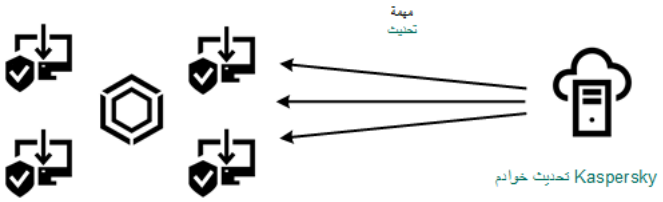
تم تحديث الكائنات التالية على أجهزة الكمبيوتر الخاصة بالمستخدمين:

- 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 Download updates to the Administration Server repository.

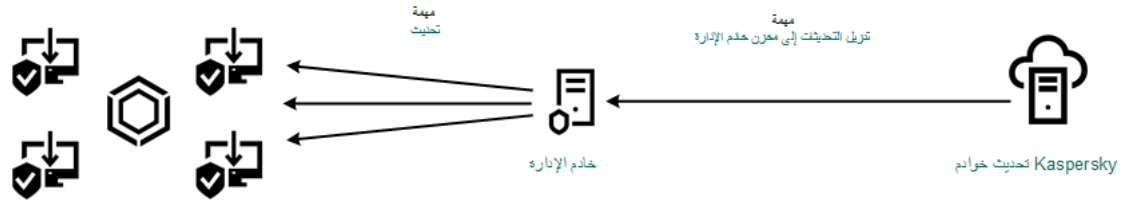
2. قم بتنزيل حزمة التحديث إلى مجلد مشترك (اختياري).

   يمكنك تنزيل حزمة التحديث إلى مجلد مشترك باستخدام الطرق التالية:

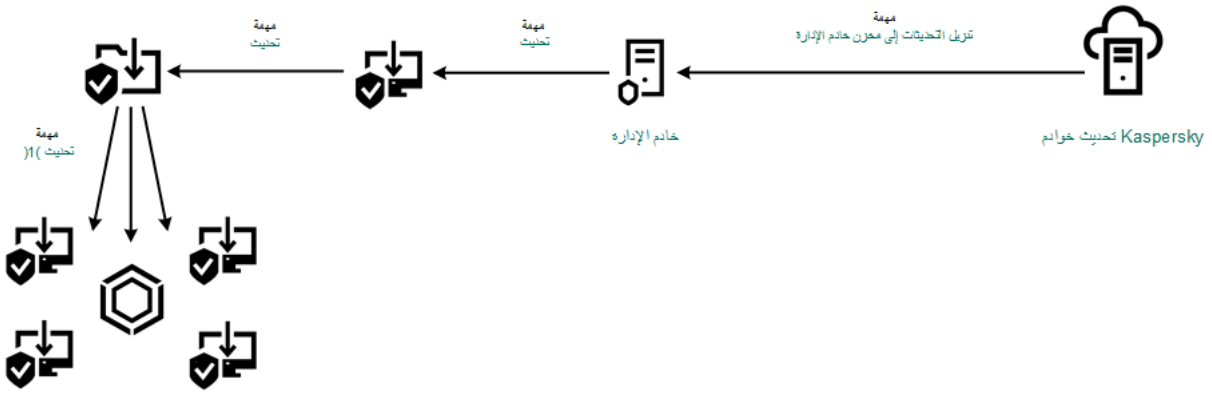
- استخدام مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق الخاصة ببرنامج Kaspersky Endpoint Security. المهمة مخصصة لأحد أجهزة الكمبيوتر الموجود في شبكة الشركة المحلية.
- باستخدام الأداة المساعدة Kaspersky Update Utility. للحصول على معلومات تفصيلية حول استخدام Kaspersky Update Utility، يُرجى الرجوع إلى قاعدة معارف Kaspersky.

3. قم بتوزيع حزمة التحديث على أجهزة الكمبيوتر العميلة.

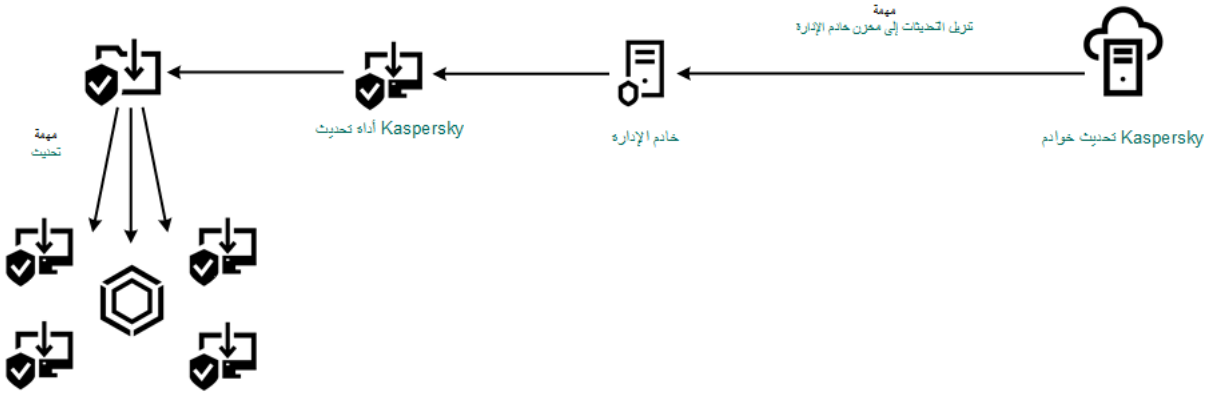
يتم توزيع حزمة التحديث على أجهزة الكمبيوتر العميلة بواسطة مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق الخاصة ببرنامج Kaspersky Endpoint Security. يمكنك إنشاء عدد غير محدود من مهام التحديث لكل مجموعة إدارة.



التحديث من مستودع الخادم



التحديث من مجلد مشترك



التحديث باستخدام برنامج Kaspersky Update Utility

بالنسبة إلى Kaspersky Security Center، تتضمن القائمة الافتراضية لمصادر التحديث خادم إدارة Kaspersky Security Center وخوادم التحديث من 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 Download updates to the Administration Server repository).

   يتم إنشاء مهمة Download updates to the Administration Server repository 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 قواعد البيانات والوحدات النمطية للتطبيق).

كيفية تكوين تحديث Kaspersky Endpoint Security من مخزن الخادم المحدد في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

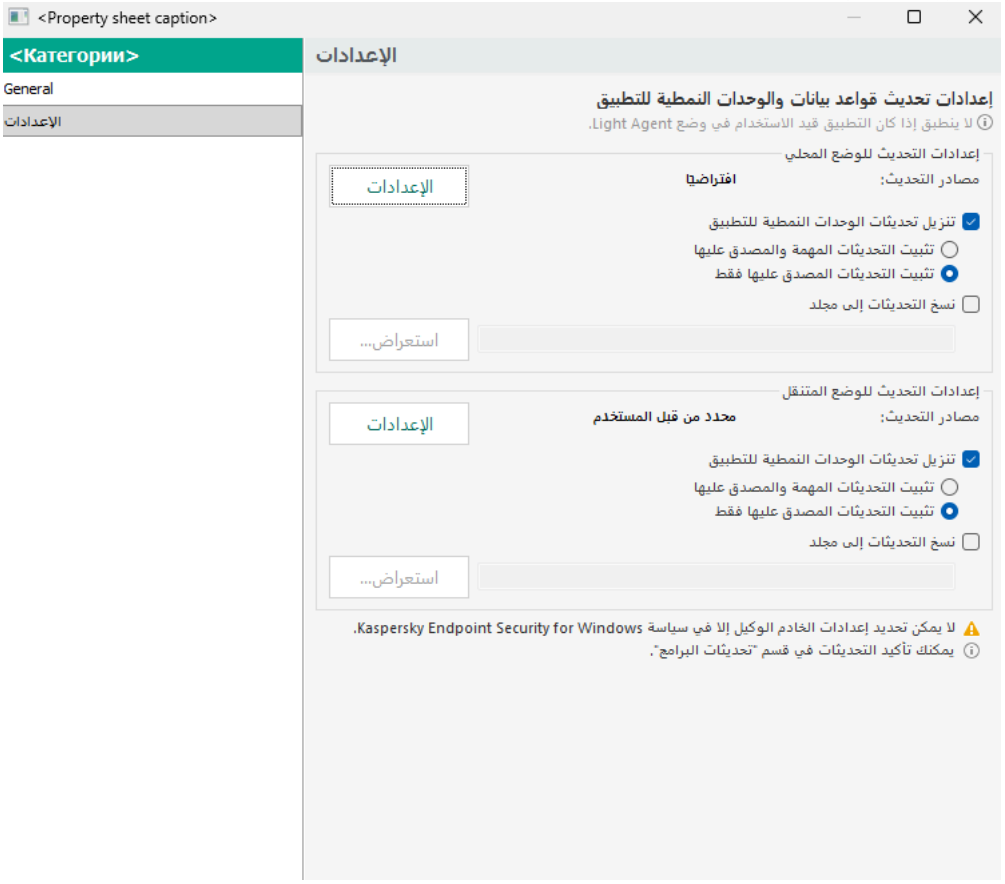
   في شجرة وحدة التحكم، حدد **Tasks**.

2. انقر فوق المهمة **تحديث قواعد البيانات والوحدات النمطية للتطبيق** في برنامج Kaspersky Endpoint Security.

   نافذة خصائص المهمة.

   يتم إنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. من نافذة خصائص المهام، حدد القسم **الإعدادات**.



إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق

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:

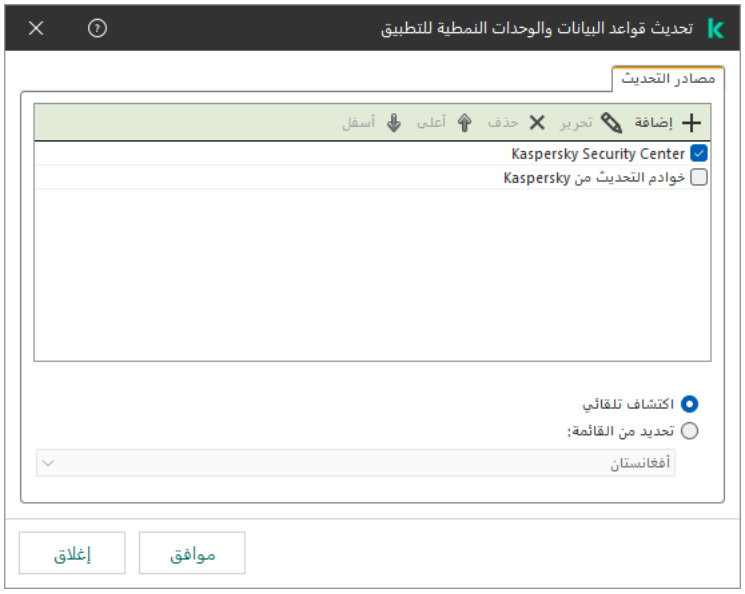
a. في قائمة مصادر التحديث انقر فوق الزر **إضافة**.

b. في الحقل **مصادر التحديث**، 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 Download updates to the Administration Server repository).

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 **Schedule** 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 نافذة Web Console الرئيسية، حدد **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 **Application settings** ← علامة التبويب **Local mode**.

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:

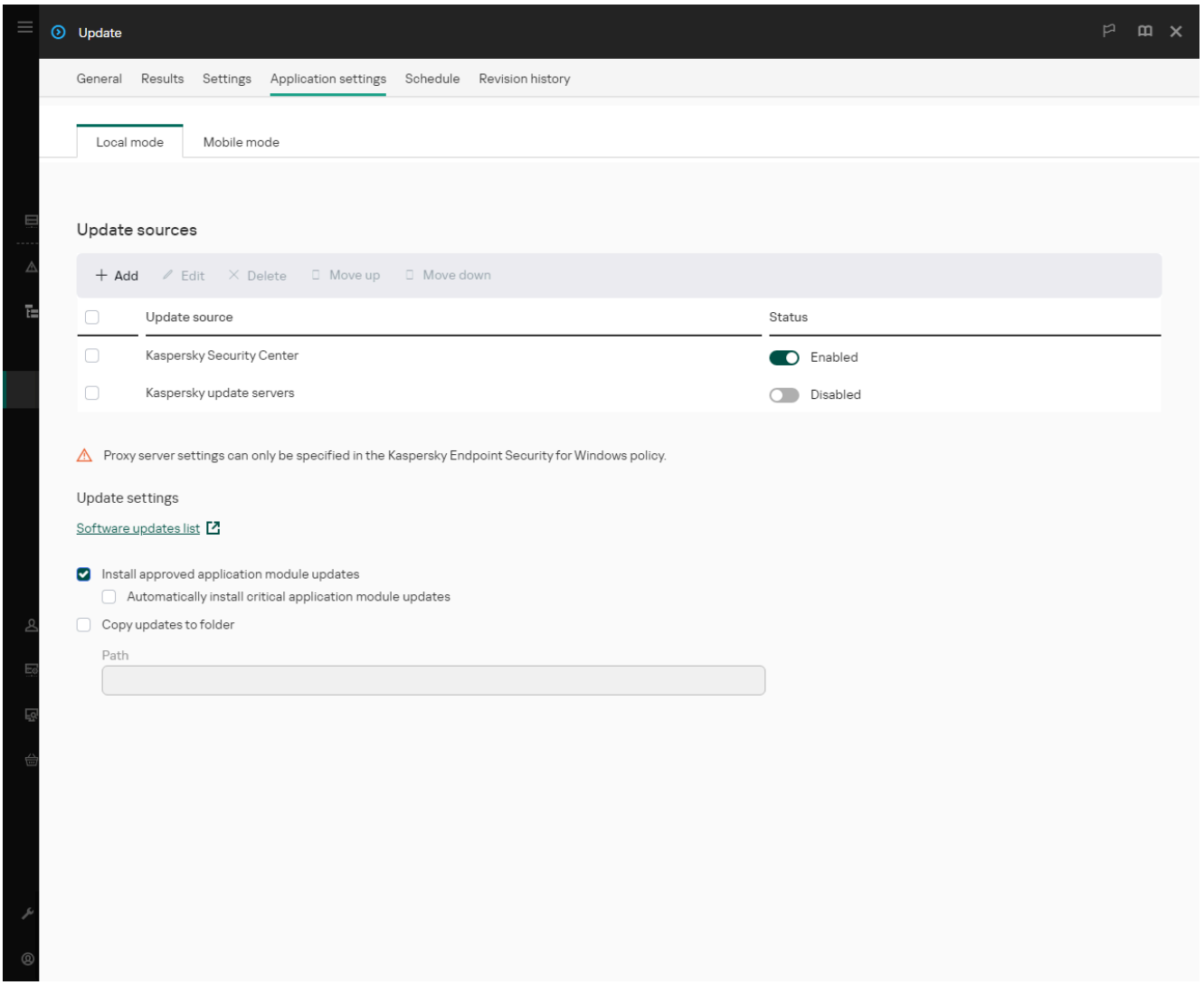
a. في قائمة مصادر التحديث انقر فوق الزر **Add**.

b. في الحقل **Update sources**، 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 Download updates to the Administration Server repository).

c. انقر على **Save**.

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 **Move up** و**Move 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.

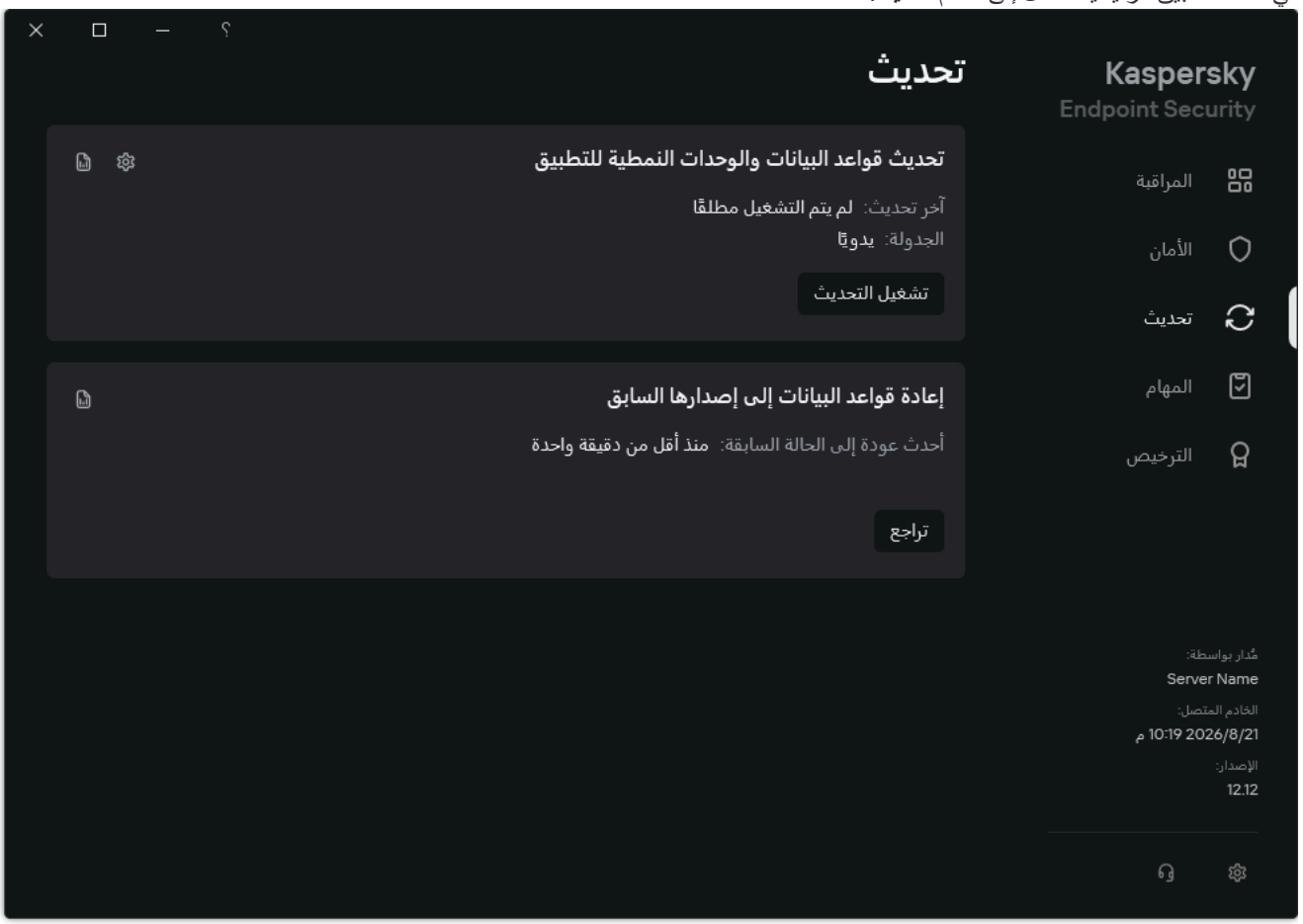
8. بشكل افتراضي، يقوم Kaspersky Endpoint Security بتشغيل المهمة في الوضع اليدوي.

9. احفظ تغييراتك.

كيفية تكوين تحديث Kaspersky Endpoint Security من مخزن الخادم المحدد في واجهة التطبيق

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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 **Folder for storing updates** عندما قمت بتكوين تنزيل التحديثات إلى مخزن الخادم (مهمة Download updates to the Administration Server repository).

b. انقر على **تحديد**.

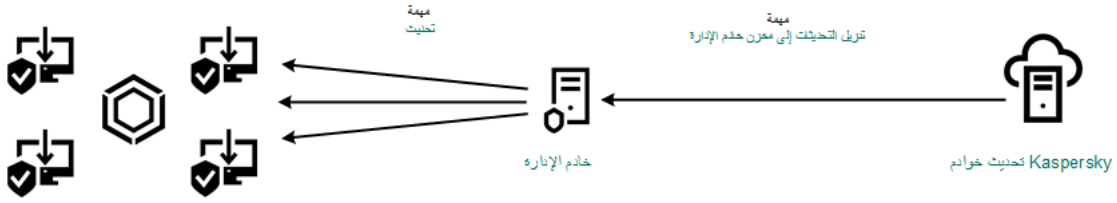
يمكنك استثناء مصدر التحديث دون إزالته من قائمة مصادر التحديث. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.

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.

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.

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 التحديث إلى أحد المجلدات المشتركة في أحد أجهزة الكمبيوتر في الشبكة المحلية.

كيفية تمكين نسخ حزمة التحديث إلى المجلد المشترك في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Tasks**.

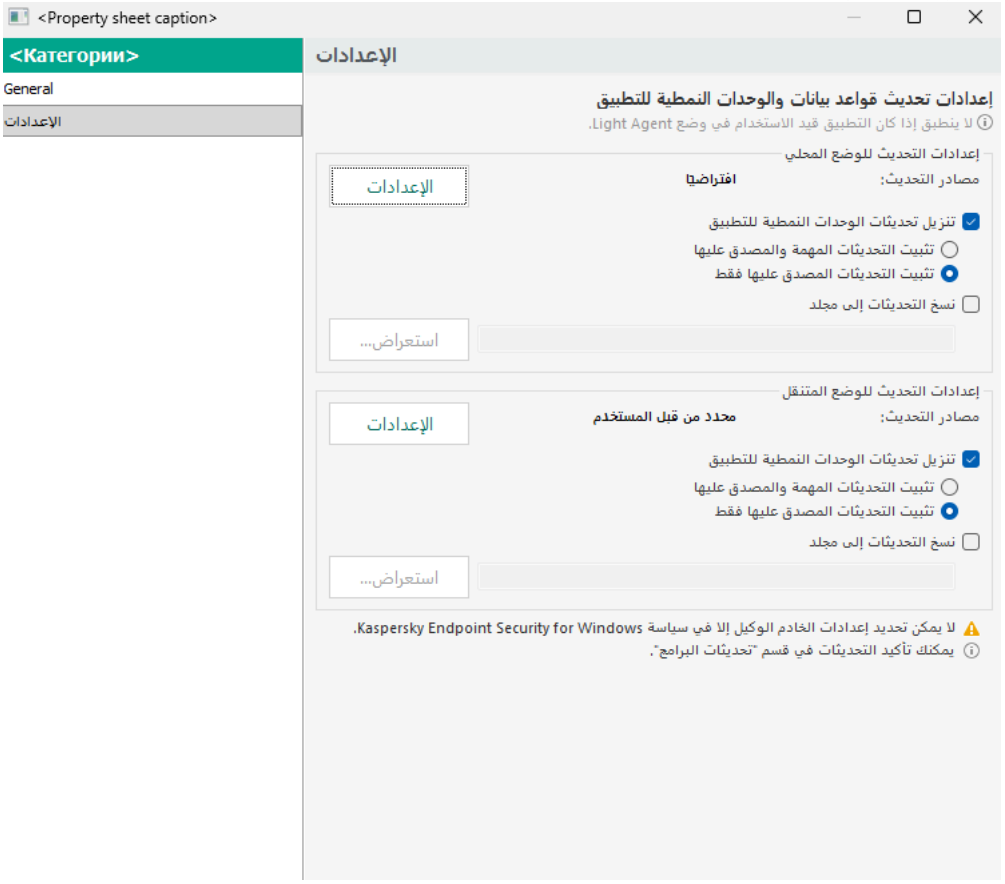
يجب تعيين مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيقلجهاز كمبيوتر واحد سيعمل كمصدر للتحديثات.

3. انقر فوق المهمة **تحديث قواعد البيانات والوحدات النمطية للتطبيق** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.



إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق

5. في القسم **إعدادات التحديث للوضع المحلي**، انقر على الزر **الإعدادات**.

6. 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.

7. حدد خانة الاختيار **نسخ التحديثات إلى مجلد**.

8. في الحقل **مسار المجلد**، أدخل مسار UNC للمجلد المشترك (على سبيل المثال، `\\<server name>\KLSHARE\Updates`).

إذا تُرك الحقل فارغًا، سينسخ Kaspersky Endpoint Security حزمة التحديث إلى المجلد `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

9. احفظ تغييراتك.

كيفية تمكين نسخ حزمة التحديث إلى المجلد المشترك في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.

تفتح قائمة المهام.

يجب تعيين مهمة Updateلجهاز 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 **Application settings** ← علامة التبويب **Local mode**.

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 (على سبيل المثال، `\\<server name>\KLSHARE\Updates`).

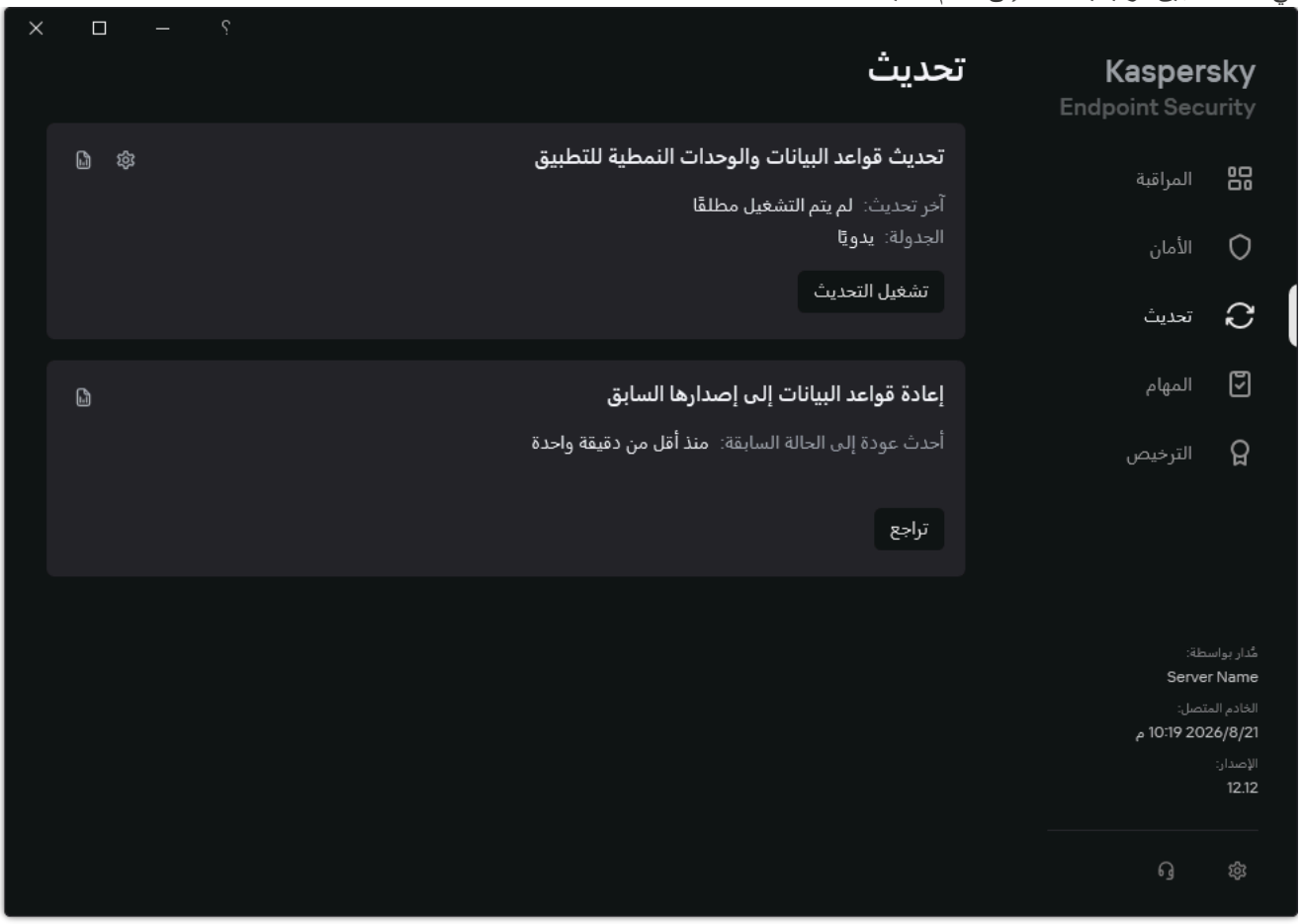
إذا تُرك الحقل فارغًا، سينسخ Kaspersky Endpoint Security حزمة التحديث إلى المجلد `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`.

7. احفظ تغييراتك.

كيفية تمكين نسخ حزمة التحديث إلى المجلد المشترك في واجهة التطبيق

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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 القسم **توزيع التحديثات**، حدد خانة الاختيار **نسخ التحديثات إلى مجلد**.

4. أدخل مسار UNC للمجلد المشترك (على سبيل المثال، `\\<server name>\KLSHARE\Updates`).

5. احفظ تغييراتك.

3. قم بتكوين تحديثات قاعدة البيانات والتطبيق من المجلد المشترك المحدد إلى أجهزة الكمبيوتر الباقية على الشبكة المحلية الخاصة بالمؤسسة .

كيفية تكوين التحديثات من المجلد المشترك في وحدة تحكم الإدارة (MMC)

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

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

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **تحديث قواعد البيانات والوحدات النمطية للتطبيق**.

4. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
تفتح قائمة المهام.

5. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **تحديث قواعد البيانات والوحدات النمطية للتطبيق**.

الخطوة 2. تحديد مصادر التحديث

إضافة مصدر تحديث جديد: مجلد مشترك. يجب أن يطابق عنوان المصدر العنوان الذي حددته في الحقل **مسار المجلد** عندما تكوّن نسخ حزمة التحديث إلى المجلد المشترك. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

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.

يجب تعيين مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق على أجهزة الكمبيوتر الخاصة بالشبكة المحلية (LAN) الخاصة بالمؤسسة، باستثناء الكمبيوتر الذي يعمل كمصدر للتحديث.

الخطوة الرابعة: اختيار الحساب لتشغيل المهمة

حدد حسابًا لتشغيل مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

الخطوة الخامسة: تكوين جدول بدء المهمة

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

الخطوة السادسة: تحديد اسم المهمة

أدخل اسم المهمة، مثل التحديث من مجلد مشترك.

الخطوة 7 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة. ونتيجة لذلك، سيتم تنفيذ مهمة الفحص على أجهزة كمبيوتر المستخدمين وفقًا للجدولة المحددة.

كيفية تكوين التحديثات من المجلد المشترك في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر على **Add**.
   يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Update**.

c. في الحقل **Task name** أدخل وصفًا موجزًا، على سبيل المثال، تحديث من مجلد مشترك.

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

يجب تعيين مهمة Update 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. قم بإنهاء المعالج.

سيتم عرض مهمة جديدة في جدول المهام.

6. انقر فوق المهمة التي تم انشاؤها حديثًا Update.

نافذة خصائص المهمة.

7. حدد **Application settings** ← علامة التبويب Local mode.

8. في القسم **Update sources**، انقر على الزر **Add**.

9. في النافذة التي تفتح، 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).

10. انقر على **OK**.

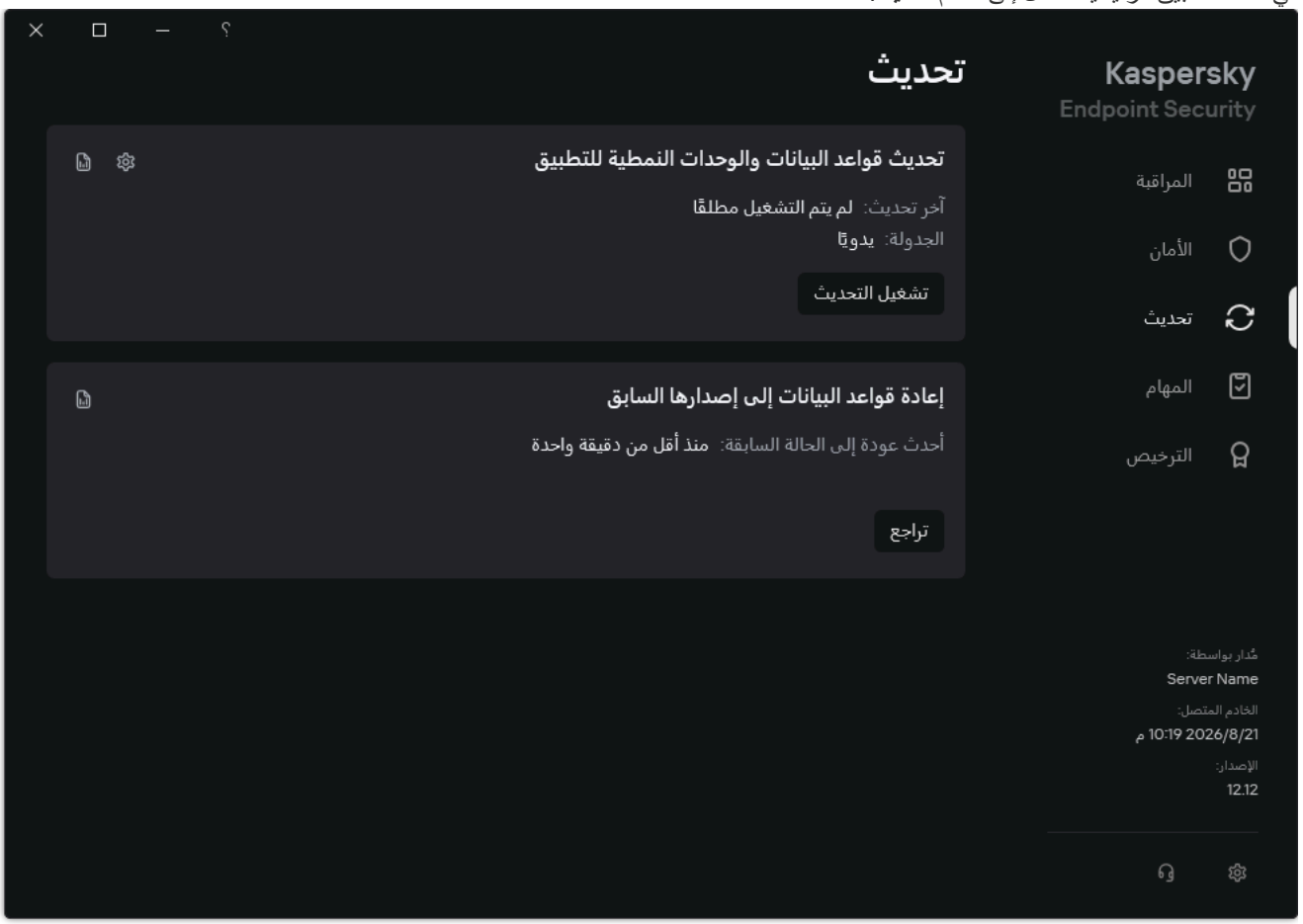
11. قم بتكوين أولويات مصادر التحديث باستخدام الزر **Move up** و**Move down**.

12. احفظ تغييراتك.

كيفية تكوين التحديثات من المجلد المشترك في واجهة التطبيق

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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. انقر على **تحديد مصادر التحديث**.

4. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

5. في النافذة التي تفتح، أدخل المسار المؤدي إلى المجلد المشترك.

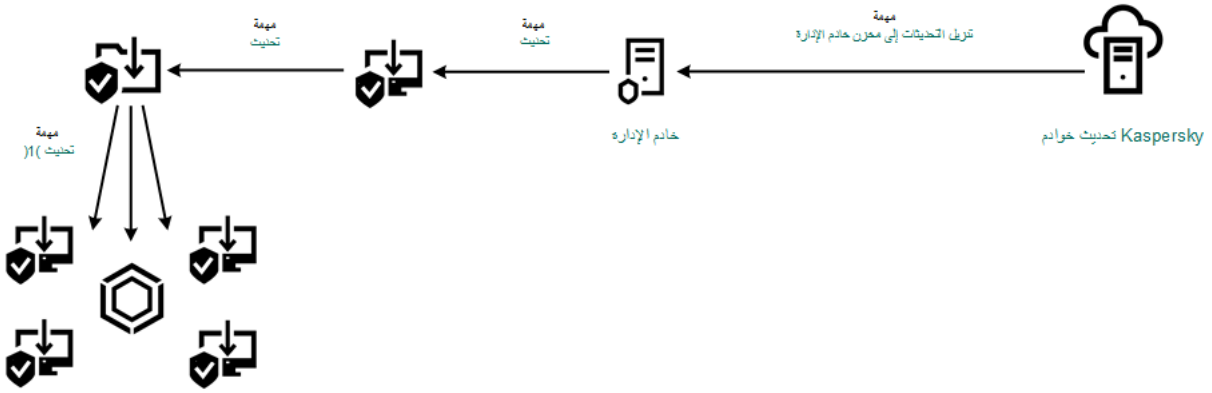
يجب أن يطابق عنوان المصدر العنوان الذي حددته عند قيامك بتكوين نسخ حزمة التحديث إلى المجلد المشترك (راجع الإرشادات أعلاه).

6. انقر على **تحديد**.

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. احفظ تغييراتك.



التحديث من مجلد مشترك

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.

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.

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.

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.

4. قم بتكوين تحديثات قاعدة البيانات والتطبيق من المجلد المشترك المحدد إلى أجهزة الكمبيوتر الباقية على الشبكة المحلية الخاصة بالمؤسسة .

كيفية تكوين التحديثات من المجلد المشترك في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

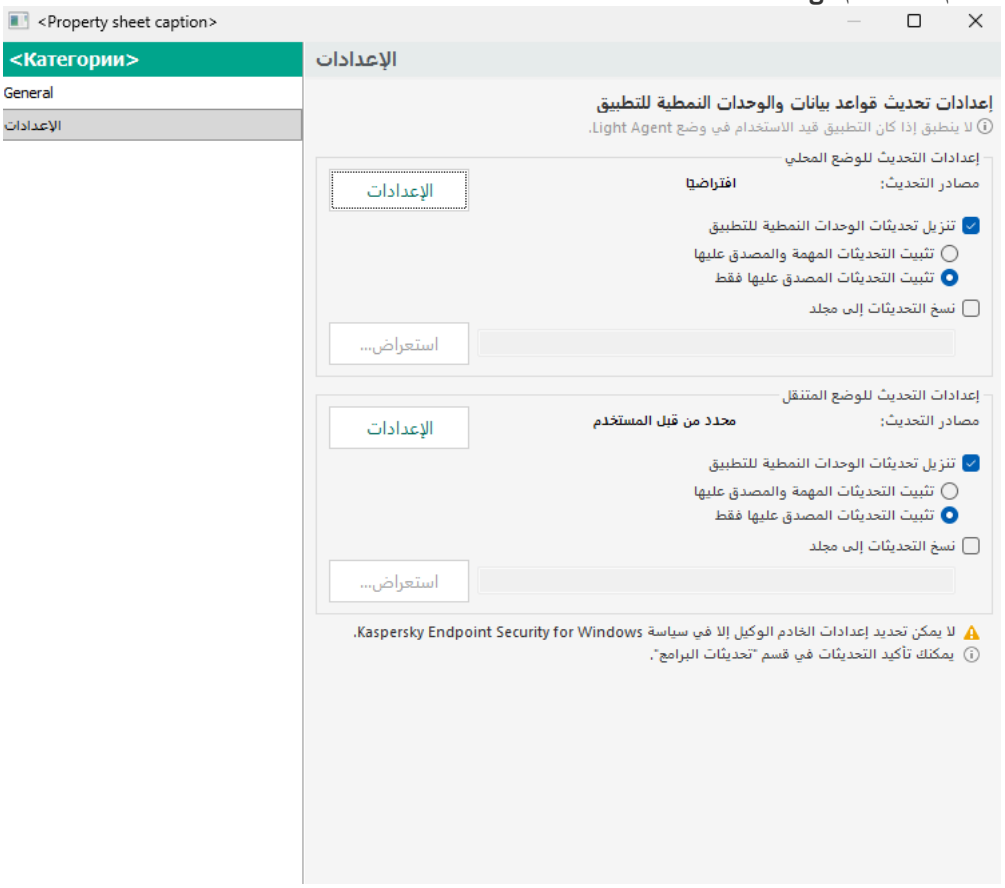
2. في شجرة وحدة التحكم، حدد **Tasks**.

3. انقر فوق المهمة **تحديث قواعد البيانات والوحدات النمطية للتطبيق** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

4. من نافذة خصائص المهام، حدد القسم **Settings**.



إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق

5. في القسم **إعدادات التحديث للوضع المحلي**، انقر على الزر **الإعدادات**.

6. في قائمة مصادر التحديث انقر فوق الزر **إضافة**.

7. في النافذة التي تفتح، أدخل مسار UNC إلى المجلد المشترك (على سبيل المثال، `\\<server name>\KLSHARE\Updates`).

يجب أن يتطابق عنوان المصدر مع العنوان الذي تمت الإشارة إليه في إعدادات أداة تحديث Kaspersky.

8. انقر على **موافق**.

9. 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.

10. احفظ تغييراتك.

كيفية تكوين التحديثات من المجلد المشترك في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **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 **Application settings** ← علامة التبويب **Local mode**.

4. في قائمة مصادر التحديث انقر فوق الزر **Add**.

5. في النافذة التي تفتح، أدخل مسار UNC إلى المجلد المشترك (على سبيل المثال، `\\<server name>\KLSHARE\Updates`).

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**.

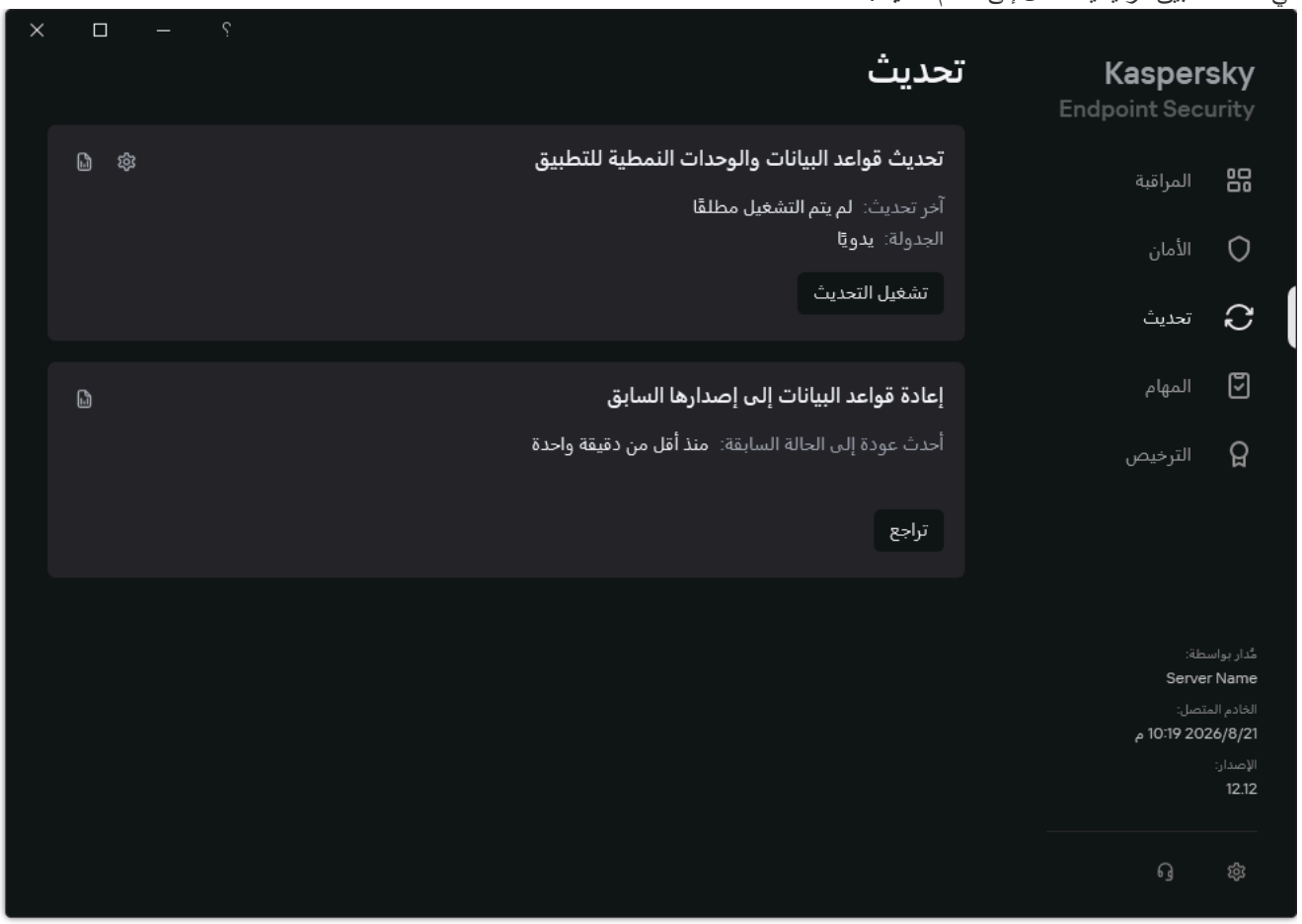
في حالة تعذر إجراء تحديث من مصدر التحديث الأول، فإن برنامج Kaspersky Endpoint Security ينتقل تلقائيًا إلى المصدر التالي.

8. احفظ تغييراتك.

كيفية تكوين التحديثات من المجلد المشترك في واجهة التطبيق

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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**.



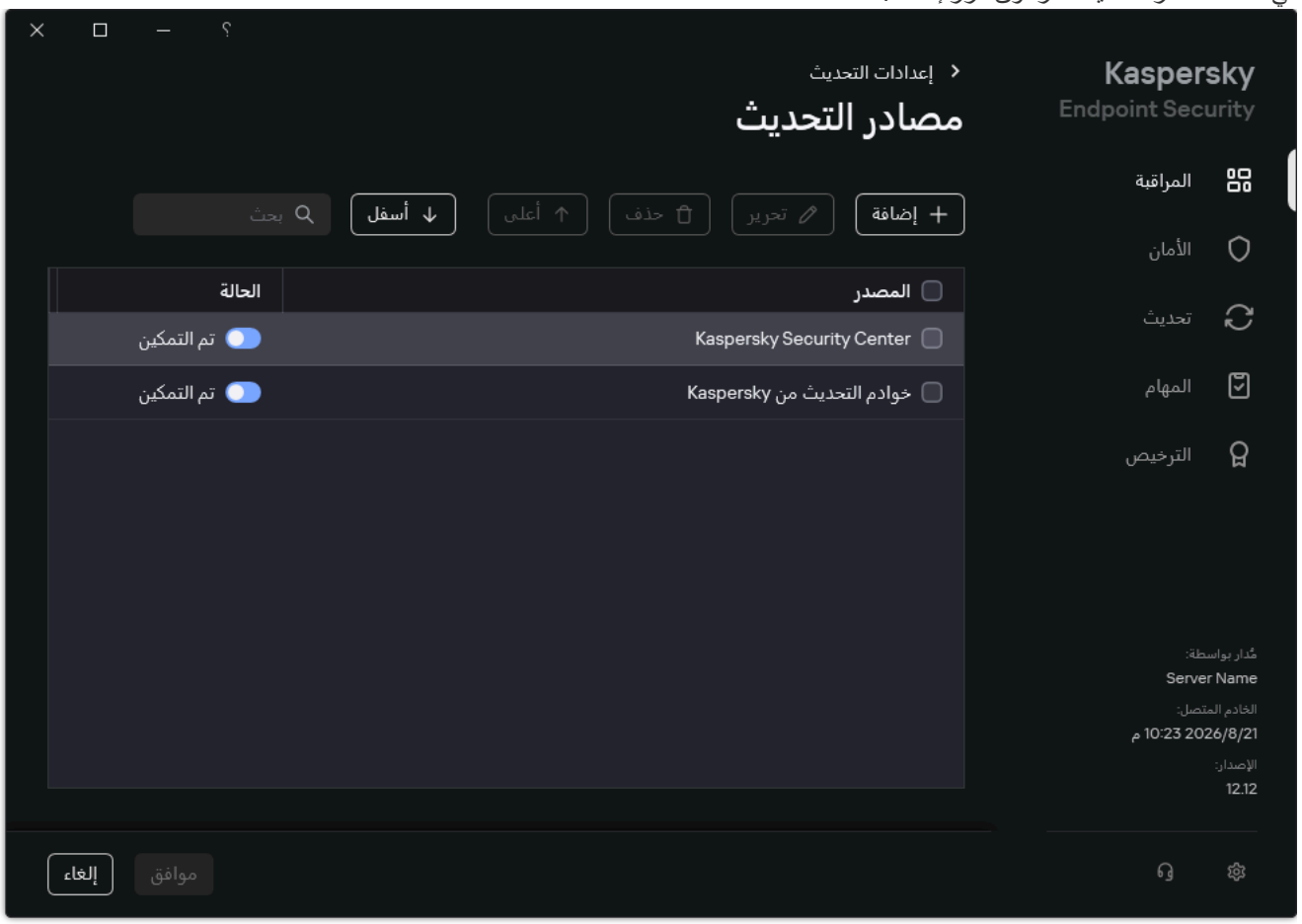
مهام التحديث المحلية

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 انقر فوق الزر **إضافة**.



مصادر التحديث

5. أدخل مسار UNC للمجلد المشترك (على سبيل المثال، `\\<server name>\KLSHARE\Updates`).

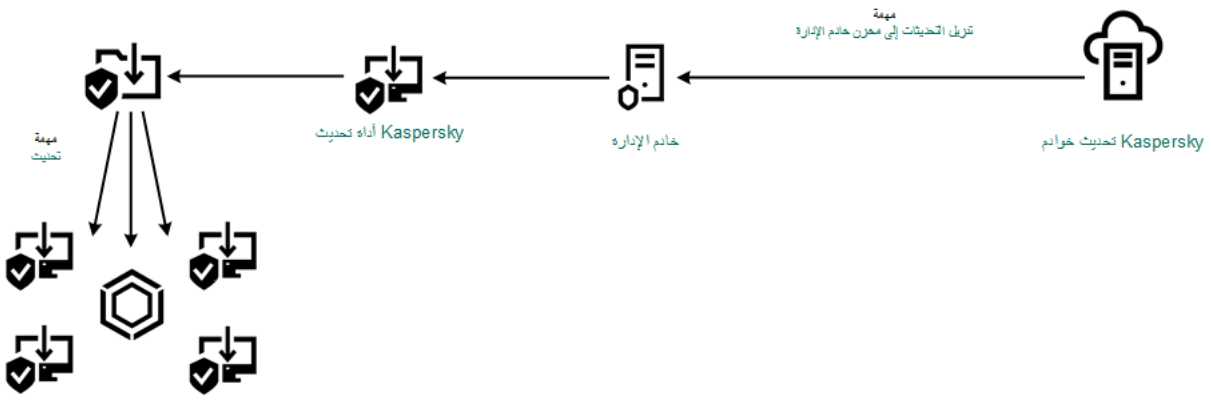
يجب أن يتطابق عنوان المصدر مع العنوان الذي تمت الإشارة إليه في إعدادات أداة تحديث Kaspersky.

6. انقر على **تحديد**.

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. احفظ تغييراتك.



التحديث باستخدام برنامج Kaspersky Update Utility

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.

كيفية تكوين إعدادات التحديث لوضع الهاتف المحمول في وحدة التحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

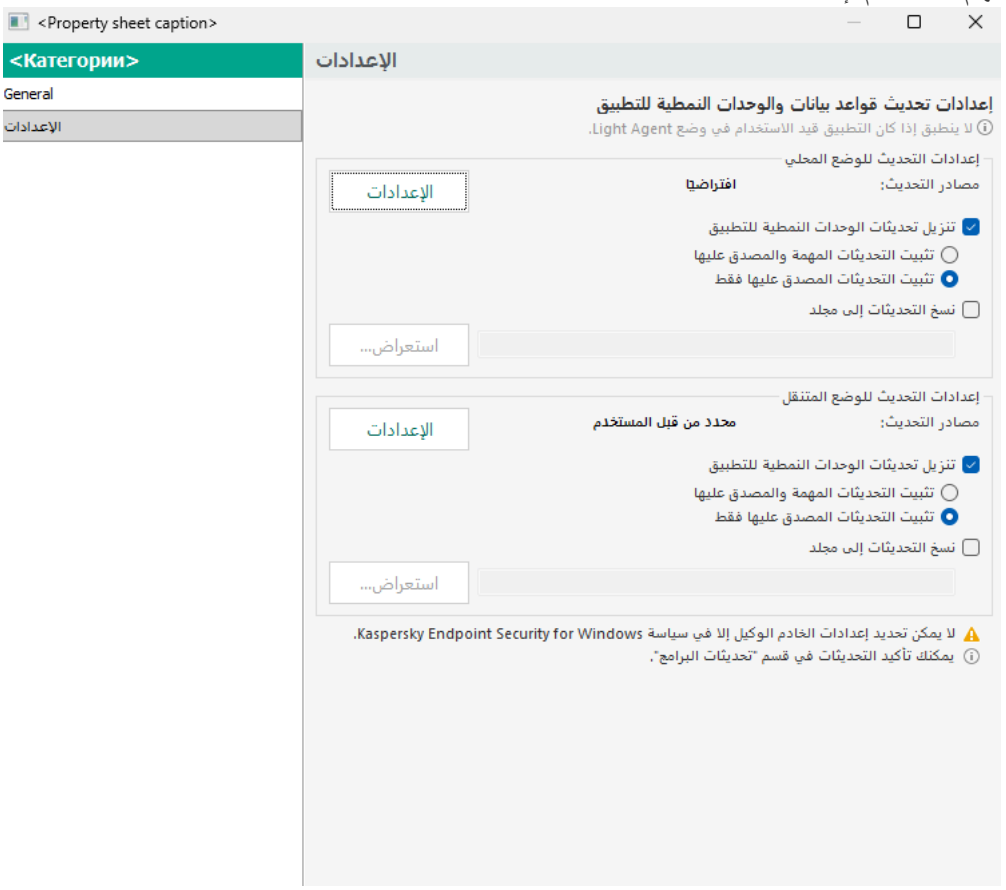
2. في شجرة وحدة التحكم، حدد **Tasks**.

3. انقر فوق المهمة **تحديث قواعد البيانات والوحدات النمطية للتطبيق** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.



إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق

5. في القسم **إعدادات التحديث للوضع المتنقل**، انقر على الزر **الإعدادات**.

6. تكوين مصادر التحديثات. يمكن أن تكون مصادر التحديث هي خوادم التحديث الخاصة بـ Kaspersky، أو خوادم FTP- وHTTP الأخرى، أو المجلدات المحلية، أو مجلدات الشبكة.

7. احفظ تغييراتك.

كيفية تكوين إعدادات التحديث لوضع الهاتف المحمول في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **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 **Application settings** ← علامة التبويب **Mobile mode**.

4. تكوين مصادر التحديثات. يمكن أن تكون مصادر التحديث 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

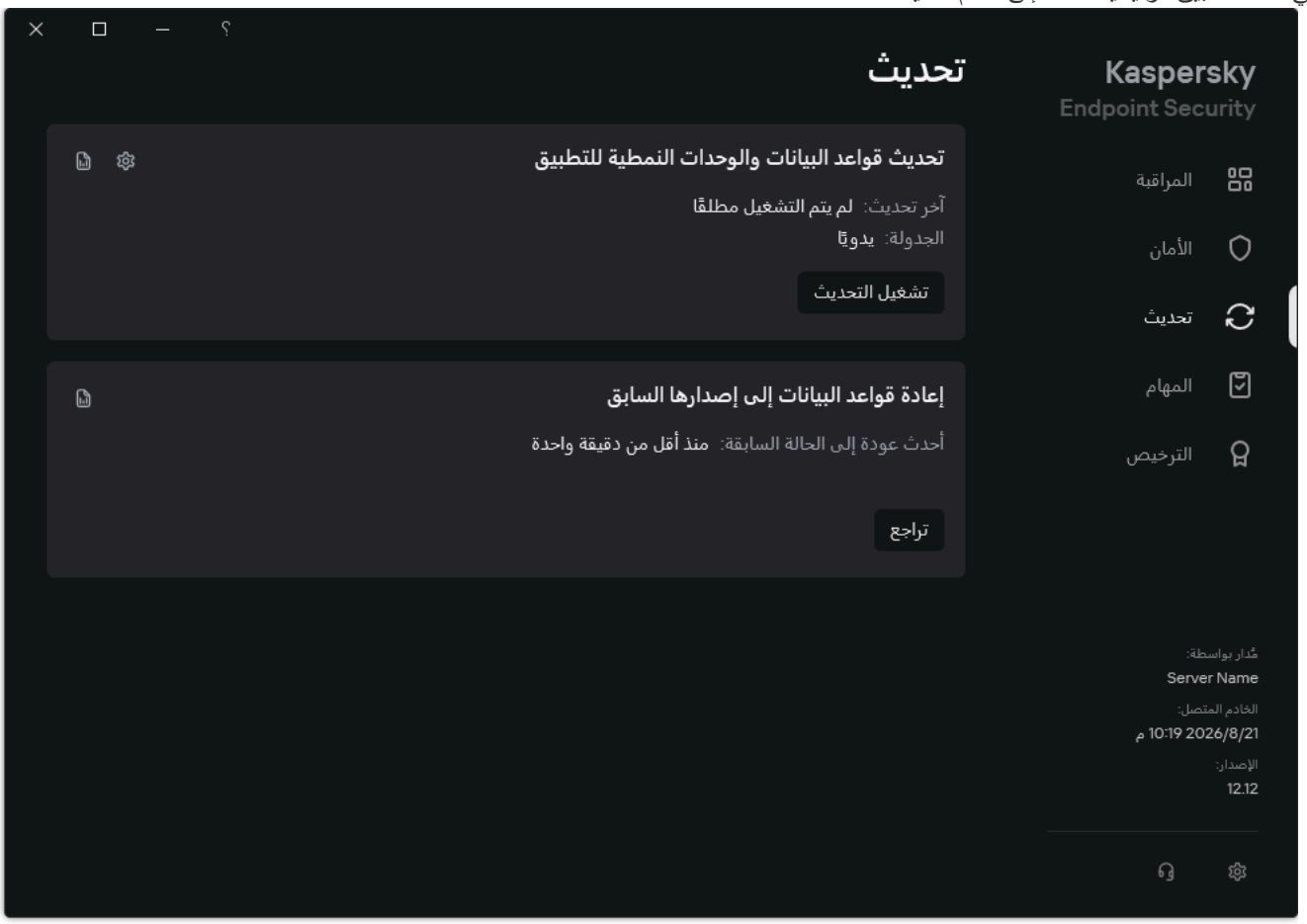
بدء مهمة تحديث تحت حقوق حساب مستخدم مختلف

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:

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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. 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

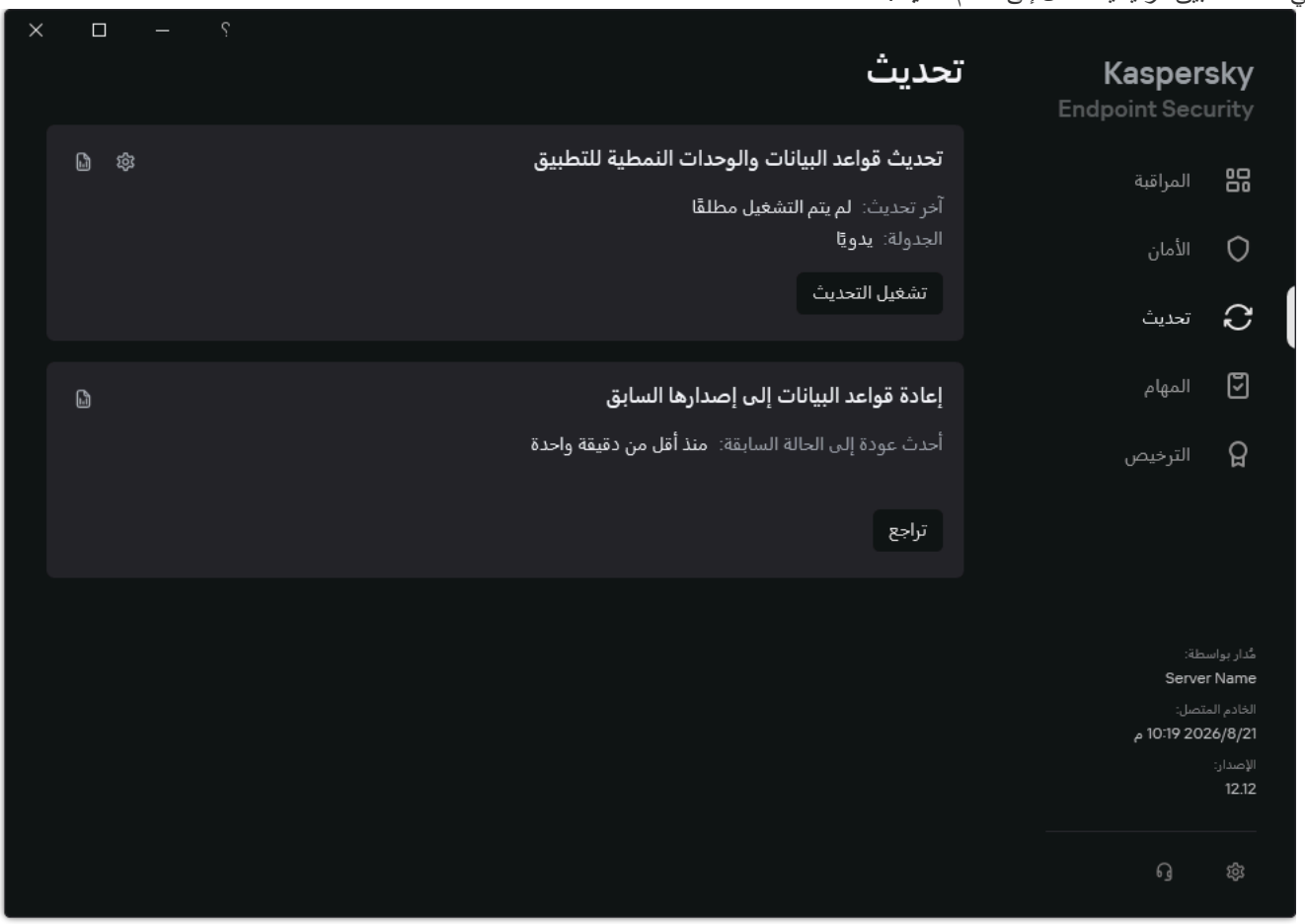
إذا تعذر تشغيل مهمة التحديث لأي سبب (على سبيل المثال: عدم تشغيل الكمبيوتر في ذلك الوقت)، يمكنك تكوين المهمة التي تم تخطيها لتبدأ تلقائيًا في أقرب وقت ممكن.

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:

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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. 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. وعندما يحصل التطبيق على فرصة لتنفيذ المهام الفائتة، يقوم بتشغيل المهام بشكل عشوائي خلال فترة زمنية معينة لتوزيع الحمل على الكمبيوتر.

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.

إذا كانت خوادم تحديث Kaspersky غير متوفرة، فيمكن أن يستخدم Kaspersky Endpoint Security مجالات بديلة لتحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق الخاصة به. وللحصول على معلومات مفصلة، ارجع إلى قاعدة معارف الدعم الفني.

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.

بشكل افتراضي، يستخدم Kaspersky Endpoint Security خادم Kaspersky Security Center كأول مصدر تحديث. ويساعد هذا في الحفاظ على حركة المرور عند التحديث. وإذا لم يتم تطبيق سياسة على الكمبيوتر، سيتم تحديد خوادم Kaspersky كأول مصدر تحديث في إعدادات المهمة المحلية تحديث قواعد البيانات والوحدات النمطية للتطبيق لأن التطبيق قد لا يتمكن من الوصول إلى خادم Kaspersky Security Center.

إذا كان التطبيق يعمل في وضع Light Agent، يتم تحديد مجلد على SVM كمصدر للتحديث.

كيفية إضافة مصدر تحديث في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

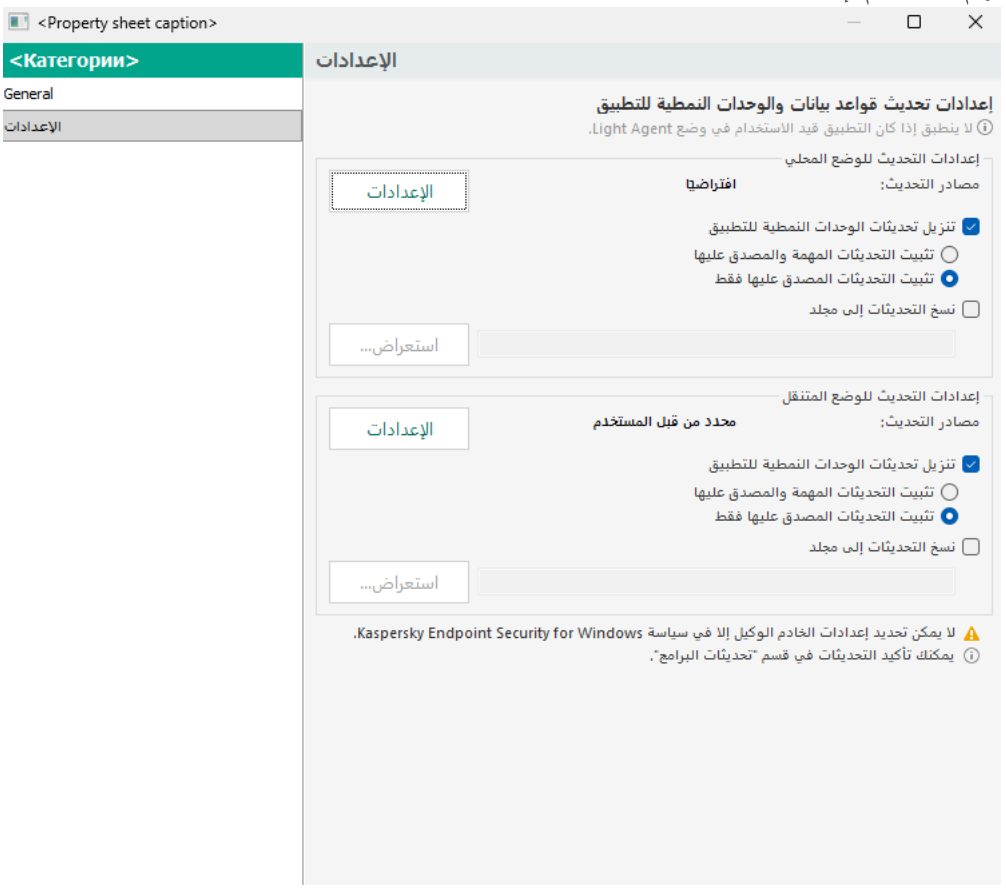
   في شجرة وحدة التحكم، حدد **Tasks**.

2. انقر فوق المهمة **تحديث قواعد البيانات والوحدات النمطية للتطبيق** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. من نافذة خصائص المهام، حدد القسم **الإعدادات**.



إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق

4. في القسم **إعدادات التحديث للوضع المحلي**، انقر على الزر **الإعدادات**.



مصادر التحديث

5. في قائمة مصادر التحديث انقر فوق الزر **إضافة**.

6. في الحقل **مصادر التحديث**، 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.

  علي 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\AVP12\Update distribution\`.

يمكنك استثناء مصدر التحديث دون إزالته من قائمة مصادر التحديث. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

7. انقر على **OK**.

8. 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.

9. اذا كان ضروريًا، أضف مصدر تحديث لوضع الهاتف المحمول. الوضع المتنقل هو وضع تشغيل برنامج Kaspersky Endpoint Security، عندما يترك الكمبيوتر شبكة مؤسسة محيطة (جهاز كمبيوتر غير متصل).

10. احفظ تغييراتك.

كيفية إضافة مصدر تحديث في Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.

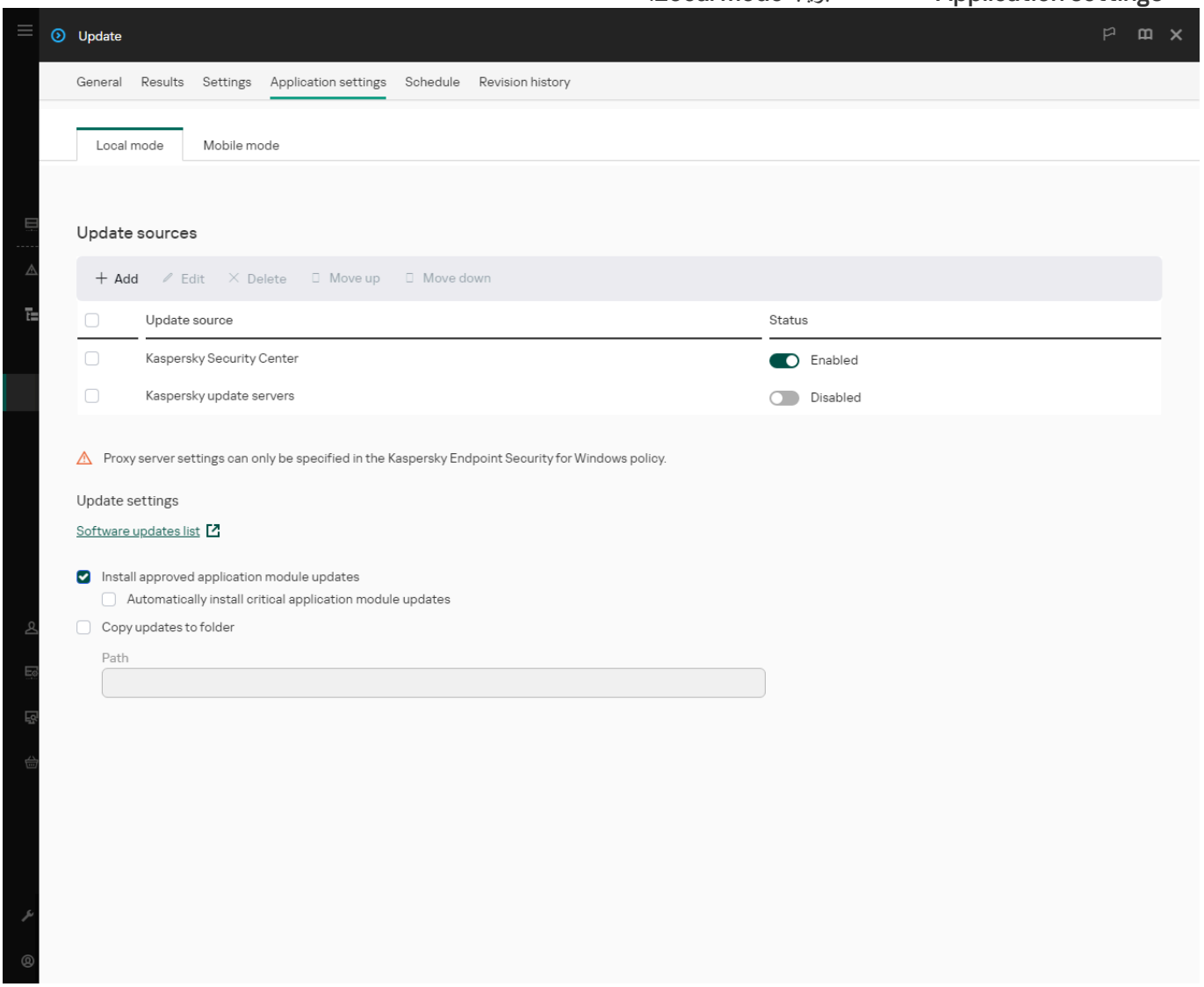
   تفتح قائمة المهام.

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 **Application settings** ← علامة التبويب **Local mode**.



مصادر التحديث

4. في قائمة مصادر التحديث انقر فوق الزر **Add**.

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\AVP12\Update distribution\`.

يمكنك استثناء مصدر التحديث دون إزالته من قائمة مصادر التحديث. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.

6. انقر على **OK**.

7. قم بتكوين أولويات مصادر التحديث باستخدام الزر **Move up** و**Move down**.

في حالة تعذر إجراء تحديث من مصدر التحديث الأول، فإن برنامج Kaspersky Endpoint Security ينتقل تلقائيًا إلى المصدر التالي.

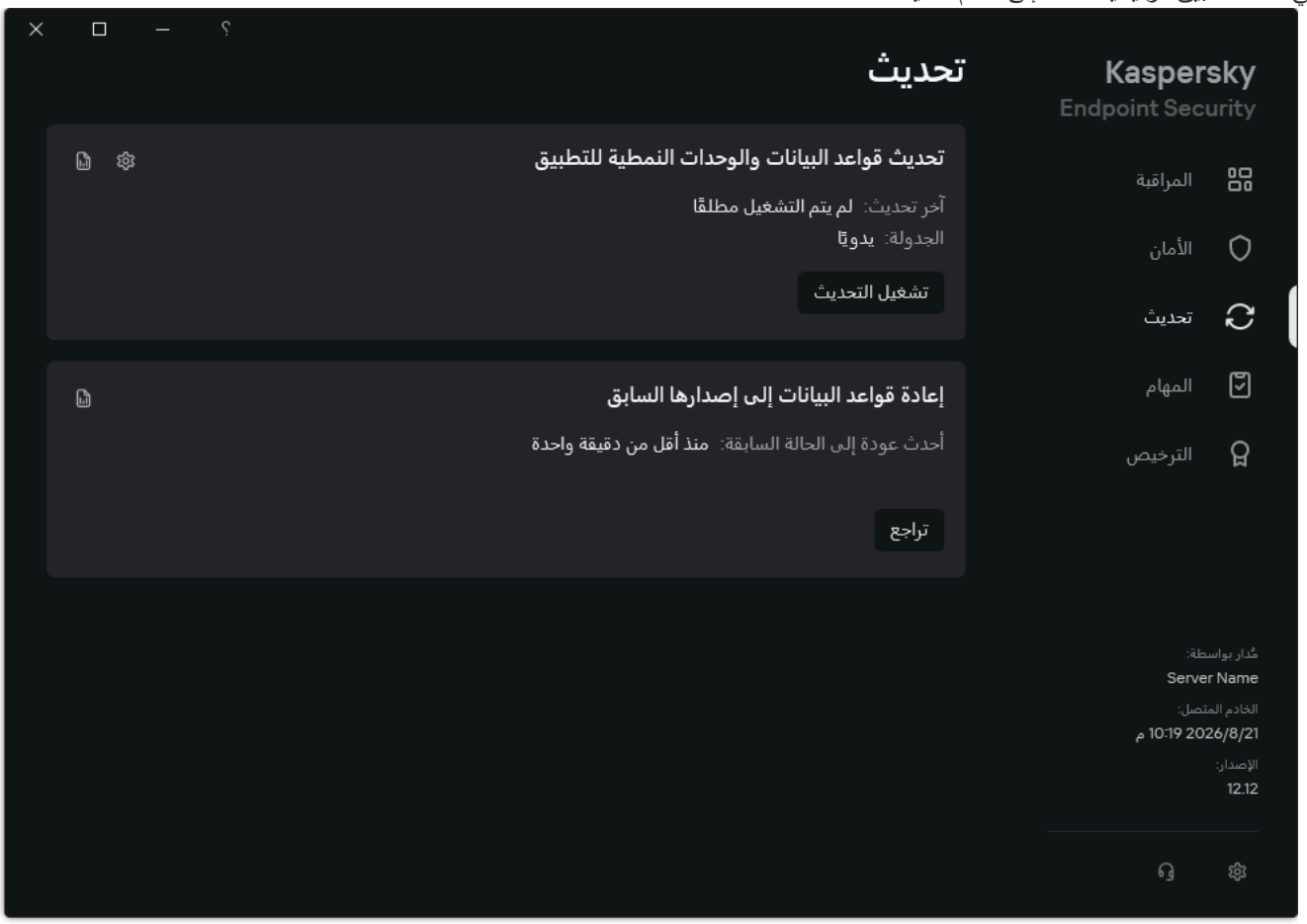
8. اذا كان ضروريًا، أضف مصدر تحديث لوضع الهاتف المحمول. الوضع المتنقل هو وضع تشغيل برنامج Kaspersky Endpoint Security، عندما يترك الكمبيوتر شبكة مؤسسة محيطة (جهاز كمبيوتر غير متصل).

9. احفظ تغييراتك.

كيفية إضافة مصدر تحديث في واجهة التطبيق

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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**.



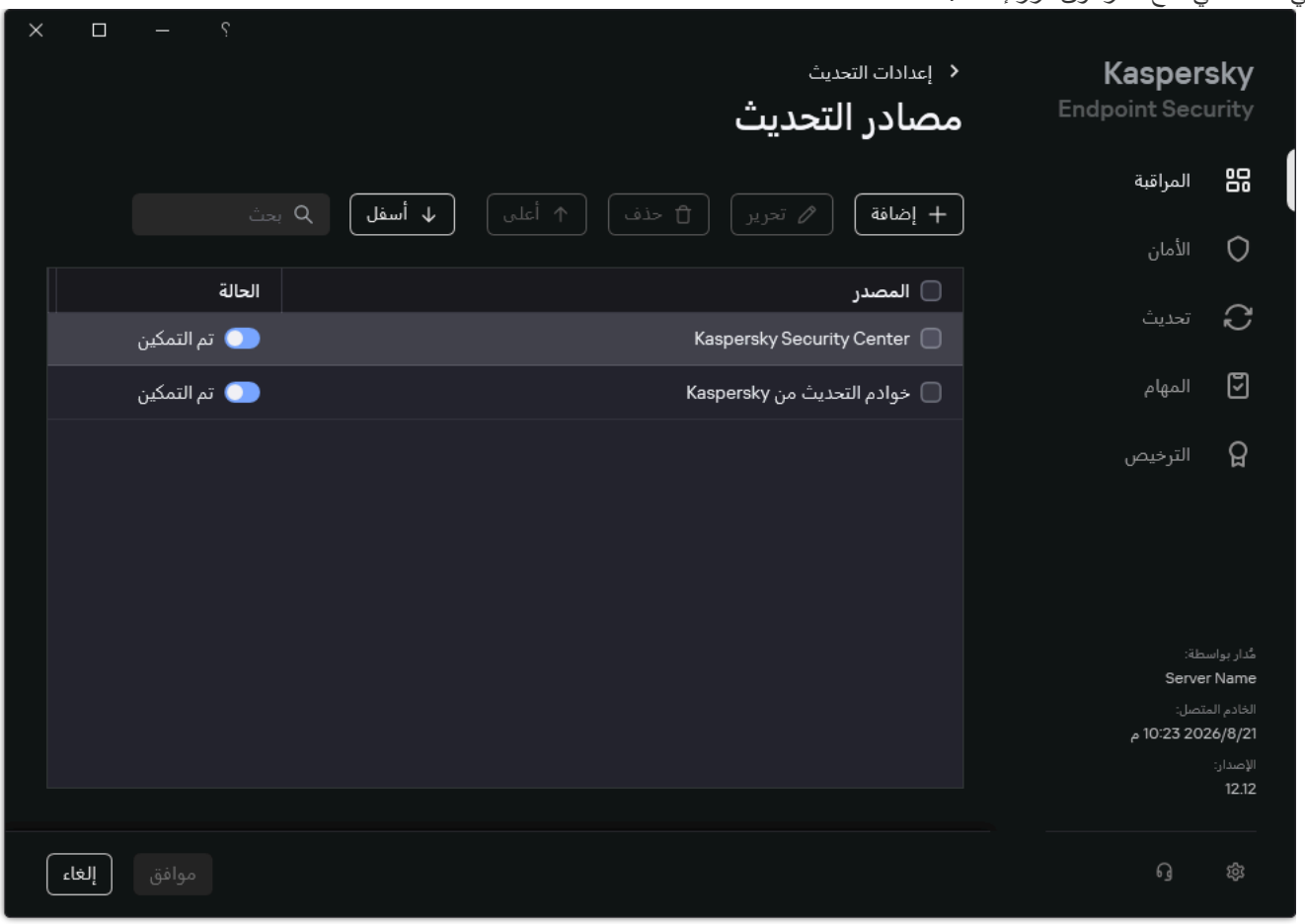
مهام التحديث المحلية

2. يفتح هذا قائمة المهام؛ وحدد مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق وانقر فوق ⚙.

نافذة خصائص المهمة.

3. انقر على **تحديد مصادر التحديث**.

4. في النافذة التي تفتح، 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\AVP12\Update distribution\`.

6. انقر على **تحديد**.

7. قم بتكوين أولويات مصادر التحديث باستخدام الزر **أعلى** و**أسفل**.

8. 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.

بعد تثبيت تحديث التطبيق، قد تتم مطالبتك بإعادة تشغيل جهاز الكمبيوتر الخاص بك.

كيفية تكوين تحديثات وحدة التطبيق في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

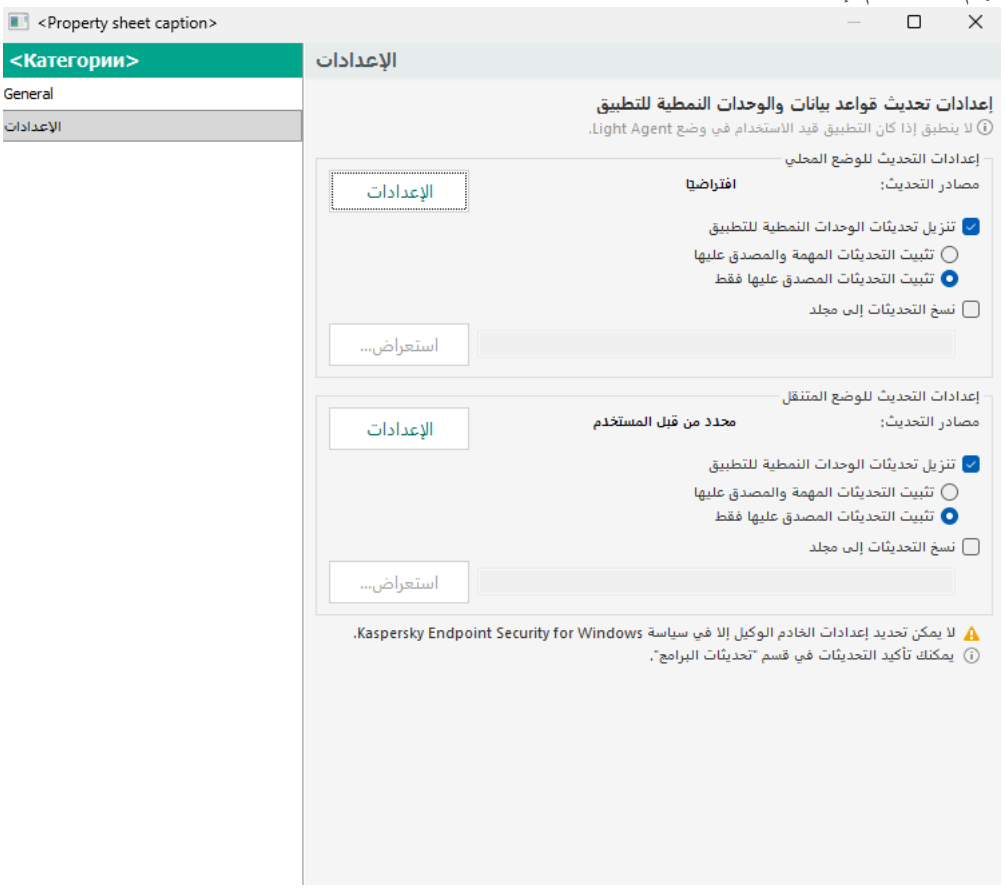
2. في شجرة وحدة التحكم، حدد **Tasks**.

3. انقر فوق المهمة **تحديث قواعد البيانات والوحدات النمطية للتطبيق** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.



إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق

5. في القسم **إعدادات التحديث للوضع المحلي**، حدد خانة الاختيار **تنزيل تحديثات الوحدات النمطية للتطبيق**.

إذا كنت ترغب في منع تنزيل تحديثات الوحدة النمطية للتطبيق، فقم بإلغاء تحديد خانة الاختيار **تنزيل تحديثات الوحدات النمطية للتطبيق** و[احظر استخدام المهام المحلية من قبل المستخدم](#).

6. حدد تحديثات وحدات التطبيق التي تريد تثبيتها.

- **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.

7. إذا لزم الأمر، كوّن تحديثات الوحدة النمطية للتطبيق لوضع الهاتف المحمول. الوضع المتنقل هو وضع تشغيل برنامج Kaspersky Endpoint Security، عندما يترك الكمبيوتر شبكة مؤسسة محيطة (جهاز كمبيوتر غير متصل).

8. احفظ تغييراتك.

كيفية تكوين تحديثات الوحدة النمطية للتطبيق في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.

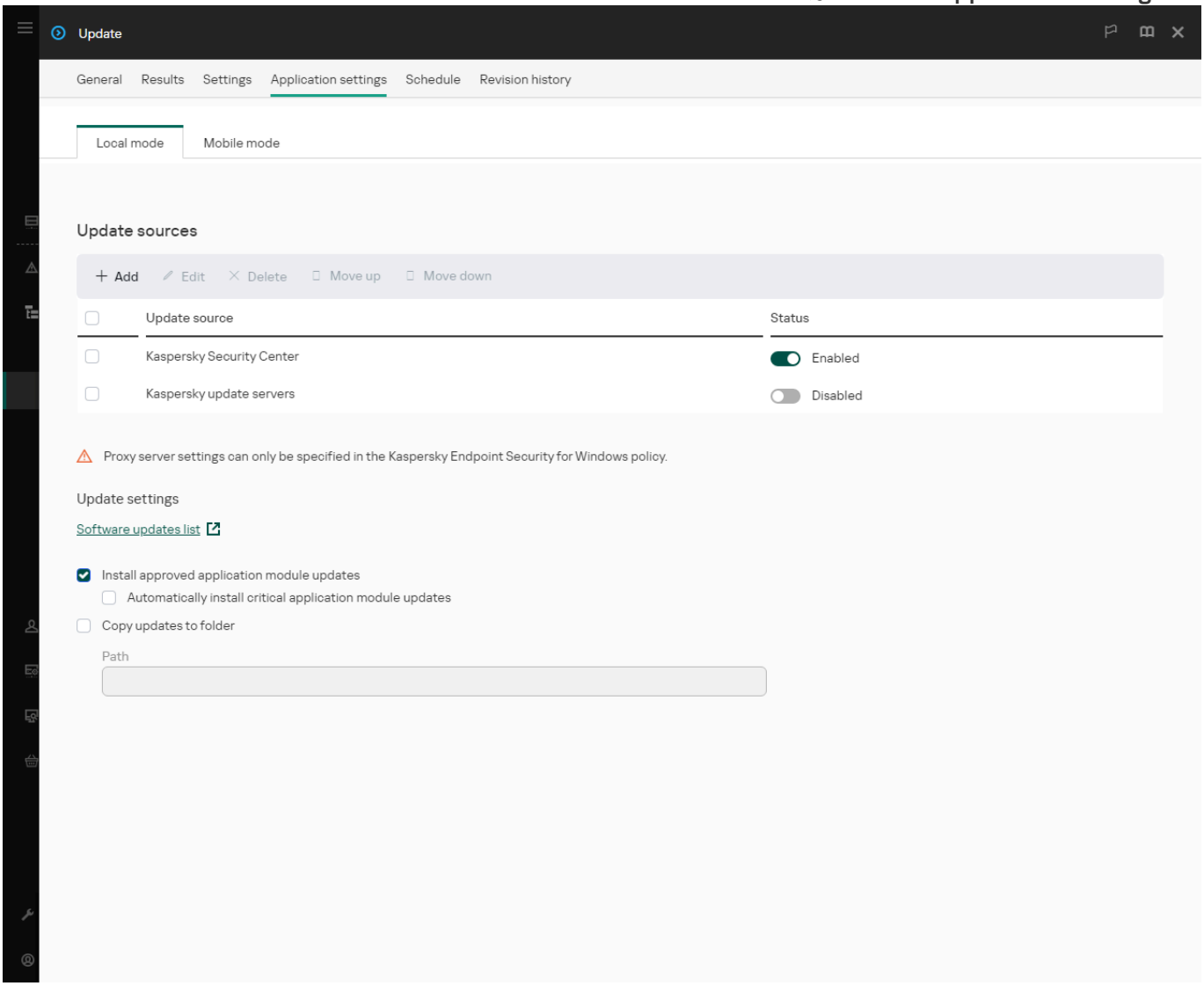
تفتح قائمة المهام.

2. انقر فوق المهمة **تحديث قواعد البيانات والوحدات النمطية للتطبيق** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

يتم إنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا بواسطة معالج بدء التشغيل السريع لخادم الإدارة. ولإنشاء مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق، قم بتثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows أثناء تشغيل المعالج.

3. حدد **Application settings** ← علامة التبويب **Local mode**.



إعدادات مهمة Update

4. تحت **Update settings**، حدد تحديثات الوحدة النمطية للتطبيق التي تريد تثبيتها:

- **Install approved application module updates**. 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.
- **Automatically install critical application module updates**. 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.

إذا كنت ترغب في منع تنزيل تحديثات الوحدة النمطية للتطبيق، فقم بإلغاء تحديد خانتي الاختيار **Install approved application module updates** و**Automatically install critical application module updates** و[احظر استخدام المهام المحلية من قبل المستخدم](#).

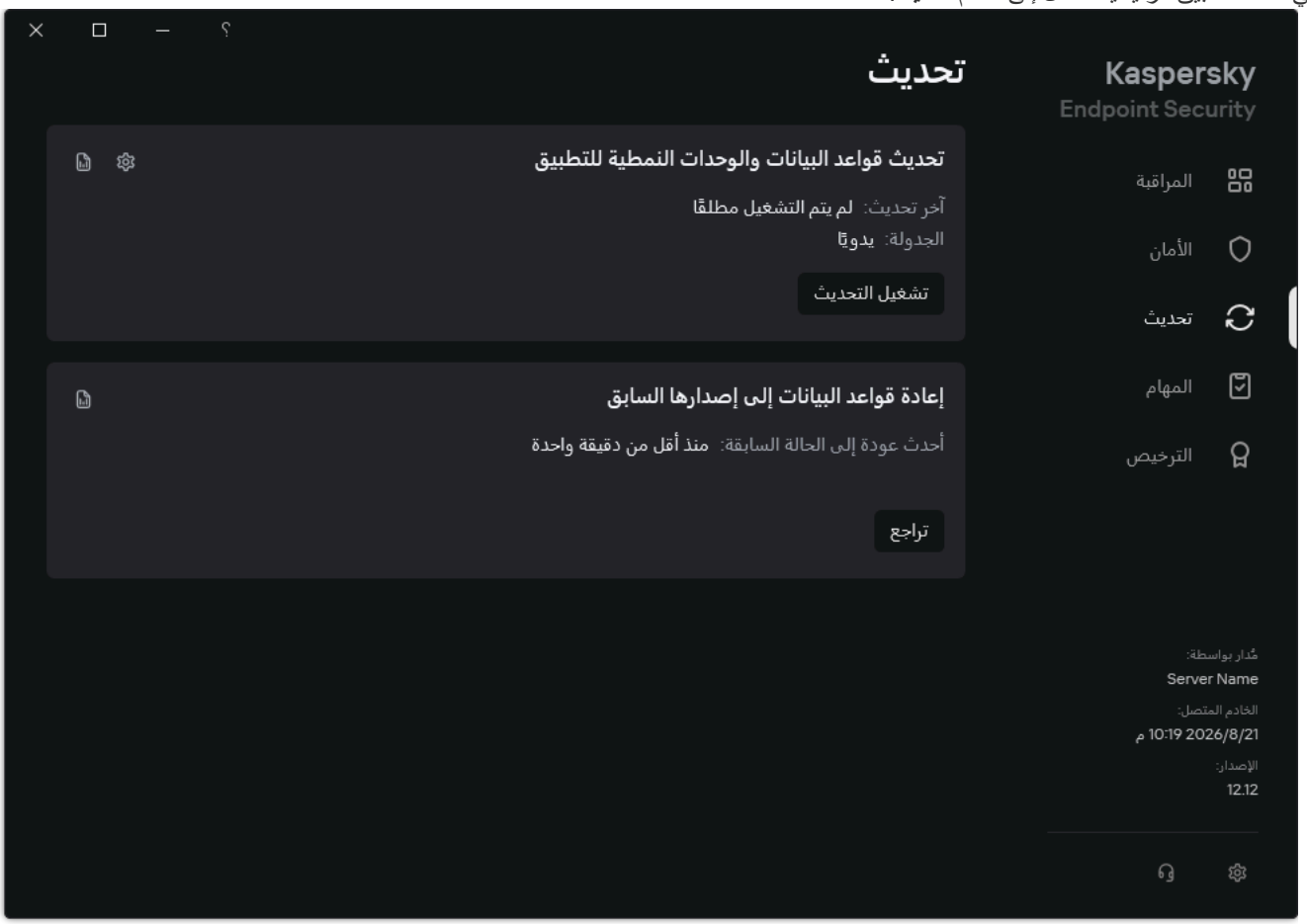
5. إذا لزم الأمر، [كوّن تحديثات الوحدة النمطية للتطبيق لوضع الهاتف المحمول](#). الوضع المتنقل هو وضع تشغيل برنامج Kaspersky Endpoint Security، عندما يترك الكمبيوتر شبكة مؤسسة محيطة (جهاز كمبيوتر غير متصل).

6. احفظ تغييراتك.

كيفية تكوين تحديثات الوحدة النمطية للتطبيق في واجهة التطبيق

لا يمكنك تكوين المهمة الجماعية تحديث قواعد البيانات والوحدات النمطية للتطبيق 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 القسم **تنزيل وتثبيت تحديثات الوحدات النمطية للتطبيق**، حدد خانة الاختيار **تنزيل تحديثات الوحدات النمطية للتطبيق**.

4. حدد تحديثات وحدات التطبيق التي تريد تثبيتها.

- **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.

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 اختيار **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 نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.
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 **Proxy server**، انقر على الزر **Settings**.
6. في النافذة التي تفتح، حدد خانة الاختيار **Bypass a proxy server for local addresses**.
7. 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:

- **استخدام إعدادات الخادم الوكيل السابقة على نظام التشغيل**.

  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. حدد كيف تريد أن يصادق التطبيق على الخادم الوكيل. وبشكل افتراضي، يستخدم التطبيق مصادقة NTLM للمجال للمستخدم الحالي.

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 الثانية، 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 التحديث الأخير مفيدًا، على سبيل المثال، إذا تسببت نسخة قاعدة البيانات الجديدة في رصد خاطئ أدى إلى حظر تطبيق آمن بواسطة Kaspersky Endpoint Security.

لا يدعم Kaspersky Endpoint Security في وضع Light Agent مهمة تراجع عن التحديث.

كيفية التراجع عن التحديث الأخير في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

1. حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **تراجع عن التحديث**.

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

كوّن جدول المهام، على سبيل المثال، يدويًا.

الخطوة الرابعة: تحديد اسم المهمة

أدخل اسمًا للمهمة.

الخطوة 7 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية التراجع عن التحديث الأخير في Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

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

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Rollback**.

c. في الحقل **Task name** أدخل وصفًا مختصرًا، مثل تراجع عن التحديث.

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

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

5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

6. قم بإنهاء المعالج.

7. سيتم عرض مهمة جديدة في قائمة المهام.

8. حدد خانة الاختيار المجاورة للمهمة.

9. انقر فوق **Start**.

كيفية التراجع عن التحديث الأخير في واجهة التطبيق

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**.

تقنية التنظيف المتقدمة

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.

إذا لم يتمكن Kaspersky Endpoint Security من إيقاف تنفيذ جزء من البرامج الضارة، فيمكنك استخدام تقنية التنظيف المتقدم. وبالنسبة لأجهزة الكمبيوتر الخاضعة للسياسة، يتم تعطيل التنظيف المتقدم افتراضيًا لأن هذه التقنية تستخدم قدرًا كبيرًا من موارد الحوسبة. وبالنسبة لأجهزة الكمبيوتر التي لا تخضع للسياسة، يتم تمكين التنظيف المتقدم بشكل افتراضي.

ويعمل التنظيف المتقدم بشكل مختلف لمحطات العمل والخوادم. ولاستخدام التقنية على الخوادم، يجب تمكين التنظيف المتقدم الفوري 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.
4. في القسم **عام**، حدد أو امسح خانة الاختيار **تمكين تقنية التنظيف المتقدم** لتمكين تقنية التنظيف المتقدم أو تعطيلها.
5. احفظ تغييراتك.

كيفية تمكين أو تعطيل تقنية التنظيف المتقدمة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. حدد **Detection Settings** ← **General Settings**.
5. في القسم **Advanced Disinfection Technology**، قم بتشغيل أو إيقاف تشغيل مفتاح التبديل **Advanced Disinfection Technology ENABLED** 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 **عام**، 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 المتقدم. وعند اكتمال التنظيف، سيتم إعادة تشغيل الكمبيوتر.

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، يمكنك 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.

القضاء على التهديدات غير المعالجة

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).



قائمة بالتهديدات 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 **إعلام**. وبعد ذلك، عندما يتم عرض إخطار الملف المصاب على الشاشة، حدد المستخدم **تجاهل**.

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 . – Critical

كيفية معالجة تهديد في وحدة تحكم الإدارة (MMC)

1. في وحدة تحكم الإدارة، انتقل إلى المجلد **Active threats** ← **Repositories** ← **Advanced** ← **Administration Server**.
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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **Delete**. في حالة تحديد هذا الخيار، يحذف التطبيق الملفات المصابة المكتشفة من مستودع التهديدات النشطة. وفي هذه الحالة، يحتفظ التطبيق بالملف المكتشف في ذاكرة الكمبيوتر. ولإزالة التهديد من الكمبيوتر، حدد **Disinfect**.

كيفية معالجة تهديد في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Operations** ← **Repositories** ← **Active threats**.
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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **Delete**. في حالة تحديد هذا الخيار، يحذف التطبيق الملفات المصابة المكتشفة من مستودع التهديدات النشطة. وفي هذه الحالة، يحتفظ التطبيق بالملف المكتشف في ذاكرة الكمبيوتر. ولإزالة التهديد من الكمبيوتر، حدد **Disinfect**.

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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **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 OK. 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 قاعدة بيانات الثغرات الأمنية والتهديدات لدى Kaspersky.

لمعالجة التهديدات النشطة في وحدة تحكم Kaspersky Security Center، يجب عليك تمكين نقل المعلومات عن الملفات التي لم تتم معالجتها إلى خادم الإدارة. ويتم تمكين نقل البيانات بشكل افتراضي.

كيفية تمكين نقل بيانات الملفات التي لم تتم معالجتها في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **التقارير والمخزن**.

4. في القسم **نقل البيانات إلى خادم الإدارة**، انقر على الزر **الإعدادات**.

5. حدد خانة الاختيار **الملفات التي لم تتم معالجتها**.

6. احفظ تغييراتك.

كيفية تمكين نقل بيانات الملفات التي لم تتم معالجتها في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

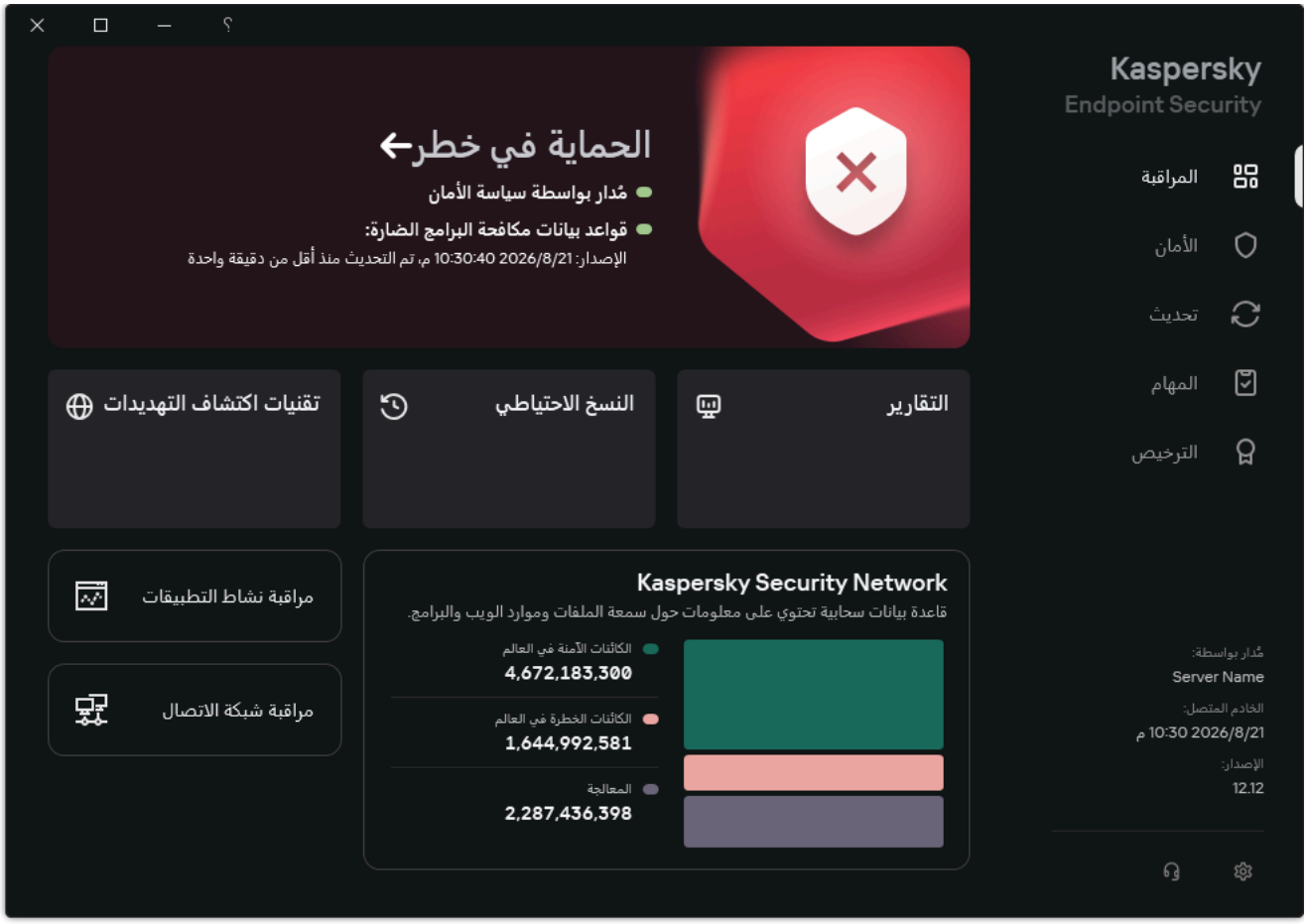
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.

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

4. انتقل إلى **General Settings** ← **KSC Integration**.

5. في القسم **Data transfer to Administration Server**، حدد خانة الاختيار **About unprocessed files**.

6. احفظ تغييراتك.



نافذة التطبيق الرئيسية عند اكتشاف تهديد

حماية الكمبيوتر

حالة الحماية في الوقت الحقيقي

يرسل Kaspersky Endpoint Security إعداد **Real-time protection status** إلى خادم إدارة Kaspersky Security Center؛ وتعتمد قيمة هذا الإعداد على الحالة الحالية لمكونات حماية التطبيق على الكمبيوتر المحمي (انظر الجدول أدناه).

يحدد Kaspersky Endpoint Security حالة الحماية في الوقت الحقيقي بناءً على حالة مكونات التطبيق التالية:

- الحماية من تهديدات الملفات.
- الحماية من تهديدات الويب.
- الحماية من تهديدات البريد.
- حماية AMSI.
- منع هجمات BadUSB.
- الحماية من تهديدات الشبكة.
- جدار الحماية.
- منع الاستغلال.
- اكتشاف السلوك.
- محرك المعالجة.
- منع اختراق المضيف.

يمكنك التحقق من حالة الحماية في الوقت الحقيقي للتطبيق في وحدة تحكم Kaspersky Security Center.

كيفية معرفة حالة الحماية في الوقت الحقيقي في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Managed devices**.

يتم عرض حالة الحماية في الوقت الحقيقي الحالية في قائمة الأجهزة، في العمود **Real-time protection status**. وإذا كان العمود **Real-time protection status** مفقودًا، قم بإدارة إعدادات العمود بالنقر فوق الرابط **Add/Remove Columns**.

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Managed devices**.

يتم عرض حالة الحماية في الوقت الحقيقي الحالية في قائمة الأجهزة، في العمود **Real-time protection status**. وإذا كان العمود **Real-time protection status** مفقودًا، قم بإدارة إعدادات العمود بالنقر فوق الرابط **Add/Remove Columns**.

كيفية معرفة حماية الكمبيوتر في الوقت الحقيقي في Web Console

في نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.

يتم عرض حالة الحماية في الوقت الحقيقي الحالية في قائمة الأجهزة، في العمود **Real-time protection status**. إذا كان العمود **Real-time protection status** مفقودًا، قم بإدارة إعدادات العمود (⚙).

القيم الممكنة للإعداد Real-time protection status

القيمة	الوصف
Unknown	لا يحتوي خادم الإدارة على معلومات عن حالة الحماية في الوقت الحقيقي لهذا الكمبيوتر.
Not installed	لم يتم تثبيت أي مكونات.
Not supported by license	لم يتم تفعيل التطبيق أو لا يسمح الترخيص للمكونات المثبتة بالعمل.
Failed	تعطل مكون واحد أو أكثر.
Stopped	تم تعطيل مكون واحد أو أكثر.
Paused	يوجد مكون واحد أو أكثر تم إيقافه مؤقتًا.
Starting	جارٍ تشغيل مكون واحد أو أكثر.
Running	مكونات التطبيق قيد التشغيل.

إذا كانت قيمة إعداد **Real-time protection status** في Kaspersky Security Center تختلف عن Running، تحقق من تمكين مكونات Kaspersky Endpoint Security المثبتة من القائمة ومن تفعيل التطبيق.

الحماية من تهديدات الملفات

يتيح لك مكون الحماية من تهديدات الملفات منع إصابة نظام ملفات الكمبيوتر. وبشكل افتراضي، يوجد مكون الحماية من تهديدات الملفات بشكل دائم في ذاكرة الوصول العشوائي للكمبيوتر ويفحص جميع الملفات التي يتم فتحها وحفظها وبدء تشغيلها، في الوقت الحقيقي. ويفحص هذا المكون الملفات الموجودة على جميع محركات أقراص الكمبيوتر، بما في ذلك محركات الأقراص المتصلة. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

يفحص المكون الملفات التي تم الوصول إليها بواسطة مستخدم أو تطبيق. 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 توجد محتوياته في وحدة تخزين سحابية في 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.

يستخدم مكون الحماية من تهديدات الملفات البيانات الواردة من مكونات التطبيق الأخرى. تمكين هذه المكونات اختياري. تتضمن المكونات التي توفر بيانات إضافية ما يلي:

- Kaspersky Security Network.
- منع اختراق المضيف.
- اكتشاف السلوك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات الملفات في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية ← الحماية من تهديدات الملفات**.
4. استخدم خانة الاختيار **الحماية من تهديدات الملفات** لتمكين المكون أو تعطيله.
5. 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.
- **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 **الإعدادات** وحدد إعدادات المكون الخاص بك (انظر الجدول أدناه).

  يمكنك استعادة قيم مستويات الأمان المعينة مسبقًا بالنقر فوق الزر **افتراضيًا**.

6. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد الإجراء الذي سينفذه تطبيق Kaspersky Endpoint Security على الكائنات الضارة:

- **تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يمنع التطبيق هذا الملف.
- **منع**. إذا تم تحديد هذا الخيار، فسيحظر التطبيق تلقائيًا الملف المصاب دون محاولة تنظيفه أو حذفه.
- **إعلام**. 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.

7. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات الملفات في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Host Threat Protection** ← **File Threat Protection**.

5. استخدم مفتاح تبديل **File Threat Protection ENABLED** لتمكين المكون أو تعطيله.

6. إذا كنت تريد إضافة كائن جديد إلى نطاق الحماية:

a. تحت **Advanced settings**، حدد علامة التبويب **Protection scope**.

b. انقر على **Add**.

c. في النافذة التي تفتح؛ في تلك النافذة، حدد الكائنات التي تريد إضافتها إلى نطاق الحماية.
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 الحماية بدون إزالته من قائمة الكائنات في نطاق الحماية. ولفعل ذلك، اضبط مفتاح التبديل المجاور له على وضع إيقاف التشغيل.

d. احفظ تغييراتك.

7. في القسم **Action on threat detection**، حدد الإجراء الذي سينفذه تطبيق Kaspersky Endpoint Security على الكائنات الضارة:

- **Disinfect, delete if disinfection fails**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **Disinfect, block if disinfection fails**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يمنع التطبيق هذا الملف.
- **Block**. إذا تم تحديد هذا الخيار، فسيحظر التطبيق تلقائيًا الملف المصاب دون محاولة تنظيفه أو حذفه.

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.

8. إذا لزم الأمر، حرر الإعدادات المتقدمة للحماية من تهديدات الملفات.

9. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات الملفات في واجهة التطبيق

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.
- **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 (انظر الجدول أدناه).

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 تطبيق Kaspersky Endpoint Security على الكائنات الضارة:

- **تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يمنع التطبيق هذا الملف.

- **منع**. إذا تم تحديد هذا الخيار، فسيحظر التطبيق تلقائيًا الملف المصاب دون محاولة تنظيفه أو حذفه.
- **إعلام**. 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.

6. 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 الملفات من عمليات 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. ويفحص التطبيق الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
فحص ملفات تنسيق البريد الإلكتروني	**تشغيل**	يفحص ملفات تنسيق البريد الإلكتروني. يفحص التطبيق ملفات MSG وEML. وتتضمن ملفات تنسيق البريد الإلكتروني كائنات OLE وملفات MHT كذلك. ويفحص تطبيق Kaspersky Endpoint Security ملفات البريد الإلكتروني 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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.

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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف.
- **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يمنع التطبيق هذا الملف.
- **منع**. إذا تم تحديد هذا الخيار، فسيحظر التطبيق تلقائيًا الملف المصاب دون محاولة تنظيفه أو حذفه.

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. في الحقل **المسار**، 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\`.

يتضمن كائن **هذا الكمبيوتر** في قائمة موارد الملفات الخاصة بالكمبيوتر الكائنات التالية: **كل محركات الأقراص الثابتة** و**كل محركات أقراص الشبكة** و**جميع محركات الأقراص القابلة للإزالة**.

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 الملفات من عمليات 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 التوزيع، أو البريد، أو الملفات بتنسيق 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 ضغط 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 الأصغر 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.

فحص الحاوية

الحاوية هي بيئة معزولة حيث يمكن تشغيل أحد التطبيقات دون التفاعل المباشر مع نظام التشغيل. ينطوي استخدام الحاويات على المخاطر التالية:

- قد يتمكن المتسللون من استغلال الثغرات الأمنية في الحاويات لاختراق التطبيقات داخل الحاوية.
- قد يستغل المتسللون تكوينًا غير آمن لبيئة الحاوية للحصول على وصول غير مصرح به إلى البيانات الموجودة على الكمبيوتر أو للإضرار بسلامة النظام.
- قد يسمح هجوم ناجح على حاوية للمتسلل بالوصول إلى البيانات الموجودة على الكمبيوتر.
- قد يستغل المتسللون الثغرات الأمنية في الشبكة لاعتراض حركة مرور الشبكة.

يفحص Kaspersky Endpoint Security الملفات ليس فقط على الأقراص لكن داخل الحاويات أيضًا. أي أن Kaspersky Endpoint Security عبارة عن أداة خارجية لاكتشاف النشاط الضار داخل الحاويات. ويسمح هذا بالحفاظ على أداء الحاويات ويمنع التعارض مع التطبيقات الأخرى داخل الحاوية. لا يتم دعم تثبيت Kaspersky Endpoint Security داخل الحاوية.

بالإضافة إلى توفير أمان الحاوية ، يتيح Kaspersky Endpoint Security إدارة التطبيقات داخل الحاويات باستخدام التحكم في التطبيقات. ويتم تكوين التحكم في التطبيق للحاويات بالطريقة ذاتها الخاصة بتكوين التطبيقات المثبتة على الكمبيوتر. تدعم مراقبة سلامة النظام أيضًا الحاويات.

متطلبات الحاوية

- يجب أن تكون الحاوية عبارة عن حاوية Docker. ولا يتم دعم أدوات النقل بالحاويات الأخرى.
- يجب تشغيل الحاوية في وضع عزل العملية. ولا يتم دعم وضع عزل Hyper-V.
- يجب وضع الحاوية على خادم Windows Server 2016 أو 2019 أو 2022 (Docker Host).
- يجب أن تتضمن الحاوية صورة Windows (Docker Image). لا يتم دعم Windows 10 وWindows 11. ولا يتم دعم صور Linux.

الإجراء المطلوب اتخاذه عند اكتشاف تهديد

إذا تم اكتشاف تهديد داخل حاوية، فسيطبق التطبيق الإجراء المحدد لمكون الحماية من تهديدات الملفات. يحتوي فحص الحاوية على إعدادات إضافية (انظر التعليمات أدناه). وإذا تم اكتشاف تهديد، يحظر التطبيق النشاط الخبيث وينفذ الإجراء المحدد (على سبيل المثال، محاولات تنظيف الكائن). ويمكن لبرنامج Kaspersky Endpoint Security إيقاف الحاوية إذا تعذر تنظيف الكائن المكتشف. وبشكل افتراضي، يتم تعطيل وظيفة إيقاف الحاوية.

كيفية تكوين فحص الحاويات في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.
4. انقر على **الإعدادات**.
5. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **إضافي**.
6. في القسم **فحص عمليات الملفات المنفذة في حاويات Windows**، كوّن إعدادات فحص الحاويات:
   - **إيقاف الحاوية إذا فشل التنظيف**. قد لا يمتلك التطبيق حقوق قراءة وكتابة كافية للكائن المكتشف. وفي هذه الحالة، يستحيل تنظيف أو حذف الكائن المكتشف. وإذا تم تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف ويوقف الحاوية. وإذا تم إلغاء تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف فقط.
   - **لا تفحص عمليات الملفات المنفذة في حاويات Windows**. في حالة تحديد خانة الاختيار، سيفحص التطبيق الحاوية فقط عند بدء تشغيل الحاوية. وإذا تم إلغاء تحديد خانة الاختيار، سيفحص التطبيق الحاوية باستمرار في الوقت الحقيقي.
7. احفظ تغييراتك.

كيفية تكوين فحص الحاويات في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Host Threat Protection** ← **File Threat Protection**.

5. تحت **Advanced settings**، حدد علامة التبويب **Performance**.

6. في القسم **Scan optimization**، كوّن إعدادات فحص الحاويات:

- **Stop container if disinfection fails**. قد لا يمتلك التطبيق حقوق قراءة وكتابة كافية للكائن المكتشف. وفي هذه الحالة، يستحيل تنظيف أو حذف الكائن المكتشف. وإذا تم تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف ويوقف الحاوية. وإذا تم إلغاء تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف فقط.

- **Do not scan file operations executed in Windows containers**. في حالة تحديد خانة الاختيار، سيفحص التطبيق الحاوية فقط عند بدء تشغيل الحاوية. وإذا تم إلغاء تحديد خانة الاختيار، سيفحص التطبيق الحاوية باستمرار في الوقت الحقيقي.

7. احفظ تغييراتك.

كيفية تكوين فحص الحاويات في واجهة التطبيق.

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 **فحص عمليات الملفات المنفذة في حاويات Windows**، كوّن إعدادات فحص الحاويات:

- **إيقاف الحاوية إذا فشل التنظيف**. قد لا يمتلك التطبيق حقوق قراءة وكتابة كافية للكائن المكتشف. وفي هذه الحالة، يستحيل تنظيف أو حذف الكائن المكتشف. وإذا تم تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف ويوقف الحاوية. وإذا تم إلغاء تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف فقط.

- **لا تفحص عمليات الملفات المنفذة في حاويات Windows**. في حالة تحديد خانة الاختيار، سيفحص التطبيق الحاوية فقط عند بدء تشغيل الحاوية. وإذا تم إلغاء تحديد خانة الاختيار، سيفحص التطبيق الحاوية باستمرار في الوقت الحقيقي.

4. 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 (على سبيل المثال، الملفات والتطبيقات)

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة مكون 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

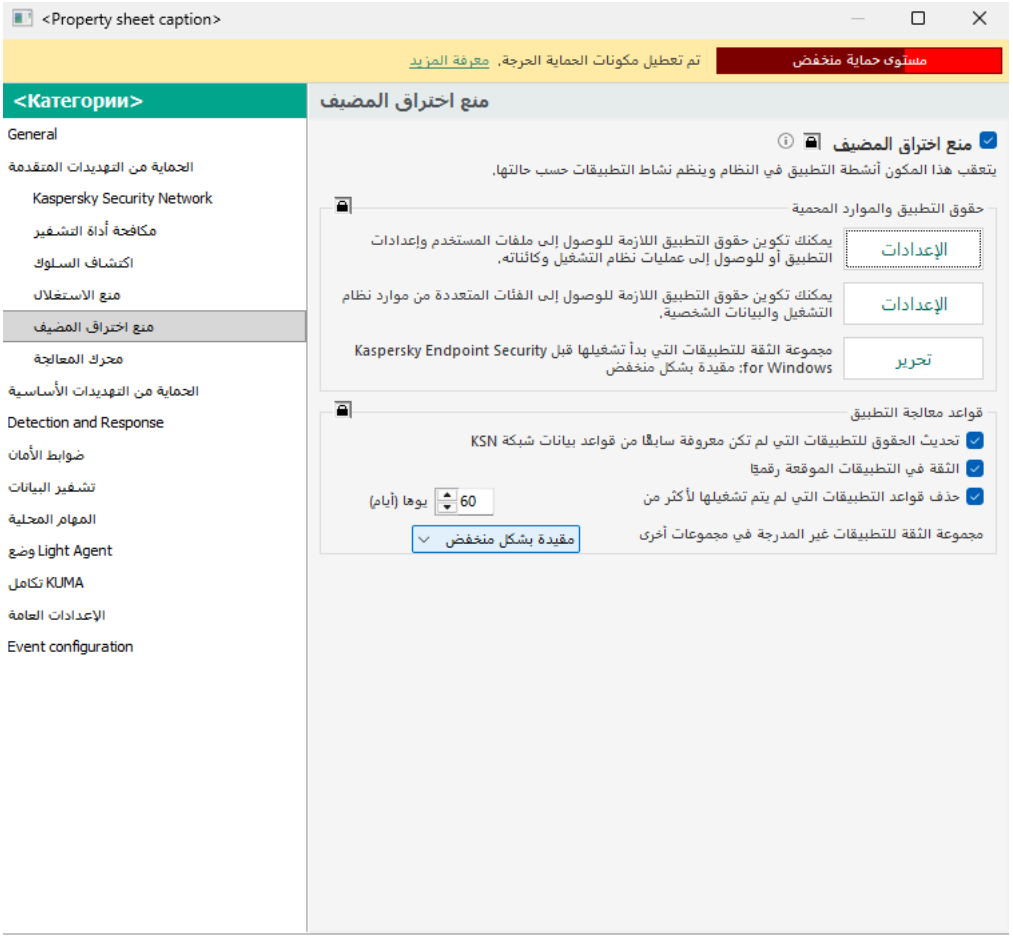
بشكل افتراضي، يتم تكوين مكون منع اختراق المضيف وتشغيله في الوضع الموصى به من خبراء Kaspersky.

كيفية تمكين أو تعطيل مكون منع اختراق المضيف في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. استخدم خانة الاختيار **منع اختراق المضيف** لتمكين المكون أو تعطيله.

5. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل مكون منع اختراق المضيف في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.

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

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

4. انتقل إلى **Host Threat Protection ← Host Intrusion Prevention**.

5. استخدم مفتاح تبديل **Host Intrusion Prevention ENABLED** 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 تريد أن يضع Kaspersky Endpoint Security لها كل التطبيقات غير المعروفة بشكل تلقائي. ويتم وضع التطبيقات التي كانت قيد التشغيل قبل بدء تشغيل Kaspersky Endpoint Security تلقائيًا في مجموعة الثقة تم ضبطه في إعدادات 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.

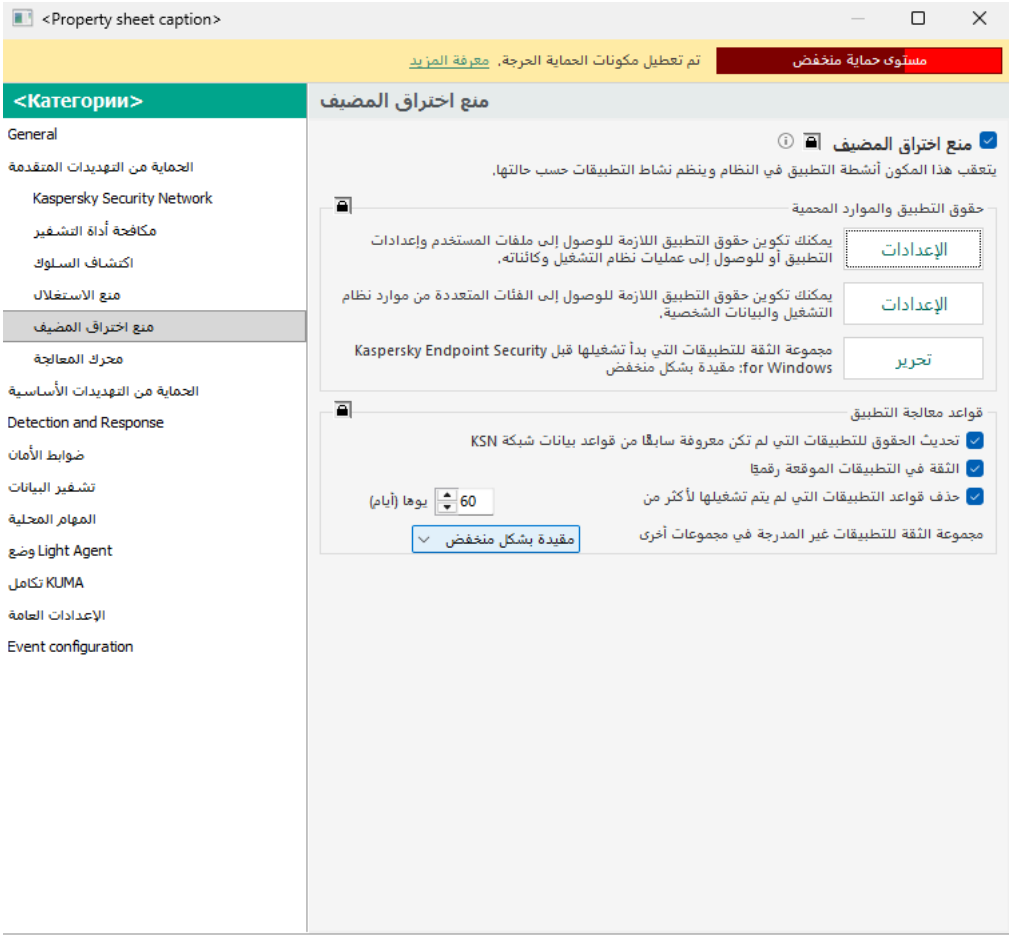
لا يوصي المتخصصون في Kaspersky بنقل التطبيقات من المجموعة الموثوقة التلقائية إلى مجموعة موثوقة أخرى. بدلاً من ذلك تستطيعتعديل الحقوق للطلبات الفردية إذا لزم الأمر.

كيفية تغيير مجموعة الثقة لتطبيق في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

5. حدد علامة التبويب **حقوق التطبيق**.

6. انقر على **إضافة**.

7. 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.

8. 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.

9. حدد التطبيق المطلوب.

10. في القائمة المنسدلة **إضافة التطبيق المحدد إلى مجموعة الثقة**، حدد مجموعة الثقة اللازمة للتطبيق.

11. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تغيير مجموعة الثقة لتطبيق في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Host Threat Protection** ← **Host Intrusion Prevention**.

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. قم بإنهاء 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 (مُعرَّف 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

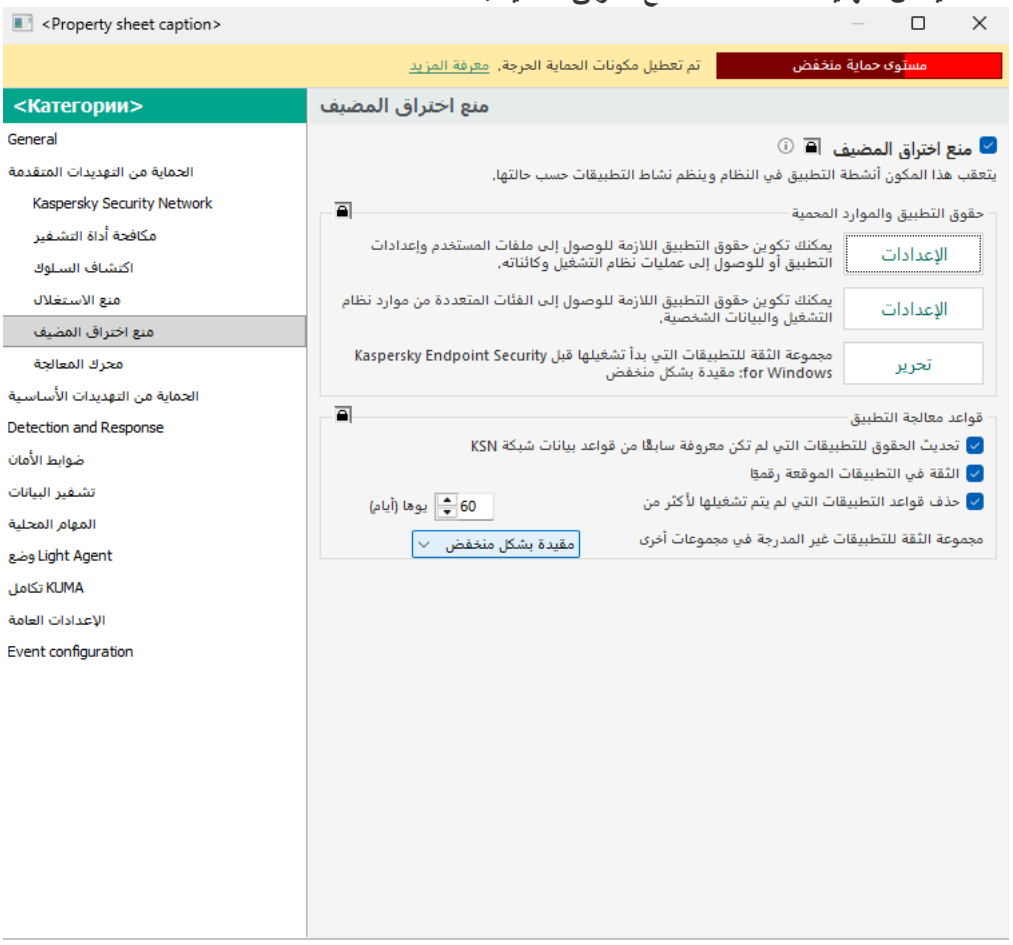
يتم إنشاء حقوق التطبيق المثلى لمجموعات ثقة مختلفة بشكل افتراضي. وترث إعدادات حقوق مجموعات التطبيق الموجودة في مجموعة الثقة قيمًا من إعدادات حقوق هذه المجموعة.

كيفية تغيير حقوق مجموعة الثقة في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

5. انتقل إلى علامة التبويب **حقوق التطبيق**.

6. حدد المجموعة الموثوقة اللازمة.

7. في قائمة السياق الخاصة بمجموعة الثقة، حدد **حقوق المجموعات**.

يفتح هذا خصائص مجموعة الثقة.

8. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد **الحقوق**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة مكون جدار الحماية باستخدام قواعد الشبكة.

9. للمورد ذي الصلة، في عمود الإجراء المتوافق، انقر بزر الماوس الأيمن لفتح قائمة السياق وتحديد الخيار اللازم: **توريث** أو **سماح** (✓) أو **منع** (⊘).

10. 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.

11. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تغيير حقوق مجموعة الثقة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Host Threat Protection** ← **Host Intrusion Prevention**.

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. انتقل إلى 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 مكون 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 **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد **الحقوق**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة مكون 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

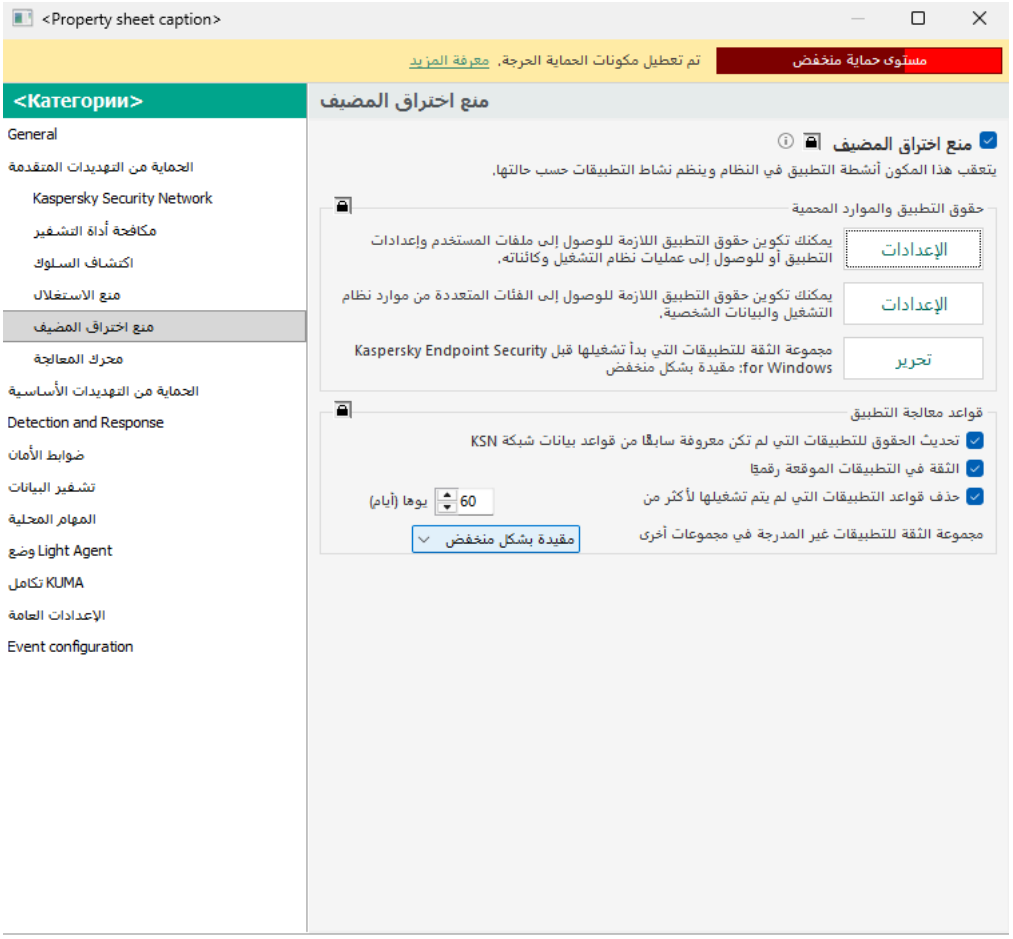
بالنسبة للتطبيقات التي بدأ تشغيلها قبل Kaspersky Endpoint Security، يتم التحكم في نشاط الشبكة فقط. يتم تنفيذ التحكم وفقًا لقواعد الشبكة المحددة في إعدادات جدار الحماية. لتحديد أي من قواعد الشبكة يجب تطبيقها لمراقبة نشاط الشبكة لمثل هذه التطبيقات، يجب تحديد مجموعة ثقة.

كيفية تحديد مجموعة ثقة للتطبيقات التي بدأت قبل Kaspersky Endpoint Security في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **تحرير**.

5. لضبط **Trust group for applications started before Kaspersky Endpoint Security**، حدد مجموعة الثقة المناسبة.

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تحديد مجموعة ثقة للتطبيقات التي بدأت قبل Kaspersky Endpoint Security في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.

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

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

4. انتقل إلى **Host Threat Protection ← Host Intrusion Prevention**.

5. لضبط **Trust group for applications started before Kaspersky Endpoint Security**، 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 **مجموعة الثقة للتطبيقات التي بدأ تشغيلها قبل Kaspersky Endpoint Security**، 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

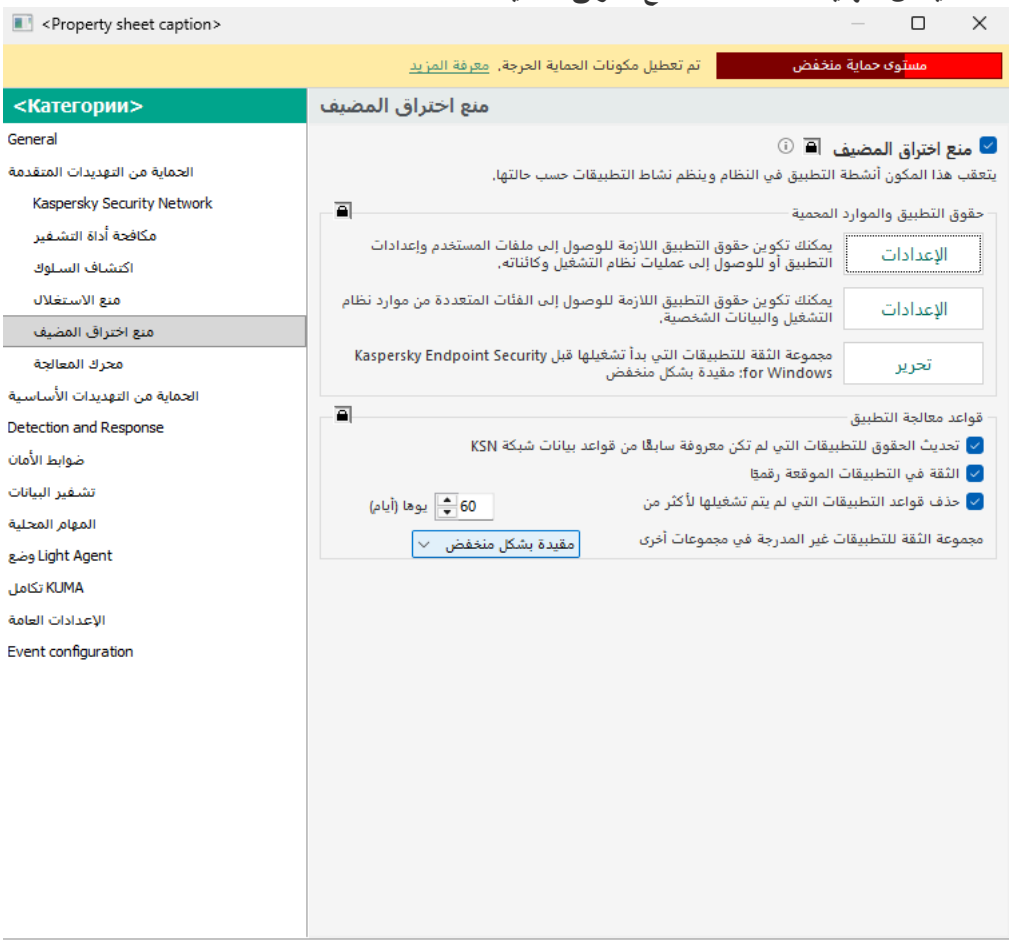
أثناء بدء التشغيل الأول لأحد التطبيقات، يحدد مكون منع اختراق المضيف مجموعة الثقة للتطبيق. وإذا لم يكن لديك وصول للإنترنت أو إذا لم يكن لدى Kaspersky Security Network أي معلومات حول هذا التطبيق، فسوف يضع Kaspersky Endpoint Security التطبيق في المجموعة مقيد بشكل منخفض افتراضيًا. وعند اكتشاف معلومات حول 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. في القسم **Application processing rules**، استخدم القائمة المنسدلة **Trust group for applications not included in other groups** 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.

5. استخدم خانة الاختيار **Update rights for previously unknown applications from KSN database** لتكوين التحديث التلقائي لحقوق التطبيقات غير المعروفة.

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تحديد مجموعة ثقة للتطبيقات غير المعروفة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Host Threat Protection** ← **Host Intrusion Prevention**.

5. في القسم **Application processing rules**، استخدم القائمة المنسدلة **Trust group for applications not included in other groups** 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 **Update rights for previously unknown applications from KSN database** 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 KSN** لتكوين التحديث التلقائي لحقوق التطبيقات غير المعروفة.

5. احفظ تغييراتك.

تحديد مجموعة ثقة للتطبيقات الموقعة رقمياً

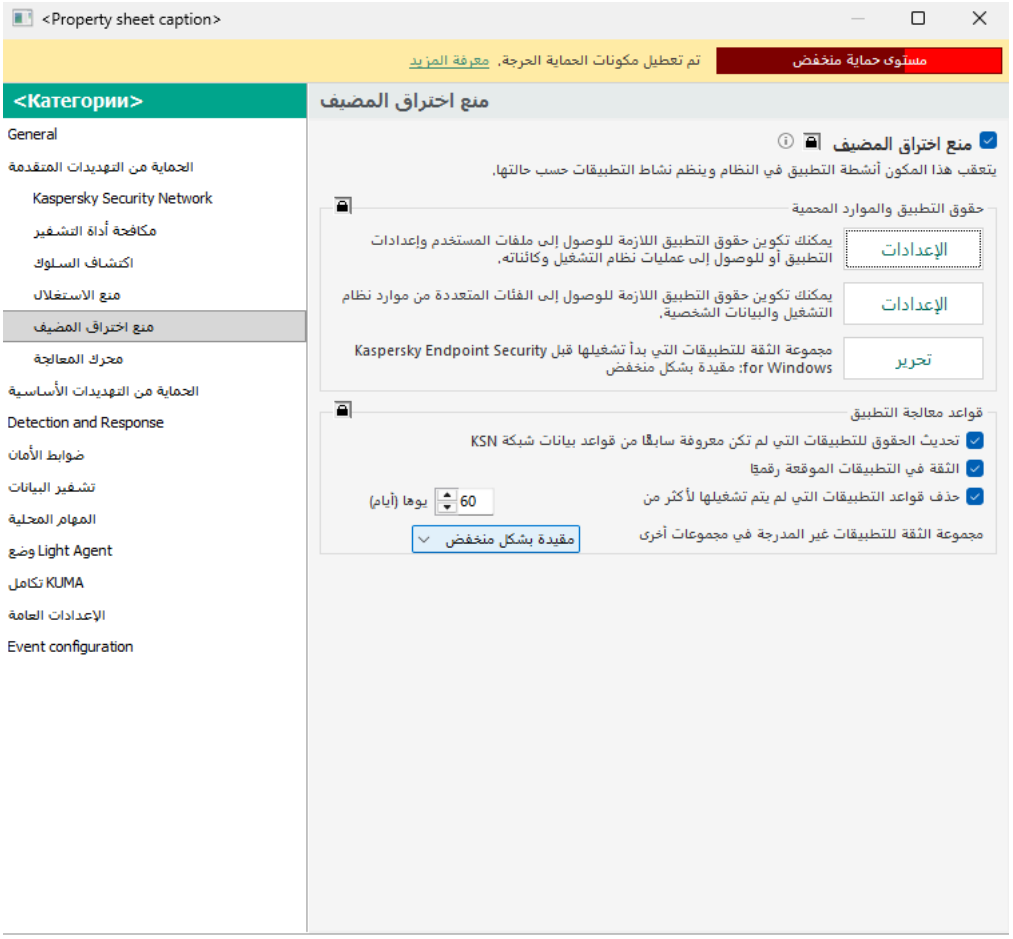
يضع Kaspersky Endpoint Security دائمًا التطبيقات الموقعة بواسطة شهادات Microsoft أو شهادات Kaspersky في المجموعة موثوق.

كيفية تحديد مجموعة ثقة للتطبيقات الموقعة رقمياً في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. في القسم **Application processing rules**، استخدم خانة الاختيار **Trust digitally signed applications** لتمكين التعيين التلقائي أو تعطيله لمجموعة الثقة Trusted 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.

5. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تحديد مجموعة ثقة للتطبيقات الموقعة رقميًا في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management ← Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Host Threat Protection ← Host Intrusion Prevention**.

5. في القسم **Application processing rules**، استخدم خانة الاختيار **Trust digitally signed applications** لتمكين التعيين التلقائي أو تعطيله لمجموعة الثقة Trusted 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 **Application processing rules**، استخدم خانة الاختيار **Trust digitally signed applications** لتمكين التعيين التلقائي أو تعطيله لمجموعة الثقة Trusted 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.

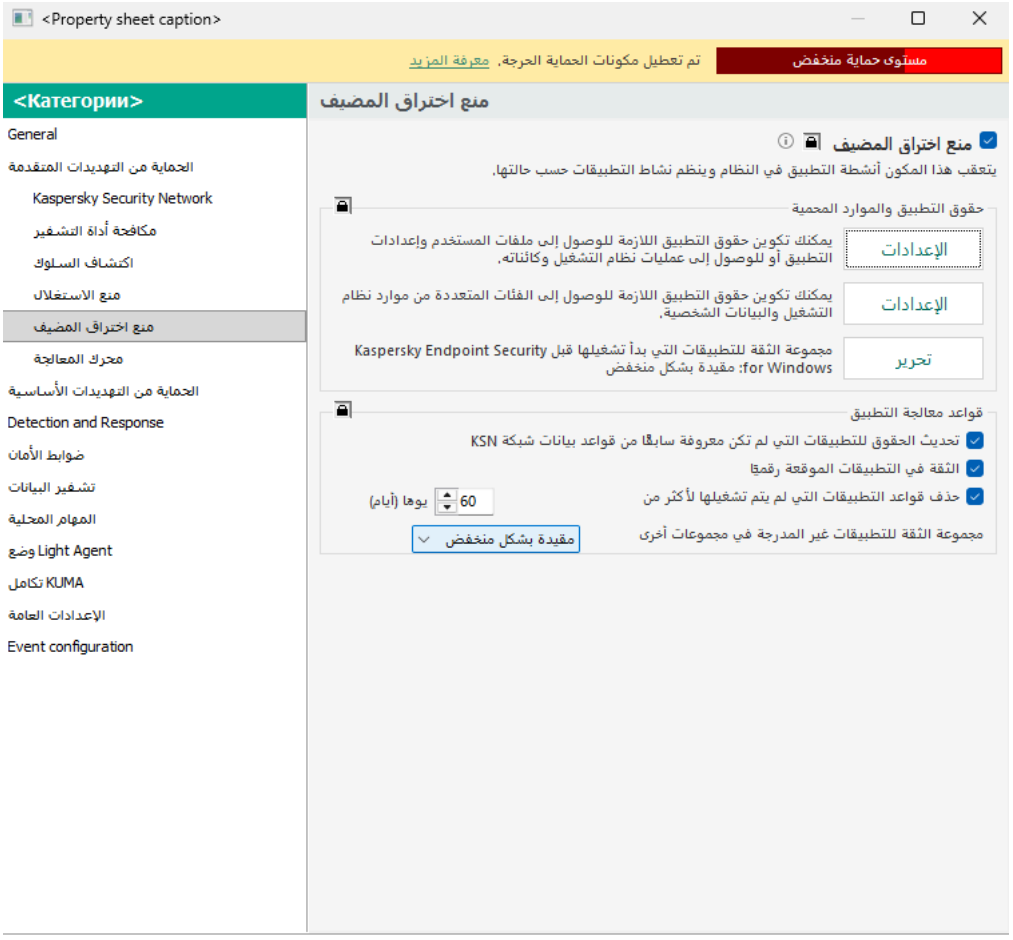
يتم توريث القواعد التي تنشؤها للتطبيقات بواسطة التطبيقات الفرعية. على سبيل المثال، إذا رفضت كل أنشطة الشبكة لبرنامج cmd.exe، فسيتم رفض كل أنشطة الشبكة أيضًا لبرنامج notepad.exe إذا بدأ تشغيله باستخدام cmd.exe. عندما لا يكون تطبيق تابعًا للتطبيق الذي يتم تشغيله منه، لا يتم وراثة القواعد.

كيفية تغيير حقوق التطبيق في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

5. انتقل إلى علامة التبويب **حقوق التطبيق**.

6. انقر على **إضافة**.

7. 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.

8. 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.

9. حدد التطبيق المطلوب.

10. في القائمة المنسدلة **إضافة التطبيق المحدد إلى مجموعة الثقة**، حدد **المجموعات الافتراضية** وانقر فوق **موافق**.

ستتم إضافة التطبيق إلى المجموعة الافتراضية.

11. حدد التطبيق ذي الصلة، ثم حدد **حقوق التطبيق** من قائمة السياق الخاصة بالتطبيق.

تفتح هذه الخطوة خصائص التطبيق.

12. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم العمليات باستخدام سجل نظام التشغيل وملفات المستخدم وإعدادات التطبيق، فحدد **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد **الحقوق**.

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة مكون جدار الحماية باستخدام قواعد الشبكة.

13. للمورد ذي الصلة، في عمود الإجراء المتوافق، انقر بزر الماوس الأيمن لفتح قائمة السياق وتحديد الخيار اللازم: **توريث** أو **سماح** (✓) أو **منع** (⊘).

14. 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.

15. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تغيير حقوق التطبيق في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Host Threat Protection** ← **Host Intrusion Prevention**.

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. انتقل إلى 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. قم بإنهاء 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 مكون 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 **سجل الملفات والنظام**.
- إذا كنت ترغب في تحرير حقوق مجموعة الثقة التي تنظم الوصول إلى عمليات وكائنات نظام التشغيل، فحدد **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.

المعلمة	الوصف
عدم فحص الملفات التي فتحها التطبيق	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. ويمكنك تكوين مراقبة نشاط التطبيق لمكونات مختلفة من Kaspersky Endpoint Security: • **عدم مراقبة مكونات الحماية والتحكم**. تتم مراقبة نشاط التطبيق من خلال المكونات التالية: اكتشاف السلوك ومنع الاستغلال ومنع اختراق المضيف ومحرك المعالجة وجدار الحماية. • **عدم مراقبة Managed Detection and Response وEndpoint Detection and Response**. ويتم مراقبة نشاط التطبيق بواسطة عميل MDR مدمج وعميل EDR (KATA) مدمج. • **عدم اعتراض الإدخال التفاعلي لوحدة التحكم لحل Endpoint Detection and Response**. 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 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. ويمكنك تطبيق الاستثناء بشكل متكرر. بحيث لا يراقب التطبيق نشاط سلسلة التطبيقات التابعة بالكامل.
السماح بالتفاعل مع واجهة تطبيق Kaspersky Endpoint Security	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. لا يدعم الإصدار 14.0 أو الإصدارات الأقدم من Kaspersky Endpoint Security استثناء حركة الشبكة إذا تم تحديد تجزئة لتطبيق موثوق به بدلاً من المسار.

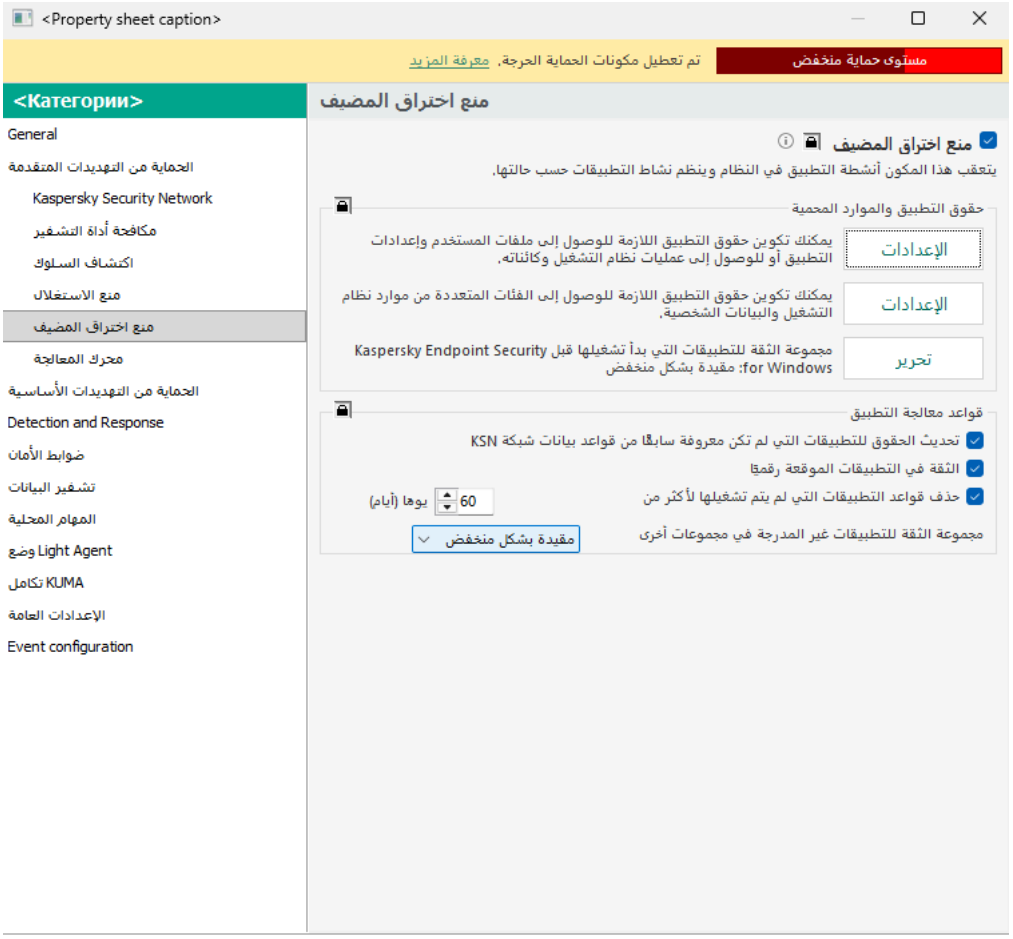
حماية موارد نظام التشغيل والبيانات الشخصية

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. في القسم **حقوق التطبيق والموارد المحمية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

5. انتقل إلى علامة التبويب **الموارد المحمية**.

سترى قائمة بالموارد المحمية في الجزء الأيمن من النافذة والحقوق المقابلة للوصول إلى هذه الموارد حسب مجموعة الثقة المحددة.

6. حدد فئة الموارد المحمية التي تريد إضافة مورد محمي جديد إليها.

إذا كنت ترغب في إضافة فئة فرعية، فانقر فوق **إضافة ← الفئة**.

7. انقر على الزر **إضافة**. في القائمة المنسدلة، حدد نوع المورد الذي تريد إضافته: **الملف أو المجلد** أو **مفتاح التسجيل**.

8. 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.

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إضافة مورد محمي في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Host Threat Protection** ← **Host Intrusion Prevention**.

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. انتقل إلى 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. في القسم **Group name** ، حدد 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. قم بإنهاء 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.

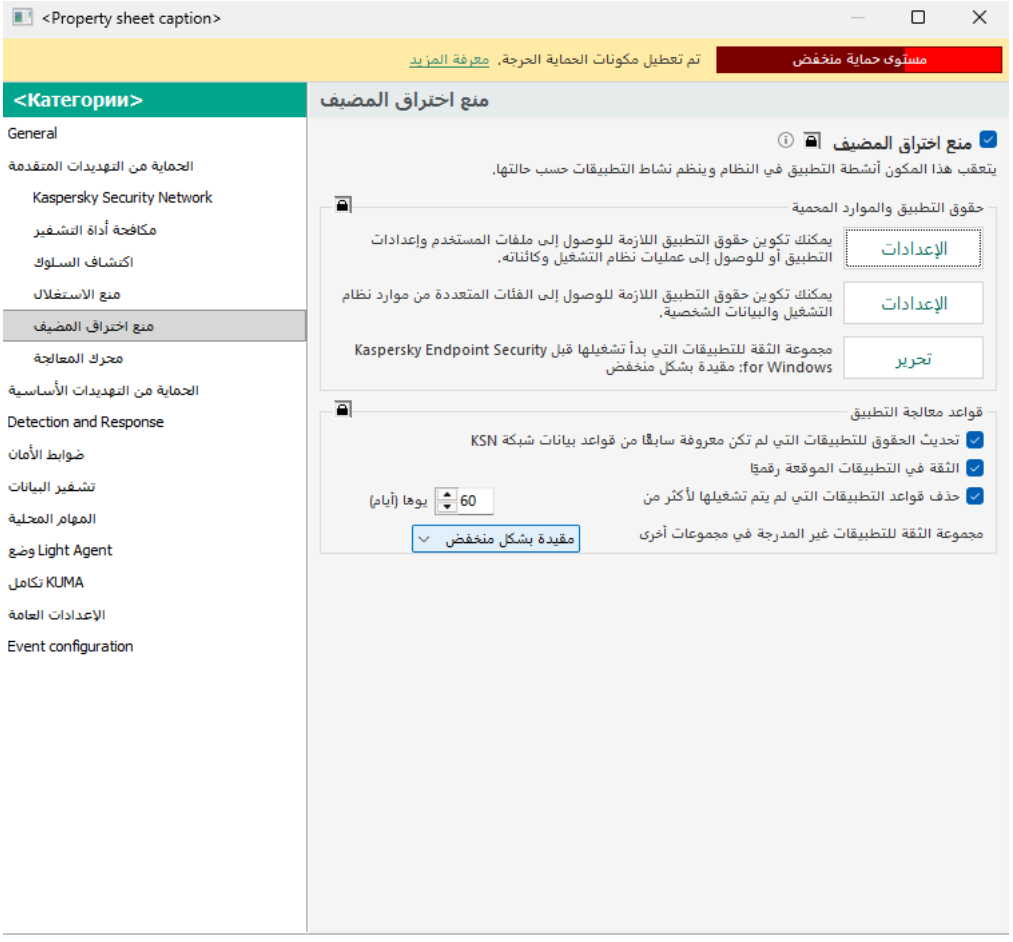
يقوم Kaspersky Endpoint Security تلقائيًا بحذف المعلومات عن التطبيقات غير المستخدمة بهدف المحافظة على موارد الكمبيوتر. يقوم Kaspersky Endpoint Security بحذف معلومات التطبيق وفق القواعد التالية:

- 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.

كيفية تكوين الحذف التلقائي للمعلومات حول التطبيقات غير المستخدمة في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع اختراق المضيف**.



إعدادات منع الاختراق

4. 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 يومًا (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 يومًا (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.

5. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين الحذف التلقائي للمعلومات حول التطبيقات غير المستخدمة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Host Threat Protection** ← **Host Intrusion Prevention**.

5. في القسم **Application processing rules**، نفذ أحد الإجراءات التالية:

- إذا كنت ترغب في تكوين الحذف التلقائي، حدد خانة الاختيار **Delete rules for applications that have not been started for longer than (days, 1 to 90)** 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 **Delete rules for applications that have not been started for longer than (days, 1 to 90)**.

  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 الأيام (من 1 إلى 90)** 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 الأيام (من 1 إلى 90)**.

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

لا يتم دعم وظيفة حماية الإشارة الصوتية ووظيفة حماية الوصول إلى كاميرا الويب على أجهزة الكمبيوتر القائمة على بنية Arm.

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.

بشكل افتراضي، يسمح Kaspersky Endpoint Security بتلقي تدفقات الصوت والفيديو فقط للتطبيقات من المجموعة موثوق. ولا يسمح للتطبيقات من المجموعات مقيد بشكل منخفض ومقيد بشكل عالٍ وغير موثوق بتلقي تدفق الصوت والفيديو من الأجهزة. 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.

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 بكمبيوتر ويتم 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.

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.



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.

كيفية تمكين أو تعطيل مكون منع هجوم BadUSB في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **منع هجمات BadUSB**.
4. استخدم خانة الاختيار **منع هجمات BadUSB** لتمكين المكون أو تعطيله.

5. في القسم **مصادقة جهاز USB عند التوصيل**، 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، يحظر التطبيق جهاز USB بعد المحاولة الخامسة غير الناجحة. ويعرض Kaspersky Endpoint Security مدة الحظر لجهاز USB. وبعد انقضاء هذا الوقت، سيصبح لديك مرة أخرى خمس محاولات لإدخال رمز المصادقة.

- **المهلة عند الوصول إلى الحد الأقصى لعدد المحاولات (بالدقائق)**. مدة حظر جهاز USB بعد العدد المحدد من المحاولات غير الناجحة لإدخال رمز المصادقة. القيم الصالحة من 1 إلى 180 (دقيقة).

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل مكون منع هجوم BadUSB في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **Host Threat Protection** ← **BadUSB Attack Prevention**.

5. استخدم مفتاح تبديل **BadUSB Attack Prevention ENABLED** لتمكين المكون أو تعطيله.

6. في القسم **Authorization of USB devices**، اضبط إعدادات الأمان لإدخال رمز التفويض:

- **Maximum number of USB device authorization attempts**. 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، يحظر التطبيق جهاز USB بعد المحاولة الخامسة غير الناجحة. ويعرض Kaspersky Endpoint Security مدة الحظر لجهاز USB. وبعد انقضاء هذا الوقت، سيصبح لديك مرة أخرى خمس محاولات لإدخال رمز المصادقة.

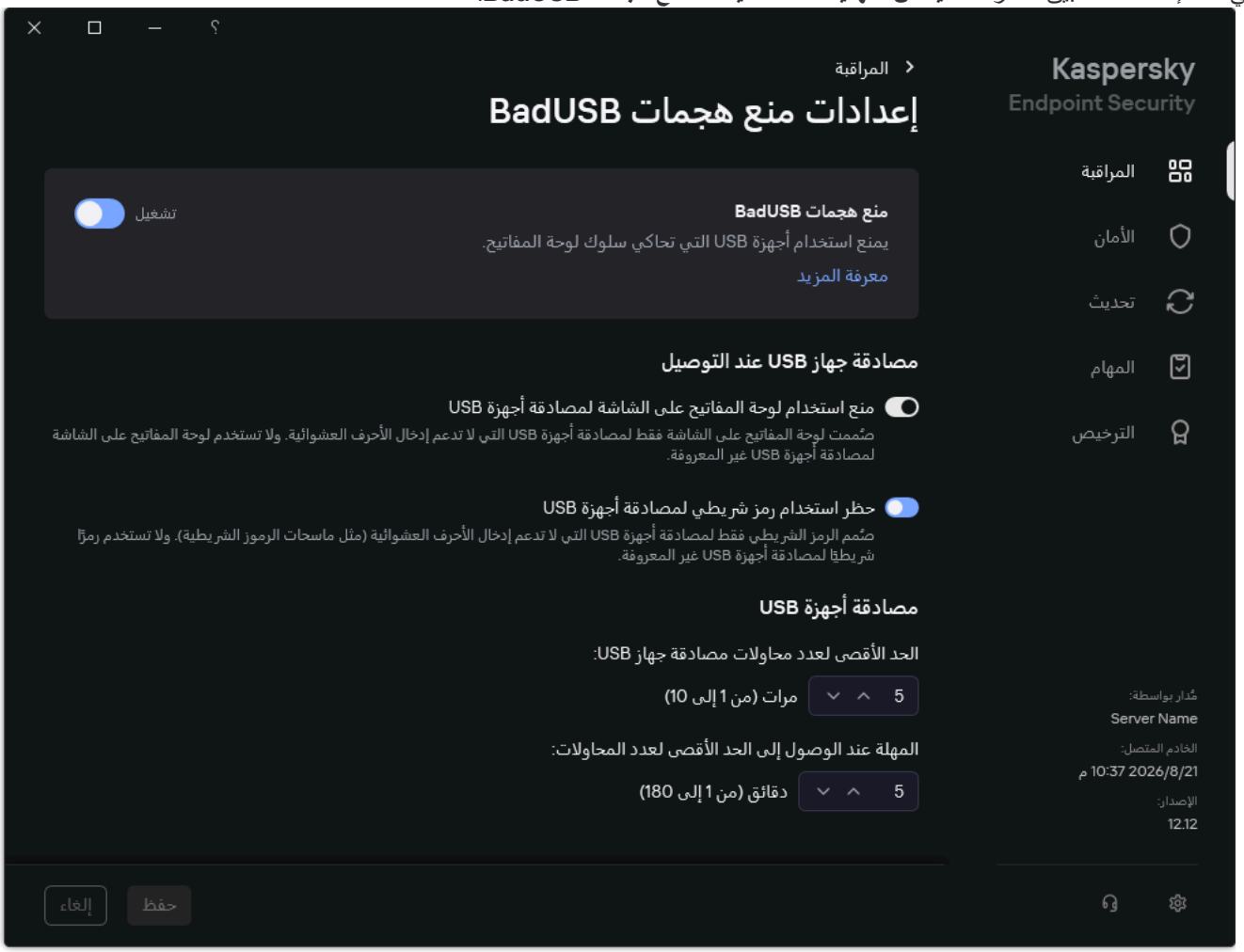
- **Timeout when reaching the maximum number of attempts (min)**. مدة حظر جهاز USB بعد العدد المحدد من المحاولات غير الناجحة لإدخال رمز المصادقة. القيم الصالحة من 1 إلى 180 (دقيقة).

7. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون منع هجوم BadUSB في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **منع هجمات BadUSB**.



إعدادات مكون منع هجمات BadUSB

3. استخدم مفتاح تبديل **منع هجمات BadUSB** لتمكين المكون أو تعطيله.

4. في القسم **مصادقة جهاز USB عند التوصيل**، 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، يحظر التطبيق جهاز USB بعد المحاولة الخامسة غير الناجحة. ويعرض Kaspersky Endpoint Security مدة الحظر لجهاز USB. وبعد انقضاء هذا الوقت، سيصبح لديك مرة أخرى خمس محاولات لإدخال رمز المصادقة.

- **المهلة عند الوصول إلى الحد الأقصى لعدد المحاولات**. مدة حظر جهاز USB بعد العدد المحدد من المحاولات غير الناجحة 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 (مثل الماسحات الضوئية للرمز الشريطي). من غير المستحسن استخدام لوحة المفاتيح على الشاشة للحصول على تصريح لأجهزة USB غير المعروفة.

كيفية السماح باستخدام لوحة المفاتيح على الشاشة أو منع استخدامها للحصول على إذن في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **منع هجمات BadUSB**.
4. استخدم خانة الاختيار **منع استخدام لوحة المفاتيح على الشاشة لمصادقة أجهزة USB** لمنع استخدام لوحة المفاتيح على الشاشة أو السماح باستخدامها للمصادقة.
5. احفظ تغييراتك.

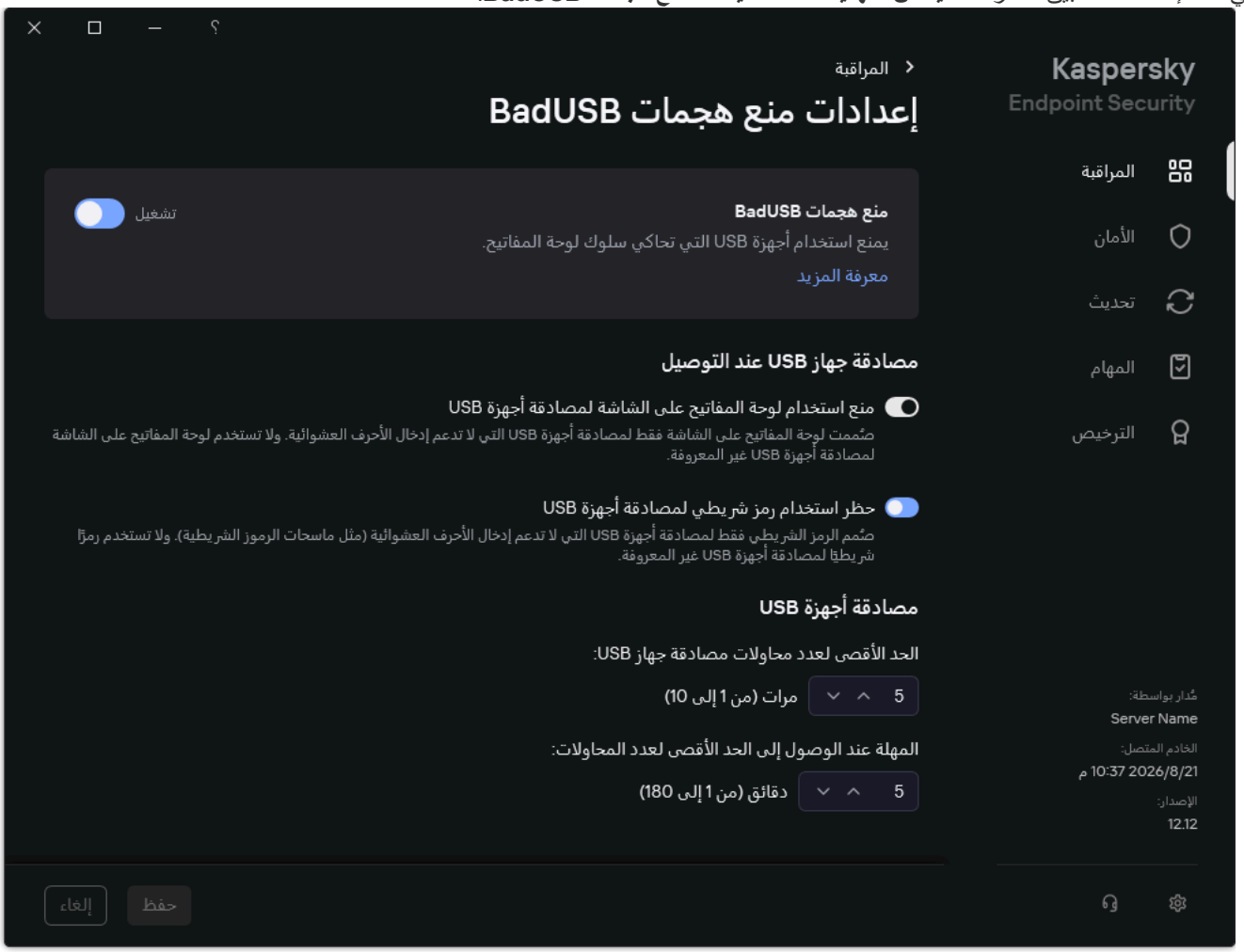
كيفية السماح باستخدام لوحة المفاتيح على الشاشة أو منع استخدامها للحصول على إذن في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Host Threat Protection** ← **BadUSB Attack Prevention**.
5. استخدم مفتاح التبديل **Prohibit use of On-Screen Keyboard for authorization of USB devices** لمنع استخدام لوحة المفاتيح على الشاشة أو السماح باستخدامها للمصادقة.
6. احفظ تغييراتك.

للسماح أو تعطيل استخدام لوحة المفاتيح على الشاشة للمصادقة في واجهة التطبيق:

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **منع هجمات BadUSB**.



إعدادات مكون منع هجمات BadUSB

3. استخدم مفتاح التبديل **منع استخدام لوحة المفاتيح على الشاشة لمصادقة أجهزة USB** لمنع استخدام لوحة المفاتيح على الشاشة أو السماح باستخدامها للمصادقة.

4. احفظ تغييراتك.



مصادقة أجهزة USB

إذن الماسح الضوئي للرمز الشريطي

عند توصيل ماسح ضوئي للرمز الشريطي بالكمبيوتر، يحدد مكون منع هجمات BadUSB هذا الجهاز كجهاز إدخال ويطالبك بمنح الإذن. ولمنح الإذن للماسح الضوئي للرمز الشريطي، يجب عليك مسح الرمز الشريطي المعروض على الشاشة. وينشئ التطبيق رمزًا شريطيًا بتنسيق Code39 المدعوم بواسطة معظم الماسحات الضوئية للرموز الشريطية ورموز الاستجابة السريعة.

يدعم Kaspersky Endpoint Security أيضًا طريقة مصادقة أخرى للماسح الضوئي للرمز الشريطي. وإذا كنت تستخدم أجهزة تعمل باللمس، فيمكنك استخدام لوحة مفاتيح على الشاشة لكتابة رمز. ولفعل ذلك، تحتاج إلى السماح بلوحة المفاتيح على الشاشة. وهذه الطريقة مناسبة، على سبيل المثال، في حالة الماسحات الضوئية للرموز الشريطية الثابتة المضمنة في ماكينات تسجيل النقد. ويتم منع طرق المصادقة الأخرى للماسح الضوئي للرموز الشريطية.

بشكل افتراضي لا يستخدم التطبيق رمزًا شريطيًا لمصادقة أجهزة USB.

كيفية تمكين مصادقة جهاز USB بواسطة الرمز الشريطي في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **منع هجمات BadUSB**.

5. استخدم خانة الاختيار **حظر استخدام رمز شريطي لمصادقة أجهزة USB** لمنع استخدام الرموز الشريطية للمصادقة.

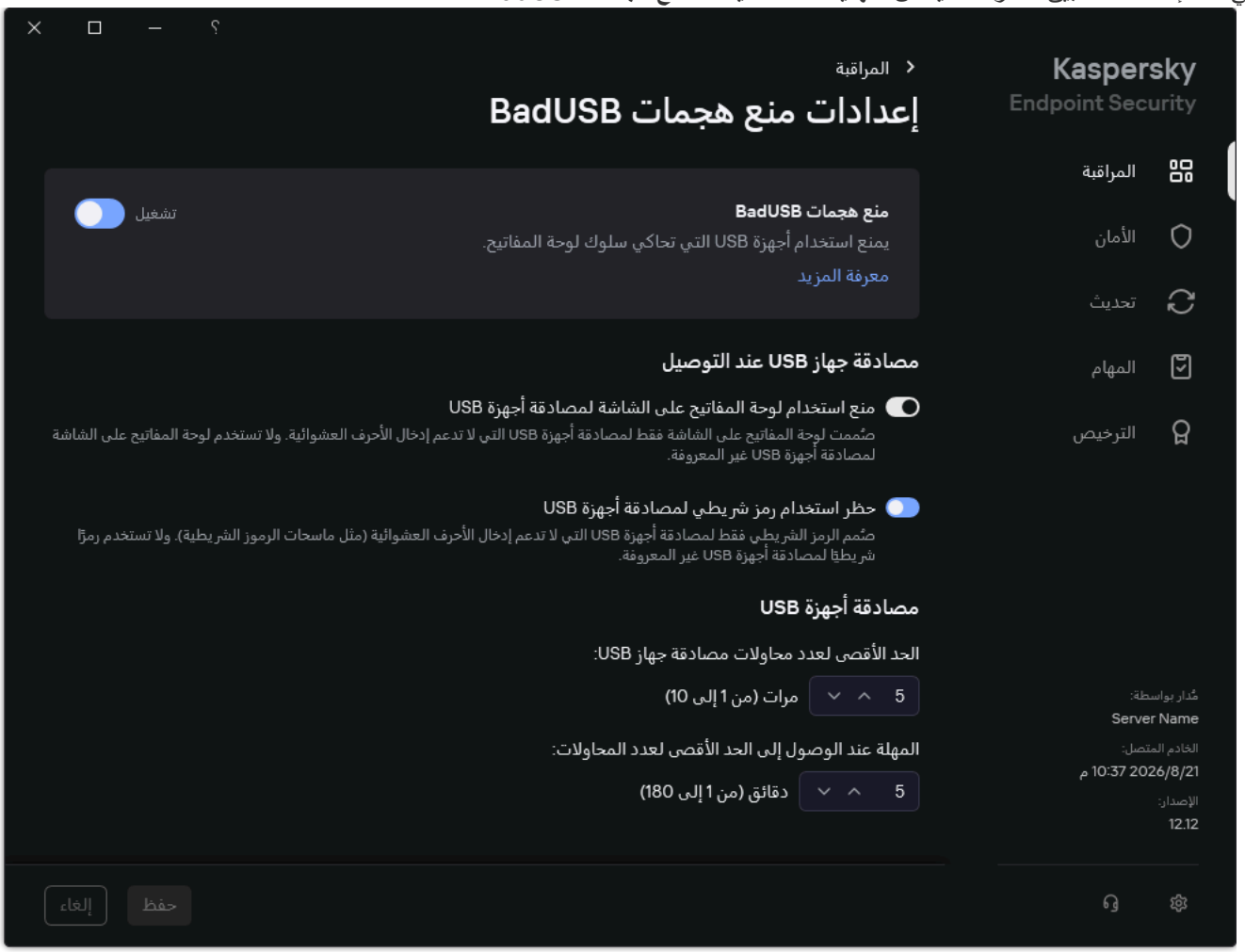
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين مصادقة جهاز USB بواسطة الرمز الشريطي في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Host Threat Protection** ← **BadUSB Attack Prevention**.
5. استخدم مفتاح التبديل **Prohibit use of a barcode for authorization of USB devices** لمنع استخدام الرموز الشريطية أو السماح باستخدامها للمصادقة.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين مصادقة جهاز USB عن طريق الرمز الشريطي في واجهة التطبيق

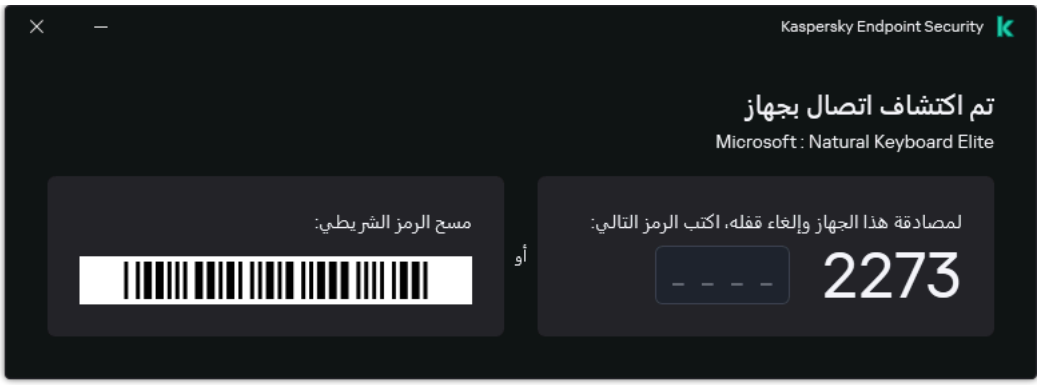
1. في نافذة التطبيق الرئيسية، انقر فوق الزر .
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **منع هجمات BadUSB**.



إعدادات مكون منع هجمات BadUSB

3. استخدم مفتاح التبديل **حظر استخدام رمز شريطي لمصادقة أجهزة USB** لمنع استخدام الرموز الشريطية أو السماح باستخدامها للمصادقة.

4. احفظ تغييراتك.

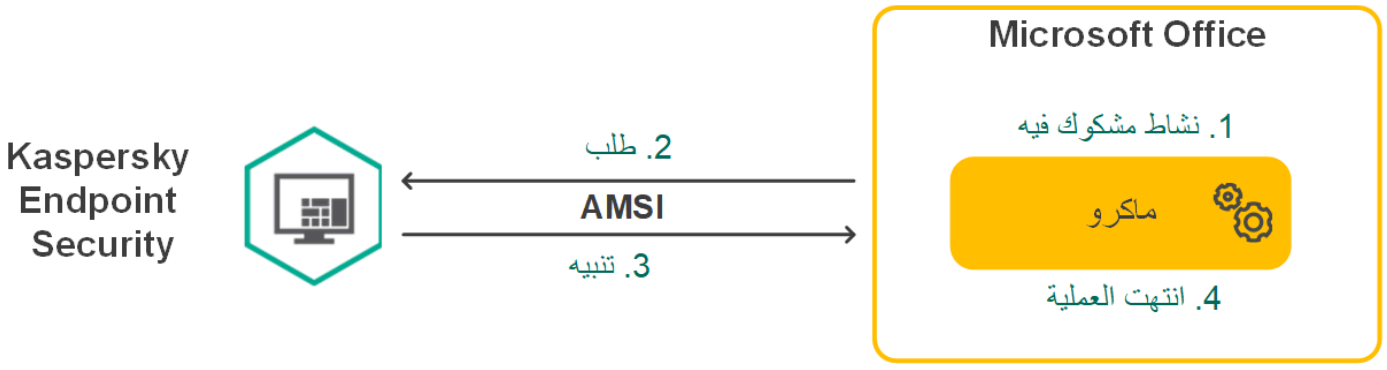


إذن الماسح الضوئي للرمز الشريطي

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.

يستطيع مكون حماية AMSI فقط اكتشاف التهديدات وإخطار تطبيق خارجي بالتهديد المكتشف. لا يسمح التطبيق الخارجي بعد استلام الإخطار بوجود تهديد بإجراءات مشكوك فيها (على سبيل المثال، ينهي الإجراء).



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 / Enterprise متعدد الجلسات؛
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise متعدد الجلسات؛
- Windows Server 2016 Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)

- Windows Server 2019 Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (بما في ذلك وضع Server Core)
- Windows Server 2025 Standard / Datacenter

تمكين حماية AMSI وتعطيلها

بشكل افتراضي، يتم تمكين حماية AMSI وتعمل في الوضع الموصى به بواسطة Kaspersky (انظر الجدول أدناه).

كيفية تمكين أو تعطيل حماية AMSI في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **أداة فحص AMSI**.
4. استخدم خانة الاختيار **أداة فحص AMSI** لتمكين المكون أو تعطيله.
5. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

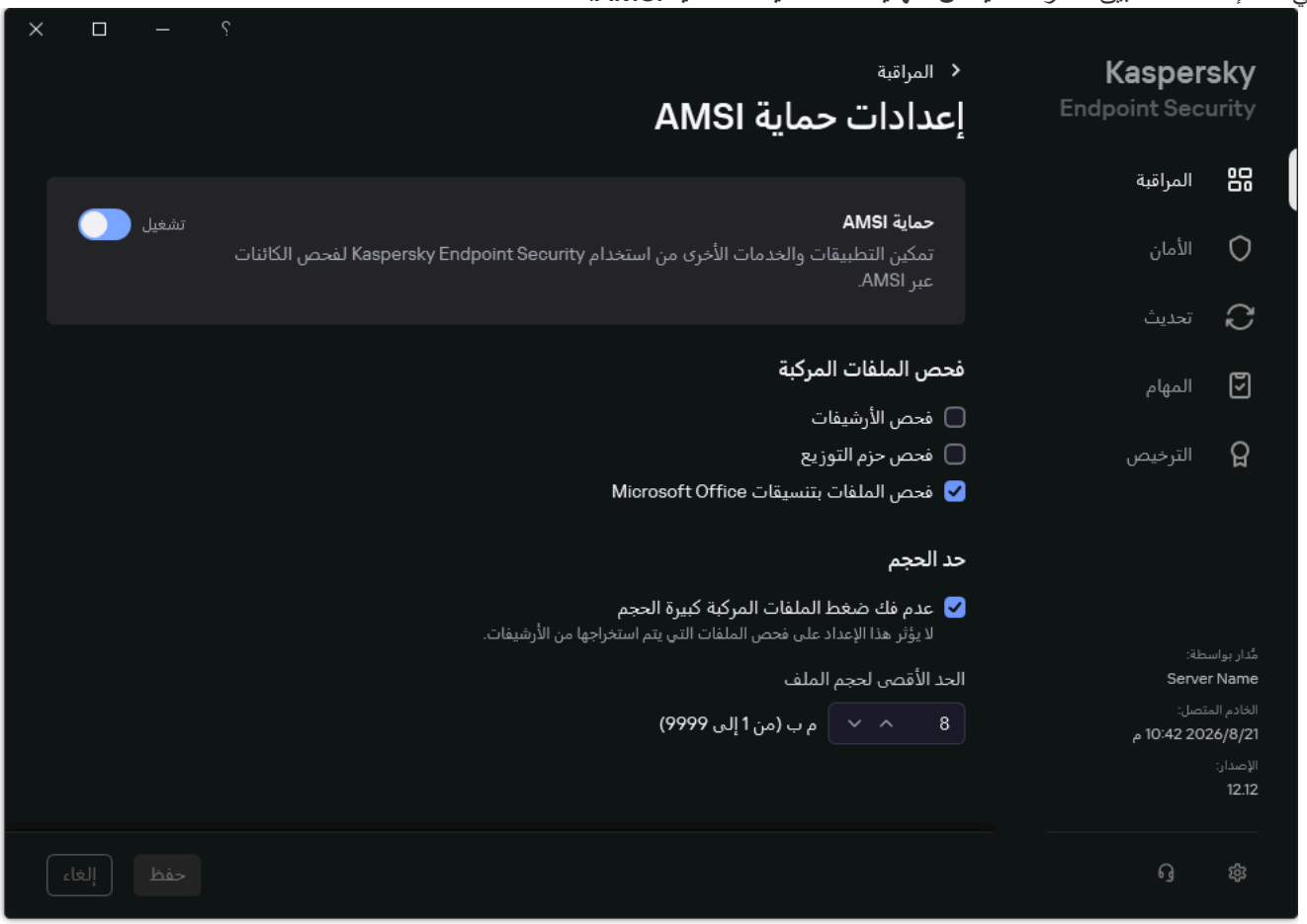
كيفية تمكين أو تعطيل حماية AMSI في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Host Threat Protection** ← **AMSI Protection**.
5. استخدم مفتاح تبديل **AMSI Protection ENABLED** لتمكين المكون أو تعطيله.
6. احفظ تغييراتك. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

كيفية تمكين أو تعطيل حماية AMSI في واجهة التطبيق

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.

إعدادات حماية AMSI الموصى بها من خبراء Kaspersky

المعلمة	القيمة	الوصف
فحص الأرشيفات	**إيقاف التشغيل**	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	**إيقاف التشغيل**	فحص حزم توزيع تطبيقات الجهات الخارجية.
فحص الملفات بتنسيقات Microsoft Office	**تشغيل**	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. ويفحص التطبيق 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	**الحد الأقصى لحجم الملف 8 م ب**	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.

تحسين فحص الملفات عن طريق حماية AMSI

يمكنك تحسين فحص الملفات: تقليل وقت الفحص وزيادة سرعة تشغيل أمان نقطة النهاية من Kaspersky. يمكنك تحديد الملفات المركبة التي تحتاج إلى فحص: أرشيفات أو حزم توزيع أو ملفات بتنسيقات Office. ويمكنك أيضًا تحديد حجم الملفات المركبة التي سيتم فحصها. لن يفك مكون الحماية AMSI حزمة الملفات المركبة التي يزيد حجمها عن الحجم المحدد.

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 المطلوب فحصها، وبالتالي زيادة سرعة عميلة الفحص.

كيفية تحسين فحص الملفات بواسطة حماية AMSI في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **أداة فحص AMSI**.
4. في القسم **فحص الملفات المركبة**، حدد أنواع الملفات المركبة التي تريد فحصها: ملفات الأرشيف، أو حِزم التثبيت، أو الملفات بتنسيقات office.
5. 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. 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.

6. احفظ تغييراتك. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

كيفية تحسين فحص الملفات بواسطة حماية AMSI.في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Host Threat Protection** ← **AMSI Protection**.
5. في القسم **Scan of compound files**، حدد أنواع الملفات المركبة التي تريد فحصها: ملفات الأرشيف، أو حِزم التثبيت، أو الملفات بتنسيقات office.
6. في القسم **Scan optimization**، نفذ أحد الإجراءات التالية:
   - لمنع مكون حماية AMSI من فك حزمة الملفات المركبة كبيرة الحجم، حدد خانة الاختيار **Size limits enabled** وحدد القيمة المطلوبة في الحقل. 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 **Size limits enabled**.

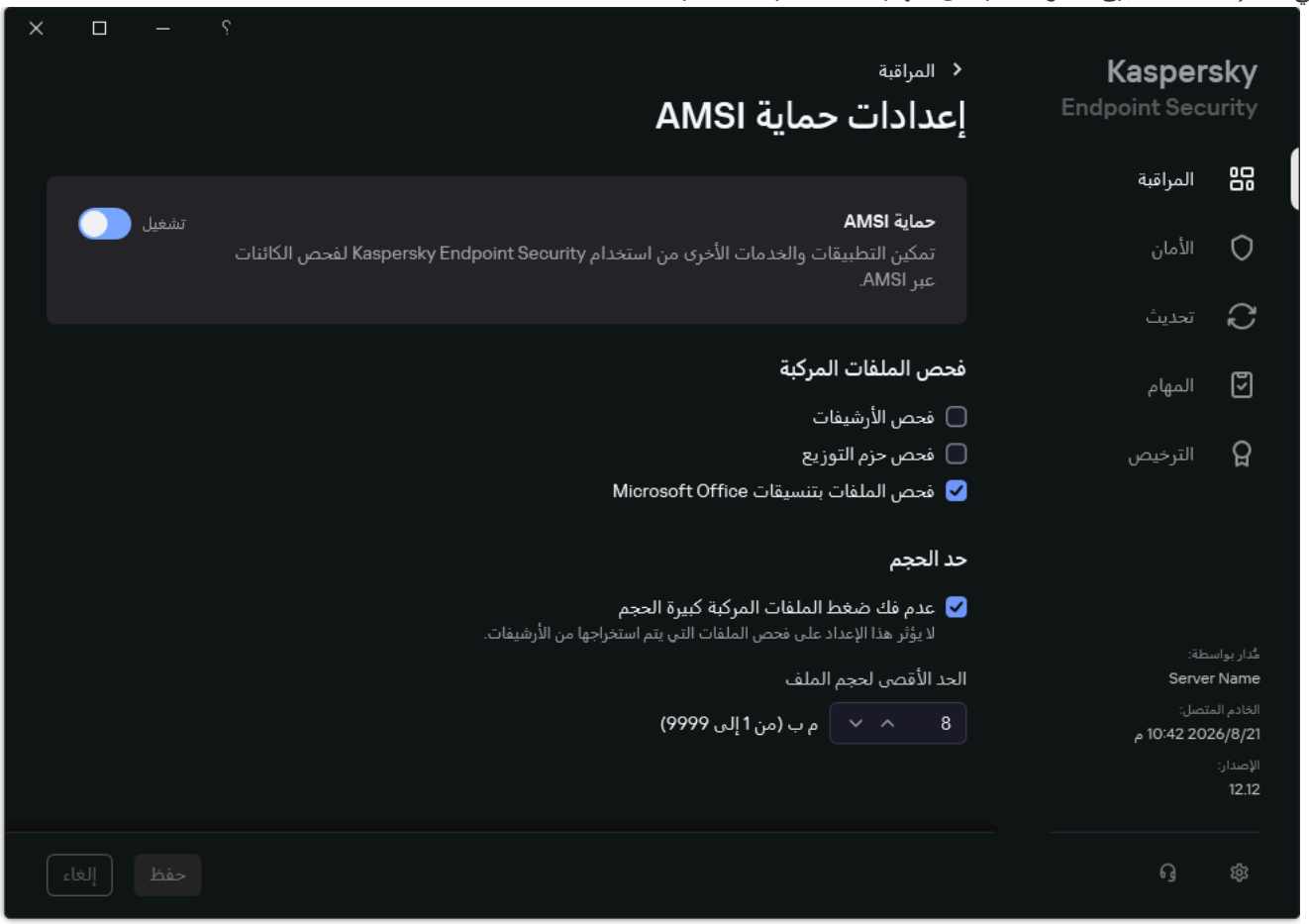
يفحص مكون حماية AMSI الملفات الكبيرة التي يتم استخراجها من الأرشيفات، بغض النظر عن تحديد خانة الاختيار **Size limits enabled** أم لا.

7. احفظ تغييراتك. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

كيفية تحسين فحص الملفات بواسطة حماية AMSI في واجهة التطبيق

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. 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.

الحماية من تهديدات الويب

يمنع مكون الحماية من تهديدات الويب تنزيلات الملفات الضارة عبر الإنترنت، ويحظر أيضًا الاتصال بمواقع الويب الضارة والخاصة بالتصيد الاحتيالي. 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.

لاستخدام الحماية من تهديدات الويب، يجب عليك إكمال التكوين الأولي للتطبيق:

- لمراقبة حركة مرور HTTPS، قم بتمكين فحص الاتصالات المشفرة (يتم التمكين بشكل افتراضي).
- حدد المنافذ التي يجب أن يراقبها Kaspersky Endpoint Security (بشكل افتراضي، يراقب التطبيق كل المنافذ).
- حدد التطبيقات التي تريد أن يراقب Kaspersky Endpoint Security حركة البيانات الخاصة بها. وتوجد معظم المستعرضات بالفعل في قائمة التطبيقات التي أوصت بها Kaspersky. وإذا كان المستعرض الخاص بك مفقودًا من القائمة، فقم بإضافته يدويًا.
- نوصي بإدخال برنامج نصي لتفاعل صفحة الويب في حركة مرور الويب (بشكل افتراضي، يتم تعطيل إدخال البرنامج النصي). يتيح هذا البرنامج النصي تسجيل أحداث الحماية من تهديدات الويب لسجل أحداث التطبيق، وسجل أحداث نظام التشغيل والتقارير.

عندما يحاول مستخدم فتح موقع إلكتروني ضار أو احتيالي، فإن Kaspersky Endpoint Security سوف يحجب الوصول إلى ذلك الموقع ويعرض تحذيرًا.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.
4. استخدم خانة الاختيار **الحماية من تهديدات الويب** لتمكين المكون أو تعطيله.

5. 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 كمبيوتر عبر 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 التطبيق 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 (انظر الجدول أدناه).

  يمكنك استعادة قيم مستويات الأمان المعينة مسبقًا بالنقر فوق الزر **افتراضيًا**.

6. 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.

7. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات الويب في Web Console

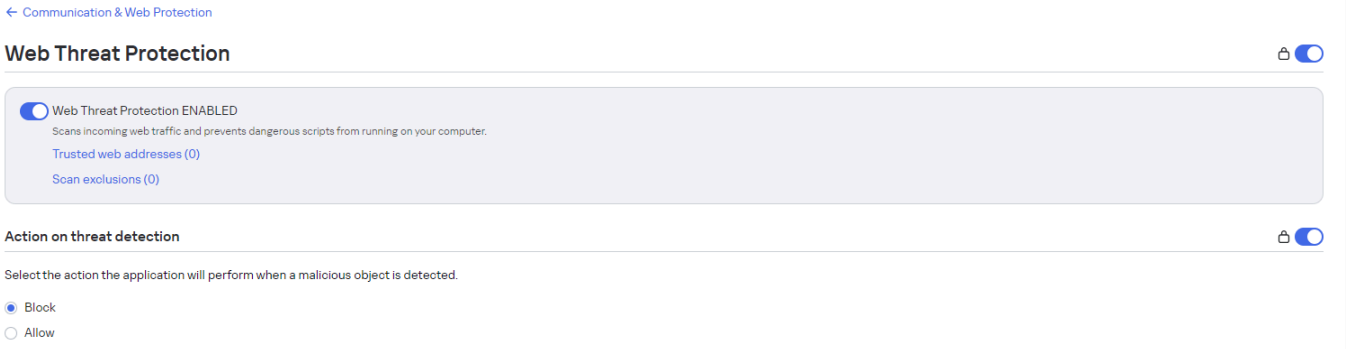
1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Communication & Web Protection** ← **Web Threat Protection**.



إعدادات الحماية من تهديدات الويب

5. استخدم مفتاح تبديل **Web Threat Protection ENABLED** 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 هذ الاختيار واكتشاف كائن مصاب في حركة المرور على الويب، يمنع مكون الحماية من تهديدات الويب الوصول إلى الكائن ويعرض رسالةً في المستعرض.
- **Allow, inform, or prompt for action (depends on OS)**. 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. إذا لزم الأمر، أنشئ قائمة بعناوين الويب الموثوقة.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ 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 كمبيوتر عبر 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 التطبيق 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 (انظر الجدول أدناه).

  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.

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 تهديدات الويب)	**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 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 Security 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.
4. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

5. 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.

6. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

4. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

5. في النافذة التي تفتح، 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.

6. 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.

7. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الويب**.

4. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

5. 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.

6. 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.

7. 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 يعترض مكون الحماية من تهديدات الويب 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 **Policies**.

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 هذا الخيار، 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. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إضافة عنوان ويب موثوق في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى القسم **Trusted Zone**.

5. في النافذة التي تفتح، انقر فوق الرابط **Web addresses**.

يفتح هذا نافذة تحتوي على قائمة بعنوان 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 JSON.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ 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 هذا الخيار، 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 وWeb Control 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية ← الحماية من تهديدات الويب**.
4. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.
5. في النافذة التي تفتح، حدد القسم **عناوين الويب الموثوقة**.
6. 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.
7. 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.
8. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة عناوين الويب الموثوقة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Communication & Web Protection ← Web Threat Protection**.

5. لتصدير قائمة الاستثناءات في القسم **Rules list**:

a. حدد عناوين الويب الموثوقة التي تريد تصديرها.

b. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة العناوين الموثوقة إلى ملف JSON في مجلد التنزيلات الافتراضي.

6. لاستيراد قائمة الاستثناءات في القسم **Rules list**:

a. انقر على الزر ← **Import**.

في النافذة التي تفتح، حدد ملف JSON 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 JSON.

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
- MyOffice Mail
- R7-Office Organizer

لفحص حركة البيانات في عملاء بريد Mozilla Thunderbird وMyOffice Mail وR7-Office Organizer، فإنك تحتاج إلى إضافة شهادة Kaspersky إلى مخزن الشهادات وتحديد مخزن الشهادات الخاص.

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 إصدارات 32 بت و64 بت من Outlook 2010 و2013 و2016 و2019 و2021 و2024 و365. وعلى أجهزة الكمبيوتر المستندة إلى بنية Arm، يدعم ملحق الحماية من تهديدات البريد إصدارات 32 بت و64 بت من Outlook 2016 وOutlook 2021 وOutlook 2024 وOutlook 365 for Arm64.

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. للحماية من تهديدات البريد، فإن التطبيق باستطاعته تطبيق 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.

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.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات البريد في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.
4. استخدم خانة الاختيار **الحماية من تهديدات البريد** لتمكين المكون أو تعطيله.
5. 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 التطبيق 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 **الإعدادات** وحدد إعدادات المكون الخاص بك (انظر الجدول أدناه).

يمكنك استعادة قيم مستويات الأمان المعينة مسبقًا بالنقر فوق الزر **افتراضيًا**.

6. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد الإجراء الذي سينفذه تطبيق Kaspersky Endpoint Security على الكائنات الضارة:

- **تنظيف؛ حذف إذا فشل التنظيف**. عند اكتشاف كائن مصاب في رسالة واردة أو صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف التطبيق الكائن المصاب. ويضيف التطبيق 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 التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. وإذا تعذّر تنظيف الكائن، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. عند اكتشاف كائن مصاب في رسالة صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. إذا تعذّر تنظيف الكائن، يحظر التطبيق إرسال الرسالة ويظهر عميل البريد خطأ.

- **منع**. في حالة اكتشاف كائن مصاب في رسالة واردة، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. إذا تم اكتشاف كائن مصاب في رسالة صادرة، يحظر التطبيق إرسال الرسالة، ويظهر عميل البريد خطأ.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات البريد في Web Console

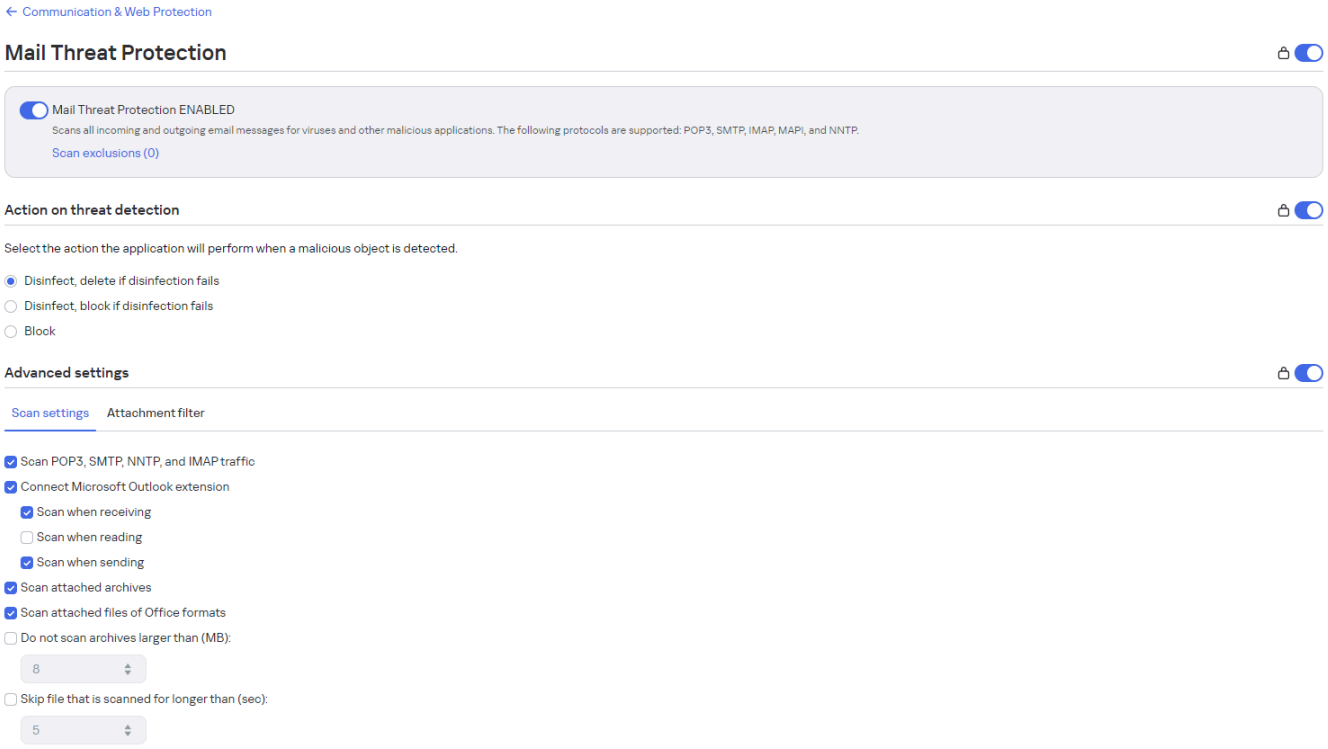
1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Communication & Web Protection** ← **Mail Threat Protection**.



إعدادات الحماية من تهديدات البريد

5. استخدم مفتاح تبديل **Mail Threat Protection ENABLED** لتمكين المكون أو تعطيله.

6. في القسم **Action on threat detection**، حدد الإجراء الذي سينفذه تطبيق Kaspersky Endpoint Security على الكائنات الضارة:

- **Disinfect, delete if disinfection fails**. عند اكتشاف كائن مصاب في رسالة واردة أو صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف التطبيق الكائن المصاب. ويضيف التطبيق معلومات عن الإجراء المتخذ إلى موضوع الرسالة، على سبيل المثال: [تمت معالجة الرسالة] <موضوع الرسالة>.

- **Disinfect, block if disinfection fails**. عند اكتشاف كائن مصاب في رسالة واردة، يحاول التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. وإذا تعذّر تنظيف الكائن، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. عند اكتشاف كائن مصاب في رسالة صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. إذا تعذّر تنظيف الكائن، يحظر التطبيق إرسال الرسالة ويظهر عميل البريد خطأ.

- **Block**. في حالة اكتشاف كائن مصاب في رسالة واردة، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. إذا تم اكتشاف كائن مصاب في رسالة صادرة، يحظر التطبيق إرسال الرسالة، ويظهر عميل البريد خطأ.

7. إذا لزم الأمر، حرر الإعدادات المتقدمة للحماية من تهديدات البريد.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل مكون الحماية من تهديدات البريد في واجهة التطبيق

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 التطبيق 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 (انظر الجدول أدناه).

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 تطبيق Kaspersky Endpoint Security على الكائنات الضارة:

- **تنظيف؛ حذف إذا فشل التنظيف**. عند اكتشاف كائن مصاب في رسالة واردة أو صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف التطبيق الكائن المصاب. ويضيف التطبيق 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 التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. وإذا تعذّر تنظيف الكائن، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. عند اكتشاف كائن مصاب في رسالة صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. إذا تعذّر تنظيف الكائن، يحظر التطبيق إرسال الرسالة ويظهر عميل البريد خطأ.

- **منع**. في حالة اكتشاف كائن مصاب في رسالة واردة، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. إذا تم اكتشاف كائن مصاب في رسالة صادرة، يحظر التطبيق إرسال الرسالة، ويظهر عميل البريد خطأ.

6. 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 Cached Exchange Mode. 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. ويفحص التطبيق 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 التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف التطبيق الكائن المصاب. ويضيف التطبيق 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 التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف التطبيق الكائن المصاب. ويضيف التطبيق 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 التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. وإذا تعذّر تنظيف الكائن، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. عند اكتشاف كائن مصاب في رسالة صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. إذا تعذّر تنظيف الكائن، يحظر التطبيق إرسال الرسالة ويظهر عميل البريد خطأ.

- **منع**. في حالة اكتشاف كائن مصاب في رسالة واردة، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. إذا تم اكتشاف كائن مصاب في رسالة صادرة، يحظر التطبيق 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. ويفحص التطبيق 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 التطبيق 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 م ب (من 1 إلى 9999)**. 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 (من 1 إلى 9999)**. إذا تم تحديد خانة الاختيار، فإن الوقت المخصص لفحص الأرشيفات المرفقة في رسائل البريد الإلكتروني يكون مقصورًا على المدة المحدد.

5. احفظ تغييراتك.

تصفية مرفقات رسائل البريد الإلكتروني

لا يتم تطبيق عامل 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. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Communication & Web Protection** ← **Mail Threat Protection**.

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.

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات البريد**.

4. في القسم **مستوى الأمان**، انقر على الزر **الإعدادات**.

5. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **عامل تصفية المرفقات**.

6. لتصدير قائمة الملحقات:

a. حدد الملحقات التي تريد تصديرها. لتحديد منافذ متعددة، استخدم مفتاحي **CTRL** أو **SHIFT**.

b. انقر على رابط **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.

7. لاستيراد قائمة الملحقات:

a. انقر على رابط **استيراد**.

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.

8. 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). يسمح الملحق بفحص الرسائل على مستوى عميل البريد بدلاً من مستوى البروتوكول. وبالإضافة إلى الرسائل، يتيح لك الملحق فحص الكائنات المستلمة عبر واجهة MAPI من مستودعات Microsoft Exchange (على سبيل المثال، الكائنات الموجودة في التقويم). ويجري هذا الفحص في عميل البريد.

يمكنك فتح إعدادات الحماية من تهديدات البريد من داخل Outlook، وتحديد الوقت الذي يتم فيه فحص رسائل البريد الإلكتروني للبحث عن الفيروسات والتهديدات الأخرى.

يدعم ملحق الحماية من تهديدات البريد إصدارات 32 بت و64 بت من Outlook 2010 و2013 و2016 و2019 و2021 و2024 و365.

وعلى أجهزة الكمبيوتر المستندة إلى بنية Arm، يدعم ملحق الحماية من تهديدات البريد إصدارات 32 بت و64 بت من Outlook 2016 وOutlook 2021 وOutlook 2024 وOutlook 365 for Arm64.

في برنامج Outlook، يتم أولاً فحص رسائل البريد الإلكتروني الواردة بواسطة GIFT (في حالة تحديد خانة الاختيار فحص حركة POP3 وSMTP وNNTP وIMAP 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.

عند فحص البريد الإلكتروني باستخدام ملحق الحماية من تهديدات البريد لبرنامج Outlook، نوصي باستخدام وضع التخزين المؤقت في خادم Exchange (Use Cached Exchange Mode). للمزيد من المعلومات التفصيلية حول وضع التبادل المخزن مؤقتًا والتوصيات حول استخدامه، يُرجى الرجوع إلى قاعدة معارف Microsoft.

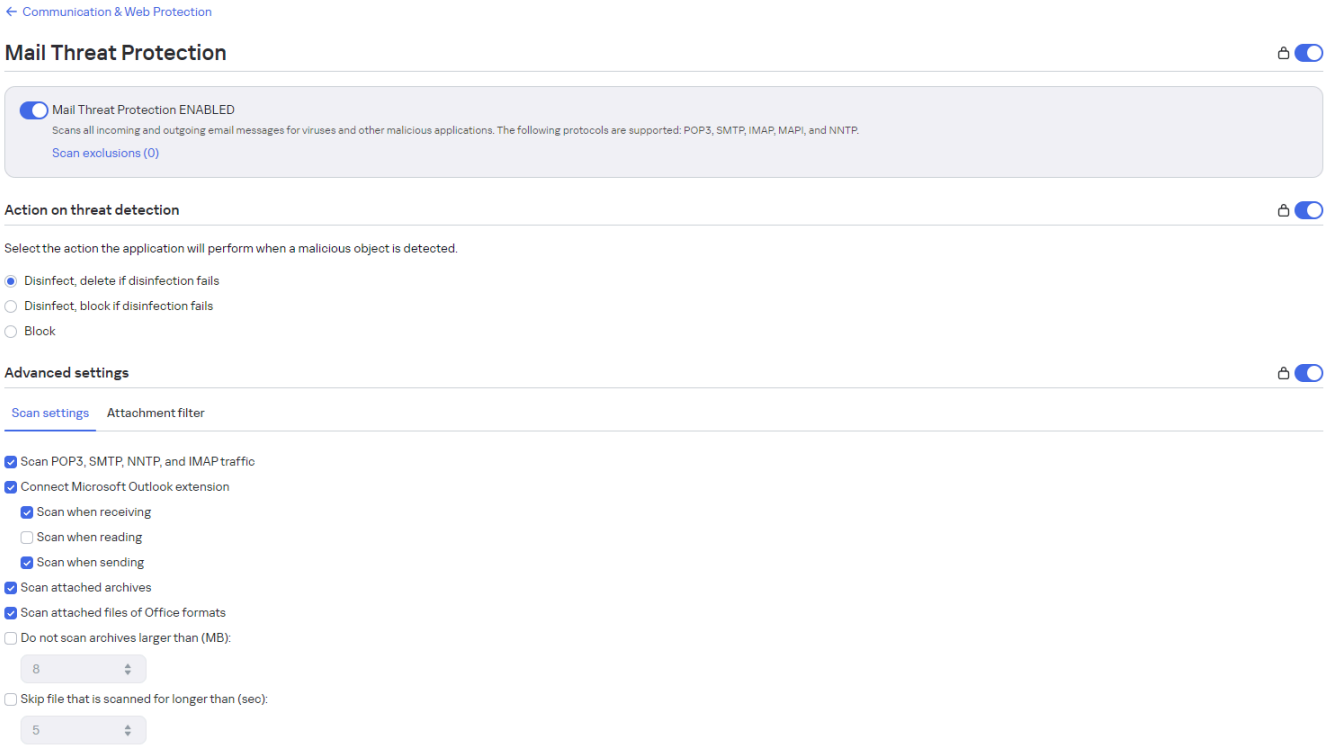
كيفية تكوين وضع التشغيل لملحق الحماية من تهديدات البريد لبرنامج Outlook في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
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، في القسم **الاتصال**، حدد خانة الاختيار **توصيل ملحق Microsoft Outlook**.
7. انقر على **الإعدادات**.
8. 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.
9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين وضع التشغيل لملحق الحماية من تهديدات البريد لبرنامج Outlook في وحدة Web Console

1. في نافذة Web Console الرئيسية، حدد علامة التبويب **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Communication & Web Protection** ← **Mail Threat Protection**.



إعدادات الحماية من تهديدات البريد

5. تحت **Advanced settings**، حدد علامة التبويب **Scan settings**.

6. حدد خانة الاختيار **Connect Microsoft Outlook extension**.

7. تكوين وضع الملحق:

- حدد خانة الاختيار **Scan when receiving** إذا كنت تريد أن يقوم ملحق الحماية من تهديدات البريد لبرنامج Outlook بفحص الرسائل الواردة بمجرد وصولها إلى علبة الوارد.
- حدد خانة الاختيار **Scan when reading** إذا كنت تريد أن يقوم ملحق الحماية من تهديدات البريد لبرنامج Outlook بفحص الرسائل الواردة عندما يفتحها المستخدم.
- حدد خانة الاختيار **Scan when sending** إذا كنت تريد أن يقوم ملحق الحماية من تهديدات البريد لبرنامج Outlook بفحص الرسائل الصادرة بمجرد إرسالها.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

فحص رسائل البريد الإلكتروني في Thunderbird وMyOffice وR7-Office

يفحص مكون الحماية من تهديدات البريد مرفقات رسائل البريد الإلكتروني الصادرة والواردة للحماية من الفيروسات والتهديدات الأخرى. بالنسبة لعملاء بريد Mozilla Thunderbird وMyOffice Mail وR7-Office Organizer، يحصل التطبيق على حق الوصول إلى الرسائل فقط على مستوى البروتوكول (POP3، SMTP، IMAP، NNTP).

لفحص حركة البيانات في عملاء بريد Mozilla Thunderbird وMyOffice Mail وR7-Office Organizer، فإنك تحتاج إلى إضافة شهادة Kaspersky إلى مخزن الشهادات وتحديد مخزن الشهادات الخاص.

لا يقوم مكون الحماية من تهديدات البريد بفحص الرسائل إذا كان عميل البريد مفتوحًا في مستعرض.

الحماية من تهديدات البريد في الوقت الحقيقي

تستطيع الحماية من تهديدات البريد فحص كل من الرسائل الواردة والصادرة. 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. 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>.

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.

فحص البرامج الضارة في قواعد بيانات البريد

تمنع ميزة "الحماية من تهديدات البريد" إصابة الكمبيوتر على مستوى البروتوكول، لكن إذا كان الكمبيوتر قد أصيب قبل تثبيت Kaspersky Endpoint Security، فقد يكتشف التطبيق التهديد في قواعد بيانات البريد باستخدام مهمة فحص البرامج الضارة. ولا ينظف التطبيق أو يحذف الملفات المصابة في قواعد بيانات البريد، بغض النظر عن إعدادات المهمة. ويرجع ذلك إلى أن Kaspersky Endpoint Security لا يحلل الرسائل الواردة من Thunderbird وMyOffice وP7-Office إلى أجزائها (الرأس ونَص الرسالة والمرفقات) بالطريقة نفسها المتبعة مع الرسائل الواردة من Microsoft Office Outlook. ويضيف التطبيق فقط معلومات عن الكائنات المكتشفة إلى قائمة التهديدات النشطة.

للقضاء على التهديدات النشطة:

1. يمكنك العثور على الرسالة التي تحتوي على الكائن المكتشف في واجهة عميل البريد وحذفها يدويًا.

ويعرض التطبيق معلومات عن الكائن المكتشف في قائمة التهديدات النشطة.

مثال على بطاقة الكائن المكتشف:

!	HEUR:Trojan.PDF.Phish.gen الكائن: C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox//[From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf

2. نفذ عملية ضغط قاعدة البيانات.

عند حذف رسالة في واجهة المستخدم، يضيف عميل البريد علامة حذف فقط. ويحذف عميل البريد بالفعل الرسالة فقط بعد ضغط قاعدة البيانات. وللحصول على تفاصيل عن ضغط قاعدة البيانات، راجع تعليمات عميل البريد الخاص بك (على سبيل المثال، Mozilla Thunderbird).

3. قم بتشغيل مهمة فحص البرامج الضارة مرة أخرى وتأكد من عدم وجود التهديد.

إذا لم يكن حذف الرسائل التي تحتوي على ملفات مصابة متاحًا في الوقت الحالي لأي سبب من الأسباب، فيمكنك معالجة هذه التهديدات في واجهة مستخدم Kaspersky Endpoint Security. وبالنسبة لملفات عميل البريد الإلكتروني، لديك خياران لمعالجة التهديد: **تجاهل** و**إضافة إلى الاستثناءات**. ولمنع التطبيق من إضافة هذه الكائنات إلى قائمة التهديدات النشطة أثناء إعادة الفحص، أضفها إلى قائمة الاستثناءات من الفحص.

الحماية من تهديدات الشبكة

يراقب مكون الحماية من تهديدات الشبكة (يسمى أيضًا Intrusion Detection System، IDS) حركة شبكة الاتصال الواردة للبحث عن خاصية النشاط لهجمات الشبكة. عندما يكتشف التطبيق محاولة هجوم على الشبكة على كمبيوتر مستخدم، فإنه يحظر اتصال الشبكة مع الكمبيوتر المهاجم. وتتوفر أوصاف لأنواع هجمات الشبكة المعروفة حاليًا وطرق إبطالها في قواعد بيانات التطبيق. 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. يراقب Kaspersky Endpoint Security حركة شبكة الاتصال الواردة للبحث عن خاصية النشاط لهجمات الشبكة ويمنع الهجمات.

كيفية تمكين أو تعطيل الحماية من تهديدات الشبكة في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.

4. استخدم خانة الاختيار **الحماية من تهديدات الشبكة** لتمكين المكون أو تعطيله.

5. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

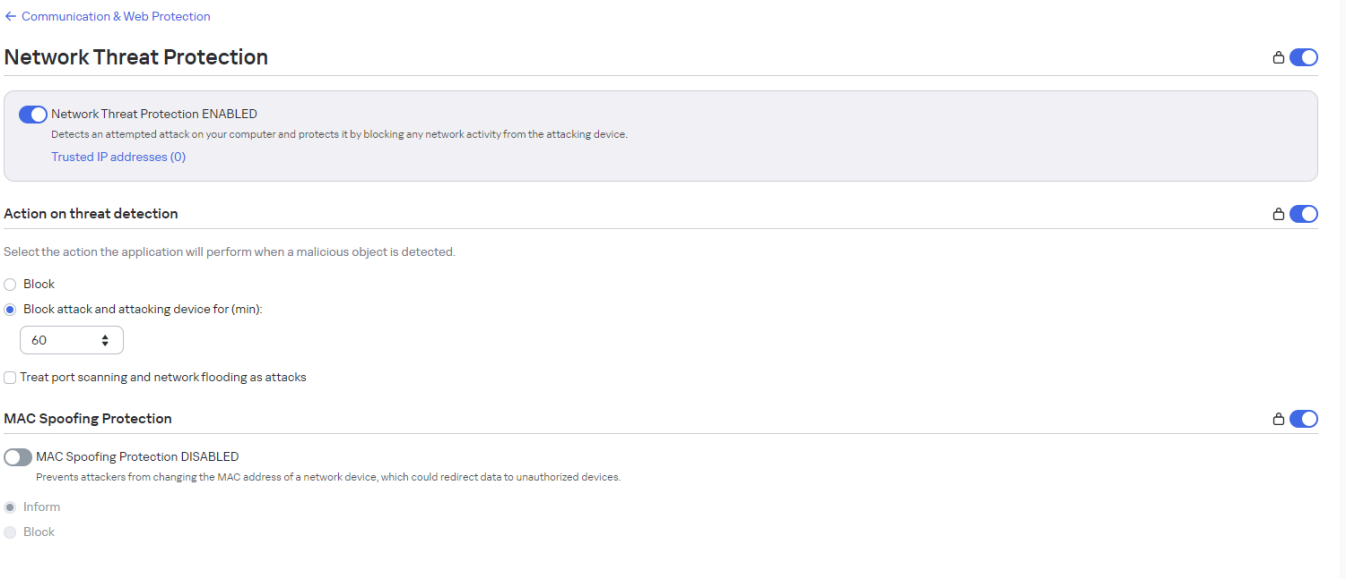
كيفية تمكين أو تعطيل الحماية من تهديدات الشبكة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **Communication & Web Protection** ← **Network Threat Protection**.



إعدادات الحماية من تهديدات الشبكة

5. استخدم مفتاح تبديل **Network Threat Protection ENABLED** لتمكين المكون أو تعطيله.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل الحماية من تهديدات الشبكة في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.



إعدادات الحماية من تهديدات الشبكة

3. استخدم مفتاح تبديل **الحماية من تهديدات الشبكة** لتمكين المكون أو تعطيله.

4. احفظ تغييراتك.

منع الكمبيوتر المهاجم

في حالة تمكين مكون الحماية من تهديدات الشبكة، يمنع Kaspersky Endpoint Security تهديدات الشبكة تلقائيًا. بالإضافة إلى ذلك، يستطيع التطبيق منع الكمبيوتر المهاجم وتقييد إرسال حزم شبكة الاتصال لفترة زمنية معينة. وافتراضيًا، يمنع Kaspersky Endpoint Security الكمبيوتر لمدة ساعة واحدة.

كيفية منع الكمبيوتر المهاجم في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية ← الحماية من تهديدات الشبكة**.

4. تحت **إعدادات الحماية من تهديدات الشبكة**، حدد خانة الاختيار **حظر أجهزة الهجوم لمدة N دقيقة**.

في حالة تمكين هذا الخيار، 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.

5. قم بتعيين مدة حظر مختلفة لجهاز كمبيوتر مهاجم في الحقل الموجود على يسار خانة الاختيار **حظر أجهزة الهجوم لمدة N دقيقة**.

6. احفظ تغييراتك.

كيفية منع كمبيوتر مهاجم في Web Console

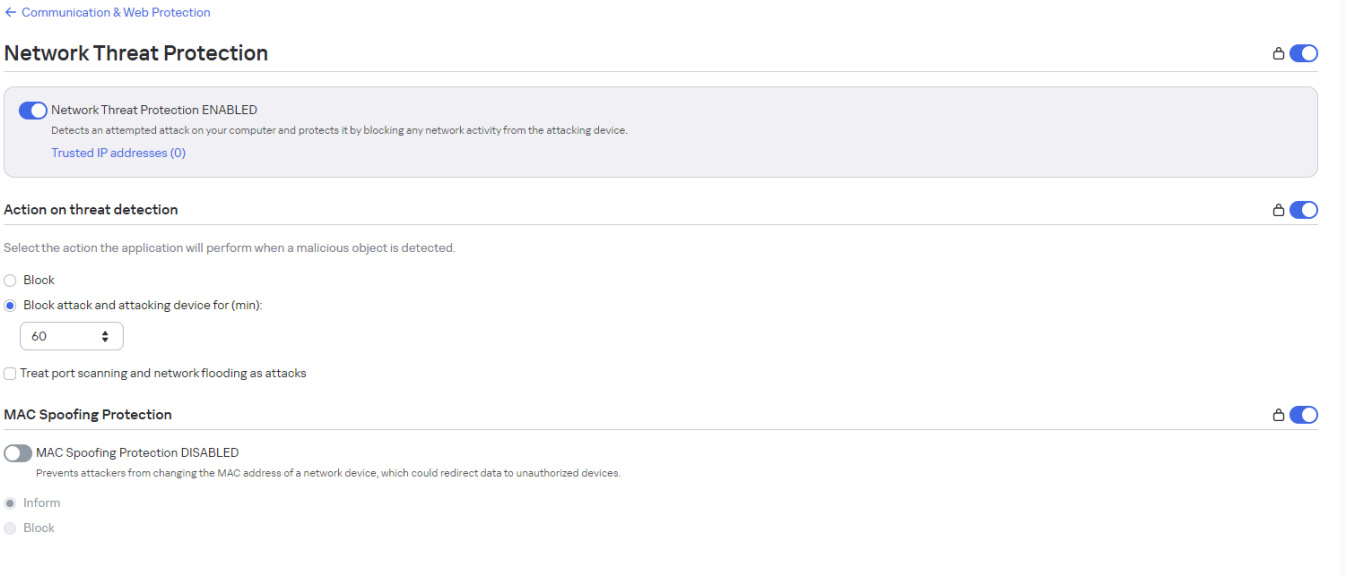
1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Communication & Web Protection** ← **Network Threat Protection**.



إعدادات الحماية من تهديدات الشبكة

5. في القسم **Action on threat detection**، حدد خانة الاختيار **Block attack and attacking device for (min)**.

في حالة تمكين هذا الخيار، 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.

6. قم بتغيير مدة المنع للكمبيوتر المهاجم.

7. احفظ تغييراتك.

كيفية منع الكمبيوتر المهاجم في واجهة المستخدم الخاصة بالتطبيق

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.



إعدادات الحماية من تهديدات الشبكة

3. قم بتشغيل مفتاح **حظر أجهزة الهجوم لمدة N دقيقة**.

في حالة تمكين هذا الخيار، 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.

4. قم بتعيين مدة منع مختلفة للكمبيوتر المهاجم في الحقل الموجود أسفل مفتاح التبديل **حظر أجهزة الهجوم لمدة N دقيقة**.

5. احفظ تغييراتك.

نتيجة لذلك، عندما يكتشف Kaspersky Endpoint Security محاولة هجوم شبكة اتصال تم إطلاقه على كمبيوتر مستخدم، فسوف يمنع كل الاتصالات بالكمبيوتر المهاجم. وينشئ Kaspersky Endpoint Security حدث Network attack detected. ويحتوي الحدث على معلومات عن الكمبيوتر المهاجم: عناوين IP وMAC.

يمكنك عرض عنوان MAC الخاص بالكمبيوتر المهاجم في واجهة مستخدم التطبيق أو في وحدة تحكم Kaspersky Security Center الإصدار 15.1 أو أحدث.



إخطار حول اكتشاف الهجوم عبر الشبكة

يلغي Kaspersky Endpoint Security منع الكمبيوتر عند انتهاء الوقت المحدد. ولا توفر وحدة تحكم Kaspersky Security Center أدوات لمراقبة أجهزة الكمبيوتر المحظورة بخلاف أحداث Network attack detected في التقرير. ويمكنك فقط عرض قائمة بأجهزة الكمبيوتر المحظورة في واجهة التطبيق. ويتم توفير هذه الوظيفة بواسطة أداة مراقبة شبكة الاتصال. ويمكنك أيضًا استخدام أداة مراقبة شبكة الاتصال لإلغاء منع جهاز كمبيوتر.

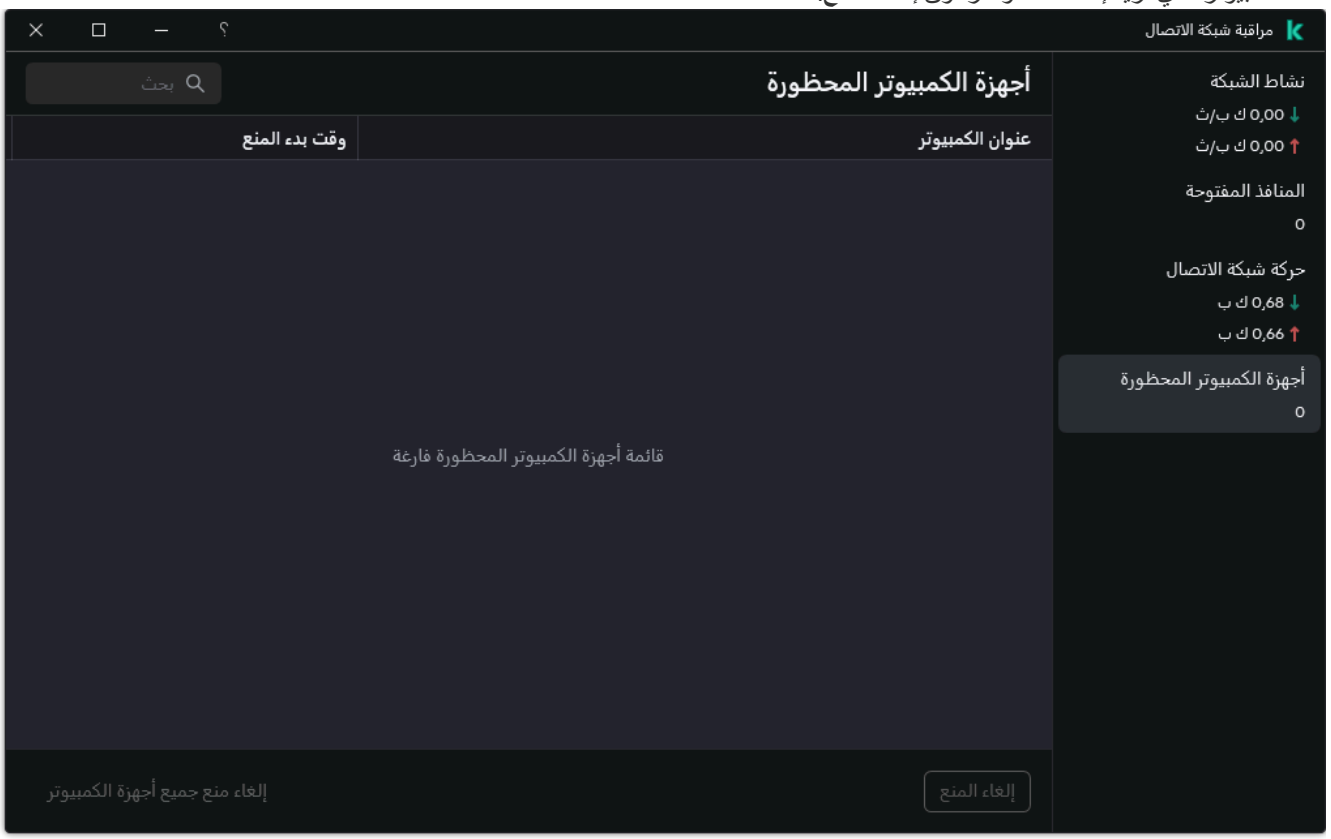
لإلغاء منع جهاز كمبيوتر:

1. في نافذة التطبيق الرئيسية، في القسم **المراقبة**، انقر فوق لوحة **مراقبة شبكة الاتصال**.
2. انتقل إلى علامة التبويب **أجهزة الكمبيوتر المحظورة**.

يفتح هذا قائمة بأجهزة الكمبيوتر المحظورة (انظر الشكل أدناه).

يمسح Kaspersky Endpoint Security قائمة المنع عند إعادة تشغيل التطبيق وعندما تتغير إعدادات الحماية من تهديدات الشبكة.

3. حدد الكمبيوتر الذي تريد إلغاء منعه وانقر فوق **إلغاء المنع**.



قائمة أجهزة الكمبيوتر المحظورة

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. ويمكنك أيضًا تحديد البروتوكول والمنفذ المستخدمين للاتصال والسماح بأنشطة شبكة محددة.

كيفية تكوين عناوين الاستثناءات من المنع في وحدة التحكم الإدارة (MMC)

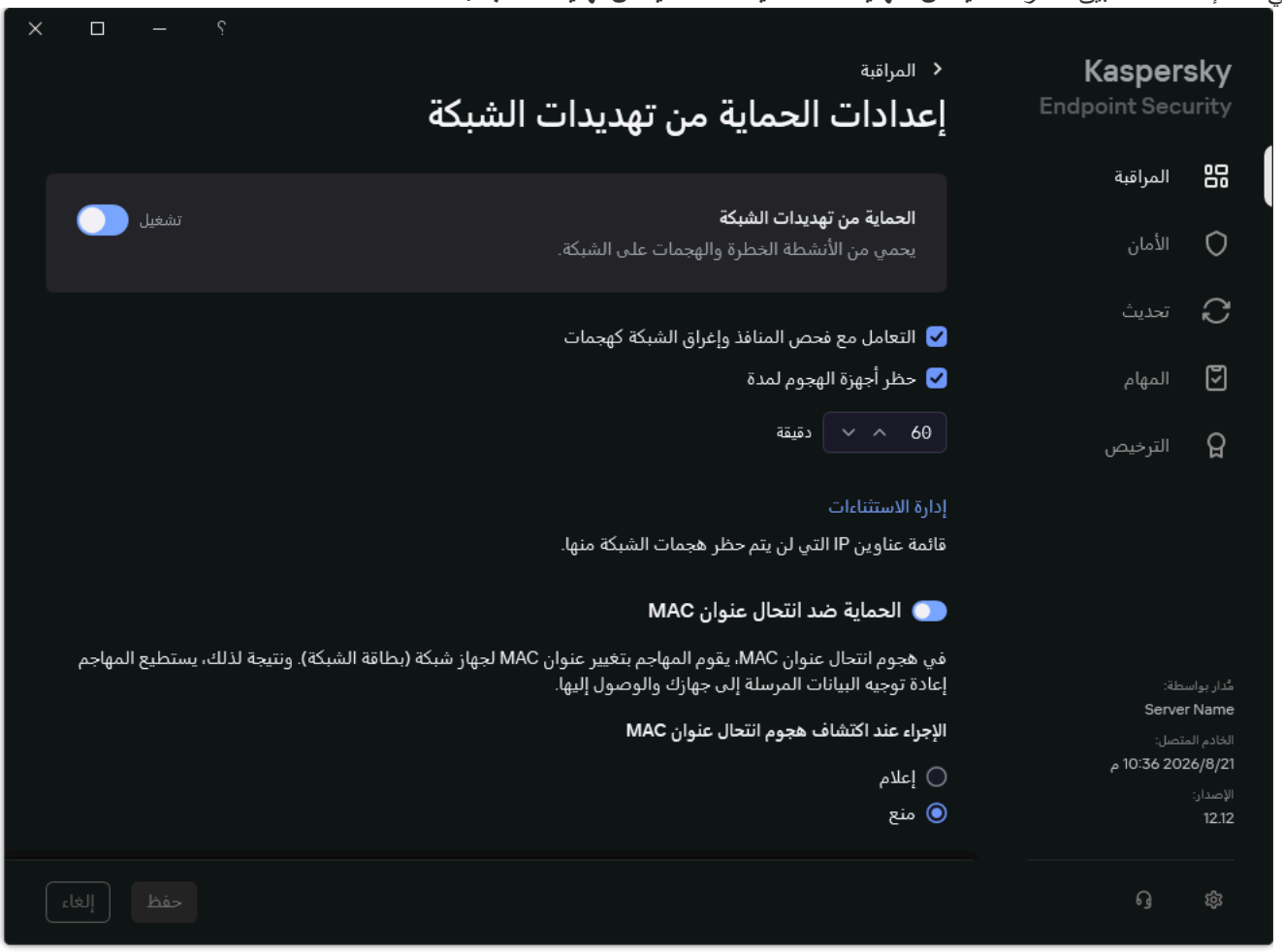
1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.
5. في القسم **إعدادات الحماية من تهديدات الشبكة**، انقر على الزر **الاستثناءات**.
6. في النافذة التي تفتح، انقر فوق الزر **إضافة**.
7. أدخل عنوان IP للكمبيوتر الذي يجب عدم منع هجمات الشبكة منه.
   إذا لزم الأمر، حدد البروتوكول والمنافذ التي يتم نقل البيانات من خلالها.
8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين العناوين المستثناة من المنع في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى القسم **Trusted Zone**.
5. في النافذة التي تفتح، انقر فوق الرابط **IP addresses**.
   يفتح هذا نافذة تحتوي على قائمة بعناوين IP الموثوقة.
6. في النافذة التي تفتح، انقر فوق الزر **Add**.
7. أدخل عنوان IP للكمبيوتر الذي يجب عدم منع هجمات الشبكة منه.
   إذا لزم الأمر، حدد الشبكة الفرعية.
8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين عناوين الاستثناءات من المنع في واجهة مستخدم التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر .
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.



إعدادات 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.

إذا لزم الأمر، حدد البروتوكول والمنافذ التي يتم نقل البيانات من خلالها.

6. احفظ تغييراتك.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.

4. في القسم **إعدادات الحماية من تهديدات الشبكة**، انقر على الزر **الاستثناءات**.

5. 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 الزر ← **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.

6. لاستيراد قائمة الاستثناءات:

a. انقر على الزر ← **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.

7. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة استثناءات في Kaspersky Security Center Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Network Threat Protection** ← **Communication & Web Protection**.

5. في الجزء العلوي من النافذة، انقر على الرابط **Trusted IP addresses**.
تفتح قائمة الاستثناءات.

6. لتصدير قائمة القواعد:

a. حدد الاستثناءات التي تريد تصديرها.

b. انقر على الزر ← **Export**.
يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات إلى ملف JSON في مجلد التنزيلات الافتراضي.

7. لاستيراد قائمة الاستثناءات:

a. انقر على الزر ← **Import**.
في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد قائمة الاستثناءات منه.

b. 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 JSON.

8. احفظ تغييراتك.

تكوين الحماية من تهديدات الشبكة 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.

لا يمكنك تكوين استثناءات منفصلة لهذه الأنواع من الهجمات. ويعني هذا أنه حتى لو تمت إضافة عناوين IP الفردية إلى المنطقة الموثوقة، فإن Kaspersky Endpoint Security يحظر الكمبيوتر المهاجم في حالة اكتشاف مثل هذا الهجوم. ويمكنك تمكين أو تعطيل اكتشاف مثل هذه الهجمات.

لا نوصي بتمكين الحماية من انتحال عناوين MAC على الأجهزة الافتراضية في البنية التحتية لمنصة Microsoft Hyper-V. ونظرًا لخصائص منصة Microsoft Hyper-V، قد يمنع Kaspersky Industrial CyberSecurity for Nodes برنامج Hypervisor بسبب النتائج الإيجابية الخاطئة.

كيفية تكوين الحماية من تهديدات الشبكة حسب النوع في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.
4. استخدم خانة الاختيار **التعامل مع فحص المنافذ وإغراق الشبكة كهجمات** لتمكين أو تعطيل اكتشاف هذه الهجمات.

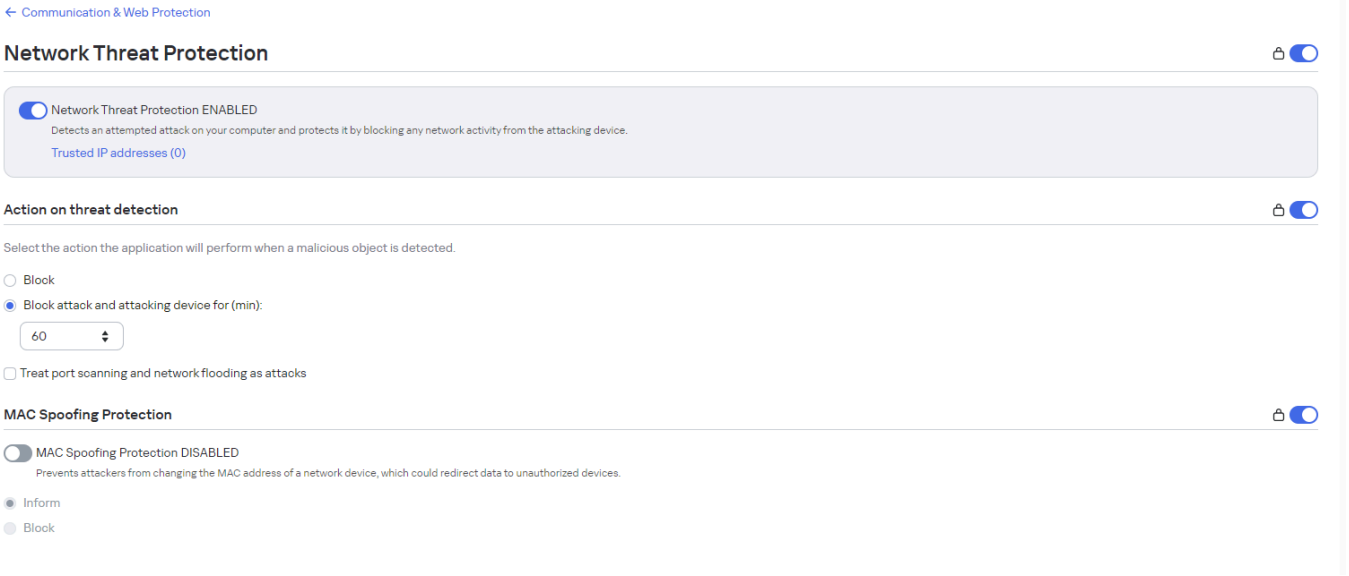
   في حالة تمكين هذه الوظيفة، يراقب Kaspersky Endpoint Security حركة مرور الشبكة لفحص المنافذ وإغراق الشبكة. وفي حالة اكتشاف هذا السلوك، يخطر التطبيق المستخدم ويرسل الحدث المقابل إلى Kaspersky Security Center. ويوفر التطبيق معلومات عن الكمبيوتر الذي يقدم الطلبات. وهذه المعلومات ضرورية للرد في الوقت المناسب. ومع ذلك، لا يحظر Kaspersky Endpoint Security الكمبيوتر الذي يقدم الطلبات لأن حركة المرور هذه قد تكون حدثًا عاديًا على شبكة الشركة.
5. في القسم **وضع الحماية من انتحال عنوان MAC**، حدد أحد الخيارات التالية:
   - **عدم تتبع انتحال عنوان MAC**.
   - **إعلام**.
   - **منع**.
6. احفظ تغييراتك.

كيفية تكوين الحماية من تهديدات الشبكة حسب النوع في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Communication & Web Protection** ← **Network Threat Protection**.



إعدادات الحماية من تهديدات الشبكة

5. استخدم خانة الاختيار **Treat port scanning and network flooding as attacks** 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.

6. تحت **MAC Spoofing Protection**، كوّن اكتشاف هجمات انتحال عنوان MAC :

a. استخدم مفتاح التبديل **MAC Spoofing Protection ENABLED** لتمكين أو تعطيل اكتشاف هذه الهجمات.

b. حدد الإجراء الذي سيتم تنفيذه عند اكتشاف هجوم انتحال عنوان MAC:

- **Inform**.
- **Block**.

7. احفظ تغييراتك.

كيفية تكوين الحماية من تهديدات الشبكة حسب النوع في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الشبكة**.



إعدادات 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** لتمكين أو تعطيل اكتشاف هذه الهجمات.

5. في القسم **الإجراء عند اكتشاف هجوم انتحال عنوان MAC**، حدد أحد الخيارات التالية:

- **إعلام**.
- **منع**.

6. احفظ تغييراتك.

جدار الحماية

يمنع مكون جدار الحماية الاتصالات غير المصرح بها لجهاز كمبيوتر 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.

أنواع اتصال الشبكة

يسمح لك جدار الحماية بالتحكم في نشاط الشبكة اعتمادًا على نوع اتصال الشبكة. يتلقى Kaspersky Endpoint Security نوع اتصال الشبكة من نظام تشغيل الكمبيوتر. يقوم المستخدم بتعيين نوع اتصال الشبكة في نظام التشغيل عند إعداد الاتصال. يمكنك تغيير نوع اتصال الشبكة في إعدادات Kaspersky Endpoint Security. سيراقب جدار الحماية نشاط الشبكة اعتمادًا على نوع الشبكة المحدد في إعدادات Kaspersky Endpoint Security وليس في نظام التشغيل.

تتوفر أنواع اتصال الشبكة 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.

  يُعين جدار الحماية نوع الشبكة العامة إلى الإنترنت بشكل افتراضي. لا يمكنك تغيير نوع 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 جهاز كمبيوتر للهجمات أو محاولات الوصول للبيانات غير المسموح بها. ويسمح جدار الحماية بأي نشاط للشبكة ضمن الشبكات التي تتمتع بهذه الحالة.

توافق Windows Defender Firewall

يحتوي نظام التشغيل على جدار الحماية المدمج الخاص به، وهو Windows Defender Firewall. ويختلف سلوك التطبيق وفقًا لنوع نظام التشغيل:

- **محطة عمل**. قد يؤدي استخدام Kaspersky Firewall بالتوازي مع Windows Defender Firewall إلى تشغيل خاطئ لنظام التشغيل. لذلك، يحتوي Kaspersky Endpoint Security على آلية تمنع استخدام كل من جداري الحماية في الوقت نفسه. وعند تمكين Kaspersky Firewall، يُعطل نظام التشغيل تلقائيًا Windows Defender Firewall. وعند إيقاف تشغيل Kaspersky Firewall، يعيد نظام التشغيل تلقائيًا تشغيل Windows Defender Firewall للحفاظ على حماية الكمبيوتر.
- **خادم**. لا يتوافق Kaspersky Firewall وWindows Defender Firewall مع بعضهما البعض. ويزيل مُثبّت Kaspersky Endpoint Security تلقائيًا Windows Defender Firewall عند تثبيت التطبيق.

تمكين أو تعطيل جدار الحماية

افتراضيًا يتم تمكين جدار الحماية والوظائف في الوضع الأمثل.

كيفية تمكين أو تعطيل جدار الحماية في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **جدار الحماية**.
4. استخدم خانة الاختيار **جدار الحماية** لتمكين المكون أو تعطيله.
5. احفظ تغييراتك.

كيفية تمكين أو تعطيل جدار الحماية في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. حدد **Firewall** ← **Communication & Web Protection**.
5. استخدم مفتاح تبديل **Firewall ENABLED** لتمكين المكون أو تعطيله.
6. احفظ تغييراتك.

كيفية تمكين أو تعطيل جدار الحماية في واجهة التطبيق

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. يراقب مكون الحماية من تهديدات الشبكة (يسمى أيضًا Intrusion Detection System، IDS) حركة شبكة الاتصال الواردة للبحث عن خاصية النشاط لهجمات 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 نوع اتصال الشبكة

يُعين جدار الحماية نوع الشبكة العامة إلى الإنترنت بشكل افتراضي. لا يمكنك تغيير نوع الإنترنت.

لتغيير نوع 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 نوعه.

5. في العمود **نوع شبكة الاتصال**، حدد نوع 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 جهاز كمبيوتر 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

يقوم جدار الحماية بتصفية كل نشاط الشبكة على الكمبيوتر وفقًا لقواعد حزمة الشبكة. وتحتوي قواعد حزمة الشبكة على شروط (مثل الاتجاه والبروتوكول) التي يطبقها جدار الحماية للتحكم في اتصالات الشبكة بالكمبيوتر. وتحدد قواعد حزمة الشبكة أيضًا الإجراء الذي ينفذه جدار الحماية مع الاتصال الذي يطابق القاعدة (السماح بالاتصال أو حظره).

توصيات لإنشاء قواعد حزمة الشبكة

يمكنك تحديد عنوان IP أو نطاق من عناوين IP لتصفية نشاط الشبكة. ويمكنك أيضًا تحديد اسم DNS.

في حالة استخدام اسم DNS في إحدى القواعد، يحلل Kaspersky Endpoint Security اسم DNS هذا إلى عنوان IP وبالتالي يتعامل مع القاعدة كما لو تم تحديد عنوان IP هذا فيها.

يستطيع Kaspersky Endpoint Security حل أسماء DNS في الحالات التالية:

- بدء تشغيل التطبيق
- تغيير إعدادات جدار الحماية

عندما يحلل التطبيق أسماء DNS من الكمبيوتر الذي تم تثبيت التطبيق عليه، يمكن إجراء عدد كبير من الاستعلامات إلى خادم DNS. ولتجنب ذلك، نوصي باستخدام عناوين IP بدلاً من أسماء DNS عند إنشاء القواعد.

في بعض الحالات، قد يكون استخدام أسماء DNS في أسماء حزم الشبكة غير آمن لأن مالك خادم DNS يمكنه تعديل معلمات سجل DNS. ويمكن لمهاجم ضار أيضًا تزييف رسائل DNS وتجاوز قواعد جدار الحماية.

يمكنك التحكم في اتصالات الشبكة عن طريق أسماء DNS باستخدام قواعد التحكم في الويب. وإذا كنت بحاجة إلى تحديد اسم DNS في قواعد جدار الحماية:

- تأكد من أمان شبكة الاتصال المحلية الخاصة بالشركة.
- تأكد من أمان التخزين المؤقت وخوادم DNS الرسمية.
- قم بتمكين حماية سجل DNS من التعديل.

عند إنشاء قواعد حزم الشبكة، تذكر أن لها الأولوية عن قواعد تطبيقات الشبكة.

طرق إنشاء قواعد 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.

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. انتقل إلى 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. باستخدام القائمة المنسدلة **إضافة**، حدد موقع القاعدة في القائمة: في أعلى القائمة، أو أسفل القائمة، أو بجوار القاعدة المحددة.
يحدد موضع القاعدة في القائمة أولوية القاعدة. وتكون للقاعدة الموجودة أعلى القائمة الأولوية القصوى.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

4. في القسم **إعدادات جدار الحماية**، انقر على الزر **الإعدادات**.
يفتح هذا قائمة قواعد حزم الشبكة وقائمة قواعد الشبكة للتطبيق.

5. انتقل إلى علامة التبويب **قواعد حزمة الشبكة**.
يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

6. باستخدام القائمة المنسدلة **إضافة**، حدد موقع القاعدة في القائمة: في أعلى القائمة، أو أسفل القائمة، أو بجوار القاعدة المحددة.
يحدد موضع القاعدة في القائمة أولوية القاعدة. وتكون للقاعدة الموجودة أعلى القائمة الأولوية القصوى.

7. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.

8. 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.

9. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.

10. حفظ قاعدة الشبكة الجديدة

11. استخدم الزرين **أعلى** / **أسفل** 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. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

كيفية إنشاء قاعدة حزمة شبكة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. حدد **Communication & Web Protection** ← **Firewall**.

5. حدد علامة التبويب **Network packet rules**.
يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

6. انقر على **Add**.
يفتح هذا النموذج لقاعدة شبكة جديدة.

7. أدخل اسم خدمة الشبكة يدويًا في الحقل **Rule name**.

8. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).
يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **Select rule template**. تصف قوالب القواعد اتصالات الشبكة متكررة الاستخدام.
سيتم ملء جميع إعدادات قواعد الشبكة تلقائيًا.

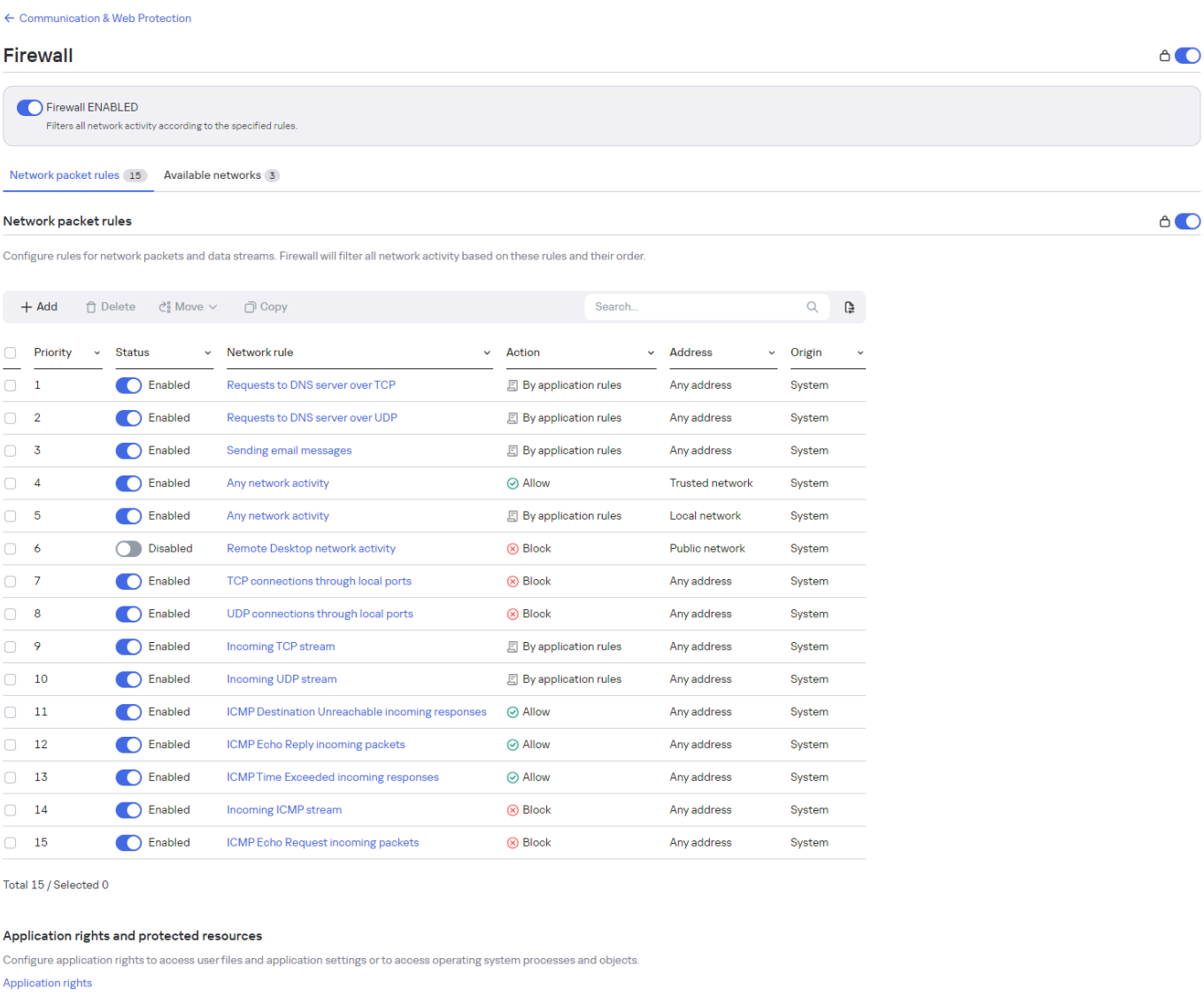
9. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **Log events**.

10. احفظ قاعدة الشبكة.
ستتم إضافة قاعدة الشبكة الجديدة إلى القائمة.

11. استخدم الزر **Move** 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.



قواعد حزمة جدار الحماية

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 و UDP و ICMP و ICMPv6 و IGMP و GRE. 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 لأجهزة الكمبيوتر المحلية والبعيدة التي سيتم مراقبة الاتصال بينها. نطاق القيم الممكنة لأرقام المنافذ: 0-65535. وفي كل حقل، يمكنك إدخال قيم متعددة مفصولة باستخدام `,` أو تحديد نطاق من القيم باستخدام `-`. على سبيل المثال: • `100,101` • `100-130` • `100,110-130`
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 حزم الشبكة الواردة والصادرة. **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.

المعلمة	الوصف
مدة البقاء (TTL)	تقييد التحكم في حزم الشبكة حسب عمرها الافتراضي (Time to Live، TTL).
العناوين البعيدة	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. إذا أضفت في قاعدة حزمة الشبكة اسم DNS لا يمكن تحديد عنوان IP له، سيعرض Kaspersky Endpoint Security تحذيرًا. وفي قائمة قواعد حزم الشبكة في Web Console، تتم إضافة عمود مع وصف للخطأ. وفي وحدة تحكم الإدارة (MMC)، يكون وصف الخطأ غير متاح. ويتم تمييز قواعد الحزمة هذه بالألوان.
العناوين المحلية	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. يخزن التطبيق العناوين المحلية فقط في حالة تحديد قائمة بالعناوين البعيدة. أي تم تحديد قيمة **عناوين من القائمة** لخيار **العناوين البعيدة** وتمت إضافة عنوان واحد على الأقل. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

4. في القسم **إعدادات جدار الحماية**، انقر على الزر **الإعدادات**.
يفتح هذا قائمة قواعد حزم الشبكة وقائمة قواعد الشبكة للتطبيق.

5. انتقل إلى علامة التبويب **قواعد حزمة الشبكة**.

6. 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.

7. 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.

8. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد حزمة الشبكة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. حدد **Communication & Web Protection** ← **Firewall**.

5. لتصدير قائمة القواعد، في القسم **Network packet rules**:

a. حدد القواعد التي تريد تصديرها.

b. انقر على الزر ← **Export**.
يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف JSON في مجلد التنزيلات الافتراضي.

6. لاستيراد قائمة القواعد، في القسم **Network packet rules**:

a. انقر على الزر ← **Import**.
في النافذة التي تفتح، حدد ملف JSON 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 JSON.

7. 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** (الشبكات الموثوقة). `125` – **أي نشاط للشبكة** (الشبكات المحلية). `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`.

المعلمة	الوصف	القيمة
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 – **الشبكات الموثوقة**. 51 – **الشبكات المحلية**. 52 – **الشبكات العامة**. <Network Identifier> - **عناوين من القائمة** (يتم تحديد العناوين يدويًا).
AccessFlag	قيمة معلمة **الإجراء**.	0 – **سماح**. 2 – **حسب قواعد التطبيق**. 3 – **منع**. 4 – **سماح وأحداث السجل**. 6 – **حسب قواعد التطبيق وأحداث السجل**. 7 – **منع وأحداث 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

```
                                                
```

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**.

المعلمة	الوصف	القيمة
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**. **بروتوكول 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**.

المعلمة	الوصف	القيمة
		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 `Rules`).	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. انتقل إلى علامة التبويب**نشاط الشبكة** أو **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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

4. في القسم **إعدادات جدار الحماية**، انقر على الزر **الإعدادات**.
يفتح هذا قائمة قواعد حزم الشبكة وقائمة قواعد الشبكة للتطبيق.

5. انتقل إلى علامة التبويب **قواعد شبكة الاتصال للتطبيق**.

6. انقر على **إضافة**.

7. 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.

8. 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.

9. حدد التطبيق المطلوب.

10. في القائمة المنسدلة **إضافة التطبيق المحدد إلى مجموعة الثقة**، حدد **المجموعات الافتراضية** وانقر فوق **موافق**.
ستتم إضافة التطبيق إلى المجموعة الافتراضية.

11. حدد التطبيق ذي الصلة، ثم حدد **حقوق التطبيق** من قائمة السياق الخاصة بالتطبيق.
تفتح نافذة قواعد التطبيق والخصائص.

12. حدد علامة التبويب **قواعد شبكة الاتصال**.
يؤدي ذلك إلى فتح قائمة بقواعد الشبكة الافتراضية التي يتم تعيينها بواسطة جدار الحماية.

13. انقر على **إضافة**.
يفتح هذا خصائص قاعدة الشبكة.

14. أدخل اسم خدمة الشبكة يدويًا في الحقل **الاسم**.

15. 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.

16. إذا رغبت في أن تنعكس إجراءات قاعدة الشبكة في تقرير، فحدد خانة الاختيار **أحداث السجل**.

17. حفظ قاعدة الشبكة الجديدة

18. استخدم الزرين **أعلى** / **أسفل** لتعيين أولوية قاعدة الشبكة.

19. احفظ تغييراتك.

كيفية إنشاء قاعدة شبكة لتطبيق في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. حدد **Firewall** ← **Communication & Web Protection**.

5. في القسم **Application rights and protected resources**، انقر على الرابط **Application rights**.
يفتح هذا نافذة تكوين حقوق التطبيق وقائمة الموارد المحمية.

6. انتقل إلى علامة التبويب **Application rights**.
سترى قائمة تتضمن مجموعات الثقة على الجانب الأيمن من النافذة وخصائصها على الجانب الأيسر.

7. في القسم **Applications**، انقر على الزر **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. قم بإنهاء 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 **Rule name**.

16. قم بتكوين إعدادات قاعدة الشبكة (انظر الجدول أدناه).
يمكنك تحديد قالب قاعدة محدد مسبقًا بالنقر فوق الرابط **Select rule 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 الزر **Move** 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 لأجهزة الكمبيوتر المحلية والبعيدة التي سيتم مراقبة الاتصال بينها. نطاق القيم الممكنة لأرقام المنافذ: 0-65535. وفي كل حقل، يمكنك إدخال قيم متعددة مفصولة باستخدام `,` أو تحديد نطاق من القيم باستخدام `-`. على سبيل المثال: • `100,101` • `100-130` • `100,110-130`
الاتجاه	**الوارد**. **الوارد / الصادر**. **الصادر**.
العناوين البعيدة	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. إذا أضفت في قاعدة حزمة الشبكة اسم DNS لا يمكن تحديد عنوان IP له، سيعرض Kaspersky Endpoint Security تحذيرًا. وفي قائمة قواعد حزم الشبكة في Web Console، تتم إضافة عمود مع وصف للخطأ. وفي وحدة تحكم الإدارة (MMC)، يكون وصف الخطأ غير متاح. ويتم تمييز قواعد الحزمة هذه بالألوان.
العناوين المحلية	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. يخزن التطبيق العناوين المحلية فقط في حالة تحديد قائمة بالعناوين البعيدة. أي تم تحديد قيمة **عناوين من القائمة** لخيار **العناوين البعيدة** وتمت إضافة عنوان واحد على الأقل. 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 الاستغلال

يكتشف مكون منع الاستغلال 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.

بالإضافة إلى ذلك، يراقب مكون منع الاستغلال منافذ الشبكة لعمليات التطبيق التي قد تهدد أمان الكمبيوتر. ويحصل التطبيق على معلومات عن هذه العمليات مع قواعد بيانات مكافحة الفيروسات.

تمكين وتعطيل منع الاستغلال

افتراضيًا، يتم تمكين منع الاستغلال والوظائف في الوضع الأمثل. يراقب Kaspersky Endpoint Security الملفات القابلة للتنفيذ التي يتم تشغيلها بواسطة تطبيقات بها ثغرات أمنية. 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).

كيفية تمكين أو تعطيل منع الاستغلال في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع الاستغلال**.
4. استخدم خانة الاختيار **منع الاستغلال** لتمكين المكون أو تعطيله.

5. حدد الإجراء المناسب من القسم **عند اكتشاف استغلال**:

- **منع**. في حالة تحديد هذا العنصر، عند اكتشاف استغلال، يمنع Kaspersky Endpoint Security عمليات هذا الاستغلال ويدون إدخال سجل بالمعلومات حول هذا الاستغلال.
- **إعلام**. 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.

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل منع الاستغلال في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Exploit Prevention** ← **Behavior Analysis** ← **Host Threat Protection**.
5. استخدم مفتاح تبديل **Exploit Prevention** لتمكين المكون أو تعطيله.
6. حدد الإجراء المناسب من القسم **Action on threat detection**:

- **Block**. في حالة تحديد هذا العنصر، عند اكتشاف استغلال، يمنع Kaspersky Endpoint Security عمليات هذا الاستغلال ويدون إدخال سجل بالمعلومات حول هذا الاستغلال.
- **Inform**. 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.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل منع الاستغلال في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **منع الاستغلال**.



إعدادات منع الاستغلال

3. استخدم مفتاح تبديل **منع الاستغلال** لتمكين المكون أو تعطيله.

4. حدد الإجراء المناسب من القسم **عند اكتشاف استغلال**:

- **منع**. في حالة تحديد هذا العنصر، عند اكتشاف استغلال، يمنع Kaspersky Endpoint Security عمليات هذا الاستغلال ويدون إدخال سجل بالمعلومات حول هذا الاستغلال.
- **إعلام**. 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.

5. احفظ تغييراتك.



الإخطار حول التهديد النشط

حماية ذاكرة عمليات النظام

بشكل افتراضي، يتم تمكين حماية ذاكرة عملية النظام. يحظر Kaspersky Endpoint Security العمليات الخارجية التي تحاول الوصول إلى عمليات النظام.

كيفية تمكين أو تعطيل حماية ذاكرة عمليات النظام في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← منع الاستغلال**.
4. استخدم خانة الاختيار **تمكين حماية ذاكرة عملية النظام** لتمكين أو تعطيل الخيار.
5. احفظ تغييراتك.

كيفية تمكين أو تعطيل حماية ذاكرة عمليات النظام في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Exploit Prevention ← Behavior Analysis ← Host Threat Protection**.

5. استخدم مفتاح التبديل **System process memory protection ENABLED** لتمكين هذه الميزة أو تعطيلها.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل حماية ذاكرة عمليات النظام في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← منع الاستغلال**.



إعدادات منع الاستغلال

3. استخدم مفتاح التبديل **تمكين حماية ذاكرة عملية النظام** لتمكين هذه الميزة أو تعطيلها.

4. احفظ تغييراتك.

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. وتعتمد وظيفة Kaspersky Endpoint Security على توقيعات تدفق السلوك وتوفر دفاعًا استباقيًا للكمبيوتر.

بالإضافة إلى ذلك، يراقب مكون اكتشاف السلوك منافذ الشبكة لعمليات التطبيق التي قد تهدد أمان الكمبيوتر. ويحصل التطبيق على معلومات عن هذه العمليات مع قواعد بيانات مكافحة الفيروسات.

بشكل افتراضي، يتم تمكين اكتشاف السلوك ويعمل في الوضع الموصى به من قبل Kaspersky. وعند اكتشاف نشاط ضار، يحذف Kaspersky Endpoint Security الملف القابل للتنفيذ الخاص بالتطبيق الضار.

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.

كيفية تمكين أو تعطيل اكتشاف السلوك في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **اكتشاف السلوك**.
5. استخدم خانة الاختيار **اكتشاف السلوك** لتمكين المكون أو تعطيله.
6. حدد الإجراء المناسب من القسم **الإجراء عند اكتشاف نشاط برنامج ضار**:
   - **حذف**. 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.
   - **منع**. في حالة تحديد هذا العنصر، يقوم برنامج Kaspersky Endpoint Security بإنهاء هذا التطبيق في حالة اكتشاف وجود أي نشاط خبيث.
   - **إعلام**. 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.
7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل اكتشاف السلوك في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Behavior Detection** ← **Behavior Analysis** ← **Host Threat Protection**
5. استخدم مفتاح تبديل **Behavior Detection ENABLED** لتمكين المكون أو تعطيله.
6. حدد الإجراء المناسب من القسم **Action on threat detection**:
   - **Delete**. 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.
   - **Block**. في حالة تحديد هذا العنصر، يقوم برنامج Kaspersky Endpoint Security بإنهاء هذا التطبيق في حالة اكتشاف وجود أي نشاط خبيث.
   - **Inform**. 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.
7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل اكتشاف السلوك في واجهة التطبيق

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. حدد الإجراء المناسب من القسم **الإجراء عند اكتشاف نشاط برنامج ضار**:

- **حذف**. 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.
- **منع**. في حالة تحديد هذا العنصر، يقوم برنامج Kaspersky Endpoint Security بإنهاء هذا التطبيق في حالة اكتشاف وجود أي نشاط خبيث.
- **إعلام**. 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.

5. احفظ تغييراتك.

نتيجة لذلك، في حالة تمكين اكتشاف السلوك، سيستخدم Kaspersky Endpoint Security توقيعات بث السلوك لتحليل نشاط التطبيقات في نظام التشغيل.

مكافحة التشفير

بدءًا من Kaspersky Endpoint Security 12.12 for Windows، أصبحت حماية المجلدات المشتركة من التشفير الخارجي الذي كان في السابق جزءًا من مكون اكتشاف السلوك مكونًا منفصلاً يسمى مكافحة التشفير.

يراقب المكون العمليات التي يتم تنفيذها فقط مع هذه الملفات المخزنة على أجهزة تخزين كبيرة السعة بنظام ملف NTFS وغير المشفرة بنظام EFS.

يحلل مكون مكافحة التشفير النشاط في المجلدات المشتركة. إذا توافق هذا النشاط مع توقيع تدفق السلوك المشابه للتشفير الخارجي، فإن Kaspersky Endpoint Security يقوم باتخاذ الإجراء المحدد.

لكي يعمل مكون مكافحة التشفير، يجب عليك تمكين مكون اكتشاف السلوك.

إذا اكتشف 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.
- يضيف إدخالاً إلى تقارير واجهة التطبيق المحلية ويرسل معلومات عن النشاط الخبيث المكتشف إلى Kaspersky Security Center.
- وأيضًا، في حال تمكين مكون محرك المعالجة، يتم استرداد الملفات المعدّلة من النسخ الاحتياطية.

تمكين وتعطيل حماية المجلدات المشتركة ضد التشفير الخارجي

بشكل افتراضي، يتم تمكين حماية المجلدات المشتركة ضد التشفير الخارجي وتعمل على النحو الموصى به بواسطة خبراء Kaspersky. ولتكوين هذه الوظيفة، يمكنك إنشاء نطاق حماية وتكوين الاستثناءات، إذا لزم الأمر. وبشكل افتراضي ، يحدد التطبيق تلقائيًا المجلدات المشتركة ويراقب نشاط الملفات في جميع المجلدات. وعند اكتشاف محاولة لتشفير الملفات خارجيًا في مجلدات مشتركة، يحظر Kaspersky Endpoint Security جلسة المستخدم عن بُعد لمدة ساعة واحدة (بشكل افتراضي).

بعد تثبيت Kaspersky Endpoint Security، سوف تكون حماية المجلدات المشتركة ضد التشفير الخارجي محدودة حتى تتم إعادة تشغيل الكمبيوتر.

كيفية تمكين أو تعطيل حماية المجلدات المشتركة من التشفير الخارجي في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **مكافحة أداة التشفير**.
4. استخدم خانة الاختيار **مكافحة أداة التشفير** لتمكين الكشف عن النشاط المعتاد للتشفير الخارجي أو تعطيله.

5. حدد الإجراء ذي الصلة الذي سيتخذه التطبيق عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة:

- **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 للجلسة التي بدأت النشاط الضار وينشئ نسخًا احتياطية من الملفات المعدلة.

في حالة تمكين مكون محرك المعالجة وتحديد الخيار **منع الاتصال لمدة**، سيتم استعادة الملفات المعدلة من النسخ الاحتياطية.

- **إعلام**. في حالة تحديد هذا الخيار، عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة، يضيف Kaspersky Endpoint Security معلومات عن هذه المحاولة إلى قائمة التهديدات النشطة، ويضيف إدخالاً إلى تقارير واجهة التطبيق المحلية ويرسل معلومات عن النشاط الخبيث المكتشف إلى Kaspersky Security Center.

6. إذا لزم الأمر، حرر نطاق حماية وحدد الاستثناءات.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل حماية المجلدات المشتركة من التشفير الخارجي في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **Anti-Cryptor** ← **Behavior Analysis** ← **Host Threat Protection**.

5. استخدم مفتاح التبديل **Anti-Cryptor ENABLED** لتمكين الكشف عن النشاط المعتاد للتشفير الخارجي أو تعطيله.

6. حدد الإجراء ذي الصلة الذي سيتخذه التطبيق عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة:

- **Block connection for (min) N min**. في حالة تحديد هذا الخيار، عندما يكتشف Kaspersky Endpoint Security محاولة لتعديل الملفات في المجلدات المشتركة، فإنه يمنع الوصول إلى تعديل الملف للجلسة التي بدأت النشاط الضار وينشئ نسخًا احتياطية من الملفات المعدلة.

في حالة تمكين مكون محرك المعالجة وتحديد الخيار **Block connection for (min)**، سيتم استعادة الملفات المعدلة من النسخ الاحتياطية.

- **Inform**. في حالة تحديد هذا الخيار، عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة، يضيف Kaspersky Endpoint Security معلومات عن هذه المحاولة إلى قائمة التهديدات النشطة، ويضيف إدخالاً إلى تقارير واجهة التطبيق المحلية ويرسل معلومات عن النشاط الخبيث المكتشف إلى Kaspersky Security Center.

7. إذا لزم الأمر، حرر نطاق حماية وحدد الاستثناءات.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل حماية المجلدات المشتركة من التشفير الخارجي في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر .

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **مكافحة أداة التشفير**.

3. استخدم خانة الاختيار **حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي** لتمكين الكشف عن النشاط المعتاد للتشفير الخارجي أو تعطيله.

4. استخدم خانة الاختيار **حماية المجلدات التي تتم مشاركتها ضد التشفير الخارجي** لتمكين الكشف عن النشاط المعتاد للتشفير الخارجي أو تعطيله.

5. حدد الإجراء ذي الصلة الذي سيتخذه التطبيق عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة:

- **منع الاتصال لمدة (دقيقة) N min**. في حالة تحديد هذا الخيار، عندما يكتشف Kaspersky Endpoint Security محاولة لتعديل الملفات في المجلدات المشتركة، فإنه يمنع الوصول إلى تعديل الملف للجلسة التي بدأت النشاط الضار وينشئ نسخًا احتياطية من الملفات المعدلة.

في حالة تمكين مكون محرك المعالجة وتحديد الخيار **منع الاتصال لمدة (دقيقة)**، سيتم استعادة الملفات المعدلة من النسخ الاحتياطية.

- **إعلام**. في حالة تحديد هذا الخيار، عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة، يضيف Kaspersky Endpoint Security معلومات عن هذه المحاولة إلى قائمة التهديدات النشطة، ويضيف إدخالاً إلى تقارير واجهة التطبيق المحلية ويرسل معلومات عن النشاط الخبيث المكتشف إلى Kaspersky Security Center.

6. إذا لزم الأمر، حرر نطاق حماية وحدد الاستثناءات.

7. احفظ تغييراتك.

تكوين فترة الحظر لجهاز كمبيوتر غير موثوق به

الكمبيوتر غير الموثوق به هو كمبيوتر بعيد يشارك في نشاط ضار أو تشفير البيانات. وبشكل افتراضي، يحظر Kaspersky Endpoint Security جلسة المستخدم البعيد لمدة ساعة واحدة. وعند انتهاء صلاحية فترة الحظر، يزيل Kaspersky Endpoint Security الكمبيوتر من قائمة الحظر ويستعيد الوصول إلى المجلد المشترك.

كيفية تكوين فترة الحظر لكمبيوتر غير موثوق به في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← مكافحة أداة التشفير**.

4. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد **منع الاتصال لمدة N دقيقة**.

5. كوّن فترة الحظر لكمبيوتر غير موثوق به يشارك في نشاط ضار أو تشفير البيانات.

6. احفظ تغييراتك.

كيفية تكوين فترة الحظر لكمبيوتر غير موثوق به في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.

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

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

4. انتقل إلى **Anti-Cryptor ← Behavior Analysis ← Host Threat Protection**.

5. تحت **Action on threat detection**، كوّن فترة الحظر لكمبيوتر غير موثوق به يشارك في نشاط ضار أو تشفير البيانات.

6. احفظ تغييراتك.

كيفية تكوين فترة الحظر لكمبيوتر غير موثوق به في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة ← مكافحة أداة التشفير**.
3. في القسم **الإجراء المطلوب اتخاذه عند اكتشاف تهديد**، حدد **منع الاتصال لمدة (دقيقة)**.
4. كوّن فترة الحظر لكمبيوتر غير موثوق به يشارك في نشاط ضار أو تشفير البيانات.
5. احفظ تغييراتك.

نتيجة لذلك، سيتم قفل الكمبيوتر البعيد. ولإلغاء قفل الكمبيوتر البعيد، يمكنك إعادة تشغيل Kaspersky Endpoint Security.

تحرير نطاق المراقبة

نطاق الحماية هو قائمة بمسارات المجلدات المشتركة التي يراقب فيها Kaspersky Endpoint Security نشاط الملفات. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. وبشكل افتراضي ، يحدد التطبيق تلقائيًا المجلدات المشتركة ويراقب نشاط الملفات في جميع المجلدات.

ومن الممكن أن يؤدي استثناء مجلد من نطاق الحماية 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.

يمكنك أيضًا استثناء أجهزة الكمبيوتر التي يجب عدم معالجة محاولات التشفير الخارجية منها.

كيفية تحرير نطاق حماية في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← مكافحة أداة التشفير**.
4. في القسم **نطاق الحماية**، حدد **المجلدات المشتركة المحددة فقط**.
5. في قائمة المجلدات، انقر فوق **إضافة**.
6. يفتح هذا نافذة؛ وفي تلك النافذة، أدخل المسار إلى المجلد المشترك الذي تريد تضمينه في نطاق الحماية (على سبيل المثال، `C:\Share`).

لإضافة مجلد مشترك إلى نطاق الحماية، استخدم مسارًا محليًا.

7. انقر على **موافق**.
8. إذا لزم الأمر، حدد استثناءات نطاق الحماية:
   a. في القسم **استثناءات الفحص**، انقر على الزر **حسب القناع**.
   b. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

c. في النافذة المعروضة، حدد ملحق ملف بتنسيق `*.<file extension>` أو مسار مجلد. يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع.

لا يدعم التطبيق بعض ملحقات ملف الاستثناءات. وبالتالي، يمكنك تحديد استثناء بتنسيق `*.docx` أو `**\Folder\**`.

يمكنك استثناء كائن من عمليات الفحص بدون إزالته من قائمة الكائنات في نطاق الحماية. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

9. احفظ تغييراتك.

كيفية تحرير نطاق حماية في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Anti-Cryptor** ← **Behavior Analysis** ← **Host Threat Protection**.

5. في القسم **Protection scope**، حدد **Only specified shared folders**.

6. في قائمة المجلدات، انقر فوق **Add**.

7. يفتح هذا نافذة؛ وفي تلك النافذة، أدخل المسار إلى المجلد المشترك الذي تريد تضمينه في نطاق الحماية (على سبيل المثال، `C:\Share`).

لإضافة مجلد مشترك إلى نطاق الحماية، استخدم مسارًا محليًا.

8. انقر على **OK**.

9. إذا لزم الأمر، حدد استثناءات نطاق الحماية:

a. في الجزء العلوي من النافذة، انقر على الرابط **Scan exclusions**.

b. في النافذة التي تفتح، انقر فوق الزر **Add**.

c. في النافذة المعروضة، حدد ملحق ملف بتنسيق `*.<file extension>` أو مسار مجلد. يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع.

لا يدعم التطبيق بعض ملحقات ملف الاستثناءات. وبالتالي، يمكنك تحديد استثناء بتنسيق `*.docx` أو `**\Folder\**`.

يمكنك استثناء كائن من عمليات الفحص بدون إزالته من قائمة الكائنات في نطاق الحماية. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

10. احفظ تغييراتك.

كيفية تحرير نطاق حماية في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **مكافحة أداة التشفير**.

3. في القسم **نطاق الحماية**، حدد **المجلدات المشتركة المحددة فقط**.

4. في قائمة المجلدات، انقر فوق **إضافة**.

5. يفتح هذا نافذة؛ وفي تلك النافذة، أدخل المسار إلى المجلد المشترك الذي تريد تضمينه في نطاق الحماية (على سبيل المثال، `C:\Share`).

لإضافة مجلد مشترك إلى نطاق الحماية، استخدم مسارًا محليًا.

6. انقر على **موافق**.

7. إذا لزم الأمر، حدد استثناءات نطاق الحماية:

a. في الجزء العلوي من النافذة، انقر على الرابط **الاستثناءات حسب القناع**.

b. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

c. في النافذة المعروضة، حدد ملحق ملف بتنسيق `*.<file extension>` أو مسار مجلد. يدعم Kaspersky Endpoint Security حرفي `*` و`?` عند إدخال قناع.

لا يدعم التطبيق بعض ملحقات ملف الاستثناءات. وبالتالي، يمكنك تحديد استثناء بتنسيق `*.docx` أو `**\Folder\**`.

يمكنك استثناء كائن من عمليات الفحص بدون إزالته من قائمة الكائنات في نطاق الحماية. ولفعل ذلك، قم بإلغاء تحديد خانة الاختيار بجوار الكائن.

8. احفظ تغييراتك.

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 `?:\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.

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى القسم **Trusted Zone**.

5. في النافذة التي تفتح، انقر فوق الرابط **Malware 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. أيضًا، في حالة إلغاء تحديد خانة الاختيار هذه، يخفي Kaspersky Endpoint Security القائمة الموحدة لاستثناءات الفحص في واجهة المستخدم الخاصة بالتطبيق.

8. انقر فوق **Add** وحدد إجراءً:

- **Category**. يمكنك تجميع استثناءات الفحص في فئات منفصلة. ولإنشاء فئة جديدة، أدخل اسم الفئة وأضف استثناء فحص واحد على الأقل إلى الفئة.
- **New exclusion**. يضيف Kaspersky Endpoint Security استثناءً جديدًا للفحص إلى جذر القائمة.
- **Select exclusion from list**. لتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق استثناءات الفحص المحددة مسبقًا. وتمت أيضًا إضافة استثناءات فحص محددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد استثناءات من الفحص محددة مسبقًا وفقًا للغرض من الخادم المحمي.

9. حدد كيف تريد إضافة الاستثناء **Path to the file or folder**.

10. أدخل المسار إلى 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 **Apply exclusion to**، حدد المكون **Behavior Detection**.

12. إذا لزم الأمر، في الحقل **Comment**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

13. حدد الحالة **Add to exclusions** للاستثناء.

يمكنك استخدام مفتاح التبديل إيقاف استثناء في أي وقت.

14. احفظ تغييراتك.

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.

4. في القسم **استثناءات الفحص والتطبيقات الموثوقة** ← **استثناءات الفحص**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تحتوي على قائمة استثناءات.

5. 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.

6. 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. أيضًا، في حالة إلغاء تحديد خانة الاختيار هذه، يخفي Kaspersky Endpoint Security القائمة الموحدة لاستثناءات الفحص في واجهة المستخدم الخاصة بالتطبيق.

7. انقر فوق **إضافة** وحدد إجراءً:

- **الفئة**. يمكنك تجميع استثناءات الفحص في فئات منفصلة. ولإنشاء فئة جديدة، أدخل اسم الفئة وأضف استثناء فحص واحد على الأقل إلى الفئة.
- **استثناء جديد**. يضيف Kaspersky Endpoint Security استثناءً جديدًا للفحص إلى جذر القائمة.
- **تحديد الاستثناء من القائمة**. لتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق استثناءات الفحص المحددة مسبقًا. وتمت أيضًا إضافة استثناءات فحص محددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد استثناءات من الفحص محددة مسبقًا وفقًا للغرض من الخادم المحمي.

8. انقر على **إضافة**.

9. في القسم **الخصائص**، حدد خانة الاختيار **الملف أو المجلد**.

10. 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**.

11. 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 `?:\Users\*\Folder\`.

12. إذا لزم الأمر، في الحقل **تعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

13. انقر فوق الرابط في القسم **وصف الاستثناء من الفحص (انقر فوق العناصر التي تحتها خط لتحريرها)** لفتح النافذة **مكونات الحماية**.

14. حدد خانة الاختيار الموجودة بجوار المكون **اكتشاف السلوك**.

15. احفظ تغييراتك.

إضافة أجهزة كمبيوتر موثوقة لتشفير البيانات الخارجية

إذا كانت مؤسستك تستخدم تشفير البيانات الخارجية في سير عمل تبادل الملفات الخاص بها، فيجب عليك إنشاء قائمة بأجهزة الكمبيوتر الموثوق بها. ولا يراقب Kaspersky Endpoint Security تشفير البيانات بواسطة أجهزة الكمبيوتر الموثوق بها.

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.

كيفية إضافة كمبيوتر موثوق به لتشفير البيانات الخارجية في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← مكافحة أداة التشفير**.

5. في القسم **استثناءات الفحص**، انقر على الزر **حسب الاسم أو عنوان IP**.

6. في النافذة التي تفتح، انقر فوق الزر **حسب الاسم أو عنوان IP**.

7. أدخل عناوين IP أو نطاق عناوين IP أو اسم الكمبيوتر الذي يجب عدم التعامل مع محاولات التشفير الخارجي منه.
أمثلة:

- `192.168.0.0 - 192.168.255.255`
- `192.168.0.0/24`
- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إضافة كمبيوتر موثوق للتشفير الخارجي للبيانات في Kaspersky Security Center Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى القسم **Trusted Zone**.
5. في الجزء الأيسر من النافذة، انقر على الرابط **Anti-Cryptor exclusions**.
6. في النافذة التي تفتح، انقر فوق الزر **Add**.
7. أدخل عناوين IP أو نطاق عناوين IP أو اسم الكمبيوتر الذي يجب عدم التعامل مع محاولات التشفير الخارجي منه.
أمثلة:

- `192.168.0.0 - 192.168.255.255`
- `192.168.0.0/24`
- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إضافة كمبيوتر موثوق به لتشفير البيانات الخارجية في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **الحماية من التهديدات المتقدمة** ← **مكافحة أداة التشفير**.
3. في الجزء العلوي من النافذة، انقر على الرابط **الاستثناءات حسب الاسم أو عنوان IP**.
4. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

5. أدخل عناوين IP أو نطاق عناوين IP أو اسم الكمبيوتر الذي يجب عدم التعامل مع محاولات التشفير الخارجي منه.
أمثلة:

- `192.168.0.0 - 192.168.255.255`
- `192.168.0.0/24`
- `192.168.2-3.0-128`
- `2001:db8:fd0c::/64`
- `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← مكافحة أداة التشفير**.
4. في القسم **استثناءات الفحص**، انقر على الزر **حسب الاسم أو عنوان IP**.
5. 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 الزر ← **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.
6. لاستيراد قائمة الاستثناءات:
   a. انقر على الزر ← **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.

7. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة الاستثناءات في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Anti-Cryptor** ← **Behavior Analysis** ← **Host Threat Protection**.

5. انقر على رابط **Exclusions by name or IP address**.

6. لتصدير قائمة القواعد:

a. حدد الاستثناءات التي تريد تصديرها.

b. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات إلى ملف JSON في مجلد التنزيلات الافتراضي.

7. لاستيراد قائمة الاستثناءات:

a. انقر على الزر ← **Import**.

في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد قائمة الاستثناءات منه.

b. 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 JSON.

8. احفظ تغييراتك.

محرك المعالجة

يتيح مكون 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة ← محرك المعالجة**.
4. استخدم خانة الاختيار **محرك المعالجة** لتمكين المكون أو تعطيله.
5. احفظ تغييراتك.

كيفية تمكين أو تعطيل مكون محرك المعالجة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Remediation Engine ← Behavior Analysis ← Host Threat Protection**.

5. استخدم مفتاح تبديل **Remediation Engine ENABLED** 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.

قد لا تكون وظيفة KSN متاحة في التطبيق في الولايات المتحدة.

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. في حال مشاركتك في Kaspersky Security Network (KSN)، فإن خدمات KSN تزود Kaspersky Endpoint Security بمعلومات عن سمعة عناوين الويب المفحوصة، بالإضافة إلى معلومات عن فئة وسمعة الملفات التي يتم فحصها. وللمزيد من التفاصيل عن تكوين الوصول إلى KSN، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

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.

تمكين وتعطيل استخدام Kaspersky Security Network

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.

كيفية تمكين أو تعطيل استخدام KSN في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **Kaspersky Security Network**.
4. 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.
5. إذا لزم الأمر، امسح خانة الاختيار **تمكين وضع KSN الموسع**. بشكل افتراضي، يتم تمكين وضع KSN الموسع.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل استخدام KSN في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Kaspersky Security Network**.

5. استخدم مفتاح تبديل **Use of Kaspersky Security Network (KSN) ENABLED** 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.

6. عند الحاجة، قم بتغيير خانة الاختيار **Use extended KSN mode** إلى إيقاف التشغيل. بشكل افتراضي، يتم تمكين وضع KSN الموسع.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل استخدام KSN في واجهة التطبيق

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.

4. عند الحاجة، قم بتغيير خانة الاختيار **تمكين وضع KSN الموسع** إلى إيقاف التشغيل. بشكل افتراضي، يتم تمكين وضع KSN الموسع.

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.

- يتصل Kaspersky Endpoint Security في وضع Light Agent مع خوادم KSN من خلال خادم وكيل KSN. الاتصال المباشر مع KSN غير مدعوم.

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.

إذا كان التطبيق يعمل في وضع Light Agent، فإن وضع السحابة غير متاح.

كيفية تمكين أو تعطيل الوضع السحابي لمكونات الحماية في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **Kaspersky Security Network**.
4. استخدم خانة الاختيار **تمكين وضع السحابة** لتمكين المكون أو تعطيله.
5. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل الوضع السحابي لمكونات الحماية في Web Control وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Kaspersky Security Network**.
5. استخدم مفتاح تبديل **Use cloud mode** لتمكين المكون أو تعطيله.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين أو تعطيل الوضع السحابي لمكونات الحماية في واجهة التطبيق

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 KSN إما مباشرة أو عبر خدمة KSN Proxy.

إذا كان التطبيق يعمل في وضع Light Agent، فإن الاتصال المباشر مع KSN غير مدعوم. ويتصل Kaspersky Endpoint Security بخوادم KSN من خلال خادم وكيل KSN.

توفر خدمة KSN Proxy الإمكانيات التالية:

- يستطيع كمبيوتر المستخدم الاستعلام بسرعة من KSN وتقديم المعلومات إليها، حتى بدون الوصول المباشر إلى الإنترنت.
- تخزن خدمة KSN Proxy 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 KSN Proxy على النحو التالي: تمكين أو تعطيل KSN Proxy، وتكوين المنفذ للاتصال. ولفعل ذلك، تحتاج إلى فتح خصائص خادم الإدارة. وللمزيد من التفاصيل عن تكوين KSN Proxy، يُرجى الرجوع إلى تعليمات Kaspersky Security Center. ويمكنك أيضًا تمكين أو تعطيل KSN Proxy لأجهزة الكمبيوتر الفردية في سياسة Kaspersky Endpoint Security.

كيفية تمكين أو تعطيل وكيل KSN في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الحماية من التهديدات المتقدمة** ← **Kaspersky Security Network**.
4. في القسم **إعدادات وكيل KSN**، استخدم خانة الاختيار **استخدام خادم الإدارة كخادم وكيل لشبكة KSN** لتمكين أو تعطيل وكيل KSN.

5. وإذا لزم الأمر، حدد خانة الاختيار **استخدام خوادم Kaspersky Security Network عندما يكون الخادم الوكيل لشبكة KSN غير متاح**.

إذا تم تحديد خانة الاختيار، سيستخدم Kaspersky Endpoint Security خوادم شبكة KSN عند عدم توافر خدمة KSN Proxy. قد يتم وضع خوادم KSN على جانب Kaspersky وعلى جانب أطراف خارجية (عند استخدام Kaspersky Private Security Network).

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل وكيل KSN في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **General Settings** ← **Kaspersky Security Network**.

5. استخدم خانة الاختيار **Use Administration Server as a KSN proxy server** لتمكين أو تعطيل KSN Proxy.

6. وإذا لزم الأمر، حدد خانة الاختيار **Use Kaspersky Security Network servers if the KSN proxy server is unavailable**.

إذا تم تحديد خانة الاختيار، سيستخدم Kaspersky Endpoint Security خوادم شبكة KSN عند عدم توافر خدمة KSN Proxy. قد يتم وضع خوادم KSN على جانب Kaspersky وعلى جانب أطراف خارجية (عند استخدام Kaspersky Private Security Network). بشكل افتراضي، يتم إلغاء تحديد خانة الاختيار.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

يتطابق عنوان KSN Proxy مع عنوان خادم الإدارة. وعندما يتم تغيير اسم مجال خادم الإدارة، فأنت بحاجة إلى تحديث عنوان KSN Proxy يدويًا.

لتكوين عنوان وكيل KSN:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Remote installation** ← **Advanced** ← مجلد **Installation packages**.

3. في قائمة السياق الخاصة بالمجلد **Installation packages**، حدد **Properties**.

4. في علامة التبويب **General** في النافذة المفتوحة، حدد العنوان الجديد لخادم وكيل KSN.

5. 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). يعتبر التطبيق الملف موثوقًا به في حالة استيفاء شرط واحد أو أكثر من الشروط التالية:

- تم توقيع الملف رقميًا بواسطة بائع موثوق؛
- يتمتع الملف بسمعة موثوقة في Kaspersky Security Network؛
- وضع المستخدم الملف في المجموعة "موثوق".

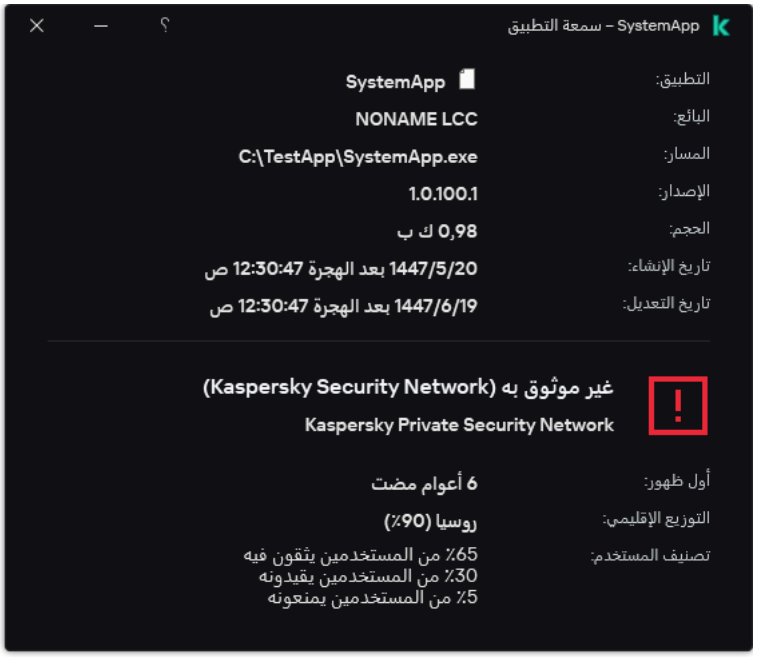
برامج قانونية يمكن أن يستخدمها المجرمون لإتلاف جهازك أو بياناتك الشخصية. رغم أنها لا تحتوي على أي وظائف ضارة، إلا أنه المتسللين يستطيعون استغلال هذه التطبيقات. وللحصول على تفاصيل عن البرامج الشرعية التي يمكن أن يستخدمها المجرمون لإلحاق الضرر بالكمبيوتر أو البيانات الشخصية للمستخدم، يرجى الرجوع إلى موقع 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 واكتشاف السلوك ومنع الاستغلال 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

بشكل افتراضي، لا يفحص Kaspersky Endpoint Security دائمًا الاتصالات المشفرة، لكن فقط عندما تطلبه مكونات الحماية.

كيفية تمكين فحص الاتصالات المشفرة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
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**، حدد وضع فحص الاتصال المشفر:

- **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.

6. يمكنك عند الضرورة إضافة الاستثناءات من الفحص: العناوين والتطبيقات الموثوقة.

7. يمكنك تكوين الإعدادات لفحص الاتصالات المشفرة (انظر الجدول أدناه).

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين فحص الاتصالات المشفرة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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. تحت **Encrypted Connections Scan**، قم بتشغيل مفتاح **Encrypted Connections Scan ENABLED**.
في حالة إيقاف تشغيل مفتاح التبديل، لن يتمكن Kaspersky Endpoint Security من الوصول إلى محتويات مواقع الويب التي تبدأ بالحروف `https://`.

6. انقر على **Settings** وحدد وضع فحص الاتصال المشفر:

- **Scan encrypted connections upon request from protection components**. سوف يفحص Kaspersky Endpoint Security الحركة المشفرة فقط عند طلبها بواسطة مكونات الحماية من تهديدات الويب والحماية من تهديدات البريد والتحكم في الويب.
- **Always scan encrypted connections**. 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.

7. يمكنك عند الضرورة إضافة الاستثناءات من الفحص: العناوين والتطبيقات الموثوقة.

8. يمكنك تكوين الإعدادات لفحص الاتصالات المشفرة (انظر الجدول أدناه).

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين فحص الاتصالات المشفرة في واجهة التطبيق

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.
زيارة مجال بشهادة 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**. 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.
زيارة مجال يتضمن خطأ في فحص الاتصالات المشفرة	• **منع**. في حالة ظهور خطأ في فحص الاتصالات المشفرة، يحظر Kaspersky Endpoint Security اتصال الشبكة. • **السماح بالمجال وإضافته إلى الاستثناءات**. في حالة 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**. ينشئ Kaspersky Endpoint Security أيضًا حدثًا لخطأ فحص الاتصال المشفر.
منع اتصالات SSL 2.0	في حالة تحديد خانة الاختيار، يراقب التطبيق ويحظر 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. ومع ذلك، لا يراقب التطبيق حركة شبكة الاتصال عبر هذا البروتوكول.
منع اتصالات SSL 3.0	في حالة تحديد خانة الاختيار، لن يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 3.0. في حالة إلغاء تحديد خانة الاختيار، لا يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 3.0. ويراقب التطبيق حركة شبكة الاتصال عبر هذا البروتوكول. وتعمل جميع مكونات التطبيق دون قيود.

المعلمة	الوصف
منع اتصالات TLS 1.0	في حالة تحديد خانة الاختيار، لن يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول TLS 1.0. في حالة إلغاء تحديد خانة الاختيار، لا يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول TLS 1.0. ويراقب التطبيق حركة شبكة الاتصال عبر هذا البروتوكول. وتعمل جميع مكونات التطبيق دون قيود.
فك تشفير اتصال مشفر بموقع الويب الذي يستخدم شهادات تحقق من الصحة موسعة	تؤكد شهادات EV (Extended Validation Certificate) 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.
4. في القسم **شهادات الجذر الموثوق بها**، انقر على الزر **إضافة**.
5. يفتح هذا نافذة؛ وفي تلك النافذة، حدد شهادة جذر موثوقًا بها.
   يدعم Kaspersky Endpoint Security الشهادات بملحقات PEM وDER وCRT.
6. احفظ تغييراتك.

كيفية تثبيت شهادات الجذر الموثوق بها في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.
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.

  في بعض الحالات، يتعذر على Kaspersky Endpoint Security عرض صفحة HTML من الناحية الفنية مع تحذير في المستعرض (انظر الشكل أدناه). على سبيل المثال، إذا كان مورد الويب يستخدم إصدارًا قديمًا من بروتوكول شبكة الاتصال ومنفذًا غير قياسي. وفي هذه الحالات، يمنع Kaspersky Endpoint Security الوصول إلى هذا المجال وسيعرض المستعرض نافذة `ERR_CONNECTION_RESET` القياسية. وللوصول إلى مورد ويب، ذلك إضافة مجال إلى الاستثناءات أو استخدم شهادة موثوقة.

- 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.

4. في القسم **فحص الاتصالات المشفرة**، انقر على الزر **إعدادات متقدمة**.

5. في النافذة التي تفتح، حدد وضع تشغيل التطبيق عند زيارة مجال له شهادة غير موثوق بها: **سماح** أو **منع**.

6. احفظ تغييراتك.

كيفية تكوين فحص الاتصالات المشفرة بشهادة غير موثوقة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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 الرابط **Settings**.

6. في النافذة التي تفتح، حدد وضع تشغيل التطبيق عند زيارة مجال له شهادة غير موثوق بها: **Allow connection** أو **Block connection**.

7. 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: **سماح** أو **منع**.

4. احفظ تغييراتك.



تحذير عند زيارة مجال له شهادة غير موثوق بها

إضافة شهادة Kaspersky إلى مخزن الشهادات الخاص

تستخدم المستعرضات وعملاء البريد الشهادة للتحقق من أمان ومصادقة موارد الويب. وتوفر الشهادة أيضًا تشفير البيانات بين موارد الويب والمستخدم. وتستخدم معظم المستعرضات وعملاء البريد مخزن الشهادات الموثوق به (مخزن شهادات Windows). على سبيل المثال، Google Chrome. وتستخدم بعض المستعرضات وعملاء البريد مخزن الشهادات الخاص بها بشكل افتراضي بدلاً من مخزن شهادات Windows. على سبيل المثال، Firefox وThunderbird.

بعد التثبيت، يضيف Kaspersky Endpoint Security شهادة Kaspersky إلى محزن النظام للحصول على شهادات موثوقة (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 المستعرضات وعملاء البريد لفحص حركة مرور هذه التطبيقات. وإذا لم يتم تطبيق سياسة ما على الكمبيوتر، فيمكنك اختيار مخزن الشهادة الذي سيُستخدم بواسطة المستعرضات وعملاء البريد. وإذا حددت مخزن الشهادات الخاص، فأضف شهادة Kaspersky إلى المتجر يدويًا. 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. ويجب أيضًا تمكين فحص الاتصالات المشفرة لفحص حركة البيانات في عميلي البريد MyOffice Mail وR7-Office Organizer.

قبل إضافة شهادة إلى المستعرض أو مخزن الشهادات الخاص بعميل البريد، قم بتصدير شهادة Kaspersky من لوحة تحكم Windows (خصائص الإنترنت). ويمكنك معرفة المزيد عن إضافة شهادة إلى المخزن، على سبيل المثال، في موقع ويب الدعم الفني من Mozilla.

يمكنك اختيار مخزن الشهادات فقط في الواجهة المحلية للتطبيق.

لاختيار مخزن شهادات لفحص الاتصالات المشفرة في المستعرضات وعملاء البريد:

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 خانة الاختيار **لفحص الاتصالات المشفرة في التطبيقات باستخدام مخزن الشهادات الخاص بها، استخدم**.
4. تحديد مخزن شهادات:
   - **مخزن شهادات Windows (مستحسن)**. تتم إضافة شهادة جذر Kaspersky إلى هذا المخزن أثناء تثبيت Kaspersky Endpoint Security.
   - **مخزن الشهادات الخاص**. 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.

     يستخدم عميلا البريد MyOffice Mail وR7-Office Organizer أيضًا مخزن الشهادات الخاص بهما.
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 وWeb Control 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 **Policies**.
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 **تكوين 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. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية استثناء عنوان ويب من عمليات فحص الاتصال المشفر في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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 domains**.

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. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ 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 **تكوين 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 التي تتضمن أخطاء فحص**.

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.

منع الوصول إلى المجالات ذات الشهادات غير الموثوقة

في بعض الحالات، عند حظر الوصول إلى مجال بشهادة غير موثوقة، يعرض Kaspersky Endpoint Security صفحة تحذير بتنسيق HTML في المستعرض ينقصها الرابط المؤدي إلى مورد الويب المطلوب.

يمكن أن يحدث هذا للأسباب التالية:

- منع المسؤول الوصول إلى مجال بشهادات غير موثوقة.
- يحتوي المجال على شهادة غير موثوقة أو غير صالحة، ويستخدم خادم الويب آلية HTTP Strict Transport Security (HSTS). وHSTS هي آلية أمان تفرض استخدام بروتوكول HTTPS الآمن للاتصال بين عميل وخادم ويب. وفي هذه الحالة، لا يمكنك الوصول إلى المجال حتى إذا أضفته إلى قائمة العناوين الموثوقة. وتم وصف آلية HSTS في RFC 6797.

في بعض الحالات، يمكن فتح موقع الويب مباشرة في المستعرض دون استخدام Kaspersky Endpoint Security. ولا تكتشف المستعرضات دائمًا الشهادات الملغاة، بينما يجري Kaspersky Endpoint Security فحصًا عبر الإنترنت لإلغاء الشهادة عند إنشاء اتصال. ويسمح هذا للتطبيق باكتشاف مشكلة الشهادة قبل أن يفعل المستعرض ذلك ويعرض رسالة الخطأ المقابلة.



تحذير عند زيارة مجال له شهادة غير موثوق بها

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 نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.
2. انقر على **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.
   b. في القائمة المنسدلة **Task type**، حدد **Wipe data**.
   c. في حقل **Task name** أدخل وصفًا موجزًا، على سبيل المثال، مسح البيانات (مكافحة السرقة).
   d. في القسم **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. قم بإنهاء 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 حذف البيانات المؤجل، ضع في اعتبارك أن الموظفين قد يكون لديهم جداول عمل مختلفة. 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 إيقاف تشغيل الكمبيوتر وتغيب الاتصال لفترة أطول من المدة التي تم تكوينها، بعد تشغيل الكمبيوتر، لا يحذف Kaspersky Endpoint Security البيانات على الفور. وينتظر التطبيق المزامنة مع Kaspersky Security Center لمدة ساعة واحدة. ويعد ذلك ضروريًا لمنع حذف البيانات غير المصرح به على أجهزة كمبيوتر المستخدمين الذين أوقفوا تشغيل أجهزة الكمبيوتر الخاصة بهم، على سبيل المثال، قبل الذهاب في عطلة.

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 فوق **Start**.

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 الكمبيوتر

التحكم في الويب

يقوم المكون التحكم في الويب بإدارة وصول المستخدم 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).

لاستخدام التحكم في الويب، يجب عليك إكمال التكوين الأولي للتطبيق:

- لمراقبة حركة مرور HTTPS، قم بتمكين فحص الاتصالات المشفرة (يتم التمكين بشكل افتراضي).
- حدد المنافذ التي يجب أن يراقبها Kaspersky Endpoint Security (بشكل افتراضي، يراقب التطبيق كل المنافذ).
- حدد التطبيقات التي تريد أن يراقب Kaspersky Endpoint Security حركة البيانات الخاصة بها. وتوجد معظم المستعرضات بالفعل في قائمة التطبيقات التي أوصت بها Kaspersky. وإذا كان المستعرض الخاص بك مفقودًا من القائمة، فقم بإضافته يدويًا.
- نوصي بإدخال برنامج نصي لتفاعل صفحة الويب في حركة مرور الويب (بشكل افتراضي، يتم تعطيل إدخال البرنامج النصي). يتيح هذا البرنامج النصي تسجيل أحداث التحكم في الويب لسجل أحداث التطبيق، وسجل أحداث نظام التشغيل، والتقارير.

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 المستخدم إلى البيانات الموجودة على موقع الويب، وإخفاء الصور، 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 تطبيقات Office فقط لفئة 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.

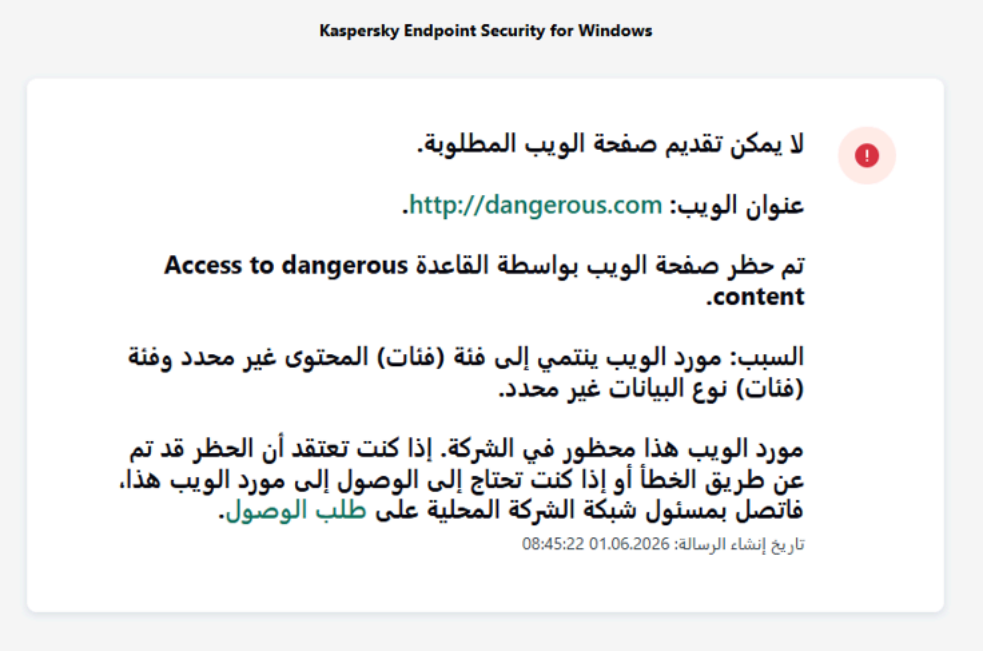
  على سبيل المثال، يمكنك تقييد وصول جميع مستخدمي الشركة إلى الإنترنت من خلال المستعرض باستثناء قسم تكنولوجيا المعلومات.

- 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

إضافة قاعدة وصول إلى موارد الويب

قاعدة الوصول إلى موارد الويب هي مجموعة من عوامل التصفية والإجراءات التي يطبقها Kaspersky Endpoint Security عندما يزور المستخدمون موارد الويب. ويمكن أن تتضمن قواعد الوصول جدولًا زمنيًا للقواعد.

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.

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.

كيفية إضافة قاعدة الوصول إلى موارد الويب في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الويب**.
4. حدد خانة الاختيار **التحكم في الويب**.
5. في القسم **إعدادات التحكم في الويب**، انقر على الزر **إضافة**.
   تفتح النافذة **قاعدة الوصول إلى موارد الويب**.
6. كوّن قاعدة الوصول إلى موارد الويب (انظر الجدول أدناه).
7. إذا كنت تريد أن ينهي WebControl الاتصال بمورد الويب المحظور مباشرة بعد تطبيق السياسة، فحدد خانة الاختيار **إنهاء جلسات مستعرض المستخدم النشطة بعد تطبيق القاعدة**.

يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط.

إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

8. احفظ تغييراتك.

كيفية إضافة قاعدة الوصول إلى موارد الويب في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
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. قم بتشغيل مفتاح **Web Control ENABLED**.
6. في القسم **Rules list**، انقر على الزر **Add**.
7. كوّن قاعدة الوصول إلى موارد الويب (انظر الجدول أدناه).
8. إذا كنت تريد أن ينهي WebControl الاتصال بمورد الويب المحظور مباشرة بعد تطبيق السياسة، فحدد خانة الاختيار **Terminate active user browser sessions after the rule is applied**.

يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط.

إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

9. احفظ تغييراتك.

كيفية إضافة قاعدة الوصول إلى موارد الويب في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.



إعدادات التحكم في الويب

3. قم بتشغيل مفتاح **التحكم في الويب**.

4. في القسم **الإعدادات**، انقر على الزر **قواعد الوصول إلى موارد الويب**.

5. في النافذة التي تفتح، انقر فوق الزر **إضافة**.

تفتح النافذة **قاعدة الوصول إلى موارد الويب**.

6. كوّن قاعدة الوصول إلى موارد الويب (انظر الجدول أدناه).

7. إذا كنت تريد أن ينهي WebControl الاتصال بمورد الويب المحظور مباشرة بعد تطبيق السياسة، فحدد خانة الاختيار **إنهاء جلسات مستعرض المستخدم النشطة بعد تطبيق القاعدة**.

يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط.

إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

8. احفظ تغييراتك.

نتيجة لذلك، تتم إضافة قاعدة التحكم في الويب الجديدة إلى القائمة. إذا لزم الأمر، قم بتغيير أولوية قاعدة التحكم في الويب. ويمكنك أيضًا استخدام مفتاح التبديل لتعطيل قاعدة الوصول إلى موارد الويب في أي وقت دون إزالتها من القائمة.

معلمات قاعدة التحكم في الويب

المعلمة	الوصف
اسم القاعدة	اسم قاعدة التحكم في الويب.
الحالة	• **تشغيل**. • **إيقاف التشغيل**. يمكنك استخدام مفتاح التبديل لتعطيل قاعدة الوصول إلى موارد الويب في أي وقت.
الإجراء	• **سماح**. يسمح التحكم في الويب بالوصول إلى موارد الويب التي تطابق معلمات القاعدة. • **منع**. يمنع التحكم في الويب الوصول إلى موارد الويب التي تطابق معلمات القاعدة ويعرض رسالة رفض الوصول إلى موقع الويب. • **تحذير**. عندما يحاول المستخدم الوصول إلى مورد ويب يطابق القاعدة، يعرض التحكم في الويب تحذيرًا بأن زيارة مورد الويب غير مستحسن. عن طريق استخدام الارتباطات من رسالة التحذير، يمكن للمستخدم التمتع بالوصول إلى مورد الويب المطلوب.
محتوى عامل التصفية	• **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).
العناوين	• **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. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال. إذا كان فحص الاتصالات المشفرة معطلاً، فبالنسبة لبروتوكول HTTPS، فيمكنك التصفية فقط عن طريق اسم الخادم.
المستخدمون	• **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. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.
جدولة القاعدة	يحدد جدول القاعدة الفترة الزمنية التي يقوم خلالها Kaspersky Endpoint Security بمراقبة الوصول إلى موارد الويب الخاضعة للقاعدة. على سبيل المثال، يمكنك تقييد الوصول إلى الإنترنت من خلال المستعرض خلال ساعات العمل فقط.

التصفية حسب عناوين موارد الويب

للتحكم في الوصول إلى موارد الويب الفردية، يجب عليك إنشاء قاعدة التحكم في الويب، وإنشاء قائمة بعناوين الويب، وتحديد إجراء التحكم في الويب. وعند إنشاء قائمة عناوين الويب، يمكنك إدخال عناوين URL أو استخدام الأقنعة.

قد تتضمن القواعد جدولًا زمنيًا للقواعد وقائمة بالمستخدمين الذين تنطبق عليهم القاعدة. على سبيل المثال، يمكنك تقييد الوصول إلى مواقع الويب أثناء ساعات العمل فقط، أو السماح بزيارة مواقع الويب لمستخدمين في مجموعات معينة.

كيفية تمكين عامل تصفية عنوان مورد الويب في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الويب**.

4. حدد خانة الاختيار **التحكم في الويب**.

5. في القسم **إعدادات التحكم في الويب**، انقر على الزر **إضافة**.
تفتح النافذة **قاعدة الوصول إلى موارد الويب**.

6. لتكوين قاعدة الوصول إلى موارد الويب:

a. في الحقل **الاسم** أدخل اسم القاعدة.

b. في القائمة المنسدلة **تطبيق على العناوين** حدد **على العناوين الفردية**.

c. أنشئ قائمة بعناوين موارد الويب. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT.

إذا كان فحص الاتصالات المشفرة معطلاً، فبالنسبة لبروتوكول HTTPS، فيمكنك التصفية فقط عن طريق اسم الخادم.

d. في القائمة المنسدلة **تطبيق على المستخدمين**، حدد عامل التصفية ذي الصلة للمستخدمين:

- **على جميع المستخدمين**. لن يقوم التحكم في الويب بتصفية موارد الويب حسب العنوان.
- **على مستخدمين أفراد أو مجموعات**. سيقوم التحكم في الويب بتصفية عناوين موارد الويب فقط من القائمة. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

e. في القائمة المنسدلة **الإجراء**، حدد خيارًا:

- **سماح**. يسمح التحكم في الويب بالوصول إلى موارد الويب التي تطابق معلمات القاعدة.
- **منع**. يمنع التحكم في الويب الوصول إلى موارد الويب التي تطابق معلمات القاعدة ويعرض رسالة رفض الوصول إلى موقع الويب.
- **تحذير**. عندما يحاول المستخدم الوصول إلى مورد ويب يطابق القاعدة، يعرض التحكم في الويب تحذيرًا بأن زيارة مورد الويب غير مستحسن. عن طريق استخدام الارتباطات من رسالة التحذير، يمكن للمستخدم التمتع بالوصول إلى مورد الويب المطلوب.

f. في القائمة المنسدلة **جدولة القاعدة**، حدد جدولاً أو أنشئ جدولاً جديدًا.

7. إذا كنت تريد أن ينهي WebControl الاتصال بمورد الويب المحظور مباشرة بعد تطبيق السياسة، فحدد خانة الاختيار **إنهاء جلسات مستعرض المستخدم النشطة بعد تطبيق القاعدة**.

يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط.

إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

8. احفظ تغييراتك.

كيفية تمكين عامل تصفية عنوان مورد الويب في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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. قم بتشغيل مفتاح **Web Control ENABLED**.

6. في القسم **Rules list**، انقر على الزر **Add**.

7. لتكوين قاعدة الوصول إلى موارد الويب:

a. في الحقل **Rule name** أدخل اسم القاعدة.

b. حدد الحالة **Enabled** لقاعدة الوصول إلى موارد الويب.
يمكنك استخدام مفتاح التبديل لتعطيل قاعدة الوصول إلى موارد الويب في أي وقت دون إزالتها من القائمة.

c. في القسم **Action**، حدد الخيار المناسب:

- **Allow**. يسمح التحكم في الويب بالوصول إلى موارد الويب التي تطابق معلمات القاعدة.
- **Block**. يمنع التحكم في الويب الوصول إلى موارد الويب التي تطابق معلمات القاعدة ويعرض رسالة رفض الوصول إلى موقع الويب.
- **Inform**. عندما يحاول المستخدم الوصول إلى مورد ويب يطابق القاعدة، يعرض التحكم في الويب تحذيرًا بأن زيارة مورد الويب غير مستحسن. عن طريق استخدام الارتباطات من رسالة التحذير، يمكن للمستخدم التمتع بالوصول إلى مورد الويب المطلوب.

d. تحت **Scope**، حدد **Individual websites**.

e. تكوين عامل تصفية المحتوى:

- **Individual address**. أنشئ قائمة بعناوين موارد الويب. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT.

إذا كان فحص الاتصالات المشفرة معطلاً، فبالنسبة لبروتوكول HTTPS، فيمكنك التصفية فقط عن طريق اسم الخادم.

- **Data type**. يمكنك التحكم في وصول المستخدم إلى موارد الويب بناءً على نوع البيانات المحدد لبياناته المنشورة (على سبيل المثال، الرسومات).

f. تحت **User or group**، حدد المستخدمين الذين تريد أن يطبق Web Control القاعدة عليهم.
سيقوم التحكم في الويب بتصفية عناوين موارد الويب فقط من القائمة. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

g. في القسم **Access schedule**، حدد جدولاً أو أنشئ جدولاً جديدًا.

8. احفظ تغييراتك.

كيفية تمكين عامل تصفية عنوان مورد ويب في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.



إعدادات 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**. يسمح التحكم في الويب بالوصول إلى موارد الويب التي تطابق معلمات القاعدة.
- **منع**. يمنع التحكم في الويب الوصول إلى موارد الويب التي تطابق معلمات القاعدة ويعرض رسالة رفض الوصول إلى موقع الويب.
- **تحذير**. عندما يحاول المستخدم الوصول إلى مورد ويب يطابق القاعدة، يعرض التحكم في الويب تحذيرًا بأن زيارة مورد الويب غير مستحسن. عن طريق استخدام الارتباطات من رسالة التحذير، يمكن للمستخدم التمتع بالوصول إلى مورد الويب المطلوب.

8. تحت **العناوين**، حدد **على العناوين الفردية**.

أنشئ قائمة بعناوين موارد الويب. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT.

إذا كان فحص الاتصالات المشفرة معطلاً، فبالنسبة لبروتوكول HTTPS، فيمكنك التصفية فقط عن طريق اسم الخادم.

9. 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 عناوين موارد الويب فقط من القائمة. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

10. في القائمة المنسدلة **جدولة القاعدة**، حدد جدولاً أو أنشئ جدولاً جديدًا.

11. إذا كنت تريد أن ينهي WebControl الاتصال بمورد الويب المحظور مباشرة بعد تطبيق السياسة، فحدد خانة الاختيار **إنهاء جلسات مستعرض المستخدم النشطة بعد تطبيق القاعدة**.

يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط.

إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

12. احفظ تغييراتك.

نتيجة لذلك، تتم إضافة قاعدة التحكم في الويب الجديدة إلى القائمة. إذا لزم الأمر، قم بتغيير أولوية قاعدة التحكم في الويب. ويمكنك أيضًا استخدام مفتاح التبديل لتعطيل قاعدة الوصول إلى موارد الويب في أي وقت دون إزالتها من القائمة.

التصفية حسب محتوى مورد الويب

للتحكم في الوصول عن طريق محتوى موارد الويب، يوفر التحكم في الويب عامل تصفية للفئة وعامل تصفية لنوع البيانات.

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.

يمكنك تقييد وصول المستخدم إلى موقع ويب بناءً على نوع البيانات، على سبيل المثال، لإخفاء الصور. يحدد برنامج Kaspersky Endpoint Security نوع البيانات بناءً على تنسيق الملف وليس بناءً على ملحقاته. ويميز التحكم في الويب بين أنواع البيانات التالية:

- الفيديو
- صوت
- ملفات تطبيقات Office
- الملفات القابلة للتنفيذ
- الأرشيفات

- الرسومات
- البرامج النصية

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.

قد تتضمن القواعد جدولًا زمنيًا للقواعد وقائمة بالمستخدمين الذين تنطبق عليهم القاعدة. على سبيل المثال، يمكنك تقييد الوصول إلى مواقع الويب أثناء ساعات العمل فقط، أو السماح بزيارة مواقع الويب لمستخدمين في مجموعات معينة.

كيفية تمكين عامل تصفية محتوى موارد الويب في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الويب**.
4. حدد خانة الاختيار **التحكم في الويب**.
5. في القسم **إعدادات التحكم في الويب**، انقر على الزر **إضافة**.
   تفتح النافذة **قاعدة الوصول إلى موارد الويب**.
6. لتكوين قاعدة الوصول إلى موارد الويب:
   a. في الحقل **الاسم** أدخل اسم القاعدة.
   b. في القائمة المنسدلة **تصفية المحتوى**، 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).
   - **حسب فئات المحتوى وأنواع البيانات**. يتم تمكين عوامل التصفية حسب فئات المحتوى وأنواع البيانات.

   بعد تحديد عوامل التصفية، قم بتكوين معلمات عامل التصفية.
   c. في القائمة المنسدلة **تطبيق على المستخدمين**، حدد عامل التصفية ذي الصلة للمستخدمين:
   - **على جميع المستخدمين**. لن يقوم التحكم في الويب بتصفية موارد الويب حسب العنوان.
   - **على مستخدمين أفراد أو مجموعات**. سيقوم التحكم في الويب بتصفية عناوين موارد الويب فقط من القائمة. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

d. في القائمة المنسدلة **الإجراء**، حدد خيارًا:

- **سماح**. يسمح التحكم في الويب بالوصول إلى موارد الويب التي تطابق معلمات القاعدة.
- **منع**. يمنع التحكم في الويب الوصول إلى موارد الويب التي تطابق معلمات القاعدة ويعرض رسالة رفض الوصول إلى موقع الويب.
- **تحذير**. عندما يحاول المستخدم الوصول إلى مورد ويب يطابق القاعدة، يعرض التحكم في الويب تحذيرًا بأن زيارة مورد الويب غير مستحسن. عن طريق استخدام الارتباطات من رسالة التحذير، يمكن للمستخدم التمتع بالوصول إلى مورد الويب المطلوب.

e. في القائمة المنسدلة **جدولة القاعدة**، حدد جدولاً أو أنشئ جدولاً جديدًا.

7. إذا كنت تريد أن ينهي WebControl الاتصال بمورد الويب المحظور مباشرة بعد تطبيق السياسة، فحدد خانة الاختيار **إنهاء جلسات مستعرض المستخدم النشطة بعد تطبيق القاعدة**.

يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط.

إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

8. احفظ تغييراتك.

كيفية تمكين عامل تصفية محتوى مورد الويب في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
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. قم بتشغيل مفتاح **Web Control ENABLED**.
6. في القسم **Rules list**، انقر على الزر **Add**.
7. لتكوين قاعدة الوصول إلى موارد الويب:
   a. في الحقل **Rule name** أدخل اسم القاعدة.
   b. حدد الحالة **Enabled** لقاعدة الوصول إلى موارد الويب.
   يمكنك استخدام مفتاح التبديل لتعطيل قاعدة الوصول إلى موارد الويب في أي وقت.
   c. في القسم **Action**، حدد الخيار المناسب:
   - **Allow**. يسمح التحكم في الويب بالوصول إلى موارد الويب التي تطابق معلمات القاعدة.
   - **Block**. يمنع التحكم في الويب الوصول إلى موارد الويب التي تطابق معلمات القاعدة ويعرض رسالة رفض الوصول إلى موقع الويب.
   - **Inform**. عندما يحاول المستخدم الوصول إلى مورد ويب يطابق القاعدة، يعرض التحكم في الويب تحذيرًا بأن زيارة مورد الويب غير مستحسن. عن طريق استخدام الارتباطات من رسالة التحذير، يمكن للمستخدم التمتع بالوصول إلى مورد الويب المطلوب.

   d. تحت **Scope**، حدد **Content category**.

e. تكوين عامل تصفية المحتوى:

- **Content category**. يمكنك التحكم في وصول المستخدم إلى موارد الويب حسب category (على سبيل المثال، فئة الشبكات الاجتماعية).
- **Data type**. يمكنك التحكم في وصول المستخدم إلى موارد الويب بناءً على نوع البيانات المحدد لبياناته المنشورة (على سبيل المثال، الرسومات).

f. تحت **User or group**، حدد المستخدمين الذين تريد أن يطبق Web Control القاعدة عليهم.

سيقوم التحكم في الويب بتصفية عناوين موارد الويب فقط من القائمة. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

g. في القسم **Access schedule**، حدد جدولاً أو أنشئ جدولاً جديدًا.

8. احفظ تغييراتك.

كيفية تمكين عامل تصفية محتوى مورد ويب في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.



إعدادات 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**. يسمح التحكم في الويب بالوصول إلى موارد الويب التي تطابق معلمات القاعدة.
- **منع**. يمنع التحكم في الويب الوصول إلى موارد الويب التي تطابق معلمات القاعدة ويعرض رسالة رفض الوصول إلى موقع الويب.
- **تحذير**. عندما يحاول المستخدم الوصول إلى مورد ويب يطابق القاعدة، يعرض التحكم في الويب تحذيرًا بأن زيارة مورد الويب غير مستحسن. 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 **المستخدمون**، حدد عامل التصفية المناسب للمستخدمين:

- **على جميع المستخدمين**. لن يقوم التحكم في الويب بتصفية موارد الويب حسب العنوان.
- **على مستخدمين أفراد و/أو مجموعات**. سيقوم التحكم في الويب بتصفية عناوين موارد الويب فقط من القائمة. يمكنك إدخال عنوان الويب أو استخدام الأقنعة. يمكنك أيضًا تصدير قائمة بعناوين موارد الويب من ملف TXT. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال. لإنشاء قائمة بالمستخدمين الذين تريد تطبيق القاعدة عليهم:

a. انقر على **إضافة**.

b. في النافذة التي تفتح، حدد المستخدمين أو مجموعات المستخدمين الذين تريد تطبيق قاعدة الوصول إلى موارد الويب عليهم.

c. ارجع إلى النافذة لتكوين قاعدة الوصول إلى مورد الويب.

10. 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.

11. إذا كنت تريد أن ينهي WebControl الاتصال بمورد الويب المحظور مباشرة بعد تطبيق السياسة، فحدد خانة الاختيار **إنهاء جلسات مستعرض المستخدم النشطة بعد تطبيق القاعدة**.

يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط.

إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

12. احفظ تغييراتك.

نتيجة لذلك، تتم إضافة قاعدة التحكم في الويب الجديدة إلى القائمة. إذا لزم الأمر، قم بتغيير أولوية قاعدة التحكم في الويب. ويمكنك أيضًا استخدام مفتاح التبديل لتعطيل قاعدة الوصول إلى موارد الويب في أي وقت دون إزالتها من القائمة.

اختبار قواعد الوصول إلى موارد الويب

عند تكوين التحكم في الويب، قد تمنع دون قصد الوصول إلى موارد الويب التي يحتاجها المستخدمون لعملهم. ولمعرفة قاعدة التحكم في الويب التي تمنع الوصول إلى موارد الويب، يمكنك استخدام أداة تشخيص قواعد التحكم في الويب. وتتوفر تشخيصات قواعد التحكم في الويب فقط في واجهة Kaspersky Endpoint Security. وفي وحدة تحكم Kaspersky Security Center، لا يمكنك معرفة قاعدة التحكم في الويب التي تتضمن موردًا معينًا.

إذا اعتقد المستخدم أنه قد تم منع مورد الويب عن طريق الخطأ، يمكن للمستخدم النقر فوق الرابط في رسالة إخطار منع مورد الويب لإرسال رسالة التي تم إنشاؤها مسبقًا إلى مسؤول الشبكة المحلية للشركة.

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**.



إعدادات 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.

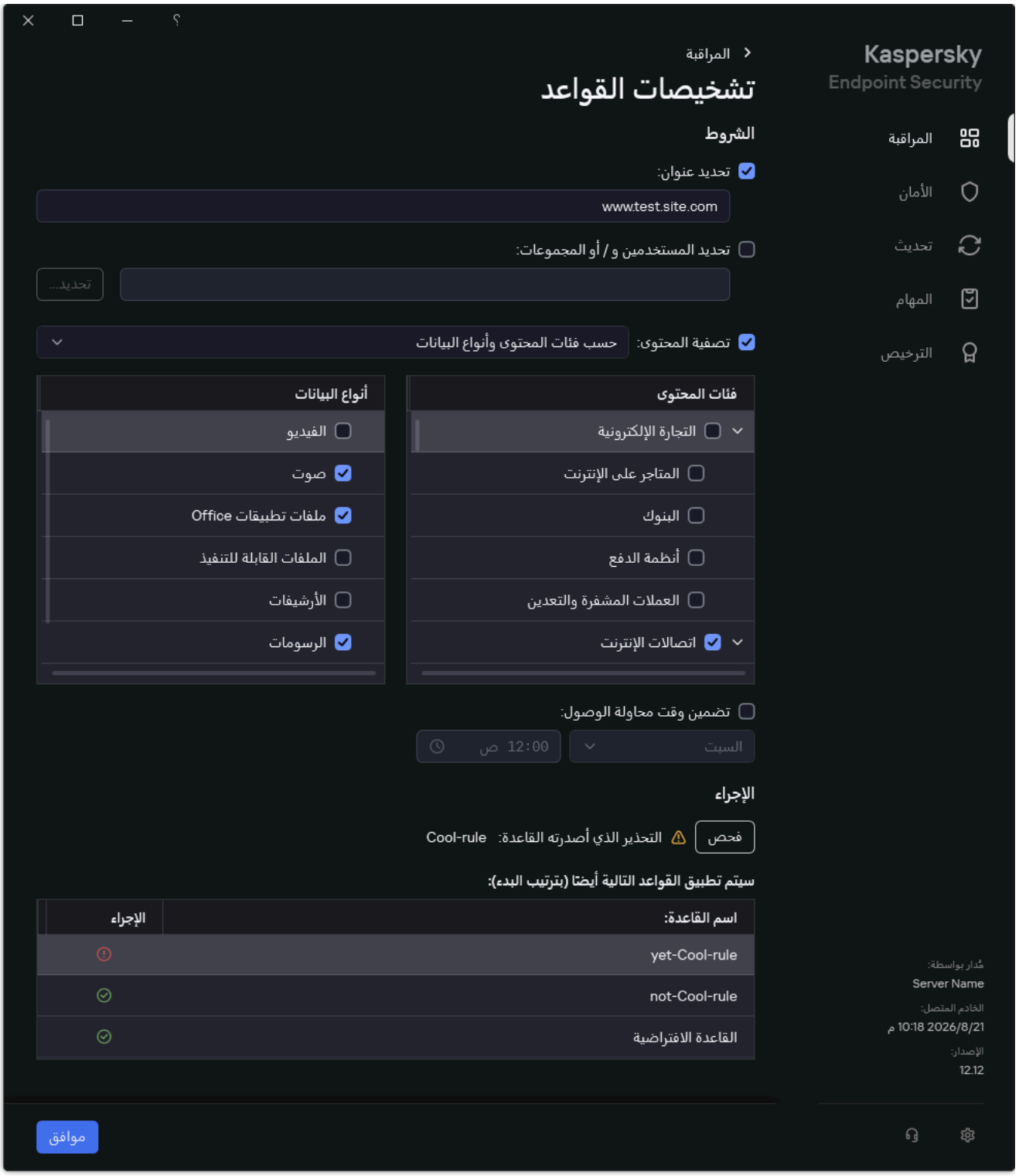
5. إذا كنت تريد اختبار القواعد التي يستخدمها Kaspersky Endpoint Security للتحكم في الوصول إلى موارد الويب بالنسبة إلى مستخدمين معيّنين و / أو مجموعات معيّنة من المستخدمين، فحدد قائمة بهؤلاء المستخدمين و / أو مجموعات المستخدمين.

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.



نتيجة اختبار الوصول إلى موارد الويب

تصدير واستيراد قواعد التحكم في الويب

يمكنك تصدير قائمة قواعد التحكم في الويب إلى ملف XML أو JSON. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الويب**.

4. 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.

5. 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.

6. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد التحكم في الويب في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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 **Rules list**:

a. حدد القواعد التي تريد تصديرها.

b. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف JSON في مجلد التنزيلات الافتراضي.

6. لاستيراد قائمة القواعد، في القسم **Rules list**:

a. انقر على الزر ← **Import**.

في النافذة التي تفتح، حدد ملف JSON 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 JSON.

7. احفظ تغييراتك.

تصدير واستيراد عناوين موارد الويب لقاعدة التحكم في الويب

إذا أنشأت قائمة بعناوين مورد ويب في قاعدة الوصول إلى موارد الويب، فيمكنك تصديرها إلى ملف:

- بتنسيق TXT في وحدة تحكم الإدارة (MMC)
- بتنسيق JSON في Web Console
- بتنسيق CSV في واجهة التطبيق

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.

يمكنك أيضًا تصدير/استيراد كل قواعد التحكم في الويب وليس فقط عناوين موارد الويب الخاصة بقاعدة فردية.

كيفية تصدير/استيراد عناوين موارد الويب لقاعدة التحكم في الويب في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الويب**.
5. في القسم **إعدادات التحكم في الويب**، حدد القاعدة التي تريد تصدير أو استيراد قائمة عناوين موارد الويب الخاصة بها.
   يتم عرض خصائص قاعدة التحكم في الويب.
6. لتصدير قائمة موارد الويب، نفذ ما يلي في قائمة العناوين:
   a. حدد العناوين التي تريد تصديرها.
      إذا لم تحدد أي عنوان، فسيقوم Kaspersky Endpoint Security بتصدير كل العناوين.
   b. انقر فوق الزر .
   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.
7. لاستيراد قائمة موارد الويب، نفذ ما يلي في قائمة العناوين:
   a. انقر فوق الزر .
      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.
8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تصدير/استيراد عناوين موارد الويب لقاعدة التحكم في الويب في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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. في القسم **Rules list**، حدد القاعدة التي تريد تصدير أو استيراد قائمة عناوين موارد الويب الخاصة بها.
يتم عرض خصائص قاعدة التحكم في الويب.

6. في القسم **Individual websites** ← **Scope**، انقر على الزر **Edit**.

7. لتصدير قائمة موارد الويب، نفذ ما يلي في قائمة العناوين:

a. حدد العناوين التي تريد تصديرها.

b. انقر على الزر ← **Export**.
يقوم Kaspersky Endpoint Security بتصدير قائمة العناوين مورد الويب إلى ملف JSON في مجلد التنزيلات الافتراضي.

8. لاستيراد قائمة موارد الويب، نفذ ما يلي في قائمة العناوين:

a. انقر على الزر ← **Import**.
في النافذة التي تفتح، حدد ملف JSON الذي تريد استيراد قائمة عناوين مورد الويب منه.

b. افتح الملف.

إذا كان جهاز الكمبيوتر يتضمن قائمة أجهزة موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف JSON.

يمكنك تصدير واستيراد مجموعات مواقع الويب بالطريقة ذاتها.

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تصدير/استيراد عناوين موارد الويب لقاعدة التحكم في الويب في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.



إعدادات 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 CSV 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 CSV.

6. لاستيراد قائمة موارد الويب، نفذ ما يلي في القسم **العناوين**:

   a. انقر على **استيراد**.

   في النافذة التي تفتح، حدد ملف CSV الذي تريد استيراد قائمة موارد الويب منه.

b. افتح الملف.

إذا كان جهاز الكمبيوتر يتضمن قائمة أجهزة موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف CSV.

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 (الحالة Critical).
- زيارة لموقع غير مرغوبة (الحالة Warning).
- زيارة موقع ويب مسموح به (الحالة Info).

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.

حقن برنامج نصي للتفاعل مع صفحة الويب

كيفية إدخال برنامج نصي لتفاعل صفحة الويب في حركة مرور الويب في وحدة تحكم الإدارة (MMC)

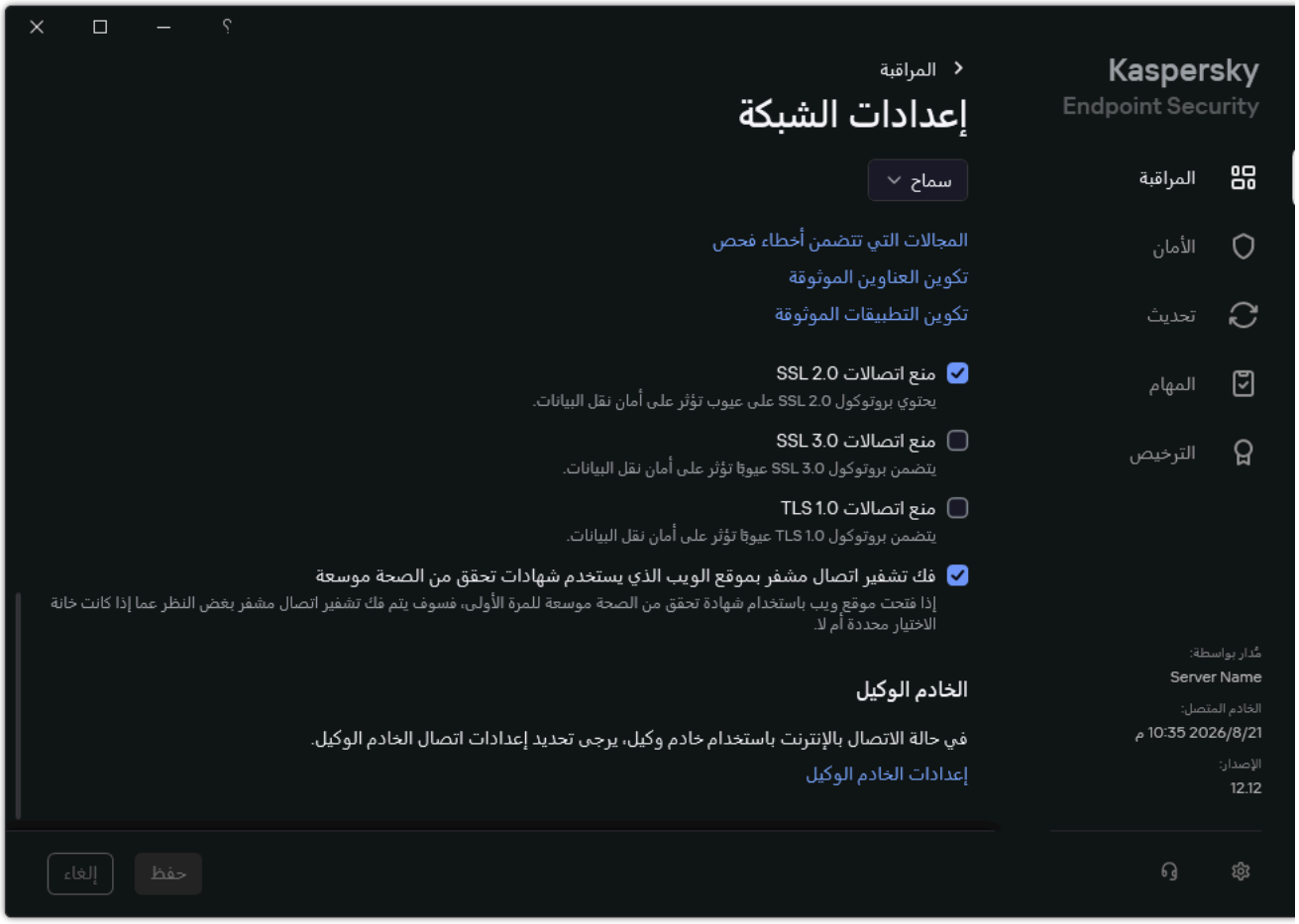
1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.
4. في القسم **فحص الاتصالات المشفرة**، حدد خانة الاختيار **إدخال البرنامج النصي في حركة مرور الويب للتفاعل مع صفحات الويب**.
5. احفظ تغييراتك.

كيفية إدخال برنامج نصي لتفاعل صفحة الويب في حركة مرور الويب في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. في نافذة السياسة، حدد **General Settings** ← **Network Settings**.
5. تحت **Monitoring of internet connections**، قم بتشغيل مفتاح **Monitoring of internet connections ENABLED**.
6. احفظ تغييراتك.

كيفية إدخال برنامج نصي لتفاعل صفحة الويب في حركة مرور الويب 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 **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](#).

تكوين تسجيل أحداث التحكم في الويب

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 **تكوين الإخطارات**.

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 وhttp://www.example.com/icon.ico وhttp://www.example.com/file.js، وما إلى ذلك.

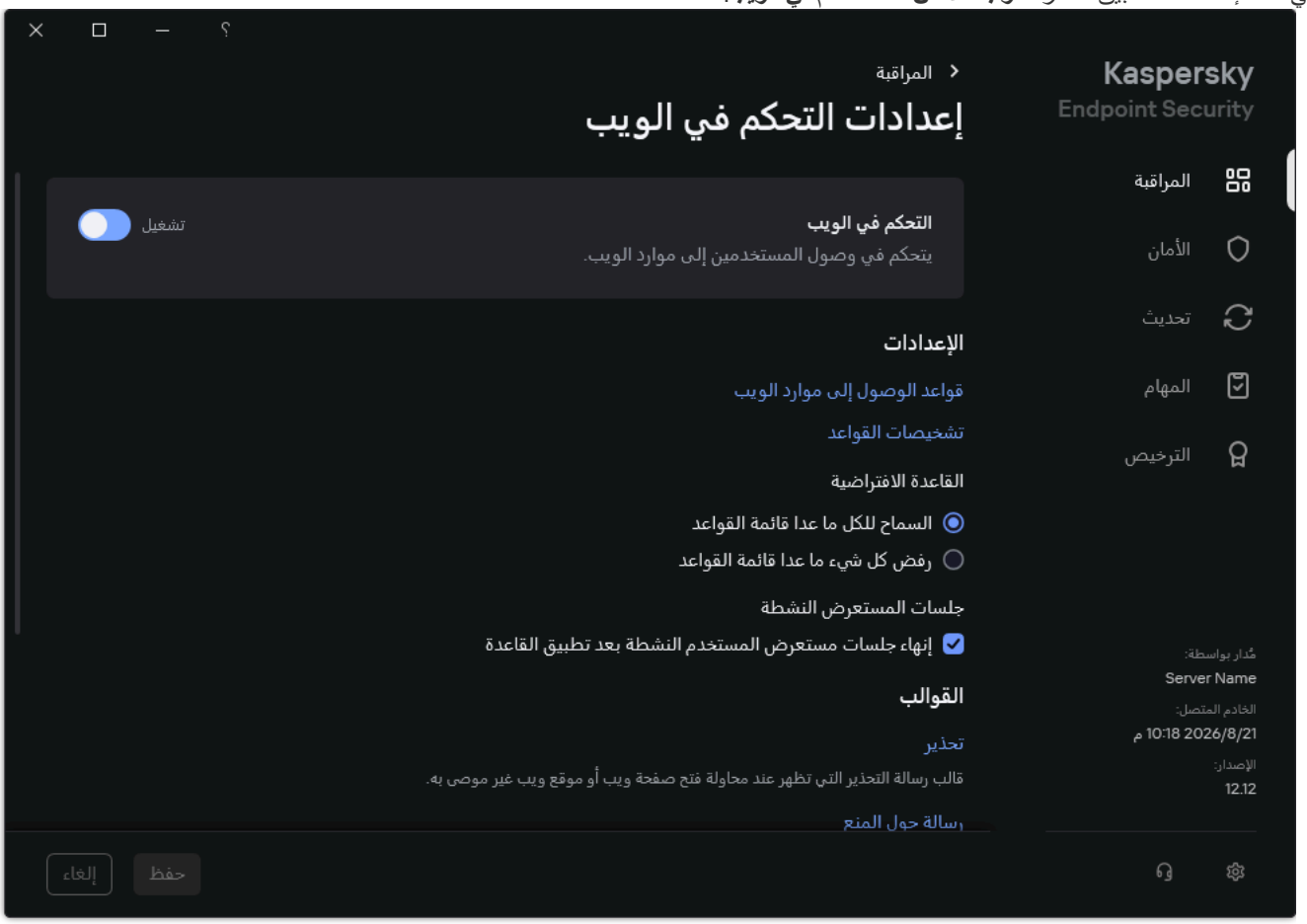
- إذا كنت تستخدم Kaspersky Security Center Cloud Console، فإن التحكم في الويب تقوم بتجميع الأحداث وترسل فقط البروتوكول والنطاق للموقع الإلكتروني. على سبيل المثال: إذا كان المستخدم يزور صفحات الويب غير المرغوبة http://www.example.com/main وhttp://www.example.com/contact وhttp://www.example.com/gallery، سوف يرسل Kaspersky Endpoint Security حدثًا واحدًا فقط بالكائن http://www.example.com.

تسجيل الأحداث عند زيارة المواقع المسموح بها

لتمكين تسجيل الأحداث عند زيارة مواقع الويب المسموح بها:

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

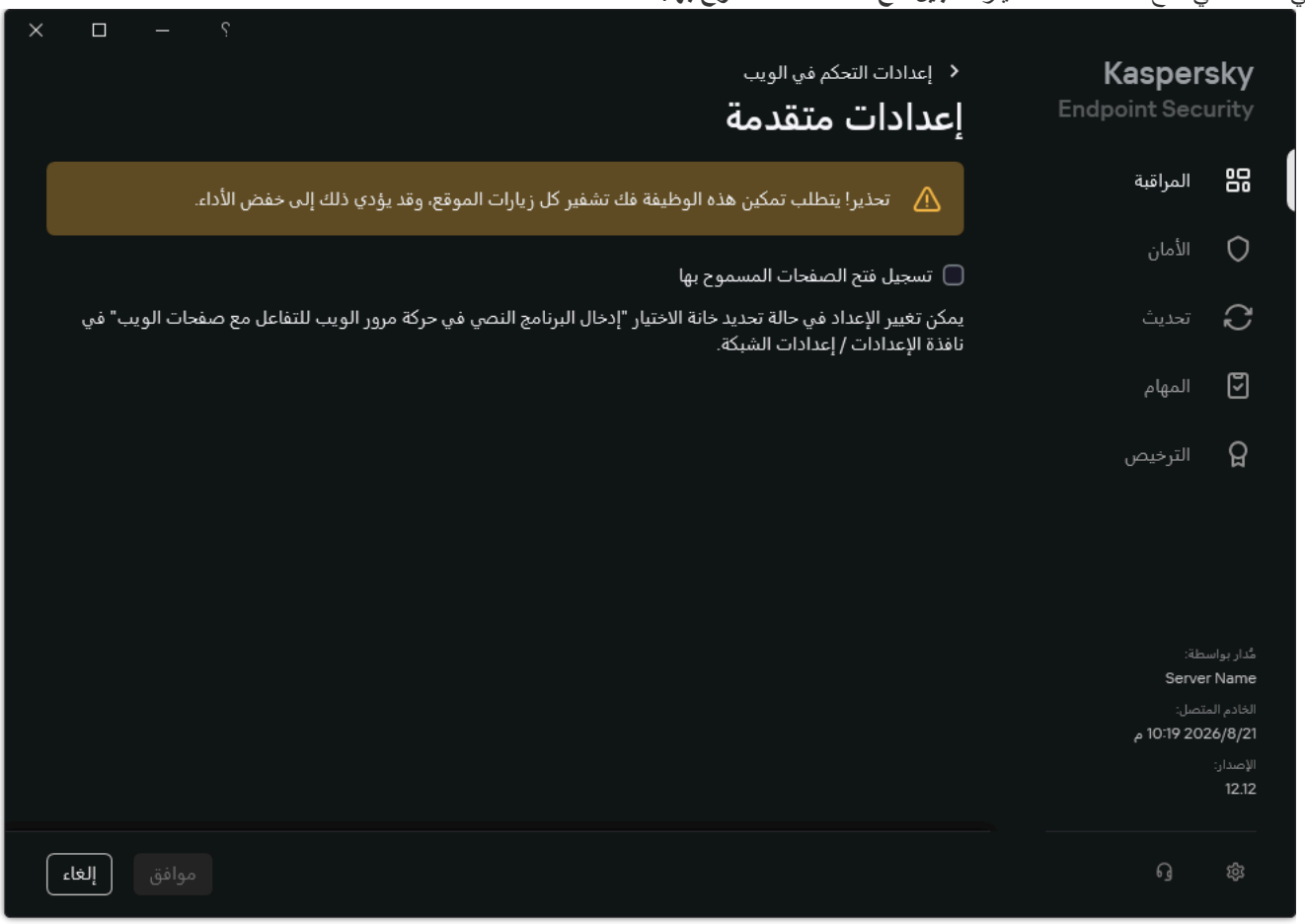
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.



إعدادات 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**.



الإعدادات المتقدمة لمكون التحكم في الويب

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 (انظر الشكل أدناه) 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.



رسالة حول منع موارد الويب

تتوفر قوالب خاصة لرسائل التحذير، والرسائل التي تبلّغ بأن مورد الويب ممنوع، ورسالة يتم إرسالها إلى مسؤول الشبكة المحلية. يتم توفير متغيرات خاصة لإدارة قوالب الرسائل (على سبيل المثال، %USER_NAME%). وتسمح المتغيرات باستخدام قالب رسالة واحدة لأجهزة الكمبيوتر المختلفة. وعند إنشاء رسالة، يسترجع Kaspersky Endpoint Security قيمة المتغير من إعدادات نظام التشغيل ويدرجها في الرسالة التي تتطابق مع الكمبيوتر والمستخدم والحدث المحدد.

كيفية تغيير قالب رسالة التحكم في الويب في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الويب**.
4. في القسم **إعدادات قوالب الرسائل**، انقر على الزر **القوالب**.
5. تكوين قوالب رسائل 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 **User requests**. 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.

   لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **المتغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.

   يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **افتراضيًا**.
6. احفظ تغييراتك.

كيفية تغيير قالب رسالة التحكم في الويب في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Web Control** ← **Security Controls**.

5. في القسم **Message templates**، انقر فوق الرابط **Message about website blocking** وكوّن القوالب لرسائل Web Control:

- **Warning**. يتكون حقل الإدخال من قالب للرسالة التي يتم عرضها إذا تم تشغيل قاعدة للتحذير بشأن محاولات وصول إلى مورد ويب غير مرغوب فيه.
- **Message about blocking**. يحتوي حقل الإدخال على قالب الرسالة التي تظهر في حالة تشغيل قاعدة تمنع الوصول إلى أحد موارد الويب.
- **Message to administrator**. 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 **User requests**. 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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **Add variable** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.
يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **Reset to default**.

6. احفظ تغييراتك.

كيفية تغيير قالب رسالة التحكم في الويب في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في الويب**.



إعدادات 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 **User requests**. 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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **إضافة متغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.

يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **إعادة تعيين**.

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 المجال `pictures.*.`.
   - `http://user.pictures.example.com`. يمثل قناع المجال `user.*.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: قناع العنوان `example.com` يغطي عنواني `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.

الرقم.	قناع العنوان	عنوان مورد الويب للتحقق	هل يغطي قناع العنوان	التعليق
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 الويب للأجهزة الافتراضية

يتحكم التحكم في الويب في حركة البيانات على الكمبيوتر وكذلك على جهاز افتراضي يتم نشره محليًا على الكمبيوتر. ويعمل هذا دون الحاجة إلى تثبيت تطبيق Kaspersky Endpoint Security على الجهاز الافتراضي المحلي. ويعني هذا أنه إذا حاول المستخدم فتح موقع ويب تم حظره بواسطة قاعدة التحكم في الويب في مستعرض على الجهاز الافتراضي، يمنع التطبيق المثبت على نظام التشغيل المضيف للكمبيوتر الوصول إلى موقع الويب هذا.

يعمل التحكم في الويب بشكل مختلف على الأجهزة الافتراضية المختلفة.

Oracle VM VirtualBox

يدعم Kaspersky Endpoint Security قواعد التحكم في الويب على أجهزة Oracle VM VirtualBox الافتراضية دون قيود. ويستطيع التطبيق التحكم في كل حركة مرور الجهاز الافتراضي. وإذا تم تكوين عامل تصفية حسب المستخدم في قواعد التحكم في الويب، يعمل التطبيق بشكل صحيح لأن كل عمليات الأجهزة الافتراضية يتم تشغيلها بواسطة المستخدم المحلي.

VMware Workstation

يدعم Kaspersky Endpoint Security قواعد التحكم في الويب على أجهزة VMware Workstation الافتراضية بقيود. ولا يدعم التطبيق القواعد مع تكوين عامل تصفية حسب المستخدم. ويتم تشغيل عمليات الجهاز الافتراضي تحت مستخدم النظام (SYSTEM). ويجعل هذا من المستحيل تحديد المستخدم الذي يحاول فتح موقع الويب على الجهاز الافتراضي.

Microsoft Hyper-V

لا يدعم Kaspersky Endpoint Security قواعد التحكم في الويب على أجهزة Microsoft Hyper-V الافتراضية.

المتغيرات في قوالب رسالة Web Control

يمكنك استخدام المتغيرات التالية في قوالب رسائل المستخدم أو قوالب رسائل المسؤول:

- **اسم المستخدم** – %USER_NAME%.

  اسم حساب المستخدم الحالي على الكمبيوتر الذي تم إنشاء الرسالة عليه، بتنسيق <device name>\<user alias> (على سبيل المثال، DESKTOP-123\John.Smith).

- **عنوان مورد الويب** – %CANONIC_REQUEST_URL%.

  عنوان مورد الويب الممنوع.

- **اسم القاعدة** – %RULE%.

  اسم القاعدة التي منعت مورد الويب.

- **البريد الإلكتروني لإرسال رسالة** – %COMPLAIN_EMAIL%.

  عنوان البريد الإلكتروني للملاحظات عن منع موارد الويب. ويؤدي النقر فوق عنوان البريد الإلكتروني إلى فتح نافذة يمكن للمستخدم من خلالها كتابة رسالة إلى المسؤول.

- **اسم فئة المحتوى** – %CONTENT_CATEGORY_LIST%.

  فئة موقع الويب التي ينتمي إليها المورد الممنوع (على سبيل المثال، أنظمة الدفع).

- **اسم فئة نوع البيانات** – %TYPE_CATEGORY_LIST%.

  فئة نوع البيانات على مورد الويب الممنوع (على سبيل المثال، الرسومات).

- **ارتباط إلى مورد الويب المطلوب** – %CONTINUE_PAGE%.

  رابط إلى صفحة الويب المطلوبة (على سبيل المثال، http://www.example.com/pagename.html).

- **الارتباط إلى موقع الويب** – %CONTINUE_SITE%.

  رابط إلى موقع الويب الذي يحتوي على صفحة الويب المطلوبة (على سبيل المثال، http://www.example.com/).

- **ارتباط للوصول إلى المجالات** – %CONTINUE_DOMAIN%.

  الرابط الذي يمكن النقر فوقه للوصول إلى جميع صفحات الويب الموجودة لاسم المجال. على سبيل المثال، إذا كان عنوان صفحة الويب الممنوعة هو http://www.example.com يحل المتغير %CONTINUE_DOMAIN% محل الرابط http://*.example.com. ويتيح النقر فوق هذا الرابط الوصول إلى جميع عناوين الويب الخاصة باسم المجال الأساسي http://www.example.com/ بما في ذلك المجالات الفرعية، على سبيل المثال، */http://start.example.com أو */http://domain.domain.example.com، حيث يرمز الحرف * إلى أي سلسلة أحرف (بما في ذلك سلسلة فارغة).

التحكم في الجهاز

يعمل التحكم في الجهاز على إدارة إمكانية وصول المستخدم إلى الأجهزة المثبت عليها أو المتصلة بجهاز كمبيوتر (على سبيل المثال، الأقراص الصلبة أو الكاميرات أو وحدات شبكة Wi-Fi). ويتيح لك هذا حماية جهاز الكمبيوتر من الإصابة بالفيروسات عند اتصال مثل هذه الأجهزة به، ومنع فقدان البيانات أو تسريباتها.

في حالة تمكين التحكم في الأجهزة، ينقل التطبيق معلومات عن الأجهزة المتصلة إلى Kaspersky Security Center. يمكنك عرض قائمة الأجهزة المتصلة في Kaspersky Security Center في المجلد **Hardware** ← **Repositories** ← **Advanced**.

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). إذا تم تحديد وضع **يعتمد على ناقل الاتصال** لنوع الجهاز، يسمح التطبيق أو يرفض الوصول إلى الجهاز وفقًا لواجهة الاتصال (مثل 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 (Hardware ID 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**. لكل جهاز Vendor ID (VID) وProduct ID (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.

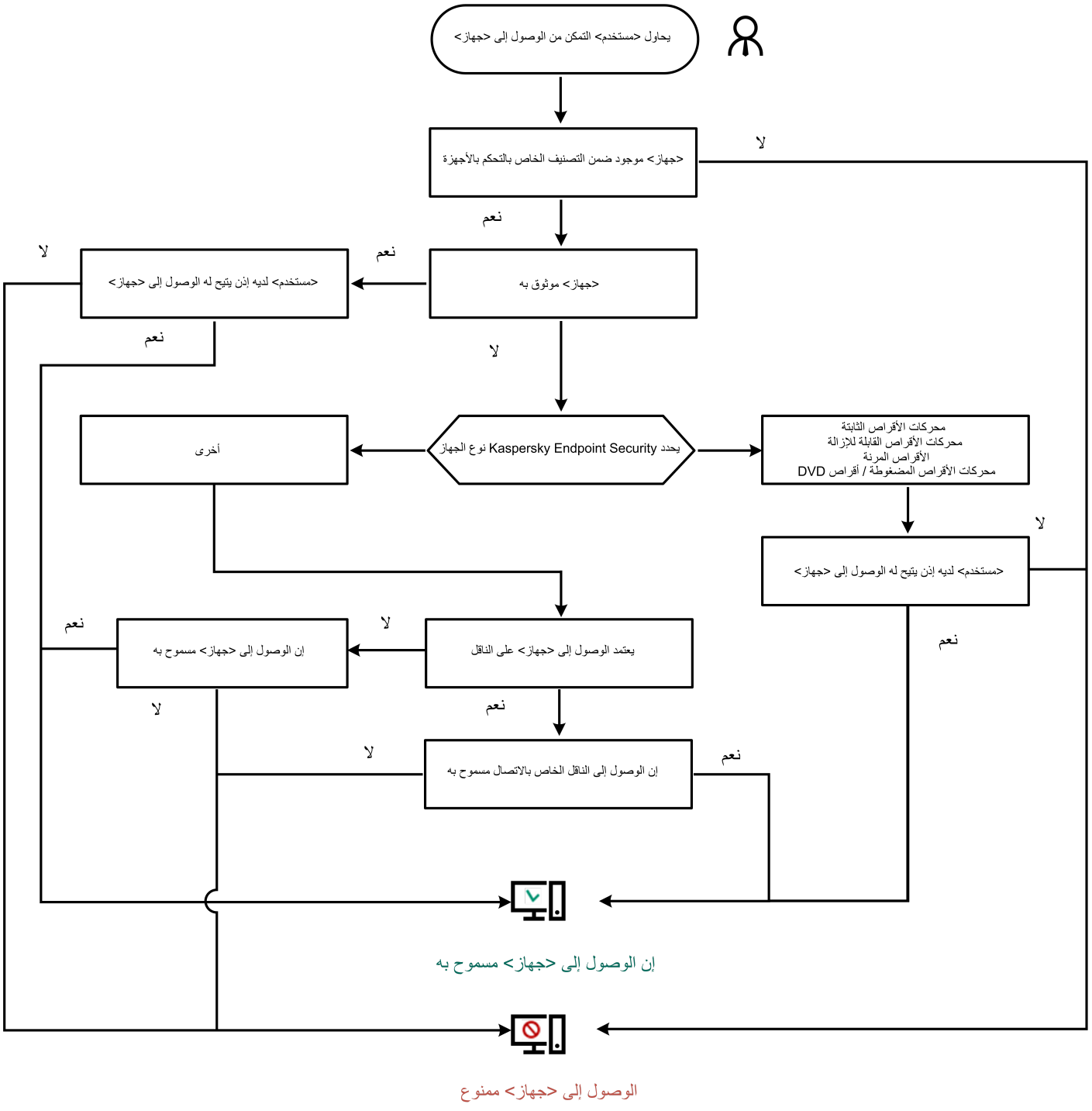
عند حظر جهاز متصل بجهاز كومبيوتر بواسطة التحكم في الجهاز، فإن برنامج Kaspersky Endpoint Security سيقوم بحظر الوصول وإظهار إخطار (انظر الشكل أدناه).



إخطار التحكم في الجهاز

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.

حول قواعد الوصول

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. 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

إذا تم تحديد القيمة **يعتمد على ناقل الاتصال** لقاعدة الوصول حسب نوع الجهاز، ويسمح التطبيق أو يرفض الوصول إلى الجهاز وفقًا لواجهة الاتصال. القواعد التي تسمح للنواقل التي تم إنشاؤها بشكل افتراضي لجميع نواقل الاتصال الموجودة في تصنيف مكون التحكم في الجهاز.

تحدد قواعد وصول ناقل الاتصال ما إذا كان يسمح الاتصال بالجهاز مسموح (الحالة ✓) أم محظور (الحالة ⊘). وتكون أولوية قواعد الوصول إلى نوع الجهاز أعلى من أولوية قواعد الوصول إلى ناقل الاتصال.

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.

الحصول على معلومات عن الأجهزة المثبتة

يتلقى Kaspersky Security Center معلومات عن الأجهزة المثبتة من المزودين التاليين: عميل الشبكة و Kaspersky Endpoint Security. وتوجد حاجة إلى معلومات عن الأجهزة المثبتة لإدارة الوصول وإنشاء قائمة بالأجهزة الموثوقة.

معلومات عن أجهزة الكمبيوتر

في حالة تثبيت عميل الشبكة على جهاز يعمل بنظام التشغيل Windows، فإنه يرسل المعلومات التالية عن مكونات الجهاز إلى خادم الإدارة:

- ذاكرة الوصول العشوائي (RAM)
- أجهزة التخزين (بما في ذلك محركات الأقراص الثابتة)
- اللوحة الأم
- وحدة المعالجة المركزية
- محول الشبكة
- الشاشات
- وحدة معالجة الرسومات
- بطاقة الصوت

يقدم عميل الشبكة المعلومات عند كل مزامنة مع Kaspersky Security Center. ويمكنك عرض أجهزة الكمبيوتر في خصائص الكمبيوتر (**سجل الأجهزة**).

معلومات الأجهزة

يوفر Kaspersky Endpoint Security معلومات عن الأجهزة المثبتة: الطابعات ومحركات الأقراص القابلة للإزالة والأجهزة المحمولة (MTP) وما إلى ذلك. ولتلقي معلومات الأجهزة، تحتاج إلى تطبيق سياسة نشطة تتيح إرسال معلومات الأجهزة المثبتة (يتم تمكين هذا الإرسال بشكل افتراضي).

كيفية تمكين إرسال البيانات عن الأجهزة المثبتة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
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. حدد خانة الاختيار **الأجهزة المثبتة**.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين نقل البيانات عن الأجهزة المثبتة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **General Settings** ← **KSC Integration**.

5. في القسم **Data transfer to Administration Server**، انقر على الزر **Advanced settings**.

6. حدد خانة الاختيار **About installed devices**.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

نتيجة لذلك، يمكنك عرض قائمة الأجهزة المثبتة في وحدة تحكم Kaspersky Security Center (**Repositories** ← **Hardware**).

إدارة الوصول إلى الأجهزة حسب النوع

يسمح التحكم في الأجهزة بإدارة الوصول إلى الأجهزة حسب النوع. ويتم تحديد نوع الجهاز بواسطة نظام التشغيل عند توصيل الجهاز. ويمكنك البحث عن نوع الجهاز باستخدام أداة إدارة الأجهزة المضمنة في نظام التشغيل. ولإدارة الوصول إلى الأجهزة، يجب عليك تكوين القواعد. 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. لا يمكنك إضافة جهاز يوجد خارج تصنيف التحكم في الجهاز. يتم السماح بالوصول إلى كل الأجهزة لجميع المستخدمين.

بشكل افتراضي، يسمح التحكم في الأجهزة بالوصول إلى جميع الأجهزة لجميع المستخدمين.

يمكنك تكوين الوصول إلى الأجهزة على النحو التالي:

- **سماح**.
يمنح Kaspersky Endpoint Security جميع المستخدمين وصولاً كاملاً إلى الأجهزة.
- **منع**.
يحظر Kaspersky Endpoint Security اتصالات الأجهزة. يسمح التطبيق للأجهزة الموثوقة فقط بالاتصال.
- **يعتمد على ناقل الاتصال**.
يحدد Kaspersky Endpoint Security واجهة اتصال الأجهزة ويقيد الوصول إلى الأجهزة وفقًا لحالة اتصال الناقل الخاصة بها. ويسمح التطبيق أيضا بتوصيل الأجهزة الموثوقة.

- **حسب القواعد**.

بالنسبة لبعض أنواع الأجهزة، يمكنك تعيين مستخدمين فرديين أو مجموعة من المستخدمين المسموح لهم باستخدام الأجهزة، وإعداد جدول زمني للوصول إلى الأجهزة، وتكوين أذونات القراءة والكتابة. ويسمح التطبيق أيضا بتوصيل الأجهزة الموثوقة.

كن حذرًا عند تكوين الوصول إلى أجهزة من نوع **محركات الأقراص الثابتة**. وإذا حظرت الوصول إلى قرص النظام، فقد يتسبب التطبيق في حدوث عطل (BSOD) عند تشغيل نظام التشغيل.

إذا لم يكن الجهاز مناسبًا لنظام تصنيف التحكم في الأجهزة، فلا يمكن تقييد الوصول إلى هذا الجهاز.

كيفية إدارة الوصول إلى الأجهزة حسب النوع في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
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**.
   تعرض علامة التبويب **أنواع الأجهزة** قواعد الوصول لجميع الأجهزة المدرجة في تصنيف التحكم في الأجهزة.
6. تكوين قواعد الوصول للأجهزة:
   a. حدد وضع الوصول: **سماحو منع** أو **يعتمد على ناقل الاتصال** أو **حسب القواعد**.
      لتحديد وضع الوصول **حسب القواعد**، يجب أن تنقر نقرًا مزدوجًا لفتح خصائص قاعدة الوصول.
   b. إذا حددت **يعتمد على ناقل الاتصال** في وضع الوصول، يجب عليك تكوين قواعد الوصول لواجهات الاتصال في علامة التبويب **ناقلات الاتصال**.
   c. في حالة أجهزة التخزين (على سبيل المثال، الوسائط القابلة للإزالة)، يمكنك تكوين أذونات الوصول للمستخدمين الفرديين. ويمكنك أيضًا إعداد جدول للوصول إلى الأجهزة وتكوين أذونات القراءة والكتابة.
      يمكنك إضافة الأجهزة إلى القائمة الموثوقة. الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.
   d. إذا لزم الأمر، كوّن قواعد الطباعة.
   e. إذا لزم الأمر، كوّن قواعد الوصول إلى جهاز Bluetooth.
   f. إذا لزم الأمر، كوّن قواعد اتصال Wi-Fi الخاصة بالكمبيوتر.
7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إدارة الوصول إلى الأجهزة حسب النوع في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
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. تحت **Device access rules**، حدد علامة التبويب **Devices and Wi-Fi networks**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. تكوين قواعد الوصول للأجهزة:

a. حدد وضع الوصول: **Allow** و**Block** أو **Depends on bus** أو **Custom**.

إذا كان وضع الوصول مفقودًا من القائمة المنسدلة فافتح خصائص قاعدة الوصول عن طريق النقر نقرًا مزدوجًا فوق نوع الجهاز.

b. إذا حددت **Depends on bus** في وضع الوصول، يجب عليك تكوين قواعد الوصول لواجهات الاتصال في علامة التبويب **Connection buses**.

c. في حالة أجهزة التخزين (على سبيل المثال، الوسائط القابلة للإزالة)، يمكنك تكوين أذونات الوصول للمستخدمين الفرديين. ويمكنك أيضًا إعداد جدول للوصول إلى الأجهزة وتكوين أذونات القراءة والكتابة.

يمكنك إضافة الأجهزة إلى القائمة الموثوقة. الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

d. إذا لزم الأمر، كوّن قواعد الطباعة.

e. إذا لزم الأمر، كوّن قواعد الوصول إلى جهاز Bluetooth.

f. إذا لزم الأمر، كوّن قواعد اتصال Wi-Fi الخاصة بالكمبيوتر.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إدارة الوصول إلى الأجهزة 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 الرابط **الأجهزة وشبكات Wi-Fi**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

4. تكوين قواعد الوصول للأجهزة:

a. حدد وضع الوصول: **سماحو منع** أو **يعتمد على ناقل الاتصال** أو **حسب القواعد**.

إذا كان وضع الوصول مفقودًا من القائمة المنسدلة فافتح خصائص قاعدة الوصول عن طريق النقر نقرًا مزدوجًا فوق نوع الجهاز.

b. إذا حددت **يعتمد على ناقل الاتصال** في وضع الوصول، يجب عليك تكوين قواعد الوصول لواجهات الاتصال في علامة التبويب **ناقلات الاتصال**.

c. في حالة أجهزة التخزين (على سبيل المثال، الوسائط القابلة للإزالة)، يمكنك تكوين أذونات الوصول للمستخدمين الفرديين. ويمكنك أيضًا إعداد جدول للوصول إلى الأجهزة وتكوين أذونات القراءة والكتابة.

يمكنك إضافة الأجهزة إلى القائمة الموثوقة. الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

d. إذا لزم الأمر، كوّن قواعد الطباعة.

e. إذا لزم الأمر، كوّن قواعد الوصول إلى جهاز Bluetooth.

f. إذا لزم الأمر، كوّن قواعد اتصال Wi-Fi الخاصة بالكمبيوتر.

5. احفظ تغييراتك.

نتيجة لذلك، عندما يحاول مستخدم الوصول إلى جهاز، يمنع التطبيق الوصول وفقًا للقواعد. ويسجل Kaspersky Endpoint Security أيضًا حدثًا مطابقًا.
وإذا كنت ترغب في منح حق الوصول إلى الأجهزة الفردية، فيمكنك إضافة هذه الأجهزة إلى قائمة الأجهزة الموثوقة.

إدارة الوصول إلى الأجهزة عن طريق 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.

تمييز حقوق وصول المستخدمين إلى الأجهزة

يمكنك تكوين حقوق وصول المستخدمين حسب نوع الجهاز أو الأجهزة الموثوقة.

تمييز حقوق وصول المستخدمين حسب نوع الجهاز

يسمح التحكم في الأجهزة بتكوين حقوق وصول المستخدمين إلى البيانات على أجهزة التخزين. وبالنسبة لهذه الأجهزة، يمكنك تكوين أذونات الكتابة والقراءة. ويدعم التحكم في الأجهزة الأنواع التالية من أجهزة التخزين:

- محركات الأقراص الثابتة
- محركات الأقراص القابلة للإزالة (بما في ذلك محركات أقراص USB المحمولة)
- الأقراص المرنة
- محركات أقراص CD/DVD
- أجهزة محمولة (MTP) تتضمن الأجهزة المحمولة (MTP)، على سبيل المثال، الأجهزة المحمولة وكاميرات الصور ومشغلات الوسائط، وما إلى ذلك.

بهذه الطريقة يمكنك، على سبيل المثال، السماح باستخدام الوسائط القابلة للإزالة فقط لمجموعة المسؤولين. وبالنسبة لأنواع الأجهزة الأخرى، يمكنك رفض الوصول أو السماح لجميع المستخدمين بالوصول. ويمكنك أيضا تكوين حقوق وصول المستخدم لاستخدام الطابعات.

كيفية تكوين حقوق وصول المستخدم إلى البيانات الموجودة على أجهزة التخزين في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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**.
تعرض علامة التبويب **أنواع الأجهزة** قواعد الوصول لجميع الأجهزة المدرجة في تصنيف التحكم في الأجهزة.

6. لتكوين قواعد الوصول إلى جهاز التخزين، انقر نقرًا مزدوجًا لفتح قائمة القواعد.

7. تكوين قاعدة الوصول إلى جهاز التخزين:

a. في القسم **قواعد الوصول**، انقر على الزر **إضافة**.
يفتح هذا نافذة لإضافة قاعدة وصول جديدة لجهاز التخزين.

b. في الحقل **أولوية القاعدة**، قم بتعيين أولوية كتابة القاعدة. 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 لك 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. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

d. انقر على **موافق**.

8. تحت **جداول قاعدة الوصول المحددة**، كوّن جدولاً للوصول إلى جهاز التخزين للمستخدمين.
على سبيل المثال، يمكنك السماح للمستخدمين باستخدام أجهزة التخزين أثناء ساعات العمل فقط.

9. كوّن أذونات وصول المستخدمين إلى أجهزة التخزين في برنامج إدارة الملفات (**قراءة / كتابة**).

10. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين حقوق وصول المستخدم إلى البيانات على أجهزة التخزين في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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 access rules**، في جدول قواعد الوصول، افتح خصائص قواعد الوصول لأجهزة التخزين.

6. في القسم **Device access rules**، حدد **Custom**.

7. تكوين قاعدة الوصول إلى جهاز التخزين:

a. في القسم **Users and their rights**، انقر على الزر **Add**.

يفتح هذا نافذة لإضافة قاعدة وصول جديدة لجهاز التخزين.

b. في الحقل **Priority**، قم بتعيين أولوية كتابة القاعدة. 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 لك 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 **User or group**، حدد المستخدمين أو مجموعات المستخدمين. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

d. تحت **Access schedule**، كوّن جدولاً للوصول إلى جهاز التخزين للمستخدمين.

على سبيل المثال، يمكنك السماح للمستخدمين باستخدام أجهزة التخزين أثناء ساعات العمل فقط.

e. كوّن أذونات وصول المستخدمين إلى أجهزة التخزين في برنامج إدارة الملفات (**Read / Write**).

f. انقر على **Save**.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين حقوق وصول المستخدم إلى البيانات الموجودة على أجهزة التخزين 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 الرابط **الأجهزة وشبكات Wi-Fi**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

4. لتكوين قواعد الوصول إلى الأجهزة المحمولة، انقر بزر الماس الأيمن لفتح قائمة القواعد.

5. تكوين قاعدة الوصول إلى جهاز التخزين:

a. في القسم **حقوق المستخدمين**، انقر على الزر **إضافة**.

يفتح هذا نافذة لإضافة قاعدة وصول جديدة لجهاز التخزين.

b. في الحقل **الأولوية**، قم بتعيين أولوية كتابة القاعدة. 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 لك 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 **المستخدمون**، حدد المستخدمين أو مجموعات المستخدمين. ويمكنك تحديد المستخدمين في Active Directory أو إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

d. انقر على **موافق**.

6. تحت **جدول الوصول إلى الأجهزة**، كوّن جدولاً للوصول إلى جهاز التخزين للمستخدمين.

على سبيل المثال، يمكنك السماح للمستخدمين باستخدام أجهزة التخزين أثناء ساعات العمل فقط.

7. كوّن أذونات وصول المستخدمين إلى أجهزة التخزين في برنامج إدارة الملفات (**قراءة / كتابة**).

8. احفظ تغييراتك.

تمييز حقوق وصول المستخدم إلى الأجهزة 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. يمكنك تكوين حقوق وصول المستخدم في خصائص الجهاز الموثوق.

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 Android Debug Bridge (ADB) أو iTunes أو ما يعادلهما من تطبيقات على الكمبيوتر، يحدد نظام التشغيل 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 حالة 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.
4. تحت **إعدادات التحكم في الجهاز**، حدد علامة التبويب **أنواع الأجهزة**.

   يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.
5. في قائمة السياق لنوع الجهاز **أجهزة محمولة (MTP)**، قم بتكوين وضع الوصول إلى الجهاز المحمول: **سماح** أو **منع** أو **يعتمد على ناقل الاتصال**.
6. لتكوين قواعد الوصول إلى الأجهزة المحمولة، انقر نقرًا مزدوجًا لفتح قائمة القواعد.
7. 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 لك 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. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

   d. انقر على **موافق**.

8. 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).

9. كوّن أذونات وصول المستخدمين إلى الأجهزة المحمولة في برنامج إدارة الملفات (**قراءة / كتابة**).

10. 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.

11. 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.

12. احفظ تغييراتك.

كيفية تكوين قواعد الوصول إلى الجهاز المحمول في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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 access rules**، انقر على الرابط **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. قم بتكوين وضع الوصول إلى الأجهزة المحمولة: **Allow** أو **Block** أو **Depends on bus** أو **Custom**.

8. باستخدم مفتاح التبديل **Access via iTunes for all users ENABLED**، 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. إذا حددت الوضع **Custom**، يجب عليك إضافة قواعد الوصول للأجهزة. ولفعل ذلك، تحت **Users and their rights**، انقر على الزر **Add** وكوّن قاعدة الوصول إلى الجهاز المحمول:

a. في الحقل **Priority**، 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 لك 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 **User or group**، حدد المستخدمين أو مجموعات المستخدمين للوصول إلى الأجهزة المحمولة. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

c. تحت **Access schedule**، 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**.

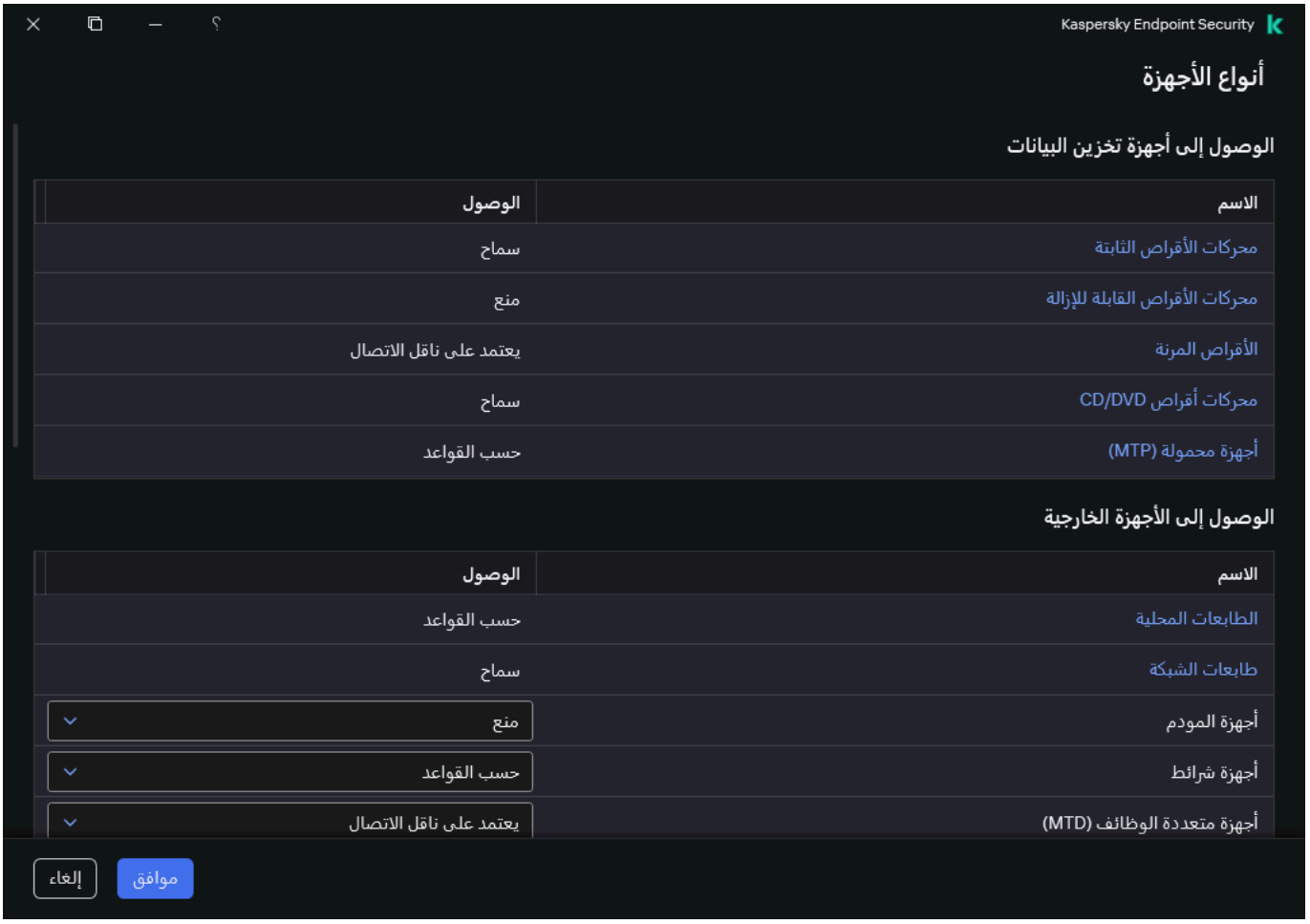
في حالة إلغاء تحديد خانة الاختيار، عند توصيل الجهاز المحمول، يتم منع تطبيق ADB من اكتشاف الجهاز.

10. 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 لك 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. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

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

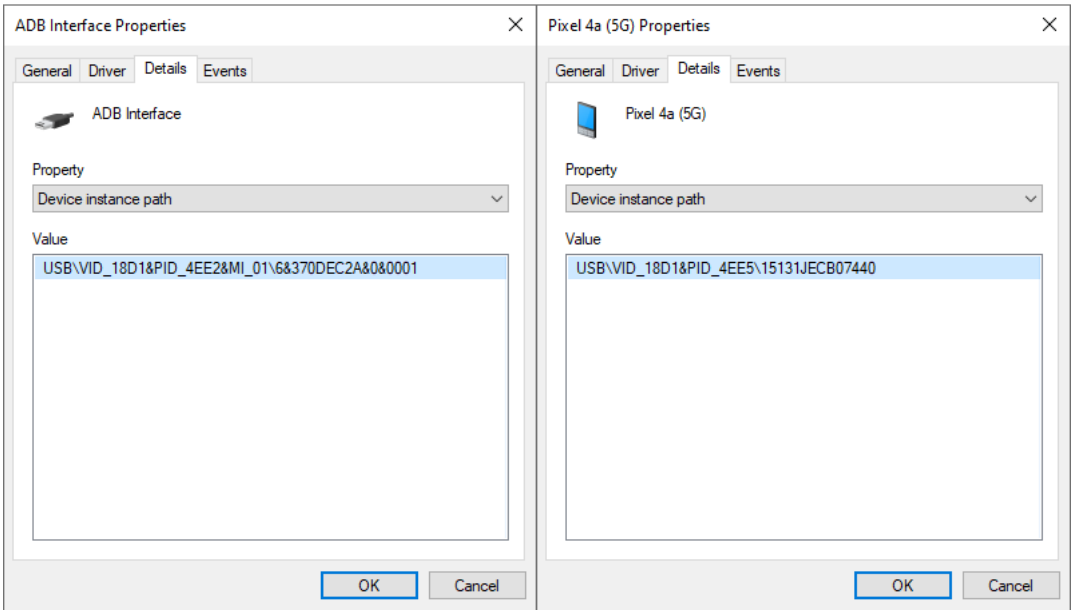
الأجهزة الموثوقة هي الأجهزة التي يتمتع المستخدمون المحددون في إعدادات الأجهزة الموثوقة بالوصول الكامل إليها في جميع الأوقات.

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 (Hardware ID – 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: `6&370DEC2A&0&0001`. إضافة الأجهزة حسب المُعرّف 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 Vendor ID (VID) وProduct ID (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

إدارة الوصول إلى أجهزة Bluetooth

يسمح Kaspersky Endpoint Security بإدارة الوصول إلى أجهزة Bluetooth. وتتضمن أجهزة Bluetooth لوحات المفاتيح وأجهزة الماوس وسماعات الرأس والطابعات اللاسلكية وما إلى ذلك. ويمكنك أيضًا استخدام Bluetooth للاتصال بجهاز محمول على سبيل المثال.

عند توصيل أجهزة Bluetooth أو فصلها، قد يقوم التطبيق بإنشاء أحداث متعددة حول الجهاز. والسبب هو أن نظام التشغيل قد يكتشف جهاز Bluetooth على أنه أجهزة متعددة من أنواع مختلفة. ويدير Kaspersky Endpoint Security أيضًا محول Bluetooth الذي يتم من خلاله توصيل الجهاز كجهاز منفصل. ولهذا السبب ينشئ التطبيق حدثًا لكل جهاز من الأجهزة المكتشفة.

يمكنك تحديد أحد الأوضاع التالية للوصول إلى أجهزة Bluetooth:

- **السماح وعدم التسجيل**. يسمح Kaspersky Endpoint Security بتوصيل أي أجهزة Bluetooth ولا يحفظ معلومات حول الاتصال في سجل الأحداث. ويمكنك توصيل أجهزة الإدخال التي تعمل عن طريق Bluetooth (لوحات المفاتيح وأجهزة الماوس وما إلى ذلك)، وإرسال البيانات عبر Bluetooth، وإدارة أجهزة Bluetooth الأخرى (سماعات الرأس، وما إلى ذلك).
- **سماح**. يسمح Kaspersky Endpoint Security بتوصيل أي أجهزة تعمل بتقنية Bluetooth. ويمكنك توصيل أجهزة الإدخال التي تعمل عن طريق Bluetooth (لوحات المفاتيح وأجهزة الماوس وما إلى ذلك)، وإرسال البيانات عبر Bluetooth، وإدارة أجهزة Bluetooth الأخرى (سماعات الرأس، وما إلى ذلك).
- **منع**. يقيد Kaspersky Endpoint Security الوصول إلى أجهزة Bluetooth. ويمكنك السماح بتوصيل أجهزة إدخال Bluetooth فقط (فئة Human Interface Devices). وتتضمن هذه الأجهزة لوحات المفاتيح وأجهزة الماوس وعصي التحكم، وما إلى ذلك.

لا يمكن إنشاء قائمة بأجهزة Bluetooth الموثوقة. وإذا كان لديك وصول مقيد إلى أجهزة Bluetooth، فيمكنك فقط الاتصال بأجهزة الإدخال المزودة باتصال Bluetooth.

كيفية تكوين قواعد الوصول إلى جهاز Bluetooth في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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 **تقنية Bluetooth**، كوّن وضع الوصول إلى جهاز Bluetooth: **سماح**، **منع**، **السماح وعدم التسجيل**.

7. إذا حددت وضع **منع**، يمكنك السماح بتوصيل أجهزة إدخال Bluetooth فقط (لوحات المفاتيح، وأجهزة الماوس، وما إلى ذلك). ولفعل ذلك، تحت **الاستثناءات**، حدد خانة الاختيار **أجهزة الإدخال (الماوس ولوحات المفاتيح)**.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين قواعد الوصول إلى جهاز Bluetooth في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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 access rules**، انقر على الرابط **Devices and Wi-Fi networks**.
يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. حدد نوع الجهاز **Bluetooth devices**.
يؤدي هذا إلى فتح إعدادات الوصول إلى جهاز Bluetooth.

7. تكوين وضع الوصول إلى جهاز Bluetooth: **Allow**، **Block**، **Allow and do not log**.

8. إذا حددت وضع **Block**، يمكنك السماح بتوصيل أجهزة إدخال Bluetooth فقط (لوحات المفاتيح، وأجهزة الماوس، وما إلى ذلك). ولفعل ذلك، تحت **Exclusions**، حدد خانة الاختيار **Input devices (mice and keyboards)**.

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

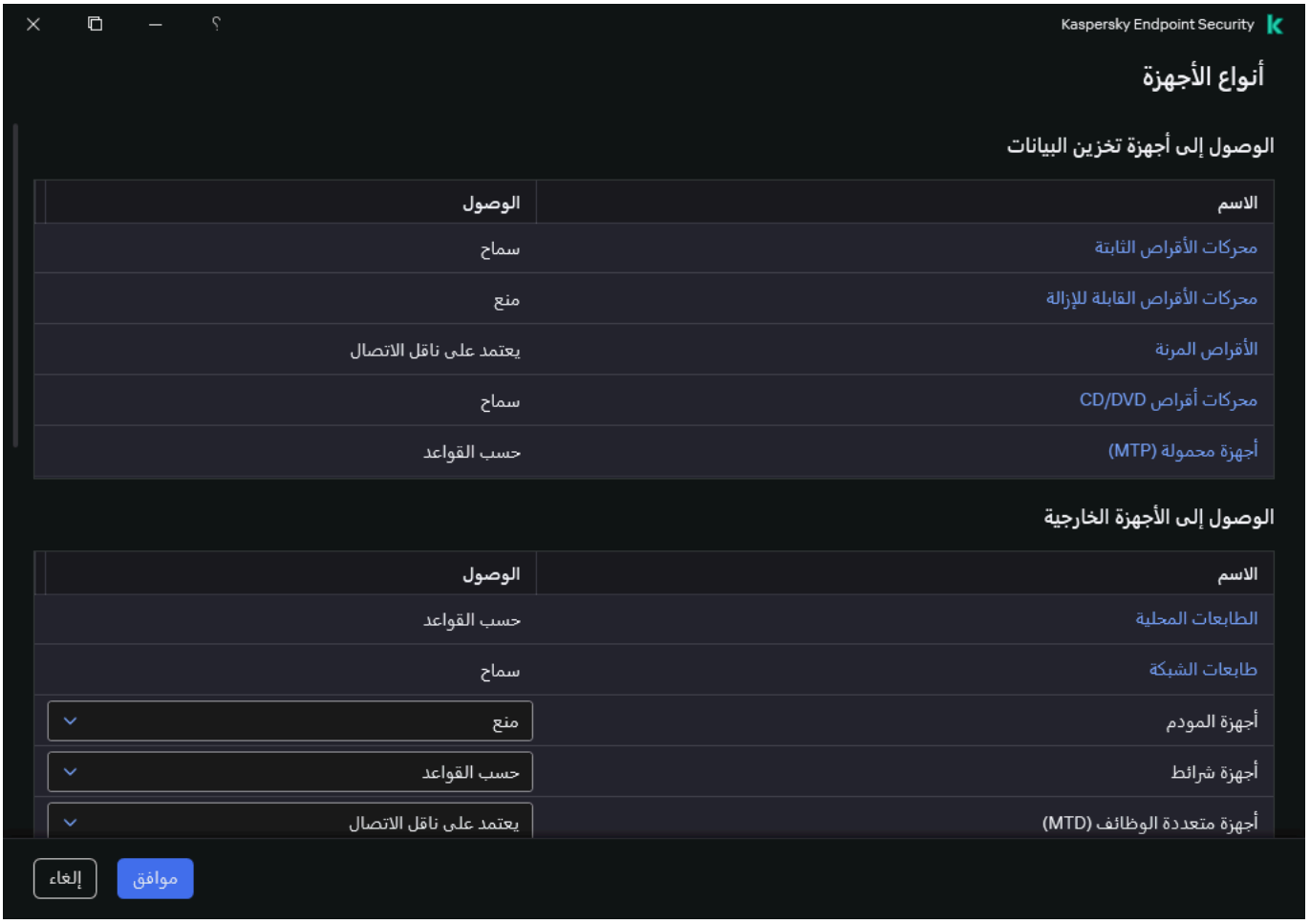
كيفية تكوين قواعد الوصول إلى جهاز Bluetooth في واجهة التطبيق

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 الأجهزة الخارجية**، انقر على الرابط **تقنية Bluetooth**.

يؤدي هذا إلى فتح إعدادات الوصول إلى جهاز Bluetooth.

5. تحت **الوصول**، كوّن وضع الوصول إلى جهاز Bluetooth: **سماح**، **منع**، **السماح وعدم التسجيل**.

6. إذا حددت وضع **منع**، يمكنك السماح بتوصيل أجهزة إدخال Bluetooth فقط (لوحات المفاتيح، وأجهزة الماوس، وما إلى ذلك). ولفعل ذلك، تحت **الاستثناءات**، حدد خانة الاختيار **أجهزة الإدخال (الماوس ولوحات المفاتيح)**.

7. احفظ تغييراتك.

التحكم في الطباعة

لا يتم دعم التحكم في الطباعة على أجهزة الكمبيوتر القائمة على بنية Arm.

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 Kaspersky Endpoint Security في اتصال الطابعات المحلية بمنافذ COM وLPT على مستوى الناقل فقط. وبالتالي، لمنع اتصالات الطابعة عبر منافذ COM وLPT، فإنك تحتاج إلى تحديد وضع الوصول إليه‌عتمد على ناقل الاتصال للطابعات المحلية وحظر الاتصالات بناقلات COM وLPT.

وبالنسبة للطابعات المتصلة بمنفذ USB، يمارس التطبيق التحكم على مستويين: نوع الجهاز (الطابعات المحلية) وناقل الاتصال (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. يمنح التطبيق حق الوصول إلى الطباعة لجميع المستخدمين ولا يحفظ معلومات عن 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.

4. تحت **إعدادات التحكم في الجهاز**، حدد علامة التبويب **أنواع الأجهزة**.

يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

5. في قائمة السياق لأنواع أجهزة **الطابعات المحلية وطابعات الشبكة**، كوّن وضع الوصول للطابعات ذات الصلة: **سماح** ✓ و**منع** ⊘ و**السماح وعدم التسجيل** (لطابعات الشبكة فقط)، أو **يعتمد على ناقل الاتصال** (للطابعات المحلية فقط).

6. لتكوين قواعد الطباعة على الطابعات المحلية وطابعات الشبكة، انقر نقرًا مزدوجًا فوق قوائم القواعد لفتحها.

7. يختار **حسب القواعد** كوضع وصول للطابعة.

8. 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 لك 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. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

e. انقر على **موافق**.

9. احفظ تغييراتك.

كيفية إضافة قواعد طباعة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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 access rules**، انقر على الرابط **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**Allow and do not log** (لطابعات الشبكة فقط)، و**Depends on bus** (للطابعات المحلية فقط)، أو **Custom**.

8. إذا حددت وضع **Custom**، 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 لك 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 **User or group**، حدد المستخدمين أو مجموعات المستخدمين للوصول إلى الطباعة. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

12. احفظ تغييراتك.

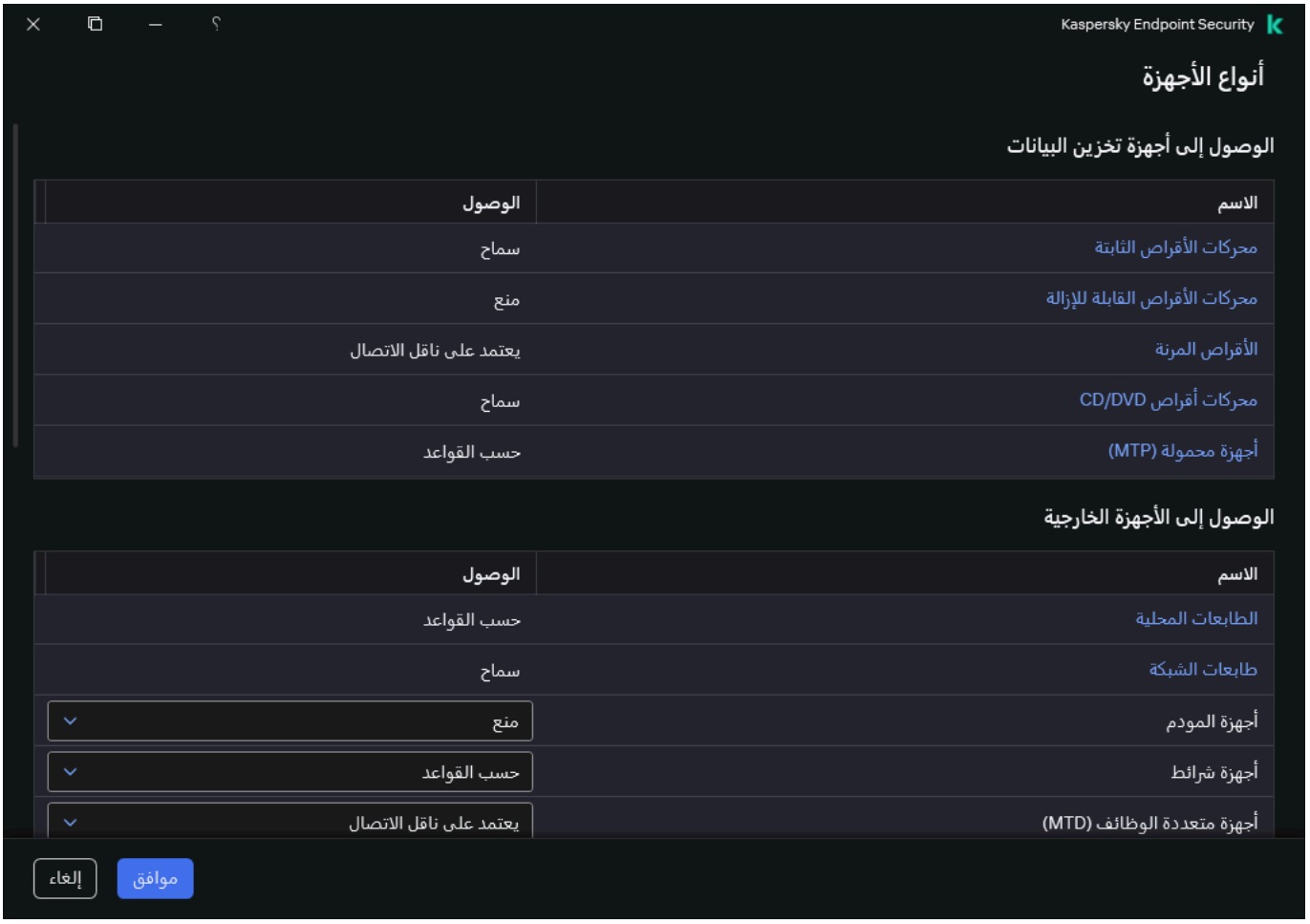
كيفية إضافة قواعد طباعة في واجهة التطبيق

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** or **الوصول إلى طابعات الشبكة**، كوّن وضع الوصول للطابعات: **سماح** أو **منع** أو **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 لك 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. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

7. احفظ تغييراتك.

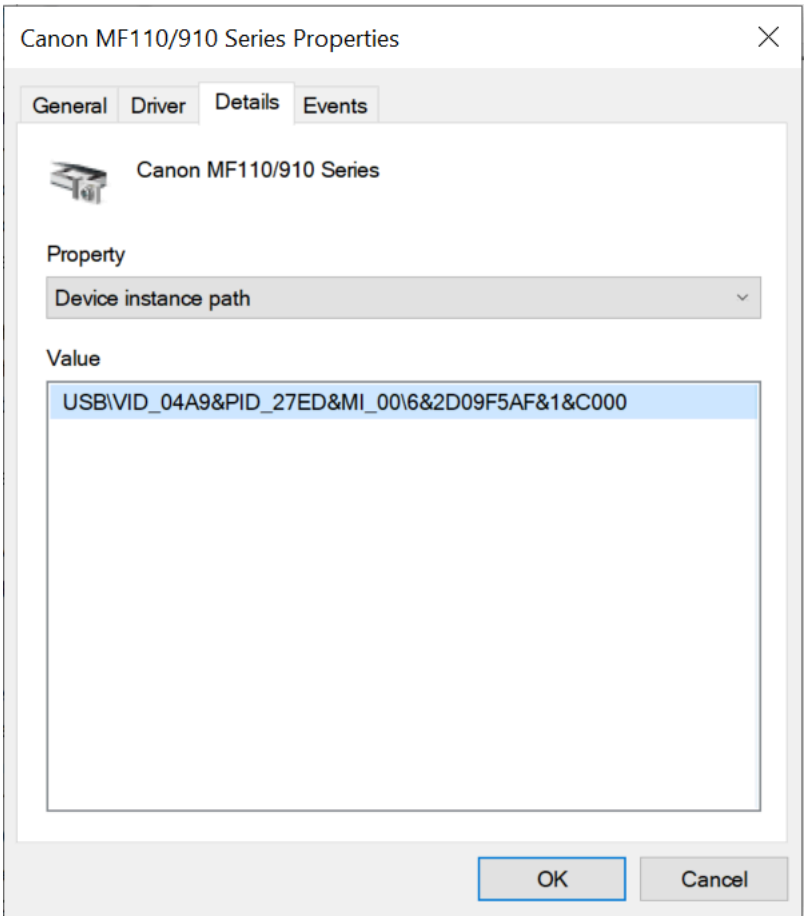
الطابعات الموثوقة

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 (Hardware ID – HWID). ويمكنك العثور على المعرف في خصائص الجهاز باستخدام أدوات نظام التشغيل (انظر الشكل أدناه). وتتيح لك أداة Device Manager فعل ذلك. وقد يبدو معرف الطابعة المحلية كما يلي: `6&2D09F5AF&1&C000`. 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 Vendor ID (VID) وProduct ID (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.

على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 11، تحتاج إلى تمكين خدمات الموقع للتحكم في اتصالات Wi-Fi. ولفعل ذلك ، تحتاج إلى تمكين مفتاح **خدمات الموقع** في إعدادات نظام التشغيل (**الإعدادات** ← **الخصوصية والأمان** ← **الموقع**). وفي حالة تعطيل خدمات الموقع، فلن يتحكم Kaspersky Endpoint Security في الاتصالات بشبكات Wi-Fi.

كيفية تقييد اتصالات Wi-Fi في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.
4. تحت **إعدادات التحكم في الجهاز**، حدد علامة التبويب **أنواع الأجهزة**.

   يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.
5. 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** (⊞).
6. 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 (Service Set Identifier) لشبكة Wi-Fi.
   - **نوع المصادقة**. نوع المصادقة المستخدم عند الاتصال بشبكة Wi-Fi.

     بدءًا من Kaspersky Endpoint Security for Windows الإصدار 12.0، تمت إضافة دعم بروتوكول WPA3 إلى التطبيق. وفي حالة تطبيق سياسة Kaspersky Endpoint Security الإصدار 12.2 على جهاز كمبيوتر، سيتم تحديد بروتوكول WPA2 على أجهزة الكمبيوتر التي يعمل عليها تطبيق Kaspersky Endpoint Security الإصدار 11.11.0 والإصدارات الأقدم؛ وتم تحديد WPA2 / WPA3 للإصدارات من 12.0 إلى 12.1؛ وتم تحديد WPA3 للإصدار 12.2 والإصدارات الأحدث.
   - **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.

7. احفظ تغييراتك.



إعدادات شبكة Wi-Fi الموثوقة

كيفية تقييد اتصالات Wi-Fi في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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. تحت **Device access rules**، حدد علامة التبويب **Devices and Wi-Fi networks**.
يسرد الجدول قواعد الوصول لجميع الأجهزة الموجودة في تصنيف مكون التحكم في الجهاز.

6. في القسم **Wi-Fi networks**، انقر على الرابط **Wi-Fi**.

7. في النافذة التي تفتح، حدد إجراء التحكم في الجهاز الذي تم اتخاذه عند الاتصال بشبكة Wi-Fi: **Allow** أو **Block** أو **Block with exclusions**.

8. إذا حددت الخيار **Block with exclusions**، 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):

   - **Name**. الاسم أو SSID (Service Set Identifier) لشبكة Wi-Fi.
   - **Authentication type**. نوع المصادقة المستخدم عند الاتصال بشبكة Wi-Fi.

بدءًا من Kaspersky Endpoint Security for Windows الإصدار 12.0، تمت إضافة دعم بروتوكول WPA3 إلى التطبيق. وفي حالة تطبيق سياسة Kaspersky Endpoint Security الإصدار 12.2 على جهاز كمبيوتر، سيتم تحديد بروتوكول WPA2 على أجهزة الكمبيوتر التي يعمل عليها تطبيق Kaspersky Endpoint Security الإصدار 11.11.0 والإصدارات الأقدم؛ وتم تحديد WPA2 / WPA3 للإصدارات من 12.0 إلى 12.1؛ وتم تحديد WPA3 للإصدار 12.2 والإصدارات الأحدث.

- **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.

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 (Service Set Identifier) لشبكة Wi-Fi.
- **نوع المصادقة**. نوع المصادقة المستخدم عند الاتصال بشبكة Wi-Fi.

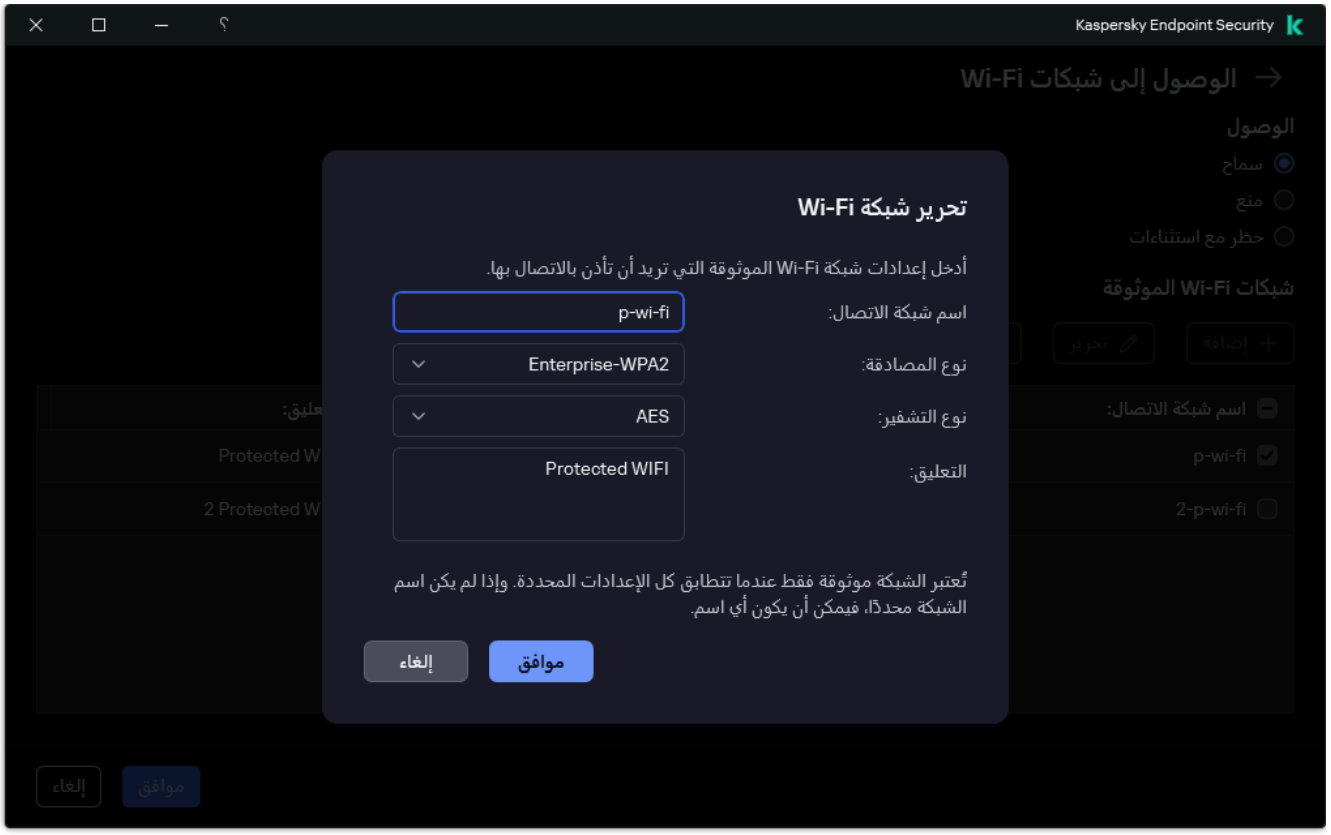
بدءًا من Kaspersky Endpoint Security for Windows الإصدار 12.0، تمت إضافة دعم بروتوكول WPA3 إلى التطبيق. وفي حالة تطبيق سياسة Kaspersky Endpoint Security الإصدار 12.2 على جهاز كمبيوتر، سيتم تحديد بروتوكول WPA2 على أجهزة الكمبيوتر التي يعمل عليها تطبيق Kaspersky Endpoint Security الإصدار 11.11.0 والإصدارات الأقدم؛ وتم تحديد WPA2 / WPA3 للإصدارات من 12.0 إلى 12.1؛ وتم تحديد WPA3 للإصدار 12.2 والإصدارات الأحدث.

- **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:

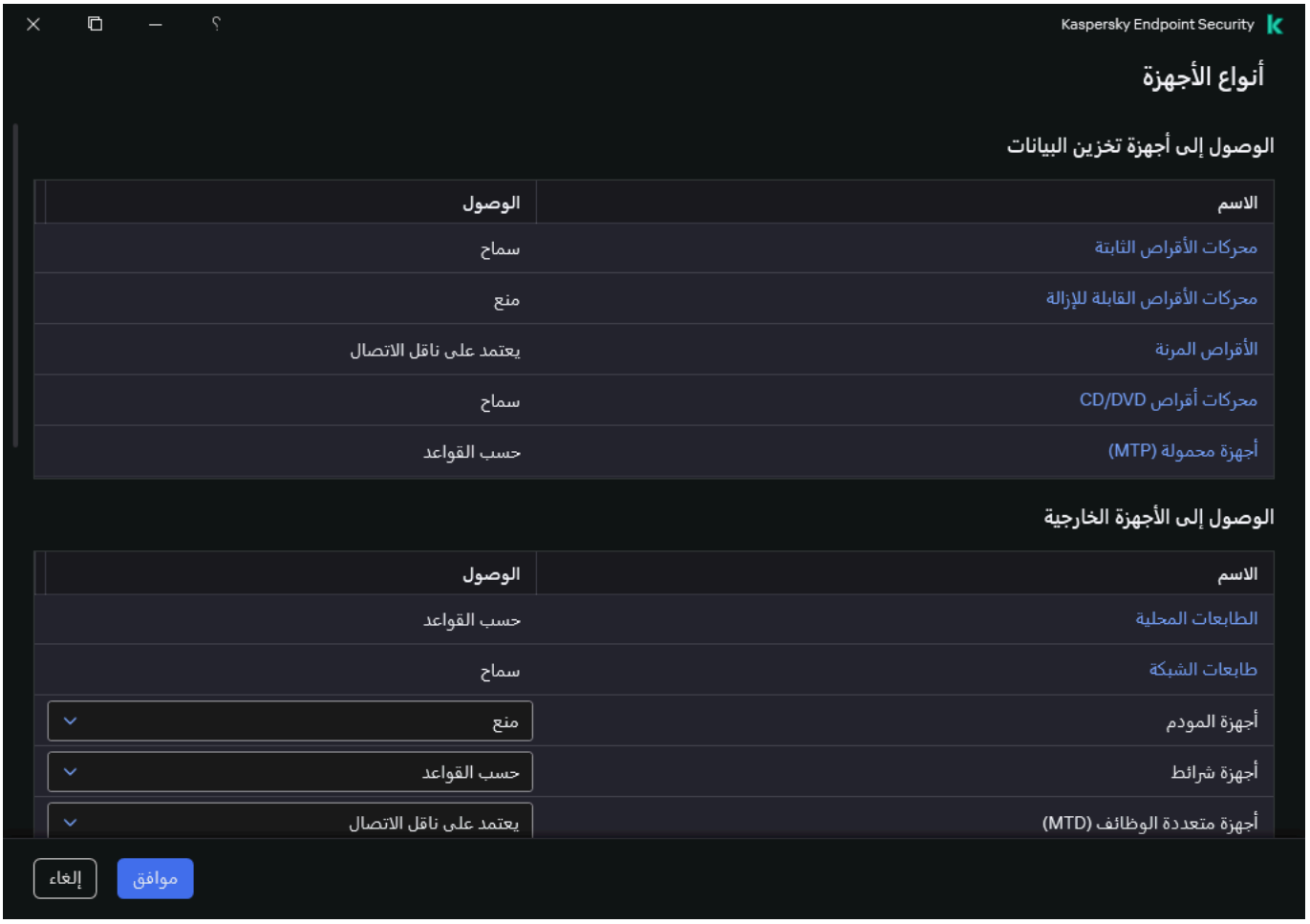
- مراقبة العمليات على الملفات الموجودة على محركات الأقراص القابلة للإزالة.
- مراقبة الاتصال وقطع الاتصال لمحركات الأقراص القابلة للإزالة الموثوقة.

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 رسائل معلوماتية.

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**.

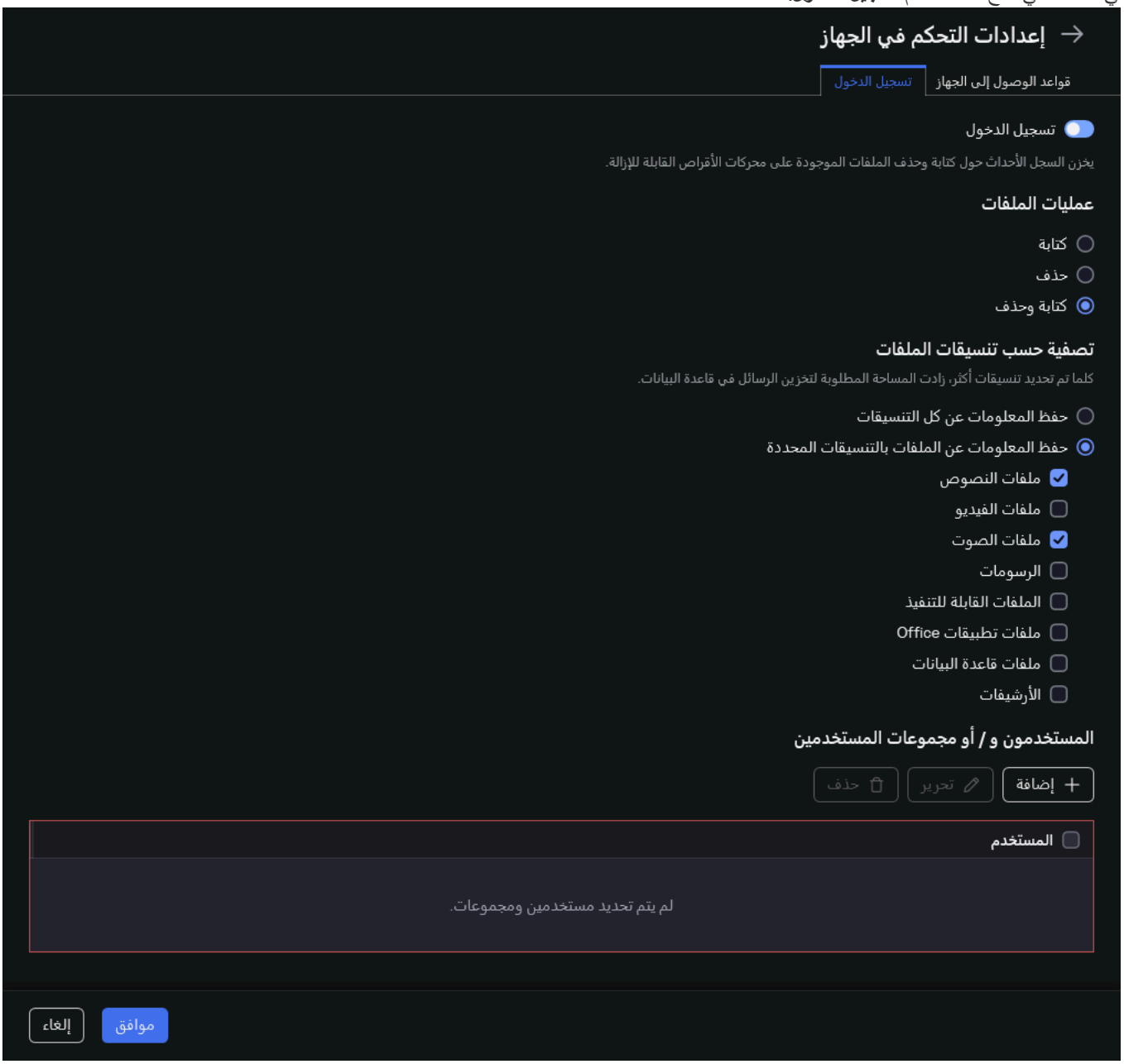
تعرض النافذة المفتوحة قواعد الوصول لجميع الأجهزة المدرجة في تصنيف مكون التحكم في الجهاز.



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 **Administration Server** من علامة التبويب **Events**. 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.14.2\environment]`
   - لأنظمة تشغيل 32 بت:
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES.14.2\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 5000 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 لم يتم نشره في مؤسستك، يمكنك توصيل الجهاز بالكمبيوتر ثم إضافته إلى القائمة "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 Informational messages.

إضافة جهاز إلى القائمة الموثوقة

يستقبل Kaspersky Security Center معلومات عن الأجهزة إذا كان Kaspersky Endpoint Security مثبتًا على أجهزة الكمبيوتر، وتم تمكين التحكم في الجهاز وتم تمكين نقل بيانات الجهاز. من غير الممكن إضافة جهاز إلى القائمة الموثوقة ما لم تكن المعلومات عن الجهاز متوفرة في Kaspersky Security Center.

عندما تتم إضافة جهاز لقائمة الأجهزة الموثوقة، يتم منح حق الوصول للجهاز، بشكل افتراضي، لجميع المستخدمين (مجموعة المستخدمين "الكل").

يمكنك إضافة جهاز إلى القائمة الموثوقة وفق البيانات التالية:

- **الأجهزة حسب المُعرِّف**. كل جهاز له معرف فريد (Hardware ID 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**. لكل جهاز Vendor ID (VID) وProduct ID (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_*`.

كيفية إضافة جهاز إلى القائمة الموثوقة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
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**).

لا يدعم Kaspersky Endpoint Security إضافة أجهزة من نوع **الأقراص المرنة** إلى القائمة الموثوقة.

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 الزر **Upgrade**. لعرض قائمة الأجهزة بشكل صحيح، يمكنك إضافة أجهزة عن طريق قناع معرف الجهاز.

10. لتصفية الأجهزة، في حقل **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 **Upgrade**.

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**.

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

الوصول إلى الأجهزة الموثوقة متاح لمجموعة "الكل" بشكل افتراضي.

15. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إضافة جهاز إلى القائمة الموثوقة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى القسم **Trusted Zone**.

5. في النافذة التي تفتح، انقر فوق الرابط **Devices**.

يفتح هذا نافذة تحتوي على قائمة بالأجهزة الموثوقة.

6. في الجزء الأيسر من النافذة، حدد علامة التبويب **الأجهزة الموثوقة**.

7. حدد خانة الاختيار **Merge values when inheriting** 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.

8. انقر على **Add**.

يفتح هذا النموذج لإضافة جهاز موثوق.

9. تحت **User or group**، حدد المستخدمين الذين تريد السماح لهم بالوصول إلى الأجهزة الموثوقة.

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

الوصول إلى الأجهزة الموثوقة متاح لمجموعة "الكل" بشكل افتراضي.

10. لتصفية الأجهزة، حدد نوع جهاز من القائمة المنسدلة **Device type** (مثل **Removable drives**).

لا يدعم Kaspersky Endpoint Security إضافة أجهزة من نوع **Floppy disks** إلى القائمة الموثوقة.

11. إذا كنت لا تعرف معرّف الجهاز أو طراز الجهاز بالضبط، فحدد خانة الاختيار **Use mask**.

12. حدد الطريقة التي تريد بها إضافة الجهاز: حسب معرف الجهاز أو الطراز (VID وPID).

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. في الوقت نفسه، سيتم عرض قائمة الأجهزة الفارغة في Kaspersky Security Center. لعرض قائمة الأجهزة بشكل صحيح، يمكنك إضافة أجهزة عن طريق قناع معرف الجهاز.

13. لتصفية الأجهزة، في حقل **Search for trusted devices** أدخل اسم الكمبيوتر أو قناعًا لاسم الكمبيوتر الذي يتصل الجهاز به.

الحرف `*` يستبدل أي مجموعة من الرموز. الحرف `?` يستبدل أي حرف مفرد.

تعرض الطاولة قائمة بالأجهزة التي تطابق معايير التصفية المحددة.

14. حدد مربعات الاختيار المجاورة لأسماء الأجهزة التي ترغب في إضافتها إلى قائمة الأجهزة الموثوقة.

15. في حقل **Comment**، أدخل وصفًا لسبب إضافة الأجهزة إلى القائمة الموثوقة.

16. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إضافة جهاز إلى القائمة الموثوقة 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 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.

لا يدعم Kaspersky Endpoint Security إضافة أجهزة من نوع **الأقراص المرنة** إلى القائمة الموثوقة.

6. في الحقل **التعليق**، يمكنك تقديم أي معلومات ذات صلة بالجهاز الموثوق به.

7. حدد المستخدمين أو مجموعات المستخدمين الذين تريد السماح لهم بالوصول إلى الأجهزة الموثوقة.

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

8. 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.

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.

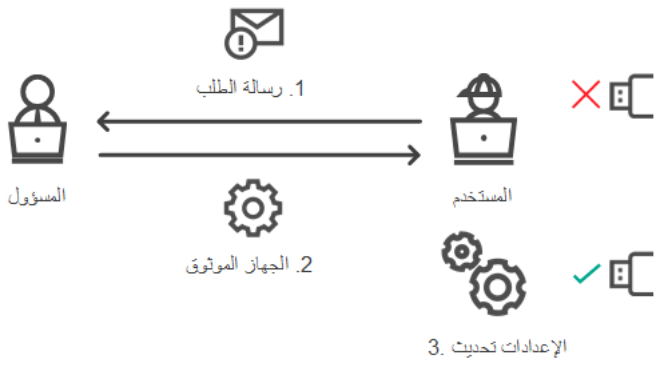
2. يتلقى المسؤول رسالة بالطلب في وحدة تحكم Kaspersky Security Center.

تحتوي وحدة تحكم Kaspersky Security Center على User requests 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.



رسم تخطيطي لمنح صلاحية وصول إلى جهاز بوضع الاتصال بالإنترنت

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 بطلبات للوصول المؤقت**.

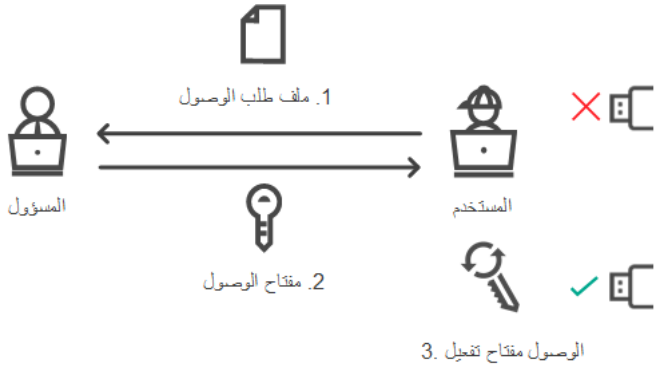
إذا كنت تحتاج إلى منح صلاحية وصول مؤقت إلى جهاز محظور ولكن لا يمكنك إضافة الجهاز إلى القائمة الموثوقة، يمكنك منح صلاحية الوصول إلى الجهاز بالوضع غير متصل بالإنترنت. وبهذه الطريقة، يمكنك منح صلاحية الوصول إلى جهاز محظور حتى إذا لم يكن جهاز الكمبيوتر لديه حق الوصول إلى الشبكة أو إذا كان جهاز الكمبيوتر 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، يتلقى المسؤول في وحدة تحكم Kaspersky Security Center الحدث رسالة منع الوصول للجهاز إلى المسؤول. ويتضمن الحدث اسم المستخدم واسم الكمبيوتر وتفاصيل الجهاز الذي يحاول المستخدم الوصول إليه ومعلومات أخرى. ويمكنك تكوين كيفية إخطار المسؤول بهذه الأحداث، وعلى سبيل المثال، تحديد إخطارات البريد الإلكتروني. تحتوي وحدة تحكم Kaspersky Security Center على User requests كتحديد لحدث معين مسبقًا لسهولة تتبع الرسائل من المستخدمين.

للسماح بالوصول، يجب عليك إضافة الجهاز إلى القائمة الموثوق بها. وبعد تحديث إعدادات Kaspersky Endpoint Security على الكمبيوتر، يستطيع المستخدم 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 بطلبات 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 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 **Managed devices** 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 **Devices**.

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. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **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 الوصول**.
في الوضع الافتراضي، يأخذ إعداد **مدة 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 نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.

2. في قائمة أجهزة الكمبيوتر العميلة، حدد جهاز الكمبيوتر الذي يجب أن يحصل على حق وصول مؤقت إلى جهاز ممنوع.

3. انقر فوق زر النقاط الثلاث (...) الموجود فوق 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 **Overview** وقم بتنزيل ملف طلب الوصول الذي تم استلامه من المستخدم.

ستری 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. يوفر خبراء Kaspersky قالبًا لرسالة إلى المستخدم تصف أسباب منع الوصول إلى الجهاز (انظر الشكل أدناه).

يتم توفير متغيرات خاصة لإدارة قوالب الرسائل (على سبيل المثال، %USER_NAME%). وتسمح المتغيرات باستخدام قالب رسالة واحدة لأجهزة الكمبيوتر المختلفة. وعند إنشاء رسالة، يسترجع Kaspersky Endpoint Security قيمة المتغير من إعدادات نظام التشغيل ويدرجها في الرسالة التي تتطابق مع الكمبيوتر والمستخدم والحدث المحدد.



إخطار التحكم في 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. ولفعل ذلك ، يجب على المستخدم النقر على الزر **طلب الوصول** أو **طلب وصول مؤقت** وإرسال رسالة إلى المسؤول تصف الموقف. ويمكنك أيضًا إعداد قالب الرسالة للمسؤول، مع إضافة بيانات قد تفيد في قرارك بالسماح بالوصول إلى الجهاز أو منعه. 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 **User requests**. 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.

كيفية تغيير قوالب رسائل التحكم في الجهاز في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في الجهاز**.
4. في القسم **إعدادات قوالب الرسائل**، انقر على الزر **القوالب**.
5. يفتح هذا نافذة؛ وفي تلك النافذة، كوّن قوالب التحكم في التطبيقات:

- **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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **المتغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.

يمكنك أيضًا استعادة نص القالب الافتراضي.

6. احفظ تغييراتك.

كيفية تغيير قوالب رسائل التحكم في الجهاز في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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 **Message templates**، كوّن قوالب لرسائل التحكم في التطبيقات:

- **Message to user**. 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.
- **Message to administrator**. 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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **Add variable** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.
يمكنك أيضًا استعادة نص القالب الافتراضي.

6. احفظ تغييراتك.

كيفية تغيير قوالب رسالة التحكم في الجهاز في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.

3. في القسم **قوالب الرسائل**، كوّن قوالب لرسائل التحكم في التطبيقات:

- **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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **إضافة متغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.
يمكنك أيضًا استعادة نص القالب الافتراضي.

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 الأحداث في تقرير تشغيل القاعدة ومستودع **Rule triggers in Smart Training state**.

2. تحليل تقرير تشغيل القاعدة.

يحلل المسؤول تقرير تشغيل القاعدة أو محتويات مستودع **Rule triggers in Smart Training state**. 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 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 **Rule triggers in Smart Training state**. ونوصي بالتحقق من التقرير عن تشغيل القواعد ومحتويات تخزين **Rule triggers in Smart Training state**.

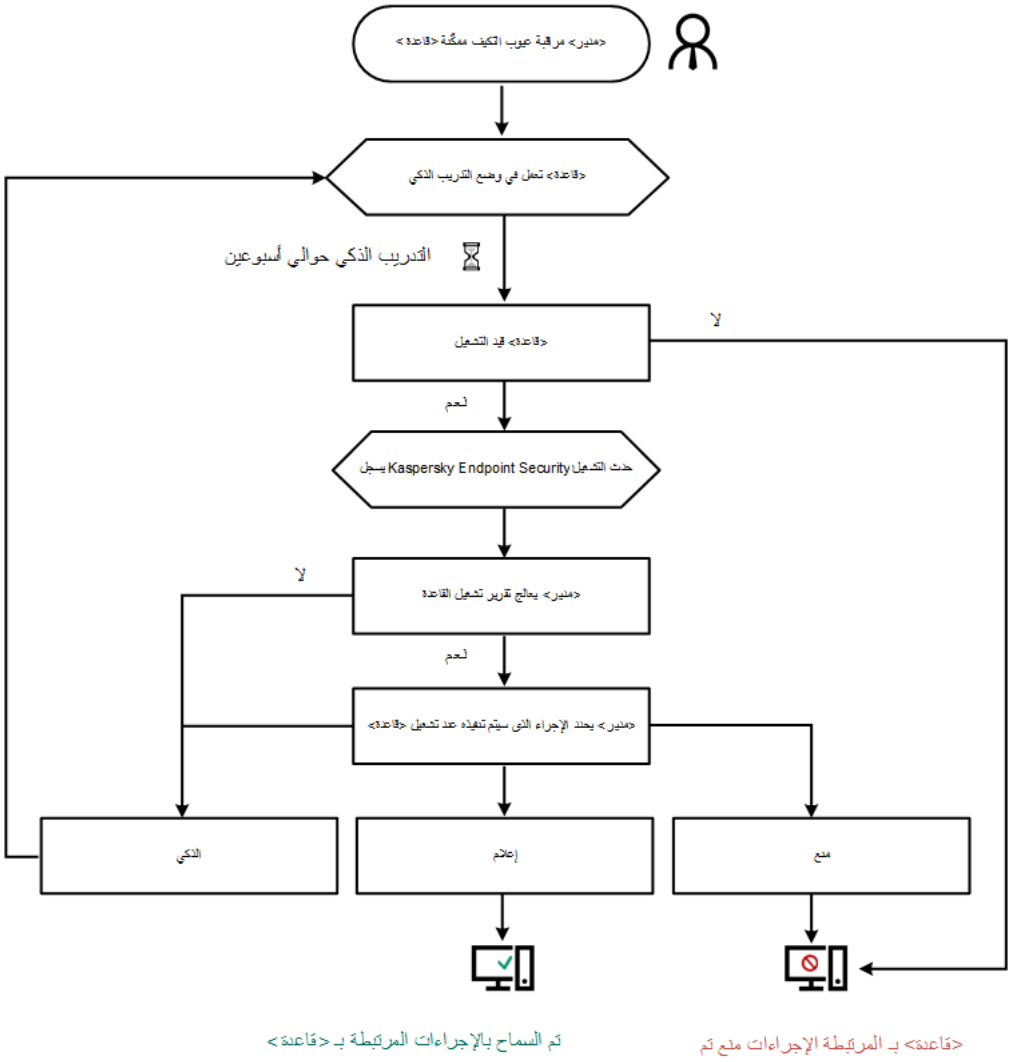
عندما يحاول تطبيق ضار تنفيذ إجراء ما، سيحظر Kaspersky Endpoint Security الإجراء ويعرض إخطارًا (انظر الشكل أدناه).



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

تدريب مكون مراقبة عيوب التكيف

يتضمن مكون مراقبة عيوب التكيف مجموعة من القواعد (أنماط السلوك). 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. لا يمنع مكون مراقبة عيوب التكيف نشاط التطبيق على الكمبيوتر ، لكنه يُخطر المسؤول فقط. ويمكنك أيضًا تحديد الإجراء الذي يتم تنفيذه يدويًا عند تشغيل قاعدة مراقبة عيوب التكيف.

كيفية عرض قائمة قواعد مراقبة عيوب التكيف في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Security Controls** ← **Adaptive Anomaly Control**.

5. حدد خانة الاختيار **مراقبة عيوب التكيف**.

6. تحت **إعدادات قاعدة مراقبة عيوب التكيف**، انظر إلى قائمة القواعد.
بشكل افتراضي، تعمل جميع القواعد في وضع **الذكي**.

7. إذا لزم الأمر، تأكد من تحديث قاعدة مراقبة عيوب التكيف.

8. إذا لزم الأمر، قم حدد إجراءً عند إطلاق قاعدة مراقبة عيوب التكيف:

- **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.
- **إعلام**. 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.

9. إذا لزم الأمر، قم بتعطيل القواعد التي لا تريد استخدامها.

10. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية عرض قواعد مراقبة عيوب التكيف في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **Security Controls** ← **Adaptive Anomaly Control**.

5. قم بتشغيل مفتاح **Adaptive Anomaly Control ENABLED**.

6. تحت **Rules**، انظر إلى قائمة القواعد.
بشكل افتراضي، تعمل جميع القواعد في وضع **Smart**.

7. إذا لزم الأمر، تأكد من تحديث قاعدة مراقبة عيوب التكيف.

8. إذا لزم الأمر، قم حدد إجراءً عند إطلاق قاعدة مراقبة عيوب التكيف:

- **Block**. 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.
- **Inform**. 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.

9. إذا لزم الأمر، قم بتعطيل القواعد التي لا تريد استخدامها.

10. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية عرض قائمة قواعد مراقبة عيوب التكيف في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **Security Controls** ← **Adaptive Anomaly Control**.

3. قم بتشغيل مفتاح **مراقبة عيوب التكيف**.

4. في القسم **القواعد**، انقر على الرابط **تحرير القواعد**.
تفتح قائمة قاعدة مراقبة عيوب التكيف. بشكل افتراضي، تعمل جميع القواعد في وضع **الذكي**.

5. إذا لزم الأمر، تأكد من تحديث قاعدة مراقبة عيوب التكيف.

6. إذا لزم الأمر، قم حدد إجراءً عند إطلاق قاعدة مراقبة عيوب التكيف:

- **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.
- **إعلام**. 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. إذا لزم الأمر، قم بتعطيل القواعد التي لا تريد استخدامها.

8. احفظ تغييراتك.

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.

إذا لم يتم إطلاق قاعدة أثناء التدريب، فإن مكون مراقبة عيوب التكيف يعتبر هذا السلوك غير نمطي ويغير حالة القاعدة إلى **المنع الذكي**. وبالتالي، يمنع التطبيق أي نشاط يطابق هذه القاعدة.

في حالة تشغيل قاعدة أثناء التدريب، فأنت بحاجة إلى تكوين الإجراء الذي يطبقه التطبيق يدويًا على النشاط المكتشف الذي يطابق هذه القاعدة. وإذا لم تحدد الإجراء عند تشغيل القاعدة، يستمر مكون مراقبة عيوب التكيف في وضع التدريب.

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 **Rule triggers in Smart Training state** 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.
- **إعلام**. 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.

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

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**. تجزئة SHA256 للملف.
- **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` أو `object://ipconfig` أو `object://HKEY_USERS`. يمكنك أيضًا استخدام الأقنعة، على سبيل المثال، `object://*C:\Windows\temp\*`.
- **تجزئة الكائن المصدر**. تجزئة SHA256 للملف.

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**. تجزئة SHA256 للملف.
- **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**. تجزئة SHA256 للملف.

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 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.
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 للرسائل الموجهة إلى المسؤول حول حظر الإجراءات الضارة المحتملة. يتم توفير متغيرات خاصة لإدارة قوالب الرسائل (على سبيل المثال، %USER_NAME%). وتسمح المتغيرات باستخدام قالب رسالة واحدة لأجهزة الكمبيوتر المختلفة. وعند إنشاء رسالة، يسترجع Kaspersky Endpoint Security قيمة المتغير من إعدادات نظام التشغيل ويدرجها في الرسالة التي تتطابق مع الكمبيوتر والمستخدم والحدث المحدد.

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 **User requests**. 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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **إضافة متغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.
يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **إعادة تعيين**.

4. احفظ تغييراتك.

عمليات مراقبة عيوب التكيف

تتضمن مراقبة عيوب التكيف العديد من أدوات المراقبة. ويعد الغرض الرئيسي من مراقبة عيوب التكيف هو تكوين المكون أثناء التدريب.

تقارير مراقبة عيوب التكيف

تستخدم مراقبة عيوب التكيف التقارير التالية:

- **تقرير حول حالة قواعد مراقبة عيوب التكيف**. يحتوي التقرير على معلومات عن حالة قواعد مراقبة عيوب التكيف (Off وSmart Training وSmart Block وNotify وBlock). ويسمح هذا التقرير بتحليل مستوى تدريب مراقبة عيوب التكيف وتقييم عدد القواعد التي تحولت من وضع Smart Training إلى وضع التشغيل العادي (على سبيل المثال، Smart Block).
- **تقرير حول قواعد مراقبة عيوب التكيف التي تم تشغيلها**. يحتوي التقرير على معلومات عن مشغلات القاعدة. ويعرض التقرير أيضًا وضع تشغيل القاعدة: Block (بما في ذلك Smart Block) أو Notify. وتسمح هذه التقارير بتقييم نشاط مراقبة عيوب التكيف على أجهزة كمبيوتر المستخدم.

كيفية عرض تقارير مراقبة عيوب التكيف في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **مراقبة عيوب التكيف**.
4. قم بأحد الإجراءات التالية:
   - إذا كنت تريد عرض التقرير عن حالة قواعد مراقبة عيوب التكيف، فانقر فوق الرابط **تقرير حول حالة قواعد مراقبة عيوب التكيف**.
   - إذا كنت تريد عرض التقرير عن قواعد مراقبة عيوب التكيف التي تم تشغيلها، فانقر فوق الرابط **تقرير حول قواعد مراقبة عيوب التكيف التي تم تشغيلها**.
5. تبدأ عملية إنشاء التقرير.

يتم عرض التقرير في نافذة جديدة.

كيفية عرض تقارير مراقبة عيوب التكيف في Web Console

1. في نافذة Web Console الرئيسية، حدد علامة التبويب **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Security Controls** ← **Adaptive Anomaly Control**.
5. في القسم **Rules**، نفذ أحد الإجراءات التالية:
   - إذا كنت تريد عرض التقرير عن حالة قواعد مراقبة عيوب التكيف، فانقر فوق **Rules state** ← **View report**.
   - إذا كنت تريد عرض التقرير عن قواعد مراقبة عيوب التكيف التي تم تشغيلها، فانقر فوق **Detections** ← **View report**.
6. تبدأ عملية إنشاء التقرير.

يتم عرض التقرير في نافذة جديدة.

لإنشاء تقارير في وحدة تحكم Kaspersky Security Center، يجب عليك تمكين نقل البيانات إلى خادم الإدارة. ويتم تمكين نقل البيانات بشكل افتراضي.

كيفية تمكين نقل البيانات لمراقبة عيوب التكيف في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **التقارير والمخزن**.
4. في القسم **نقل البيانات إلى خادم الإدارة**، انقر على الزر **الإعدادات**.
5. حدد المربعات التالية:
   - **تقرير حول حالة قواعد مراقبة عيوب التكيف**.
   - **تقرير حول قواعد مراقبة عيوب التكيف التي تم تشغيلها**.
6. احفظ تغييراتك.

كيفية تمكين نقل البيانات لمراقبة عيوب التكيف في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **KSC Integration**.
5. تحت **Data transfer to Administration Server**، حدد خانات الاختيار التالية:
   - **Report on Adaptive Anomaly Control rules state**.
   - **Report on triggered Adaptive Anomaly Control rules**.
6. احفظ تغييراتك.

مخزن Rule triggers in Smart Training state

في وضع التدريب، يرسل مكون مراقبة عيوب التكيف معلومات عن القواعد التي تم تشغيلها إلى وحدة تخزين منفصلة، **Rule triggers in Smart Training state**. ويتم تمثيل المعلومات عن القواعد التي تم تشغيلها في وحدة التخزين كقائمة من الأحداث. لضبط مراقبة عيوب التكيف، يمكنك إما تأكيد السلوك غير النمطي على الكمبيوتر أو إضافة استثناء من القاعدة.

أحداث مراقبة عيوب التكيف

تقوم قاعدة سجلات مراقبة عيوب التكيف بتشغيل الأحداث في Block (بما في ذلك وضعي Smart Block) وNotify. ويتم توفير الأحداث التالية لهذا الغرض:

Process action blocked

Process action skipped

تحتوي الأحداث على معلومات عن النشاط المريب بما في ذلك المجاميع الاختبارية للملف والمستخدمين المشاركين ووقت بدء تشغيل القاعدة واسم الكمبيوتر. وبعد تحليل الحدث، يمكنك إضافة استثناءات على الفور من القاعدة إذا وجدت أن النشاط مشروع.

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. ولإنشاء فئة، يمكنك استخدام المعايير التالية: فئة KL (على سبيل المثال المستعرضات او فئة أخرى)، وتجزئة الملف وبائع التطبيق ومعايير أخرى.

2. إنشاء قواعد التحكم في التطبيقات.

   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. ويمكن للمسؤول إنشاء العديد من القواعد. وقد يتطابق تطبيق واحد مع معايير القواعد المتعددة. تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. ويتحقق Kaspersky Endpoint Security مما إذا كان التطبيق يتطابق مع قاعدة في كل مرة يتم تشغيلها فيها. ويطابق Kaspersky Endpoint Security بشكل تسلسلي التطبيق مقابل جميع قواعد التحكم في التطبيق.

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.

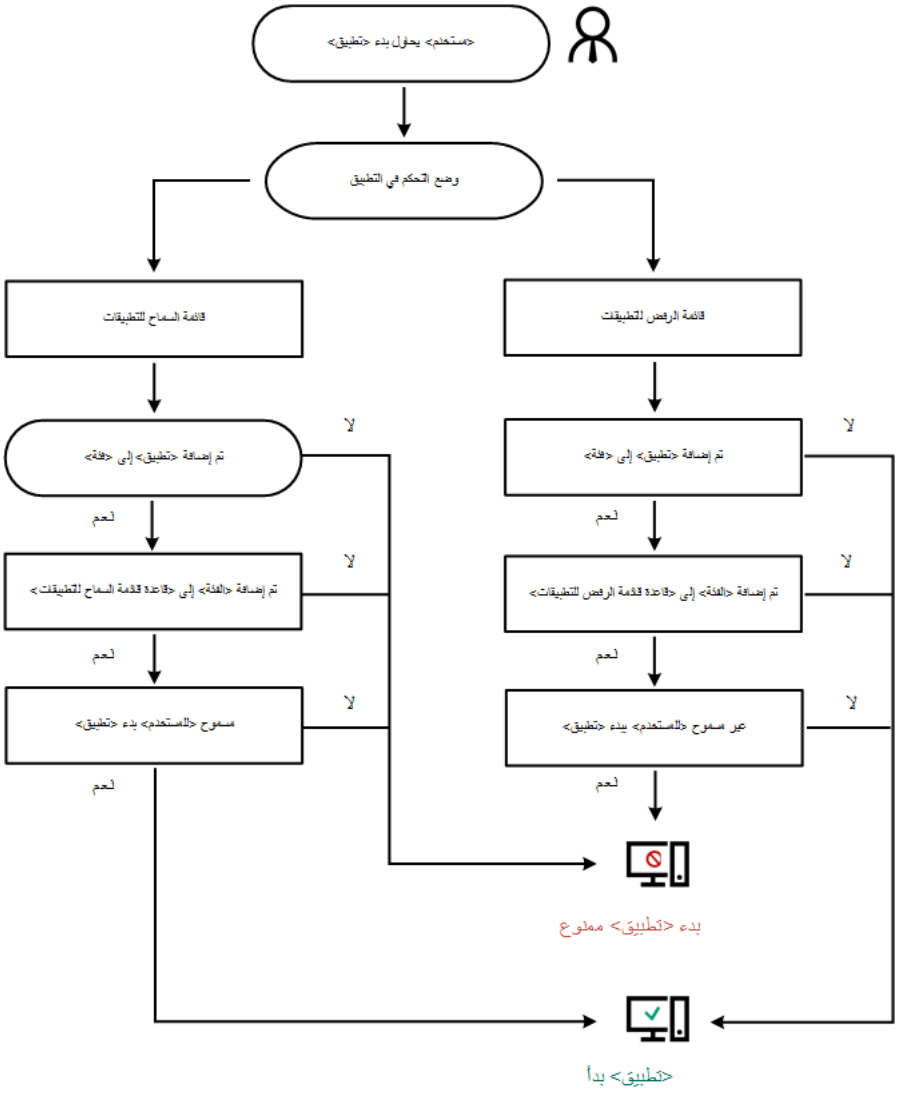
  تستند قواعد التحكم في التطبيقات التي تم إنشاؤها في وحدة تحكم إدارة Kaspersky Security Center إلى فئات التطبيقات المخصصة وليس على شروط التضمين والاستبعاد كما هو الحال في الواجهة المحلية لـ Kaspersky Endpoint Security.

- استلام معلومات حول التطبيقات المثبَّتة 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 **برامج أخرى\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

الحصول على معلومات عن التطبيقات المثبتة

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.

عرض معلومات التطبيق

يتم توفير المعلومات عن التطبيقات المثبتة بواسطة عميل شبكة Kaspersky Security Center. يتم إتاحة المعلومات عن التطبيقات المثبتة بواسطة وحدة تحكم Kaspersky Security Center (مجلد **Applications registry**). ويقوم عميل الشبكة بتحديث المعلومات عند كل مزامنة مع Kaspersky Security Center. وللحصول على تفاصيل عن المعلومات المرسلة بواسطة عميل الشبكة، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

لفتح نافذة خصائص التطبيقات في مجلد سجل التطبيقات:

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة تحكم الإدارة، حدد المجلد **Advanced** ← **Application management** ← **Applications registry**.
3. حدد تطبيقًا.
4. في قائمة السياق الخاصة بالتطبيق، حدد **Properties**.

عرض معلومات عن الملفات القابلة للتنفيذ

يمكنك تقليل الحمل على قاعدة البيانات عند الاستعلام عن معلومات عن الملفات القابلة للتنفيذ. ولتحقيق ذلك، نوصي بتشغيل مهمة المخزون على العديد من أجهزة الكمبيوتر المرجعية التي تم تثبيت مجموعة البرامج القياسية الخاصة بك عليها.

يتم توفير عن حول الملفات القابلة للتنفيذ بواسطة Kaspersky Endpoint Security. ولتلقي معلومات الأجهزة، تحتاج إلى تطبيق سياسة نشطة تتيح إرسال معلومات التطبيقات المثبتة (يتم تمكين هذا الإرسال بشكل افتراضي).

كيفية تمكين إرسال معلومات التطبيق في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **التقارير والمخزن**.
4. في القسم **نقل البيانات إلى خادم الإدارة**، انقر على الزر **الإعدادات**.
5. حدد خانة الاختيار **التطبيقات التي تم بدء تشغيلها**.
6. احفظ تغييراتك.

كيفية تمكين إرسال معلومات التطبيق في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **KSC Integration**.
5. في القسم **Data transfer to Administration Server**، انقر على الزر **Advanced settings**.
6. في النافذة التي تفتح، حدد خانة الاختيار **About started applications**.
7. احفظ تغييراتك.

يمكنك الحصول على قائمة بالملفات القابلة للتنفيذ باستخدام مهمة المخزون في Kaspersky Endpoint Security. ويمكنك عرض قائمة الملفات القابلة للتنفيذ في لوحة تحكم Kaspersky Security Center في المجلد **Executable files**.

قبل تشغيل مهمة المخزون، تأكد أن قاعدة البيانات تلبي توصيات Kaspersky Security Center. وللتفاصيل عن قيود قاعدة البيانات، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

كيفية تشغيل مهمة المخزون في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
تفتح قائمة المهام.
2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **المخزون**.

الخطوة الثانية: نطاق الجرد

أنشئ قائمة بالمجلدات التي تريد أن يبحث Kaspersky Endpoint Security فيها عن الملفات القابلة للتنفيذ. قم بتكوين إعدادات الجرد (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: اختيار الحساب لتشغيل المهمة

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

الخطوة الخامسة: تكوين جدول بدء المهمة

كوّن جدول المهام، على سبيل المثال، يدويًا.

الخطوة السادسة: تحديد اسم المهمة

أدخل اسم المهمة، على سبيل الجرد الأساسي.

الخطوة 7 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة. ونتيجة لذلك، يتم إجراء بحث عن الملفات القابلة للتنفيذ على أجهزة كمبيوتر المستخدمين وفقًا للجدول الذي تم تكوينه.

كيفية تشغيل مهمة المخزون في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر على **Add**.

يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Inventory**.

c. في الحقل **Task name** أدخل وصفًا مختصرًا، علي سبيل المثال، الجرد الأساسي.

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

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

5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

6. قم بإنهاء المعالج.

سيتم عرض مهمة جديدة في قائمة المهام.

7. لتكوين المهمة، انتقل إلى خصائص المهمة (انظر الجدول أدناه).

8. حدد خانة الاختيار المجاورة للمهمة.

9. انقر فوق **Start**.

يمكنك مراقبة حالة المهمة وعدد الأجهزة التي تم استكمال المهمة عليها بنجاح أو اكتمل تنفيذها مع وجود خطأ. ونتيجة لذلك، سيتم البحث عن الملفات القابلة للتنفيذ على أجهزة كمبيوتر المستخدم وفقًا للجدول المحدد.

لفتح نافذة الخصائص لملف قابل للتنفيذ في المجلد Executable files:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة تحكم الإدارة، حدد المجلد **Executable files** ← **Application management** ← **Advanced**.

3. حدد ملفًا قابلاً للتنفيذ.

4. في قائمة سياق الملف التنفيذي، حدد **الخصائص**.

لعرض معلومات عامة حول التطبيق وملفاته التنفيذية، وقائمة بأجهزة الكمبيوتر المثبت عليها تطبيق ما، افتح نافذة خصائص في تطبيق ما تم تحديده في المجلد **Applications registry** أو في المجلد **Executable files**.

تحديث المعلومات عن التطبيقات المثبتة والملفات القابلة للتنفيذ

تم تحسين تشغيل مكون التحكم في التطبيقات مع قاعدة بيانات الملفات القابلة للتنفيذ في Kaspersky Endpoint Security. ويُحدث Kaspersky Endpoint Security تلقائيًا قاعدة البيانات بعد إزالة الملف من الكمبيوتر. ويسمح ذلك بالحفاظ على قاعدة البيانات مُحدثة وحفظ موارد Kaspersky Security Center. وللحفاظ على تحديث قاعدة بيانات التطبيقات المثبتة، يجب تمكين إرسال معلومات التطبيق إلى خادم الإدارة (يتم تمكينه افتراضيًا).

المعلمة	الوصف
Inventory scopes	قائمة الكائنات التي ستشكل نطاق الجرد.
DLL modules inventory	يبحث Kaspersky Endpoint Security عن وحدات DLL في نطاق الجرد ويرسل المعلومات إلى Kaspersky Security Center. يؤدي تمكين جرد وحدات DLL إلى زيادة كبيرة في الوقت المستغرق لإكمال مهمة الجرد وحجم قاعدة البيانات.
Script files inventory	يبحث Kaspersky Endpoint Security عن البرامج النصية في نطاق الجرد ويرسل المعلومات إلى Kaspersky Security Center. يؤدي تمكين مخزون ملفات البرامج النصية إلى زيادة كبيرة في الوقت المستغرق لإكمال مهمة الجرد وحجم قاعدة البيانات.
Run only when the computer is idle	تأجيل بدء مهمة 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. يتيح لك خيار الجدولة هذا الحفاظ على موارد الكمبيوتر عند استخدام الكمبيوتر.
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.
Skip file that is scanned for longer than (sec) N ثانية	تقييد وقت تنفيذ المهمة. وبعد مدة زمنية معينة، 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.
Scan archives	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).
Scan distribution packages	فحص حزم توزيع تطبيقات الجهات الخارجية.
Do not unpack large compound files	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.

كيفية تمكين وضع التطبيقات الممنوعة

وضع التطبيقات الممنوعة هو وضع يتيح فيه التحكم في التطبيقات للمستخدمين بدء تشغيل جميع التطبيقات باستثناء التطبيقات المحظورة في قواعد التحكم في التطبيقات. بمعنى، في حالة عدم وجود قاعدة رفض، يسمح التحكم في التطبيقات ببدء تشغيل التطبيق. يتم تمكين وضع المنع لإجراءات التحكم في التطبيقات بشكلٍ افتراضي.

قبل تمكين وضع التطبيقات الممنوعة، نوصي باختبار قواعد التحكم في التطبيقات. ولهذا الغرض، يمكنك تمكين وضع الاختبار.

كيفية تمكين وضع التطبيقات الممنوعة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في التطبيقات**.
5. حدد خانة الاختيار **التحكم في التطبيقات**.

6. في القسم **إعدادات التحكم في التطبيقات** استخدم القائمة المنسدلة **وضع التحكم** لتحديد **قائمة الرفض**.

7. في القائمة المنسدلة **الإجراء** حدد الإجراء للتحكم في التطبيقات:

- **اختبار القواعد**. لا يقوم التحكم في التطبيقات بمنع التطبيقات التي تم منعها من العمل وفقًا للقواعد، لكنه ينشئ أحداثًا عن تشغيل التطبيقات التي قد يتم منعها بخلاف ذلك.
- **تطبيق القواعد**. يقوم التحكم في التطبيقات بمنع التطبيقات الممنوعة وينشئ الأحداث المقابلة.

8. حدد الحالة لقواعد التحكم في التطبيقات:

- **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.

وإذا لزم الأمر، أضف قواعد التحكم في التطبيقات الجديدة.

9. تكوين الإعدادات المتقدمة للتحكم في التطبيقات:

- **مراقبة تحميل وحدات DLL (يؤدي إلى زيادة كبيرة في الحمل على النظام)**. 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 "**صورة ذهبية\الشهادات 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.

- **استخدم التحقق الصارم من التوقيع الرقمي**. يمكنك تحديد شهادة كشرط تشغيل لقاعدة التحكم في التطبيق. وفي حالة تحديد خانة الاختيار هذه، يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بشهادات فقط من مخزن شهادات نظام موثوق. وتعتبر التطبيقات الموقعة بمثل هذه الشهادة موثوقة أيضًا بواسطة مكونات الحماية ، على سبيل المثال المهمة فحص البرامج الضارة. ومع ذلك، إذا حددت شهادة من متجر مختلف في قاعدة التحكم في التطبيقات، فلن يطبق Kaspersky Endpoint Security هذه القاعدة.

  إذا تم إلغاء تحديد خانة الاختيار، فسوف يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بواسطة شهادة من Windows Trusted Root Certificate Store. ولا تعد مثل هذه التطبيقات جزءًا من المنطقة الموثوقة. وتراقب مكونات الحماية نشاط هذه التطبيقات.

- **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.

10. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين وضع التطبيقات الممنوعة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **Security Controls** ← **App Control**.

5. قم بتشغيل مفتاح **Application Control ENABLED**.

6. في القسم **Operating mode**، حدد **Block all except the rules list**.

7. في **Action**، حدد إجراء التحكم في التطبيقات:

- **Inform**. لا يقوم التحكم في التطبيقات بمنع التطبيقات التي تم منعها من العمل وفقًا للقواعد، لكنه ينشئ أحداثًا عن تشغيل التطبيقات التي قد يتم منعها بخلاف ذلك.
- **Apply rules**. يقوم التحكم في التطبيقات بمنع التطبيقات الممنوعة وينشئ الأحداث المقابلة.

8. حدد الحالة لقواعد التحكم في التطبيقات:

- **Enabled**. تعني هذه الحالة أن القاعدة مستخدمة عند تشغيل مكون التحكم في التطبيقات.
- **Disabled**. تعني هذه الحالة أن القاعدة يتم تجاهلها عند تشغيل مكون التحكم في التطبيقات.
- **Test mode**. 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.

وإذا لزم الأمر، أضف قواعد التحكم في التطبيقات الجديدة.

9. تكوين الإعدادات المتقدمة للتحكم في التطبيقات:

- **Monitor loading of DLL modules**. 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 "**صورة ذهبية\الشهادات 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.

- **Use strict digital signature verification**. يمكنك تحديد شهادة كشرط تشغيل لقاعدة التحكم في التطبيق. وفي حالة تحديد خانة الاختيار هذه، يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بشهادات فقط من مخزن شهادات نظام موثوق. وتعتبر التطبيقات الموقعة بمثل هذه الشهادة موثوقة أيضًا بواسطة مكونات الحماية ، على سبيل المثال المهمة فحص البرامج الضارة. ومع ذلك، إذا حددت شهادة من متجر مختلف في قاعدة التحكم في التطبيقات، فلن يطبق Kaspersky Endpoint Security هذه القاعدة.

  إذا تم إلغاء تحديد خانة الاختيار، فسوف يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بواسطة شهادة من Windows Trusted Root Certificate Store. ولا تعد مثل هذه التطبيقات جزءًا من المنطقة الموثوقة. وتراقب مكونات الحماية نشاط هذه التطبيقات.

- **Message to user**. قالب الرسالة التي يتم عرضها عندما يتم بدء تشغيل قاعدة التحكم في التطبيق التي تمنع بدء تشغيل تطبيق ما.

- **Message to administrator**. قالب الرسالة التي يمكن للمستخدم إرسالها إلى مسؤول الشبكة المحلية للشركة إذا كان المستخدم يعتقد أنه قد تم حظر التطبيق عن طريق الخطأ.

10. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين وضع التطبيقات الممنوعة في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.

3. قم بتشغيل مفتاح **التحكم في التطبيقات**.

4. في القسم **وضع التحكم في بدء تشغيل التطبيق**، حدد **قائمة الرفض. يُسمح بجميع التطبيقات، باستثناء تلك المدرجة في قائمة القواعد**.

5. في **الإجراء عند بدء تشغيل التطبيقات الممنوعة بواسطة القواعد**، حدد إجراء التحكم في التطبيقات:

- **إبلاغ (وضع الاختبار) وسجل الأحداث في تقرير**. لا يقوم التحكم في التطبيقات بمنع التطبيقات التي تم منعها من العمل وفقًا للقواعد، لكنه ينشئ أحداثًا عن تشغيل التطبيقات التي قد يتم منعها بخلاف ذلك.

- **منع**. يقوم التحكم في التطبيقات بمنع التطبيقات الممنوعة وينشئ الأحداث المقابلة.

6. حدد الحالة لقواعد التحكم في التطبيقات:

- **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.

- **وضع الاختبار**. 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.

وإذا لزم الأمر، أضف قواعد التحكم في التطبيقات الجديدة.

7. تكوين الإعدادات المتقدمة للتحكم في التطبيقات:

- **مراقبة 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 "**صورة ذهبية\الشهادات 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.

- **استخدام التحقق الصارم من التوقيع الرقمي**. يمكنك تحديد شهادة كشرط تشغيل لقاعدة التحكم في التطبيق. وفي حالة تحديد خانة الاختيار هذه، يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بشهادات فقط من مخزن شهادات نظام موثوق. وتعتبر التطبيقات الموقعة بمثل هذه الشهادة موثوقة أيضًا بواسطة مكونات الحماية ، على سبيل المثال المهمة فحص البرامج الضارة. ومع ذلك، إذا حددت شهادة من متجر مختلف في قاعدة التحكم في التطبيقات، فلن يطبق Kaspersky Endpoint Security هذه القاعدة.

  إذا تم إلغاء تحديد خانة الاختيار، فسوف يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بواسطة شهادة من Windows Trusted Root Certificate Store. ولا تعد مثل هذه التطبيقات جزءًا من المنطقة الموثوقة. وتراقب مكونات الحماية نشاط هذه التطبيقات.

- **قوالب رسائل عن منع التطبيق**. قالب الرسالة التي يتم عرضها عندما يتم بدء تشغيل قاعدة التحكم في التطبيق التي تمنع بدء تشغيل تطبيق ما.

- **نص رسالة القالب الذي يتم عرضه عندما يتم حظر بدء تشغيل التطبيق**. قالب الرسالة التي يمكن للمستخدم إرسالها إلى مسؤول الشبكة المحلية للشركة إذا كان المستخدم يعتقد أنه قد تم حظر التطبيق عن طريق الخطأ.

8. احفظ تغييراتك.

نتيجة لذلك، يقوم التحكم في التطبيقات بمنع التطبيقات الممنوعة. وينشئ Kaspersky Endpoint Security أيضًا أحداث تم حظر بدء تشغيل التطبيق. ويمكنك استخدام هذه الأحداث لإنشاء Report on prohibited applications في وحدة تحكم Kaspersky Security Center . وفي ملخص التقرير، يمكنك عرض قائمة التطبيقات وأجهزة الكمبيوتر التي تم تشغيل قاعدة التحكم في التطبيقات عليها.

التحكم في التطبيق بناءً على كمبيوتر أساسي

يمكنك استخدام كمبيوتر أساسي لإنشاء صورة لمجموعة من التطبيقات التي تحتاجها. ويمكنك بعد ذلك استخدام هذه الصورة لنشر نظام التشغيل والتطبيقات على أجهزة الكمبيوتر الأخرى. وليس من الممكن دائمًا تحديث الصورة. ويتيح لك التحكم في التطبيقات الاحتفاظ بقائمة بالتطبيقات المسموح بها بناءً على كمبيوتر أساسي. ويحدد التحكم في التطبيقات تلقائيًا التطبيقات المثبتة على الكمبيوتر الأساسي ويقوم بتحديث الفئة. وبهذه الطريقة، تحصل أجهزة الكمبيوتر على قائمة محدثة بالتطبيقات المسموح بها.

يتضمن تكوين التحكم في التطبيقات بناءً على كمبيوتر أساسي الخطوات التالية:

1. إنشاء فئة يتم تحديثها تلقائيًا. عند إنشاء فئة جديدة، حدد **فئة تحتوي على ملفات تنفيذية من مجلد محدد.** وحدد الكمبيوتر الأساسي الخاص بك.

كيفية إنشاء فئة يتم تحديثها تلقائيًا في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة تحكم الإدارة، حدد المجلد **Application categories** ← **Application management** ← **Advanced**.
3. انقر فوق الزر **New category** في مساحة العمل.

   يؤدي هذا إلى بدء معالج إنشاء فئة التطبيقات.
4. اتبع تعليمات معالج إنشاء فئة التطبيقات.

الخطوة 1. تحديد نوع الفئة

حدد **فئة تتضمن ملفات تنفيذية من الأجهزة المحددة.** كنوع الفئة.

الخطوة 2. إدخال اسم فئة مستخدم

في هذه الخطوة، حدد اسمًا لفئة التطبيق.

الخطوة 3. الإعدادات

تتوفر هذه الخطوة إذا حددت نوع الفئة **فئة تتضمن ملفات تنفيذية من الأجهزة المحددة**.

في هذه الخطوة، انقر فوق الزر **Add** 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 **Executable files** 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:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.
- خانة الاختيار **Synchronize data with Administration Server repository**. 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 **Executable files**.

  إذا تم مسح خانة الاختيار **Synchronize data with Administration Server repository**، فإن Kaspersky Security Center لن يقوم بإجراء أي تعديلات لفئة التطبيق بعد إنشائها.

الخطوة 4. عامل التصفية

في هذه الخطوة، كوّن عامل تصفية للملفات.

يمكنك تحديد نوع الملف الذي تريد استخدامه لإنشاء فئة التطبيقات.

- **All files**. ستطابق الفئة كل الملفات. ويتم تحديد هذا الخيار بشكل افتراضي.
- **Only files outside the application categories**. سوف تتطابق الفئة فقط مع الملفات من خارج فئات التطبيقات.

يمكنك تحديد مجلدات أجهزة الكمبيوتر المحددة التي تحتوي على ملفات تريد استخدامها لإنشاء فئة التطبيقات.

- **All folders**. سوف تتطابق الفئة مع كل المجلدات. ويتم تحديد هذا الخيار بشكل افتراضي.
- **Specified folder**. ستطابق الفئة المجلد المحدد فقط. وإذا حددت هذا الخيار، فإنك تحتاج إلى تحديد مسار مجلد.

الخطوة 5. إنشاء فئة مخصصة

قم بإنهاء المعالج.

كيفية إنشاء فئة بمحتوى تمت إضافته تلقائيًا في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Operations** ← **Third-party applications** ← **Application categories**.
يفتح هذا قائمة فئات التطبيقات.

2. انقر على **Add**.
يؤدي هذا إلى بدء معالج إنشاء فئة التطبيقات.

3. تكوين الإعدادات العامة لفئة التطبيقات:

- اسم الفئة.
- طريقة إنشاء الفئة. حدد **Category that includes executable files from selected devices** كنوع الفئة.

انتقل إلى الخطوة التالية.

4. تكوين الإعدادات المتقدمة لفئة التطبيقات:

- حدد أجهزة الكمبيوتر التي سيضيف منها Kaspersky Security Center الملفات القابلة للتنفيذ إلى فئة التطبيقات. سوف تضاف كل الملفات القابلة للتنفيذ من أجهزة الكمبيوتر المحددة المعروضة في مجلد **Executable files** إلى فئة التطبيقات بواسطة Kaspersky Security Center.
- حدد خوارزمية لحساب دالة التجزئة.
- كوّن فاصلاً زمنيًا لمزامنة البيانات مع وحدة تخزين خادم الإدارة.
- كوّن عامل تصفية للملفات.

5. قم بإنهاء المعالج.

عند إنشاء فئة يتم تحديثها تلقائيًا، قد يكون من الملائم تقسيم الملفات إلى فئات متعددة. على سبيل المثال، ملفات نظام التشغيل والملفات من مجلد Program Files. ولفعل ذلك، يمكنك استخدام عامل تصفية في إعدادات الفئة وتحديد المجلدات الفردية.

2. حدد وضع التحكم في التطبيقات. تحتاج إلى منع تنفيذ جميع التطبيقات غير المسموح بها صراحةً. ولفعل ذلك، حدد التطبيقات الممنوعة mode.

3. إنشاء قاعدة تحكم في التطبيقات. في إعدادات القاعدة، حدد الفئة التي تنتمي إليها الملفات القابلة للتنفيذ من الكمبيوتر الأساسي.

كيفية تكوين التحكم في التطبيقات باستخدام كمبيوتر أساسي في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في التطبيقات**.

5. حدد خانة الاختيار **التحكم في التطبيقات**.

6. في القسم **إعدادات التحكم في التطبيقات** استخدم القائمة المنسدلة **وضع التحكم** لتحديد **قائمة الرفض**.

7. في القائمة المنسدلة **الإجراء** حدد الإجراء للتحكم في التطبيقات:

- **اختبار القواعد**. لا يقوم التحكم في التطبيقات بمنع التطبيقات التي تم منعها من العمل وفقًا للقواعد، لكنه ينشئ أحداثًا عن تشغيل التطبيقات التي قد يتم منعها بخلاف ذلك.
- **تطبيق القواعد**. يقوم التحكم في التطبيقات بمنع التطبيقات الممنوعة وينشئ الأحداث المقابلة.

8. في قائمة قواعد التحكم في التطبيقات، انقر فوق الزر **إضافة**.
يبدأ هذا المعالج لإضافة قاعدة التحكم في التطبيقات.

9. في القائمة المنسدلة **الفئة**، حدد فئة يتم تحديثها تلقائيًا بناءً على الكمبيوتر الأساسي.

10. حدد المستخدمين أو مجموعة المستخدمين الذين تريد تطبيق قاعدة التحكم في التطبيقات عليهم.

11. تكوين الإعدادات المتقدمة لقاعدة التحكم في التطبيقات:

- **رفض للمستخدمين الآخرين**. يمنع التطبيق تشغيل التطبيقات التي تنتمي إلى الفئة المحددة لجميع المستخدمين غير الموجودين في القائمة.
- **برامج التحديث الموثوقة**. يعتبر Kaspersky Endpoint Security التطبيقات التي تتضمنها الفئة المحددة كبرامج تحديث موثوقة مسموح لها بإنشاء ملفات تنفيذية أخرى سيتم السماح لها لاحقًا بالعمل.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين التحكم في التطبيقات باستخدام كمبيوتر أساسي في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **Security Controls** ← **App Control**.

5. قم بتشغيل مفتاح **Application Control ENABLED**.

6. في القسم **Operating mode**، حدد **Block all except the rules list**.

7. في **Action**، حدد إجراء التحكم في التطبيقات:

- **Inform**. لا يقوم التحكم في التطبيقات بمنع التطبيقات التي تم منعها من العمل وفقًا للقواعد، لكنه ينشئ أحداثًا عن تشغيل التطبيقات التي قد يتم منعها بخلاف ذلك.
- **Apply rules**. يقوم التحكم في التطبيقات بمنع التطبيقات الممنوعة وينشئ الأحداث المقابلة.

8. في قائمة قواعد التحكم في التطبيقات، انقر فوق الزر **Add**.
يبدأ هذا المعالج لإضافة قاعدة التحكم في التطبيقات.

9. تحت **Categories/Applications**، حدد فئة يتم تحديثها تلقائيًا بناءً على الكمبيوتر الأساسي.

10. حدد المستخدمين أو مجموعة المستخدمين الذين تريد تطبيق قاعدة التحكم في التطبيقات عليهم.

11. تكوين الإعدادات المتقدمة لقاعدة التحكم في التطبيقات:

- **Users**. يمنع التطبيق تشغيل التطبيقات التي تنتمي إلى الفئة المحددة لجميع المستخدمين غير الموجودين في القائمة.
- **Trusted Updaters**. يعتبر Kaspersky Endpoint Security التطبيقات التي تتضمنها الفئة المحددة كبرامج تحديث موثوقة مسموح لها بإنشاء ملفات تنفيذية أخرى سيتم السماح لها لاحقًا بالعمل.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين التحكم في التطبيقات بناءً على كمبيوتر أساسي في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.
3. قم بتشغيل مفتاح **التحكم في التطبيقات**.
4. في القسم **وضع التحكم في بدء تشغيل التطبيق**، حدد **قائمة الرفض. يُسمح بجميع التطبيقات، باستثناء تلك المدرجة في قائمة القواعد**.
5. في **الإجراء عند بدء تشغيل التطبيقات الممنوعة بواسطة القواعد**، حدد إجراء التحكم في التطبيقات:

- **إبلاغ (وضع الاختبار) وسجل الأحداث في تقرير**. لا يقوم التحكم في التطبيقات بمنع التطبيقات التي تم منعها من العمل وفقًا للقواعد، لكنه ينشئ أحداثًا عن تشغيل التطبيقات التي قد يتم منعها بخلاف ذلك.
- **منع**. يقوم التحكم في التطبيقات بمنع التطبيقات الممنوعة وينشئ الأحداث المقابلة.

6. في قائمة قواعد التحكم في التطبيقات، انقر فوق الزر **إضافة**.
يبدأ هذا المعالج لإضافة قاعدة التحكم في التطبيقات.
7. تحت **الفئة**، حدد فئة يتم تحديثها تلقائيًا بناءً على الكمبيوتر الأساسي.
8. حدد المستخدمين أو مجموعة المستخدمين الذين تريد تطبيق قاعدة التحكم في التطبيقات عليهم.
9. تكوين الإعدادات المتقدمة لقاعدة التحكم في التطبيقات:

- **رفض للمستخدمين الآخرين**. يمنع التطبيق تشغيل التطبيقات التي تنتمي إلى الفئة المحددة لجميع المستخدمين غير الموجودين في القائمة.
- **برامج التحديث الموثوقة**. يعتبر Kaspersky Endpoint Security التطبيقات التي تتضمنها الفئة المحددة كبرامج تحديث موثوقة مسموح لها بإنشاء ملفات تنفيذية أخرى سيتم السماح لها لاحقًا بالعمل.

10. احفظ تغييراتك.

إدارة قواعد التحكم في التطبيق

يتحكم Kaspersky Endpoint Security في بدء تشغيل التطبيقات بواسطة المستخدمين باستخدام القواعد. تحدد قاعدة التحكم في التطبيق شروط بدء التشغيل والإجراءات التي يتم تنفيذها بواسطة 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.
- **وضع 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 المجلد **Application categories** ← **Application management** ← **Advanced**.
3. انقر فوق الزر **New category** في مساحة العمل.
   يبدأ معالج إنشاء فئة المستخدم.
4. اتبع تعليمات معالج إنشاء الفئة الجديد.

الخطوة 1. تحديد نوع الفئة

يمكنك في هذه الخطوة تحديد أحد أنواع فئات التطبيق التالية:

- Category with content added manually. Data of executable files is manually added to the category إذا حددت هذا النوع من الفئات، فسوف تتمكن في خطوة Configuring conditions for inclusion of applications in categories وخطوة Configuring conditions for exclusion of applications from categories من تحديد المعايير التي سيتم تضمين الملفات القابلة للتنفيذ بموجبها في الفئة.

- Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category إذا حددت هذا النوع من الفئات، في خطوة Settings سوف تكون قادرًا على تحديد جهاز كمبيوتر سيتم تضمين ملفاته القابلة للتنفيذ تلقائيًا في الفئة.

- Category that includes executable files from a specific folder. Executable files of applications copied to the specified folder are automatically processed and their metrics are added to the category إذا حدد هذا النوع من الفئات، في خطوة Repository folder سوف تكون قادرًا على تحديد مجلد سيتم تضمين الملفات القابلة للتنفيذ منه تلقائيًا 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

عند إضافة عدد كبير من الشروط إلى قواعد التحكم في التطبيق (على سبيل المثال، تجزئة الملف)، يزيد استهلاك موارد الكمبيوتر. وعندما يصل العدد الإجمالي للشروط إلى 50000، قد تحدث مشكلات في الأداء. ولتحسين الأداء، يوصى بمراجعة عدد الشروط وتقليله.

تتوافر هذه الخطوة إذا حددت نوع الفئة **فئة ذات محتوى مضاف يدويًا**.

في هذه الخطوة، في القائمة المنسدلة **Add**، حدد شروط إضافة التطبيقات إلى الفئة:

- **From the list of executable files**. إضافة تطبيقات من قائمة الملفات القابلة للتنفيذ على الجهاز العميل إلى الفئة المخصصة.

- **From file properties**. حدد البيانات التفصيلية للملفات التنفيذية كشرط لإضافة التطبيقات إلى الفئة المخصصة.

- **Metadata from files in folder**. 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.

- **Checksums of the files in the folder**. 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.

- **Certificates for the files from the folder**. 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 fingerprint** في خصائصها.

- **MSI installer files metadata**. 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.

- **Checksums of the files from the MSI installer of the application**. حدد حزمة MSI. سوف يشير Kaspersky Security Center إلى تجزئات الملفات القابلة للتنفيذ المجمعة في حزمة MSI هذه كشرط لإضافة التطبيقات إلى الفئة المخصصة.

- **From KL category**. حدد فئة KL كشرط لإضافة التطبيقات إلى الفئة المخصصة. تعتبر فئة KL عبارة عن قائمة تضم التطبيقات التي تشترك في سمات موضوعية موحدة. وتتم إدارة هذه القائمة بواسطة خبراء Kaspersky. على سبيل المثال، تتضمن فئة KL المعروفة باسم Office Applications التطبيقات من مجموعة Microsoft Office وAdobe Acrobat وغيرها.

  يمكنك تحديد كل فئات KL لتوليد قائمة موسعة بالتطبيقات الموثوقة.

- **Specify path to application (masks supported)**. حدد مجلدًا على الجهاز العميل. سوف يضيف Kaspersky Security Center الملفات القابلة للتنفيذ من هذا المجلد إلى الفئة المخصصة.

- **Select certificate from repository**. 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 fingerprint** في خصائصها.

يمكنك اختيار مخزن الشهادات. وبشكل افتراضي، يطبق التحكم في التطبيقات القواعد فقط على التطبيقات الموقعة بشهادة من مخزن شهادات النظام الموثوق. يتم تمكين هذا بواسطة خانة الاختيار **استخدم التحقق الصارم من التوقيع الرقمي**.

- **Drive type**. 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 **Add**، حدد شروط استثناء التطبيقات من الفئة:

- **From the list of executable files**. إضافة تطبيقات من قائمة الملفات القابلة للتنفيذ على الجهاز العميل إلى الفئة المخصصة.

- **From file properties**. حدد البيانات التفصيلية للملفات التنفيذية كشرط لإضافة التطبيقات إلى الفئة المخصصة.

- **Metadata from files in folder**. 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.

- **Checksums of the files in the folder**. 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.

- **Certificates for the files from the folder**. 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.

- **MSI installer files metadata**. 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.

- **Checksums of the files from the MSI installer of the application**. حدد حزمة MSI. سوف يشير Kaspersky Security Center إلى تجزئات الملفات القابلة للتنفيذ المجمعة في حزمة MSI هذه كشرط لإضافة التطبيقات إلى الفئة المخصصة.

- **From KL category**. حدد فئة KL كشرط لإضافة التطبيقات إلى الفئة المخصصة. تعتبر فئة KL عبارة عن قائمة تضم التطبيقات التي تشترك في سمات موضوعية موحدة. وتتم إدارة هذه القائمة بواسطة خبراء Kaspersky. على سبيل المثال، تتضمن فئة KL المعروفة باسم Office Applications التطبيقات من مجموعة Microsoft Office وAdobe Acrobat وغيرها.

  يمكنك تحديد كل فئات KL لتوليد قائمة موسعة بالتطبيقات الموثوقة.

- **Specify path to application (masks supported)**. حدد مجلدًا على الجهاز العميل. سوف يضيف Kaspersky Security Center الملفات القابلة للتنفيذ من هذا المجلد إلى الفئة المخصصة.

- **Select certificate from repository**. حدد الشهادات التي تم استخدامها لتوقيع الملفات القابلة للتنفيذ باعتبارها شرط لإضافة تطبيقات إلى الفئة المخصصة.

- **Drive type**. 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 **Add** 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 **Executable files** 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:

  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.

  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- خانة الاختيار **Synchronize data with Administration Server repository**. 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 **Executable files**.

  إذا تم مسح خانة الاختيار **Synchronize data with Administration Server repository**، فإن Kaspersky Security Center لن يقوم بإجراء أي تعديلات لفئة التطبيق بعد إنشائها.

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 **Include dynamic-link libraries (DLL) in this category**. 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 **Include script data in this category**. 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:
  - **Calculate SHA256 for files in this category (supported by Kaspersky Endpoint Security 10 Service Pack 2 for Windows and later versions)**.
  - **Calculate MD5 for files in this category (supported by versions earlier than Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**.

- خانة الاختيار **Force folder scan for changes**. 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 **Force folder scan for changes**، 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 **Scan interval (1–168 hours)**. 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 الحقل في حالة تحديد خانة الاختيار **Force folder scan for changes**.

الخطوة 7. إنشاء فئة مخصصة

قم بإنهاء 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 **التطبيقات الممنوعة** 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: **رمز تجزئة 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 تشترك في سمات موضوعية موحدة. وتتم إدارة هذه القائمة بواسطة خبراء Kaspersky. على سبيل المثال، تتضمن فئة KL المعروفة باسم "تطبيقات Office" التطبيقات من مجموعة Microsoft Office و®®Adobe Acrobat وغيرها.
- **شرط مخصص**. يمكنك تحديد ملف التطبيق وتحديد أحد شروط تشغيل القاعدة: **رمز تجزئة 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: **رمز تجزئة 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:

- يدعم Kaspersky Endpoint Security حرفي * و ? لإدخال قناع في البيانات الوصفية: **اسم الملف** و**اسم التطبيق** و**البائع**.
- 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**موضوع الشهادة** 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 **Executable files**، 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 Executable files إلى فئة التطبيق:

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة تحكم الإدارة، حدد المجلد **Executable files** ← **Application management** ← **Advanced**.

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:
  - **Add to a new application category**. اختر هذا الخيار إذا كنت تريد إنشاء فئة تطبيق جديدة، وأضف الملفات القابلة للتنفيذ إليه.
  - **Add to an existing application category**. اختر هذا الخيار إذا كنت تريد تحديد فئة تطبيق موجودة وإضافة الملفات القابلة للتنفيذ إليها.
- في القسم **نوع القاعدة**، حدد أحد الخيارات التالية:
  - **Rules for adding to inclusions**. حدد هذا الخيار إذا كنت تريد إنشاء شرط يضيف الملفات القابلة للتنفيذ إلى فئة التطبيق.
  - **Rules for adding to exclusions**. حدد هذا الخيار إذا كنت تريد إنشاء شرط يستثني الملفات القابلة للتنفيذ إلى فئة التطبيق.
- في القسم **المعلمة المستخدمة كشرط**، حدد أحد الخيارات التالية:
  - **Certificate details (or SHA256 hashes for files without a certificate)**.
  - **Certificate details (files without a certificate will be skipped)**.
  - **Only SHA256 (files without a hash will be skipped)**.
  - **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**.

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 **Administration Server** 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في التطبيقات**.
في الجزء الأيسر من النافذة، يتم عرض إعدادات مكون التحكم في التطبيقات.

4. انقر على **إضافة**.
تفتح النافذة **قاعدة التحكم في التطبيقات**.

5. 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 الفئة الجديد.

  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.

6. في الجدول **المستخدمون وحقوقهم**، انقر فوق الزر **إضافة**.

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

7. في الجدول **المستخدمون 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 **منع** في الصفوف ذات الصلة.

8. حدد خانة الاختيار **رفض للمستخدمين الآخرين** إذا كنت تريد منع جميع المستخدمين الذين لا يظهرون في العمود **المستخدم أو المجموعة** والذين ليسوا جزءًا من مجموعة المستخدمين المحددة في العمود **المستخدم أو المجموعة** من بدء التطبيقات التي تنتمي للفئة المحددة.

9. 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.

10. 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 **التطبيقات الممنوعة** 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. في الجدول **المستخدمون وحقوقهم**، انقر فوق الزر **إضافة**.

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.

تُطبق القاعدة على كل المستخدمين افتراضيًا.

إذا لم يتم تحديد مستخدم في الجدول، فلا يمكن حفظ القاعدة.

d. في الجدول **المستخدمون 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 **المستخدمون وحقوقهم** وليسوا أعضاء في مجموعات المستخدمين المدرجة في الجدول **المستخدمون 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 **المستخدمون وحقوقهم** والذين لا ينتمون إلى مجموعات المستخدمين المحددة في الجدول **المستخدمون 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في التطبيقات**.

في الجزء الأيسر من النافذة، يتم عرض إعدادات مكون التحكم في التطبيقات.

4. 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.

5. احفظ تغييراتك.

لتغيير حالة قاعدة تحكم في التطبيقات 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 **التطبيقات الممنوعة** 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.
- **وضع 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان ← التحكم في التطبيقات**.

4. 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.

5. 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.

6. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد التحكم في التطبيق في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Security Controls** ← **App Control**.

5. تحت **Operating mode**، حدد قائمة قواعد: قائمة الرفض أو قائمة السماح الخاصة بالتطبيق.

6. لتصدير قائمة القواعد:

a. حدد القواعد التي تريد تصديرها.

b. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف JSON في مجلد التنزيلات الافتراضي.

7. لاستيراد قائمة القواعد:

a. انقر على الزر ← **Import**.

في النافذة التي تفتح، حدد ملف JSON 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 JSON.

8. 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 **Administration Server** 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 **Administration Server** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **Reports**.
3. انقر فوق **New report template**.
   بدء تشغيل معالج قالب تقرير جديد.
4. اتبع تعليمات معالج قالب التقرير. في الخطوة **Selecting the report template type**، حدد **Other ← Report on prohibited applications**.
   بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول في علامة التبويب **Reports**.
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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في التطبيقات**.
   في الجزء الأيسر من النافذة، يتم عرض إعدادات مكون التحكم في التطبيقات.
4. 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 تطبيق، 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 تطبيق، إلا في الحالات التي تفي بشروط قواعد السماح بالتحكم في التطبيقات.
5. 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**.
6. احفظ تغييراتك.

لتمكين اختبار قواعد التحكم في التطبيقات أو لتحديد إجراء منع للتحكم في التطبيقات:

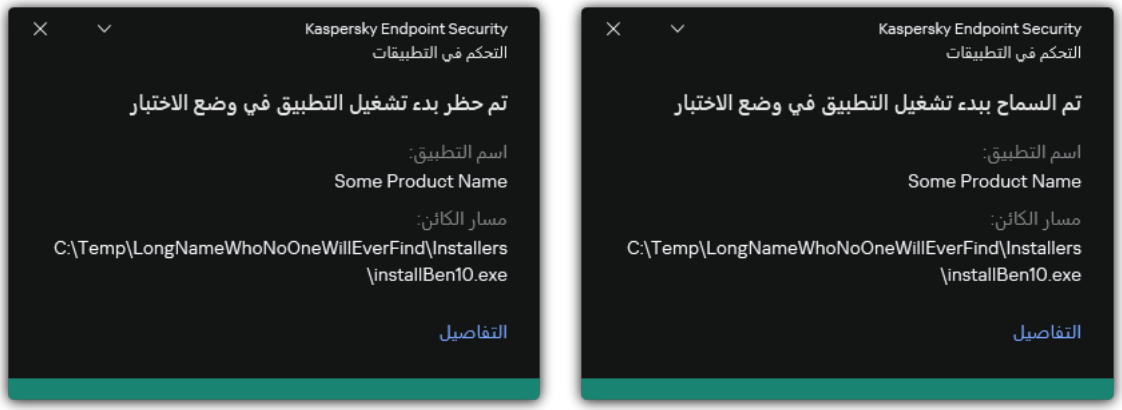
1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **التحكم في التطبيقات**.
3. انقر فوق الزر **التطبيقات الممنوعة** أو **التطبيقات المسموح بها**.
   يفتح هذا قائمة قواعد التحكم في التطبيقات.

4. في العمود **الحالة**، حدد **وضع 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 **Administration Server** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **Reports**.

3. انقر فوق **New report template**.

بدء تشغيل معالج قالب تقرير جديد.

4. اتبع تعليمات معالج قالب التقرير. في الخطوة **Selecting the report template type**، حدد **Other** ← **تقرير عن التطبيقات الممنوعة في وضع الاختبار**.

بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول في علامة التبويب **Reports**.

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 **Administration Server** 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

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.

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 مستخدم، فيمكنك تقييد وصول المستخدم إلى أداة مراقبة نشاط التطبيق.

كيفية إخفاء مراقبة نشاط التطبيق في واجهة التطبيق باستخدام وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

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

4. استخدم خانة الاختيار **إخفاء قسم مراقبة نشاط التطبيقات** لمنح حق الوصول إلى الأداة أو إبطاله.

5. احفظ تغييراتك.

كيفية إخفاء مراقبة نشاط التطبيقات في واجهة التطبيق باستخدام Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **General Settings** ← **User Interaction**.

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. يوفر خبراء Kaspersky قالبًا لرسالة إلى المستخدم تصف أسباب حظر التطبيق (انظر الشكل أدناه). يتم توفير متغيرات خاصة لإدارة قوالب الرسائل (على سبيل المثال، %USER_NAME%). وتسمح المتغيرات باستخدام قالب رسالة واحدة لأجهزة الكمبيوتر المختلفة. وعند إنشاء رسالة، يسترجع Kaspersky Endpoint Security قيمة المتغير من إعدادات نظام التشغيل ويدرجها في الرسالة التي تتطابق مع الكمبيوتر والمستخدم والحدث المحدد.



إشعار التحكم في التطبيقات

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. ولفعل ذلك، يجب على المستخدم النقر فوق الزر **طلب الوصول** وإرسال رسالة إلى المسؤول تصف الموقف. ويمكنك أيضًا إعداد قالب الرسالة للمسؤول، مع إضافة بيانات قد تفيد في قرارك بالسماح بالوصول إلى التطبيق أو منعه. 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 **User requests**. 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.

كيفية تحرير رسالة التحكم في التطبيقات في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **التحكم في التطبيقات**.
4. في القسم **إعدادات قوالب الرسائل**، انقر على الزر **القوالب**.
5. يفتح هذا نافذة؛ وفي تلك النافذة، كوّن قوالب 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.

  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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **المتغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.

يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **افتراضيًا**.

6. احفظ تغييراتك.

كيفية تغيير قالب رسالة التحكم في التطبيقات في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Security Controls** ← **App Control**.

5. في القسم **Message templates**، انقر فوق الرابط **Messages about application startup block** وكوّن القوالب لرسائل التحكم في التطبيقات:

- **Message to user**. قالب الرسالة التي يتم عرضها عندما يتم بدء تشغيل قاعدة التحكم في التطبيق التي تمنع بدء تشغيل تطبيق ما.
لا يمكنك تكوين قوالب الرسائل للتحكم في التطبيقات في وضع الاختبار. ويعرض التحكم في التطبيقات في وضع الاختبار إخطارات محددة مسبقًا.
- **Message to administrator**. قالب الرسالة التي يمكن للمستخدم إرسالها إلى مسؤول الشبكة المحلية للشركة إذا كان المستخدم يعتقد أنه قد تم حظر التطبيق عن طريق الخطأ.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **Add variable** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.
يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **Reset to default**.

6. احفظ تغييراتك.

كيفية تحرير قالب رسالة التحكم في التطبيقات في واجهة التطبيق

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.
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.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **إضافة متغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.
يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **إعادة تعيين**.

4. احفظ تغييراتك.

المتغيرات في قوالب رسائل التحكم في التطبيقات

يمكنك استخدام المتغيرات التالية في قوالب رسائل المستخدم أو قوالب رسائل المسؤول:

- **اسم القاعدة التي تم تشغيلها** – %RULE%.

  اسم القاعدة التي منعت تنفيذ ملف.

- **التاريخ الحالي** – %DATE%.

  التاريخ الذي تم فيه منع تنفيذ الملف بتنسيق DD.MM.YYYY.

- **الوقت الحالي** – %TIME%.

  الوقت الذي تم فيه حظر تنفيذ الملف بتنسيق HH: MM.

- **اسم المستخدم** – %USER_NAME%.

  اسم حساب المستخدم الحالي على الكمبيوتر الذي تم حظر تنفيذ الملف عليه، بتنسيق `<device name>\<user alias>` (على سبيل المثال، `DESKTOP-123\John.Smith`).

- **اسم الكمبيوتر** – %COMPUTER_NAME%.

  اسم الكمبيوتر الذي تم منع تنفيذ الملف عليه.

- **اسم الملف القابل للتنفيذ** – %FILE_NAME%.

  اسم الملف القابل للتنفيذ للتطبيق الممنوع.

- **فئة KL الخاصة بالملف القابل للتنفيذ** – %KL_CAT%.

  فئة KL التي ينتمي إليها التطبيق الممنوع (على سبيل المثال، المستعرضات أو فئة أخرى).

- **المسار المؤدي للملف القابل للتنفيذ** – %FILE_PATH%.

  المسار الكامل للملف القابل للتنفيذ للتطبيق الممنوع.

- **إصدار الملف القابل للتنفيذ** – %FILE_VERSION%.

  إصدار الملف القابل للتنفيذ للتطبيق الممنوع.

- **الاسم الأصلي للملف القابل للتنفيذ** – %ORIGINAL_FILE_NAME%.

  الاسم الأصلي للملف القابل للتنفيذ للتطبيق الممنوع. يتم تحديد اسم الملف في خصائص الملف القابل للتنفيذ الخاص بالتطبيق.

- **البائع** – %FILE_PUBLISHER%.

  بائع التطبيق الممنوع.

- **اسم التطبيق** – %FILE_PRODUCT_NAME%.

  اسم التطبيق الممنوع.

- **إصدار التطبيق** – %PRODUCT_VERSION%.

  إصدار التطبيق الممنوع.

- **تجزئة الملف القابل للتنفيذ** – %FILE_HASH%.

  تجزئة الملف القابل للتنفيذ للتطبيق الممنوع.

- **جهة إصدار الشهادة** – %CERT_ISSUER%.

  جهة إصدار الشهادة التي تم توقيع الملف القابل للتنفيذ بها.

- **موضوع الشهادة** – %CERT_SUBJECT%.

  موضوع الشهادة التي تم توقيع الملف القابل للتنفيذ بها.

- **بصمة الشهادة** – %CERT_THUMBPRINT%.

  بصمة الشهادة التي تم توقيع الملف القابل للتنفيذ بها.

أفضل الممارسات لإجراء جرد للملفات القابلة للتنفيذ

تحصل مهمة Inventory على معلومات عن الملفات القابلة للتنفيذ (على سبيل المثال، EXE وBAT وCMD) ووحدات DLL والبرامج النصية (PowerShell وJS وغيرها). وهذه المعلومات مطلوبة لتكوين فئات التحكم في التطبيقات و أذونات التطبيق لمكون منع اختراق المضيف. ويجب تشغيل مهمة Inventory بشكل دوري للحفاظ على تحديث المعلومات. وتعتبر مهمة Inventory، تمامًا مثل مهمة Malware Scan، كثيفة الاستخدام للموارد. لذلك، نوصي بتكوين المهمة لتعمل أثناء الليل أو في عطلات نهاية الأسبوع.

خطوات جرد الملفات القابلة للتنفيذ

1. حدد مجموعة أجهزة الكمبيوتر المرجعية التي تم تثبيت مجموعة البرامج النموذجية عليها. ونوصي بالحفاظ على عدد أجهزة الكمبيوتر عند حد أدنى لإجراء جرد الملفات القابلة للتنفيذ. وكلما كانت مهام Inventory أقل، انخفض الحمل على خادم إدارة Kaspersky Security Center .

2. انقل أجهزة الكمبيوتر المرجعية إلى مجموعة إدارة منفصلة في وحدة تحكم Kaspersky Security Center. ويمكنك تسمية المجموعة، على سبيل المثال، أجهزة الكمبيوتر المرجعية.

3. أنشئ مهمة Inventory لمجموعة إدارة أجهزة الكمبيوتر المرجعية. ونوصي بالاحتفاظ بإعدادات المهمة الافتراضية.

مثال على جرد ملف قابل للتنفيذ في مؤسسة

على سبيل المثال، تمتلك مؤسستك 100 جهاز كمبيوتر تعمل بنظام التشغيل Windows 11 25H2. وتحتوي جميع أجهزة الكمبيوتر على إصدار نظام التشغيل نفسه والترجمة نفسها. كما أن مجموعة التحديثات المثبتة على أجهزة الكمبيوتر متطابقة أيضًا.

وفي هذه المؤسسة، لا تحتاج إلى تشغيل مهمة Inventory على جميع أجهزة الكمبيوتر. وتكون معظم الملفات القابلة للتنفيذ على أجهزة الكمبيوتر هذه متطابقة. ويكفي إنشاء مهمة لجهاز كمبيوتر مرجعي واحد. ويمكنك إنشاء مهام Inventory لأجهزة الكمبيوتر التي يختلف تكوينها عن التكوين المرجعي.

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 **Application folder** غير آمن لأن أي تطبيق من المجلد المحدد سيتم السماح ببدء تشغيله. ويوصى بتطبيق القواعد التي تستخدم فئات التطبيق مع حالة **Application folder** 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 **Executable files**.

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 باسم صورة ذهبية برامج تضمن التشغيل العادي لنظام التشغيل. تتضمن فئة KL باسم 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 **Subject** 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 أنشئ فئة التطبيق من خلال الشرط **Application folder** وحدد المسار المؤدي إلى ذلك المجلد. ثم قم بإنشاء قاعدة سماح وحدد هذه الفئة.

> قد يكون استخدام **Application folder** غير آمن لأن أي تطبيق من المجلد المحدد سيتم السماح ببدء تشغيله. ويوصى بتطبيق القواعد التي تستخدم فئات التطبيق مع حالة **Application folder** 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 Web Control والحماية من تهديدات البريد والحماية من تهديدات الويب واكتشاف السلوك ومنع الاستغلال 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.

للمساعدة في ضمان أمان الكمبيوتر، يراقب مكونا اكتشاف السلوك ومنع الاستغلال أيضًا تدفقات البيانات التي تمر عبر منافذ الشبكة. ويراقب هذان المكونان باستمرار حركة الشبكة للعمليات الفردية التي قد تكون مسببة للتهديدات.

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. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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.

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات الشبكة**.

4. في القسم **المنافذ قيد المراقبة**، حدد **مراقبة منافذ الشبكة المحددة فقط**.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

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 ما، ينشئ التطبيق حدثًا بحالة Critical (انظر الشكل أدناه).

إذا كنت ترغب في استخدام فحص السجل، تأكد من تكوين إعدادات 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **ضوابط الأمان ← فحص السجل**.

4. تأكد من تحديد خانة الاختيار **فحص السجل**.

5. في القسم **القواعد المحددة مسبقًا**، انقر على الزر **الإعدادات**.

6. حدد خانات الاختيار أو امسحها لتكوين القواعد المحددة مسبقًا:

- **توجد أنماط لهجوم محتمل باستخدام تخمين كلمة المرور 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**.

7. إذا لزم الأمر، قم بتكوين القاعدة **توجد أنماط لهجوم محتمل باستخدام تخمين كلمة المرور 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**.

8. 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).

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال. لا يراقب Kaspersky Endpoint Security محاولات تسجيل الدخول لهؤلاء المستخدمين وأجهزة الكمبيوتر.

d. انقر فوق **موافق**.

9. احفظ تغييراتك.

كيفية تكوين القواعد المحددة مسبقًا في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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 ENABLED** 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).

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال. 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 تخمين كلمة المرور 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 تخمين كلمة المرور 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).

يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال. 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 حدث حرج.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **فحص السجل**.
4. تأكد من تحديد خانة الاختيار **فحص السجل**.
5. في القسم **قواعد مخصصة**، انقر على الزر **الإعدادات**.
6. في النافذة التي تفتح، حدد خانات الاختيار بجوار القواعد المخصصة التي تريد تمكينها.
7. إذا لزم الأمر، انقر فوق **إضافة** لإنشاء القواعد المخصصة الخاصة بك.
8. 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.
9. احفظ تغييراتك.

كيفية إضافة قاعدة مخصصة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
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 ENABLED** 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**.
   - **Custom log name**. سجلات أحداث Windows. تتاح السجلات التالية: Application أو Security أو System.
   - **Origin**. 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).
   - **Event Identifiers**. 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 حدثًا حرجًا.

مراقبة سلامة النظام

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.

بدءًا من الإصدار 12.6، يتضمن Kaspersky Endpoint Security for Windows مكون مراقبة سلامة النظام بدلاً من مكون مراقبة سلامة الملفات. يتضمن مكون مراقبة سلامة النظام كل وظائف مراقبة سلامة الملفات ويسمح بالإضافة إلى ذلك بمراقبة تغييرات السجل واتصال الأجهزة الخارجية.

يراقب مكون مراقبة سلامة النظام التغييرات في نظام التشغيل التي قد تشير إلى خروقات أمان الكمبيوتر. وعند اكتشاف هذه التغييرات، ينشئ Kaspersky Endpoint Security الأحداث المقابلة وينبه المسؤول. يمكن أن تعمل مراقبة سلامة النظام في وضع الوقت الحقيقي ويمكنها أيضًا إجراء التحقق من سلامة النظام عند الطلب.

مراقبة سلامة النظام في الوقت الحقيقي

في وضع الوقت الحقيقي، يتبع مكون مراقبة سلامة النظام التغييرات في الكائنات التي قمت بتضمينها في نطاق المكون (نطاق المراقبة). وتسمح مراقبة سلامة النظام أيضًا بمنع الوصول غير المصرح به إلى هذه الكائنات في الوقت الحقيقي.

التحقق من سلامة النظام عند الحاجة

يعد التحقق من سلامة النظام عند الحاجة مهمة يمكنك تشغيلها يدويًا أو وفقًا لجدول زمني. ولتشغيل مهمة التحقق من سلامة النظام، يجب عليك تكوين نطاق المكون (نطاق المراقبة) وإنشاء خط أساس. ويعد خط الأساس بمثابة حالة مسجلة للكائنات في النظام، التي يستخدمها التطبيق كمرجع عند مقارنتها بالحالة الحالية.

ترحيل إعدادات مراقبة سلامة الملفات

عند تحديث Kaspersky Endpoint Security إلى الإصدار 12.6، يتم ترحيل إعدادات مراقبة سلامة الملفات تلقائيًا. وكجزء من الترحيل، ينقل التطبيق قواعد المراقبة إلى مراقبة سلامة النظام. ويتم أيضًا ترحيل قواعد مراقبة سلامة الملفات إلى مراقبة سلامة النظام عند الترحيل من KSWS إلى KES.

لضمان التشغيل الصحيح لنظام مراقبة سلامة النظام، يجب تحديث تطبيق Kaspersky Endpoint Security والمكوّن الإضافي للإدارة إلى الإصدار 12.6. إذا كان لديك إصدار سابق مُثبت من المكون الإضافي للإدارة، فلن تتمكن من تكوين مراقبة سلامة النظام لأن المكون الإضافي للإدارة يفتقر إلى قسم **مراقبة سلامة النظام**.

حول قواعد مراقبة سلامة النظام

لكي تعمل مراقبة سلامة النظام، يجب إضافة قاعدة واحدة على الأقل. وقاعدة مراقبة سلامة النظام هي مجموعة من المعايير التي تحدد وصول المستخدمين إلى الملفات والتسجيل. تكتشف مراقبة سلامة النظام التغييرات في الملفات والسجل ضمن نطاق المراقبة المحدد. ويعد نطاق المراقبة أحد معايير قاعدة مراقبة سلامة النظام.

تسمح مراقبة سلامة النظام بمراقبة الكائنات التالية:

- الملفات
- السجل
- الأجهزة الخارجية

الاعتبارات الخاصة التي تتضمنها مراقبة الملفات

يراقب مكون مراقبة سلامة النظام التغييرات في الملفات والمجلدات بالإضافة إلى الملفات التي تتم إضافتها إلى نطاق المراقبة أو إزالتها منه. وقد تشير هذه التغييرات إلى حدوث خرق لأمان الكمبيوتر. ونوصي بإضافة الكائنات التي نادرًا ما يتم تعديلها أو الكائنات التي يمتلك المسؤول فقط حق الوصول إليها. ويساعد هذا في تقليل عدد أحداث مراقبة سلامة النظام.

لا يراقب مكون مراقبة سلامة النظام التغييرات التي يتم إجراؤها على الملفات في مجلدات الخادم المشتركة. ولا يمكن استخدام مراقبة سلامة النظام إلا محليًا.

يراقب Kaspersky Endpoint Security تغييرات الملفات والمجلدات فقط على تلك الأقراص التي يتم توصيلها عند بدء تشغيل مراقبة سلامة النظام في الوقت الحقيقي. وإذا لم يكن القرص متصلاً عند بدء تشغيل "مراقبة سلامة النظام في الوقت الحقيقي"، فلن يراقب التطبيق تغييرات الملفات والمجلدات الموجودة على هذا القرص حتى إذا تمت إضافة الملفات والمجلدات إلى نطاق المراقبة.

الاعتبارات الخاصة التي تتضمنها مراقبة السجل

تراقب مراقبة سلامة النظام السجل. وقد تشير هذه التغييرات إلى حدوث خرق لأمان الكمبيوتر.

تراقب مراقبة سلامة النظام مفاتيح الجذر التالية للسجل:

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE

- HKEY_USERS
- HKEY_CURRENT_CONFIG (متاح فقط في مراقبة سلامة النظام في الوقت الحقيقي)
- HKEY_CURRENT_USER (متاح فقط في مراقبة سلامة النظام في الوقت الحقيقي)

لا تدعم المهمة التحقق من سلامة النظام مفتاح HKEY_CURRENT_USER. يمكنك تحديد مفتاح ضمن HKEY_USERS مثل HKEY_USERS\<user profile ID>\<key>.

الاعتبارات الخاصة التي تتضمنها مراقبة الجهاز الخارجي

تراقب مراقبة سلامة النظام اتصال وفصل الأجهزة الخارجية. ويعد ذلك ضروريًا لحماية الكمبيوتر من التهديدات الأمنية التي قد تنتج عن تبادل الملفات مع هذه الأجهزة. ولا تراقب مراقبة سلامة النظام الوصول إلى الأجهزة الخارجية ولا تمنع تبادل الملفات. ويمكنك تكوين الوصول إلى الأجهزة باستخدام مكون تطبيق مختلف هو التحكم في الجهاز.

عند تشغيل مهمة مراقبة سلامة النظام الأساسي، يتجاهل التطبيق إعادة توصيل الأجهزة الخارجية إذا كان للأجهزة حرف محرك الأقراص نفسه في نظام التشغيل. ولكي يتم تسجيل الدخول، يجب أن تحتوي الأجهزة المعاد توصيلها على أحرف محركات أقراص مختلفة.

تراقب مراقبة سلامة النظام اتصال الأنواع التالية من الأجهزة الخارجية:

- محرك الأقراص القابل للإزالة (بما في ذلك محركات أقراص USB المحمولة)
- محرك الأقراص الثابت
- محول شبكة خارجية
- محرك أقراص CD/DVD/Blu-ray
- ماسح ضوئي / كاميرا

مراقبة سلامة النظام في الوقت الحقيقي

تسمح مراقبة سلامة النظام بتتبع التغييرات في نظام التشغيل في الوقت الحقيقي. ويمكنك تتبع التغييرات التي قد تشير إلى خروقات الأمان على الكمبيوتر. ويسمح المكون بمنع هذه التغييرات أو مجرد تسجيل أحداث التغيير.

لكي تعمل مراقبة سلامة النظام، يجب إضافة قاعدة واحدة على الأقل. وقاعدة مراقبة سلامة النظام هي مجموعة من المعايير التي تحدد وصول المستخدمين إلى الملفات والتسجيل. تكتشف مراقبة سلامة النظام التغييرات في الملفات والسجل ضمن نطاق المراقبة المحدد. ويعد نطاق المراقبة أحد معايير قاعدة مراقبة سلامة النظام.

أوضاع مراقبة سلامة النظام في الوقت الحقيقي

وللتأكد من أن قواعد مراقبة سلامة النظام لا تمنع أي إجراءات مع موارد ضرورية لعمل نظام التشغيل أو الخدمات الأخرى، نوصي بتمكين وضع الاختبار وتحليل كيفية تأثير المكون على النظام. ومع تشغيل وضع الاختبار، لا يمنع Kaspersky Endpoint Security نشاط المستخدم المحظور بموجب القواعد، وبدلاً من ذلك ينشئ أحداث تحذير ⚠.

يتكون مكون مراقبة سلامة النظام في الوقت الحقيقي من وضعين:

- منع

وفي هذا الوضع، تتبع مراقبة سلامة النظام التغييرات في النظام وتنفذ إجراءً وفقًا للقاعدتين: **سماح** أو **منع**. وتنشئ مراقبة سلامة النظام أيضًا حدثًا مطابقًا وتغير حالة الجهاز في وحدة تحكم Kaspersky Security Center.

- إعلام

في هذا الوضع، تسمح مراقبة سلامة النظام باتخاذ إجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة. وفي حالة منع الإجراء مع الملفات أو السجل، سينشئ التطبيق حدثًا: تم السماح بالعملية الممنوعة في وضع الاختبار. ولتحليل كيفية تأثير القواعد على النظام، يمكنك إلقاء نظرة على التقارير.

تمكين مراقبة سلامة النظام في الوقت الحقيقي

كيفية تمكين مراقبة سلامة النظام في الوقت الحقيقي في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **ضوابط الأمان** ← **مراقبة سلامة النظام**.
4. حدد خانة الاختيار **مراقبة سلامة النظام**.
5. تحت **وضع التشغيل لقواعد الحظر**، حدد وضعًا لمراقبة سلامة النظام في الوقت الحقيقي:
   - **منع**. وفي هذا الوضع، تمنع مراقبة سلامة النظام الإجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا.
   - **إعلام**. وفي هذا الوضع، تسمح مراقبة سلامة النظام باتخاذ إجراءات مع الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا.
6. في القسم **مراقبة سلامة النظام في الوقت الحقيقي**، حدد خانة الاختيار **مراقبة سلامة النظام في الوقت الحقيقي**.
7. تكوين مراقبة الجهاز الخارجي:
   a. حدد خانة الاختيار **مراقبة الأجهزة**.
   b. في القائمة المنسدلة **مستوى خطورة الحدث**، حدد مستوى أهمية أحداث مراقبة الجهاز الخارجي: معلوماتي وتحذير وحرج.

تسجل مراقبة سلامة النظام الاتصال الحالي للأجهزة الخارجية. ويبدأ التطبيق في مراقبة اتصال الأجهزة الخارجية وفصلها بعد تمكين المكون في إعدادات التطبيق. وبالتالي، عند توصيل جهاز خارجي أو فصله، ينشئ التطبيق حدثًا مطابقًا.

8. تكوين مراقبة الملفات والسجل:
   a. حدد خانة الاختيار **مراقبة الملفات والسجل**.
   b. انقر على **الإعدادات**.

يؤدي ذلك إلى فتح قائمة قواعد مراقبة سلامة النظام.

c. انقر على **إضافة**.

يمكنك أيضًا استيراد القواعد من مصدر آخر.

d. قم بتكوين قاعدة مراقبة سلامة النظام (انظر الجدول أدناه).

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين مراقبة سلامة النظام في الوقت الحقيقي في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Security Controls** ← **System Integrity Monitoring**.

5. قم بتشغيل مفتاح **System Integrity Monitoring ENABLED**.

6. حدد علامة التبويب **Windows**.

7. تحت **Real-Time System Integrity Monitoring**، حدد وضعًا لمراقبة سلامة النظام في الوقت الحقيقي:

- **Apply rules**. وفي هذا الوضع، تمنع مراقبة سلامة النظام الإجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا.
- **Test rules (Inform)**. وفي هذا الوضع، تسمح مراقبة سلامة النظام باتخاذ إجراءات مع الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا.

8. تكوين مراقبة الملفات والسجل:

a. حدد خانة الاختيار **Monitor files and the registry**.

b. انقر على **Rules**.

يؤدي ذلك إلى فتح قائمة قواعد مراقبة سلامة النظام.

c. انقر على **Add**.

يمكنك أيضًا استيراد القواعد من مصدر آخر.

d. قم بتكوين قاعدة مراقبة سلامة النظام (انظر الجدول أدناه).

9. تكوين مراقبة الجهاز الخارجي:

a. حدد خانة الاختيار **Monitor devices**.

b. في القائمة المنسدلة **Event severity level**، حدد مستوى أهمية أحداث مراقبة الجهاز الخارجي: Informational وWarning وCritical.

تسجل مراقبة سلامة النظام الاتصال الحالي للأجهزة الخارجية. ويبدأ التطبيق في مراقبة اتصال الأجهزة الخارجية وفصلها بعد تمكين المكون في إعدادات التطبيق. وبالتالي، عند توصيل جهاز خارجي أو فصله، ينشئ التطبيق حدثًا مطابقًا.

10. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين مراقبة سلامة النظام في الوقت الحقيقي في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة سلامة النظام**.
3. قم بتشغيل مفتاح التبديل **مراقبة سلامة النظام**.
4. تحت **وضع التشغيل لقواعد الحظر**، حدد وضعًا لمراقبة سلامة النظام في الوقت الحقيقي:
   - **منع**. وفي هذا الوضع، تمنع مراقبة سلامة النظام الإجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا.
   - **إعلام**. وفي هذا الوضع، تسمح مراقبة سلامة النظام باتخاذ إجراءات مع الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا.
5. في القسم **مراقبة سلامة النظام في الوقت الحقيقي**، حدد خانة الاختيار **مراقبة سلامة النظام في الوقت الحقيقي**.
6. تكوين مراقبة الجهاز الخارجي:
   a. حدد خانة الاختيار **مراقبة الأجهزة**.
   b. في القائمة المنسدلة **مستوى خطورة الحدث**، حدد مستوى أهمية أحداث مراقبة الجهاز الخارجي: معلوماتي ⓘ وتحذير ⚠ وحرج ⓘ.

   تسجل مراقبة سلامة النظام الاتصال الحالي للأجهزة الخارجية. ويبدأ التطبيق في مراقبة اتصال الأجهزة الخارجية وفصلها بعد تمكين المكون في إعدادات التطبيق. وبالتالي، عند توصيل جهاز خارجي أو فصله، ينشئ التطبيق حدثًا مطابقًا.
7. تكوين مراقبة الملفات والسجل:
   a. حدد خانة الاختيار **مراقبة الملفات والسجل**.
   b. انقر على **إعداد**.

   يؤدي ذلك إلى فتح قائمة قواعد مراقبة سلامة النظام.
   c. انقر على **إضافة**.

   يمكنك أيضًا استيراد القواعد من مصدر آخر.
8. قم بتكوين قاعدة مراقبة سلامة النظام (انظر الجدول أدناه).
9. احفظ تغييراتك.

إعدادات قاعدة مراقبة سلامة النظام في الوقت الحقيقي

المعلمة	الوصف
اسم القاعدة	اسم قاعدة مراقبة سلامة النظام في الوقت الحقيقي
العمليات مع الملفات والتسجيل	• **سماح**. تسمح مراقبة سلامة النظام باتخاذ إجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة. • **منع**. يعتمد سلوك مراقبة سلامة النظام على الوضع المحدد. إذا حددت وضع حماية النظام، تمنع مراقبة سلامة النظام الإجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا، وتُغير حالة الجهاز في وحدة تحكم Kaspersky Security Center. وإذا حددت وضع الاختبار، تسمح مراقبة سلامة النظام باتخاذ إجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة.

المعلمة	الوصف
مستوى خطورة الحدث	يسجل Kaspersky Endpoint Security أحداث تعديل الملف كلما تم تعديل ملف أو مفتاح سجل في نطاق المراقبة. وتتوفر مستويات خطورة الحدث التالية: معلوماتي وتحذير وحرج.
نطاق المراقبة	• **الملف**. قائمة الملفات والمجلدات التي يراقبها المكون. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع. 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. • **التسجيل**. قائمة مفاتيح السجل والقيم التي يراقبها المكون. يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع.
الاستثناءات	• **الملف**. 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. 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. • **التسجيل**. قائمة الاستثناءات من نطاق المراقبة. يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع. وتتمتع إدخالات الاستثناء بأولوية أعلى من إدخالات نطاق المراقبة.
المستخدمون و/أو مجموعات المستخدمين الموثوقة	المستخدم الموثوق هو مستخدم يُسمح له بتنفيذ إجراءات باستخدام الملفات ومفاتيح السجل في نطاق المراقبة. وإذا اكتشف Kaspersky Endpoint Security إجراءً تم تنفيذه بواسطة مستخدم موثوق، فإن مراقبة سلامة النظام تنشئ حدث معلوماتي. يمكنك تحديد المستخدمين في Active Directory، أو في قائمة الحسابات في Kaspersky Security Center، أو عن طريق إدخال اسم مستخدم محلي يدويًا. توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال.
علامات عملية الملف / العمليات التي يتم مراقبتها	علامات تميز الإجراء المتخذ مع الملفات أو مفاتيح السجل التي سيراقبها التطبيق.
التجزئة	حساب تجزئة الملف عند التعديل. يضيف Kaspersky Endpoint Security معلومات عن تجزئة الملف عند إنشاء حدث.

التحقق من سلامة النظام عند الحاجة

يعد التحقق من سلامة النظام عند الحاجة مهمة يمكنك تشغيلها يدويًا أو وفقًا لجدول زمني. عند تشغيل مهمة التحقق من سلامة النظام، يقارن التطبيق الحالة الحالية للكائنات المدرجة في نطاق المراقبة مع حالة خط الأساس الخاصة بها. وعلى عكس مراقبة سلامة النظام في الوقت الحقيقي، تساعد مهمة التحقق من سلامة النظام على الحد من عدد الأحداث وتتيح لك إنشاء تقرير عام بالتغييرات في نظام التشغيل.

لكي تعمل مراقبة سلامة النظام، يجب إضافة قاعدة واحدة على الأقل. وقاعدة مراقبة سلامة النظام هي مجموعة من المعايير التي تحدد وصول المستخدمين إلى الملفات والتسجيل. تكتشف مراقبة سلامة النظام التغييرات في الملفات والسجل ضمن نطاق المراقبة المحدد. ويعد نطاق المراقبة أحد معايير قاعدة مراقبة سلامة النظام. يمكنك تكوين القواعد التي ستتم مشاركتها بواسطة مراقبة سلامة النظام في الوقت الحقيقي ومهمة التحقق من سلامة النظام أو إنشاء قواعد منفصلة للمهمة. لإنشاء خط أساس، يطبق Kaspersky Endpoint Security نطاق المراقبة من مهمة التحقق من سلامة النظام إلى مهمة تحديث خط الأساس.

إنشاء وتحديث خط الأساس

تحتاج مهمة التحقق من سلامة النظام إلى خط أساس للعمل. ويعد خط الأساس بمثابة حالة مسجلة للكائنات في النظام، التي يستخدمها التطبيق كمرجع عند مقارنتها بالحالة الحالية. وإذا كانت الحالة الحالية للنظام مختلفة عن حالة النظام كما هو مسجل في خط الأساس، ينشئ Kaspersky Endpoint Security الحدث المطابق. ويمكنك إنشاء أو تحديث خط أساس باستخدام مهمة تحديث خط الأساس.

يمكنك تحديث خط الأساس في الأوضاع التالية:

- تحديث كامل.

  يقوم التطبيق بتحديث كل الكائنات في نطاق المراقبة.

- تحديث تزايدي.

  يقوم التطبيق باكتشاف وتحديث الكائنات المعدلة أو الجديدة فقط.

كيفية إنشاء أو تحديث خط أساس في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.

   تفتح قائمة المهام.

2. انقر فوق **New task**.

   يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **تحديث خط الأساس**.

الخطوة 2. تحديد وضع تحديث خط الأساس

حدد وضع تحديث خط الأساس:

- **تحديث كامل**. يقوم التطبيق بتحديث كل الكائنات في نطاق المراقبة.
- **تحديث تزايدي**. يقوم التطبيق باكتشاف وتحديث الكائنات المعدلة أو الجديدة فقط.

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، على سبيل المثال، Baseline 2024.

الخطوة 5 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية إنشاء أو تحديث خط أساس في Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.
2. انقر على **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.
   b. في القائمة المنسدلة **Task type**، حدد **Baseline update**.
   c. في الحقل **Task name**، أدخل وصفًا مختصرًا، علي سبيل المثال، Baseline 2024.
   d. في القسم **Devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.
5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.
6. قم بإنهاء المعالج.
سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.

نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. حدد وضع تحديث خط الأساس:

- **Full update**. يقوم التطبيق بتحديث كل الكائنات في نطاق المراقبة.
- **Incremental update**. يقوم التطبيق باكتشاف وتحديث الكائنات المعدلة أو الجديدة فقط.

10. احفظ تغييراتك.

11. حدد خانة الاختيار المجاورة للمهمة.

12. انقر فوق **Start**.

تكوين نطاق المراقبة لمهمة التحقق من سلامة النظام

بشكل افتراضي، يكون نطاق المراقبة لمهمة التحقق من سلامة النظام هو نطاق مراقبة سلامة النظام في الوقت الحقيقي نفسه. ويمكنك تكوين نطاق مراقبة مختلف للمهمة.

لا تدعم مراقبة سلامة النظام استيراد مفاتيح HKEY_CURRENT_USER و HKEY_CURRENT_CONFIG لمهمة التحقق من سلامة النظام. وإذا كان نطاق مراقبة المهمة يحتوي على هذه المفاتيح، فسيقوم التطبيق بتكوين حدث يتضمن نطاق المراقبة كائنات غير صحيحة.

كيفية تكوين نطاق مراقبة مختلف لمهمة التحقق من سلامة النظام في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **ضوابط الأمان** ← **مراقبة سلامة النظام**.

4. حدد خانة الاختيار **مراقبة سلامة النظام**.

5. تحت **التحقق من سلامة النظام**، حدد وضع تكوين المهمة: **الإعدادات المخصصة**.

6. تكوين مراقبة الجهاز الخارجي:

a. حدد خانة الاختيار **مراقبة الأجهزة**.

b. في القائمة المنسدلة **مستوى خطورة الحدث**، حدد مستوى أهمية أحداث مراقبة الجهاز الخارجي: معلوماتي وتحذير وحرج.

تسجل مراقبة سلامة النظام معلومات عن الأجهزة الخارجية المتصلة في وقت إنشاء خط الأساس. وبالتالي، عند توصيل جهاز خارجي، ينشئ التطبيق حدثًا مطابقًا. وعند تشغيل مهمة التحقق من سلامة النظام، لا يراقب التطبيق فصل اتصال الأجهزة الخارجية.

7. تكوين مراقبة الملفات والسجل:

a. حدد خانة الاختيار **مراقبة الملفات والسجل**.

b. انقر على **الإعدادات**.

يؤدي ذلك إلى فتح قائمة قواعد مراقبة سلامة النظام.

c. انقر على **إضافة**.

يمكنك أيضًا استيراد القواعد من مصدر آخر.

d. قم بتكوين قاعدة مراقبة سلامة النظام (انظر الجدول أدناه).

8. احفظ تغييراتك.

كيفية تكوين نطاق مراقبة مختلف لمهمة System Integrity Check في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Security Controls** ← **System Integrity Monitoring**.

5. حدد علامة التبويب **Windows**.

6. قم بتشغيل مفتاح **System Integrity Monitoring ENABLED**.

7. تحت **System Integrity Check**، حدد وضع تكوين المهمة: **Custom settings**.

8. تكوين مراقبة الجهاز الخارجي:

a. حدد خانة الاختيار **Monitor devices**.

b. في القائمة المنسدلة **Event severity level**، حدد مستوى أهمية أحداث مراقبة الجهاز الخارجي: Informational وWarning وCritical.

تسجل مراقبة سلامة النظام معلومات عن الأجهزة الخارجية المتصلة في وقت إنشاء خط الأساس. وبالتالي، عند توصيل جهاز خارجي، ينشئ التطبيق حدثًا مطابقًا. وعند تشغيل مهمة التحقق من سلامة النظام، لا يراقب التطبيق فصل اتصال الأجهزة الخارجية.

9. تكوين مراقبة الملفات والسجل:

a. حدد خانة الاختيار **Monitor files and the registry**.

b. انقر على **Rules**.

يؤدي ذلك إلى فتح قائمة قواعد مراقبة سلامة النظام.

c. انقر على **Add**.

يمكنك أيضًا استيراد القواعد من مصدر آخر.

d. قم بتكوين قاعدة مراقبة سلامة النظام (انظر الجدول أدناه).

10. احفظ تغييراتك.

كيفية تكوين نطاق مراقبة مختلف لمهمة التحقق من سلامة النظام في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، اختر **ضوابط الأمان** ← **مراقبة سلامة النظام**.
3. قم بتشغيل مفتاح التبديل **مراقبة سلامة النظام**.
4. تحت **التحقق من سلامة النظام**، حدد وضع تكوين المهمة: **إعدادات مخصصة**.
5. تكوين مراقبة الجهاز الخارجي:
   a. حدد خانة الاختيار **مراقبة الأجهزة**.
   b. في القائمة المنسدلة **مستوى خطورة الحدث**، حدد مستوى أهمية أحداث مراقبة الجهاز الخارجي: معلوماتي ⓘ وتحذير ⚠ وحرج ⓘ.

تسجل مراقبة سلامة النظام معلومات عن الأجهزة الخارجية المتصلة في وقت إنشاء خط الأساس. وبالتالي، عند توصيل جهاز خارجي، ينشئ التطبيق حدثًا مطابقًا. وعند تشغيل مهمة التحقق من سلامة النظام، لا يراقب التطبيق فصل اتصال الأجهزة الخارجية.

6. تكوين مراقبة الملفات والسجل:
   a. حدد خانة الاختيار **مراقبة الملفات والسجل**.
   b. انقر على **إعداد**.
   يؤدي ذلك إلى فتح قائمة قواعد مراقبة سلامة النظام.
   c. انقر على **إضافة**.
   يمكنك أيضًا استيراد القواعد من مصدر آخر.
   d. قم بتكوين قاعدة مراقبة سلامة النظام (انظر الجدول أدناه).
7. احفظ تغييراتك.

المعلمة	الوصف
اسم القاعدة	اسم قاعدة مهمة التحقق من سلامة النظام.
مستوى خطورة الحدث	يسجل Kaspersky Endpoint Security أحداث تعديل الملف كلما تم تعديل ملف أو مفتاح سجل في نطاق المراقبة. وتتوفر مستويات خطورة الحدث التالية: معلوماتي وتحذير ⚠ وحرج ⊗.
نطاق المراقبة	• **الملف**. قائمة الملفات والمجلدات التي يراقبها المكون. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع. 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. • **التسجيل**. قائمة مفاتيح السجل والقيم التي يراقبها المكون. يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع.
الاستثناءات	• **الملف**. 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. 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. • **التسجيل**. قائمة الاستثناءات من نطاق المراقبة. يدعم Kaspersky Endpoint Security حرفي `*` و `?` عند إدخال قناع. وتتمتع إدخالات الاستثناء بأولوية أعلى من إدخالات نطاق المراقبة.

تشغيل مهمة التحقق من سلامة النظام

تسمح مهمة التحقق من سلامة النظام بفحص الملفات أو مفاتيح السجل بحثًا عن التغييرات وأيضًا التحقق من اتصال الأجهزة الخارجية. وللتحقق من الملفات للبحث عن التغييرات، يمكنك تشغيل مهمة التحقق من سلامة النظام في الأوضاع التالية:

- فحص سريع.

  عند التحقق من الملفات للبحث عن التغييرات، تتحقق التطبيقات من سمات الملف فقط. ولا يتحقق التطبيق من محتوى الملفات.

- فحص كامل.

  عند التحقق من الملفات للبحث عن التغييرات، تتحقق التطبيقات من كل سمات الملفات ومحتوى الملفات.

لا يؤثر الوضع الذي يتم تشغيل المهمة فيه على فحص السجل أو الأجهزة الخارجية.

كيفية تشغيل مهمة التحقق من سلامة النظام في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Tasks**.
تفتح قائمة المهام.

3. انقر فوق **New task**.
يبدأ معالج المهمة. اتبع تعليمات المعالج.

4. حدد **Kaspersky Endpoint Security** ← **مراقبة سلامة النظام الأساسي**. حدد وضعًا لمراقبة سلامة النظام:

- **فحص كامل**. في هذا الوضع، يتحقق التطبيق من جميع سمات الملفات وتجزئتها.
- **فحص سريع**. في هذا الوضع، يتحقق التطبيق من سمات الملفات فقط.

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

- 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.
- حدد مجموعة الأجهزة التي تريد تشغيل المهمة لها.
- تعيين المهمة إلى مجموعة إدارة. في هذه الحالة يتم تعيين المهمة لأجهزة الكمبيوتر ضمن مجموعة إدارة تم إنشاؤها مسبقًا.

6. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

7. قم بتكوين جدول لبدء مهمة، على سبيل المثال، يدويًا أو في يوم محدد من الأسبوع.

8. أدخل اسمًا للمهمة.

9. قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية تشغيل مهمة System Integrity Check في Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

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

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **System Integrity Check**.

c. في الحقل **Task name**، أدخل وصفًا مختصرًا، علي سبيل المثال، التحقق من سلامة النظام أسبوعيًا.

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

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

5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

6. قم بإنهاء المعالج.
سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة الجديدة.
نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. حدد وضع التحقق من سلامة النظام:

- **Quick Scan**. يتحقق التطبيق من سمات الملف فقط. ولا يتحقق التطبيق من محتوى الملفات.
- **Full Scan**. يتحقق التطبيق من كل سمات الملفات بالإضافة إلى محتوياتها.

10. احفظ تغييراتك.

11. حدد خانة الاختيار المجاورة للمهمة.

12. انقر فوق **Start**.

لإنهاء مهمة التحقق من سلامة النظام بنجاح، يجب أن يتطابق نطاق مراقبة مهمة التحقق من سلامة النظام تمامًا مع خط الأساس. وإذا كان نطاق المراقبة مختلفًا، ستنتهي المهمة بخطأ. ولمزامنة نطاقات المراقبة، قم بتشغيل مهمة تحديث خط الأساس باستخدام نطاق مراقبة جديد.

تصدير واستيراد قواعد مراقبة سلامة النظام

يمكنك تصدير قائمة قواعد مراقبة سلامة النظام إلى ملف XML. وبعد ذلك يمكنك تعديل الملف، على سبيل المثال، إضافة عدد كبير من السجلات من النوع نفسه. ويمكنك استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من قائمة قواعد مراقبة سلامة النظام أو لترحيل القائمة إلى خادم مختلف.

لا تدعم مراقبة سلامة النظام استيراد مفاتيح HKEY_CURRENT_USER و HKEY_CURRENT_CONFIG لمهمة التحقق من سلامة النظام. وإذا كان نطاق مراقبة المهمة يحتوي على هذه المفاتيح، فسيقوم التطبيق بتكوين حدث يتضمن نطاق المراقبة كائنات غير صحيحة.

كيفية تصدير واستيراد قائمة قواعد مراقبة سلامة النظام في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **ضوابط الأمان** ← **مراقبة سلامة النظام**.

4. لتصدير أو استيراد قواعد مراقبة سلامة النظام في الوقت الحقيقي:

a. في القسم **مراقبة سلامة النظام في الوقت الحقيقي**، انقر على الزر **الإعدادات**.

b. لتصدير قائمة بقواعد مراقبة سلامة النظام في الوقت الحقيقي:

1. 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.

2. انقر على رابط **تصدير**.

3. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة القواعد إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.

4. احفظ الملف.
يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد بالكامل إلى ملف XML.

c. لاستيراد قائمة بقواعد مراقبة سلامة النظام في الوقت الحقيقي:

1. انقر على رابط **استيراد**.
في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

2. 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.

5. لتصدير أو استيراد قواعد التحقق من سلامة النظام:

a. في القسم **التحقق من سلامة النظام**، حدد **الإعدادات المخصصة**.

b. انقر على **الإعدادات**.

c. لتصدير قائمة قواعد التحقق من سلامة النظام:

1. 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.

2. انقر على رابط **تصدير**.

3. في النافذة التي تفتح، حدد اسم ملف XML الذي تريد تصدير قائمة القواعد إليه، وحدد المجلد الذي تريد حفظ هذا الملف به.

4. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد بالكامل إلى ملف XML.

d. لاستيراد قائمة بقواعد التحقق من سلامة النظام:

1. انقر على رابط **استيراد**.
في النافذة التي تفتح، حدد ملف XML الذي ترغب في استيراد قائمة القواعد منه.

2. 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.

6. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة قواعد مراقبة سلامة النظام في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Security Controls** ← **System Integrity Monitoring**.

5. حدد علامة التبويب **Windows**.

6. لتصدير أو استيراد قواعد مراقبة سلامة النظام في الوقت الحقيقي:

a. في القسم **Real-Time System Integrity Monitoring**، انقر على الرابط **Rules**.

b. لتصدير قائمة بقواعد مراقبة سلامة النظام في الوقت الحقيقي:

1. حدد القواعد التي تريد تصديرها.

2. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف JSON في مجلد التنزيلات الافتراضي.

c. لاستيراد قائمة بقواعد مراقبة سلامة النظام في الوقت الحقيقي:

1. انقر على الزر ← **Import**.

في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد قائمة العناوين الموثوقة منه.

2. 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 JSON.

7. لتصدير أو استيراد قواعد التحقق من سلامة النظام:

a. في القسم **On-Demand System Integrity Check**، حدد **Custom settings**.

b. انقر على رابط **Rules**.

c. لتصدير قائمة قواعد التحقق من سلامة النظام:

1. حدد القواعد التي تريد تصديرها.

2. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة القواعد إلى ملف JSON في مجلد التنزيلات الافتراضي.

d. لاستيراد قائمة بقواعد التحقق من سلامة النظام:

1. انقر على الزر ← **Import**.

في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد قائمة العناوين الموثوقة منه.

2. 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 JSON.

8. احفظ تغييراتك.

عرض تقارير مراقبة سلامة النظام

لتحليل أداء قواعد مراقبة سلامة النظام، يمكنك الاطلاع على التقارير والأحداث التي تم إنشاؤها بواسطة التطبيق. ينشئ Kaspersky Endpoint Security التقارير التالية المتعلقة بالمكون:

- في واجهة التطبيق:
  - تقرير مراقبة سلامة النظام
  - تقرير التحقق من سلامة النظام
  - تقرير تحديث خط الأساس

تحتوي التقارير على أحداث مراقبة سلامة النظام.

- في Kaspersky Security Center Console.
  - تقرير عن أجهزة الكمبيوتر التي تم تشغيل قواعد المراقبة عليها أكبر عدد من المرات
  - تقرير عن قواعد المراقبة التي يتم تشغيلها بشكل متكرر

بشكل افتراضي، يتم إنشاء تقرير لآخر 30 يومًا، بما في ذلك تاريخ إنشاء التقرير.

كيفية عرض تقارير مراقبة سلامة النظام في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في العقدة **Administration Server** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **Reports**.

3. انقر فوق **New report template**.

بدء تشغيل معالج قالب تقرير جديد.

4. اتبع تعليمات معالج قالب التقرير. في الخطوة **Selecting the report template type**، حدد تقرير مراقبة سلامة النظام (القسم **Other**):

- **Top 10 devices with File Integrity Monitor / System Integrity Monitoring rules most frequently triggered**.
- **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول في علامة التبويب **Reports**.

5. افتح التقرير بالنقر المزدوج عليه.

تبدأ عملية إنشاء التقرير. يتم عرض التقرير في نافذة جديدة.

كيفية عرض تقارير مراقبة سلامة النظام في Web Console

1. في نافذة Web Console الرئيسية، حدد **Monitoring ← Reports**.

2. انقر على **Add**.

بدء تشغيل معالج قالب تقرير جديد.

3. تحت **Template type**، في القسم **Other**، حدد تقرير مراقبة سلامة النظام:

- **Top 10 devices with File Integrity Monitor / System Integrity monitoring rules most frequently triggered**.
- **Top 10 rules of File Integrity Monitor / System Integrity Monitoring that were triggered on devices most frequently**.

بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول.

4. حدد التقرير وقم بتشغيله.

تبدأ عملية إنشاء التقرير. يتم عرض التقرير في نافذة جديدة.

لعرض الأحداث التي تم إنشاؤها بواسطة التطبيق، يمكنك أيضًا استخدام مجموعات الأحداث في وحدة تحكم Kaspersky Security Center.

إعادة تعيين حالة سلامة النظام

تتمتع أجهزة الكمبيوتر في وحدة تحكم Kaspersky Security Center بإحدى الحالات التالية: OK أو Warning أو Critical. وإذا اكتشفت مراقبة سلامة النظام تعديل الملفات أو مفاتيح السجل في نطاق المراقبة، تتغير حالة الكمبيوتر إلى Warning أو Critical. وتسمى الحالة المعينة بواسطة مراقبة سلامة النظام حالة سلامة النظام. ويمكنك إعادة تعيين حالة سلامة النظام، على سبيل المثال، إذا أقنعك التحليل بأن التعديل المكتشف للكائنات لا يؤثر على أمان الكمبيوتر.

كيفية إعادة تعيين حالة سلامة النظام في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2) ← إعادة ضبط حالة سلامة النظام**.

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

كوّن جدول المهام، على سبيل المثال، يدويًا.

الخطوة الرابعة: تحديد اسم المهمة

أدخل اسم المهمة، على سبيل المثال، إعادة تعيين الحالة بعد تعديل نطاق المراقبة.

الخطوة 5 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية إعادة تعيين حالة سلامة النظام في Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.
2. انقر على **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.
   b. في القائمة المنسدلة **Task type**، حدد **System integrity status reset**.
   c. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، إعادة تعيين الحالة بعد تعديل نطاق المراقبة.
   d. في القسم **Devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.

5. حدد حسابًا لتشغيل المهمة. الوضع الافتراضي أن Kaspersky Endpoint Security سيبدأ المهمة بحقوق حساب مستخدم محلي.

6. قم بإنهاء المعالج.

سيتم عرض مهمة جديدة في قائمة المهام.

7. حدد خانة الاختيار المجاورة للمهمة.

8. انقر فوق **Start**.

نتيجة لذلك، إذا تم تغيير حالة الكمبيوتر إلى Warning أو Critical بسبب أحداث مراقبة سلامة النظام، تتم إعادة تعيين حالة الكمبيوتر إلى OK. وإذا تم تغيير حالة الكمبيوتر أيضًا بسبب أحداث أخرى، تظل حالة الكمبيوتر بدون تغيير.

Cloud Discovery

ويدير Cloud Discovery وصول المستخدم إلى الخدمات السحابية. وتشمل الخدمات السحابية، على سبيل المثال، Microsoft Teams وSalesforce وMicrosoft Office 365. يتم تجميع الخدمات السحابية في فئات، على سبيل المثال، File sharing وMessengers وEmail. ويتولى خبراء Kaspersky تحديث فئات Cloud Discovery والخدمات السحابية المصنفة في الفئات بانتظام. ويحدّث Kaspersky Endpoint Security مجموعة الفئات والخدمات السحابية مع قواعد بيانات التطبيق. ويعني هذا أن Cloud Discovery لا يستخدم شبكة Kaspersky Security Network لتصنيف الخدمات السحابية.

يوفر Cloud Discovery الوظائف التالية:

- مراقبة استخدام الخدمة السحابية
- منع وصول المستخدم إلى الخدمات السحابية

متطلبات النظام

يتوفر Cloud Discovery في حالة استيفاء الشروط التالية:

- تثبيت التطبيق على كمبيوتر يعمل بنظام Windows for workstations.

  لا يتوفر المكون للخوادم.

- Kaspersky Security Center الإصدار 15.1 أو أحدث.

  المكون غير متوفر في وحدة تحكم الإدارة (MMC). ويمكنك تكوين Cloud Discovery في Kaspersky Security Center Web Console وKaspersky Security Center Cloud Console.

- ترخيص Kaspersky Next.

تمكين وظائف التطبيق التي يتطلبها مكون Cloud Discovery:

1. **فحص الاتصالات المشفرة**. يعد ذلك ضروريًا لمراقبة حركة مرور HTTPS. ويمكنك إدارة هذه الوظيفة في قسم **إعدادات الشبكة**.

2. **إدخال البرنامج النصي في حركة مرور الويب للتفاعل مع صفحات الويب**. يتيح البرنامج النصي تسجيل أحداث Cloud Discovery. يوفر البرنامج النصي أيضًا حظرًا كاملاً للوصول إلى الخدمات السحابية. وبدون البرنامج النصي، يحظر التطبيق الوصول فقط عن طريق مجالات الخدمة السحابية. ويمكنك إدارة هذه الوظيفة في قسم **إعدادات الشبكة**.

يمكنك أيضًا تمكين وظيفة **تسجيل فتح الصفحات المسموح بها**. وتتضمن الوظيفة تجميع الأحداث عندما يزور المستخدم صفحات الويب التي تنتمي إلى المجال نفسه. وبهذه الطريقة، عندما يستخدم المستخدم خدمة سحابية، يسجل حل Cloud Discovery حدثًا واحدًا فقط بدلاً من أحداث متعددة لكل صفحة ويب. ويمكنك إدارة هذه الوظيفة في قسم **التحكم في الويب**.

مراقبة الخدمات السحابية

عندما يبدأ المستخدم في استخدام خدمة سحابية، يسجل Kaspersky Endpoint Security هذا الحدث وينشئ إدخالاً في التقرير. ويتحكم Cloud Discovery في استخدام الخدمة السحابية في المستعرض وكذلك في التطبيقات المقابلة. ويتحكم Cloud Discovery في استخدام الخدمة السحابية عبر HTTP وHTTPS.

كيفية تمكين مراقبة الخدمة السحابية في Cloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Communication & Web Protection** ← **Cloud Discovery**.
5. قم بتشغيل مفتاح **Cloud Discovery ENABLED**.
6. احفظ تغييراتك.

نتيجة لذلك، يعيد التطبيق توجيه المعلومات عن الخدمات السحابية المستخدمة إلى Kaspersky Security Center. ويمكنك عرض معلومات استخدام الخدمة السحابية في التقارير. وإذا لزم الأمر، يمكنك منع الوصول إلى الخدمات السحابية.

منع الوصول إلى الخدمات السحابية

لا يتوفر حظر الوصول إلى الخدمات السحابية إلا لترخيص Kaspersky Next EDR Optimum وXDR Expert . ولا تتوفر هذه الميزة لترخيص Kaspersky Next EDR Foundations. مقارنة وظائف التطبيق حسب نوع ترخيص Kaspersky Next، راجع تعليمات Kaspersky Next.

يستطيع المسؤول تقييد وصول المستخدم إلى فئات Cloud Discovery أو الخدمات السحابية الفردية. وبهذه الطريقة، يستطيع المسؤول السماح بالخدمات السحابية الآمنة فقط وتجنب تسرب البيانات. يتم عرض معلومات مستوى المخاطر لكل خدمة سحابية في Cloud Discovery. ويساعد مستوى المخاطرة في اكتشاف الخدمات التي لا تلبي متطلبات الأمان الخاصة بالمؤسسة.

يكون مستوى المخاطرة عبارة عن تقدير ولا يتضمن أي بيانات حول جودة الخدمة السحابية أو بائعها. ويمثل مستوى المخاطرة مجرد توصية من خبراء Kaspersky.

يتم عرض مستويات المخاطر للخدمات السحابية في القسم **Cloud Discovery** في السياسة في قائمة جميع الخدمات السحابية الخاضعة للتحكم.

وتوفر مكونات Kaspersky Endpoint Security الأخرى الحماية من التهديدات وتتبع نشاط المستخدم المشبوه عند استخدام الخدمات السحابية.



إخطار Cloud Discovery

لا يمنع Cloud Discovery التطبيقات السحابية التي تم تشغيلها قبل Kaspersky Endpoint Security.

كيفية حظر الوصول إلى الخدمات السحابية في Cloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Communication & Web Protection** ← **Cloud Discovery**.
5. قم بتشغيل مفتاح **Cloud Discovery ENABLED**.
   يتم عرض قائمة بجميع الخدمات السحابية. يتم تجميع الخدمات السحابية في فئات، على سبيل المثال، File sharing وMessengers وEmail. ويتولى خبراء Kaspersky تحديث فئات Cloud Discovery والخدمات السحابية المصنفة في الفئات بانتظام. ويحدّث Kaspersky Endpoint Security مجموعة الفئات والخدمات السحابية مع قواعد بيانات التطبيق.
6. استخدم زر التبديل في العمود **Access** لتكوين الوصول إلى الخدمات السحابية.
7. احفظ تغييراتك.

نتيجة لذلك، يتحكم التطبيق في استخدام الخدمة السحابية في المستعرض وكذلك في التطبيقات المقابلة.

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.

بدءًا من Kaspersky Endpoint Security 12.5 for Windows، يمكنك إضافة قياس EDR عن بُعد إلى المنطقة الموثوقة. ويسمح ذلك بتحسين البيانات التي يرسلها التطبيق إلى خادم جمع القياس عن بُعد لحل Kaspersky Anti Targeted Attack Platform (EDR).

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم.

بدءًا من الإصدار Kaspersky Endpoint Security 12.8 for Windows، يمكنك تثبيت التطبيق في وضع Light Agent لحماية البيئات الافتراضية. ويمكن أن تساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في البيئات الافتراضية في Citrix وVMware

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. تتيح استثناءات الفحص إمكانية الاستخدام الآمن للبرامج الشرعية التي يمكن للمجرمين استغلالها لإتلاف جهاز الكمبيوتر أو بيانات المستخدم. وليس بالضرورة أن يكون لمثل هذه التطبيقات أغراض ضارة، لكن يمكن للقراصنة استغلالها. وللحصول على معلومات مفصلة عن التطبيقات المشروعة التي يمكن أن يستخدمها الدخلاء لاختراق الكمبيوتر أو بيانات المستخدم، يرجى زيارة موقع ويب موسوعة 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.

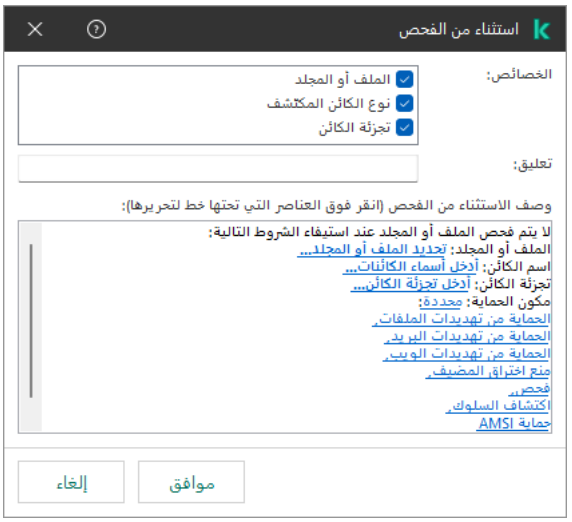
- الحماية من تهديدات البريد.
- مهمة فحص البرامج الضارة

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 **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.
5. في القسم **استثناءات الفحص والتطبيقات الموثوقة** ← **استثناءات الفحص**، انقر على الزر **الإعدادات**.
   يفتح هذا نافذة تحتوي على قائمة استثناءات.
6. 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.
7. 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. أيضًا، في حالة إلغاء تحديد خانة الاختيار هذه، يخفي Kaspersky Endpoint Security القائمة الموحدة لاستثناءات الفحص في واجهة المستخدم الخاصة بالتطبيق.
8. انقر فوق **إضافة** وحدد إجراءً:
   - **الفئة**. يمكنك تجميع استثناءات الفحص في فئات منفصلة. ولإنشاء فئة جديدة، أدخل اسم الفئة وأضف استثناء فحص واحد على الأقل إلى الفئة.
   - **استثناء جديد**. يضيف Kaspersky Endpoint Security استثناءً جديدًا للفحص إلى جذر القائمة.
   - **تحديد الاستثناء من القائمة**. لتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق استثناءات الفحص المحددة مسبقًا. وتمت أيضًا إضافة استثناءات فحص محددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد استثناءات من الفحص محددة مسبقًا وفقًا للغرض من الخادم المحمي.
   - **استثناء جديد للفئة المحددة**. ولإضافة استثناء فحص جديد إلى فئة معينة، حدد فئة.

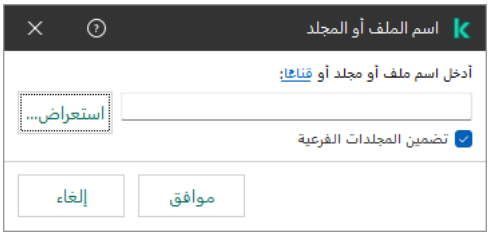
9. لاستثناء ملف أو مجلد من الفحص:



إعدادات الاستثناءات

a. في القسم **الخصائص**، حدد خانة الاختيار **الملف أو المجلد**.

b. انقر فوق الرابط الموجود في القسم أدناه لفتح النافذة **اسم الملف أو المجلد**.



تحديد ملف أو مجلد

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 `?:\Users\*\Folder\`.

يدعم Kaspersky Endpoint Security متغيرات البيئة

يمكنك استثناء مجلدات الشبكة. ولفعل ذلك، أدخل المسار إلى مجلد الشبكة يدويًا (على سبيل المثال، `\\Network Share\*`).

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.

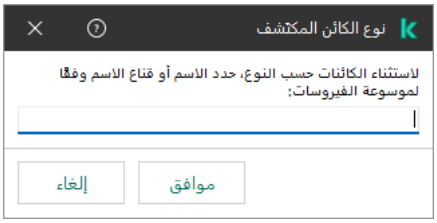
b. إذا لزم الأمر، قم بتعطيل وظيفة **تضمين المجلدات الفرعية**. وفي حالة تمكين هذه الوظيفة، فلن يفحص التطبيق الملفات في كل المجلدات الفرعية. وفي حالة تعطيل هذه الوظيفة، يستثني التطبيق المجلد المحدد فقط من نطاق الفحص. ويتم تمكين هذا الخيار بشكل افتراضي.

c. احفظ تغييراتك.

10. لاستبعاد كائنات ذات اسم محدد من الفحص:

a. في القسم **الخصائص**، حدد خانة الاختيار **نوع الكائن المكتَشف**.

b. انقر فوق الرابط الموجود في القسم أدناه لفتح النافذة **نوع الكائن المكتَشف**.



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.

11. إذا كنت ترغب في استثناء ملف فردي من عمليات الفحص:

a. في القسم **الخصائص**، حدد خانة الاختيار **تجزئة الكائن**.

b. انقر فوق الرابط الموجود في القسم أدناه 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.

12. إذا لزم الأمر، في الحقل **تعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

13. حدد مكونات Kaspersky Endpoint Security التي يجب أن تستخدم استثناء من الفحص:

a. انقر فوق الرابط الموجود في القسم أدناه لفتح النافذة **مكونات الحماية**.



تحديد مكونات الحماية

a. حدد خانات الاختيار المقابلة للمكونات التي يجب تطبيق استثناء من الفحص إليها.

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.

14. انقر على **موافق**.

ستتم إضافة الاستثناء الجديد إلى القائمة. ويمكنك تعطيل الاستثناء في أي وقت باستخدام خانة الاختيار بجوار الكائن.

15. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إنشاء استثناء من الفحص في Kaspersky Security Center Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى القسم **Trusted Zone**.

5. في النافذة التي تفتح، انقر فوق الرابط **Malware 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. أيضًا، في حالة إلغاء تحديد خانة الاختيار هذه، يخفي Kaspersky Endpoint Security القائمة الموحدة لاستثناءات الفحص في واجهة المستخدم الخاصة بالتطبيق.

8. انقر فوق **Add** وحدد إجراءً:

- **Category**. يمكنك تجميع استثناءات الفحص في فئات منفصلة. ولإنشاء فئة جديدة، أدخل اسم الفئة وأضف استثناء فحص واحد على الأقل إلى الفئة.
- **New exclusion**. يضيف Kaspersky Endpoint Security استثناءً جديدًا للفحص إلى جذر القائمة.
- **Select exclusion from list**. لتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق استثناءات الفحص المحددة مسبقًا. وتمت أيضًا إضافة استثناءات فحص محددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد استثناءات من الفحص محددة مسبقًا وفقًا للغرض من الخادم المحمي.

لإضافة استثناء من الفحص جديد إلى فئة محددة، حدد خانة الاختيار بجوار تلك الفئة وحدد الخيار **New exclusion**.

9. حدد كيف تريد إضافة الاستثناء: **Path to the file or folder** أو **Object type** 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 `?:\Users\*\Folder\`.

  يمكنك استثناء مجلدات الشبكة. ولفعل ذلك، أدخل المسار إلى مجلد الشبكة يدويًا (على سبيل المثال، `\\Network Share\*`).

11. إذا كنت ترغب في استثناء نوع معين من الكائنات من عمليات الفحص، في الحقل **Object type** أدخل اسم نوع 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.

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 **Apply exclusion to**، 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. انقر على **OK**.

  ستتم إضافة الاستثناء الجديد إلى القائمة. يمكنك استخدام مفتاح التبديل إيقاف استثناء في أي وقت.

16. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

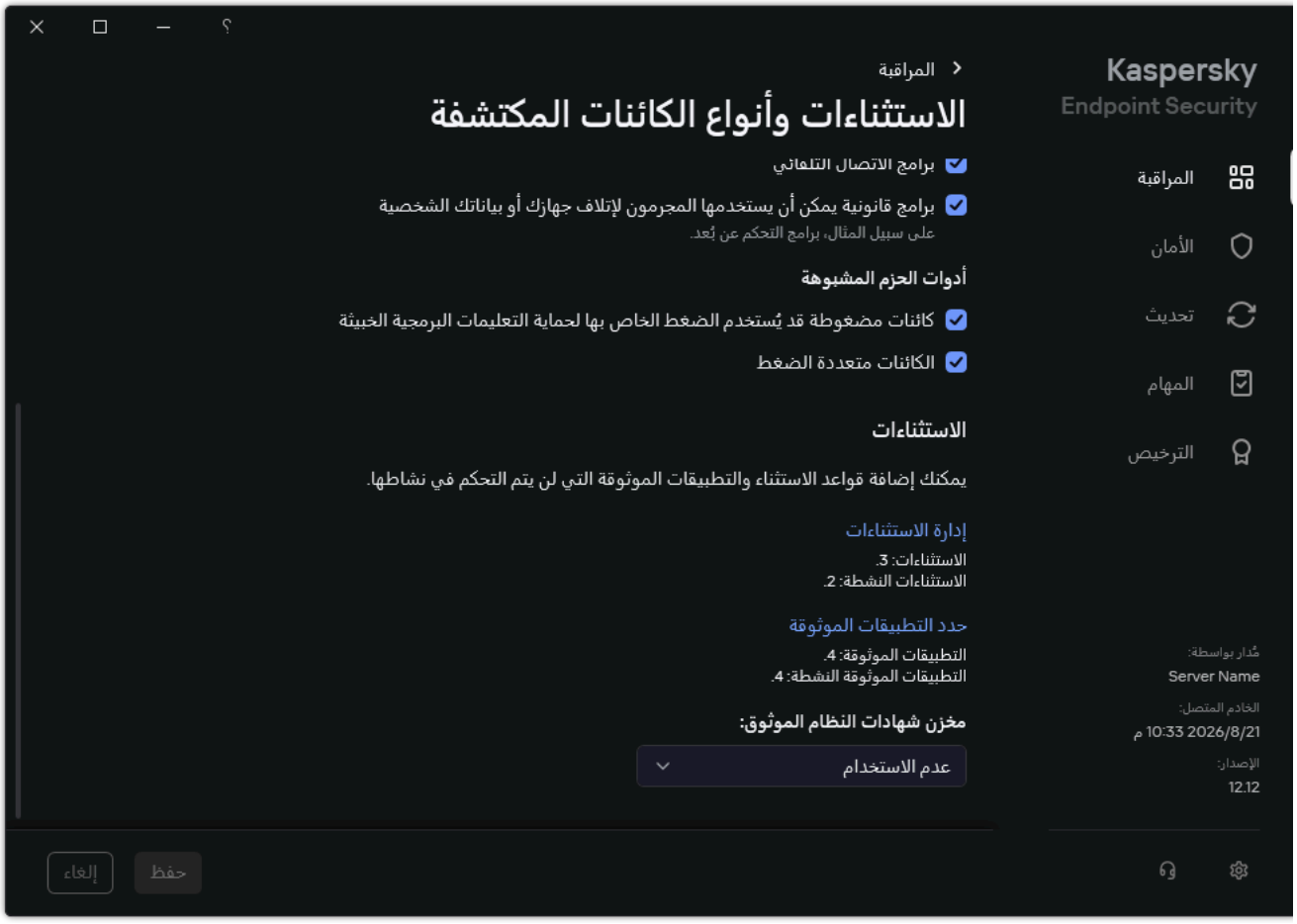
كيفية إنشاء استثناء من الفحص في واجهة التطبيق

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**.

يخفي Kaspersky Endpoint Security قائمة استثناءات الفحص في واجهة المستخدم الخاصة بالتطبيق إذا تم حظر تكوين استثناءات الفحص بواسطة المسؤول في وحدة التحكم (رمز "القفل المغلق") وتم حظر استثناءات الفحص المحلية (تم إلغاء تحديد خانة الاختيار **السماح باستخدام الاستثناءات المحلية**).



إعدادات الاستثناءات

4. انقر فوق **إضافة** وحدد إجراءً:

- **الفئة**. يمكنك تجميع استثناءات الفحص في فئات منفصلة. ولإنشاء فئة جديدة، أدخل اسم الفئة وأضف استثناء فحص واحد على الأقل إلى الفئة.
- **استثناء جديد**. يضيف Kaspersky Endpoint Security استثناءً جديدًا للفحص إلى جذر القائمة.
- **تحديد الاستثناء من القائمة**. لتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق استثناءات الفحص المحددة مسبقًا. وتمت أيضًا إضافة استثناءات فحص محددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد استثناءات من الفحص محددة مسبقًا وفقًا للغرض من الخادم المحمي.

لإضافة استثناء من الفحص جديد إلى فئة محددة، حدد خانة الاختيار بجوار تلك الفئة وحدد الخيار **استثناء جديد**.

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 `?:\Users\*\Folder\`.

  يمكنك استثناء مجلدات الشبكة. ولفعل ذلك، أدخل المسار إلى مجلد الشبكة يدويًا (على سبيل المثال، `\\Network Share\*`).

6. إذا كنت ترغب في استثناء نوع معين من الكائنات من عمليات الفحص، في الحقل **نوع الكائن المكتَشف** أدخل اسم نوع 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.

7. إذا كنت ترغب في استثناء ملف فردي من عمليات الفحص، فأدخل تجزئة الملف في الحقل **تجزئة الكائن**.

   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.

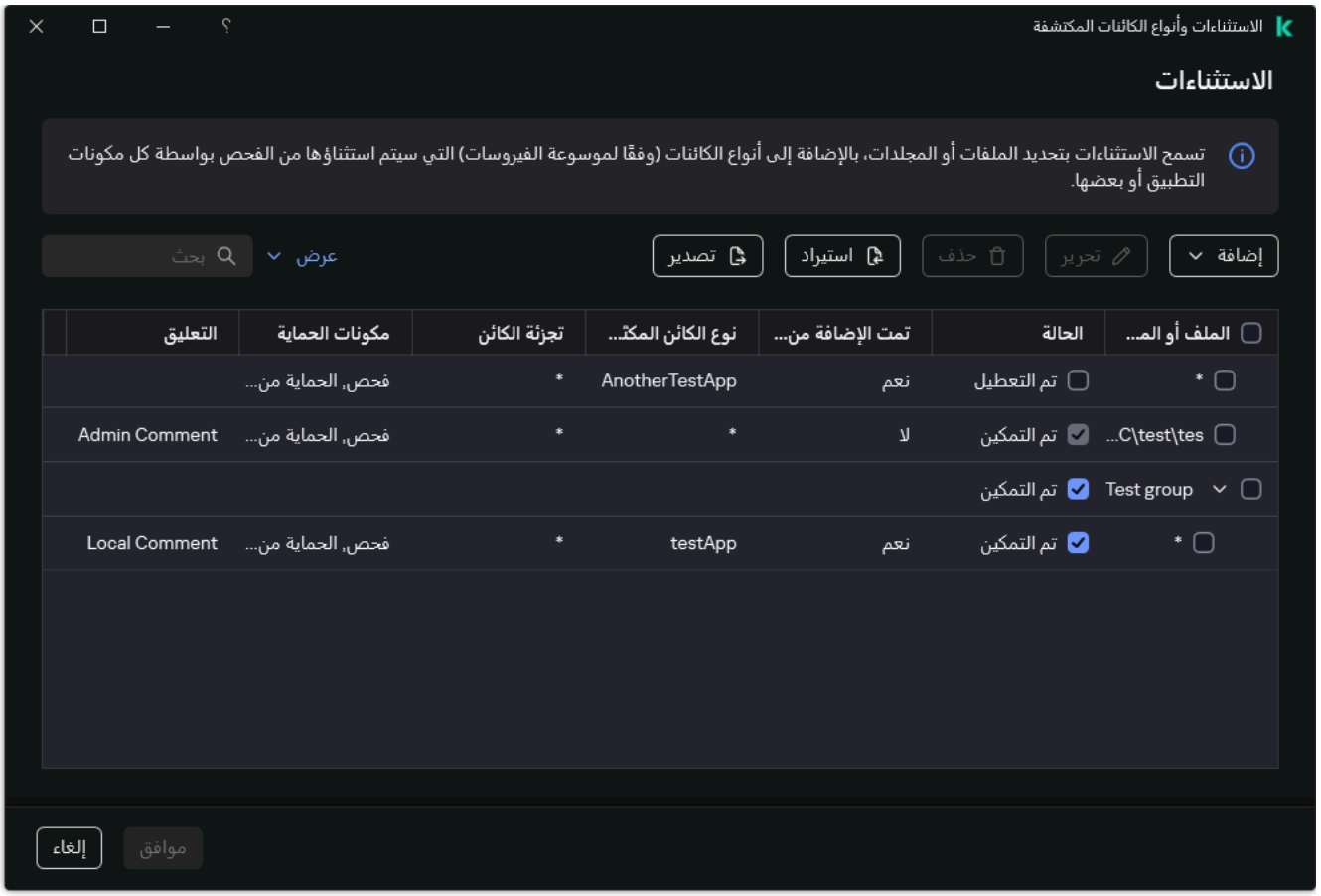
9. إذا لزم الأمر، في الحقل **التعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

10. حدد الحالة **فعال** للاستثناء.

11. انقر على **إضافة**.

    ستتم إضافة الاستثناء الجديد إلى القائمة. ويمكنك تعطيل الاستثناء في أي وقت باستخدام خانة الاختيار الموجودة في عمود **الحالة**.

12. احفظ تغييراتك.



قائمة الاستثناءات

أمثلة قناع المسار:

نوصي بتحديد المسارات النسبية بدلاً من المسارات المطلقة. ولا يسمح هذا باستثناء كائنات نظام الملفات فحسب، بل يسمح أيضًا باستثناء الكائنات التي ليس لها ملفات. على سبيل المثال، `*\Program Files (x86)\Folder\Subfolder`.

مسارات الملفات الموجودة في أي مجلد:

- سيشمل القناع `*.exe` كافة المسارات إلي 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 المجلد `C:\dir\` لكنها ليست موجودة في المجلدات الفرعية للمسار `C:\dir\`.
- سيشمل القناع `C:\dir\*\test` جميع المسارات إلى الملفات المسماة "test" الموجودة في المجلد `C:\dir\` وفي المجلدات الفرعية `C:\dir\`.
- سيشمل القناع `C:\dir1\*\dir3\` جميع مسارات الملفات الموجودة في المجلدات dir3 الفرعية بمستوى واحد في المجلد `C:\dir1\`.
- سيشمل القناع `C:\dir1\**\dirN\` جميع مسارات الملفات في المجلدات 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" لكنها 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.

إنشاء استثناء حسب نوع الكائنات المكتشفة

يصنف Kaspersky Endpoint Security الكائنات المكتشفة على النحو التالي:

- **الفيروسات والفيروسات المتنقلة**

الفئة الفرعية: الفيروسات والفيروسات المتنقلة (Viruses_and_Worms)

مستوي الخطر: مرتفع

تقوم الفيروسات التقليدية والفيروسات المتنقلة بإجراءات غير مسموح بها من قِبل المستخدم. فيمكنها إنشاء نسخ من أنفسها كما تتمكن هذه النسخ من نسخ نفسها.

فيروس تقليدي

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. تكتب فيروسات Overwriting رمزها الخاص فوق رمز الملف المصاب، ثم تمسح محتوى الملف. ولذا، يتوقف ملف مصاب عن العمل ويتعذر استعادته. تقوم فيروسات Parasitic بتعديل الملفات مع تركها تعمل كليًا أو جزئيًا. تقوم فيروسات Companion بتعديل الملفات، لكنها تنشئ نُسخًا 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 Link وفيروسات OBJ وفيروسات LIB وفيروسات التعليمات البرمجية المصدرية والعديد من الفيروسات الأخرى.

الفيروس المتنقل

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 Internet Relay Chats، وهي أنظمة خدمة تتيح التواصل مع الآخرين 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 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.
الفيروس المتنقل	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 الخطر: مرتفع

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	أدوات النقر لفيروس 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 (IM) (Trojan-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.

النوع	الاسم	الوصف
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 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

مستوى الخطر: متوسط

على عكس الأنواع الأخرى من البرمجيات الضارة، لا تقوم الأدوات الخبيثة بإجراءاتها فور بدء تشغيلها. فيمكن تخزينها بأمان وبدء تشغيلها 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 "تلويث" 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).

النوع	الاسم	الوصف
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: برامج إعلانية (Adware)

مستوي الخطر: 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: برامج الاتصال التلقائي (برنامج الاتصال).

مستوي الخطر: متوسط

يستطيع برنامج الاتصال التلقائي إنشاء اتصالات هاتفية خلسة باستخدام مودم.

- **برامج قانونية يمكن أن يستخدمها المجرمون لإتلاف جهازك أو بياناتك الشخصية**

الفئة الفرعية: تم اكتشاف برامج قانونية يمكن أن يستخدمها المجرمون لإتلاف جهازك 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.
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 فيروسات 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 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 لمكافحة الفيروسات تعرض عن حول اكتشاف البرامج الضارة. برغم ذلك، فإنها لا تكتشف في الواقع أي شيء أو تنظفه.

- **كائنات مضغوطة قد يُستخدم الضغط الخاص بها لحماية التعليمات البرمجية الخبيثة**

الفئة الفرعية: الملفات المحزومة التي قد تتسبب في حدوث أضرار

مستوي الخطر: متوسط.

يتم حزم الملف باستخدام أداة حزم خاصة يتم استخدامها لحزم البرامج الضارة: الفيروسات والفيروسات المتنقلة وفيروسات حصان طروادة. يفحص Kaspersky Endpoint Security الوحدة النمطية لفك الحزمة داخل الأرشيفات ذاتية الاستخراج (SFX).

لإخفاء البرامج الضارة من الاكتشاف بواسطة برنامج مكافحة الفيروسات، يقوم المتسللون بحزمها باستخدام برامج حزم خاصة. حدد خبراء Kaspersky برامج الحزم الأكثر شيوعًا بين القراصنة.

- **الكائنات متعددة الضغط**

الفئة الفرعية: الملفات متعددة الضغط.

مستوي الخطر: متوسط.

يكون الملف مضغوطًا مع واحد أو أكثر من برامج الحزم ثلاث مرات أو أكثر.

لإخفاء البرامج الضارة من اكتشافها بواسطة برنامج مكافحة الفيروسات، قد يقوم المتسللون بحزم ملف عدة مرات. يفحص Kaspersky Endpoint Security الملفات المحزمة.

بشكل افتراضي، يكتشف Kaspersky Endpoint Security جميع أنواع الكائنات. ونوصي بترك ميزة اكتشاف جميع أنواع الكائنات ممكّنة لتحسين أمان الكمبيوتر. وإذا كنت تستخدم أدوات مساعدة داخلية يكتشفها التطبيق كخبيثة، أضف هذه الأدوات المساعدة إلى قائمة الاستثناءات، لكن لا تقم بتعطيل اكتشاف نوع الكائنات بالكامل.

كيفية تحديد أنواع الكائنات القابلة للاكتشاف في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.
5. في القسم **أنواع الكائنات المكتشفة**، انقر على الزر **الإعدادات**.
6. في النافذة التي تفتح، حدد خانات الاختيار المقابلة لأنواع الكائنات التي تريد أن يكتشفها Kaspersky Endpoint Security.
7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تحديد أنواع الكائنات القابلة للاكتشاف في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Detection Settings**.
5. في القسم **Detection of other types of objects**، حدد خانات الاختيار المقابلة لأنواع الكائنات التي تريد أن يكتشفها Kaspersky Endpoint Security.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تحديد أنواع الكائنات القابلة للاكتشاف 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 **أنواع الكائنات المكتشفة**، حدد خانات الاختيار المقابلة لأنواع الكائنات التي تريد أن يكتشفها Kaspersky Endpoint Security.

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. وبشكل افتراضي، يراقب 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 **Policies**.

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

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.

5. في القسم **استثناءات الفحص والتطبيقات الموثوقة** ← **التطبيقات الموثوقة**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تحتوي على قائمة بالتطبيقات الموثوقة.

6. 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.

7. 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. أيضًا، إذا تم إلغاء تحديد خانة الاختيار هذه ، يخفي Kaspersky Endpoint Security القائمة الموحدة للتطبيقات الموثوقة في واجهة المستخدم الخاصة بالتطبيق.

8. انقر فوق **إضافة** وحدد إجراءً:

- **الفئة**. يمكنك تجميع التطبيقات الموثوقة في فئات منفصلة. لإنشاء فئة جديدة، أدخل اسم الفئة وأضف تطبيقًا موثوقًا واحدًا على الأقل إلى الفئة.
- **استثناء جديد**. يضيف Kaspersky Endpoint Security تطبيقًا موثوقًا جديدًا إلى جذر القائمة.
- **تحديد الاستثناء من القائمة**. ولتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق التطبيقات الموثوقة المحددة مسبقًا. وتمت أيضًا إضافة التطبيقات الموثوقة المحددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد التطبيقات الموثوقة المحددة مسبقًا وفقًا للغرض من الخادم المحمي.
- **استثناء جديد للفئة المحددة**. ولإضافة تطبيق جديد موثوق إلى فئة معينة، حدد فئة.

9. حدد معايير الثقة:

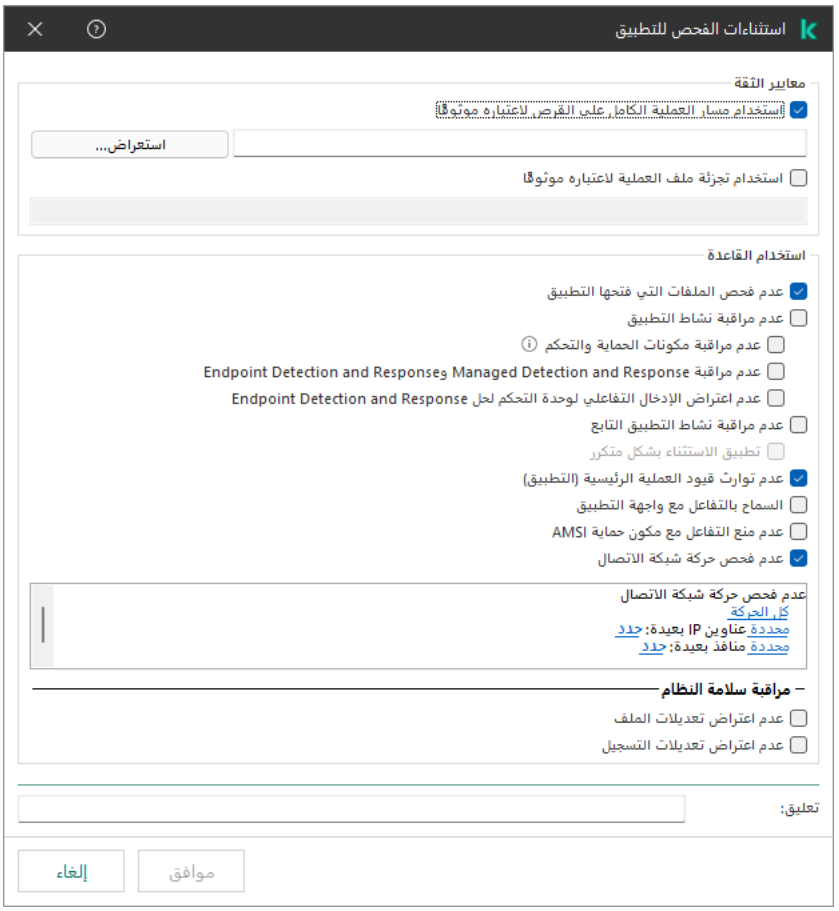
- **استخدام مسار العملية الكامل على القرص لاعتباره موثوقًا**. أدخل مسار الملف القابل للتنفيذ الخاص بالتطبيق الموثوق به.

يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع.

يتعامل Kaspersky Endpoint Security مع اسم الملف الخاص بالتطبيق الموثوق به على أنه حساس لحالة الأحرف. وإذا كانت حالة أحرف اسم الملف الذي تدخله غير صحيحة، فلن يتعرف Kaspersky Endpoint Security على التطبيق الموثوق به.

- **استخدام تجزئة ملف العملية لاعتباره موثوقًا**.

لا يدعم Kaspersky Endpoint Security متغير البيئة %userprofile% عند توليد قائمة بالتطبيقات الموثوقة في 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. انقر على **موافق**.

ستتم إضافة التطبيق الموثوق الجديد إلى القائمة. ويمكنك استثناء تطبيق من المنطقة الموثوقة في أي وقت باستخدام خانة الاختيار بجوار الكائن.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.



قائمة التطبيقات الموثوقة

كيفية إضافة تطبيق إلى القائمة الموثوقة في Kaspersky Security Center Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى القسم **Trusted Zone**.

5. في النافذة التي تفتح، انقر فوق الرابط **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 exclusions** 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. أيضًا، إذا تم إلغاء تحديد خانة الاختيار هذه ، يخفي Kaspersky Endpoint Security القائمة الموحدة للتطبيقات الموثوقة في واجهة المستخدم الخاصة بالتطبيق.

8. انقر فوق **Add** وحدد إجراءً:

- **Category**. يمكنك تجميع التطبيقات الموثوقة في فئات منفصلة. لإنشاء فئة جديدة، أدخل اسم الفئة وأضف تطبيقًا موثوقًا واحدًا على الأقل إلى الفئة.
- **New exclusion**. يضيف Kaspersky Endpoint Security تطبيقًا موثوقًا جديدًا إلى جذر القائمة.
- **Select exclusion from list**. ولتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق التطبيقات الموثوقة المحددة مسبقًا. وتمت أيضًا إضافة التطبيقات الموثوقة المحددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد التطبيقات الموثوقة المحددة مسبقًا وفقًا للغرض من الخادم المحمي.

لإضافة تطبيق موثوق جديد إلى فئة محددة، حدد خانة الاختيار بجوار تلك الفئة وحدد الخيار **New exclusion**.

9. حدد معايير الثقة:

- **Path to the file or folder**. أدخل مسار الملف القابل للتنفيذ الخاص بالتطبيق الموثوق به.

  يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع.

  يتعامل Kaspersky Endpoint Security مع اسم الملف الخاص بالتطبيق الموثوق به على أنه حساس لحالة الأحرف. وإذا كانت حالة أحرف اسم الملف الذي تدخله غير صحيحة، فلن يتعرف Kaspersky Endpoint Security على التطبيق الموثوق به.

- **Application hash**.

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.

10. قم بتكوين الإعدادات المتقدمة للتطبيق الموثوق به (انظر الجدول أدناه).

11. انقر على **OK**.

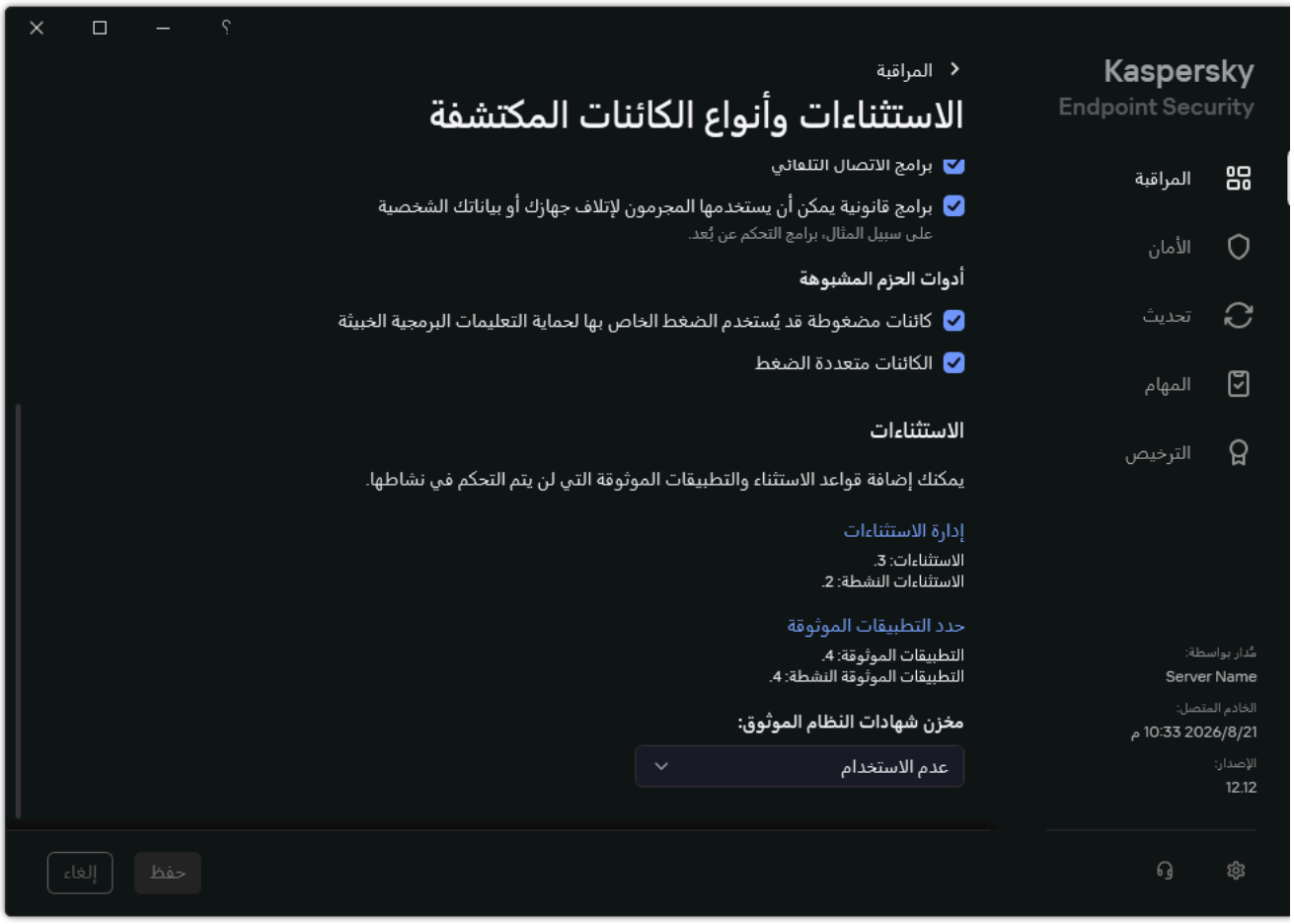
ستتم إضافة التطبيق الموثوق الجديد إلى القائمة. ويمكنك استثناء تطبيق من المنطقة الموثوقة في أي وقت باستخدام خانة الاختيار في العمود **Status**.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ 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**.

يخفي Kaspersky Endpoint Security القائمة الموحدة للتطبيقات الموثوقة في واجهة المستخدم الخاصة بالتطبيق إذا تم حظر تكوين التطبيقات الموثوقة بواسطة المسؤول في وحدة التحكم (رمز "القفل المغلق") وتم حظر التطبيقات الموثوقة المحلية (تم إلغاء تحديد خانة الاختيار **السماح باستخدام التطبيقات الموثوقة المحلية**).



إعدادات الاستثناءات

4. انقر فوق **إضافة** وحدد إجراءً:

- **الفئة**. يمكنك تجميع التطبيقات الموثوقة في فئات منفصلة. لإنشاء فئة جديدة، أدخل اسم الفئة وأضف تطبيقًا موثوقًا واحدًا على الأقل إلى الفئة.
- **استثناء جديد**. يضيف Kaspersky Endpoint Security تطبيقًا موثوقًا جديدًا إلى جذر القائمة.
- **تحديد الاستثناء من القائمة**. ولتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق التطبيقات الموثوقة المحددة مسبقًا. وتمت أيضًا إضافة التطبيقات الموثوقة المحددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد التطبيقات الموثوقة المحددة مسبقًا وفقًا للغرض من الخادم المحمي.

لإضافة تطبيق موثوق جديد إلى فئة محددة، حدد خانة الاختيار بجوار تلك الفئة وحدد الخيار **استثناء جديد**.

5. حدد معايير الثقة:

- **استخدام مسار العملية الكامل على القرص لاعتباره موثوقًا**. أدخل مسار الملف القابل للتنفيذ الخاص بالتطبيق الموثوق به.

  يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع.

  يتعامل Kaspersky Endpoint Security مع اسم الملف الخاص بالتطبيق الموثوق به على أنه حساس لحالة الأحرف. وإذا كانت حالة أحرف اسم الملف الذي تدخله غير صحيحة، فلن يتعرف Kaspersky Endpoint Security على التطبيق الموثوق به.

- **استخدام تجزئة ملف العملية لاعتباره موثوقًا**.

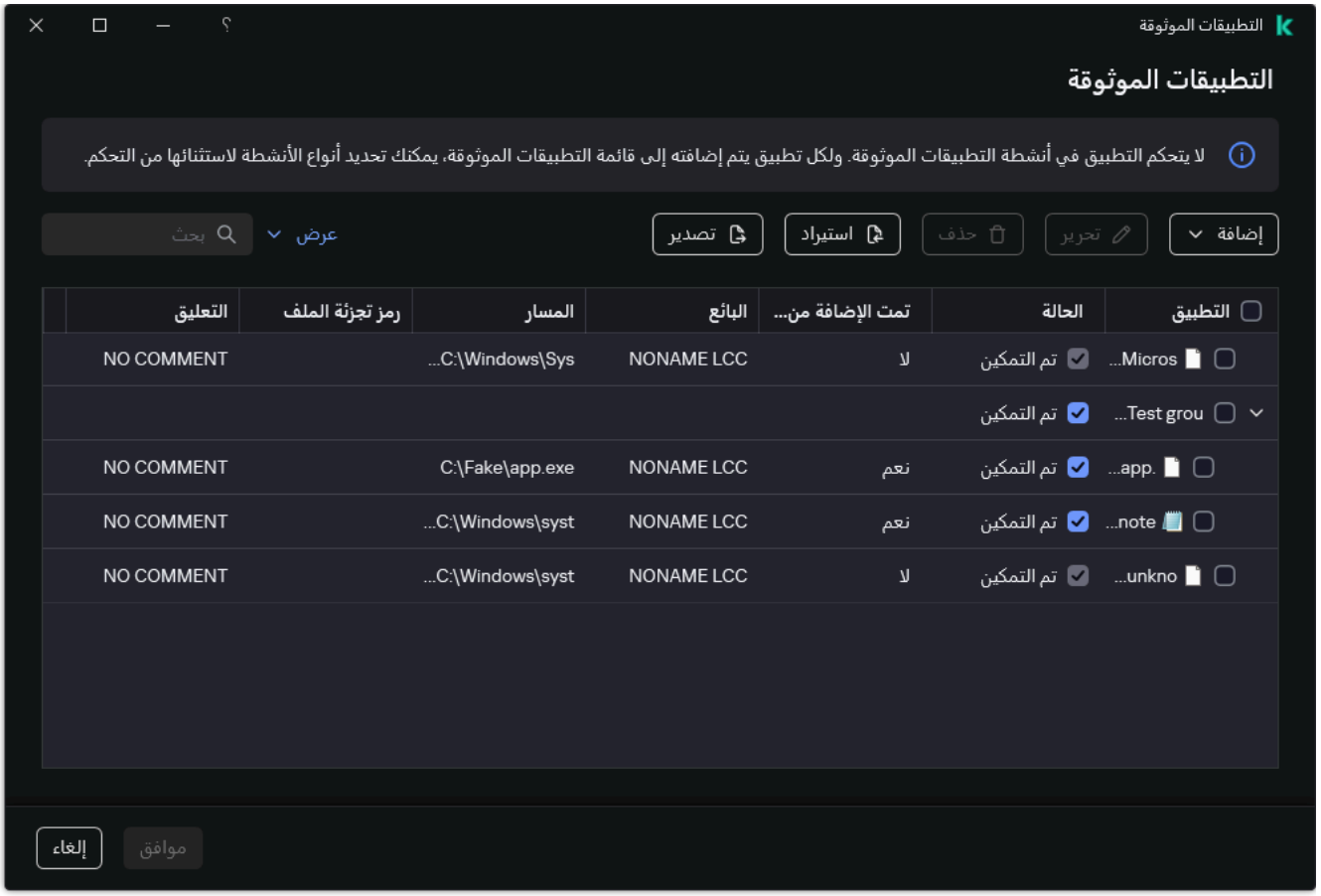
يدعم Kaspersky Endpoint Security متغيرات البيئة ويحول المسار في الواجهة المحلية للتطبيق. بعبارة أخرى، إذا أدخلت مسار الملف `%userprofile%\Documents\File.exe`، يتم إضافة سجل `C:\Users\Fred123\Documents\File.exe` في الواجهة المحلية للتطبيق للمستخدم Fred123. ووفقًا لذلك، يتجاهل Kaspersky Endpoint Security 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.

7. انقر على **موافق**.

ستتم إضافة التطبيق الموثوق الجديد إلى القائمة. ويمكنك استثناء تطبيق من المنطقة الموثوقة في أي وقت باستخدام خانة الاختيار في العمود **الحالة**.

8. احفظ تغييراتك.



قائمة التطبيقات الموثوقة

إعدادات التطبيق الموثوق

المعلمة	الوصف
عدم فحص الملفات التي فتحها التطبيق	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. ويمكنك تكوين مراقبة نشاط التطبيق لمكونات مختلفة من Kaspersky Endpoint Security: • **عدم مراقبة مكونات الحماية والتحكم**. تتم مراقبة نشاط التطبيق من خلال المكونات التالية: اكتشاف السلوك ومنع الاستغلال ومنع اختراق المضيف ومحرك المعالجة وجدار الحماية. • **عدم مراقبة Managed Detection and Response وEndpoint Detection and Response**. ويتم مراقبة نشاط التطبيق بواسطة عميل MDR مدمج وعميل EDR (KATA) مدمج. • **عدم اعتراض الإدخال التفاعلي لوحدة التحكم لحل Endpoint Detection and Response**. 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 مراقبة نشاط التطبيق التابع	لن يراقب Kaspersky Endpoint Security نشاط الملف ونشاط الشبكة للتطبيقات التي يتم بدء تشغيلها بواسطة التطبيق. ويمكنك تطبيق الاستثناء بشكل متكرر. بحيث لا يراقب التطبيق نشاط سلسلة التطبيقات التابعة بالكامل.

المعلمة	الوصف
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. ويمكنك تطبيق الاستثناء بشكل متكرر. بحيث لا يراقب التطبيق نشاط سلسلة التطبيقات التابعة بالكامل.
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 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. لا يدعم الإصدار 14.0 أو الإصدارات الأقدم من Kaspersky Endpoint Security استثناء حركة الشبكة إذا تم تحديد تجزئة لتطبيق موثوق به بدلاً من المسار.
عدم اعتراض تعديلات الملف (متوفر فقط في Kaspersky Security Center Console)	لا يراقب Kaspersky Endpoint Security التغييرات في الملفات من نطاق المراقبة مراقبة سلامة النظام. ويطبق التطبيق الاستثناء على جميع أوضاع مراقبة سلامة النظام: مراقبة سلامة النظام في الوقت الحقيقي والتحقق من سلامة النظام عند الحاجة.
عدم اعتراض تعديلات التسجيل (متوفر فقط في Kaspersky Security Center Console)	لا يراقب Kaspersky Endpoint Security التغييرات في مفاتيح التسجيل من نطاق المراقبة مراقبة سلامة النظام. ويطبق التطبيق الاستثناء على جميع أوضاع مراقبة سلامة النظام: مراقبة سلامة النظام في الوقت الحقيقي والتحقق من سلامة النظام عند الحاجة.
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.

إنشاء منطقة موثوقة محلية

يمكن للمستخدم الآن إنشاء المنطقة المحلية الموثوقة الخاصة به لجهاز كمبيوتر معين. وبهذه الطريقة، يستطيع المستخدم إنشاء قوائم محلية من استثناءات الفحص والتطبيقات الموثوقة الخاصة به بالإضافة إلى المنطقة العامة الموثوقة في سياسة ما. ويستطيع المسؤول باستخدام الاستثناءات المحلية أو التطبيقات الموثوقة المحلية أو منعها في إعدادات السياسة. ولفعل ذلك، استخدم خانتي الاختيار **السماح باستخدام الاستثناءات المحلية** و**السماح باستخدام التطبيقات الموثوقة المحلية** في قسم **الاستثناءات** من السياسة.

إذا كان المسؤول يسمح بإنشاء منطقة محلية موثوقة، يستطيع المستخدم إضافة استثناءات الفحص الخاصة به والتطبيقات الموثوقة في واجهة المستخدم الخاصة بالتطبيق. وفي الوقت نفسه، ليس لدى المستخدم أذونات لتعديل الكائنات أو حذفها من المنطقة الموثوقة التي تم تكوينها في السياسة. ويمكن للمسؤول أيضًا عرض عناصر القائمة أو إضافتها أو تعديلها أو حذفها في وحدة تحكم Kaspersky Security Center إذا كانت هناك حاجة إلى إضافة الاستثناءات لجهاز كمبيوتر فردي.

يخفي Kaspersky Endpoint Security قوائم استثناءات الفحص والتطبيقات الموثوقة في واجهة المستخدم الخاصة بالتطبيق إذا تم حظر تكوين المنطقة الموثوقة بواسطة المسؤول في وحدة التحكم (رمز "القفل المغلق") وتم حظر استثناءات الفحص المحلية والتطبيقات الموثوقة.

كيفية إضافة كائن إلى المنطقة الموثوقة في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في مجلد **Managed devices** 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 **Devices**.

4. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.

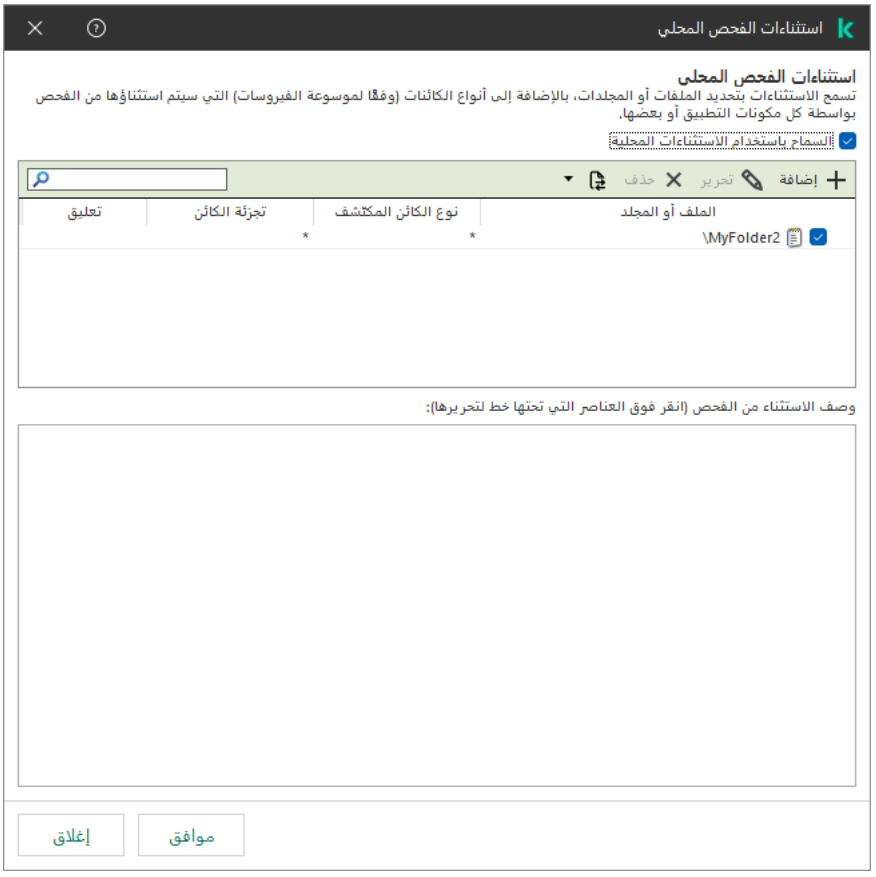
5. من نافذة خصائص الكمبيوتر، حدد القسم **Applications**.

6. في قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر، حدد **Kaspersky Endpoint Security for Windows (14.2)** وانقر نقرًا مزدوجًا لفتح خصائص التطبيق.

7. في نافذة إعدادات التطبيق، اختر **الإعدادات العامة ← الاستثناءات وأنواع الكائنات**.

8. في القسم **استثناءات الفحص والتطبيقات الموثوقة ← استثناءات الفحص المحلي**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تحتوي على قائمة الاستثناءات المحلية.



إعدادات المنطقة الموثوقة

9. أنشئ قائمة باستثناءات الفحص المحلي.

قواعد إنشاء استثناءات الفحص المحلي هي نفسها الخاصة بالاستثناءات العامة. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع.

10. في القسم **استثناءات الفحص والتطبيقات الموثوقة ← التطبيقات الموثوقة المحلية**، انقر على الزر **الإعدادات**.

يفتح هذا نافذة تحتوي على قائمة بالتطبيقات الموثوقة المحلية.

11. أنشئ قائمة بالتطبيقات الموثوقة المحلية.

تعتبر قواعد إضافة التطبيقات إلى قائمة التطبيقات الموثوقة المحلية هي نفس قواعد الإضافة إلى القائمة العامة. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع.

12. احفظ تغييراتك.

كيفية إضافة كائن إلى المنطقة الموثوقة المحلية في Kaspersky Security Center Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management ← Assets (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 **General settings ← Exclusions and types of detected objects**.

7. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Local scan exclusions**.

8. أنشئ قائمة باستثناءات الفحص المحلي.

تعتبر قواعد إنشاء الاستثناءات المحلية هي نفسها قواعد إنشاء الاستثناءات العامة. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع.

9. في القسم **Scan exclusions and trusted applications**، انقر على الرابط **Local trusted applications**.

10. أنشئ قائمة بالتطبيقات الموثوقة المحلية.

تعتبر قواعد إضافة التطبيقات إلى قائمة التطبيقات الموثوقة المحلية هي نفس قواعد الإضافة إلى القائمة العامة. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع.

11. احفظ تغييراتك.

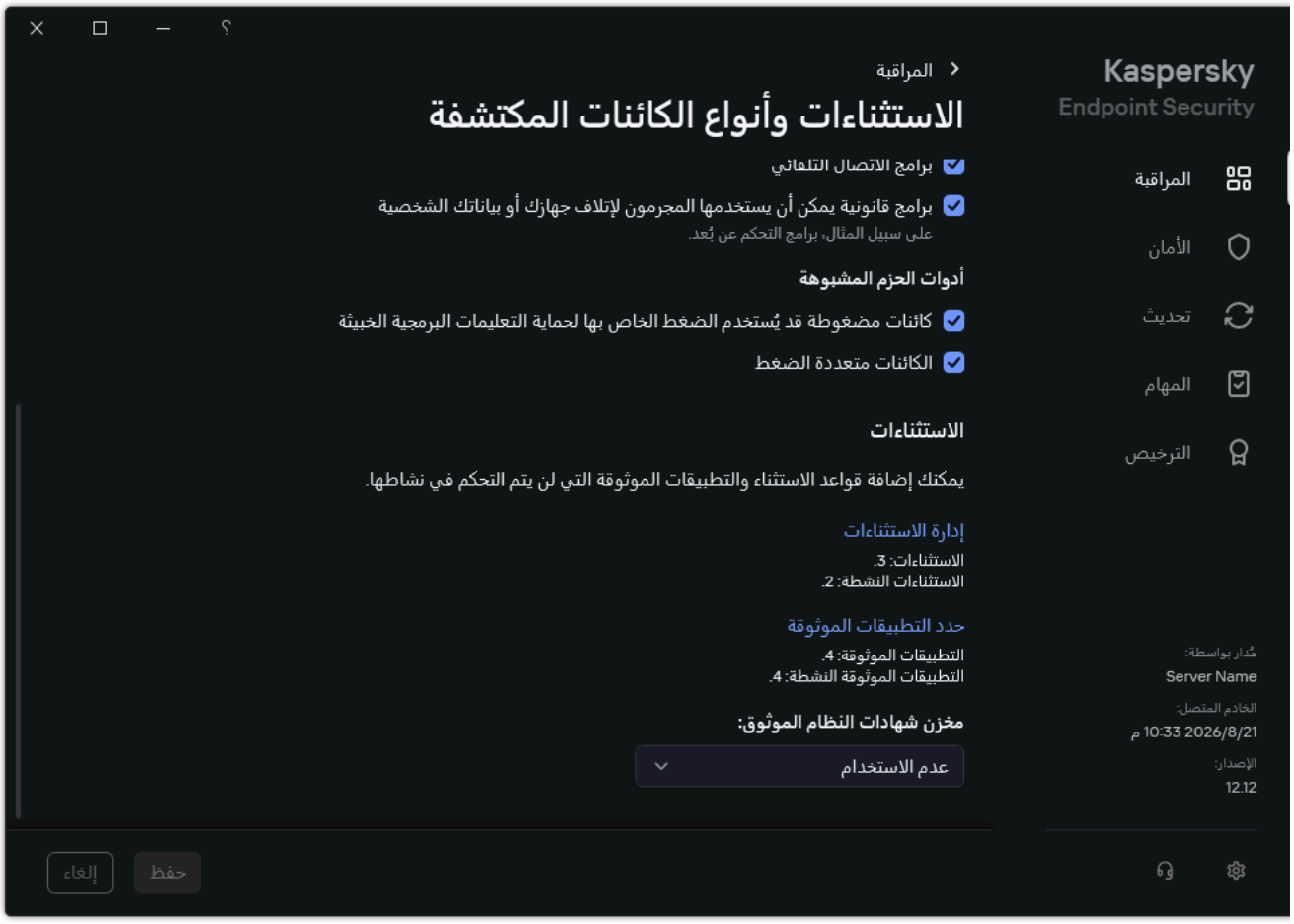
كيفية إنشاء استثناء فحص محلي في واجهة التطبيق

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**.

يخفي Kaspersky Endpoint Security قائمة استثناءات الفحص في واجهة المستخدم الخاصة بالتطبيق إذا تم حظر تكوين استثناءات الفحص بواسطة المسؤول في وحدة التحكم (رمز "القفل المغلق") وتم حظر استثناءات الفحص المحلية (تم إلغاء تحديد خانة الاختيار **السماح باستخدام الاستثناءات المحلية**).



إعدادات الاستثناءات

4. انقر فوق **إضافة** وحدد إجراءً:

- **الفئة**. يمكنك تجميع استثناءات الفحص في فئات منفصلة. ولإنشاء فئة جديدة، أدخل اسم الفئة وأضف استثناء فحص واحد على الأقل إلى الفئة.
- **استثناء جديد**. يضيف Kaspersky Endpoint Security استثناءً جديدًا للفحص إلى جذر القائمة.
- **تحديد الاستثناء من القائمة**. لتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق استثناءات الفحص المحددة مسبقًا. وتمت أيضًا إضافة استثناءات فحص محددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد استثناءات من الفحص محددة مسبقًا وفقًا للغرض من الخادم المحمي.

لإضافة استثناء من الفحص جديد إلى فئة محددة، حدد خانة الاختيار بجوار تلك الفئة وحدد الخيار **استثناء جديد**.

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 `?:\Users\*\Folder\`.

  يمكنك استثناء مجلدات الشبكة. ولفعل ذلك، أدخل المسار إلى مجلد الشبكة يدويًا (على سبيل المثال، `\\Network Share\*`).

6. إذا كنت ترغب في استثناء نوع معين من الكائنات من عمليات الفحص، في الحقل **نوع الكائن المكتَشف** أدخل اسم نوع 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.

7. إذا كنت ترغب في استثناء ملف فردي من عمليات الفحص، فأدخل تجزئة الملف في الحقل **تجزئة الكائن**.

   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.

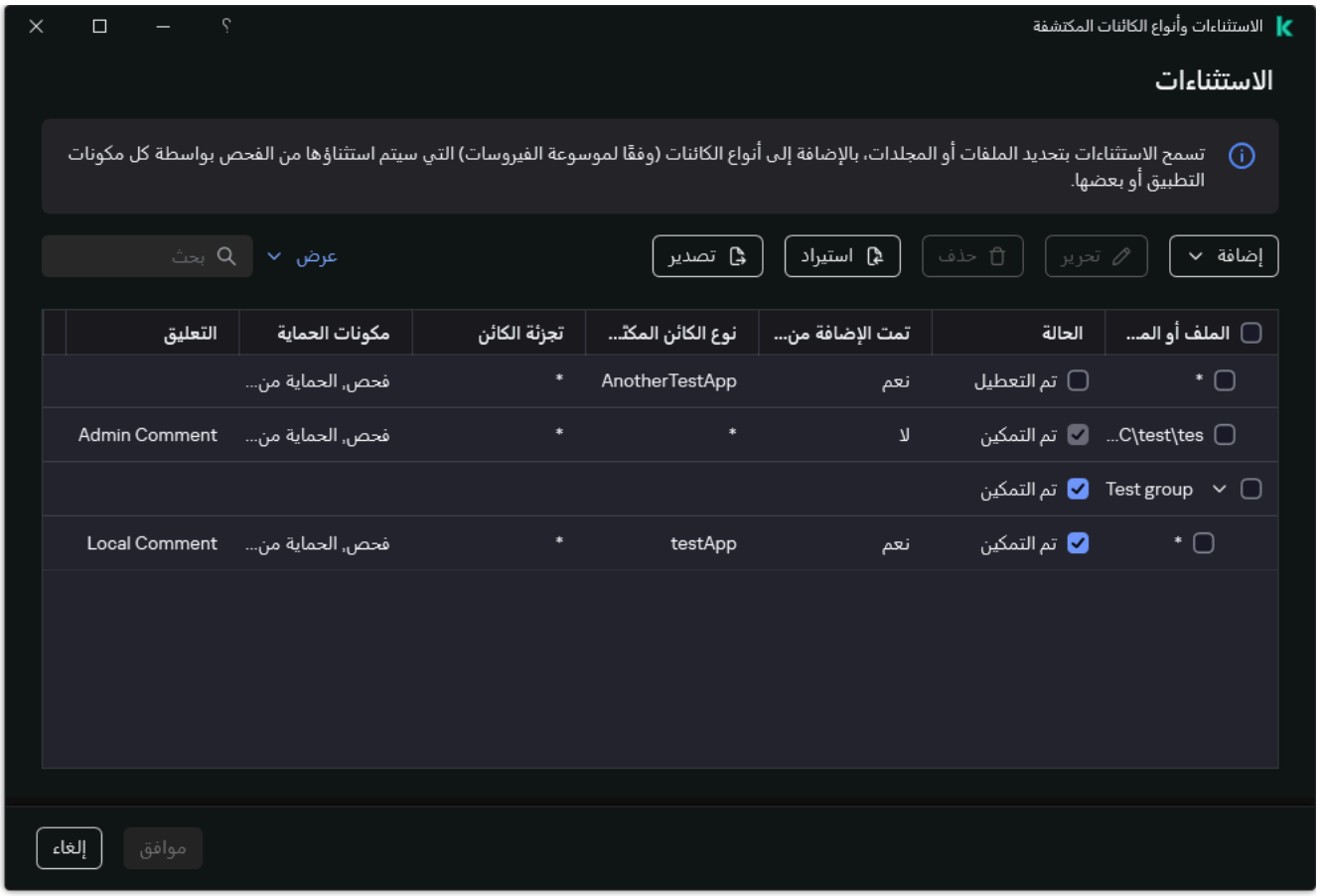
9. إذا لزم الأمر، في الحقل **التعليق**، أدخل تعليقًا مختصرًا على استثناء من الفحص الذي تقوم بإنشائه.

10. حدد الحالة **فعال** للاستثناء.

11. انقر على **إضافة**.

    ستتم إضافة الاستثناء الجديد إلى القائمة. ويمكنك تعطيل الاستثناء في أي وقت باستخدام خانة الاختيار الموجودة في عمود **الحالة**.

12. احفظ تغييراتك.

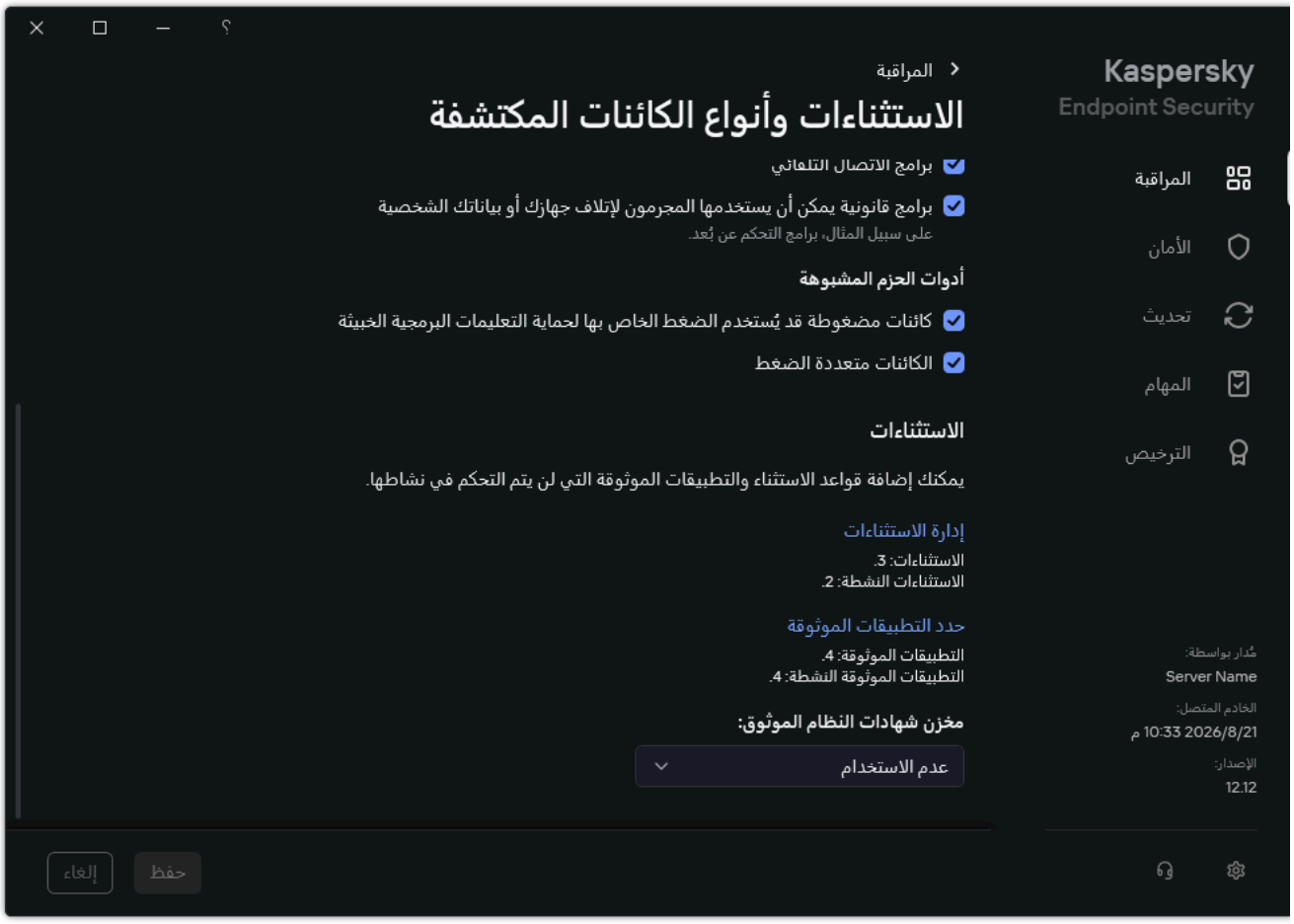


قائمة الاستثناءات

كيفية إضافة تطبيق إلى قائمة التطبيقات المحلية 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**.

يخفي Kaspersky Endpoint Security القائمة الموحدة للتطبيقات الموثوقة في واجهة المستخدم الخاصة بالتطبيق إذا تم حظر تكوين التطبيقات الموثوقة بواسطة المسؤول في وحدة التحكم (رمز "القفل المغلق") وتم حظر التطبيقات الموثوقة المحلية (تم إلغاء تحديد خانة الاختيار **السماح باستخدام التطبيقات الموثوقة المحلية**).



إعدادات الاستثناءات

4. انقر فوق **إضافة** وحدد إجراءً:

- **الفئة**. يمكنك تجميع التطبيقات الموثوقة في فئات منفصلة. لإنشاء فئة جديدة، أدخل اسم الفئة وأضف تطبيقًا موثوقًا واحدًا على الأقل إلى الفئة.
- **استثناء جديد**. يضيف Kaspersky Endpoint Security تطبيقًا موثوقًا جديدًا إلى جذر القائمة.
- **تحديد الاستثناء من القائمة**. ولتكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وSystem Center Configuration Manager، يتضمن التطبيق التطبيقات الموثوقة المحددة مسبقًا. وتمت أيضًا إضافة التطبيقات الموثوقة المحددة مسبقًا لدعم إعداد التطبيق في بيئات Citrix وVMware الافتراضية. ويجب تحديد التطبيقات الموثوقة المحددة مسبقًا وفقًا للغرض من الخادم المحمي.

لإضافة تطبيق موثوق جديد إلى فئة محددة، حدد خانة الاختيار بجوار تلك الفئة وحدد الخيار **استثناء جديد**.

5. حدد معايير الثقة:

- **استخدام مسار العملية الكامل على القرص لاعتباره موثوقًا**. أدخل مسار الملف القابل للتنفيذ الخاص بالتطبيق الموثوق به.

  يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و`?` عند إدخال قناع.

  يتعامل Kaspersky Endpoint Security مع اسم الملف الخاص بالتطبيق الموثوق به على أنه حساس لحالة الأحرف. وإذا كانت حالة أحرف اسم الملف الذي تدخله غير صحيحة، فلن يتعرف Kaspersky Endpoint Security على التطبيق الموثوق به.

- **استخدام تجزئة ملف العملية لاعتباره موثوقًا**.

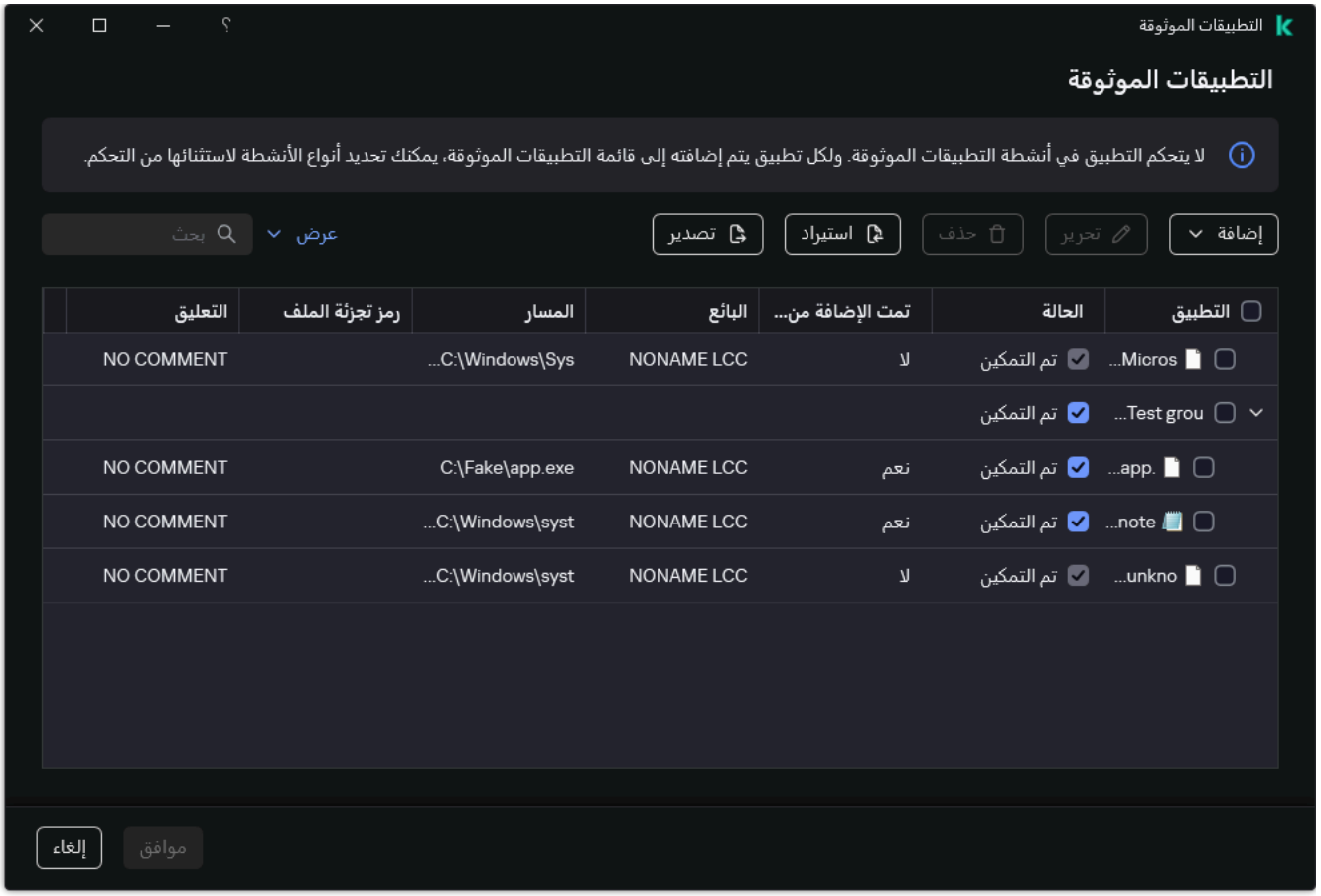
يدعم Kaspersky Endpoint Security متغيرات البيئة ويحول المسار في الواجهة المحلية للتطبيق. بعبارة أخرى، إذا أدخلت مسار الملف `%userprofile%\Documents\File.exe`، يتم إضافة سجل `C:\Users\Fred123\Documents\File.exe` في الواجهة المحلية للتطبيق للمستخدم Fred123. ووفقًا لذلك، يتجاهل Kaspersky Endpoint Security 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.

7. انقر على **موافق**.

ستتم إضافة التطبيق الموثوق الجديد إلى القائمة. ويمكنك استثناء تطبيق من المنطقة الموثوقة في أي وقت باستخدام خانة الاختيار في العمود **الحالة**.

8. احفظ تغييراتك.



قائمة التطبيقات 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 و trusted 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.

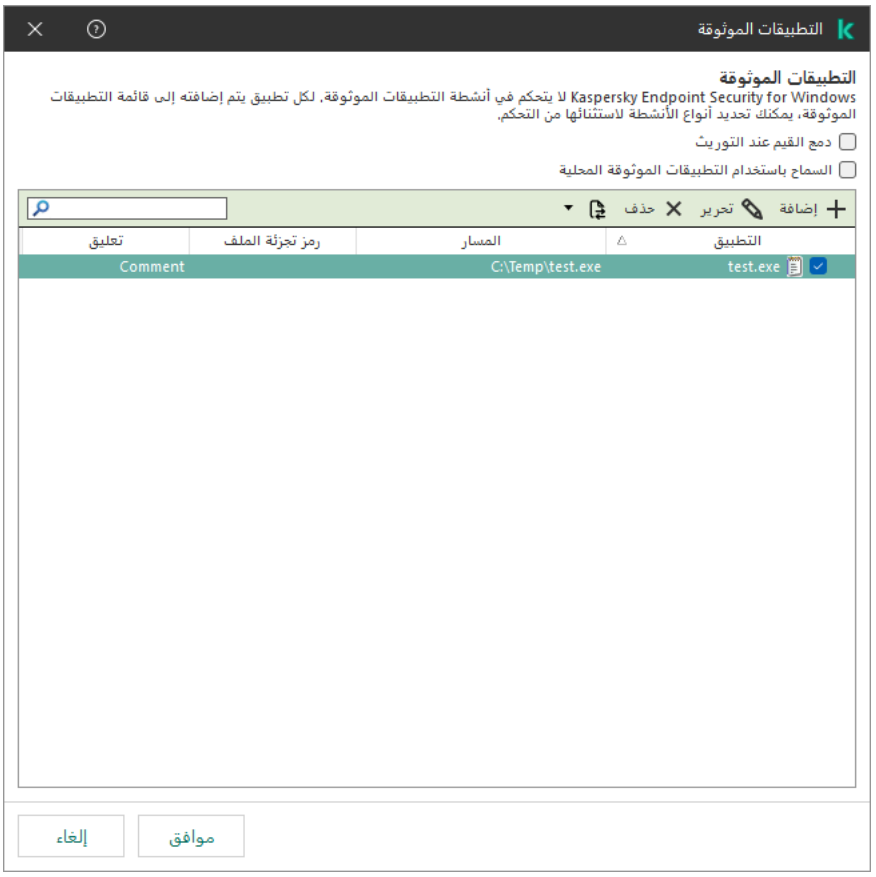
يستخدم Kaspersky Endpoint Security تنسيق XML لتصدير واستيراد قائمة التطبيقات الموثوقة.

كيفية تصدير واستيراد المنطقة الموثوقة في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.
4. تحت **استثناءات الفحص والتطبيقات الموثوقة**، حدد مكون المنطقة الموثوق بها التي تريد تصديرها أو استيرادها: **استثناءات الفحص** أو **التطبيقات الموثوقة**.
5. انقر على **الإعدادات**.
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 الزر ← **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. يدعم Kaspersky Endpoint Security أيضًا تصدير قائمة الاستثناءات إلى ملف DAT.



قائمة التطبيقات الموثوقة

7. لاستيراد قائمة الاستثناءات:

a. انقر على الزر ← **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. يدعم Kaspersky Endpoint Security أيضًا استيراد قائمة الاستثناءات من ملف DAT.

8. احفظ تغييراتك.

كيفية تصدير واستيراد المنطقة الموثوقة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى القسم **Trusted Zone**.

5. لتصدير قائمة القواعد:

a. انقر على رابط **Malware Scan exclusions**.

b. حدد الاستثناءات التي تريد تصديرها.

c. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات إلى ملف JSON في مجلد التنزيلات الافتراضي.

6. لتصدير قائمة التطبيقات الموثوقة:

a. حدد التطبيقات الموثوقة التي تريد تصديرها.

b. انقر على الزر ← **Export**.

يقوم Kaspersky Endpoint Security بتصدير قائمة التطبيقات الموثوقة إلى ملف JSON في مجلد التنزيلات الافتراضي.

7. لاستيراد قائمة الاستثناءات:

a. انقر على رابط **Malware Scan exclusions**.

b. انقر على الزر ← **Import**.

في النافذة التي تفتح، حدد ملف JSON 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 JSON.

8. لاستيراد قائمة التطبيقات الموثوقة:

a. انقر على رابط **Applications**.

b. انقر على الزر ← **Import**.

يفتح هذا نافذة، وفي تلك النافذة، حدد ملف JSON الذي ترغب في استيراد قائمة التطبيقات منه.

c. افتح الملف.

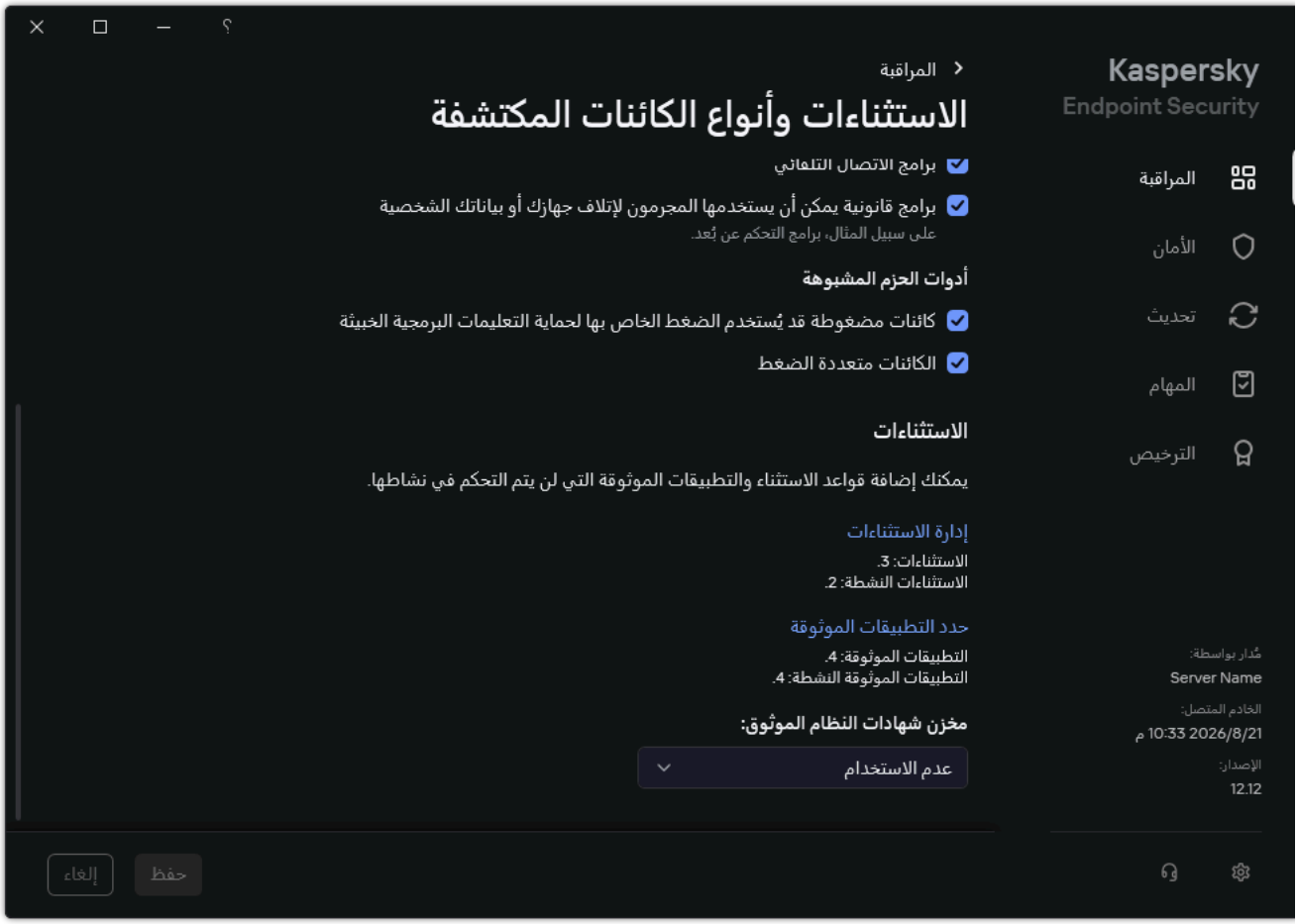
إذا كان جهاز الكمبيوتر يحتوي على قائمة تطبيقات موثوقة بالفعل، فسوف يطلب منك Kaspersky Endpoint Security حذف القائمة الحالية أو إضافة إدخالات جديدة إليها من ملف JSON.

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.

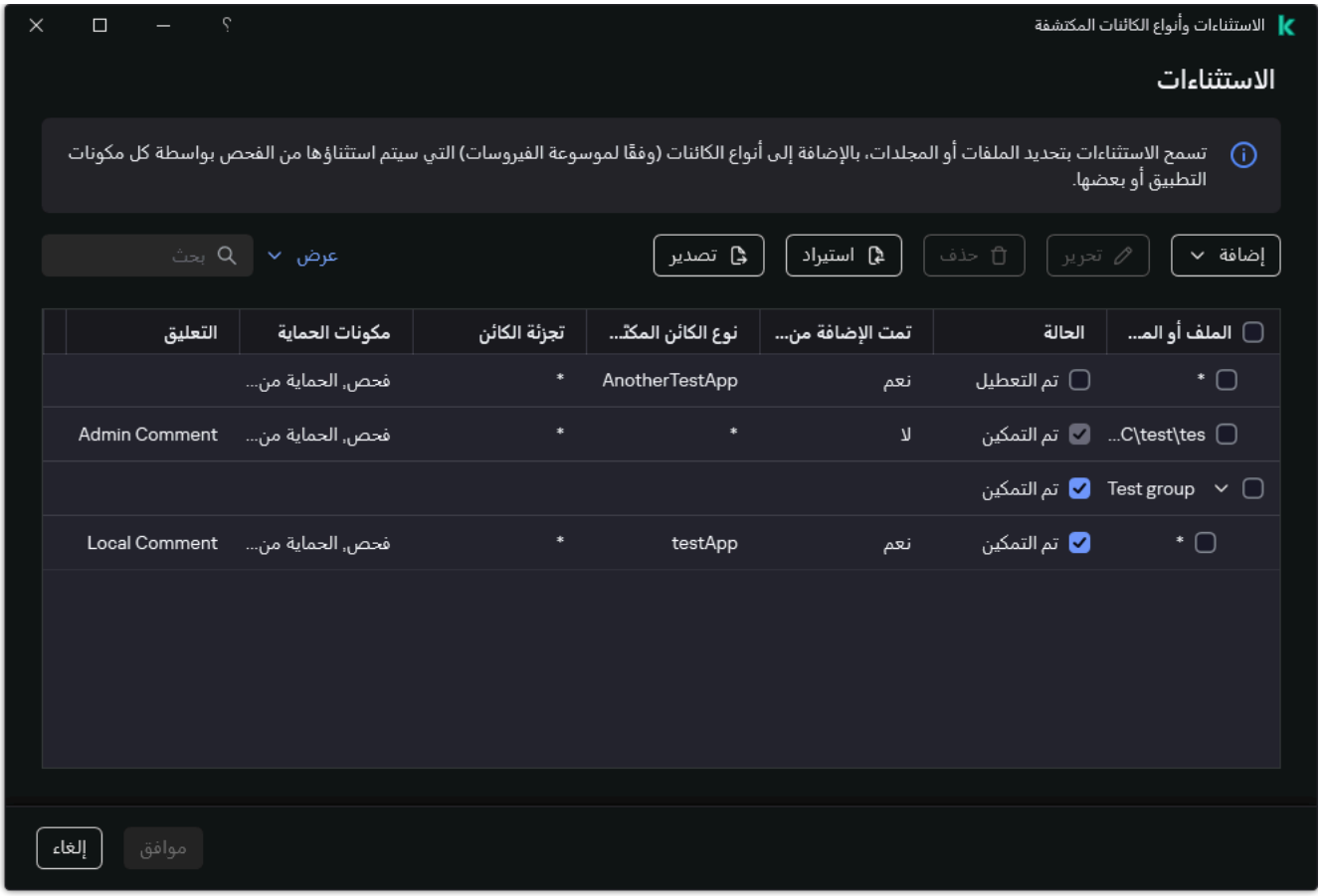
c. انقر على **تصدير**.

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.

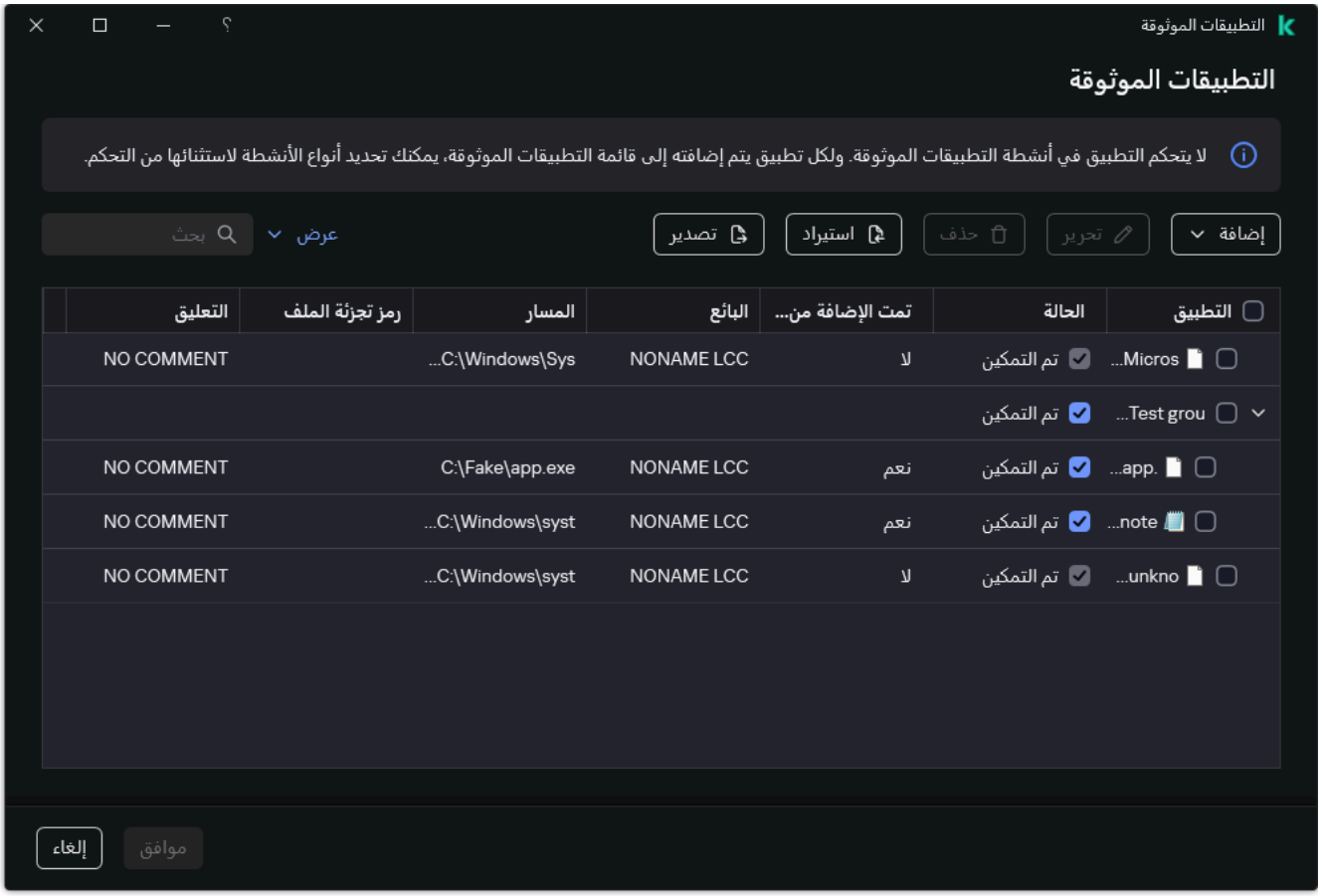
c. انقر على **تصدير**.

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.

التعامل مع التطبيقات بتوقيع رقمي موثوق

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 موثوق.

كيفية بدء استخدام مخزن شهادات نظام موثوق به في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.

4. في القسم **مخزن شهادات النظام الموثوق**، حدد خانة الاختيار **استخدام مخزن شهادات النظام الموثوق**.

5. في القائمة المنسدلة، حدد مخزن النظام الذي يجب وضعه في الاعتبار كموثوق به بواسطة Kaspersky Endpoint Security.

6. احفظ تغييراتك.

كيفية بدء استخدام تخزين شهادة نظام موثوق به في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى القسم **Trusted Zone**.

5. في النافذة التي تفتح، انقر فوق الرابط **Root certificates**.

6. في النافذة التي تفتح، حدد خانة الاختيار **Use trusted system certificate store**.

7. حدد متجر النظام الذي يجب اعتباره موثوقًا به بواسطة Kaspersky Endpoint Security.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية بدء استخدام مخزن شهادات نظام موثوق به 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 القائمة المنسدلة **مخزن شهادات النظام الموثوق**، حدد مخزن النظام الذي يجب وضعه في الاعتبار كموثوق بواسطة Kaspersky Endpoint Security.

4. احفظ تغييراتك.

الملحق. استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم. بدءًا من الإصدار Kaspersky Endpoint Security 12.8 for Windows، يمكنك تثبيت التطبيق في وضع Light Agent لحماية البيئات الافتراضية. ويمكن أن تساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في البيئات الافتراضية في Citrix وVMware

يمكنك تحديد الاستثناءات المحددة مسبقًا والتطبيقات الموثوقة بالطرق التالية:

- تثبيت التطبيق.
  - تثبيت التطبيق محليًا باستخدام المعالج
  - خصائص حزمة التثبيت
- تعيين السياسة.
  - معالج السياسة الجديد
  - خصائص السياسة: استثناءات الفحص والتطبيقات الموثوقة

Microsoft SQL Server

عند تثبيت Kaspersky Endpoint Security على خادم SQL، يجب عليك إنشاء منطقة موثوقة من الاستثناءات والتطبيقات الموثوقة المحددة مسبقًا للتأكد من عدم التدخل في تشغيل الخادم.

استثناءات الفحص المحددة مسبقًا

المسار	إصدار SQL
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
Data*.mdf*\?.%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL	2012
Data*.mdf*\?.%ProgramFiles%\Microsoft SQL Server\MSSQL	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
Data*.ldf*\?.%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL	2012
Data*.ldf*\?.%ProgramFiles%\Microsoft SQL Server\MSSQL	2012

إصدار SQL	المسار
2012 2014 2016 2017 2019 2022	%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf
2012 2014 2016 2017 2019 2022	%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf

Microsoft Exchange Server

عند تثبيت Kaspersky Endpoint Security على خادم Microsoft Exchange، يجب عليك إنشاء منطقة موثوقة من الاستثناءات والتطبيقات الموثوقة المحددة مسبقًا للتأكد من عدم التدخل في تشغيل الخادم.

استثناءات الفحص المحددة مسبقًا

إصدار Microsoft Exchange	المسار
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que
2013 2016 2019	C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl

التطبيقات الموثوقة المحددة مسبقًا

المسار	إصدار Microsoft Exchange
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

Microsoft System Center Configuration Manager

في حال تثبيت Microsoft System Center Configuration Manager في نظام تشغيل الكمبيوتر المحمي، ستحتاج إلى إضافة استثناء محدد مسبقًا إلى قائمة استثناءات الفحص لضمان التشغيل المستقر للحل.

استثناءات الفحص المحددة مسبقًا

المسار	إصدار مدير تكوين مركز النظام
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 R2 2012

Citrix

عند تثبيت Kaspersky Endpoint Security في بيئة Citrix الافتراضية، يجب عليك إنشاء منطقة موثوقة من الاستثناءات والتطبيقات الموثوقة المحددة مسبقًا للتأكد من عدم التدخل في تشغيل الخادم.

استثناءات الفحص المحددة مسبقًا

المسار
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys

المسار
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

التطبيقات الموثوقة المحددة مسبقًا

المسار	محلول Citrix
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	التطبيقات الافتراضية وأجهزة سطح المكتب

المسار	محلول Citrix
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%SystemRoot%\System32\drivers\CVhdFilter.sys	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\System32\ctxgfx.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	التطبيقات الافتراضية وأجهزة سطح المكتب

المسار	محلول Citrix
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	التطبيقات الافتراضية وأجهزة سطح المكتب
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	تطبيق مساحة العمل
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	تطبيق مساحة العمل
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	التزويد
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	التزويد
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	التزويد
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	التزويد
%SystemRoot%\System32\drivers\bnistack6.sys	التزويد
%SystemRoot%\System32\drivers\CfsDep2.sys	التزويد
%SystemRoot%\System32\drivers\cnicteam.sys	التزويد
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	التزويد

المسار	محلول Citrix
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	التزويد
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	التزويد
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	التزويد
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	التزويد
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

عند تثبيت Kaspersky Endpoint Security في بيئة افتراضية لبرنامج VMware، يجب عليك إنشاء منطقة موثوقة من التطبيقات الموثوقة المحددة مسبقًا للتأكد من عدم التدخل في تشغيل الخادم.

التطبيقات الموثوقة المحددة مسبقًا

المسار	حل VMware
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon

حل VMware	المسار
Horizon	C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe
Horizon	C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe
Horizon	C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe
Horizon	C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe
Horizon	C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe
Horizon	C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe
Horizon	C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe
Horizon	C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe
Horizon	C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe
Horizon	C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe
Horizon	C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe
Horizon	C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe
Horizon	C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe
Horizon	C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe
Horizon	C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe
Horizon	C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe

إلغاء البيانات المكررة في Microsoft Windows Server

في حالة تمكين إلغاء البيانات المكررة في نظام التشغيل Microsoft Windows Server الذي تم تثبيت Kaspersky Endpoint Security عليه، ستحتاج إلى تطبيق موثوق محدد مسبقًا في القائمة موثوق لتحسين Kaspersky Endpoint Security وتقليل حمل وحدة المعالجة المركزية.

التطبيقات الموثوقة المحددة مسبقًا

إصدار Microsoft Windows Server	المسار
كل الإصدارات المدعومة	%SystemRoot%\system32\fsdmhost.exe

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.14.2\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، تحت **الإعدادات العامة** انقر فوق لوحة **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 **النسخ الاحتياطي**. 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، تحت **الإعدادات العامة** انقر فوق لوحة **التقارير والمخزن**.



إعدادات النسخ الاحتياطي

3. في القسم **النسخ الاحتياطي**، 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 لم يتم التنظيف 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 Windows Store باستخدام أدوات المناسبة لنظام التشغيل (راجع ملفات تعليمات Microsoft Windows للحصول على تفاصيل عند استعادة تطبيق Windows Store).

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 **النسخ الاحتياطي**.
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.



النسخ الاحتياطي

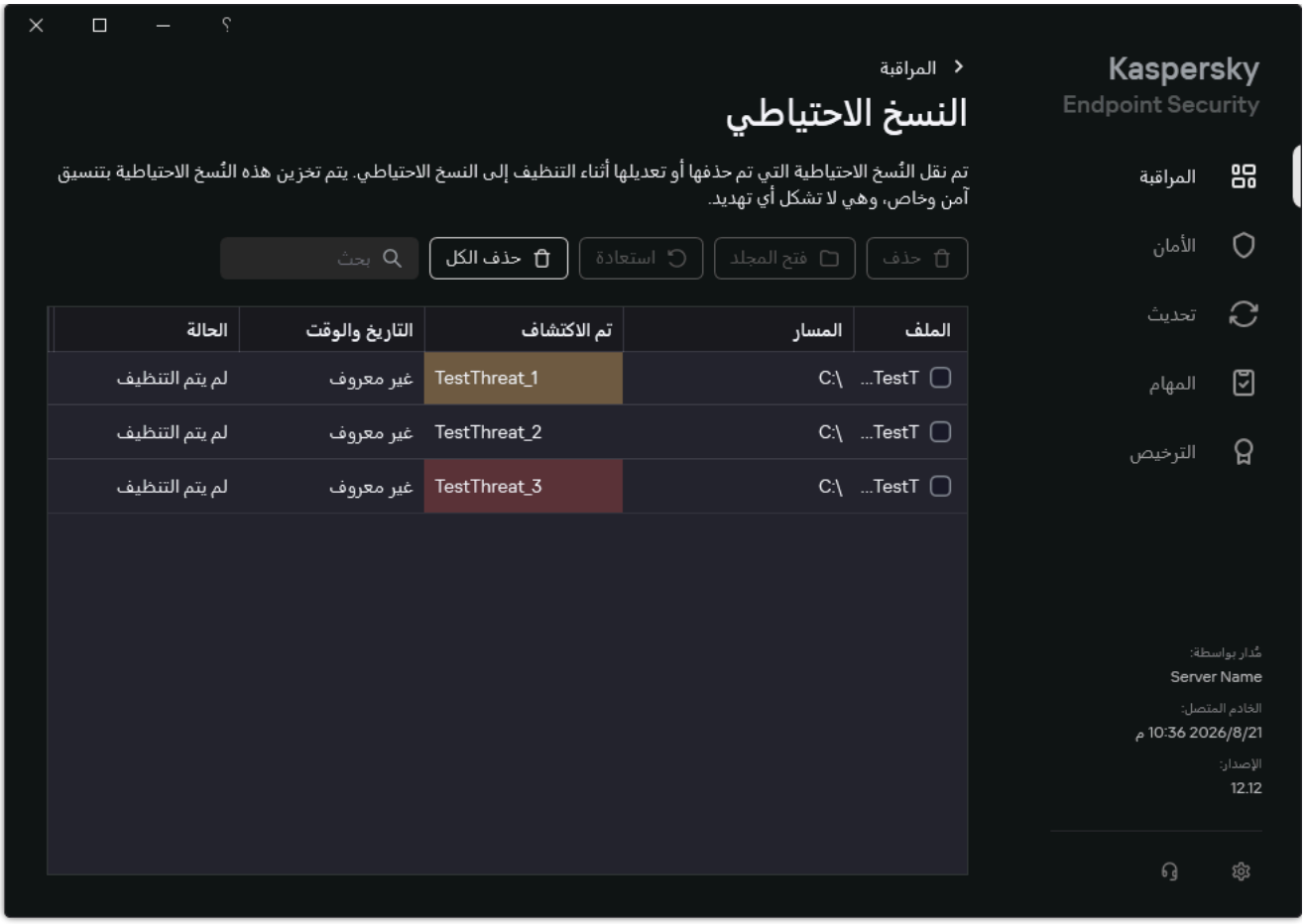
حذف النسخ الاحتياطية للملفات من النسخ الاحتياطي

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 **النسخ الاحتياطي**.
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.



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 **تكوين الإخطارات**.

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 **تكوين الإخطارات**.

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 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 **تكوين الإخطارات عبر 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 **Administration Server** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **Events**.

   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 **Event selections**، حدد **User requests**.
4. حدد الرسالة التي تم إرسالها إلى المسؤول.
5. انقر فوق الزر **Open event properties window** 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.14.2\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.

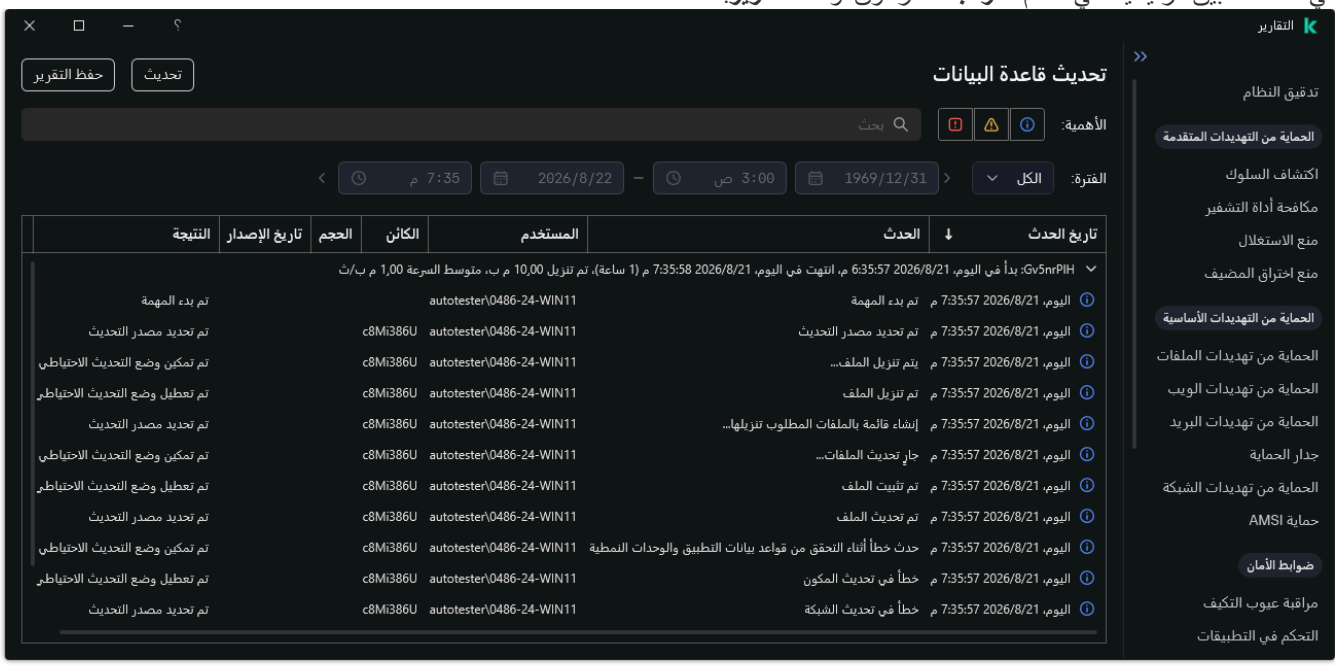
إذا كان Kaspersky Endpoint Security يعمل تحت إدارة Kaspersky Security Center، فإن المعلومات المتوفرة عن الأحداث قد تُرحل إلى خادم إدارة Kaspersky Security Center (للمزيد من التفاصيل، يرجى الرجوع إلى تعليمات Kaspersky Security Center).

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.

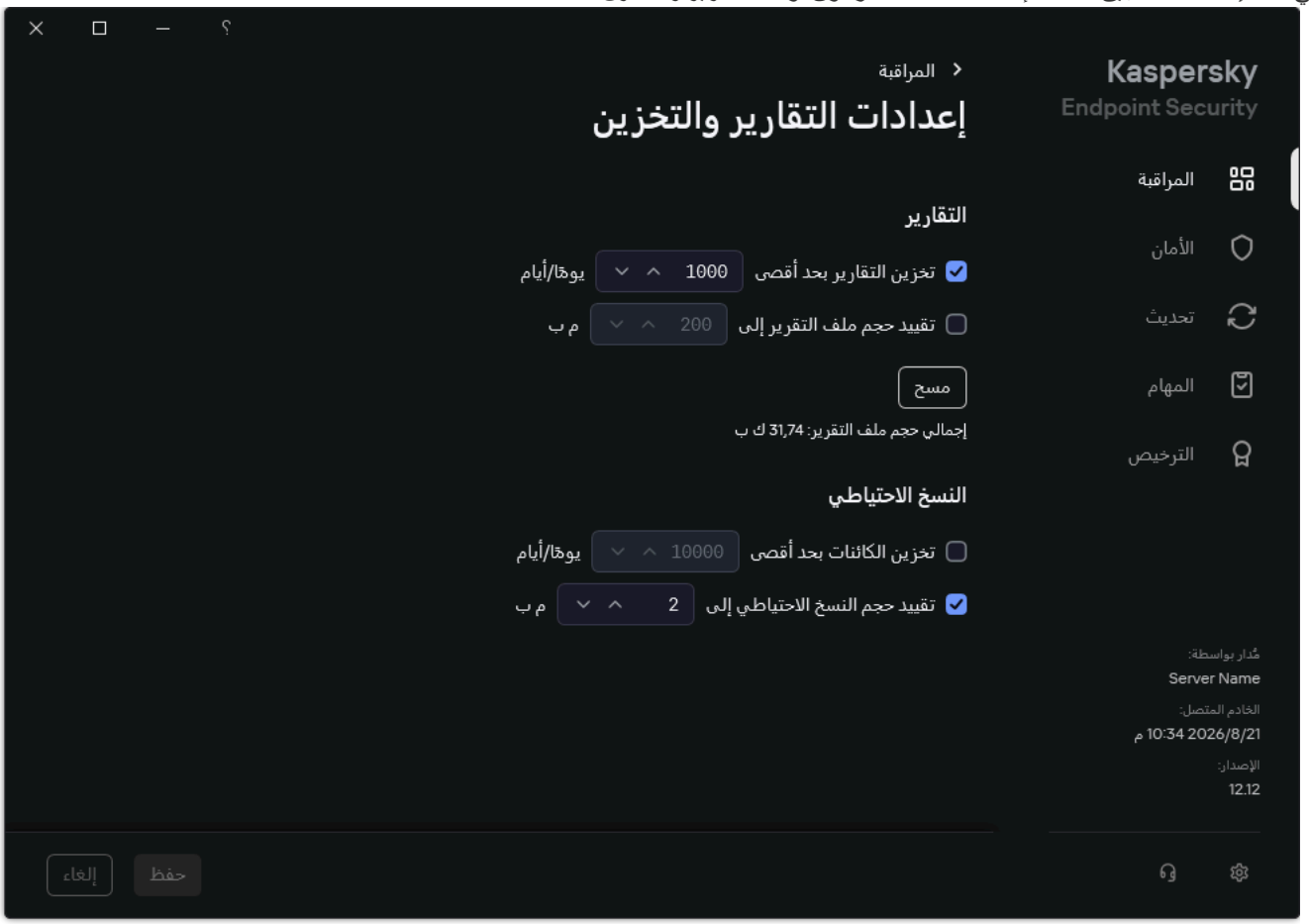
تكوين الفترة الزمنية القصوى لتخزين التقرير

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، تحت **الإعدادات العامة** انقر فوق لوحة **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، تحت **الإعدادات العامة** انقر فوق لوحة **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

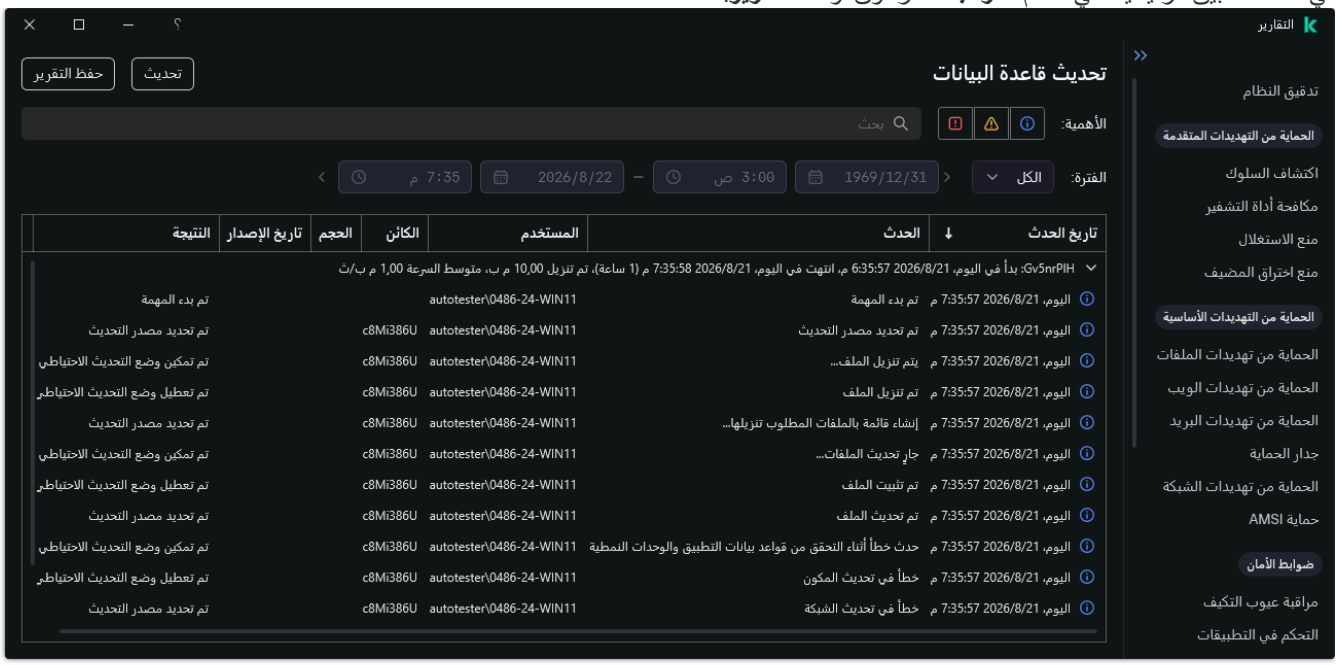
يتحمل المستخدم شخصيًا مسؤولية ضمان أمن المعلومات من تقرير تم حفظه إلى ملف، وخاصة لمراقبة وتقييد الوصول إلى هذه المعلومات.

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.

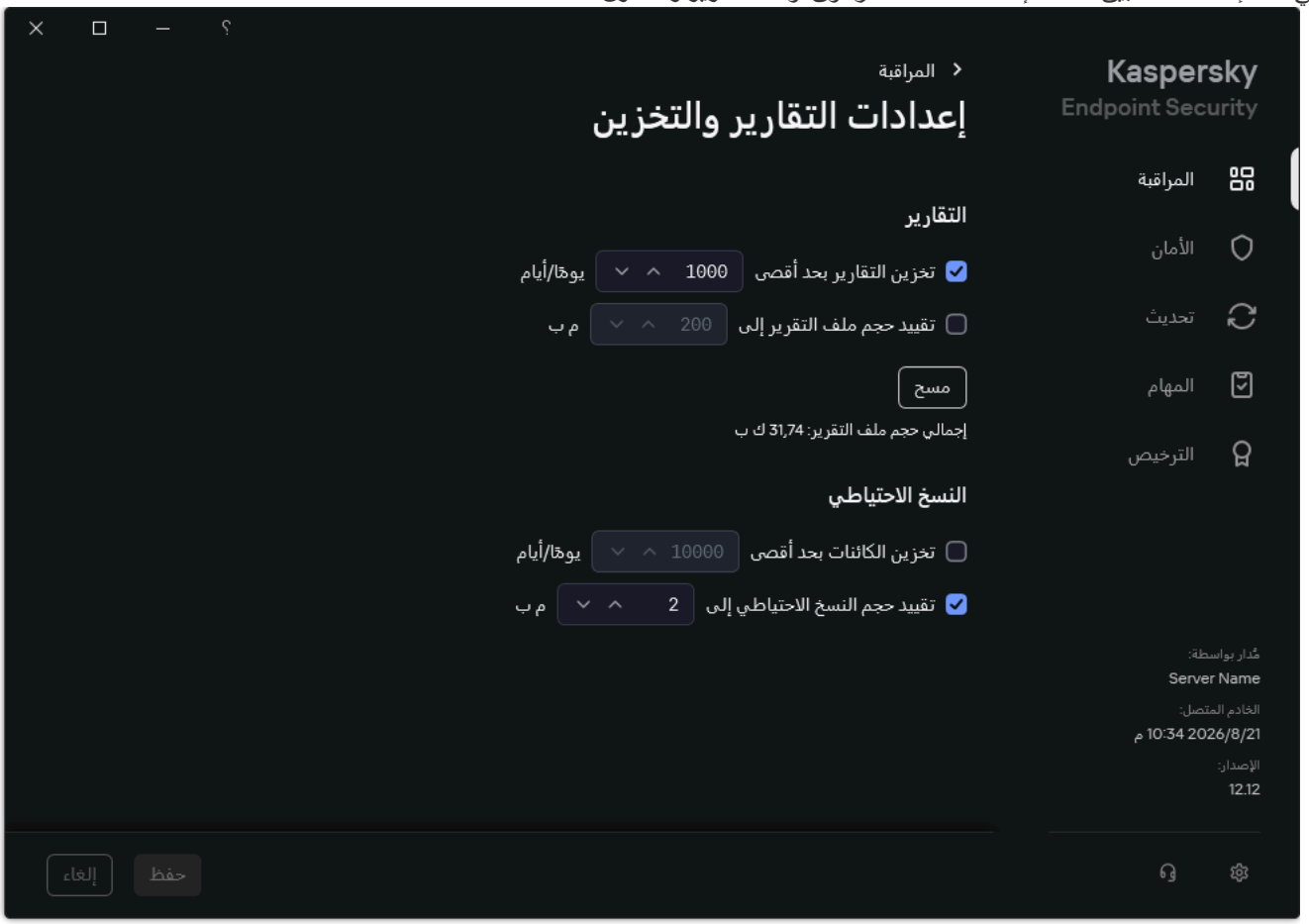
8. احفظ تغييراتك.

مسح التقارير

لإزالة معلومات من التقارير:

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

2. في نافذة إعدادات التطبيق، تحت **الإعدادات العامة** انقر فوق لوحة **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). يتضمن الدفاع الذاتي أيضًا الحماية بكلمة مرور وحماية اتصال خادم الإدارة.

تتيح لك الحماية بكلمة المرور تقييد وصول المستخدمين إلى Kaspersky Endpoint Security طبقا للأذونات الممنوحة لهم (على سبيل المثال، إذن الخروج من التطبيق).

تمنع حماية اتصال خادم الإدارة إعادة الاتصال غير المصرح به للكمبيوتر بخادم غير موثوق به.

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 التطبيقات الأخرى (على سبيل المثال، TeamViewer أو RemotelyAnywhere) من الوصول إلى Kaspersky Endpoint Security.	✓	– (باستثناء Windows 7)

تمكين وتعطيل الدفاع الذاتي

يمنع Kaspersky Endpoint Security أي تغيير أو حذف لملفات التطبيق على محرك الأقراص الثابت وعمليات الذاكرة وإدخالات تسجيل النظام.
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.

لا تنطبق آليات الدفاع الذاتي على عمليات Kaspersky Endpoint Security التي تبدأها عمليات أصلية غير موثوقة.

يتم تمكين آلية الدفاع الذاتي ببرنامج Kaspersky Endpoint Security افتراضيًا.

كيفية تمكين أو تعطيل الدفاع الذاتي في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.

4. استخدم خانة الاختيار **تمكين الدفاع الذاتي** لتمكين أو تعطيل آلية الدفاع الذاتي.

5. احفظ تغييراتك.

كيفية تمكين أو تعطيل الدفاع الذاتي في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **General Settings** ← **Self-Defense**.

5. استخدم مفتاح التبديل **Self-Defense ENABLED** لتمكين أو تعطيل آلية الدفاع الذاتي.

6. احفظ تغييراتك.

كيفية تمكين أو تعطيل الدفاع الذاتي 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 **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.

استخدم تقنية AM-PPL بشكل مستمر. وتعد تقنية AM-PPL عنصرًا مهمًا في حماية نظام التشغيل. وقد يؤدي تعطيل دعم AM-PPL إلى فشل بعض ميزات Kaspersky Endpoint Security (على سبيل المثال، تكامل التطبيق مع Windows Security Center). ولا يُسمح بتعطيل دعم AM-PPL إلا في بيئة اختبار منفصلة لأغراض استكشاف الأخطاء وإصلاحها.

إن تقنية AM-PPL متاحة للإصدار 1703 من نظام التشغيل Windows 10 (RS2) أو إصدار أحدث، ونظام التشغيل Windows Server 2019.

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.

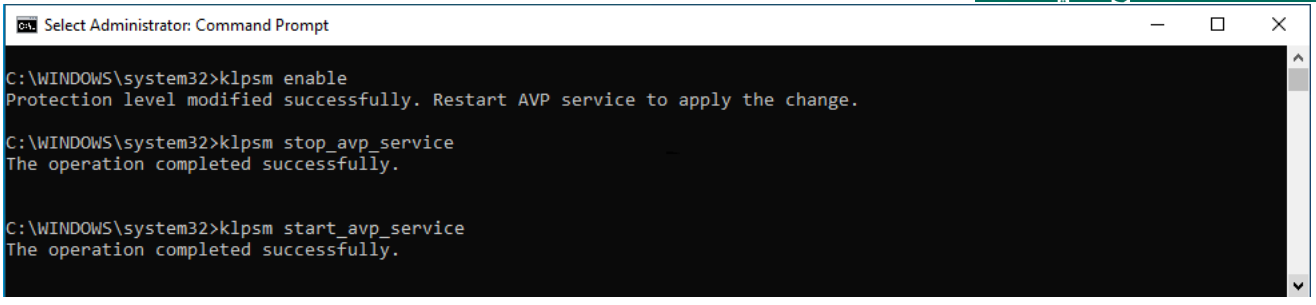
3. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.
يمكنك إضافة مسار إلى الملف القابل للتنفيذ إلى متغير النظام %PATH% أثناء تثبيت التطبيق.

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.KES.14.2)
- خدمة Kaspersky Seamless Update Service (AVPSUS.KES.14.2)

لإيقاف التطبيق من سطر الأوامر، قم بتعطيل حماية خدمات Kaspersky Endpoint Security من الإدارة الخارجية.

يمكنك السماح بالإدارة الخارجية لخدمات التطبيق فقط على أجهزة الكمبيوتر التي لا تدعم تقنية AM-PPL أو أجهزة الكمبيوتر التي تم تعطيل التقنية عليها.

كيفية تمكين أو تعطيل حماية خدمات التطبيقات من الإدارة الخارجية في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.
4. استخدم مربع الاختيار **منع الإدارة الخارجية لخدمات التطبيق** لتمكين أو تعطيل حماية خدمات Kaspersky Endpoint Security من الإدارة الخارجية.
5. احفظ تغييراتك.

كيفية تمكين أو تعطيل حماية خدمات التطبيقات من الإدارة الخارجية في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Self-Defense**.
5. استخدم مربع الاختيار **Block external management of application services** لتمكين أو تعطيل حماية خدمات Kaspersky Endpoint Security من الإدارة الخارجية.
6. احفظ تغييراتك.

كيفية تمكين أو تعطيل حماية خدمات التطبيقات من الإدارة الخارجية في واجهة التطبيق

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

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

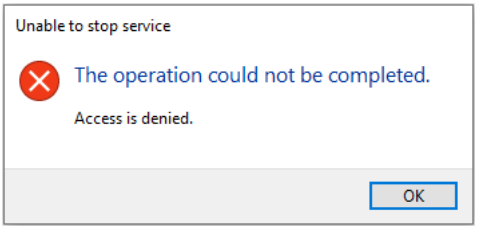


إعدادات Kaspersky Endpoint Security for Windows

3. استخدم مربع الاختيار **منع الإدارة الخارجية لخدمات التطبيق** 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.



خطأ في الوصول إلى خدمات التطبيقات

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.

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. وإذا لم يكن الكمبيوتر موجودًا في المجال، فيمكنك استخدام حساب KLAdmin أو حساب تمت إضافته يدويًا.

- أدخل كلمة مرور مؤقتة.

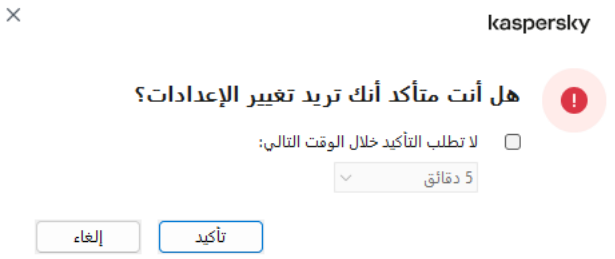
هذه الطريقة ملائمة لمنح أذونات مؤقتة لتنفيذ الإجراءات المحظورة (على سبيل المثال، الخروج من التطبيق) للمستخدمين خارج شبكة الشركة. عند انتهاء صلاحية كلمة مرور مؤقتة أو انتهاء جلسة، سيعيد Kaspersky Endpoint Security الإعدادات الخاصة به إلى حالتها السابقة.

- رمز مميز.

هذه الطريقة مناسبة للمستخدمين ذوي الامتيازات (مثل موظفي الدعم الفني). وتتيح المصادقة باستخدام الرمز المميز استخدام وضع تسجيل الدخول بالبطاقة الذكية في Active Directory. ويؤدي ذلك إلى تحسين أمان البنية التحتية للمؤسسة.

عندما يحاول المستخدم تنفيذ إجراء محمي بكلمة مرور، يطالبه Kaspersky Endpoint Security بإدخال اسم مستخدم وكلمة مرور، أو كلمة مرور الرمز المميز، أو كلمة مرور مؤقتة (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 الحساب. 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.
- **تمت إضافة الحساب يدويًا**. حساب خارج مجال Active Directory. ويمكنك استخدام حساب الخدمة هذا بدلاً من KLAdmin إذا كنت لا ترغب في مشاركة كلمة مرور المسؤول. ويمكنك تعيين أي اسم مستخدم وكلمة مرور وتكوين الأذونات الفردية.
- **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.

رمز مميز

للوصول إلى وظائف Kaspersky Endpoint Security، يجب عليك تحديد شهادة المستخدم المناسبة من قائمة الشهادات المخزنة على الرمز المميز المتصل وإدخال رمز PIN الخاص بك. وتتوفر المصادقة المستندة إلى رمز مميز فقط للمستخدمين داخل مجال Active Directory. ويستطيع المسؤول تكوين الأذونات لمستخدم فردي أو مجموعة. لكي تعمل المصادقة المستندة إلى الرمز المميز، يجب عليك نشر بنية تحتية موثوقة للمفتاح العام (PKI) وتثبيت برنامج مخصص لإدارة الرمز المميز.

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).

كيفية تمكين الحماية بكلمة مرور في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **الواجهة**.
4. في القسم **الحماية بكلمة مرور**، انقر على الزر **الإعدادات**.
   يفتح هذا نافذة تتضمن إعدادات الحماية بكلمة مرور.
5. استخدم خانة الاختيار **تمكين الحماية بكلمة مرور** لتمكين المكون أو تعطيله.
6. تحت **الأذونات**، حدد حساب KLAdmin.
7. يفتح هذا نافذة؛ وفي تلك النافذة، انقر فوق **كلمة المرور** وقم بتعيين كلمة مرور لحساب KLAdmin.
   لحساب KLAdmin الحق في اتخاذ أي إجراء محمي بكلمة مرور.

> إذا نسيت كلمة مرور حساب KLAdmin، فيمكنك إعادة تعيين كلمة المرور في خصائص السياسة.

8. ارجع إلى قائمة الحسابات.
9. تعيين/حدد الأذونات لجميع المستخدمين داخل شبكة الشركة المحلية:
   a. تحت **الأذونات**، حدد مجموعة "الكل".
      مجموعة "الكل" هي مجموعة Windows مدمجة والتي تتضمن جميع المستخدمين داخل شبكة الشركة.
   b. في النافذة التي فتحت، 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.

10. احفظ تغييراتك.

كيفية تمكين الحماية بكلمة مرور في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Self-Defense**.
5. تحت **Password Protection**، استخدم مفتاح التبديل **Password Protection ENABLED** لتمكين المكون أو تعطيله.
6. حدد كلمة المرور الخاصة بحساب KLAdmin وقم بتأكيدها.
   لحساب KLAdmin الحق في اتخاذ أي إجراء محمي بكلمة مرور.

إذا نسيت كلمة مرور حساب KLAdmin، فيمكنك إعادة تعيين كلمة المرور في خصائص السياسة.

7. ارجع إلى قائمة الحسابات.
8. تعيين/حدد الأذونات لجميع المستخدمين داخل شبكة الشركة المحلية:
   a. في جدول الحسابات، حدد مجموعة "الكل".
   مجموعة "الكل" هي مجموعة Windows مدمجة والتي تتضمن جميع المستخدمين داخل شبكة الشركة.
   b. في النافذة التي فتحت، 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 **Exit the application**، 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.

9. احفظ تغييراتك.

كيفية تمكين الحماية بكلمة مرور في واجهة التطبيق

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

تسمح حماية كلمة المرور بمنح Kaspersky Endpoint Security حق الوصول إلى حسابات مستخدمي Active Directory الفردية وحسابات المستخدمين المضافة يدويًا.

حسابات مستخدمي Active Directory

يمكنك منح Kaspersky Endpoint Security حق الوصول لمستخدمين فرديين أو مجموعات داخل مجال Active Directory. 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.

إضافة حسابات المستخدمين يدويًا

يمكنك إنشاء حساب مستخدم غير موجود في Active Directory وتعيين أذونات فردية لحساب المستخدم هذا. أي أنه يمكنك إنشاء حساب مستخدم الخدمة واستخدامه بدلاً من KLAdmin. وبهذه الطريقة، لن تحتاج إلى مشاركة كلمة مرور KLAdmin الخاصة بك مع مستخدمين آخرين أو إنشاء حسابات مستخدم Active Directory جديدة. ويمكنك تحديد أي اسم مستخدم وكلمة مرور. على سبيل المثال، يمكنك منح إذن **عرض التقارير** إلى حساب مستخدم الخدمة. ونتيجة لذلك، إذا كان عرض التقارير محظورًا على مجموعة "الكل"، فيمكنك فتح التقارير باستخدام حساب مستخدم الخدمة أو حساب مستخدم KLAdmin.

منح أذونات للمستخدمين الأفراد أو المجموعات

كيفية منح الأذونات للمستخدمين الفرديين أو المجموعات في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **الواجهة**.
4. في القسم **الحماية بكلمة مرور**، انقر على الزر **الإعدادات**.
   يفتح هذا نافذة تتضمن إعدادات الحماية بكلمة مرور.
5. في جدول الحساب، انقر فوق **إضافة**.
6. حدد نوع حساب المستخدم الذي تريد إضافته:
   - **تحديد مستخدم / مجموعة من Active Directory** – حسابات مستخدمي Active Directory.
     لتحديد حساب مستخدم، انقر فوق **تحديد**. حدد مستخدم أو مجموعة في Active Directory وقم بتأكيد اختيارك.
   - **إضافة مستخدم / مجموعة مستخدمين يدويًا** لحساب مستخدم خدمة مضاف يدويًا.
     لإضافة حساب مستخدم خدمة، أدخل اسم مستخدم وكلمة مرور (على سبيل المثال، SecureAdmin).

يمكنك إعادة تعيين كلمة مرور حساب مستخدم الخدمة في إعدادات السياسة. ويجب إعادة تعيين كلمة مرور حساب مستخدم الخدمة بالطريقة ذاتها لكلمة مرور KLAdmin. إذا كان تحرير إعدادات حماية كلمة المرور مسموحًا به (يكون "القفل" مفتوحًا) أو لم يتم تطبيق أي سياسة على الكمبيوتر، فيمكنك إعادة تعيين كلمة المرور لحساب مستخدم الخدمة في واجهة التطبيق. للقيام بذلك، قم بتأكيد التغييرات في معلومات حساب مستخدم الخدمة باستخدام كلمة مرور KLAdmin.

7. 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.

8. احفظ تغييراتك.

كيفية منح الأذونات للمستخدمين الفرديين أو المجموعات في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **General Settings** ← **Self-Defense**.

5. في القسم **Password Protection**، انقر على الرابط **User permissions**.
يؤدي ذلك إلى فتح نموذج لمنح أذونات تمكين كلمة المرور.

6. انقر على **Add**.

7. حدد نوع حساب المستخدم الذي تريد إضافته:

- **Select from Active Directory** – حسابات مستخدمي Active Directory.
لتحديد حساب مستخدم، انقر فوق **Edit**. حدد مستخدم أو مجموعة في Active Directory وقم بتأكيد اختيارك.
- **Add manually** لحساب مستخدم خدمة مضاف يدويًا.
لإضافة حساب مستخدم خدمة، أدخل اسم مستخدم وكلمة مرور (على سبيل المثال، SecureAdmin).

يمكنك إعادة تعيين كلمة مرور حساب مستخدم الخدمة في إعدادات السياسة. ويجب إعادة تعيين كلمة مرور حساب مستخدم الخدمة بالطريقة ذاتها لكلمة مرور KLAdmin. إذا كان تحرير إعدادات حماية كلمة المرور مسموحًا به (يكون "القفل" مفتوحًا) أو لم يتم تطبيق أي سياسة على الكمبيوتر، فيمكنك إعادة تعيين كلمة المرور لحساب مستخدم الخدمة في واجهة التطبيق. للقيام بذلك، قم بتأكيد التغييرات في معلومات حساب مستخدم الخدمة باستخدام كلمة مرور KLAdmin.

8. في القائمة **Permissions**، 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 **Exit the application**، 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.

9. انقر على **Add**.

10. احفظ تغييراتك.

كيفية منح أذونات للمستخدمين الفرديين أو المجموعات في واجهة مستخدم التطبيق

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. حدد نوع حساب المستخدم الذي تريد إضافته:

- **تحديد مستخدم / مجموعة من Active Directory** – حسابات مستخدمي Active Directory.

  لتحديد حساب مستخدم، انقر فوق **تحديد مستخدم أو مجموعة**. حدد مستخدم أو مجموعة في Active Directory وقم بتأكيد اختيارك.

- **إضافة مستخدم يدويًا** لحساب مستخدم خدمة مضاف يدويًا.

  لإضافة حساب مستخدم خدمة، أدخل اسم مستخدم وكلمة مرور (على سبيل المثال، SecureAdmin).

يمكنك إعادة تعيين كلمة مرور حساب مستخدم الخدمة في إعدادات السياسة. ويجب إعادة تعيين كلمة مرور حساب مستخدم الخدمة بالطريقة ذاتها لكلمة مرور KLAdmin. إذا كان تحرير إعدادات حماية كلمة المرور مسموحًا به (يكون "القفل" مفتوحًا) أو لم يتم تطبيق أي سياسة على الكمبيوتر، فيمكنك إعادة تعيين كلمة المرور لحساب مستخدم الخدمة في واجهة التطبيق. للقيام بذلك، قم بتأكيد التغييرات في معلومات حساب مستخدم الخدمة باستخدام كلمة مرور KLAdmin.

5. 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.

6. 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 **Managed devices** 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 **Devices**.

4. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.

5. من نافذة خصائص الكمبيوتر، حدد القسم **Applications**.

6. في قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر، حدد **Kaspersky Endpoint Security for Windows (14.2)** 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 النافذة التي تفتح في القسم **كلمة المرور المؤقتة**، انقر فوق الزر **قائمة كلمات المرور المؤقتة**.
تفتح نافذة إدارة كلمات المرور المؤقتة.

10. انقر على **إضافة**.

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 نافذة Web Console الرئيسية، حدد **Asset management ← Assets (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 **Temporary passwords**، انقر على الزر **Add**.

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.

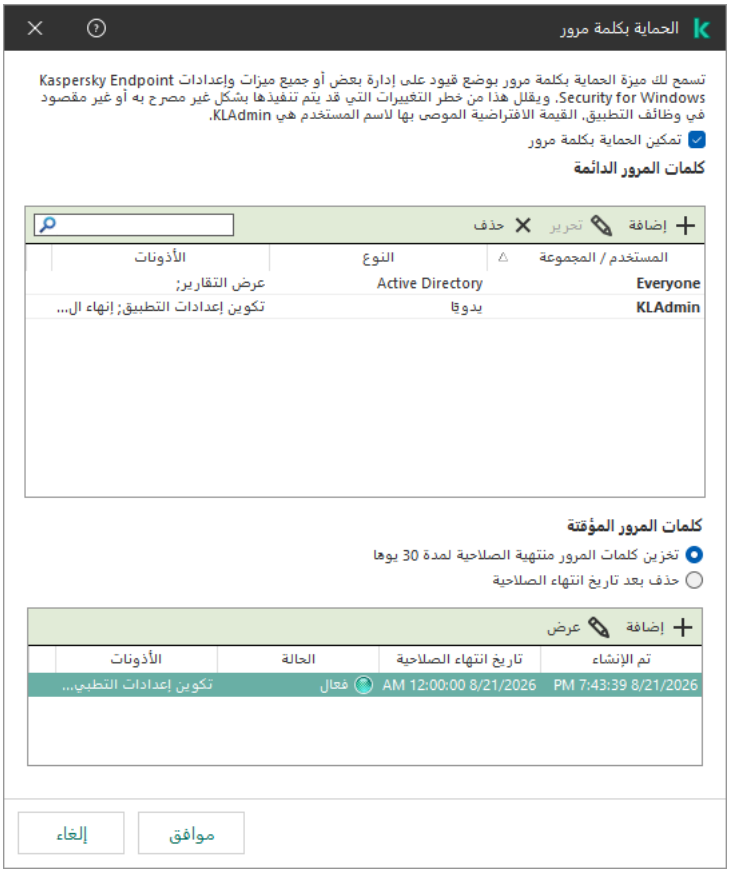


كلمة المرور المؤقتة

إلغاء كلمة المرور المؤقتة

بدءً من الإصدار 12.9، يتضمن Kaspersky Endpoint Security for Windows وظيفة إدارة كلمات المرور المؤقتة. وتتيح لك إدارة كلمات المرور المؤقتة تنفيذ الإجراءات التالية:

- حفظ سجل كلمات المرور (حتى 30 يومًا).
- مراقبة حالة كلمة المرور المؤقتة: فعالومنتهي الصلاحيةوتم الإبطال.
- إلغاء كلمات المرور المؤقتة.



إدارة كلمات المرور المؤقتة

تُجري إدارة كلمات المرور المؤقتة تحديثًا لحالة كلمة المرور وتغلي كلمة المرور فقط بعد مزامنة الكمبيوتر مع Kaspersky Security Center.

كيفية إلغاء كلمة المرور المؤقتة باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في مجلد **Managed devices** 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 **Devices**.
4. انقر نقرًا مزدوجًا فوق نافذة خصائص الكمبيوتر لفتحها.
5. من نافذة خصائص الكمبيوتر، حدد القسم **Applications**.
6. في قائمة تطبيقات Kaspersky المثبتة على الكمبيوتر، حدد **Kaspersky Endpoint Security for Windows (14.2)** 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. يفتح هذا نافذة، وفي تلك النافذة تحت **كلمة المرور المؤقتة**، يمكنك تكوين إعدادات التخزين لكلمات المرور منتهية الصلاحية.

10. انقر على **قائمة كلمات المرور المؤقتة**.
تفتح نافذة إدارة كلمات المرور المؤقتة. وتعرض إدارة كلمات المرور المؤقتة تاريخ انتهاء صلاحية كلمة المرور وحالة كلمة المرور وقائمة الأذونات.

11. حدد كلمة المرور المؤقتة النشطة التي تريد إلغاءها وانقر نقرًا مزدوجًا فوق كلمة المرور لفتح خصائصها.

12. في النافذة التي تفتح، انقر فوق الزر **إبطال**.

13. احفظ تغييراتك. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

كيفية إلغاء كلمة المرور المؤقتة باستخدام Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Assets (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. تحت **Temporary passwords**، كوّن تخزين كلمات المرور منتهية الصلاحية.

8. انقر على رابط **Temporary password**.
تفتح نافذة إدارة كلمات المرور المؤقتة. وتعرض إدارة كلمات المرور المؤقتة تاريخ انتهاء صلاحية كلمة المرور وحالة كلمة المرور وقائمة الأذونات.

9. حدد كلمة المرور المؤقتة النشطة التي تريد إلغاءها.

10. في النافذة التي تفتح، انقر فوق الزر **Revoke password**.

11. احفظ تغييراتك. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

نتيجة لذلك، تُعين إدارة كلمات المرور المؤقتة حالة كلمة المرور إلى جارٍ الإلغاء (المزامنة مع مضيف). بعد مزامنة الكمبيوتر مع Kaspersky Security Center، يلغي التطبيق كلمة المرور المؤقتة ويمنع الأذونات الممنوحة على الفور.

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.

تصدير الإعدادات

بشكل افتراضي، يتم رفض تصدير إعدادات التطبيق إلى مجموعة "الكل". ويمكنك تصدير إعدادات التطبيق باستخدام حساب مستخدم KLAdmin. ويتضمن تصدير إعدادات التطبيق فقط إنشاء ملف تكوين باستخدام إعدادات Kaspersky Endpoint Security في واجهة التطبيق. ولا يقيد الإذن تصدير قوائم استثناءات الفحص أو عناوين الويب الموثوقة أو الأجهزة الموثوقة أو القوائم الأخرى التي تحتفظ بها مكونات التطبيق.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **الواجهة**.
4. في القسم **الحماية بكلمة مرور**، انقر على الزر **الإعدادات**.
5. في النافذة التي تفتح، امسح خانة الاختيار **تمكين الحماية بكلمة مرور**
6. احفظ تغييراتك.
7. حدد خانة الاختيار **تمكين الحماية بكلمة مرور** مرة أخرى.
8. انقر فوق **موافق**.
   يفتح هذا نافذة كلمة مرور المسؤول.
9. حدد كلمة المرور الجديدة لحساب KLAdmin وقم بتأكيدها.
10. احفظ تغييراتك.

كيفية إعادة تعيين كلمة مرور حساب KLAdmin في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.
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 14.2**.
   تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.
5. حدد علامة التبويب **Application settings**.
6. انتقل إلى **General Settings** ← **Self-Defense**.
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.

حماية اتصال خادم الإدارة

يتم توصيل الكمبيوتر بخادم الإدارة باستخدام مكون عميل الشبكة في Kaspersky Security Center. وإذا امتلك لدى أحد المتطفلين حقوقًا كافية لتعديل إعدادات اتصال الخادم، فهناك خطر في احتمال توصيل الكمبيوتر بخادم غير موثوق به. ويسمح هذا للمتطفل بتطبيق سياسات المجموعة الخاصة به، وعلى سبيل المثال، تعطيل الدفاع الذاتي للتطبيق. ويستطيع Kaspersky Endpoint Security منع إعادة الاتصال غير المصرح به لجهاز كمبيوتر بخادم مختلف. ولحماية اتصال الخادم، يقترح التطبيق تعيين كلمة مرور واستخدام Password-Based key Derivation Function (PBKDF2). ونتيجة لذلك، فإن الوصول إلى التطبيق دون كلمة مرور أمر مستحيل.

لضمان الحماية الشاملة لتطبيق Kaspersky Endpoint Security وNetwork Agent من الوصول غير المصرح به، نوصي بتمكين الحماية الإضافية. ولتطبيق Kaspersky Endpoint Security، نوصي بتمكين الحماية بكلمة مرور. ولحماية عميل الشبكة، نوصي بتعيين كلمة مرور لإلغاء التثبيت. وللتفاصيل عن حماية عميل الشبكة من الإزالة، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

تتم إدارة اتصال الكمبيوتر بخادم الإدارة باستخدام المهمة حماية الاتصال بخادم الإدارة. وتُتيح لك المهمة تنفيذ الإجراءات التالية:

- تعيين كلمة مرور لحماية اتصال الخادم.
- تغيير كلمة المرور.
- إعادة توصيل الكمبيوتر بخادم مختلف.
- تعطيل حماية الاتصال بالخادم.

مصادقة جهاز الكمبيوتر عند الاتصال بخادم الإدارة

بعد تعيين كلمة المرور، ينشئ التطبيق مصفوفة بيانات باستخدام تحويل كلمة المرور PBKDF2. وبعد ذلك يشفر التطبيق مجموعة البيانات هذه باستخدام مفتاح عميل الشبكة. ويستخدم التطبيق مصفوفة البيانات المشفرة للتحقق من حقوق وامتيازات خادم الإدارة للاتصالات اللاحقة.

وبعد ذلك، كلما جرت محاولة لإعادة توصيل الكمبيوتر بخادم الإدارة، يفك التطبيق تشفير مصفوفة البيانات باستخدام مفتاح عميل الشبكة ويقارنه بالنسخة المحلية. إذا لم يكونا متطابقين، فسيتم تقييد الوصول إلى التطبيق.

حماية اتصال خادم الإدارة

كيفية تعيين كلمة مرور لحماية اتصال الخادم في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **حماية الاتصال بخادم الإدارة**.

الخطوة 2. حماية اتصال خادم الإدارة

تعيين كلمة مرور لحماية اتصال خادم الإدارة:

1. تحت **حماية الاتصال بخادم الإدارة**، حدد **الحماية بكلمة مرور**.
2. في القائمة المنسدلة **خادم الإدارة** حدد **خادم جديد**.
3. في الحقل **كلمة المرور للاتصال بخادم الإدارة**، قم بتعيين كلمة مرور للاتصال بخادم الإدارة وأكدها.

   إذا نسيت كلمة المرور، فيمكنك تغيير كلمة المرور باستخدام مهمة.
4. إذا كان لديك Kaspersky Endpoint Security 12.7 أو إصدار سابق من التطبيق تم نشره، فحدد خانة الاختيار **تمكين توافق تشفير كلمة المرور لإصدارات التطبيق السابقة (12.7 والإصدارات الأقدم)**.

   بدءًا من Kaspersky Endpoint Security 12.8 for Windows، يستخدم التطبيق تشفيرًا أقوى لكلمات المرور. وإذا كان لديك Kaspersky Endpoint Security 12.8 أو إصدار أحدث تم نشره، فإننا نوصي بإلغاء تحديد خانة الاختيار هذه واستخدام تشفير أقوى لكلمات المرور. ولا تدعم الإصدارات السابقة من التطبيق تشفير كلمات المرور القوية. ولتشغيل المهمة، يجب تحديد خانة الاختيار.

الخطوة الثالثة: اختيار الحساب لتشغيل المهمة

حدد **Default account**. افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

الخطوة الرابعة: تكوين جدول بدء المهمة

تحت **Scheduled start**، حدد **Manually**.

الخطوة الخامسة: تحديد اسم المهمة

أدخل اسم المهمة، مثل كلمة مرور الاتصال بخادم البريد.

الخطوة 6 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** أو قم بتشغيل المهمة يدويًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية تعيين كلمة مرور لحماية اتصال الخادم في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

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

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Administration Server connection protection**.

c. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، كلمة مرور الاتصال بالخادم الرئيسي.

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

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

5. حدد حساب مستخدم افتراضيًا. افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

6. قم بإنهاء المعالج.
سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة **Administration Server connection protection** في برنامج Kaspersky Endpoint Security.
نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. تحت **Administration Server connection protection**، حدد **Protect with a password**.

10. في القائمة المنسدلة **Connection to the Administration Server** حدد **New password**.

11. في الحقل **Password for connection to the Administration Server**، قم بتعيين كلمة مرور للاتصال بخادم الإدارة وأكدها.
إذا نسيت كلمة المرور، فيمكنك تغيير كلمة المرور باستخدام مهمة.

12. إذا كان لديك Kaspersky Endpoint Security 12.7 أو إصدار سابق من التطبيق تم نشره، فحدد خانة الاختيار **Enable password encryption compatibility for previous application versions (12.7 and lower)**.
بدءًا من Kaspersky Endpoint Security 12.8 for Windows، يستخدم التطبيق تشفيرًا أقوى لكلمات المرور. وإذا كان لديك Kaspersky Endpoint Security 12.8 أو إصدار أحدث تم نشره، فإننا نوصي بإلغاء تحديد خانة الاختيار هذه واستخدام تشفير أقوى لكلمات المرور. ولا تدعم الإصدارات السابقة من التطبيق تشفير كلمات المرور القوية. ولتشغيل المهمة، يجب تحديد خانة الاختيار.

13. احفظ تغييراتك.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر فوق **Start**.

يمكنك مراقبة حالة المهمة وعدد الأجهزة التي تم استكمال المهمة عليها بنجاح أو اكتمل تنفيذها مع وجود خطأ.

إعادة توصيل الكمبيوتر بخادم إدارة مختلف

تتضمن إعادة توصيل الكمبيوتر بخادم إدارة مختلف الخطوات التالية:

1. في وحدة تحكم خادم [KSC1] الحالي، قم بتشغيل مهمة Change Administration Server لعميل الشبكة.

بعد تشغيل المهمة، يتم إعادة توصيل الكمبيوتر بخادم [KSC2] الجديد.

سيتم عرض الكمبيوتر في وحدة تحكم خادم [KSC1] مع حالة Critical. من المستحيل تكوين التطبيق باستخدام السياسات أو تشغيل المهام عن بعد على الكمبيوتر.

2. في وحدة تحكم خادم [KSC2] الجديد، أنشئ مهمة حماية الاتصال بخادم الإدارة جديدة لتطبيق Kaspersky Endpoint Security. في خصائص المهمة، أدخل كلمة المرور للخادم السابق وقم بتعيين كلمة مرور للخادم الجديد.

كيفية تعيين كلمة مرور جديدة لإعادة الاتصال بخادم جديد في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **حماية الاتصال بخادم الإدارة**.

الخطوة 2. حماية اتصال خادم الإدارة

قم بتعيين كلمة مرور لحماية الاتصال بخادم الإدارة الجديد:

1. تحت **حماية الاتصال بخادم الإدارة**، حدد **الحماية بكلمة مرور**.

2. في القائمة المنسدلة **خادم الإدارة** حدد **إعادة الاتصال من خادم آخر**.

3. في الحقل **كلمة المرور الحالية**، أدخل كلمة المرور المعينة للاتصال بالخادم الموثوق به الذي تم استخدامه من قبل.

4. في الحقل **كلمة المرور الجديدة**، قم بتعيين كلمة مرور للاتصال بخادم الإدارة الجديد وأكد كلمة المرور.

إذا نسيت كلمة المرور، فيمكنك تغيير كلمة المرور باستخدام مهمة.

5. إذا كان لديك Kaspersky Endpoint Security 12.7 أو إصدار سابق من التطبيق تم نشره، فحدد خانة الاختيار **تمكين توافق تشفير كلمة المرور لإصدارات التطبيق السابقة (12.7 والإصدارات الأقدم)**.

بدءًا من Kaspersky Endpoint Security 12.8 for Windows، يستخدم التطبيق تشفيرًا أقوى لكلمات المرور. وإذا كان لديك Kaspersky Endpoint Security 12.8 أو إصدار أحدث تم نشره، فإننا نوصي بإلغاء تحديد خانة الاختيار هذه واستخدام تشفير أقوى لكلمات المرور. ولا تدعم الإصدارات السابقة من التطبيق تشفير كلمات المرور القوية. ولتشغيل المهمة، يجب تحديد خانة الاختيار.

الخطوة الثالثة: اختيار الحساب لتشغيل المهمة

حدد **Default account**. افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).

الخطوة الرابعة: تكوين جدول بدء المهمة

تحت **Scheduled start**، حدد **Manually**.

الخطوة الخامسة: تحديد اسم المهمة

أدخل اسم المهمة، مثل كلمة مرور الاتصال بخادم البريد.

الخطوة 6 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** أو قم بتشغيل المهمة يدويًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية تعيين كلمة مرور جديدة لإعادة الاتصال بخادم جديد في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.
2. انقر على **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.
   b. في القائمة المنسدلة **Task type**، حدد **Administration Server connection protection**.
   c. في الحقل **Task name**، أدخل وصفًا موجزًا، على سبيل المثال، كلمة مرور الاتصال بالخادم الرئيسي.
   d. في القسم **Devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انتقل إلى الخطوة التالية.
5. حدد حساب مستخدم افتراضيًا. افتراضيًا، يبدأ Kaspersky Endpoint Security المهمة كحساب مستخدم للنظام (SYSTEM).
6. قم بإنهاء المعالج.
سيتم عرض مهمة جديدة في قائمة المهام.

7. انقر فوق المهمة **Administration Server connection protection** في برنامج Kaspersky Endpoint Security.
نافذة خصائص المهمة.

8. حدد علامة التبويب **Application settings**.

9. تحت **Administration Server connection protection**، حدد **Protect with a password**.

10. في القائمة المنسدلة **Connection to the Administration Server** حدد **Reconnect from another server**.

11. في الحقل **Current password**، أدخل كلمة المرور المعينة للاتصال بالخادم الموثوق به الذي تم استخدامه من قبل.

12. في الحقل **New password**، قم بتعيين كلمة مرور للاتصال بخادم الإدارة الجديد وأكد كلمة المرور.
إذا نسيت كلمة المرور، فيمكنك تغيير كلمة المرور باستخدام مهمة.

13. إذا كان لديك Kaspersky Endpoint Security 12.7 أو إصدار سابق من التطبيق تم نشره، فحدد خانة الاختيار **Enable password encryption compatibility for previous application versions (12.7 and lower)**.
بدءًا من Kaspersky Endpoint Security 12.8 for Windows، يستخدم التطبيق تشفيرًا أقوى لكلمات المرور. وإذا كان لديك Kaspersky Endpoint Security 12.8 أو إصدار أحدث تم نشره، فإننا نوصي بإلغاء تحديد خانة الاختيار هذه واستخدام تشفير أقوى لكلمات المرور. ولا تدعم الإصدارات السابقة من التطبيق تشفير كلمات المرور القوية. ولتشغيل المهمة، يجب تحديد خانة الاختيار.

14. احفظ تغييراتك.

15. حدد خانة الاختيار المجاورة للمهمة.

16. انقر فوق **Start**.
يمكنك مراقبة حالة المهمة وعدد الأجهزة التي تم استكمال المهمة عليها بنجاح أو اكتمل تنفيذها مع وجود خطأ.

بعد إكمال المهمة، تأكد من أن الكمبيوتر في وحدة التحكم الخاصة بخادم [KSC2] الجديد في حالة OK. اختبر ما إذا كان بإمكانك تشغيل المهام عن بُعد وتكوين التطبيق باستخدام السياسات.

إعادة تعيين كلمة مرور الاتصال بخادم الإدارة

إذا نسيت كلمة مرور الاتصال بخادم الإدارة أو تم اختراق كلمة المرور، فيمكنك إعادة تعيين كلمة المرور في خصائص المهمة. ويمكنك أيضًا إعادة تعيين كلمة المرور وتعيين كلمة مرور جديدة لمجموعة من أجهزة الكمبيوتر ذات حالات حماية الاتصال بخادم الإدارة المختلفة. بمعنى، إذا تم تمكين الحماية في بعض أجهزة الكمبيوتر وتم تعطيلها في بعضها الآخر، فإن المهمة تقوم بتعيين كلمة مرور لجميع أجهزة الكمبيوتر.

يمكنك فقط إعادة تعيين كلمة مرور الاتصال بخادم الإدارة في وحدة التحكم الخاصة بالخادم الموثوق الذي يتصل به الكمبيوتر.

كيفية إعادة تعيين كلمة مرور الاتصال بخادم الإدارة باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

3. حدد مهمة **حماية الاتصال بخادم الإدارة** وانقر نقرًا مزدوجًا لفتح خصائص المهمة.

4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.

5. تحت **حماية الاتصال بخادم الإدارة**، حدد **الحماية وتغيير كلمة المرور**.

6. في الحقل **كلمة المرور للاتصال بخادم الإدارة**، قم بتعيين كلمة مرور جديدة للاتصال بالخادم الموثوق الحالي وتأكيد كلمة المرور.

7. احفظ تغييراتك.

8. قم بتشغيل المهمة.

كيفية إعادة تعيين كلمة مرور الاتصال بخادم الإدارة في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

2. انقر فوق المهمة **Administration Server connection protection** في برنامج Kaspersky Endpoint Security.
نافذة خصائص المهمة.

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

4. تحت **Administration Server connection protection**، حدد **Protect and change password**.

5. في الحقل **Password for connection to the Administration Server**، قم بتعيين كلمة مرور جديدة للاتصال بالخادم الموثوق الحالي وتأكيد كلمة المرور.

6. احفظ تغييراتك.

7. حدد خانة الاختيار المجاورة للمهمة.

8. انقر فوق **Start**.

ونتيجة لذلك، تتم إعادة تعيين كلمة مرور الاتصال بخادم الإدارة بعد انتهاء المهمة.

تعطيل حماية الاتصال بخادم الإدارة

يمكنك فقط تعطيل حماية الاتصال بخادم الإدارة عن بعد في وحدة التحكم الخاصة بالخادم الموثوق الذي يتصل به الكمبيوتر. ويمكنك أيضًا تعطيل الحماية محليًا في سطر الأوامر.

كيفية تعطيل حماية الاتصال بالخادم في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

3. حدد مهمة **حماية الاتصال بخادم الإدارة** وانقر نقرًا مزدوجًا لفتح خصائص المهمة.

4. من نافذة خصائص المهام، حدد القسم **الإعدادات**.

5. تحت **حماية الاتصال بخادم الإدارة**، حدد **عدم الحماية**.

6. احفظ تغييراتك.

7. قم بتشغيل المهمة.
يمكنك مراقبة حالة المهمة وعدد الأجهزة التي تم استكمال المهمة عليها بنجاح أو اكتمل تنفيذها مع وجود خطأ.

كيفية تعطيل حماية الاتصال بالخادم في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

2. انقر فوق المهمة **Administration Server connection protection** في برنامج Kaspersky Endpoint Security.
نافذة خصائص المهمة.

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

4. تحت **Administration Server connection protection**، حدد **Do not protect with a password**.

5. احفظ تغييراتك.

6. حدد خانة الاختيار المجاورة للمهمة.

7. انقر فوق **Start**.
يمكنك مراقبة حالة المهمة وعدد الأجهزة التي تم استكمال المهمة عليها بنجاح أو اكتمل تنفيذها مع وجود خطأ.

كيفية تعطيل حماية الاتصال بالخادم في 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 SERVERBINDINGDISABLE [/password=<password>]
```

حيث `<password>` هي كلمة مرور حساب مستخدم KL Admin أو كلمة المرور من مهمة حماية الاتصال بخادم الإدارة. وإذا لم يتم تحديد المعلمة، فسيطالبك Kaspersky Endpoint Security بإدخال كلمة مرور في السطر التالي.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة.

مثال

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

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 Advanced Encryption Standard (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 كان برنامج Kaspersky Endpoint Security مثبتًا على جهاز قائم على بنية Arm، فسيتوفر تشفير المحرك باستخدام BitLocker فقط. ولا يدعم التطبيق مكونات تشفير البيانات الأخرى.

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 بـ Trusted Platform Module (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. ويمكنك أيضًا استخدام تقنية Single Sign-On (SSO) التي تتيح لك تسجيل الدخول 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.
- إذا تم تثبيت Kaspersky Endpoint Security على كمبيوتر مستند إلى Arm، فلن يتوفر سوى تشفير القرص الكامل باستخدام تقنية تشفير محرك BitLocker، ولن يتم دعم مكونات التشفير الأخرى.

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

لا يتم دعم تشفير القرص من Kaspersky في أجهزة الكمبيوتر القائمة على Arm.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.
4. 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.

5. 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.

6. قم بتكوين خيارات تشفير القرص من Kaspersky المتقدمة (انظر الجدول أدناه).
7. احفظ تغييراتك.

كيفية تشغيل تشفير القرص من Kaspersky من خلال Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
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**.

يتعذر استخدام تشفير القرص من Kaspersky في حالة وجود محركات أقراص صلبة على الكمبيوتر تم تشفيرها بواسطة BitLocker.

6. في القسم **Action on devices**، حدد **Encrypt all hard drives**.

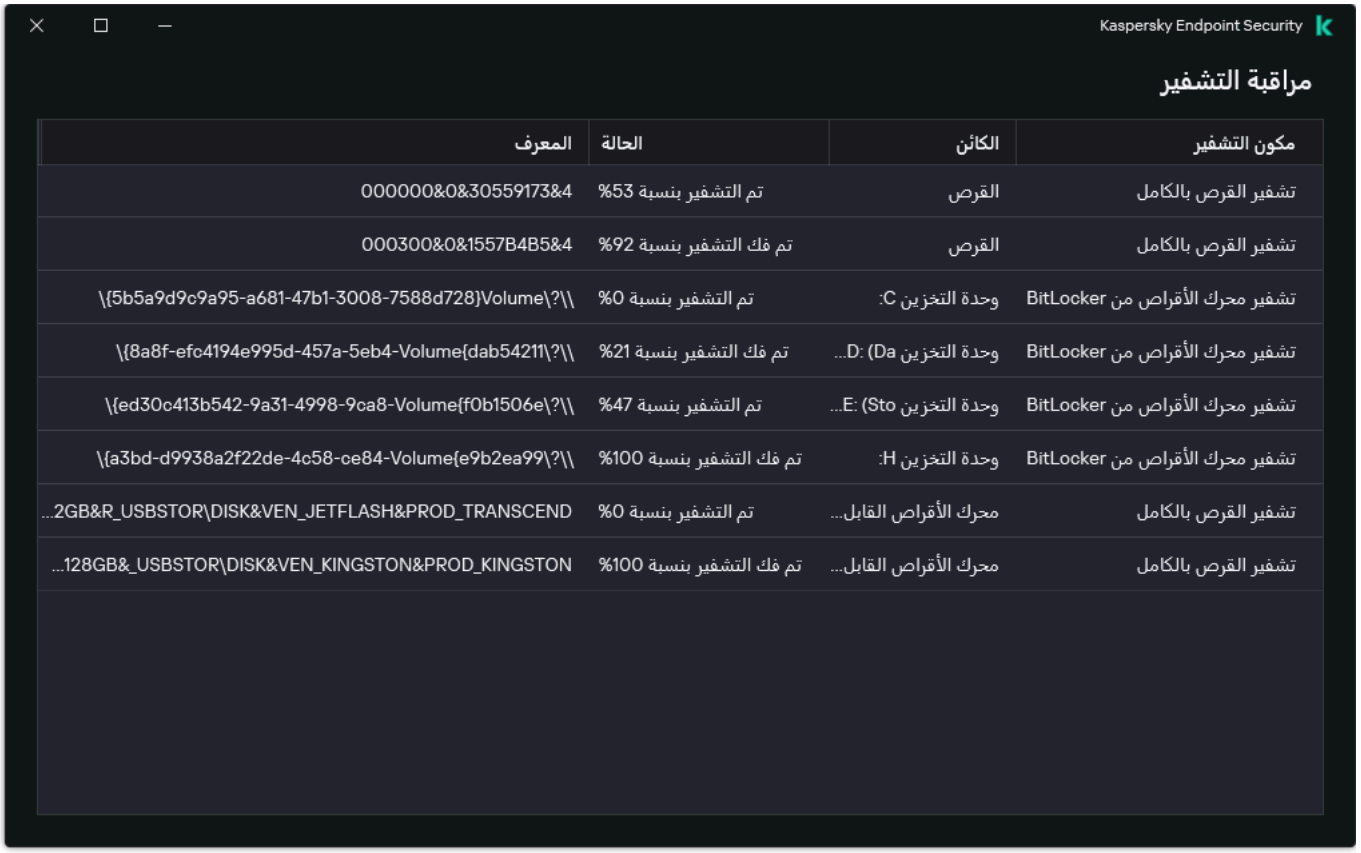
في حالة تثبيت العديد من أنظمة التشغيل على الكمبيوتر، فسوف يمكنك بعد التشفير تحميل نظام التشغيل الذي تم إجراء التشفير عليه.

إذا كنت بحاجة إلى استثناء بعض من محركات الأقراص الصلبة من التشفير، قم بإنشاء قائمة بمحركات الأقراص الصلبة هذه.

7. قم بتكوين خيارات تشفير القرص من Kaspersky المتقدمة (انظر الجدول أدناه).

8. 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.

المعلمة	الوصف
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. بشكل افتراضي، يتم إلغاء تحديد خانة الاختيار.
استخدام دعم USB القديم (غير موصى به)	تقوم خانة الاختيار هذه بتمكين أو تعطيل وظائف Legacy USB Support. 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). لا يؤثر Legacy USB Support 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 تمكين وظيفة Legacy USB Support، 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.
4. 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.
5. 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**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**.

6. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **تشفير البيانات ← تشفير القرص بالكامل**.

4. 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**.

5. 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 الزر ← **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.

6. لاستيراد قائمة القواعد:

a. انقر على الزر ← **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.

7. احفظ تغييراتك.

كيفية تصدير واستيراد قائمة استثناءات تشفير محرك الأقراص الصلبة في وحدة تحكم الويب

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Full Disk Encryption** ← **Data Encryption**.
حدد تقنية **Kaspersky Disk Encryption**.

5. انقر على رابط **Exclusions**.
تفتح قائمة الاستثناءات.

6. لتصدير قائمة القواعد:

a. حدد الاستثناءات التي تريد تصديرها.

b. انقر على الزر ← **Export**.
يقوم Kaspersky Endpoint Security بتصدير قائمة الاستثناءات إلى ملف JSON في مجلد التنزيلات الافتراضي.

7. لاستيراد قائمة الاستثناءات:

a. انقر على الزر ← **Import**.
في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد قائمة الاستثناءات منه.

b. 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 JSON.

8. احفظ تغييراتك.

تمكين تقنية تسجيل الدخول الأحادي (SSO)

تتيح لك تقنية Single Sign-On (SSO) تسجيل الدخول 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **إعدادات التشفير العامة**.
4. في القسم **إعدادات كلمة المرور**، انقر على الزر **الإعدادات**.
5. في النافذة التي تفتح، في علامة تبويب **وكيل المصادقة**، حدد خانة الاختيار **استخدام تقنية تسجيل الدخول الأحادي (SSO)**.
6. إذا كنت تستخدم موفر بيانات اعتماد خارجيًا، حدد خانة الاختيار **استخدام موفري بيانات الاعتماد الخارجيين**.
7. 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 نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
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**.
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

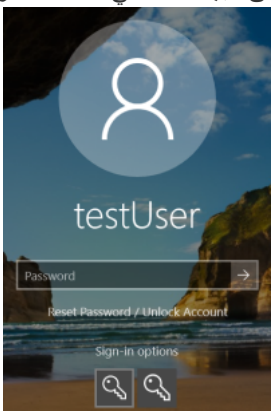
يدعم Kaspersky Endpoint Security موفر بيانات الاعتماد الخارجي ADSelfService Plus.

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 مهمةManage Authentication Agent accounts 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 Manage Authentication Agent accounts. من المستحيل كذلك إجبار مهمة على التوقف.

كيفية نشاء مهمة إدارة حسابات وكيل المصادقة في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **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

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** 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 نافذة Web Console الرئيسية، حدد **Tasks**.
   تفتح قائمة المهام.
2. انقر على **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 14.2**.

2. في القائمة المنسدلة **Task type**، حدد **Manage Authentication Agent accounts**.

3. في حقل **Task name**، أدخل وصفًا مختصرًا، مثل حسابات المسؤول.

4. في القسم **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

قم بإنهاء المعالج. سيتم عرض مهمة جديدة في قائمة المهام.

لتشغيل مهمة، 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.

لإضافة حساب وكيل المصادقة، ستحتاج إلى إضافة أمر خاص إلى مهمة Manage Authentication Agent accounts. 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 نافذة Web Console الرئيسية، حدد **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 الزر **Add** وحدد نوع الأمر **Add account**.

5. 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 (Security Identifier، SID). هذا ضروري للتحقق من الحساب. إذا أدخلت اسم المستخدم بشكل غير صحيح، فسيقوم Kaspersky Endpoint Security بإنهاء المهمة مع خطأ.

6. 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.

7. احفظ تغييراتك.

8. 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 Manage Authentication Agent accounts. 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 نافذة Web Console الرئيسية، حدد **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 الزر **Add** وحدد نوع الأمر **Edit account**.

5. 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 (Security Identifier، SID). هذا ضروري للتحقق من الحساب. إذا أدخلت اسم المستخدم بشكل غير صحيح، فسيقوم Kaspersky Endpoint Security بإنهاء المهمة مع خطأ.

6. حدد خانات الاختيار المجاورة للإعدادات التي ترغب في تعديلها.

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**.

لحذف حساب وكيل المصادقة، ستحتاج إلى إضافة أمر خاص إلى مهمة Manage Authentication Agent accounts. 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 نافذة Web Console الرئيسية، حدد **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 الزر **Add** وحدد نوع الأمر **Remove account**.

5. حدد حساب مستخدم. يمكنك تحديد حساب من قائمة حسابات المجال أو إدخال اسم الحساب يدويًا.

6. احفظ تغييراتك.

7. حدد خانة الاختيار المقابلة للمهمة وانقر فوق الزر **Start**.

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 **Tasks**.

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.

1. في نافذة Web Console الرئيسية، حدد **Asset management ← Assets (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 علامة التبويب **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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.
4. في القائمة المنسدلة **تقنية التشفير**، حدد التقنية التي سيتم تشفير محركات الأقراص الصلبة باستخدامها.

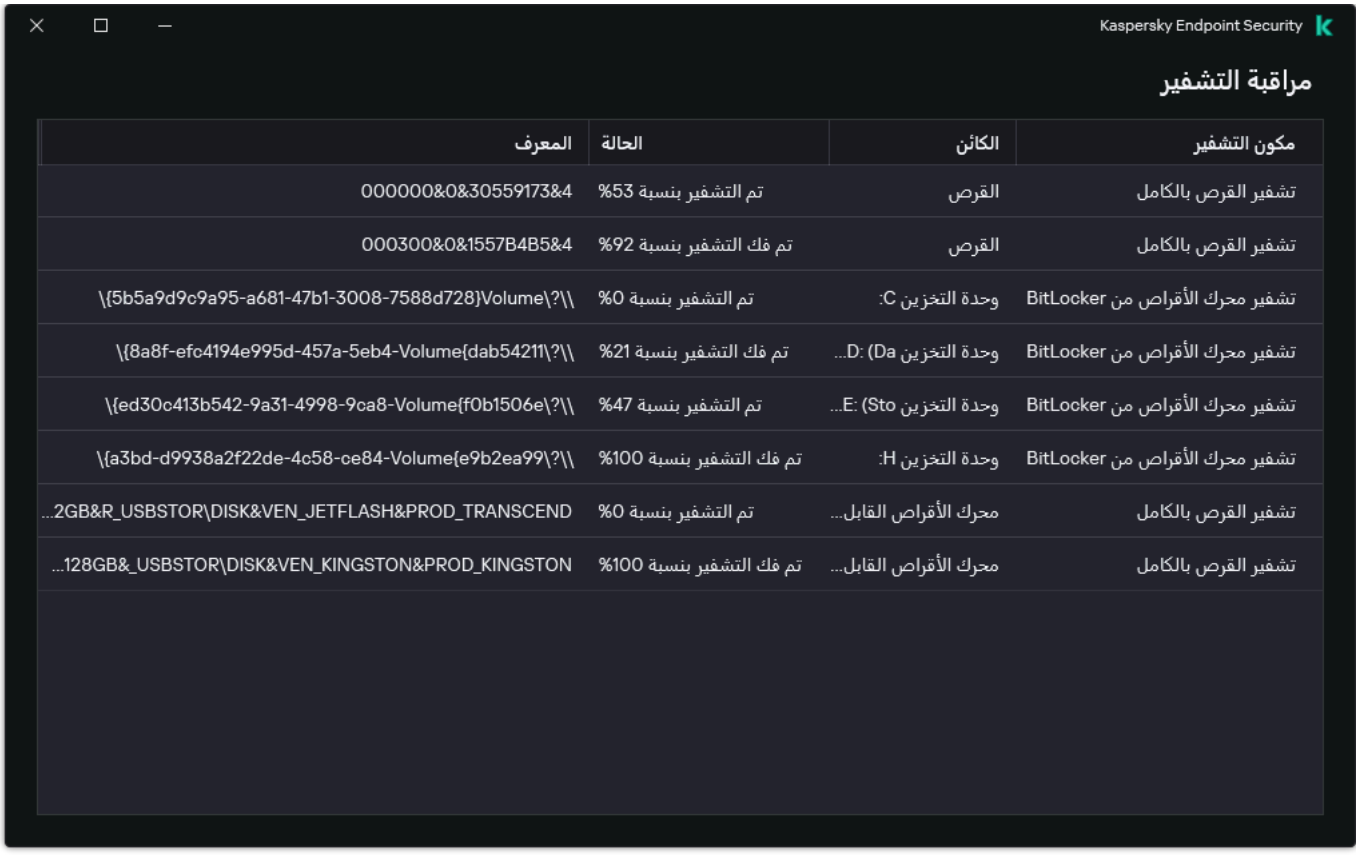
5. قم بأحد الإجراءات التالية:

- 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.

6. 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.

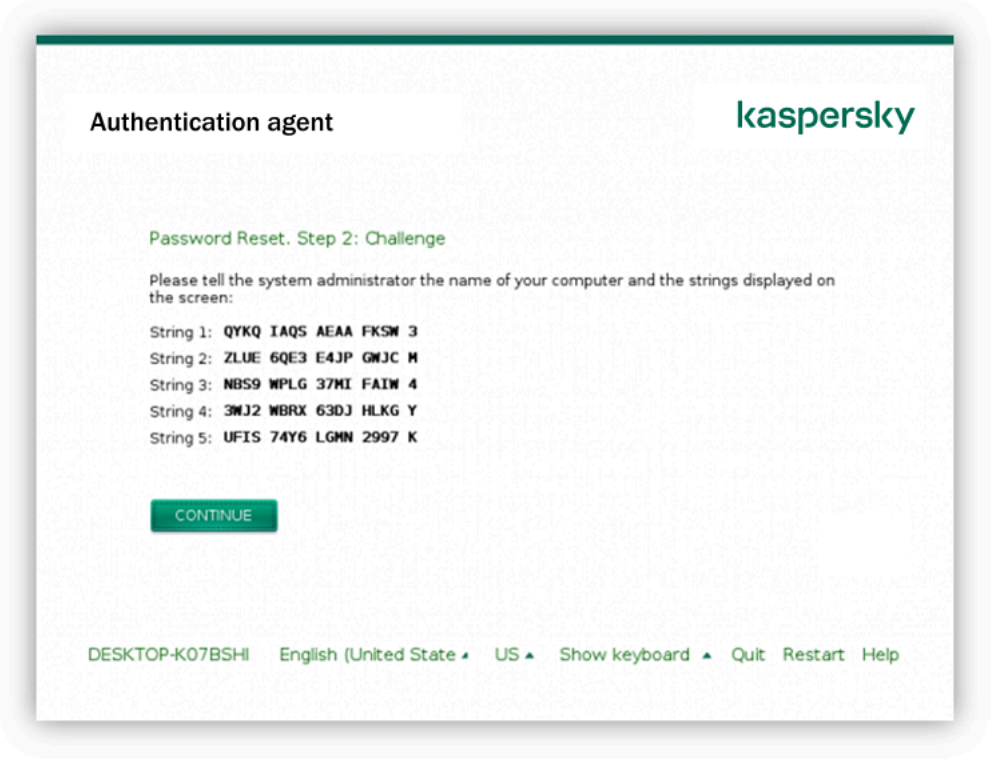
استعادة الوصول إلى محرك محمي بواسطة تقنية تشفير القرص من Kaspersky

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 **Devices**، 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. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **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: Strong encryption (AES256) أو Lite encryption (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 نافذة Web Console الرئيسية، حدد **Asset management** ← **Assets (Devices)**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى محركه.

3. انقر على **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 **Devices**، 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. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **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 نافذة Web Console الرئيسية، حدد **Asset management ← Assets (Devices)**.
2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى بياناته.
3. انقر على **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 **Tasks**.
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 نافذة Web Console الرئيسية، حدد **Asset management ← Assets (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 علامة التبويب **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.

ميزات تحديث نظام التشغيل:

- **تحديث نظام التشغيل من خلال WSUS**. يمكنك تحديث نظام التشغيل بالطريقة المعتادة.
- **تحديث نظام التشغيل من ملف ISO**. لتحديث نظام التشغيل، يجب عليك تحديد المجلد الذي يحتوي على برامج تشغيل تشفير القرص من Kaspersky. وينسخ التطبيق تلقائيًا برامج التشغيل إلى مجلد منفصل. نفذ ما يلي:

  1. قم بتركيب صورة ISO.

  2. ابدأ تثبيت تحديث النظام باستخدام المفتاح التالي:

```
setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.2\reflect_drivers
```

يتوفر التحديث التلقائي لنظام التشغيل فقط إذا كان الكمبيوتر يعمل بنظام التشغيل Windows 10 1607 (RS1) أو أحدث. ولترقية الإصدارات السابقة من نظام التشغيل، يوصى بفك تشفير القرص أولاً، وإجراء ترقية لنظام التشغيل، ثم تشفير القرص.

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 14.2.

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،

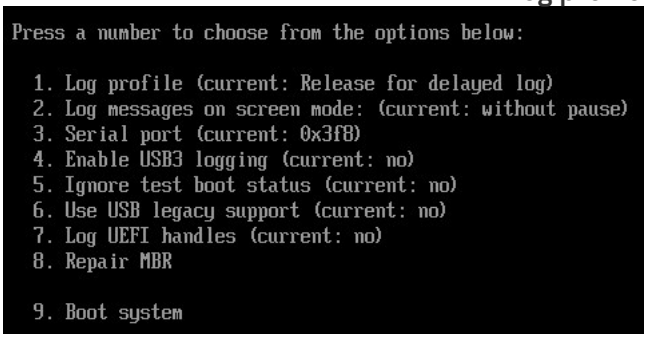
قم باستعادة الوصول إلى الأجهزة المشفرة باستخدام أداة الاستعادة المساعدة.

تتبع وكيل المصادقة

يقوم التطبيق بتسجيل معلومات الخدمة حول تشغيل وكيل المصادقة والمعلومات حول عمليات المستخدم مع وكيل المصادقة في ملف التتبع.

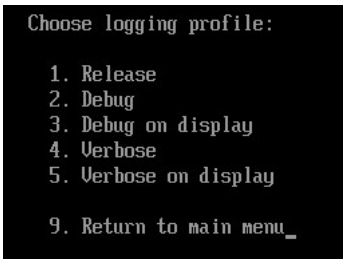
لتمكين تتبع وكيل المصادقة:

1. تمكين تتبع Kaspersky Endpoint Security.
2. أعد تشغيل الكمبيوتر.
3. بمجرد بدء تشغيل الكمبيوتر ذو محركات الأقراص الصلبة المشفرة، اضغط على الزر **F3** لاستدعاء نافذة تكوين إعدادات وكيل المصادقة.
4. بعد بدء تشغيل محمل تمهيد FDE، حدد مدير التمهيد **KES (FDE <version>)**.
5. في قائمة مدير التمهيد، انتقل إلى إعدادات **Log profile**.



قائمة مدير التمهيد

6. حدد مستوى التتبع في نافذة إعدادات ملف تعريف السجل:



مستويات تتبع وكيل المصادقة

- **Release**. إذا تم تحديد هذا الخيار، لا يسجل التطبيق المعلومات حول أحداث وكيل المصادقة في ملف التتبع.
- **Debug**. إذا تم تحديد هذا الخيار، يقوم التطبيق بتسجيل المعلومات حول تشغيل وكيل المصادقة وعمليات المستخدم التي تم إجراؤها باستخدام وكيل المصادقة في ملف التتبع.
- **Debug on display**. 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.
- **Verbose**. 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 **Debug**. يؤدي مستوى تفاصيل الإدخالات العالي إلى إبطاء بدء تشغيل وكيل المصادقة ونظام التشغيل.

- **Verbose on display**. 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 **Debug on display**. يؤدي مستوى تفاصيل الإدخالات العالي إلى إبطاء بدء تشغيل وكيل المصادقة ونظام التشغيل.

بعد تحديد مستوى التتبع، يعرض مدير التمهيد القائمة مرة أخرى.

7. في قائمة مدير التمهيد، حدد **Boot system**.

   يبدأ محمل تمهيد FDE تشغيل وكيل المصادقة.

   أعد إظهار المشكلة.

   يتم تسجيل البيانات في ملف تتبع وكيل المصادقة إذا كانت هناك محركات أقراص صلبة مشفرة على الكمبيوتر أو أثناء تشفير القرص بالكامل.

8. لإيقاف عملية التتبع، ارجع إلى النافذة أدوات الدعم وقم بتعطيل التتبع.

نتيجةً لذلك، يتم إنشاء ملفات تتبع عملية Authentication Agent KES.SRV في المجلد `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **إعدادات التشفير العامة**.
4. في القسم **القوالب**، انقر على الزر **تعليمات**.
5. 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.
6. 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.

7. 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 (Latin-1) (0080 - 00FF)
- اللاتينية الموسعة (Latin-A) (0100 - 017F)
- اللاتينية الموسعة (Latin-B) (0180 - 024F)
- 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.

لاستخدام أداة استعادة لإزالة الكائنات والبيانات التي تبقت بعد التشغيل الاختباري لوكيل المصادقة:

1. قم بتشغيل الملف باسم fdert.exe، وهو الملف التنفيذي لأداة الاستعادة. يتم إنشاء هذا الملف بواسطة Kaspersky Endpoint Security.
2. في نافذة أداة الاستعادة، حدد الجهاز المطلوب.
3. انقر على **فحص**.
4. إذا تلقيت، بعد تشخيص محرك الأقراص الثابت الخاص بالنظام، رسالة تشير إلى بقاء الكائنات والبيانات من عملية اختبار وكيل المصادقة، فانقر فوق **حذف كائنات وبيانات AA**.

يتوافر الزر **حذف كائنات وبيانات AA** فقط في حالة اكتشاف الكائنات والبيانات المتبقية بعد تشغيل اختبار وكيل المصادقة.

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. يسمح لك Kaspersky Endpoint Security بالتحكم في تقنية Bitlocker وإدارتها باستخدام البنية التحتية لتطبيق Kaspersky Next. 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.

عند تشفير القرص، يضع BitLocker أداة تحميل التمهيد والملفات المساعدة الأخرى في system partition. ويكون هذا القسم غير مشفر. وينشئ نظام التشغيل قسم النظام تلقائيًا أثناء تثبيت Windows. وإذا كان القرص مقسمًا بشكل كامل قبل تثبيت Windows، فلن يتمكن نظام التشغيل من إنشاء قسم للنظام. وفي هذه الحالة، عند بدء تشغيل تشفير القرص باستخدام BitLocker، يطالبك نظام التشغيل بإعادة تقسيم القرص وإنشاء قسم للنظام. وبعد إنشاء قسم النظام، يبدأ نظام التشغيل تشفير BitLocker.

لا تعتمد خوارزمية تشفير BitLocker على الإصدار المضمن من مكتبة AES في حزمة التوزيع (AES256 أو AES56). ويستخدم التشفير مكتبة التشفير المضمنة في نظام التشغيل.

بشكل افتراضي، يستخدم التطبيق خوارزمية تشفير BitLocker بطول مفتاح فعال من 256 بت لتشفير الأجهزة التي لم يسبق تشفيرها. وبالنسبة لجهاز تم تشفيره قبل تثبيت التطبيق، قد تكون خوارزمية التشفير مختلفة. وللحصول على معلومات مفصلة عن تحديد خوارزمية التشفير، يرجى الرجوع إلى موقع ويب الدعم الفني من Microsoft. وبدءًا من الإصدار 12.9، يرسل Kaspersky Endpoint Security مفتاح الاسترداد الأصلي للأجهزة التي سبق تشفيرها بواسطة تطبيقات الجهات الخارجية إلى Kaspersky Security Center.

توفر تقنية BitLocker تخزينًا آمنًا لمفاتيح الوصول باستخدام وحدة نمطية للنظام الأساسي الموثوق به. (TPM) Trusted Platform Module 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 النظام، يحتاج المستخدم إلى تجاوز مصادقة BitLocker لإقلاع نظام التشغيل. وبعد المصادقة، يسمح BitLocker للمستخدم بتسجيل الدخول. ولا تدعم BitLocker تقنية تسجيل الدخول الأحادي (SSO).

بعد تشفير محرك أقراص، ينشئ BitLocker مفتاح استرداد. ويرسل Kaspersky Endpoint Security مفتاح الاسترداد إلى Kaspersky Security Center حتى يمكنك استعادة الوصول إلى القرص، على سبيل المثال، إذا نسي مستخدم كلمة مروره.

إذا قام مستخدم بتشفير قرص باستخدام BitLocker، فسوف يرسل Kaspersky Endpoint Security مفتاح الاسترداد ومعلومات عن تشفير القرص إلى Kaspersky Security Center.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير القرص بالكامل**.
4. في القائمة المنسدلة **تقنية التشفير** حدد **تشفير محرك الأقراص من BitLocker**.
5. 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.

6. قم بتكوين خيارات تشفير محرك الأقراص من BitLocker المتقدمة (انظر الجدول أدناه).
7. احفظ تغييراتك.

كيفية تشغيل تشفير محرك الأقراص باستخدام BitLocker من خلال وحدة تحكم الإدارة (MMC)

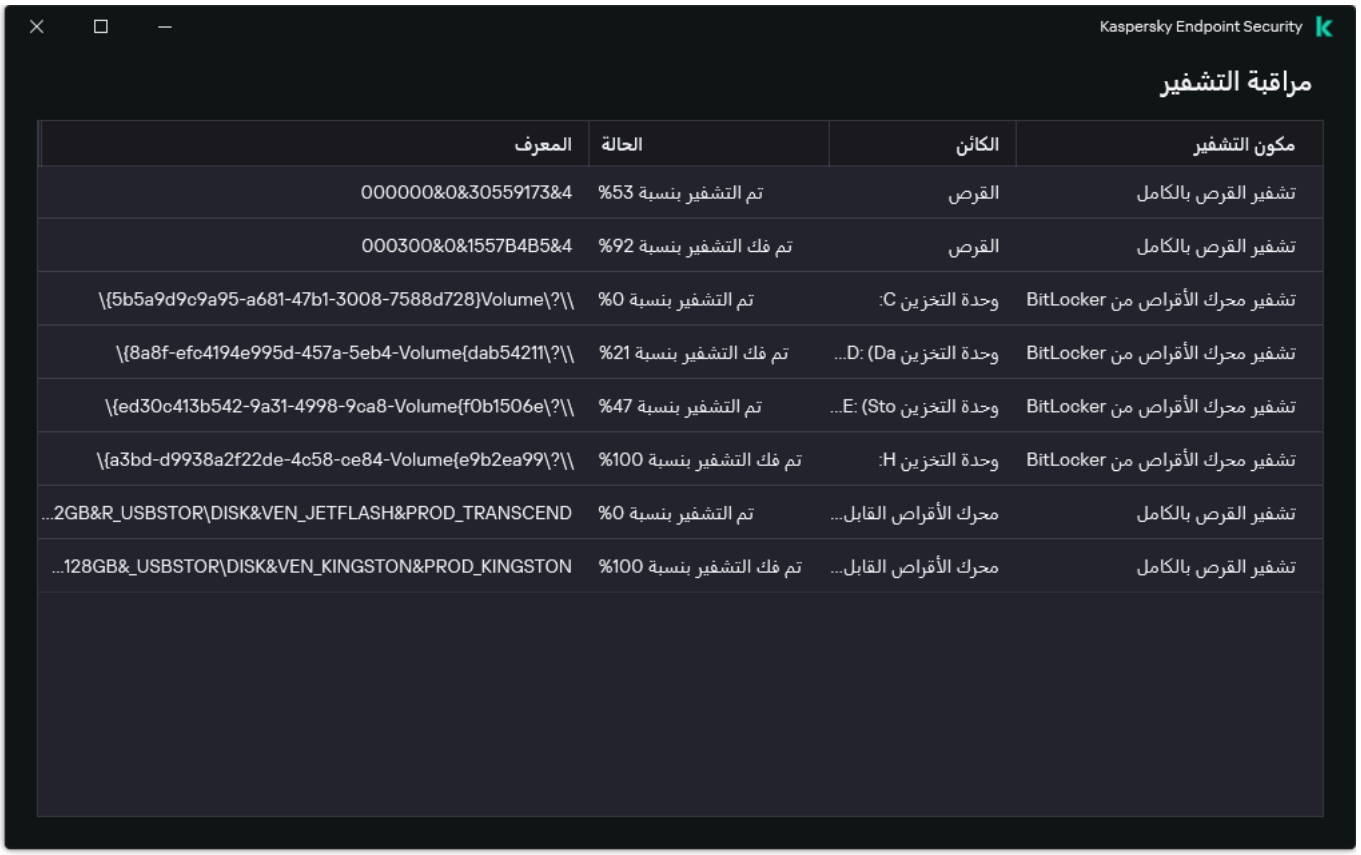
1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Data Encryption** ← **Full Disk Encryption**.
5. حدد تقنية **BitLocker Disk Encryption**.
6. في القسم **Action on devices**، 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.

7. قم بتكوين خيارات تشفير محرك الأقراص من BitLocker المتقدمة (انظر الجدول أدناه).

8. 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).

المعلمة	الوصف
تمكين استخدام مصادقة BitLocker التي تتطلب إدخال لوحة المفاتيح قبل التشغيل على أجهزة الكمبيوتر اللوحية	باستخدام المصادقة التي تتطلب إدخال بيانات في بيئة ما قبل 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. نوصي باستخدام 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. بشكل افتراضي، يتم إلغاء تحديد خانة الاختيار.

المعلمة	الوصف
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). Trusted Platform Module (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. • **وحدة النظام الأساسي الموثوق بها (TPM) أو كلمة المرور إذا لم تكن وحدة النظام الأساسي الموثوق بها متاحة**. في حالة تحديد هذا الخيار، يستطيع 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. يجب تكوين طريقة المصادقة المحددة عن طريق تحديد متطلبات كلمة المرور أو رقم التعريف الشخصي: • **الحد الأدنى لطول رمز PIN (الأحرف)** (القيمة الافتراضية هي 6). • **الحد الأدنى لطول كلمة المرور (الأحرف)** (القيمة الافتراضية هي 8). • **الحد الأقصى لعدد كلمات المرور / أرقام التعريف الشخصية المخزنة** (القيمة الافتراضية هي 5). • **الحد من فترة صلاحية كلمة المرور / رمز PIN لأجل TPM (بالأيام)** (معطل بشكل افتراضي). • **استخدام رمز PIN المُحسن (حروف وأرقام)**. يسمح رمز PIN المحسّن باستخدام أحرف أخرى بالإضافة إلى الأحرف الرقمية: الأحرف اللاتينية الكبيرة والصغيرة والأحرف الخاصة والمسافات. معطل بشكل افتراضي.
إعادة إنشاء كلمة مفتاح الاسترداد تلقائيًا (بالأيام)	قم بتحديث كلمة المرور تلقائيًا لاستعادة الوصول إلى محرك الأقراص المحمي بواسطة BitLocker. وفي حالة تحديد خانة الاختيار، حدد فترة صلاحية كلمة مرور مفتاح الاسترداد. ويساعد هذا في منع إعادة استخدام كلمة مرور مفتاح الاسترداد.

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.

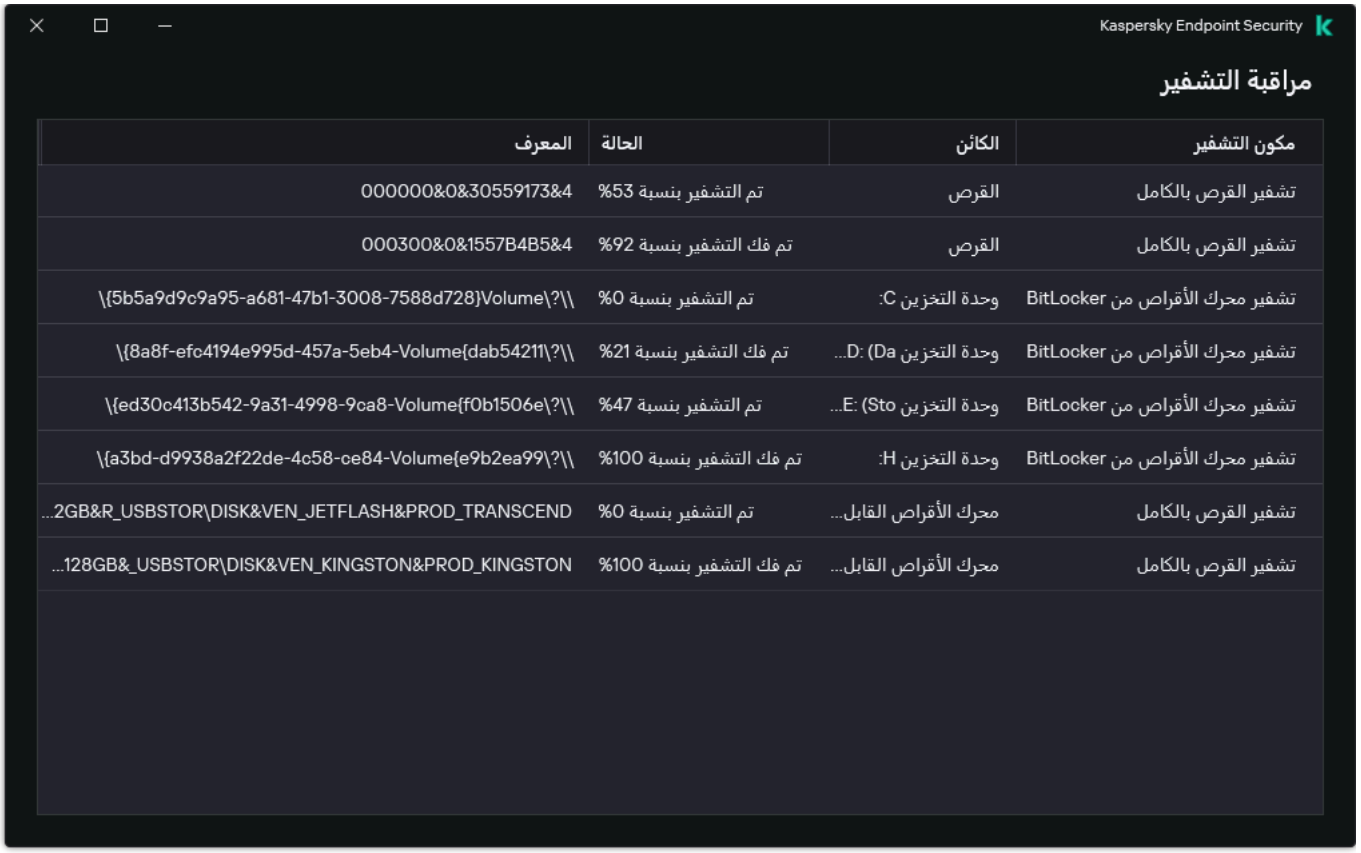
كيفية فك تشفير محرك أقراص محمي بتقنية BitLocker من خلال وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات ← تشفير القرص بالكامل**.
4. في القائمة المنسدلة **تقنية التشفير** حدد **تشفير محرك الأقراص من BitLocker**.
5. في القائمة المنسدلة **وضع التشفير** حدد **فك تشفير جميع محركات الأقراص الصلبة**.
6. احفظ تغييراتك.

كيفية فك تشفير محرك أقراص صلبة مشفر باستخدام BitLocker من خلال Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
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 Disk Encryption**.
6. في القسم **Action on devices**، 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:

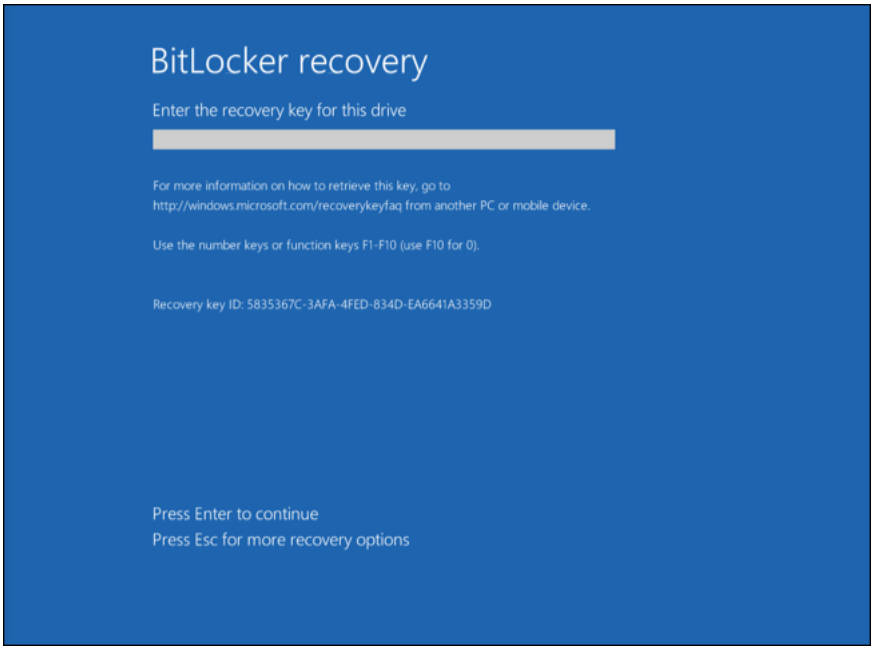
1. إخبار المستخدم للمسؤول بمعرف مفتاح الاسترداد (انظر الشكل أدناه).
2. تحقق المسؤول من معرف مفتاح الاسترداد في خصائص الكمبيوتر في Kaspersky Security Center. يجب أن يتطابق المعرف المقدم من قبل المستخدم مع المعرف المعروض في إعدادات الكمبيوتر.
3. إذا كان معرف مفتاح الاسترداد متطابقين، يقوم المسؤول بتوفير 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.

   لمنع إعادة استخدام كلمة مرور مفتاح الاسترداد، يمكنك تكوين التحديث التلقائي لكلمة المرور في إعدادات السياسة.
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 **Managed devices**.
3. في علامة التبويب **Devices**، 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. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **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 نافذة Web Console الرئيسية، حدد **Asset management ← Assets (Devices)**.
2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى محركه.

3. انقر على **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 مفتاح استرداد 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.

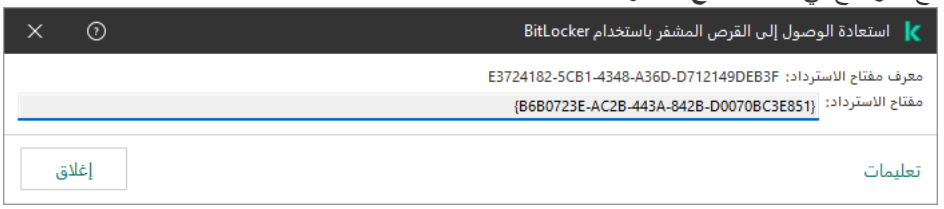
2. في شجرة وحدة تحكم الإدارة، حدد المجلد **Data encryption and protection** ← **Advanced** ← المجلد **Encrypted drives**.

3. في مساحة العمل، حدد الجهاز المشفر الذي تريد إنشاء ملف مفتاح وصول له، ثم في قائمة سياق الجهاز، انقر فوق **الحصول على الوصول إلى الجهاز في Kaspersky Endpoint Security**.

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 **Grant access to the device in offline mode**.
هذا يبدأ المعالج لمنح الوصول إلى جهاز.

4. اتبع تعليمات المعالج لمنح الوصول إلى جهاز:

a. حدد 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. ويمكنك تمكين مصادقة BitLocker في أي وقت.

كيفية إيقاف حماية BitLocker مؤقتًا باستخدام وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **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

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

كيفية إيقاف حماية BitLocker مؤقتًا باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Tasks** ← **Asset management**.
   تفتح قائمة المهام.
2. انقر على **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**.
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 **Devices to which the task will be assigned**، حدد نطاق المهمة.

الخطوة 2: إدارة حماية BitLocker

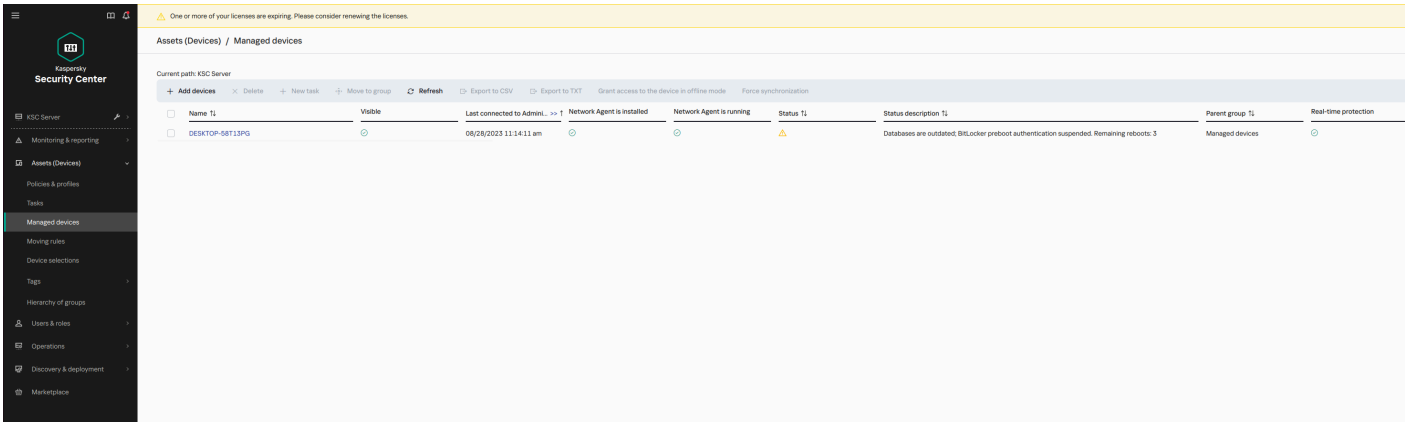
كوّن مصادقة BitLocker. لإيقاف حماية BitLocker مؤقتًا، حدد **Temporarily allow skipping BitLocker authentication** وأدخل عدد مرات إعادة التشغيل بدون مصادقة BitLocker (من 1 إلى 15 مرة). وإذا لزم الأمر، أدخل تاريخ ووقت انتهاء الصلاحية للمهمة. وفي الوقت المحدد، يتم إيقاف المهمة تلقائيًا، ويجب على المستخدم إكمال مصادقة BitLocker عند إعادة تشغيل الكمبيوتر.

الخطوة 3 إكمال إنشاء المهمة

قم بإنهاء المعالج. سيتم عرض مهمة جديدة في قائمة المهام.

لتشغيل مهمة، حدد خانة الاختيار المقابلة للمهمة 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 الاطلاع على عدد مرات إعادة التشغيل المتبقية في مجلد **Managed devices** في وحدة تحكم Kaspersky Security Center في وصف حالة الجهاز.



قائمة الأجهزة المدارة

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

لا يتم دعم تشفير الملفات على أجهزة الكمبيوتر القائمة على Arm.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.
4. في القائمة المنسدلة **وضع التشفير** حدد **وفقًا للقواعد**.

5. 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.

6. 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

بشكل افتراضي، تعمل جميع التطبيقات مع الملفات المشفرة في حالة فك تشفير. وإذا كنت تستخدم تطبيقات معينة كثيرًا (على سبيل المثال، المستعرضات أو محررات النصوص)، فيمكنك إنشاء قواعد وصول مشفرة لحماية المعلومات.

نوصي بإنشاء قاعدة وصول إلى ملف مشفر لمستعرضي Microsoft Internet Explorer وMicrosoft Edge. ونظرًا لطريقة عمل هذين المستعرضين، إذا قمت بتحميل ملف مشفر إلى موقع ويب (على سبيل المثال، التخزين السحابي)، يتم فك تشفير الملف تلقائيًا. ويمكن أن يتسبب هذا في تسرب البيانات. ولا يمكن تحميل ملف مشفر باستخدام هذين المستعرضين. نوصي بإعداد قاعدة **منح صلاحية الوصول إلى الملفات المشفرة في النص المشفر فقط**. ولا تحتاج إلى إنشاء قاعدة للمستعرضات الأخرى (مثل Google Chrome).

لتشكيل قواعد الوصول إلى الملفات المشفرة للتطبيقات:

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.
4. 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.

5. في الجزء الأيسر من النافذة، حدد علامة التبويب **قواعد التطبيقات**.
6. 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**.

7. 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**.

8. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.

4. 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.

5. في الجزء الأيسر من النافذة، حدد علامة التبويب **قواعد التطبيقات**.

6. 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**.

7. 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**.

8. احفظ تغييراتك.

إنشاء قاعدة فك تشفير

لإنشاء قاعدة فك تشفير:

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.

4. في القائمة المنسدلة **وضع التشفير** حدد **وفقًا للقواعد**.

5. 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.

6. 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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **Data Encryption** ← **File Level Encryption**.

4. في الجزء الأيسر من النافذة، حدد علامة التبويب **التشفير**.

5. 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 **حذف**.
تتم إضافة الملفات والمجلدات التي تمت إزالتها من قائمة التشفير تلقائيًا إلى قائمة فك التشفير.

6. تشكيل قائمة فك تشفير الملفات.

7. 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.

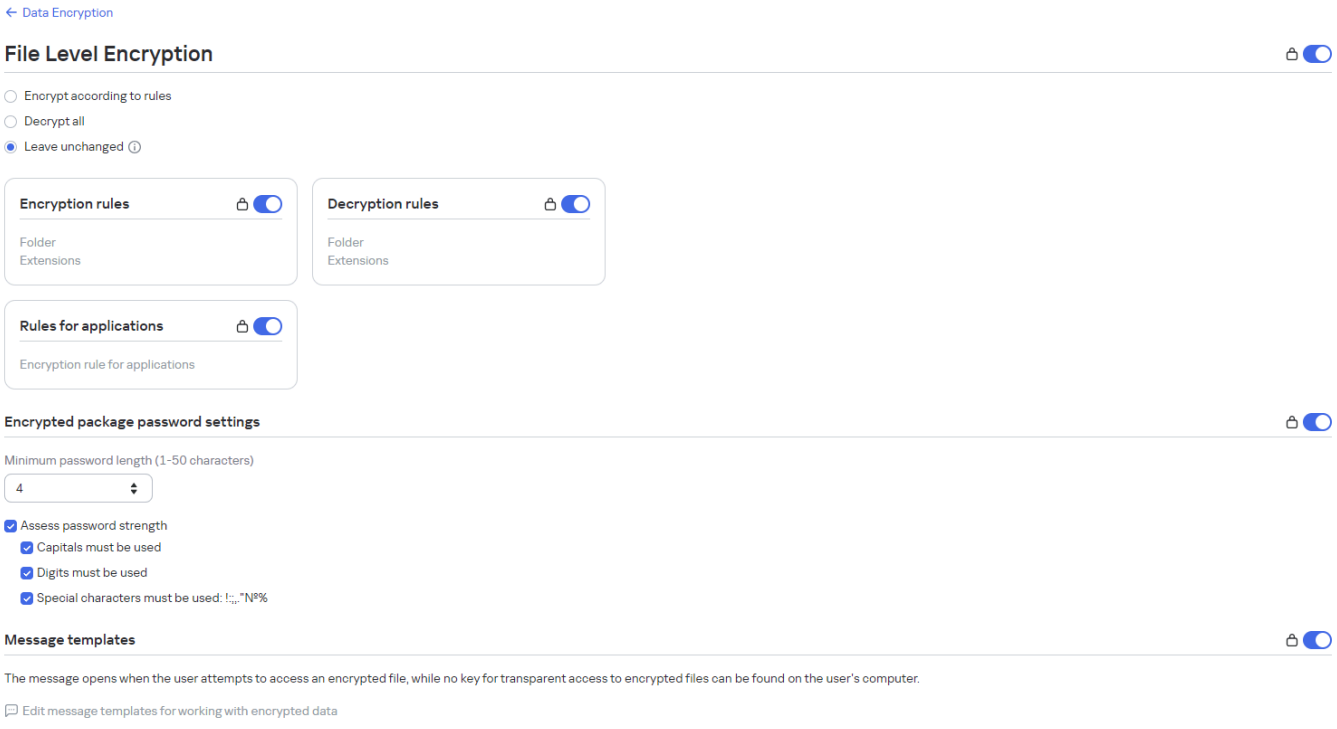
قبل إنشاء حزم مشفرة، سوف يطلب Kaspersky Endpoint Security من المستخدم إدخال كلمة المرور. لحماية بياناتك بشكل موثوق، يمكنك تفعيل التحقق من قوة كلمة المرور وتحديد متطلبات قوة كلمة المرور. هذا سوف يمنع المستخدمين من استخدام كلمات مرور بسيطة وقصيرة، مثل 1234.

كيفية تفعيل التحقق من قوة كلمة المرور عند إنشاء أجهزة مشفرة في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **إعدادات التشفير العامة**.
4. في القسم **إعدادات كلمة المرور**، انقر على الزر **الإعدادات**.
5. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **الحزم المشفرة**.
6. إعدادات تكوين كلمة المرور عند إنشاء حزم مشفرة.

كيفية تفعيل التحقق من قوة كلمة المرور عند إنشاء أجهزة مشفرة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
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.



إعدادات تشفير الملفات

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 **Devices**، 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. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **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 نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.
2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى بياناته.
3. انقر على **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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **إعدادات التشفير العامة**.
4. في القسم **القوالب**، انقر على الزر **القوالب**.
5. في النافذة التي تفتح، افعل ما يلي:

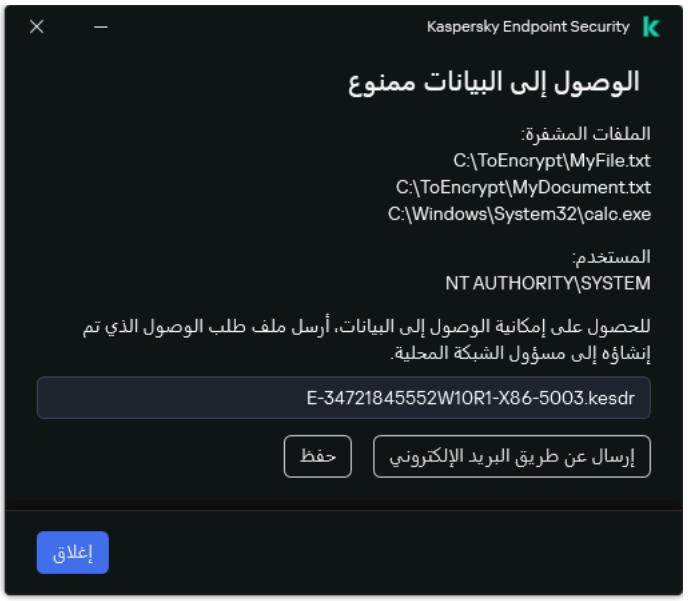
- إذا كنت تريد تحرير قالب رسالة المستخدم، فحدد علامة التبويب **رسالة المستخدم**. تفتح النافذة التالية عند محاولة المستخدم الوصول إلى ملف مشفر أثناء عدم وجود مفتاح متوفر على الكمبيوتر للوصول إلى الملفات المشفرة. يؤدي النقر فوق الزر **إرسال عن طريق البريد الإلكتروني** إلى إنشاء رسالة مستخدم تلقائيًا. يتم 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.

6. قم بتحرير قوالب الرسالة.

لإضافة متغير إلى نص القالب، ضع المؤشر في الموضع المطلوب، وانقر فوق **المتغير** وحدد المتغير المطلوب من قائمة الخيارات المتاحة.

يمكنك أيضًا استعادة نص القالب الافتراضي باستخدام الزر **افتراضيًا**.

7. احفظ تغييراتك.



طلب الوصول إلى الملفات المشفرة

تشفير محركات الأقراص القابلة للإزالة

لا يتم دعم تشفير محركات الأقراص القابلة للإزالة على أجهزة الكمبيوتر القائمة على Arm.

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:

- Full Disk Encryption (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").

- File Level Encryption (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 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.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.
4. 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.
5. 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.
6. 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.
7. إذا كنت تريد تكوين تشفير لمحركات الأقراص الفردية القابلة للإزالة، قم بتحديد قواعد التشفير.
8. 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.

9. احفظ تغييراتك.

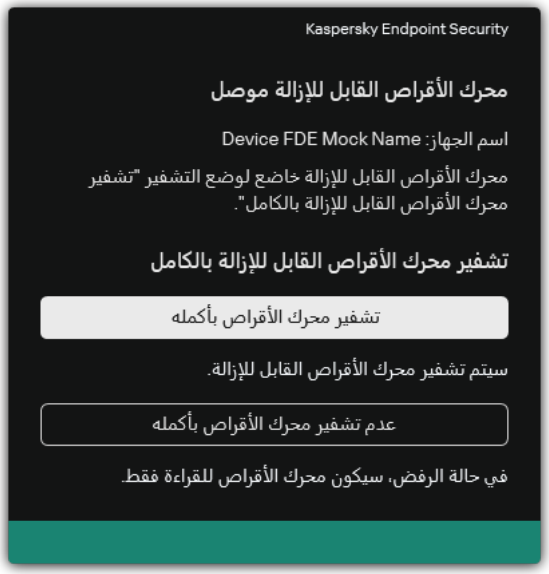
بعد تطبيق السياسة، عندما يقوم المستخدم بتوصيل محرك أقراص قابل للإزالة أو إذا كان محرك أقراص قابل للإزالة متصلاً بالفعل، يطالب برنامج Kaspersky Endpoint Security المستخدم بتأكيد إجراء عملية التشفير (انظر الشكل أدناه).

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.
4. 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**.
5. 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.
6. 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.
7. 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.
8. 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**.
9. 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. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.
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 **<N> 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.

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.

4. 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.

5. 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.

6. 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:

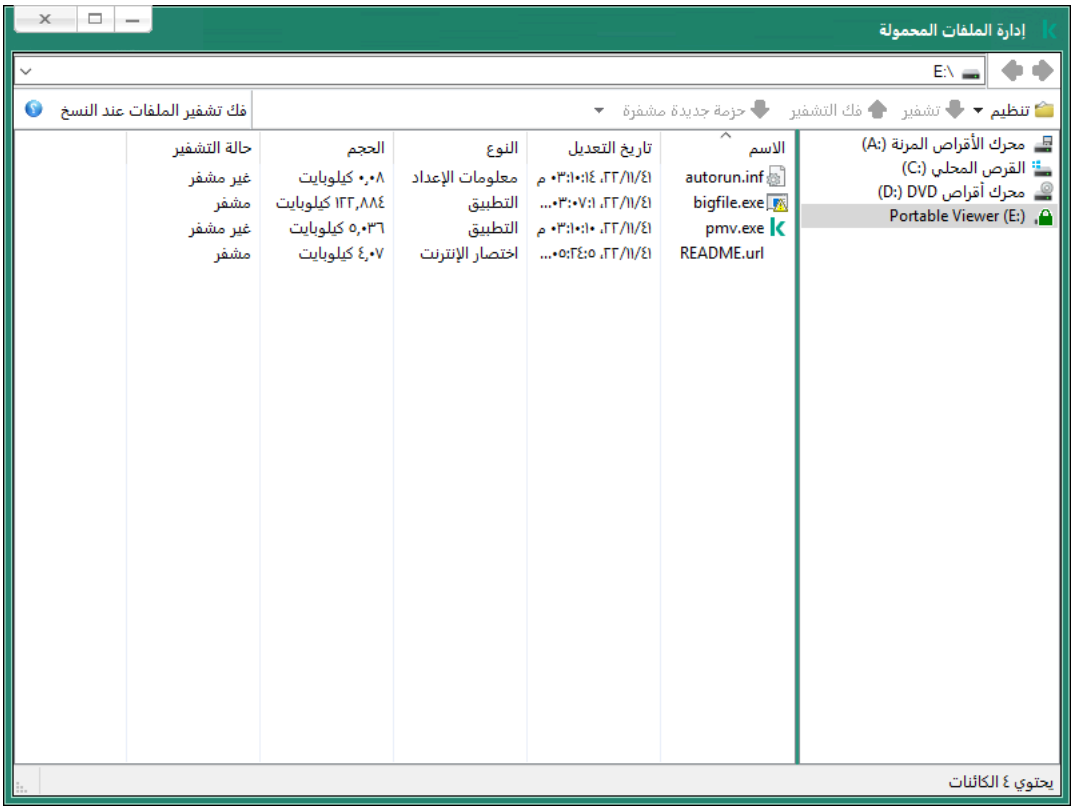
- لا يوجد اتصال بين الكمبيوتر وخادم إدارة Kaspersky Security Center.
- قد تغيرت البنية التحتية بتغير خادم إدارة Kaspersky Security Center.
- Kaspersky Endpoint Security غير مثبت على الكمبيوتر.

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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **تشفير البيانات** ← **تشفير محركات الأقراص القابلة للإزالة**.
4. 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).

5. حدد خانة الاختيار **الوضع المحمول**.
6. يمكنك إضافة قواعد التشفير لمحركات الأقراص القابلة للإزالة الفردية إذا كان ذلك ضروريًا.
7. احفظ تغييراتك.

8. بعد تطبيق السياسة، قم بتوصيل محرك الأقراص القابل للإزالة بجهاز الكمبيوتر.

9. 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

10. حدد كلمة مرور تفي بمتطلبات القوة وقم بالتأكيد عليها.

11. احفظ تغييراتك.

كيفية تفعيل دعم الوضع المحمول للعمل مع الملفات المشفرة الموجودة على محركات الأقراص القابلة للإزالة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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 **Default action**، 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 **Devices**، 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. يفتح هذا نافذة؛ وفي هذه النافذة، حدد علامة التبويب **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 نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي تريد استعادة الوصول إلى بياناته.

3. انقر على **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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **تشفير البيانات ← تشفير محركات الأقراص القابلة للإزالة**.

4. 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**.

5. 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 للزر **تعيين قاعدة**، حدد العنصر **فك تشفير محرك الأقراص القابل للإزالة بالكامل**.

6. 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.
- **Does not meet the policy due to an error**. خطأ في تشفير البيانات، على سبيل المثال، ترخيص مفقود.
- **Applying the policy; restart is required**. تشفير البيانات قيد التقدم على الكمبيوتر. أعد تشغيل الكمبيوتر لإكمال تشفير البيانات.
- **No encryption policy specified**. تم إيقاف تشفير البيانات في إعدادات السياسة.
- **(غير مدعوم)**. لم يتم تثبيت مكونات تشفير البيانات على الكمبيوتر.
- **Applying the policy**. 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 **Devices** 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 **Administration Server**.
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**Devices**.

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 **Devices**، 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:

- **Report on encryption status of managed devices**. ويتضمن التقرير معلومات عما إذا كانت حالة تشفير الكمبيوتر تتوافق مع سياسة التشفير.
- **Report on encryption status of mass storage devices**. ويتضمن التقرير معلومات عن حالة تشفير الأجهزة الخارجية وأجهزة التخزين.
- **Report on rights to access encrypted drives**. ويتضمن التقرير معلومات عن حالة الحسابات التي يمكنها الوصول إلى محركات الأقراص المشفرة.
- **Report on file encryption errors**. ويتضمن التقرير معلومات عن الأخطاء التي حدثت أثناء تنفيذ مهام تشفير البيانات أو فك تشفيرها على أجهزة الكمبيوتر.
- **Report on blockage of access to encrypted files**. 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 **Administration Server** من شجرة وحدة تحكم الإدارة، حدد علامة التبويب **Reports**.
3. انقر فوق الزر **قالب التقارير الجديد**.
   بدء تشغيل معالج قالب تقرير جديد.
4. اتبع تعليمات معالج قالب التقرير. في النافذة **Selecting the report template type** في القسم **Other** حدد أحد تقارير تشفير البيانات.
   بعد الانتهاء من استخدام معالج قالب تقرير جديد، يظهر قالب التقرير الجديد في الجدول في علامة التبويب **Reports**.
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 **Data encryption and protection** ← **Advanced** ← المجلد **Encrypted drives**.

3. في مساحة العمل، حدد الجهاز المشفر الذي تريد إنشاء ملف مفتاح وصول له، ثم في قائمة سياق الجهاز، انقر فوق **الحصول على الوصول إلى الجهاز في Kaspersky Endpoint Security**.

إذا لم تكن متأكدًا من الكمبيوتر الذي تم إنشاء ملف طلب الوصول له، ففي شجرة وحدة تحكم الإدارة حدد المجلد **Data encryption and protection** ← **Advanced** وفي مساحة العمل، انقر فوق **الحصول على مفتاح تشفير الجهاز في Kaspersky Endpoint Security**.

4. في النافذة التي تفتح، حدد خوارزمية التشفير لاستخدام: AES256 أو AES56.

تعتمد خوارزمية تشفير البيانات على مكتبة تشفير AES المضمنة في حزمة التوزيع: Strong encryption (AES256) أو Lite encryption (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 على **إلغاء تأمين**.

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 نافذة Web Console الرئيسية، حدد **Operations** ← **Data encryption and protection** ← **Encrypted drives**.

2. حدد خانة الاختيار بجوار اسم الكمبيوتر الذي ترغب في استرداد البيانات عليه.

3. انقر على **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. حدد خوارزمية التشفير التي سيتم استخدامها: AES256 أو AES56.

تعتمد خوارزمية تشفير البيانات على مكتبة تشفير AES المضمنة في حزمة التوزيع: Strong encryption (AES256) أو Lite encryption (AES56). يتم تثبيت مكتبة تشفير AES مع التطبيق.

c. حدد ملف طلب الوصول المستلم من المستخدم (ملف بامتداد FDERTC).

d. حدد مجلدًا لحفظ ملف مفتاح الوصول إلى البيانات المشفر (ملف بملحق 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

حلول Kaspersky Detection and Response هي أنظمة أمان لاكتشاف التهديدات المتقدمة ومؤشرات الهجوم على مستويات مختلفة من البنية التحتية للمؤسسة. وتوفر حلول Detection and Response معلومات عن التهديد المكتشف وتسمح بإدارة إجراءات الاستجابة للتهديدات.

لذلك، ينفذ حل Detection and Response ما يلي:

- استلام معلومات عن تشغيل الكمبيوتر أو الخادم أو الأجهزة الأخرى (القياس عن بُعد).
- تحليل المعلومات تلقائيًا لاكتشاف التهديدات.
- إنشاء تفاصيل التنبيه كأعمدة في سلسلة تطوير التهديد لتحليلها واختيار إجراءات الاستجابة للتهديد.
- تنفيذ إجراءات الاستجابة للتهديد (على سبيل المثال، عزل شبكة الاتصال الخاصة بالكمبيوتر).

يدعم Kaspersky Endpoint Security حلول Detection and Response باستخدام عامل مضمن. ويرسل العميل المدمج القياس عن بُعد إلى خوادم الحلول وينفذ إجراءات الاستجابة للتهديد. 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:
  - Endpoint Detection and Response (EDR) الإصدار 7.1 أو أقدم
  - Network Detection and Response (NDR)
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert (on-premises)
- Kaspersky Sandbox 2.0

يمكنك استخدام Kaspersky Endpoint Security مع حل Detection and Response في تكوينات مختلفة، على سبيل المثال، [EDR Optimum+MDR].

ترخيص MDR وEDR Optimum

يدعم Kaspersky Endpoint Security وظائف حلول Kaspersky Managed Detection and Response (MDR) و Kaspersky Endpoint Detection and Response Optimum (EDR Optimum). ويمكنك استخدام Kaspersky Endpoint Security مع هذه الحلول في تكوينات مختلفة وإنشاء نظام حماية مخصص يلبي متطلباتك الخاصة. ولفعل ذلك، يجب عليك شراء ترخيص لكل حل من هذين الحلين. وقد يغطي الترخيص الحق في استخدام حل واحد (على سبيل المثال، الوظيفة الإضافية لحل MDR فقط) أو عدة حلول، الوظيفة الإضافية لحل [EDR Optimum + MDR].

يدعم MDR و EDR Optimum طرق الترخيص التالية:

- تتم تغطية وظائف MDR أو EDR Optimum بواسطة ترخيص Kaspersky Endpoint Security for Windows.

  ستتوفر الوظائف فور تفعيل Kaspersky Endpoint Security for Windows. ولا تحتاج سوى إضافة مفتاح واحد.

- تراخيص منفصلة لكل من MDR أو EDR Optimum (MDR Add-on وEDR Optimum Add-on وAdd-on [EDR Optimum+MDR]).

تصبح الوظيفة متاحة بعد إضافة مفتاح منفصل للوظيفة الإضافية لحل MDR، أو الوظيفة الإضافية لحل EDR Optimum، أو الوظيفة الإضافية لحل [EDR Optimum+MDR]. ونتيجة لذلك، تتم إضافة مفتاحين على الكمبيوتر: مفتاح لحل Kaspersky Endpoint Security ومفتاح لحل MDR أو EDR Optimum. ويجب أن يكون مفتاح Kaspersky Endpoint Security هو أول مفتاح تتم إضافته.

يسمح Kaspersky Endpoint Security بإضافة مفتاح فعال واحد فقط لترخيص MDR وEDR Optimum. لذلك، إذا كنت بحاجة إلى تفعيل كلا الحلين، فيجب عليك إضافة مفتاح Add-on [EDR Optimum+MDR] واحد بدلاً من مفتاح منفصل لكل حل. ويمكنك أيضًا إضافة مفتاح احتياطي واحد.

إذا استخدمت ملف BLOB عند نشر MDR، فلن تحتاج إلى مفتاح منفصل لتفعيل MDR. ويحتوي ملف BLOB بالفعل على معلومات الترخيص.

الترخيص الأولي للحلول

عند نشر MDR وEDR Optimum لأول مرة، يتم تفعيل الحلول بالطريقة نفسها التي يتم تفعيل تطبيق Kaspersky Endpoint Security من خلالها. ويمكنك إضافة مفتاح باستخدام مهمة إضافة مفتاح أو استخدام وظيفة التوزيع التلقائي للمفاتيح. وتتم إضافة مفتاح الترخيص إلى التطبيق كمفتاح فعال ثانٍ أو كمفتاح احتياطي إذا حددت خانة الاختيار ذات الصلة.

التبديل من الترخيص إلى آخر

إذا كانت مؤسستك قد نشرت بالفعل أحد هذه الحلول، وتمت إضافة المفتاح المقابل إلى التطبيق، فهناك بعض الاعتبارات الخاصة المتعلقة بترخيص التكوين الجديد. وعند التبديل إلى ترخيص مختلف، لا يضيف التطبيق المفتاح الجديد إلى التطبيق، بل يستبدل المفتاح الحالي ليحل محل المفتاح الجديد. والسبب في ذلك هو التقييد الذي يسمح للتطبيق بإضافة مفتاح واحد فقط لتفعيل MDR وEDR Optimum.

على سبيل المثال، افترض أن مؤسستك نشرت حل [EDR Optimum+MDR]، وقررت التبديل إلى تكوين الوظيفة الإضافية لحل MDR. للتبديل إلى التكوين الجديد، يجب استبدال مفتاح Add-on [EDR Optimum+MDR] ليحل محله مفتاح MDR Add-on.

لم يعد الترخيص المنفصل لحل EDR Optimum وMDR (الوظيفة الإضافية لحل [EDR Optimum + MDR]) متاحًا. وإذا كنت تريد استخدام كلا الحلين، فيجب عليك تفعيل MDR باستخدام ملف BLOB، وEDR Optimum باستخدام مفتاح ترخيص.

باستخدام ميزة التوزيع التلقائي للمفاتيح، يرفض التطبيق مفاتيح الترخيص التي تغطي عدد الحلول نفسها. أي أنه إذا كان لديك مفتاح إضافي خاص بحل EDR، فلن يمكنك استبدال هذا المفتاح ليحل محله مفتاح الوظيفة الإضافية لحل MDR. ومع ذلك، يمكنك استبدال مفتاح الوظيفة الإضافية لحل EDR Optimum ليحل محله مفتاح الوظيفة الإضافية لحل [EDR Optimum + MDR]. ويرفض التطبيق أيضًا المفاتيح إذا حاولت استبدال مفتاح الوظيفة الإضافية لحل MDR بمفتاح الوظيفة الإضافية لحل EDR. لاستبدال مفتاح، يمكنك تشغيل مهمة إضافة مفتاح. تسمح مهمة إضافة مفتاح باستبدال مفاتيح الترخيص بأي عدد من الحلول.

إذا كان لديك مفتاح احتياطي تمت إضافته للوظيفة الإضافية لحل Add-on [EDR Optimum+MDR]، لإضافة مفتاح نشط بشكل صحيح للوظيفة الإضافية لحل EDR Optimum أو MDR، يجب عليك أولاً استبدال المفتاح الاحتياطي بمفتاح للوظيفة الإضافية لحل EDR Optimum أو الوظيفة الإضافية لحل MDR، أو بدلاً من ذلك، قم بإزالة المفتاح الاحتياطي ثم استبدل المفتاح الفعال.

التوافق مع حلول EDR للجهات الخارجية

يمكنك استخدام Kaspersky Endpoint Security لحماية محطات العمل والخوادم جنبًا إلى جنب مع حلول EDR من جهات خارجية. للتخلص من الإيجابيات الزائفة، نوصي بإضافة ملفات قابلة للتنفيذ من Kaspersky Endpoint Security وNetwork Agent إلى المنطقة الموثوقة لحل EDR الخاص بجهة خارجية.

	Kaspersky Endpoint Security for Windows	عميل شبكة Kaspersky Security Center
مجلد العمل	C:\Program Files (x86)\Kaspersky Lab\KES.14.2.0	C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
الملفات القابلة للتنفيذ	avp.exe avp.com avpsus.exe avpui.exe dump_writer_agent.exe kescli.exe kesdr.exe kldw.exe klpsm.exe kvdb_upgrader.exe modify_watcher.exe pmv.exe remediation.exe service_stub.exe	AVPDTAgt.exe fix_gflags.exe getsysteminfo.exe integrity_checker.exe klcpuld.exe klcsldcl.exe klcsngtgui.exe klcspxy.exe kldumper.exe klmover.exe klnagchk.exe klnagent.exe klnagntf.exe klnagwds.exe klosprep.exe klrbtagt.exe klscflag.exe klscmodchk.exe klshwmsg.exe klwd.exe ksnproxy.exe Patch.exe tslauncher.exe Up2Date.exe vapm.exe

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 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
3.11.0.216.mr1	11.8.0
3.11	11.7.0
3.10	11.6.0
3.9	11.5.0
3.9	11.4.0
3.9	11.3.0
3.9	11.2.0

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)	Kaspersky Anti Targeted Attack Platform (مكون Network Detection and Response)
11.5.0	Kaspersky Endpoint Agent	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	Kaspersky Endpoint Agent
11.7.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12.1	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	Kaspersky Endpoint Agent
12.6	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**	**العامل المُضمن**

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، ستتم 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 عميل الشبكة: على أجهزة كمبيوتر المستخدم وWeb Console.

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.

   لاستخدام Kaspersky Anti Targeted Attack Platform (NDR)، ستحتاج إلى مكون ويب إضافي للإصدار 12.7 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. تكون 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 الوظيفة الإضافية لحل Kaspersky Endpoint Detection and Response Optimum مستقلاً لتفعيل وظيفة EDR Optimum، فيجب عليك التأكد من إضافة مفتاح الوظيفة الإضافية لحل 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 and 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).
- إذا تم تمكين الحماية بكلمة مرور لتقييد الوصول إلى Kaspersky Endpoint Agent، فأدخل كلمة مرور إلغاء تثبيت التطبيق في إعدادات مهمة Install application remotely. ويمكنك إدخال كلمة مرور إلغاء التثبيت بدءًا من Kaspersky Security Center Linux 15.1.

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 الإصدار 13.2 أو أحدث من عميل الشبكة على الكمبيوتر.
- تحقق من حالة تشغيل العميل المدمج عن طريق عرض Report on status of application components. 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 Report on status of application components. وإذا كانت حالة مكون ما غير مشمول بالترخيص ، فتأكد من تشغيل وظيفة توزيع مفتاح الترخيص التلقائي لمكون EDR Optimum.

ترحيل السياسة والمهام لـ Kaspersky Endpoint Agent

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

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 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

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

قم بإنهاء 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>. تكون 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 **Connection 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 Kaspersky Endpoint Agent دون تغيير.

كيفية ترحيل إعدادات السياسة والمهام من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security في وحدة تحكم الإدارة (MMC) (فقط لتطبيق (KATA (EDR)

1. في وحدة تحكم الإدارة ، حدد خادم الإدارة وانقر بزر الماوس الأيمن لفتح قائمة السياق.

2. حدد **All tasks ← Policies and tasks batch conversion wizard**.

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

قم بإنهاء المعالج. ونتيجة للمعالج، سيتم إنشاء سياسة Kaspersky Endpoint Security جديدة.

Endpoint Detection and Response Agent (EDR Agent)

بدءًا من Kaspersky Endpoint Security 12.3 for Windows، يتضمن التطبيق تكوين وكيل Endpoint Detection and Response Agent (EDR Agent) . ويعد Endpoint Detection and Response Agent تطبيقًا يتم تثبيته على محطات العمل والخوادم الفردية في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة لدعم حلول Detection and Response بواسطة Kaspersky التالية:

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA) (بدءًا من الإصدار 12.6)
- Kaspersky Anti Targeted Attack Platform (NDR) (بدءًا من الإصدار 12.7)
- Kaspersky Endpoint Detection and Response Expert (on-premises) (بدءًا من الإصدار 12.11)

لا يدعم EDR Agent التكامل مع حل Kaspersky Endpoint Detection and Response Expert (cloud).

ويراقب EDR Agent العمليات التي يتم تشغيلها على أجهزة الكمبيوتر هذه بشكل مستمر، واتصالات الشبكة المفتوحة، والملفات التي يتم تعديلها. لا تتوفر مكونات الحماية والتحكم الخاصة بالتطبيق لعميل EDR.

يتوافق EDR Agent مع تطبيقات EPP التابعة لجهات خارجية. ويتيح لك ذلك استخدام أدوات أمان البنية التحتية التابعة لجهات خارجية إلى جانب Detection and Response بواسطة Kaspersky.

لنشر EDR Agent، يجب أن يكون عميل الشبكة مثبتًا على الكمبيوتر، ويجب إضافة الكمبيوتر في وحدة تحكم Kaspersky Security Center. ولتمكين تفاعل EDR Agent مع Kaspersky Security Center، يجب عليك تثبيت المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows. ويمكنك تحديد إعدادات EDR Agent باستخدام سياسة المجموعة. ولدمج EDR Agent، يجب عليك تكوين التكامل في أقسام السياسة المناسبة.

يجب تثبيت تطبيقات Kaspersky التالية على البنية التحتية لدعم حلول Kaspersky Detection and Response:

	• عميل الشبكة • EDR Agent
نقطة النهاية	

	المكون الإضافي لإدارة Kaspersky Endpoint Security for Windows
Kaspersky Security Center	
	
حلول الاكتشاف والاستجابة: MDR و(EDR) KATA و(NDR) KATA وKUMA و-EDR Expert (on-premises)	

تثبيت EDR Agent

يتم تثبيت Kaspersky Endpoint Security في تكوين عميل Endpoint Detection and Response Agent (EDR Agent) لحلول Kaspersky Detection and Response بالطريقة نفسها.

يمكن تثبيت EDR Agent على الكمبيوتر بإحدى الطرق التالية:

- عن بُعد باستخدام Kaspersky Security Center.
- محليًا، باستخدام معالج الإعداد.
- محليًا في سطر الأوامر (فقط لـ KATA (EDR) و(EDR Expert (on-premises).

لتثبيت EDR Agent، يجب عليك تحديد التكوين المناسب في إعدادات حزمة التثبيت أو في معالج الاعداد.

كيفية تثبيت EDR Agent باستخدام معالج الإعداد

1. انسخ مجلد حزمة التوزيع إلى كمبيوتر المستخدم.
2. قم بتشغيل setup_kes.exe.

يبدأ معالج الإعداد.

تكوين Kaspersky Endpoint Security



اختيار تكوين التطبيق

حدد تكوين **Endpoint Detection and Response Agent**. في هذا التكوين ، يمكنك فقط تثبيت المكونات التي توفر الدعم لحلول الاكتشاف والاستجابة: MDR و EDR (KATA) و NDR (KATA) و EDR Expert (on-premises)، وكذلك KUMA. ويعد هذا التكوين ضروريًا إذا تم نشر Endpoint Protection Platform (EPP) تابع لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.

مكونات برنامج Kaspersky Endpoint Security

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

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. يمكنك تمكين دعم Citrix Provisioning Services لتثبيت برنامج Kaspersky Endpoint Security إلى جهاز افتراضي.

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

كيفية تثبيت EDR Agent على سطر الأوامر (فقط لحل KATA (EDR) و(EDR Expert (on-premises)

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 /pSTANDALONEMODE=1 [/s]
```

أو

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
```

نتيجة لذلك، يتم تثبيت تطبيق EDR Agent للتكامل مع Kaspersky Anti Targeted Attack Platform (EDR) أو Kaspersky Endpoint Detection and Response Expert (on-premises) على الكمبيوتر. ويمكنك التأكد من تثبيت التطبيق والتحقق من إعدادات التطبيق عن طريق إصدار أمر `status`.

كيفية تثبيت EDR Agent باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Remote installation** ← **Advanced** ← المجلد **Installation packages**.

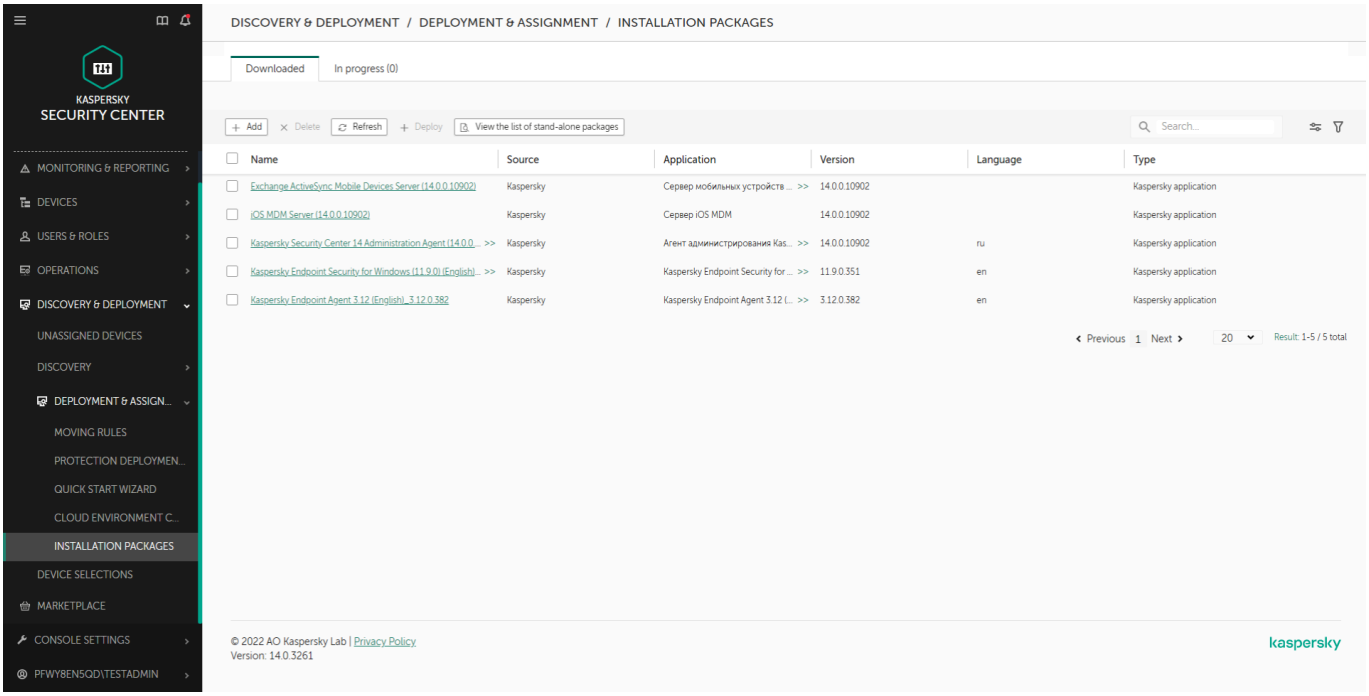
   يؤدي ذلك إلى فتح قائمة بحزم التثبيت التي تم تنزيلها إلى Kaspersky Security Center.
3. افتح خصائص حزمة التثبيت.

   اذا كان ضروريًا، أنشئ حزمة تثبيت جديدة.
4. انتقل إلى القسم **Protection components**.
5. حدد تكوين **Endpoint Detection and Response Agent للحماية من التهديدات المتقدمة والهجمات المستهدفة**. في هذا التكوين ، يمكنك فقط تثبيت المكونات التي توفر الدعم لحلول الاكتشاف والاستجابة: MDR و EDR (KATA) و NDR (KATA) و EDR Expert (on-premises)، وكذلك KUMA. ويعد هذا التكوين ضروريًا إذا تم نشر Endpoint Protection Platform (EPP) تابع لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.
6. حدد المكونات التي تريد تثبيتها.

   يمكنك تغيير مكونات التطبيقات المتاحة بعد تثبيت التطبيق.
7. احفظ تغييراتك.
8. أنشئ مهمة التثبيت عن بعد. في خصائص المهمة، حدد حزمة التثبيت التي أنشأتها.

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.



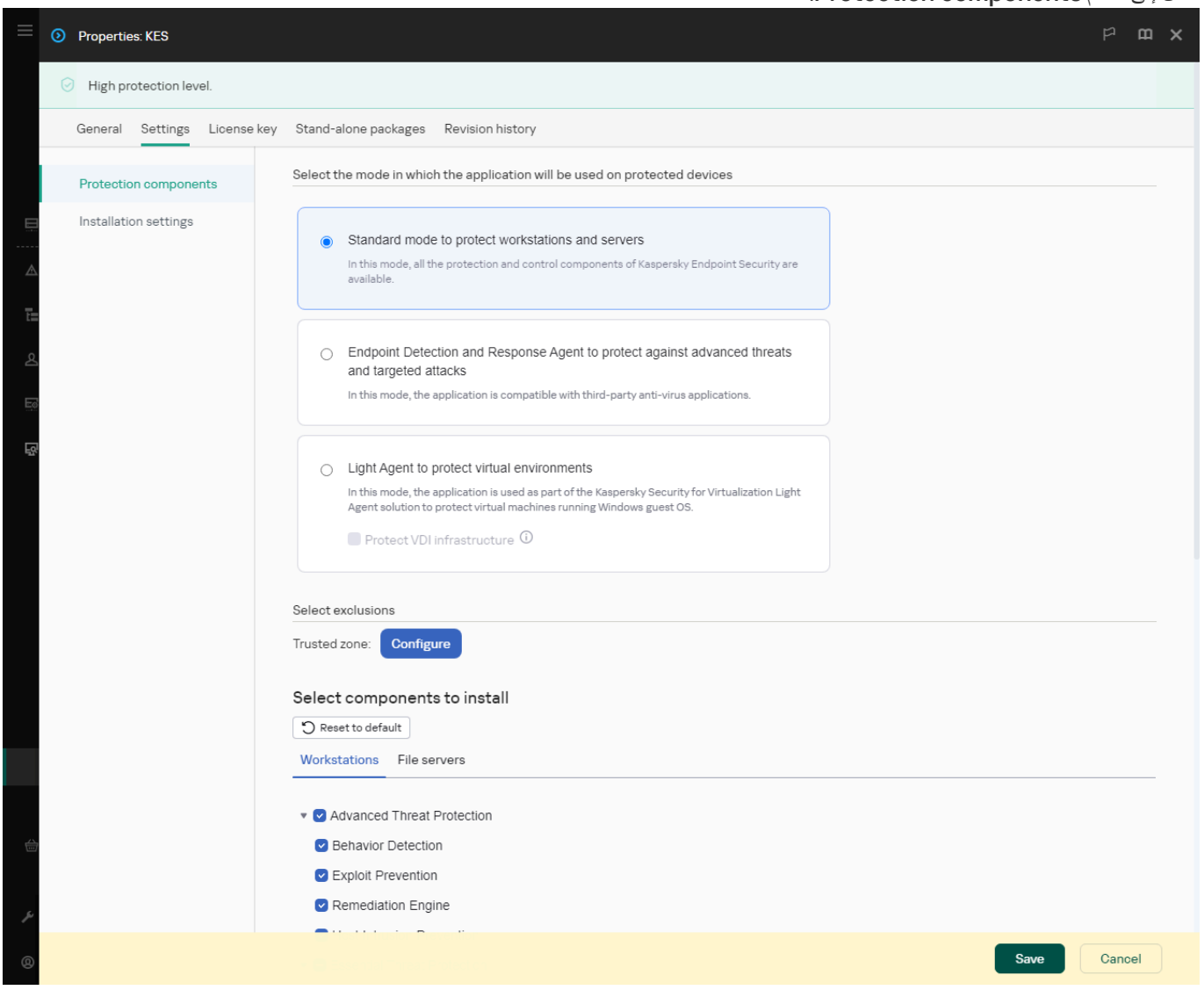
قائمة حزم التثبيت

2. افتح خصائص حزمة التثبيت.

اذا كان ضروريًا، أنشئ حزمة تثبيت جديدة.

3. حدد علامة التبويب **Settings**.

4. انتقل إلى القسم **Protection components**.



المكونات المضمنة في حزمة التثبيت

5. حدد تكوين **Endpoint Detection and Response Agent**. في هذا التكوين ، يمكنك فقط تثبيت المكونات التي توفر الدعم لحلول الاكتشاف والاستجابة: MDR و EDR (KATA) و NDR (KATA) و EDR Expert (on-premises)، وكذلك KUMA. ويعد هذا التكوين ضروريًا إذا تم نشر Endpoint Protection Platform (EPP) تابع لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.

6. حدد المكونات التي تريد تثبيتها.

يمكنك تغيير مكونات التطبيقات المتاحة بعد تثبيت التطبيق.

7. احفظ تغييراتك.

8. أنشئ مهمة التثبيت عن بعد. في خصائص المهمة، حدد حزمة التثبيت التي أنشأتها.

نتيجة لذلك، يتم تثبيت EDR Agent على الكمبيوتر. ويمكنك استخدام واجهة التطبيق ويتم عرض أيقونة التطبيق في منطقة الإخطارات.

في Kaspersky Security Center، يحتوي الكمبيوتر المثبت عليه التطبيق في تكوين EDR Agent على حالة Critical – ويتمتع الكمبيوتر بهذه الحالة لأن مكون الحماية من تهديدات الملفات مفقود. ولا يتعين عليك اتخاذ أي إجراء.

إذا لم تتمكن من تثبيت EDR Agent على جهاز كمبيوتر مزود بتطبيق EPP لجهة خارجية لأن برنامج التثبيت عثر على برنامج غير متوافق على جهاز الكمبيوتر، يمكنك تخطي فحص البرامج غير المتوافقة.



النافذة الرئيسية لحل EDR Agent

الآن يجب عليك تكوين التكامل مع Kaspersky Managed Detection and Response أو حل Kaspersky Anti Targeted Attack (EDR) أو Kaspersky Anti Targeted Attack (NDR). ويمكنك أيضًا تحديد الإعدادات المتقدمة للتطبيق، على سبيل المثال، إنشاء منطقة موثوقة أو إخفاء واجهة التطبيق. تتوفر الإعدادات في الأقسام التالية:

- Kaspersky Security Network
- إعدادات التطبيق
- إعدادات الشبكة
- الاستثناءات
- التقارير
- الواجهة
- إدارة الإعدادات

دمج EDR Agent مع MDR

يتم تثبيت EDR Agent على محطات العمل والخوادم في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة. ويعالج EDR Agent البيانات ويرسلها عبر تدفقات شبكة Kaspersky Security Network إلى Kaspersky Managed Detection and Response.

لكي يعمل Kaspersky Managed Detection and Response مع Administration Server عبر Kaspersky Security Center Web Console، يجب عليك 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.

إنشاء اتصال في الخلفية في Web Console

1. في نافذة Web Console الرئيسية، حدد **Integration** ← **Settings**.
2. انتقل إلى القسم **Integration**.
3. قم بتشغيل مفتاح **Background connection for integration Enabled**.
4. احفظ تغييراتك.

يتكون التكامل مع Kaspersky Managed Detection and Response من الخطوات التالية:

1. **تثبيت مكون Managed Detection and Response**

ويمكنك تحديد مكون MDR أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

لتثبيت مكون Managed Detection and Response دون إعادة تشغيل الكمبيوتر باستخدام مهمة تغيير مكونات التطبيق، تحتاج إلى تعطيل الخيار **التحقق من وجود تطبيقات جهات خارجية غير متوافقة** في إعدادات المهمة.

2. **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 <file name> 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: البنية التحتية: Kaspersky Private Security Network.

يجب عليك تمكين وضع KSN الموسع لكي يعمل مكون Managed Detection and Response.

3 **تفعيل Kaspersky Managed Detection and Response**

بدءًا من Kaspersky Endpoint Security for Windows 12.10، لتفعيل وظيفة الاكتشاف والاستجابة المُدارة، كبديل لرمز تفعيل، يمكنك أيضًا استخدام ملف مفتاح.

تحتاج إلى شراء ترخيص منفصل لمكون MDR (الوظيفة الإضافية لمكون Kaspersky Managed Detection and Response).

ستتوفر هذه الوظيفة بعد إضافة مفتاح منفصل لبرنامج Kaspersky Managed Detection and Response Add-on. الترخيص لوظيفة Managed Detection and Response المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

تأكد من تضمين وظيفة MDR في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

4 **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.

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تعد إضافة ملف BLOB اختياريًا لتطبيق Kaspersky Managed Detection and Response بدون مستأجرين إذا كان لديك ترخيص حالي.

كيفية تمكين مكون Managed Detection and Response في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **Detection and Response** ← **Managed Detection and Response (Industrial CyberSecurity)**.
4. حدد خانة الاختيار **Managed Detection and Response (Industrial CyberSecurity)**.
5. في القسم **الإعدادات**، انقر فوق **تحميل** وحدد ملف BLOB المستلم في وحدة تحكم Kaspersky Managed Detection and Response. يكون امتداد الملف P7.

بشكل افتراضي، يُسمح للمستخدم بإدارة إعدادات التطبيق ("القفل" مفتوح). لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

6. احفظ تغييراتك.

كيفية تكوين مكون Managed Detection and Response في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Managed Detection and Response**.
5. قم بتشغيل مفتاح **Managed Detection and Response ENABLED**.
6. انقر فوق **Upload** وحدد ملف BLOB الذي تم الحصول عليه في وحدة تحكم Kaspersky Managed Detection and Response.
يكون امتداد الملف P7.

بشكل افتراضي، يُسمح للمستخدم بإدارة إعدادات السياسة ("القفل" مفتوح). لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

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 بتنزيل الملف وإرسال الملف إلى الكمبيوتر أثناء المزامنة التالية مع Kaspersky Security Center. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. 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.

5 تكوين المكونات الأخرى للتطبيق لتلقي القياس عن بعد

يجب عليك تمكين المكونات التالية لكي يعمل مكون Managed Detection and Response:

- Kaspersky Security Network (الوضع الموسع).
- اكتشاف السلوك.
- منع الاستغلال.
- الحماية من تهديدات الويب.
- الحماية من تهديدات البريد.
- الحماية من تهديدات الملفات.

- الحماية من تهديدات الشبكة.
- جدار الحماية.
- حماية AMSI.
- فحص في الخلفية.

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Managed Detection and Response**.
5. قم بتشغيل مفتاح **Managed Detection and Response ENABLED**.
6. احفظ تغييراتك.

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **Detection and Response** ← **Managed Detection and Response (Industrial CyberSecurity)**.
4. حدد خانة الاختيار **Managed Detection and Response (Industrial CyberSecurity)**.
5. احفظ تغييراتك.

دمج EDR Agent مع EDR (KATA)

يتم تثبيت EDR Agent على محطات العمل والخوادم في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة. وعلى أجهزة الكمبيوتر هذه، يراقب EDR Agent بشكل مستمر العمليات واتصالات الشبكة المفتوحة والملفات التي يتم تعديلها، ويرسل بيانات المراقبة إلى الخادم باستخدام مكون العقدة المركزية.

للتكامل مع EDR (KATA)، يجب عليك تمكين مكون Endpoint Detection and Response (KATA) وتكوين EDR Agent.

يجب استيفاء الشروط التالية لكي يعمل Endpoint Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform الإصدارات 5.0–7.1.
- Kaspersky Security Center الإصدار 14.2 أو أحدث. في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة Endpoint Detection and Response (KATA).

https://www.youtube.com/watch?v=cZzgtBoeC7k

يتكون التكامل مع Endpoint Detection and Response (KATA) من الخطوات التالية:

1. **تفعيل Endpoint Detection and Response (KATA)**

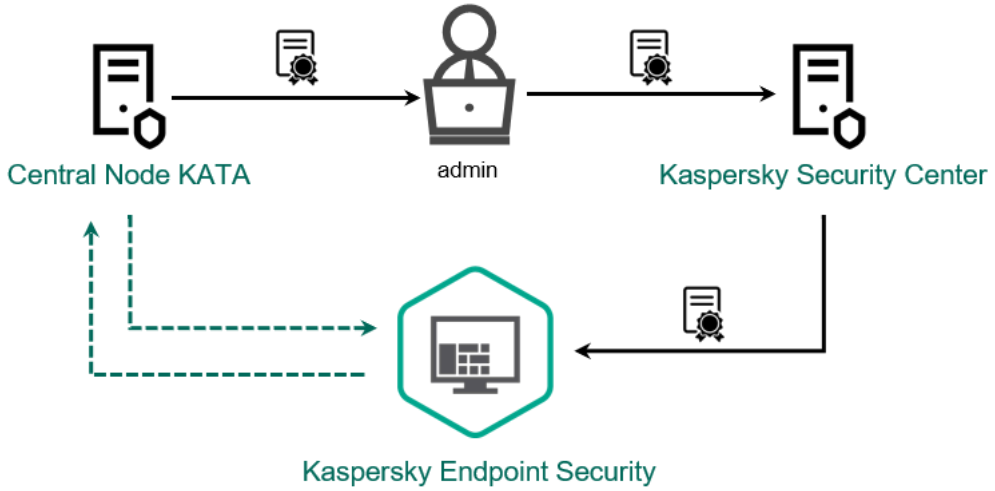
   تحتاج إلى شراء ترخيص منفصل لمكون EDR (KATA) (الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response (KATA)).

   ستتوفر الوظيفة بعد إضافة مفتاح منفصل لبرنامج 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.

2. **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 **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **Detection and Response** ← **Endpoint Detection and Response Expert (on-premises)**.
5. حدد خانة الاختيار **Endpoint Detection and Response Expert (on-premises)**.
6. انقر على **إعدادات اتصال الخادم**.
7. تكوين اتصال الخادم:
   - **المهلة (ثانية)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
   - **شهادة TLS للخادم**. 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).
   - **استخدام المصادقة ثنائية الاتجاه**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

   يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

8. انقر فوق **OK**.
9. أضف خوادم العقدة المركزية. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

   يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

10. إذا لزم الأمر، كوّن القياس عن بعد.
11. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون Central Node باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (on-premises)**.

5. قم بتشغيل مفتاح **Endpoint Detection and Response Expert (on-premises) ENABLED**.

6. لتكوين EDR (KATA)، حدد **Endpoint Detection and Response Expert (version 7.1 or earlier)** من قائمة الحلول.

7. انقر على **Connection settings**.

8. تكوين اتصال الخادم:

- **Timeout (sec)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
- **Server 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**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

9. انقر على **OK**.

10. أضف خوادم العقدة المركزية. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

11. إذا لزم الأمر، كوّن القياس عن بعد.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

نتيجة لذلك، تمت إضافة الكمبيوتر إلى وحدة تحكم Kaspersky Anti Targeted Attack Platform. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Endpoint Detection and Response Expert (on-premises)** إلى قائمة مكونات Kaspersky Endpoint Security.

دمج EDR Agent مع NDR (KATA)

يتم تثبيت EDR Agent على محطات العمل والخوادم في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة. وعلى أجهزة الكمبيوتر هذه، يراقب EDR Agent بشكل مستمر العمليات واتصالات الشبكة المفتوحة والملفات التي يتم تعديلها، ويرسل بيانات المراقبة إلى الخادم باستخدام مكون العقدة المركزية.

للتكامل مع NDR (KATA)، يجب عليك تمكين مكون Network Detection and Response (KATA) وتكوين EDR Agent.

يجب استيفاء الشروط التالية لكي يعمل Network Detection and Response (KATA):

- Kaspersky Anti Targeted Attack Platform الإصدار 7.0 أو أحدث.
- Kaspersky Security Center الإصدار 14.2 أو أحدث. في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة Network Detection and Response (KATA).

https://www.youtube.com/watch?v=gd-rySv0ThQ

يتكون التكامل مع Network Detection and Response (KATA) من الخطوات التالية:

1. **تفعيل Network Detection and Response (KATA)**

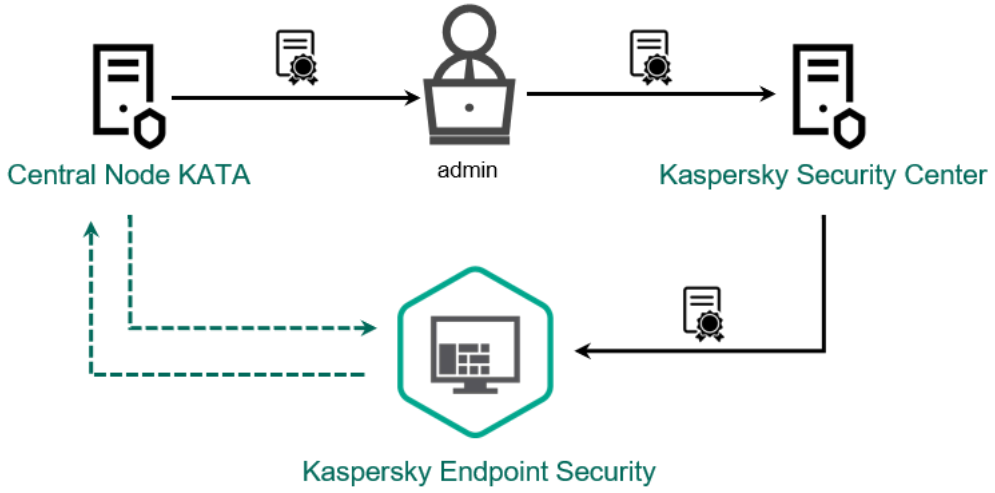
   تحتاج إلى شراء ترخيص منفصل لمكون NDR (KATA) (الوظيفة الإضافية لمكون Kaspersky Network Detection and Response (KATA)).

   ستتوفر الوظيفة بعد إضافة مفتاح منفصل لبرنامج Kaspersky Network Detection and Response (KATA). الترخيص لوظيفة Network Detection and Response (KATA) المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

   تأكد من تضمين وظيفة NDR (KATA) في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

2. **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. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **Detection and Response** ← **Network Detection and Response (KATA)**.
4. حدد خانة الاختيار **Network Detection and Response (KATA)**.
5. انقر على **Connection settings**.
6. تكوين اتصال الخادم:
   - **Timeout (sec)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
   - **Server 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**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

> يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

7. انقر على **OK**.
8. أضف خوادم العقدة المركزية. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.
9. يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.
10. إذا لزم الأمر، كوّن القياس عن بعد.
11. احفظ تغييراتك.

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون Central Node باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Built-in Agents Configuration** ← **Network Detection and Response (KATA)**.

5. قم بتشغيل مفتاح **Network Detection and Response (KATA) ENABLED**.

6. انقر على **Connection settings**.

7. تكوين اتصال الخادم:

- **Timeout (sec)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
- **Server 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**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

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. يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

11. إذا لزم الأمر، كوّن القياس عن بعد.

12. احفظ تغييراتك.

نتيجة لذلك، تمت إضافة الكمبيوتر إلى وحدة تحكم Kaspersky Anti Targeted Attack Platform. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Network Detection and Response (KATA)** إلى قائمة مكونات Kaspersky Endpoint Security.

دمج EDR Agent مع EDR Expert (on-premises)

يتم تثبيت EDR Agent على محطات العمل والخوادم في البنية التحتية لتكنولوجيا المعلومات الخاصة بالمؤسسة. وعلى أجهزة الكمبيوتر هذه، يراقب EDR Agent بشكل مستمر العمليات واتصالات الشبكة المفتوحة والملفات التي يتم تعديلها، ويرسل بيانات المراقبة إلى خادم EDR Expert (on-premises).

للتكامل مع خادم EDR Expert (on-premises)، يجب عليك تمكين مكون Endpoint Detection and Response Expert (on-premises) وتكوين EDR Agent.

يتكون التكامل مع Endpoint Detection and Response Expert (on-premises) من الخطوات التالية:

1. **تفعيل Kaspersky Endpoint Detection and Response Expert (on-premises)**

تحتاج إلى شراء ترخيص منفصل لمكون EDR Expert (on-premises) (الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response Expert (on-premises)).

ستتوفر الوظيفة بعد إضافة مفتاح منفصل لبرنامج Kaspersky Endpoint Detection and Response Expert (on-premises). الترخيص لوظيفة Endpoint Detection and Response (on-premises) المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

تأكد من تضمين وظيفة EDR Expert (on-premises) في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

2 **الاتصال بخادم جمع القياس عن بُعد وخادم الاستجابة**

يتطلب Kaspersky Endpoint Detection and Response Expert (on-premises) اتصالاً موثوقًا به بين Kaspersky Endpoint Security وخادمين:

- خادم جمع القياس عن بعد هو خادم يعد جزءًا من حل SIEM الذي يجمع المعلومات عن الأحداث التي تحدث على الكمبيوتر وتوحيدها وربطها وتحليلها وتخزينها.
- خادم الاستجابة هو خادم لاستلام البيانات وفحصها ودراسة سلوك الكائنات ونشر نتائج هذه الدراسات.

لتكوين اتصال موثوق، يجب عليك استخدام شهادة TLS. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد ذلك يجب عليك إضافة شهادة TLS إلى Kaspersky Endpoint Security (انظر الإرشادات أدناه).

بشكل افتراضي، يتحقق Kaspersky Endpoint Security فقط من شهادة TLS للخوادم. ولجعل الاتصال أكثر أمانًا، يمكنك أيضًا تمكين التحقق من الكمبيوتر على الخادم (المصادقة ثنائية الاتجاه). ولتمكين هذا التحقق، يجب عليك تشغيل المصادقة ثنائية الاتجاه في إعدادات الخادم وKaspersky Endpoint Security. ولاستخدام المصادقة ثنائية الاتجاه، ستحتاج أيضًا إلى حاوية تشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)).

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون EDR Expert (on-premises) باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (on-premises)**.
5. قم بتشغيل مفتاح **Endpoint Detection and Response Expert (on-premises) ENABLED**.
6. لتكوين EDR Expert (on-premises)، حدد **Endpoint Detection and Response Expert (version 8.0 or later)** من قائمة الحلول.
7. تكوين اتصال خوادم جمع القياس عن بعد:

   a. في القسم **Connection to telemetry collection servers**، انقر على الرابط **Connection settings**.

   b. تكوين اتصال خوادم جمع القياس عن بعد:

   - **Timeout (sec)**. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف.
   - **Server certificate**. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)).

- **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security والخادم. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات الخادم، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد تكوين إعدادات الخادم، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

c. انقر على **OK**.

d. أضف خوادم جمع القياس عن بعد. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

يمكنك إضافة عناوين متعددة لخادم جمع القياس عن بعد. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

e. إذا لزم الأمر، كوّن القياس عن بعد.

8. تكوين اتصال خوادم الاستجابة:

a. في القسم **Connection to response servers**، كوّن إعداد **Send sync request to server every (min)**. عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يتلقى Kaspersky Endpoint Security مهام الاستجابة للتهديدات ويرسل نتائج المهام.

b. انقر على رابط **Connection settings**.

c. تكوين اتصال خوادم الاستجابة:

- **Timeout (sec)**. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف.
- **Server certificate**. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security والخادم. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات الخادم، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد تكوين إعدادات الخادم، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

d. انقر على **OK**.

e. أضف خوادم الاستجابة. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

يمكنك إضافة عناوين متعددة لخادم الاستجابة. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

نتيجة لذلك، تتم إضافة الكمبيوتر إلى منصة الإدارة الواحدة المفتوحة (OSMP). تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Endpoint Detection and Response Expert (on-premises)** إلى قائمة مكونات Kaspersky Endpoint Security.

التوافق مع تطبيقات EPP للجهات الخارجية

يدعم EDR Agent وظائف حلول Kaspersky Detection and Response. لا تتوفر مكونات الحماية والتحكم لحل EDR Agent. ويسمح هذا التكوين بتثبيت تطبيقات EPP التابعة لجهات خارجية ونشر حلول Kaspersky Detection and Response في البنية التحتية للمؤسسة.

يتوافق EDR Agent مع تطبيقات EPP من الموردين التاليين:

- **Dr.Web**

  يتوافق EDR Agent مع Dr.Web Agent for Windows الإصدار 13 و 13.0.0.10200 (x64) Dr.Web Server.

- **Dallas Lock**

  يتوافق EDR Agent مع Dallas Lock 8.0-C الإصدار 843.2.

  لكي يعمل EDR Agent على جهاز كمبيوتر مثبت عليه برنامج Dallas Lock، يجب عليك السماح بالاتصال بخدمات Kaspersky الخارجية في إعدادات وحدة جدار الحماية.

- **Secret Net Studio**

  يتوافق EDR Agent مع Secret Net Studio الإصدار 8.11 (20851).

  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.

- **Trend Micro**

  يتوافق EDR Agent مع Trend Micro Vision One (بما في ذلك Security Agent الإصدار 14.0.20731).

  يتوافق EDR Agent مع Trend Micro Deep Security الإصدار 20.0.3-18160 (بما في ذلك Security Agent).

- **Windows Defender**

- **Sophos**

  يتوافق EDR Agent مع Sophos Intercept X الإصدار 2024.1.2 (بما في ذلك Endpoint Agent) وSophos Core Agent الإصدار 2026.2.1.3.

- **Bitdefender**

  يتوافق EDR Agent مع Bitdefender Endpoint Security Tools الإصدار 8.26.7.647.

- **ESET**

  يتوافق EDR Agent مع ESET Endpoint Security الإصدار 13.0.2044.0 وESET Management Agent الإصدار 13.2.1189.0.

على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 11 ببنية Arm64 ، لا يتوافق EDR Agent مع Bitdefender Endpoint Security Tools.

يجب تثبيت التطبيقات بالترتيب التالي: أولاً، قم بتثبيت تطبيق EPP، ثم Kaspersky Security Center Network Agent، ثم EDR Agent. ويعد ذلك ضروريًا لأن أداة تثبيت تطبيق EPP قد تكتشف أن EDR Agent وعميل الشبكة كبرنامجين غير متوافقين وتقوم بإزالتهما. ويجب أيضًا التحقق من تشغيل EDR Agent وNetwork Agent بعد تحديث تطبيق EPP التابع لجهة خارجية لأن المثبت الخاص به قد يعيد فحص الكمبيوتر بحثًا عن البرامج غير المتوافقة ويزيل التطبيقات.

إذا لم تتمكن من تثبيت EDR Agent على جهاز كمبيوتر مزود بتطبيق EPP لجهة خارجية لأن برنامج التثبيت عثر على برنامج غير متوافق على جهاز الكمبيوتر، يمكنك تخطي فحص البرامج غير المتوافقة.

Managed Detection and Response

يدعم Kaspersky Endpoint Security for Windows التكامل مع حل 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.

تكوينات Kaspersky Endpoint Security للتكامل مع MDR

يمكن استخدام التكوينات التالية للعمل مع MDR:

- **[KES+العميل المدمج]**. في هذا التكوين، يعمل Kaspersky Endpoint Security كتطبيق يضمن أمان الكمبيوتر وتطبيق للعمل مع MDR.
- **[EPP التابع لجهة خارجية+EDR Agent]**. في هذا التكوين، يتم توفير أمان البنية التحتية لتكنولوجيا المعلومات من خلال منصات حماية نقطة النهاية (EPP) التابعة لجهة خارجية. ويتم توفير التفاعل مع MDR بواسطة Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent (EDR Agent). وفي هذا التكوين، يكون EDR Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.

تكامل العميل المدمج مع MDR

لإعداد التكامل مع Kaspersky Managed Detection and Response، يجب عليك تمكين مكون Managed Detection and Response وتكوين Kaspersky Endpoint Security.

لكي يعمل Kaspersky Managed Detection and Response مع Administration Server عبر Kaspersky Security Center Web Console، يجب عليك 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.

إنشاء اتصال في الخلفية في Web Console

1. في نافذة Web Console الرئيسية، حدد **Integration** ← **Settings**.

2. انتقل إلى القسم **Integration**.

3. قم بتشغيل مفتاح **Background connection for integration Enabled**.

4. احفظ تغييراتك.

يتكون التكامل مع Kaspersky Managed Detection and Response من الخطوات التالية:

1 **تثبيت مكون Managed Detection and Response**

ويمكنك تحديد مكون MDR أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

لتثبيت مكون Managed Detection and Response دون إعادة تشغيل الكمبيوتر باستخدام مهمة تغيير مكونات التطبيق، تحتاج إلى تعطيل الخيار **التحقق من وجود تطبيقات جهات خارجية غير متوافقة** في إعدادات المهمة.

2 **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 `<file name>` 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: البنية التحتية: Kaspersky Private Security Network.

يجب عليك تمكين وضع KSN الموسع لكي يعمل مكون Managed Detection and Response.

3 تفعيل Kaspersky Managed Detection and Response

بدءًا من Kaspersky Endpoint Security for Windows 12.10، لتفعيل وظيفة الاكتشاف والاستجابة المُدارة، كبديل لرمز تفعيل، يمكنك أيضًا استخدام ملف مفتاح.

يدعم Kaspersky Managed Detection and Response طرق الترخيص التالية:

- تتم تغطية وظيفة Managed Detection and Response بواسطة ترخيص Kaspersky Endpoint Security for Windows.

  ستتوفر الوظائف فور تفعيل Kaspersky Endpoint Security for Windows.

- يتم استخدام ترخيص منفصل لحل MDR (الوظيفة الإضافية لحل Kaspersky Managed Detection and Response).

  ستتوفر هذه الوظيفة بعد إضافة مفتاح منفصل لبرنامج Kaspersky Managed Detection and Response Add-on. ونتيجة لذلك، تتم إضافة مفتاحين على الكمبيوتر: مفتاح لحل Kaspersky Endpoint Security ومفتاح لحل Kaspersky Managed Detection and Response.

  الترخيص لوظيفة Managed Detection and Response المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

تأكد من تضمين وظيفة MDR في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

4 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.

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تعد إضافة ملف BLOB اختياريًا لتطبيق Kaspersky Managed Detection and Response بدون مستأجرين إذا كان لديك ترخيص حالي.

كيفية تمكين مكون Managed Detection and Response في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **Detection and Response ← Managed Detection and Response (Industrial CyberSecurity)**.
4. حدد خانة الاختيار **Managed Detection and Response (Industrial CyberSecurity)**.
5. في القسم **الإعدادات**، انقر فوق **تحميل** وحدد ملف BLOB المستلم في وحدة تحكم Kaspersky Managed Detection and Response. يكون امتداد الملف P7.

بشكل افتراضي، يُسمح للمستخدم بإدارة إعدادات التطبيق ("القفل" مفتوح). لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

6. احفظ تغييراتك.

كيفية تكوين مكون Managed Detection and Response في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies ← Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** ← **Managed Detection and Response**.

5. قم بتشغيل مفتاح **Managed Detection and Response ENABLED**.

6. انقر فوق **Upload** وحدد ملف BLOB الذي تم الحصول عليه في وحدة تحكم Kaspersky Managed Detection and Response. يكون امتداد الملف P7.

بشكل افتراضي، يُسمح للمستخدم بإدارة إعدادات السياسة ("القفل" مفتوح). لتطبيق السياسة على أجهزة الكمبيوتر، أغلق الأقفال.

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 بتنزيل الملف وإرسال الملف إلى الكمبيوتر أثناء المزامنة التالية مع Kaspersky Security Center. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. 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.

5 تكوين المكونات الأخرى للتطبيق لتلقي القياس عن بعد

يجب عليك تمكين المكونات التالية لكي يعمل مكون Managed Detection and Response:

- Kaspersky Security Network (الوضع الموسع).
- اكتشاف السلوك.
- منع الاستغلال.
- الحماية من تهديدات الويب.
- الحماية من تهديدات البريد.
- الحماية من تهديدات الملفات.
- الحماية من تهديدات الشبكة.
- جدار الحماية.
- حماية AMSI.

- فحص في الخلفية.

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Managed Detection and Response**.
5. قم بتشغيل مفتاح **Managed Detection and Response ENABLED**.
6. احفظ تغييراتك.

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **Detection and Response** ← **Managed Detection and Response (Industrial CyberSecurity)**.
4. حدد خانة الاختيار **Managed Detection and Response (Industrial CyberSecurity)**.
5. احفظ تغييراتك.

دليل الترحيل من KEA إلى KES لحل MDR

يتضمن Kaspersky Endpoint Security for Windows عميلاً مضمنًا لحل Kaspersky Managed Detection and Response. ولم تعد بحاجة إلى تطبيق Kaspersky Endpoint Agent منفصل للعمل مع MDR. وسيتم تنفيذ جميع وظائف Kaspersky Endpoint Agent بواسطة Kaspersky Endpoint Security.

عند نشر Kaspersky Endpoint Security على أجهزة الكمبيوتر المُثبت عليها Kaspersky Endpoint Agent، سيستمر حل Kaspersky Managed Detection and Response 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 11.6.0 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 Kaspersky Managed Detection and Response:

- الإصدار 13.2 من Kaspersky Security Center أو أحدث (بما في ذلك عميل الشبكة). في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة Managed Detection and Response.
- يتم إنشاء اتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة. لكي يعمل MDR مع خادم الإدارة عبر Kaspersky Security Center Web Console، يجب عليك إنشاء اتصال آمن جديد، اتصال في الخلفية.

خطوات ترحيل تكوين [KES+KEA] إلى [KES+العامل المضمن] لحل MDR

1. **ترقية المكون الإضافي لتطبيق Kaspersky Endpoint Security Management**

يمكن إدارة مكون MDR باستخدام Kaspersky Endpoint Security Management Plug-in الإصدار 11.6 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 نافذة Web Console الرئيسية، 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 MDR. تخط هذه الخطوة.

الخطوة 3. اكتمال المعالج

قم بإنهاء 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>. تكون حالة السياسة الجديدة Inactive. وللمتابعة، قم بتغيير حالات سياسات Kaspersky Endpoint Security وKaspersky Endpoint Agent إلى Inactive وقم بتفعيل السياسة المدمجة الجديدة.

- 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.

3. **ترخيص وظيفة MDR**

لتفعيل Kaspersky Endpoint Security كجزء من حل Kaspersky Managed Detection and Response، تحتاج إلى ترخيص منفصل للوظيفة الإضافية لحل Kaspersky Managed Detection and Response. يمكنك استبدال المفتاح باستخدام مهمة Add key. نتيجة لذلك، ستتم إضافة مفتاحين إلى التطبيق: Kaspersky Endpoint Security وKaspersky Managed Detection and Response.

4 تثبيت / ترقية تطبيق Kaspersky Endpoint Security

لترحيل وظائف MDR أثناء تثبيت تطبيق أو ترقيته، يوصى باستخدام مهمة التثبيت عن بعد. وعند إنشاء مهمة تثبيت عن بُعد، تحتاج إلى تحديد مكون MDR 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 MDR، يقوم مُثبّت Kaspersky Endpoint Security تلقائيًا بتكوين مجموعة المكونات ويحدد مكون MDR. 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 العميل المدمج عن طريق عرض Report on status of application components. 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.

Endpoint Detection and Response

يتضمن Kaspersky Endpoint Security for Windows عميلاً مضمنًا لحل Kaspersky Endpoint Detection and Response Optimum (المشار 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.

أدوات معلومات التهديدات

يستخدم Kaspersky Endpoint Detection and Response أدوات Threat Intelligence التالية:

- التكامل مع Kaspersky Threat Intelligence Portal، التي تحتوي على معلومات عن سمعة الملفات وعناوين الويب وتعرضها.
- قاعدة بيانات التهديدات الخاصة بشركة Kaspersky.
- 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.
- تقنية Cloud Sandbox التي تتيح لك تشغيل الملفات المكتشفة في بيئة معزولة والتحقق من سمعتها.

مبدأ تشغيل الحل

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. ويعد التنبيه حدثًا في البنية التحتية لتكنولوجيا المعلومات للشركة حدده التطبيق على أنه غير عادي أو مشكوك فيه ويمكن أن يشكل تهديدًا أمنيًا للبنية التحتية لتكنولوجيا المعلومات الخاصة بالشركة. 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.

دعم الإصدارات السابقة من Kaspersky Endpoint Security

إذا كنت تستخدم Kaspersky Endpoint Security 11.2.0–11.6.0 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. 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).

تكامل العميل المدمج مع EDR Optimum / EDR Expert

لإعداد التكامل مع Kaspersky Endpoint Detection and Response، يجب عليك إضافة مكون Endpoint Detection and Response Optimum أو مكون Endpoint Detection and Response Expert (cloud) وتكوين Kaspersky Endpoint Security.

لا تتوافق مكونات Endpoint Detection and Response Optimum وEndpoint Detection and Response Expert (cloud) و Endpoint Detection and Response Expert (on-premises) 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.
- المكون الإضافي لإدارة Kaspersky Endpoint Detection and Response.

  بدءًا من الإصدار 12.6 من Kaspersky Endpoint Security، تم نقل عرض تفاصيل التنبيه من المكون الإضافي لإدارة Kaspersky Endpoint Security إلى المكون الإضافي لإدارة EDR. والمكون الإضافي لإدارة EDR هو مكون إضافي واحد للعمل مع العملاء على أنظمة تشغيل Windows وLinux وMac. والآن، عند العمل مع EDR Optimum، ستحتاج إلى مكون إدارة Kaspersky Endpoint Security الإضافي لإنشاء مهام الاستجابة للتهديدات والمكوّن الإضافي لإدارة EDR لعرض تفاصيل التنبيه.
- يدعم مكون Endpoint Detection and Response 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.
- 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**

   ويمكنك تحديد مكون Endpoint Detection and Response Optimum أو Endpoint Detection and Response Expert (cloud) 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 الوظائف 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 الوظيفة بعد إضافة مفتاح منفصل لبرنامج Kaspersky Endpoint Detection and Response. ونتيجة لذلك، تتم إضافة 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.

للمزيد من المعلومات عن اتفاقية ترخيص المستخدم النهائي لحل EDR Optimum، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum.

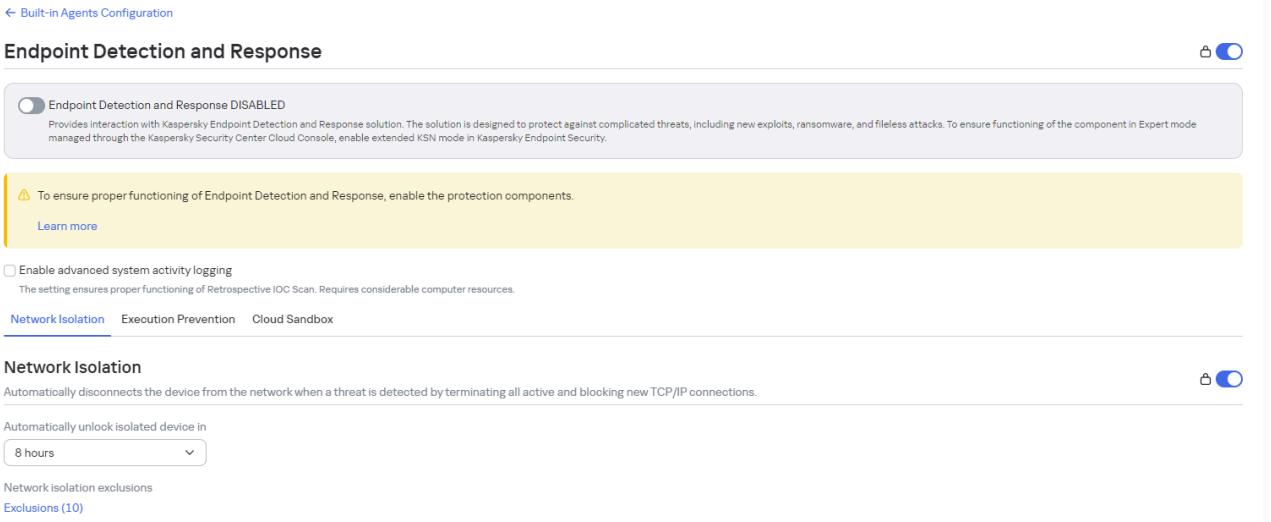
3 **تمكين مكون Endpoint Detection and Response**

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

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response**.
5. قم بتشغيل مفتاح **Endpoint Detection and Response ENABLED**.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.



إعدادات تكامل EDR

يتم تمكين مكون Kaspersky Endpoint Detection and Response. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. 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 (cloud)** 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. على سبيل المثال، يمكنك تنزيل ملف من العزل للتحليل في وحدة تحكم ويب.

- بيانات سلسلة تطور التهديد.

  البيانات مطلوبة للحصول على معلومات عن التهديدات المكتشفة على جهاز كمبيوتر في Web Console. ويمكنك عرض تفاصيل التنبيه واتخاذ إجراءات الاستجابة في Web Console.

كيفية تمكين نقل البيانات إلى خادم الإدارة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **KSC Integration**.
5. في القسم **Data transfer to Administration Server**، انقر على الرابط **Advanced settings**.
6. في النافذة التي تفتح، حدد خانات الاختيار التالية:
   - **About Quarantine files**.
   - **About a threat development chain**.
7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

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 IOC Scan 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 مؤشر الاختراق (IOC) مع معيار OpenIOC.

وضع تشغيل مهمة IOC Scan

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 مؤشر الاختراق (IOC) التي أعدها المستخدم. وإذا كنت ترغب في إضافة مؤشر الاختراق يدويًا، فيرجى قراءة متطلبات ملفات مؤشر الاختراق (IOC).

يحتوي الملف الذي يمكنك تنزيله بالنقر فوق الارتباط أدناه على جدول يحتوي على قائمة كاملة بشروط IOC لمعيار OpenIOC.

تنزيل ملف IOC_TERMS.XLSX

يدعم Kaspersky Endpoint Security أيضًا مهام مسح IOC المستقلة عند استخدام التطبيق كجزء من حل Kaspersky Sandbox.

إنشاء ملف مؤشرات الاختراق

بدءًا من Kaspersky Endpoint Security 12.10 for Windows، يمكنك إنشاء دليل ملفات مؤشرات الاختراق في إعدادات المهمة. لإنشاء ملف مؤشرات الاختراق، يجب عليك تحضير ملف TXT مع قائمة بمؤشرات الاختراق. ويمكنك إضافة قوائم بالكائنات التالية كمؤشرات اختراق:

- تجزئات الملف (MD5 / SHA256).
  يجهز التطبيق ملف مؤشرات الاختراق مع نطاق فحص FileItem/Md5sum أو FileItem/Sha256sum.
- عناوين IP (IPv4، IPv6).
  يجهز التطبيق ملف مؤشرات الاختراق مع نطاق فحص PortItem/RemoteIP.
- أسماء DNS.
  يجهز التطبيق ملف مؤشرات الاختراق مع نطاق فحص DnsEntryItem/RecordName.

كيفية إنشاء مؤشرات الاختراق في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Tasks** ← **Asset management**.
   تفتح قائمة المهام.
2. حدد مهمة **IOC Scan**.
   نافذة خصائص المهمة. إذا لزم الأمر، أنشئ مهمة **IOC Scan**.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى القسم **Threat Scan**.
5. انقر على **Redefine IOC files**.
6. يؤدي ذلك إلى فتح نموذج لإنشاء ملف مؤشرات الاختراق:
   a. تحت **IOC files source**، حدد **Generate from file**.
   b. أدخل اسمًا لملف مؤشرات الاختراق.
   c. حدد ملف TXT يتضمن قائمة مؤشرات الاختراق.
   d. حدد نوع ملف مؤشرات الاختراق: **DNS names** أو **File hashes** أو **IP addresses**.
   e. انقر على **Upload**.

   يضيف Kaspersky Endpoint Security ملفات مؤشرات الاختراق إلى مجموعة مؤشرات الاختراق. وإذا لزم الأمر، يمكنك استثناء ملفات مؤشرات الاختراق مؤقتًا من نطاق المهمة.
7. احفظ تغييراتك.

إنشاء مهمة IOC Scan

تستطيع إنشاء مهام IOC Scan 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.

يتعذر تشغيل المهمة الجماعية IOC Scan إذا تم تكوين التكامل مع Kaspersky Endpoint Detection and Response Expert (on-premises) أو Kaspersky Endpoint Detection and Response Expert (cloud) على أجهزة الكمبيوتر التي يتم فحصها. وفي هذه الحالة، نوصي باستخدام فحص IOC استجابة للبحث عن مؤشرات الحل الوسط. وللمزيد من التفاصيل، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises).

يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة IOC Scan:

1. في نافذة Web Console الرئيسية، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر على **Add**.

يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application** حدد **Kaspersky Endpoint Security for Windows 14.2**.

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

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

d. في القسم **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 IOC Scan 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. قم بإنهاء 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 **Threat Scan**.

10. قم بتحميل ملفات مؤشرات الاختراق للبحث عن مؤشرات الاختراق.

بعد تحميل ملفات مؤشرات الاختراق، يعرض التطبيق معلومات موجزة عن الملف، بما في ذلك قائمة المؤشرات التي لم تجتز الفحص. بعد تحميل ملفات مؤشرات الاختراق، يمكنك تحرير الملفات يدويًا في المحرر المدمج مباشرة في خصائص المهمة. ويدعم Kaspersky Endpoint Security تحرير ملفات مؤشرات الاختراق المتوافقة مع معيار OpenIOC 1.1. ولا يمكن تعديل محتوى ملفات مؤشر الاختراق المتوافقة مع الإصدار 1.0 من OpenIOC.

يضيف Kaspersky Endpoint Security ملفات مؤشرات الاختراق إلى مجموعة مؤشرات الاختراق. وإذا لزم الأمر، يمكنك استثناء ملفات مؤشرات الاختراق مؤقتًا من نطاق المهمة.

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. وإذا لزم الأمر، حدد خانة الاختيار **Retrospective IOC Scan**. فحص مؤشر الاختراق بأثر رجعي هو وضع لمهمة IOC Scan يفحص فيها Kaspersky Endpoint Security مؤشرات الاختراق باستخدام البيانات لفترة زمنية معينة. ويهدف هذا الوضع إلى البحث عن مؤشرات الاختراق عن طريق القياس عن بُعد للكمبيوتر المحمي مثل نشاط الشبكة والعمليات والملفات والقياس عن بُعد الآخر. ويحلل Kaspersky Endpoint Security البيانات في سجلات نظام التشغيل وسجلات المستعرض على الكمبيوتر. يحلل فحص مؤشر الاختراق الاستعادي سجلات المستعرضات التالية: Google Chrome وMozilla Firefox وMicrosoft Edge (الإصدار 79 أو أحدث).

12. تكوين الإجراءات عند اكتشاف IOC:

- **Isolate device 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.

  في حالة إلغاء تحديد خانة الاختيار هذه، يمكنك عزل الكمبيوتر عن الشبكة بعد تشغيل المهمة يدويًا. وإذا اكتشفت مهمة IOC Scan مؤشر اختراق، يمكنك عزل الكمبيوتر عن الشبكة مباشرة من مؤشر الاختراق (خصائص **Application settings** ← IOC Scan ← مهمة **IOC Scan results**). ويتيح Kaspersky Endpoint Security أيضًا إدارة الإعدادات الإضافية على الفور: فترة تعطيل عزل الشبكة واستثناءات عزل الشبكة.

- **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.

  في حالة إلغاء تحديد خانة الاختيار هذه، يمكنك عزل الملف يدويًا بعد تشغيل المهمة يدويًا. إذا اكتشفت مهمة IOC Scan ملفًا يمكن أن يعرض البيانات للخطر، ويمكنك عزل هذا الملف مباشرةً من نتائج فحص مؤشرات الاختراق (**IOC Scan results** ← **Application settings**). ونتيجة لذلك، يبدأ Kaspersky Endpoint Security معالج إنشاء المهام ببيانات محددة مسبقًا للملف المكتشف. ولست بحاجة سوى إدارة إعدادات المهام الإضافية، على سبيل المثال، إعداد جدول المهام.

  إذا لزم الأمر، حدد خانة الاختيار **Apply to system critical objects**. ويتضمن System Critical Object (SCOs) الملفات التي يتطلبها نظام التشغيل لكي يعمل.

لا نوصي بتطبيق الإجراءات على ملفات SCO. وقد يتسبب ذلك في عدم استقرار نظام التشغيل أو فشل التمهيد.

- **Run Critical Areas Scan**. في حالة تحديد هذا الخيار، يُشغل Kaspersky Endpoint Security مهمة Critical Areas Scan. بشكلٍ افتراضي، يفحص Kaspersky Endpoint Security ذاكرة kernel والعمليات قيد التشغيل وقطاعات تمهيد القرص.

13. انتقل إلى القسم **Advanced**.

14. حدد أنواع البيانات (مستندات IOC) التي يجب تحليلها كجزء من المهمة.

يحدد Kaspersky Endpoint Security تلقائيًا أنواع البيانات (مستندات IOC) لمهمة IOC Scan 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 Log - 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.

بالنسبة لمصطلح IOC source \ EventLogItem ، استخدم القيمة **اسم المزود** من مخطط XML للحدث.

- **Windows Registry - RegistryItem**. كوّن نطاق فحص مؤشرات الاختراق في التسجيل.

  بشكل افتراضي، يفحص Kaspersky Endpoint Security مجموعة من مفاتيح التسجيل.

15. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

16. تكوين جدول المهمة.

لا يتوفر Wake-on-LAN لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

17. احفظ تغييراتك.

18. حدد خانة الاختيار المجاورة للمهمة.

19. انقر على **Start**.

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**. في نتائج فحص مؤشرات الاختراق، يمكنك أيضًا عزل الملف المكتشف أو عزل الكمبيوتر عن الشبكة يدويًا.

يبحث Kaspersky Endpoint Security عن التكرارات بين السجلات التي تم إنشاؤها لملف مؤشر الاختراق نفسه ويحتفظ بالسجلات الفريدة فقط في نتائج المهام. والتكرارات هي سجلات من النوع نفسه لها القيم نفسها لجميع الحقول المقارنة. قد لا ينشئ التطبيق أيضًا سجلاً إذا كان يفتقر إلى قيمة في حقل واحد أو أكثر (انظر الجدول أدناه).

النوع	الحقول المقارنة	شرط لعدم إنشاء سجل
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• القيمة المفقودة لحقول FullPath وMd5sum وSha256sum. • القيم المفقودة لحقل FullPath والقيم المتوافقة لحقلي Md5sum وSha256sum.
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	قيمة مفقودة لواحد على الأقل من الحقول التالية: Hive وKeyPath وValueName.
ProcessItem	• startTime • PID	قيم مفقودة لحقلي startTime أو PID.

قد تعرض نافذة **Alert Details** سجلات RegistryItem بقيم حقل متطابقة. وهذه السجلات ليست تكرارًا لأن لها قيمًا مختلفة لحقل النص، والذي لا يتم عرضه في الواجهة.

يتم الاحتفاظ بنتائج فحص IOC لمدة 30 يومًا. وبعد هذه الفترة، يحذف برنامج Kaspersky Endpoint Security تلقائيًا الإدخالات القديمة.

القياس عن بُعد الموسع لفحص مؤشر الاختراق

ونوصي بتمكين القياس عن بُعد الموسع على الكمبيوتر بغرض فحص مؤشر الاختراق بأثر رجعي. تعمل ميزة القياس عن بُعد على تحسين دقة اكتشاف مؤشر الاختراق، لكنها تستخدم المزيد من موارد الكمبيوتر.

يتضمن القياس عن بُعد الموسع دعم الشروط الإضافية التالية:

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

في حالة تعطيل القياس عن بُعد الموسع، فقد يقوم Kaspersky Endpoint Security بتدوير المعلومات عن مؤشرات الاختراق التي تم اكتشافها.

لتمكين القياس عن بُعد الموسع:

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response**.
5. حدد خانة الاختيار **Enable advanced system activity logging**.
6. احفظ تغييراتك.

نقل الملف إلى العزل

عند الرد على التهديدات، يستطيع مكون Kaspersky Endpoint Detection and Response إنشاء مهام Move file to Quarantine. 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 تكامله مع حلول Kaspersky Detection and Response. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل عن 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 وتعليمات Kaspersky Endpoint Detection and Response Expert (on-premises).

تستطيع أن تنشئ مهام Move file to Quarantine 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.

- في إعدادات مهمة IOC Scan.

إذا اكتشفت مهمة IOC Scan ملفًا يمكن أن يعرض البيانات للخطر، يمكنك عزل هذا الملف مباشرةً من نتائج فحص مؤشرات الاختراق (**Application settings** ← **IOC Scan results**). ونتيجة لذلك، يبدأ Kaspersky Endpoint Security معالج إنشاء المهام ببيانات محددة مسبقًا للملف المكتشف. ولست بحاجة سوى إدارة إعدادات المهام الإضافية، على سبيل المثال، إعداد جدول المهام.

تتضمن مهمة Move file to Quarantine القيود التالية:

1. يجب ألا يتجاوز حجم الملف 100 ميجابايت.
2. لا يمكنك حذف الملفات المطلوبة لتشغيل Kaspersky Endpoint Security for Windows.

- الملفات الموجودة في نطاق تقنية الدفاع الذاتي لبرنامج Kaspersky Endpoint Security for Windows
- الملفات الموقعة رقميًا بواسطة Kaspersky

3. يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

4. لا يمكنك فحص كائن تم عزله نتيجة مهمة Move file to Quarantine.

لإنشاء مهمة Move file to Quarantine:

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.

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

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Move file to Quarantine**.

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

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

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر فوق **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر فوق **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. وإذا لزم الأمر، حدد خانة الاختيار **Apply to system critical objects**.
تتضمن System Critical Objects (SCOs) الملفات التي يتطلبها نظام التشغيل لكي يعمل.

لا نوصي بتطبيق الإجراءات على ملفات SCO. وقد يتسبب ذلك في عدم استقرار نظام التشغيل أو فشل التمهيد.

10. في قائمة الملفات، انقر فوق **Add**.
يبدأ معالج إضافة الملف.

11. 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.

12. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

13. تكوين جدول المهمة.

لا يتوفر Wake-on-LAN لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

14. احفظ تغييراتك.

15. حدد خانة الاختيار المجاورة للمهمة.

16. انقر فوق **Start**.

نتيجة لذلك، ينقل Kaspersky Endpoint Security الملف إلى العزل.

في حالة تأمين الملف بواسطة عملية مختلفة، يتم عرض حالة المهمة على أنها Done، لكن لن يتم عزل الملف نفسه إلا بعد إعادة تشغيل الكمبيوتر. وبعد إعادة تشغيل الكمبيوتر، تأكد من حذف الملف.

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 Move file to Quarantine 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 Move file to Quarantine 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. ونتيجة لتنفيذ المهمة، يتم حفظ نسخة من الملف في العزل. العزل هو مخزن محلي خاص على الكمبيوتر. ويمكنك تنزيل هذا الملف من العزل إلى جهاز الكمبيوتر الخاص بك باستخدام Web Console (**Operations** ← **Repositories** ← **Quarantine**). وعلى جهاز الكمبيوتر الخاص بالمستخدم، يظل الملف في مجلده الأصلي.

يجب ألا يتجاوز حجم الملف 2 جيجابايت.

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 نافذة Web Console الرئيسية، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر على **Add**.

يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Get file**.

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

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

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر فوق **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر فوق **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 Wake-on-LAN لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. احفظ تغييراتك.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر فوق **Start**.

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 Delete file. على سبيل المثال، يمكنك حذف ملف عن بُعد عند الاستجابة للتهديدات.

لا يمكنك حذف الملفات المطلوبة لتشغيل Kaspersky Endpoint Security for Windows.

- الملفات الموجودة في نطاق تقنية الدفاع الذاتي لبرنامج Kaspersky Endpoint Security for Windows
- الملفات الموقعة رقميًا بواسطة Kaspersky

يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة Delete file:

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.
2. انقر على **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.
   b. في القائمة المنسدلة **Task type**، حدد **Delete file**.
   c. في الحقل **Task name**، أدخل وصفًا مختصرًا.
   d. في القسم **Devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر فوق **Next**.
5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر فوق **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. 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.

10. وإذا لزم الأمر، حدد خانة الاختيار **Apply to system critical objects**.

تتضمن System Critical Objects (SCOs) الملفات التي يتطلبها نظام التشغيل لكي يعمل.

لا نوصي بتطبيق الإجراءات على ملفات SCO. وقد يتسبب ذلك في عدم استقرار نظام التشغيل أو فشل التمهيد.

11. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

12. تكوين جدول المهمة.

لا يتوفر Wake-on-LAN لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. احفظ تغييراتك.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر فوق **Start**.

نتيجة لذلك، يحذف Kaspersky Endpoint Security الملف من الكمبيوتر. وفي حالة تأمين الملف من خلال عملية مختلفة، يتم عرض المهمة على أنها Done، لكن يتم حذف الملف نفسه فقط بعد إعادة تشغيل الكمبيوتر. وبعد إعادة تشغيل الكمبيوتر، تأكد من حذف الملف.

من الممكن أن تنتهي مهمة Delete file بالخطأ Access denied or file not found 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 Process start. على سبيل المثال، يمكنك تشغيل أداة مساعدة تنشئ ملف تكوين الكمبيوتر عن بُعد. بعد ذلك يمكنك استخدام المهمة Get file 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 Process start:

1. في نافذة Web Console الرئيسية، حدد **Tasks**.

تفتح قائمة المهام.

2. انقر على **Add**.

يبدأ معالج المهمة.

3. تكوين إعدادات المهمة:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.

b. في القائمة المنسدلة **Task type**، حدد **Process start**.

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

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

4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر فوق **Next**.

5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر فوق **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.

لنفترض أنك تريد تشغيل أداة مساعدة (`utility.exe`) تحفظ المعلومات عن تكوين الكمبيوتر في ملف يسمى `conf.txt` في المجلد الحالي (بشكل افتراضي). توجد الأداة في المجلد `C:\Users\admin\Diagnostic\`. يجب عليك حفظ ملف التكوين في المجلد `C:\Users\admin\Documents\Configuration`. أدخل القيم التالية:

- **Executable command** – `C:\Users\admin\Diagnostic\utility.exe`
- **Command line arguments (optional)** – `/R conf.txt`
- **Path to the working folder (optional)** – `C:\Users\admin\Documents\Configuration`

11. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

12. تكوين جدول المهمة.

لا يتوفر Wake-on-LAN لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. احفظ تغييراتك.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر فوق **Start**.

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 Terminate process. 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 Terminate process القيود التالية:

لا يمكنك إنهاء عمليات الملف المطلوبة لتشغيل Kaspersky Endpoint Security for Windows.

- الملفات الموجودة في نطاق تقنية الدفاع الذاتي لبرنامج Kaspersky Endpoint Security for Windows
- الملفات الموقعة رقميًا بواسطة Kaspersky

يمكنك تكوين مهمة EDR Optimum في Web Console وCloud Console. وتتوفر إعدادات مهام EDR Expert فقط في Cloud Console.

لإنشاء مهمة Terminate process:

1. في نافذة Web Console الرئيسية، حدد **Tasks**.
تفتح قائمة المهام.
2. انقر على **Add**.
يبدأ معالج المهمة.
3. تكوين إعدادات المهمة:
   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Endpoint Security for Windows 14.2**.
   b. في القائمة المنسدلة **Task type**، حدد **Terminate process**.
   c. في الحقل **Task name**، أدخل وصفًا مختصرًا.
   d. في القسم **Devices to which the task will be assigned**، حدد نطاق المهمة.
4. حدد الأجهزة وفقًا لخيار نطاق المهمة المحدد. انقر فوق **Next**.
5. أدخل بيانات اعتماد حساب المستخدم الذي تريد استخدام حقوقه لتشغيل المهمة. انقر فوق **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. وإذا لزم الأمر، حدد خانة الاختيار **Apply to system critical objects**.
تتضمن System Critical Objects (SCOs) الملفات التي يتطلبها نظام التشغيل لكي يعمل.

لا نوصي بتطبيق الإجراءات على ملفات SCO. وقد يتسبب ذلك في عدم استقرار نظام التشغيل أو فشل التمهيد.

10. 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.

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 File not found.

11. من نافذة خصائص الكمبيوتر، حدد علامة التبويب **Schedule**.

12. تكوين جدول المهمة.

لا يتوفر Wake-on-LAN لهذه المهمة. تأكد من تشغيل الكمبيوتر لتشغيل المهمة.

13. انقر فوق **Save**.

14. حدد خانة الاختيار المجاورة للمهمة.

15. انقر فوق **Start**.

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 مسار المجلد 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. لا يمكنك تطبيق قاعدة منع على الملفات المطلوبة لتشغيل Kaspersky Endpoint Security for Windows:
   - الملفات الموجودة في نطاق تقنية الدفاع الذاتي لبرنامج Kaspersky Endpoint Security for Windows
   - الملفات الموقعة رقميًا بواسطة Kaspersky
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 نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response**.

5. حدد علامة التبويب **Execution Prevention**.

6. قم بتشغيل مفتاح **Execution Prevention ENABLED**.

7. في القسم **Action on execution or opening of forbidden object**، حدد وضع تشغيل المكون:

- **Block and add to event log**. 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.
إذا لزم الأمر ، حدد خانة الاختيار **Apply to system critical objects**. ويتضمن System Critical Object (SCOs) الملفات التي يتطلبها نظام التشغيل لكي يعمل.

لا نوصي بتطبيق الإجراءات على ملفات SCO. وقد يتسبب ذلك في عدم استقرار نظام التشغيل أو فشل التمهيد.

- **Add to event log**. 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.

8. 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 التجزئة ومسار المجلد.

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.

9. 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.
- الاتصالات بجهاز SVM وخادم التكامل إذا كان التطبيق يُستخدم في وضع Light Agent.
- الاتصالات بشبكة KSN عند دمج التطبيق مع Kaspersky Managed Detection and Response.

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 نافذة Web Console الرئيسية، حدد **Asset management** ← **Tasks**.
تفتح قائمة المهام.

2. انقر فوق المهمة **IOC Scan** في برنامج Kaspersky Endpoint Security.

نافذة خصائص المهمة.

إذا لزم الأمر، أنشئ مهمة IOC Scan.

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

4. حدد القسم **Response settings**.

5. في القسم **Configure response actions on IOC detection**، حدد **Alert and response** وحدد خانة الاختيار **Isolate device from the network**.

6. احفظ تغييراتك.

نتيجة لذلك، عند اكتشاف مؤشر اختراق (IOC)، يعزل التطبيق الكمبيوتر عن الشبكة لمنع انتشار التهديد.

يمكنك تكوين عزل تلقائي للشبكة ليتم تعطيله بعد فترة زمنية معينة. 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 نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

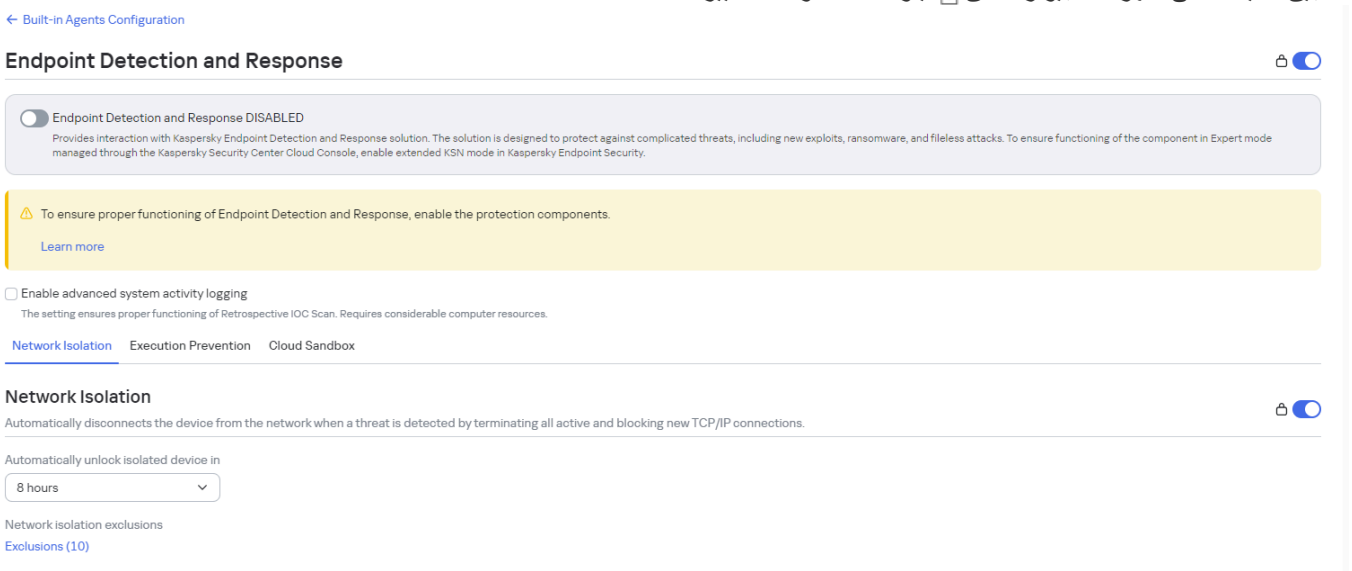
3. حدد علامة التبويب **Application settings**.

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response**.

5. حدد علامة التبويب **Network Isolation**.

6. حدد التأخير لإيقاف تشغيل عزل الشبكة.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.



إعدادات تكامل EDR

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.

- في إعدادات مهمة IOC Scan.

وإذا اكتشفت مهمة IOC Scan مؤشر اختراق، يمكنك عزل الكمبيوتر عن الشبكة مباشرة من مؤشر الاختراق (خصائص ← IOC Scan ← مهمة **IOC Scan results** ← **Application settings**). ويتيح Kaspersky Endpoint Security أيضًا إدارة الإعدادات الإضافية على الفور: فترة تعطيل عزل الشبكة واستثناءات عزل الشبكة.

كيفية تشغيل عزل شبكة الاتصال لجهاز الكمبيوتر يدويًا

1. في نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.
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 14.2**.

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 تلقائي للشبكة ليتم تعطيله بعد فترة زمنية معينة. 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 نافذة Web Console الرئيسية، حدد **Assets (Devices)** ← **Asset management**.
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 نافذة Web Console الرئيسية، حدد **Asset management** ← **Assets (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 14.2**.

تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.

5. حدد علامة التبويب **Application settings**.

6. انتقل إلى **Built-in Agents Configuration** ← **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.

بدءًا من Kaspersky Endpoint Security 12.10 for Windows، يمكنك إدارة عزل الشبكة في تفاصيل التنبيه. بالإضافة إلى ذلك، في تفاصيل التنبيه يمكنك تحديد الفترة الزمنية لعزل شبكة 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.

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 نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

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** ← **Built-in Agents Configuration**.

5. حدد علامة التبويب **Network Isolation**.

6. في القسم **Network isolation exclusions** انقر على **Exclusions**.

7. يفتح هذا نافذة؛ وفي هذه النافذة، انقر فوق **Add** ← **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** ← **Add** وحرر إعدادات اتصال الشبكة يدويًا.

9. احفظ تغييراتك.

كيفية إضافة استثناءات عزل شبكة الاتصال في الوضع اليدوي

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Assets (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.

بدءًا من Kaspersky Endpoint Security 12.10 for Windows، يمكنك إضافة استثناءات عزل الشبكة في تفاصيل التنبيه. وللحصول على التفاصيل عن إدارة تفاصيل الاكتشاف، يرجى الرجوع إلى تعليمات Kaspersky Endpoint Detection and Response Optimum وتعليمات Kaspersky Endpoint Detection and Response Expert.

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 حل Endpoint Detection and Response Optimum، يمكنك تمكين عداد منفصل للتهديدات المكتشفة بواسطة Cloud Sandbox. ويمكنك استخدام هذا العداد لتجميع الإحصائيات عند تحليل التهديدات المكتشفة. ويشير Kaspersky Endpoint Security إلى تقنية اكتشاف التهديدات في Cloud Sandbox في Report on threats وفي وحدة تحكم Kaspersky Security Center.



عدادات التهديد

لتمكين عداد Cloud Sandbox:

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response**.

5. حدد علامة التبويب **Cloud Sandbox**.

6. قم بتشغيل مفتاح **Cloud Sandbox ENABLED**.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ 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 Report on threats وفي وحدة تحكم Kaspersky Security Center.

قسم سياسة Endpoint Detection and Response

دليل الترحيل من KEA إلى KES لحل EDR Optimum

يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا لحل Kaspersky Endpoint Detection and Response Optimum. ولم تعد بحاجة إلى تطبيق Kaspersky Endpoint Agent منفصل للعمل مع EDR Optimum. وسيتم تنفيذ جميع وظائف Kaspersky Endpoint Agent بواسطة Kaspersky Endpoint Security.

عند نشر Kaspersky Endpoint Security على أجهزة الكمبيوتر المُثبت عليها Kaspersky Endpoint Agent، سيستمر حل Kaspersky Endpoint Detection and Response Optimum 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 11.7.0 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 Kaspersky Endpoint Detection and Response Optimum:

- Kaspersky Endpoint Detection and Response Optimum الإصدار 2.0 أو أحدث.
- الإصدار 13.2 من Kaspersky Security Center أو أحدث (بما في ذلك عميل الشبكة). في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة EDR Optimum.
- لا يمكن إدارة EDR Optimum إلا باستخدام Kaspersky Security Center Web Console.
- يتم تمكين نقل البيانات إلى خادم الإدارة. البيانات مطلوبة للحصول على معلومات حول الملفات المعزولة على جهاز كمبيوتر من خلال وحدة تحكم الويب.
- يتم إنشاء اتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة. لكي يعمل EDR Optimum مع خادم الإدارة عبر Kaspersky Security Center Web Console، يجب عليك إنشاء اتصال آمن جديد، اتصال في الخلفية.

خطوات ترحيل تكوين [KES+KEA] إلى [KES+العامل المضمن] لحل EDR Optimum

1. **ترقية المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security**

يمكن إدارة مكون EDR Optimum باستخدام Kaspersky Endpoint Security Management Plug-in الإصدار 11.7.0 أو أحدث.

2 ترحيل السياسات والمهام

انقل إعدادات Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows. ولفعل ذلك، استخدم المعالج للترحيل من Kaspersky Endpoint Agent في Web Console.

كيفية ترحيل إعدادات السياسة والمهام من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security في Web Console

في نافذة Web Console الرئيسية، 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

ينشئ معالج الترحيل مهام جديدة لبرنامج Kaspersky Endpoint Security. في قائمة المهام، حدد مهام Kaspersky Endpoint Agent التي تريد إنشاءها لسياسة Kaspersky Endpoint Security. انتقل إلى الخطوة التالية.

الخطوة 3. اكتمال المعالج

قم بإنهاء 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>. تكون 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.

- ينشئ مهام Kaspersky Endpoint Security جديدة.

تعد المهام الجديدة نسخًا من مهام Kaspersky Endpoint Agent. وفي الوقت نفسه، يترك المعالج مهام Kaspersky Endpoint Agent دون تغيير.

3 ترخيص وظيفة EDR Optimum

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 أو أحدث. 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 أو أحدث، 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 and Response Optimum أو Kaspersky Optimum Security. يمكنك استبدال المفتاح باستخدام مهمة Add key.

4 تثبيت / ترقية تطبيق Kaspersky Endpoint Security

لترحيل وظائف EDR Optimum أثناء تثبيت تطبيق أو ترقيته، يوصى باستخدام مهمة التثبيت عن بعد. وعند إنشاء مهمة تثبيت عن بُعد، تحتاج إلى تحديد مكون EDR Optimum 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 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 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.

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 العميل المدمج عن طريق عرض Report on status of application components. 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.

Kaspersky Sandbox

يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا للتكامل مع حل Kaspersky Sandbox. ويكتشف مكون Sandbox ويمنع تلقائيًا التهديدات المتقدمة على أجهزة الكمبيوتر. ويحلل Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Sandbox). وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Sandbox وتعليمات Kaspersky Anti Targeted Attack Platform.

تكامل العميل المدمج مع Kaspersky Sandbox

إضافة مكون Sandbox مطلوبة للتكامل مع Kaspersky Sandbox. ويمكنك تحديد مكون 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 نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **KSC Integration**.
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 نافذة Web Console الرئيسية، حدد **Integration** ← **Settings**.
2. انتقل إلى القسم **Integration**.
3. قم بتشغيل مفتاح **Background connection for integration Enabled**.
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.

- لتكوين اتصال موثوق به مع خوادم Sandbox، يجب عليك إعداد شهادة TLS. ويجب عليك بعد ذلك إضافة الشهادة إلى الكمبيوتر باستخدام سياسة. وتحتاج أيضًا إلى إضافة الشهادة إلى خادم Sandbox.

لا تتوفر المصادقة ثنائية الاتجاه باستخدام حاوية تشفير لمكون Kaspersky Sandbox.

يمكنك أيضًا إضافة شهادة TLS إلى Web Console أو محليًا باستخدام سطر الأوامر.

- تم تمكين مكون Kaspersky Sandbox.
- يتم تمكين وتشغيل مكونات التطبيق التي تضمن تشغيل Sandbox. وتضمن المكونات التالية تشغيل Sandbox:
  - الحماية من تهديدات الملفات.
  - منع اختراق المضيف.
  - جدار الحماية.
  - حماية AMSI.
  - فحص في الخلفية.

لتمكين التكامل مع Kaspersky Sandbox أو تعطيله:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Sandbox**.
5. استخدم مفتاح تبديل **Integration with Sandbox ENABLED** لتمكين المكون أو تعطيله.
6. في القسم **Integration mode**، حدد وضع تشغيل المكون: **Kaspersky Sandbox**.
7. انقر على رابط **Connection settings**.
   يفتح هذا نافذة إعدادات الاتصال بخادم Sandbox.
8. في القسم **Server TLS certificate**، انقر فوق **Upload** وحدد ملف شهادة TLS.
   من الممكن أن يتضمن Kaspersky Endpoint Security شهادة TLS واحدة فقط لخادم Sandbox. وإذا كنت قد أضفت شهادة TLS من قبل، فسيتم إبطال هذه الشهادة. ويتم استخدام آخر شهادة مضافة فقط.
9. تكوين إعدادات الاتصال المتقدمة لخوادم Sandbox:
   - **Timeout (msec)**. انتهت مهلة الاتصال لخادم Sandbox. بعد انقضاء المهلة التي تم تكوينها، يرسل Kaspersky Endpoint Security طلبًا إلى الخادم التالي. ويمكنك زيادة مهلة الاتصال لتطبيق Sandbox إذا كانت سرعة الاتصال لديك منخفضة أو إذا كان الاتصال غير مستقر. مهلة الطلب الموصى بها 0.5 ثانية أو أقل.
   - **Request queue**. حجم مجلد قائمة انتظار الطلبات. عند إرسال كائنات متعددة للفحص في Sandbox، ينشئ Kaspersky Endpoint Security قائمة انتظار للطلبات. وافتراضيًا، يقتصر حجم مجلد قائمة انتظار الطلبات على 100 ميجابايت. وبعد الوصول إلى الحد الأقصى للحجم، يتوقف 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.
10. في القسم **Connection to Sandbox servers**، انقر على الزر **Add**.

11. يفتح هذا نافذة؛ وداخل النافذة، أدخل عنوان خادم Sandbox (IPv4 وIPv6 وDNS) والمنفذ.

وللحصول على التفاصيل حول نشر الصور الافتراضية وتكوين خوادم Sandbox، يرجى الرجوع إلى تعليمات Kaspersky Sandbox.

12. 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. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Sandbox** إلى قائمة مكونات Kaspersky Endpoint Security.

يمكنك تمكين أو تعطيل التكامل مع Kaspersky Sandbox في Web Console أو محليًا باستخدام سطر الأوامر.

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.

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 IOC Scan 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 مؤشر الاختراق (IOC) مع معيار OpenIOC. يُنشئ Kaspersky Endpoint Security تلقائيًا ملفات IOC لحل Kaspersky Sandbox.

وضع تشغيل مهمة IOC Scan

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 IOC Scan

قد ينشئ Kaspersky Sandbox ويُشغّل مهام IOC Scan 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 IOC Scan:

1. في نافذة Web Console الرئيسية، حدد **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 Critical Areas Scan**. في حالة تحديد هذا الخيار، يُشغل Kaspersky Endpoint Security مهمة Critical Areas Scan. بشكلٍ افتراضي، يفحص Kaspersky Endpoint Security ذاكرة kernel والعمليات قيد التشغيل وقطاعات تمهيد القرص.
- **Run only when the computer is idle**. تأجيل بدء مهمة 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. يتيح لك خيار الجدولة هذا الحفاظ على موارد الكمبيوتر عند استخدام الكمبيوتر.

6. احفظ تغييراتك.

ويمكنك عرض نتائج المهمة في خصائص المهمة في القسم **Results**. ويمكنك عرض المعلومات عن مؤشرات الاختراق المكتشفة 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.

دليل الترحيل من KEA إلى KES لحل Kaspersky Sandbox

يتضمن Kaspersky Endpoint Security for Windows عميلاً مضمنًا لحل Kaspersky Sandbox. ولم تعد بحاجة إلى تطبيق Kaspersky Endpoint Agent منفصل للعمل مع Kaspersky Sandbox. وسيتم تنفيذ جميع وظائف Kaspersky Endpoint Agent بواسطة Kaspersky Endpoint Security.

وعند نشر Kaspersky Endpoint Security على أجهزة الكمبيوتر المُثبت عليها Kaspersky Endpoint Agent، سيستمر حل Kaspersky Sandbox 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 11.7.0 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 Kaspersky Sandbox:

- Kaspersky Sandbox الإصدار 2.0 أو أحدث.
- الإصدار 13.2 من Kaspersky Security Center أو أحدث (بما في ذلك عميل الشبكة). في الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل ميزة Kaspersky Sandbox.
- يمكن إدارة Kaspersky Sandbox فقط باستخدام Kaspersky Security Center Web Console.
- يتم تمكين نقل البيانات إلى خادم الإدارة. البيانات مطلوبة للحصول على معلومات حول الملفات المعزولة على جهاز كمبيوتر من خلال وحدة تحكم الويب.
- 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.

خطوات ترحيل تكوين [KES+KEA] إلى [KES+العامل المدمج] لحل Kaspersky Sandbox

1. **ترقية المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security**

   يمكن إدارة مكون Kaspersky Sandbox باستخدام الإصدار 11.7.0 من Kaspersky Endpoint Security Web Plug-in أو أحدث.

2. **ترحيل السياسات والمهام**

   انقل إعدادات Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security for Windows. ولفعل ذلك، استخدم المعالج للترحيل من Kaspersky Endpoint Agent في Web Console.

   كيفية ترحيل إعدادات السياسة والمهام من Kaspersky Endpoint Agent إلى Kaspersky Endpoint Security في Web Console

   في نافذة Web Console الرئيسية، 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

ينشئ معالج الترحيل مهام جديدة لبرنامج Kaspersky Endpoint Security. في قائمة المهام، حدد مهام Kaspersky Endpoint Agent التي تريد إنشاءها لسياسة Kaspersky Endpoint Security. انتقل إلى الخطوة التالية.

الخطوة 3. اكتمال المعالج

قم بإنهاء 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>. تكون 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.

- ينشئ مهام Kaspersky Endpoint Security جديدة.

تعد المهام الجديدة نسخًا من مهام Kaspersky Endpoint Agent. وفي الوقت نفسه، يترك المعالج مهام Kaspersky Endpoint Agent دون تغيير.

3 ترخيص وظيفة Kaspersky Sandbox

لتفعيل Kaspersky Endpoint Security كجزء من حل Kaspersky Sandbox، تحتاج إلى ترخيص منفصل للوظيفة الإضافية لحل Kaspersky Sandbox. يمكنك استبدال المفتاح باستخدام مهمة Add key. نتيجة لذلك، ستتم إضافة مفتاحين إلى التطبيق: Kaspersky Endpoint Security وKaspersky Sandbox.

4 تثبيت / ترقية تطبيق Kaspersky Endpoint Security

لترحيل وظائف Kaspersky Sandbox أثناء تثبيت تطبيق أو ترقيته، يوصى باستخدام مهمة التثبيت عن بعد. وعند إنشاء مهمة تثبيت عن بُعد، تحتاج إلى تحديد مكون Kaspersky Sandbox 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 Kaspersky Sandbox، فإن برنامج تثبيت Kaspersky Endpoint Security يكوّن تلقائيًا مجموعة المكونات ويحدد مكون Kaspersky Sandbox. 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 بناءً على تكوين 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 العميل المدمج عن طريق عرض Report on status of application components. 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.

Kaspersky Anti Targeted Attack Platform

يدعم Kaspersky Endpoint Security for Windows العمل مع حل Kaspersky Anti Targeted Attack Platform. Kaspersky Anti Targeted Attack Platform عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدِفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. تتضمن Kaspersky Anti Targeted Attack Platform ثلاث وحدات وظيفية:

- Kaspersky Anti Targeted Attack Platform (KATA)
- Kaspersky Endpoint Detection and Response (EDR (KATA))
- Network Detection and Response (NDR (KATA))

يمكنك شراء جميع الوحدات الوظيفية أو الوحدات الوظيفية الفردية بشكل منفصل. وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform. يتضمن التطبيق عوامل مضمنة لمكوني EDR وNDR. يدعم التطبيق أيضًا العمل مع مكون Sandbox الذي يعد جزءًا من KATA.

أدوات معلومات التهديدات

يستخدم Kaspersky Endpoint Detection and Response أدوات Threat Intelligence التالية:

- التكامل مع Kaspersky Threat Intelligence Portal، التي تحتوي على معلومات عن سمعة الملفات وعناوين الويب وتعرضها.
- قاعدة بيانات التهديدات الخاصة بشركة Kaspersky.
- 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.

مبدأ تشغيل الحل

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) وNDR (KATA) في 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.

تكوينات Kaspersky Endpoint Security للعمل مع EDR / NDR (KATA)

يمكن استخدام التكوينات التالية للعمل مع EDR / NDR (KATA):

- **[KES+العميل المدمج]**. في هذا التكوين، يعمل Kaspersky Endpoint Security كتطبيق يضمن أمان الكمبيوتر وتطبيق للعمل مع EDR / NDR (KATA). ويتوفر العميل المدمج لحل EDR (KATA) في Kaspersky Endpoint Security 12.1 for Windows أو أحدث. ويتوفر العميل المدمج لحل NDR (KATA) في Kaspersky Endpoint Security 12.7 for Windows أو أحدث.
- **[EPP التابع لجهة خارجية+EDR Agent]**. في هذا التكوين، يتم توفير أمان البنية التحتية لتكنولوجيا المعلومات من خلال منصات حماية نقطة النهاية (EPP) التابعة لجهة خارجية. ويتم توفير التفاعل مع EDR / NDR (KATA) بواسطة Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent (EDR Agent). وفي هذا التكوين، يكون EDR Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية. يتوفر EDR Agent لحل EDR (KATA) في Kaspersky Endpoint Security 12.3 for Windows أو أحدث. يتوفر EDR Agent لحل NDR (KATA) في Kaspersky Endpoint Security 12.7 for Windows أو أحدث.

دعم الإصدارات السابقة من Kaspersky Endpoint Security

إذا كنت تستخدم Kaspersky Endpoint Security 11.2.0 – 11.8.0 لإمكانية التشغيل التفاعلي مع Kaspersky Anti Targeted Attack Platform (EDR)، فإن التطبيق يتضمن Kaspersky Endpoint Agent. يمكنك تثبيت Kaspersky Endpoint Agent مع تثبيت Kaspersky Endpoint Security.

إذا كنت تستخدم Kaspersky Endpoint Security 11.9.0 - 12.0، فأنت بحاجة إلى تثبيت Kaspersky Endpoint Agent بشكل منفصل لأنه بدءًا من Kaspersky Endpoint Security 11.9.0، لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من مجموعة توزيع Kaspersky Endpoint Security.

تكامل العميل المدمج مع EDR / NDR (KATA)

للتكامل مع EDR / NDR (KATA)، يجب عليك إضافة المكون ذي الصلة: Endpoint Detection and Response (KATA) أو Network Detection and Response (KATA). يمكنك تحديد المكونات للتكامل مع EDR / NDR (KATA) عند تثبيت أو ترقية التطبيق، وكذلك استخدام مهمة تغيير مكونات التطبيق.

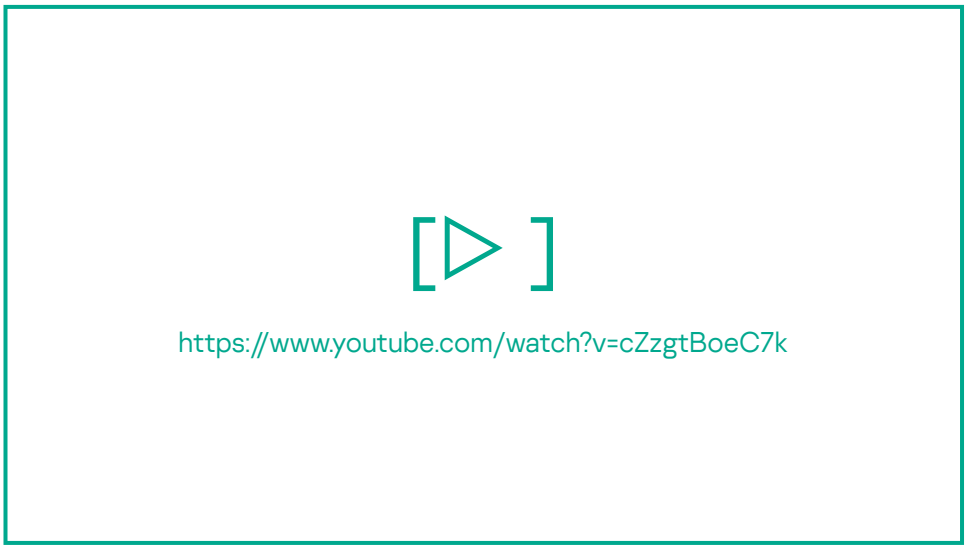
بدءًا من الإصدار 12.11 من Kaspersky Endpoint Security for Windows، تمت إعادة تسمية مكون EDR (KATA) إلى **Endpoint Detection and Response Expert (version 8.0 or later)**. في هذا الإصدار من التطبيق، يتوافق المكون مع Kaspersky Anti Targeted Attack Platform 7.1 والإصدارات الأقدم، بالإضافة إلى Kaspersky Endpoint Detection and Response Expert (on-premises).

لا تتوافق مكونات Endpoint Detection and Response Optimum و Endpoint Detection and Response Expert (cloud) و Endpoint Detection and Response Expert (on-premises) مع بعضها البعض.

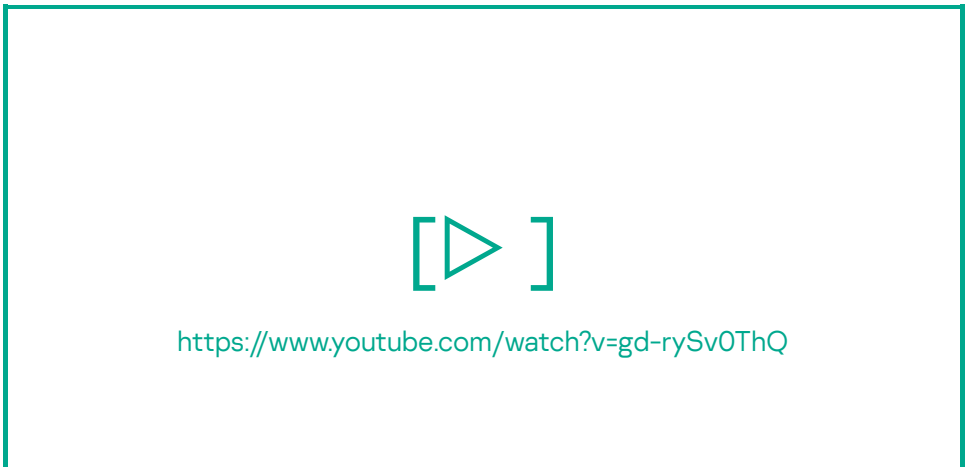
لاستخدام EDR / NDR (KATA)، يجب استيفاء الشروط التالية:

- EDR (KATA): Kaspersky Anti Targeted Attack Platform الإصدار 5.0–7.1.
- NDR (KATA): Kaspersky Anti Targeted Attack Platform الإصدار 7.0 أو أحدث.
- EDR (KATA): Kaspersky Endpoint Security for Windows 12.1 أو أحدث. وللمزيد من التفاصيل عن توافق KATA مع الإصدارات المختلفة من Kaspersky Endpoint Security، يرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

- Kaspersky Endpoint Security for Windows 12.7 أو أحدث (KATA): NDR.
- Kaspersky Security Center الإصدار 14.2 أو أحدث. وفي الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل وظيفة تكامل EDR / NDR (KATA).
- تم تفعيل التطبيق ويغطي الترخيص الوظيفة.
- يتم تمكين مكوني Endpoint Detection and Response (KATA) وNetwork Detection and Response (KATA).
- يتم تمكين وتشغيل مكونات التطبيق التي تضمن تشغيل EDR / NDR (KATA). وتضمن المكونات التالية تشغيل EDR / NDR (KATA):
  - الحماية من تهديدات الملفات.
  - الحماية من تهديدات الويب.
  - الحماية من تهديدات البريد.
  - منع الاستغلال.
  - اكتشاف السلوك.
  - منع اختراق المضيف.
  - حماية AMSI.
  - فحص في الخلفية.
  - Kaspersky Security Network.



https://www.youtube.com/watch?v=cZzgtBoeC7k



https://www.youtube.com/watch?v=gd-rySv0ThQ

يتكون التكامل مع Endpoint Detection and Response (KATA) من الخطوات التالية:

1. **تثبيت مكوني Endpoint Detection and Response (KATA) وNetwork Detection and Response (KATA)**

   يمكنك تحديد مكوني EDR (KATA) وNDR (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) وNetwork Detection and Response (KATA)**

   يتعين عليك شراء ترخيص منفصل لمكوني EDR (KATA) وNDR (KATA) (على سبيل المثال، الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response (KATA)).

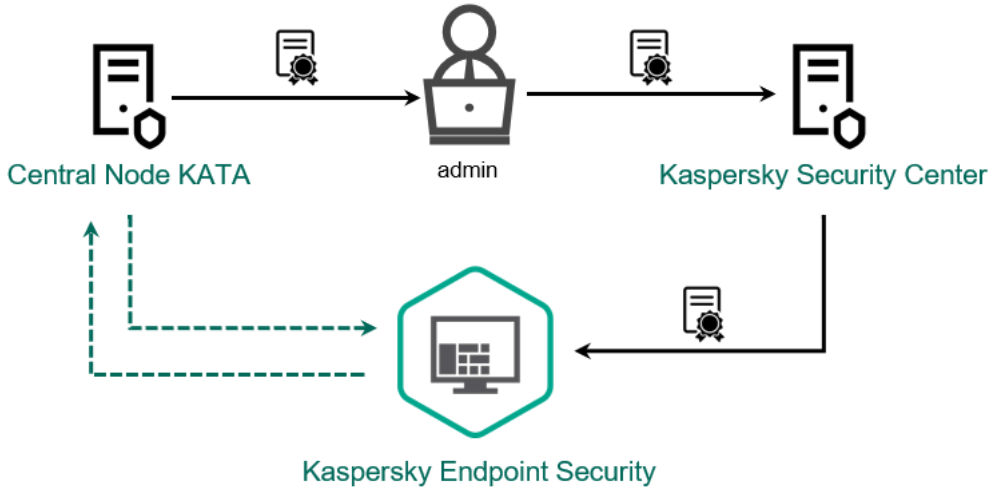
   تصبح الوظيفة متاحة بعد إضافة مفتاح منفصل يغطي وظائف EDR (KATA) وNDR (KATA). ونتيجة لذلك، تتم إضافة مفاتيح متعددة على الكمبيوتر: مفتاح لتطبيق Kaspersky Endpoint Security ومفاتيح لتطبيقي Kaspersky Endpoint Detection and Response (KATA) وNetwork Detection and Response (KATA).

   ترخيص وظيفتي EDR (KATA) وNDR (KATA) المستقلتين هو ترخيص Kaspersky Endpoint Security نفسه.

   تأكد من تضمين كل من وظيفة EDR (KATA) وNDR (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 **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.

4. في نافذة السياسة ، حدد **Detection and Response** وحدد المكون الذي تريد تكوينه: **Endpoint Detection and Response Expert (on-premises)** أو **Network Detection and Response (KATA)**.

5. حدد خانة الاختيار المقابلة: **Endpoint Detection and Response Expert (الإصدار 7.1 أو أقدم)** أو **Network Detection and Response (KATA)**.

6. انقر على **إعدادات اتصال الخادم**.

7. تكوين اتصال الخادم:

- **المهلة (ثانية)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
- **شهادة TLS للخادم**. 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).
- **استخدام المصادقة ثنائية الاتجاه**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

8. انقر فوق **OK**.

9. أضف خوادم العقدة المركزية. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

10. إذا لزم الأمر، كوّن القياس عن بعد.

11. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون Central Node باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** وحدد المكون الذي تريد تكوينه: **Endpoint Detection and Response Expert (on-premises)** أو **Network Detection and Response (KATA)**.

5. قم بتشغيل مفتاح التبديل المقابل: **Endpoint Detection and Response Expert (on-premises) ENABLED** أو **Network Detection and Response (KATA) ENABLED**.

6. لتكوين EDR (KATA)، حدد **Endpoint Detection and Response Expert (version 7.1 or earlier)** من قائمة الحلول.

7. انقر على **Connection settings**.

8. تكوين اتصال الخادم:

- **Timeout (sec)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف.
- **Server 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**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

9. انقر على **OK**.

10. أضف خوادم العقدة المركزية. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

11. إذا لزم الأمر، كوّن القياس عن بعد.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

يمكنك أيضًا إضافة شهادة TLS محليًا باستخدام سطر الأوامر.

نتيجة لذلك، تمت إضافة الكمبيوتر إلى وحدة تحكم Kaspersky Anti Targeted Attack Platform. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكوني **Endpoint Detection and Response Expert (version 8.0 or later)** و**Network Detection and Response (KATA)** إلى قائمة مكونات Kaspersky Endpoint Security.

يمكنك التحقق من حالة المكونات في وحدة تحكم Kaspersky Security Center في خصائص الكمبيوتر في ملف قسم **Components**. وضع في اعتبارك ما يلي عند التحقق من حالة المكون في وحدة التحكم. وإذا لم يتم تثبيت المكون وكانت الوظيفة غير مغطاة بترخيصك، فستعرض وحدة التحكم **Not supported by license** بدلاً من **Not installed**.

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، يمكنك مراقبة حالة مكون EDR (KATA) في وحدة تحكم الإدارة (MMC) لتطبيق Kaspersky Security Center. ويتم عرض الحالة الحالية للمكون في خصائص الكمبيوتر في العمود **Endpoint Sensor status** (Running وStarting وStopped وPaused وFailed وUnknown). ولا تعرض Web Console حالة Endpoint Sensor.

تكوين القياس عن بعد لحل EDR (KATA)

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 أدناه). 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 وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة ، حدد **Detection and Response** وحدد المكون الذي تريد تكوينه: **Endpoint Detection and Response Expert (on-premises)** أو **Network Detection and Response (KATA)**.

5. كوّن إعداد **إرسال طلب مزامنة إلى خادم KATA كل (دقيقة)**. عدد مرات إرسال طلبات المزامنة إلى الخادم. 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، قم بتكوين المزامنة مع إعدادات الخادم في القسم **إعدادات نقل البيانات**:

- **الحد الأقصى لتأخير إرسال الحدث (ثانية)**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
- **الحد الأقصى لحزم الحدث**. يتزامن التطبيق مع الخادم عندما يمتلئ المخزن المؤقت بالأحداث. الإعداد الافتراضي هو 1024 حدثًا.

8. إذا لزم الأمر ، حدد خانة الاختيار **تمكين تقييد الطلب** في القسم **تقييد الطلب**.

تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. 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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 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. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين القياس عن بعد في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (on-premises)**.

5. لتكوين EDR (KATA)، حدد **Endpoint Detection and Response Expert (version 7.1 or earlier)** من قائمة الحلول.

6. تأكد من تحديد خانة الاختيار **Send telemetry to KATA servers** في القسم **Data transmission settings**.

7. كوّن إعداد **Send sync request to server every (min)**. عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.

8. تأكد من تحديد خانة الاختيار **Send telemetry to KATA servers**.

9. إذا لزم الأمر، قم بتكوين المزامنة مع إعدادات الخادم في القسم **Data transmission settings**:

- **Maximum event transmission delay (sec)**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
- **Maximum number of event packages**. يتزامن التطبيق مع الخادم عندما يمتلئ المخزن المؤقت بالأحداث. الإعداد الافتراضي هو 1024 حدثًا.

10. إذا لزم الأمر ، حدد خانة الاختيار **Enable request throttling** في القسم **Request throttling**.
تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث.

11. 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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 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%.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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 RT_VERSION (VersionInfo).
للحصول على المزيد من المعلومات عن مورد VersionInfo، يُرجى زيارة موقع ويب Microsoft.
- **اسم الملف الأصلي**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo).
- **الإصدار**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo).
- **MD5**. تجزئة MD5 للملف.
- **SHA256**. تجزئة SHA256 للملف.
- **أنواع الأحداث**. لكي يعمل الاستثناء، يجب تحديد نوع حدث واحد على الأقل.

7. احفظ تغييراتك.

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Tasks**.
تفتح قائمة المهام.

2. انقر فوق **New task**.

يبدأ معالج المهمة. اتبع تعليمات المعالج.

الخطوة الأولى: تحديد نوع المهمة

1. حدد **Kaspersky Endpoint Security for Windows (14.2)** ← **تراجع عن التحديث**.

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

كوّن جدول المهام، على سبيل المثال، يدويًا.

الخطوة الرابعة: تحديد اسم المهمة

أدخل اسمًا للمهمة.

الخطوة 7 إكمال إنشاء المهمة

قم بإنهاء المعالج. حدد خانة الاختيار **Run the task after the wizard finishes** إذا كان ذلك ضروريًا. يمكنك متابعة تقدم المهمة من خصائص المهمة.

استثناءات القياس عن بُعد لحل EDR (KATA)

لتحسين الأداء وتحسين إرسال البيانات إلى خادم القياس عن بُعد، يمكنك تكوين استثناءات القياس عن بعد. على سبيل المثال، يمكنك اختيار عدم إرسال بيانات اتصالات الشبكة لتطبيقات فردية.

كيفية إنشاء استثناء للقياس عن بعد في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.
4. في القسم **إعدادات القياس عن بعد** ← **القياس عن بعد لحل EDR (KATA) / NDR (KATA)**، انقر على الزر **الإعدادات**.

5. في النافذة التي تفتح، قم بتكوين استثناءات القياس عن بُعد (انظر الجدول أدناه).

ويجمع التطبيق بين شروط الاستثناء وAND المنطقية. لإنشاء قاعدة، يجب عليك تحديد قيمة في الحقل **المسار الكامل** وتحديد نوع حدث واحد على الأقل في القائمة **الاستخدام لأنواع الأحداث التالية**.

6. احفظ تغييراتك.

كيفية إنشاء استثناء للقياس عن بعد في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **General Settings** ← **Telemetry Settings**.

5. حدد علامة التبويب **EDR (KATA) / NDR (KATA) telemetry**.

6. في النافذة التي تفتح، قم بتكوين استثناءات القياس عن بُعد (انظر الجدول أدناه).

ويجمع التطبيق بين شروط الاستثناء وAND المنطقية. لإنشاء قاعدة، يجب عليك تحديد قيمة في الحقل **Full path** وتحديد نوع حدث واحد على الأقل.

7. احفظ تغييراتك.

معلمات استثناء القياس عن بُعد

المعلمة	الوصف
العمليات المستثناة	**تحسين حجم القياس عن بعد للإرسال**. يسمح Kaspersky Endpoint Security بتحسين كمية البيانات المرسلة واستثناء الأحداث التي تتضمن رموزًا معينة من التتبع عن بُعد: الرمز 102 (الاتصالات الأساسية) و8 (نشاط الشبكة للعملية) لبروتوكول Microsoft SMB وخدمة WinRM وعملية klnagent.exe لعميل الشبكة، بالإضافة إلى معلومات موسعة عن أنواع حزم شبكة الاتصال لجميع أنواع بروتوكولات الشبكة. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية. **Process** و**Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 وSHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعيئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل. **الاستخدام لأنواع الأحداث التالية**: • **تعديل الملف**. • **أحداث الشبكة**. • **العملية: الإدخال التفاعلي لوحدة التحكم**. • **تم تحميل الوحدة**. • **تم تعديل التسجيل**. • **سجلات DNS**. • **الوصول إلى العملية**. • **حقن التعليمات البرمجية**. • **استعلام WMI**. • **التوصيل المؤقت**. • LDAP. • AMSI.

المعلمة	الوصف
اتصالات الشبكة المستثناة	**اسم القاعدة**. **الاتجاه**. **البروتوكول**. **المقبس الأولي**. **رقم البروتوكول**. **شهادة TLS**. **النطاق أو المنفذ المحلي**. **النطاق أو المنفذ البعيد**. **العنوان المحلي**. عنوان شبكة الكمبيوتر الذي يستثني Kaspersky Endpoint Security تتبعه من حركة بيانات الشبكة. **العنوان البعيد**. عنوان شبكة الكمبيوتر الذي يستثني Kaspersky Endpoint Security تتبعه من حركة بيانات الشبكة. يتم دعم تنسيق IPv4 فقط لعناوين IP. **التطبيقات**. قائمة بالملفات القابلة للتنفيذ الخاصة بالتطبيقات التي يستثني Kaspersky Endpoint Security قياس EDR عن بُعد لها من حركة بيانات الشبكة.
عمليات الملفات المستثناة	**اسم القاعدة**. **اسم الملف أو القناع**. اسم أو قناع ملف أو مجلد؛ ويُطبق Kaspersky Endpoint Security قاعدة الاستثناء عند الوصول إلى هذا الملف أو المجلد. يدعم Kaspersky Endpoint Security حرفي `*` و`?` عند إدخال قناع. **نوع العملية**. **المسار السابق**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة و AND المنطقية. **Process** و**Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 و SHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل.

المعلمة	الوصف
عمليات DNS المستثناة	**اسم القاعدة**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية. **Process** و**Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 وSHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل. **DNS**: • **عنوان IP لخادم DNS**. • **خيارات الاستعلام**. • **الحالة**. • **اسم المجال**. • **معرف نوع الإعدادات**. • **بيانات الاستجابة**.
عمليات LDAP المستثناة	**اسم القاعدة**. **نطاق بحث LDAP**. **عامل التصفية**. **الاسم المميز للبحث عن كائنات LDAP**. **سمات الكائن**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية. **Process** و**Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 وSHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل.

المعلمة	الوصف
استعلامات الوصول إلى العمليات المستثناة	**اسم القاعدة**. **نوع العملية**. **تم طلب الوصول إلى العملية**. **تتبع مكدس الاستدعاء**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية. **Process** و**Parent process** و**File of the target process** و**Handle to the source process** و**Handle to the target process**. • **المسار الكامل**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **نص سطر الأوامر**. الأمر المستخدم لتشغيل الملف. • **حدد معايير تشغيل القاعدة وأنواع الأحداث التي تريد استخدام هذه القاعدة لها**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **اسم الملف الأصلي**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **الإصدار**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **المجاميع الاختبارية للملف**. MD5 وSHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل.
عمليات حقن التعليمات البرمجية المستثناة	**اسم القاعدة**. **طريقة الوصول**. **مكدس الاستدعاء**. **سطر الأوامر المعدل**. **عنوان الحقن**. **اسم DLL الذي تم حقنه**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية. **Process** و**Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 وSHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل.

المعلمة	الوصف
استعلامات WMI المستثناة	**اسم القاعدة**. **نوع عملية WMI**. **الاستعلام عن بعد**. **اسم الكمبيوتر الذي نفذ أمر WMI**. **حساب مستخدم WMI**. **أمر WMI الذي تم تنفيذه**. **مساحة اسم WMI**. **سجل مستهلك حدث WMI**. **اسم مستهلك حدث WMI الذي تم إنشاؤه**. **التعليمات البرمجية المصدرية لمستهلك حدث WMI**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة و AND المنطقية. **Process** و **Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 و SHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل.
عمليات التوصيل المؤقت المستثناة	**اسم القاعدة**. **اسم التوصيل المؤقت**. **نوع العملية**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة و AND المنطقية. **Process** و **Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 و SHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل.

المعلمة	الوصف
تغييرات السجل المستثناة	**اسم القاعدة**. **نوع العملية**. **المسار**. **اسم القيمة**. **القيمة**. **الاسم الكامل لملف السجل**. يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية. **Process** و**Parent process**: • **Full path**. المسار الكامل للملف بما في ذلك اسمه وامتداده. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. • **Command line text**. الأمر المستخدم لتشغيل الملف. • **Description**. قيمة المعلمة FileDescription من مورد RT_VERSION (VersionInfo). • **Original file name**. قيمة المعلمة OriginalFilename من مورد RT_VERSION (VersionInfo). • **Version**. قيمة معلمة FileVersion من مورد RT_VERSION (VersionInfo). • **File checksums**. MD5 وSHA256. يمكنك أيضًا تحديد ملف يدويًا، وسيقوم التطبيق تلقائيًا بملء الحقول من الملف المحدد. وفي أنظمة تشغيل 64 بت، يجب عليك إدخال معلمات إصدار 64 بت للملف القابل للتنفيذ يدويًا لعملية من المجلد `C:\windows\system32` لأن التطبيق يعبئ حقول معلمات الملف القابل للتنفيذ ببيانات من خصائص 32 بت من الملف القابل للتنفيذ نفسه في المجلد `C:\windows\syswow64`. على سبيل المثال، إذا حددت `C:\windows\system32\cmd.exe`، فسيعرض المكون الإضافي معلمات `C:\windows\syswow64\cmd.exe`. وينجم هذا السلوك من خلال خصوصيات نظام التشغيل.
العمليات المستثناة مع الأجهزة	**اسم القاعدة**. **نوع الجهاز**. **معرف الجهاز**. **اسم الجهاز**.

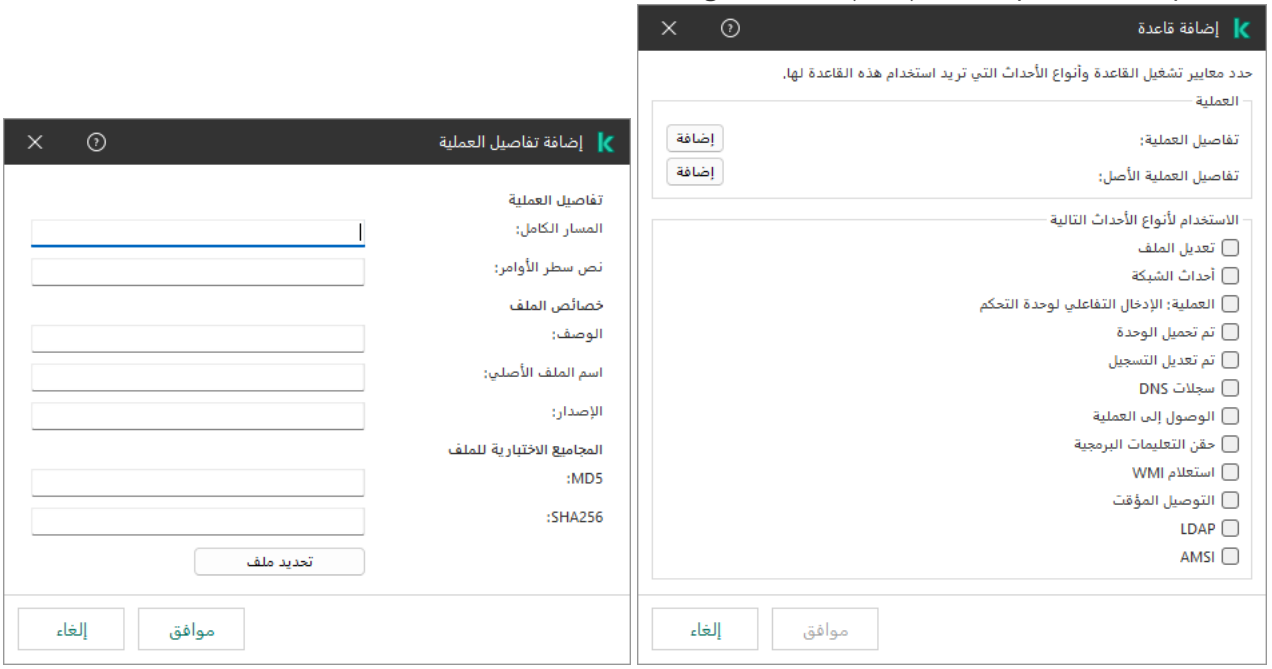
المثال 1. العمليات المستثناة

لاستثناء أحداث (عملية) تطبيق جهة خارجية من القياس عن بُعد، افتح نافذة استثناءات القياس عن بُعد لحل EDR في علامة التبويب **العمليات المستثناة** وأضف الملف القابل للتنفيذ الخاص بالتطبيق.

يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية.

يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف * و ? عند إدخال قناع. على سبيل المثال:

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`



استثناء عملية

المثال 1. تعديل الملف

إذا كنت تقوم غالبًا بتحرير البرامج النصية في تطبيق Notepad++ وتريد استثناء أحداث التعديل للبرامج النصية المقابلة، أضف ملف Notepad++ القابل للتنفيذ لاستثناءات القياس عن بُعد.

حدد الإعدادات على النحو التالي:

- **المسار الكامل**: `C:\Program Files\Notepad++\notepad++.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.
- **الاستخدام لأنواع الأحداث التالية**: تعديل الملف.

المثال 2. أحداث الشبكة

إذا كنت تستخدم تطبيق WinSCP لإدارة الملفات على خادم بعيد وتريد استثناء أحداث الشبكة، أضف ملف WinSCP القابل للتنفيذ لاستثناءات القياس عن بُعد.

حدد الإعدادات على النحو التالي:

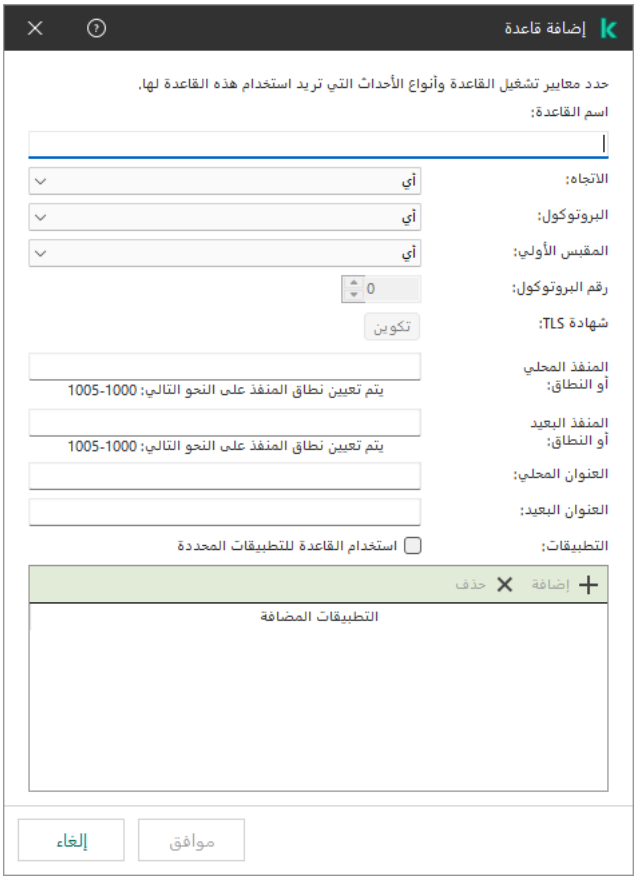
- **المسار الكامل**: `C:\Program Files (x86)\WinSCP\WinSCP.exe`.
- **SHA256**: 47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (اختياري).
- **الاستخدام لأنواع الأحداث التالية**: أحداث الشبكة.

المثال 2. اتصالات الشبكة المستثناة

لاستثناء أحداث اتصال الخدمة عن بُعد من القياس عن بُعد، افتح نافذة استثناءات القياس عن بُعد لحل EDR في علامة التبويب **اتصالات الشبكة المستثناة** وأضف إعدادات الاتصال: البروتوكول والمنفذ والاتجاه وعنوان IP وشهادة TLS، وغيرها.

يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة وAND المنطقية.

لا يمكنك تحديد عنوان شبكة فرعية (على سبيل المثال، 10.28.0.0/24). ويسمح التطبيق بتحديد عنوان IP واحد فقط (على سبيل المثال، 10.28.0.105).



استثناء اتصال الشبكة

إذا كنت تستخدم خادم ويب شركة وتريد استثناء أحداث المستعرض عند الاتصال بخادم الويب هذا، فأضف عنوان IP الخاص بالخادم والملف القابل للتنفيذ الخاص بالمستعرض إلى استثناءات التتبع عن بُعد.

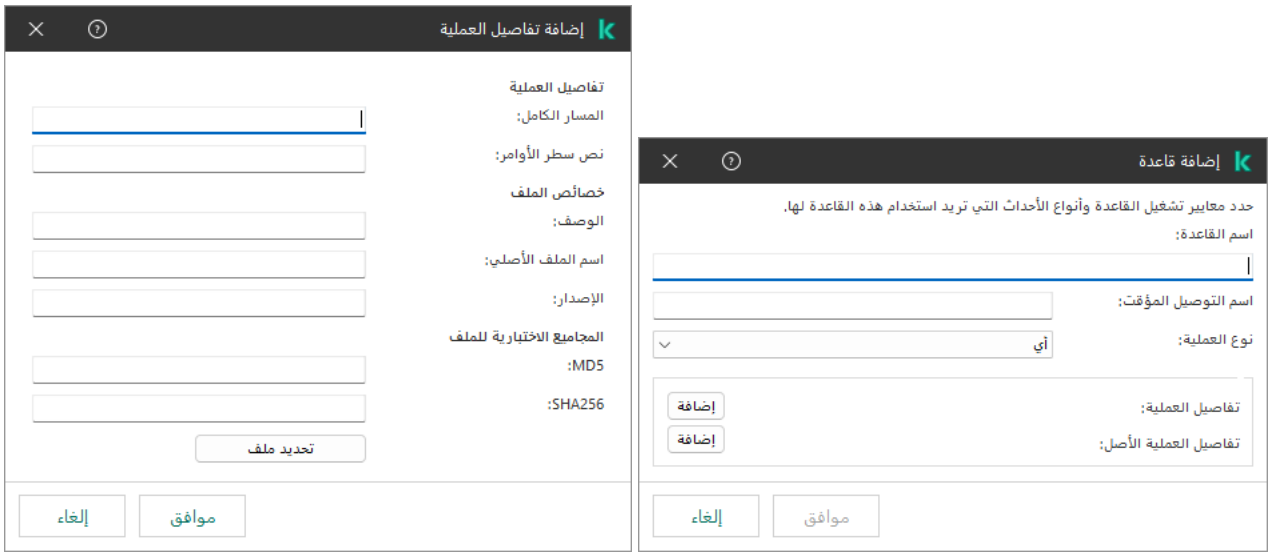
حدد الإعدادات على النحو التالي:

- **البروتوكول**: TCP.
- **النطاق أو المنفذ البعيد**: 443.
- **العنوان البعيد**: 10.28.0.105.
- **التطبيقات**: `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`؛ `C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`.

المثال 3. عمليات الملف المستثناة

لاستثناء الأحداث التي تتضمن عمليات باستخدام ملفات موثوقة من التتبع عن بُعد، افتح نافذة استثناءات القياس عن بُعد لحل EDR في علامة التبويب **عمليات الملفات المستثناة** وأضف الملف الموثوق به.

يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة و AND المنطقية.



استثناء عمليات الملف

إذا كتب أحد التطبيقات في سجل وأردت استثناء أحداث تعديل ملف السجل، فأضف ملف السجل والملف القابل للتنفيذ الخاص بالتطبيق من القياس عن بُعد.

حدد الإعدادات على النحو التالي:

- **اسم الملف أو القناع**: `C:\Apache24\logs\error.log`.
- **نوع العملية**: تعديل الملف.
- **المسار الكامل**: `C:\Apache24\bin\httpd.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

المثال 4. تعديلات التسجيل المستثناة

لاستثناء أحداث تعديل التسجيل من القياس عن بُعد، افتح نافذة استثناءات القياس عن بُعد لحل EDR في علامة التبويب **تغييرات السجل المستثناة** وأضف مفتاح تسجيل.

يجمع Kaspersky Endpoint Security بين معايير تشغيل القاعدة و AND المنطقية.

إذا قام تطبيق بتعديل قيم التسجيل الخاصة به بشكل متكرر وأردت استثناء أحداث تعديل السجل هذه من التتبع عن بُعد، فأضف مفتاح التسجيل والملف القابل للتنفيذ الخاص بالتطبيق إلى استثناءات التتبع عن بُعد.

حدد الإعدادات على النحو التالي:

- **نوع العملية**: تعديل.
- **المسار**: HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64.

- **المسار الكامل**: `C:\Program Files\PuTTY\putty.exe`.
- **SHA256**: 64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34.

KATA Sandbox

يتضمن Kaspersky Anti Targeted Attack Platform مكون Sandbox (KATA Sandbox). Sandbox هي تقنية تتيح لك اكتشاف التهديدات المتقدمة على جهاز كمبيوتر. ويحلل Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Sandbox). وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

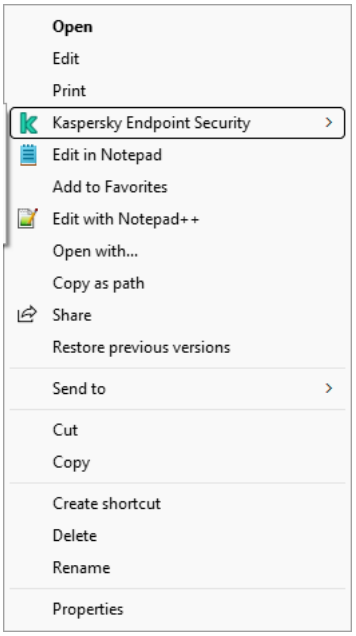
لتفعيل KATA Sandbox، تحتاج إلى مفتاح ترخيص يتضمن وظائف KATA أو KEDR. وللحصول على التفاصيل عن الوظائف المتاحة، يُرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

يسمح KATA Sandbox بفحص الملفات في الأوضاع التالية:

- يدويًا. يرسل المستخدم الملف يدويًا للفحص من قائمة السياق (**إرسال إلى Sandbox**). عند إرسال ملف إلى Sandbox، يفحص التطبيق أيضًا الملف باستخدام قواعد بيانات مكافحة الفيروسات.
- تلقائيًا. يكتشف التطبيق تلقائيًا الكائنات ويرسلها إلى Sandbox للفحص.

بعد إرسال الملف إلى Sandbox ، يظل بإمكان المستخدم الوصول إلى الملف. ويسجل Kaspersky Endpoint Security الحدث المقابل ويرسل الحدث إلى Kaspersky Security Center ووحدة تحكم Kaspersky Anti Targeted Attack Platform. إذا اكتشف Sandbox نشاطًا ضارًا ، فسوف ينفذ Kaspersky Endpoint Security إجراء الاستجابة للتهديد تلقائيًا (على سبيل المثال ، يحذف الكائن ويبدأ فحص المناطق الحرجة).

يتطلب تشغيل KATA Sandbox في الوضع اليدوي، وجود Kaspersky Anti Targeted Attack Platform 7.0 أو إصدار أحدث. لكي يعمل KATA Sandbox تلقائيًا، يجب تثبيت Kaspersky Anti Targeted Attack Platform 8.0 أو أحدث.



الفحص في KATA Sandbox من قائمة السياق

تكامل العميل المدمج مع KATA Sandbox

يلزم إضافة مكون Sandbox للتكامل مع KATA Sandbox. ويمكنك تحديد مكون Sandbox أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

لإرسال الملفات للفحص، يجب عليك تمكين التكامل مع KATA Sandbox وإضافة خادم Central Node الذي يتم نشره داخل الحل. يمكن إدارة المكون فقط باستخدام Kaspersky Security Center Web Console. لا يمكنك إدارة هذا المكون باستخدام وحدة تحكم الإدارة (MMC).

لتمكين التكامل مع KATA Sandbox أو تعطيله:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Sandbox**.
5. استخدم مفتاح تبديل **Integration with Sandbox ENABLED** لتمكين المكون أو تعطيله.
6. حدد وضع تشغيل KATA Sandbox:
   - **Manually**. يرسل المستخدم الملف يدويًا للفحص من قائمة السياق (**إرسال إلى Sandbox**).
   - **Automatically**. يكتشف التطبيق تلقائيًا الكائنات ويرسلها إلى Sandbox للفحص.
   - **Combined**.
7. انقر على رابط **Connection settings**.
8. تكوين إعدادات اتصال خادم العقدة المركزية:
   - **Timeout (msec)**. انتهت مهلة الاتصال لخادم Central Node. بعد انقضاء المهلة التي تم تكوينها، يرسل Kaspersky Endpoint Security طلبًا إلى الخادم التالي. ويمكنك زيادة مهلة الاتصال لتطبيق Sandbox إذا كانت سرعة الاتصال لديك منخفضة أو إذا كان الاتصال غير مستقر. مهلة الطلب الموصى بها 0.5 ثانية أو أقل.
   - **Request queue**. حجم مجلد قائمة انتظار الطلبات. عند إرسال كائنات متعددة للفحص في Sandbox، ينشئ Kaspersky Endpoint Security قائمة انتظار للطلبات. وافتراضيًا، يقتصر حجم مجلد قائمة انتظار الطلبات على 100 ميجابايت. وبعد الوصول إلى الحد الأقصى للحجم، يتوقف 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.
   - **Server TLS certificate**. لتكوين اتصال موثوق به مع خادم Central Node، يجب عليك إعداد شهادة TLS. ويجب عليك بعد ذلك إضافة الشهادة إلى الكمبيوتر باستخدام سياسة. تحتاج أيضًا إلى إضافة الشهادة إلى خادم Central Node.
   - **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.
9. في القسم **Connection to Sandbox servers**، انقر على الزر **Add**.

10. يفتح هذا نافذة؛ وداخل النافذة، أدخل عنوان خادم Central Node (IPv4 وIPv6 وDNS) والمنفذ.

وللحصول على التفاصيل عن نشر الصور الافتراضية وتكوين خوادم Central Node، يرجى الرجوع إلى تعليمات Kaspersky Anti Targeted Attack Platform.

11. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

نتيجة لذلك، يتم تمكين مكون Sandbox. تحقق من حالة تشغيل المكون عن طريق عرض Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Sandbox** إلى قائمة مكونات Kaspersky Endpoint Security.

تكوين إجراءات الاستجابة للتهديدات

إذا اكتشف Sandbox نشاطًا ضارًا ، فسوف ينفذ Kaspersky Endpoint Security إجراء الاستجابة للتهديد تلقائيًا (على سبيل المثال ، يحذف الكائن ويبدأ فحص المناطق الحرجة).

لتكوين إجراءات الاستجابة للتهديدات:

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** ← **Sandbox**.

5. حدد الإجراء المناسب من القسم **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 Critical Areas Scan**. في حالة تحديد هذا الخيار، يُشغل Kaspersky Endpoint Security مهمة Critical Areas Scan. 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 IOC Scan (مهمة مستقلة لفحص مؤشر الاختراق). ولهذه المهمة، يمكنك تكوين وضع التشغيل ونطاق الفحص والإجراء عند اكتشاف مؤشر الاختراق (Move copy to Quarantine, delete object أو Run Critical Areas Scan). ولتعديل الإعدادات الأخرى لمهمة IOC Scan، انتقل إلى إعدادات المهمة.

6. إذا لزم الأمر، كوّن إعدادات مهمة فحص IOC في القسم **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 drive of the computer**. في حالة تحديد هذا الخيار، ينفذ Kaspersky Endpoint Security فحص IOC على محرك أقراص النظام في الكمبيوتر.

7. إذا لزم الأمر، كوّن إعدادات مهمة فحص IOC في القسم **Run IOC Scan task**.

- **Manually**. وضع التشغيل الذي يمكنك فيه بدء مهمة IOC Scan يدويًا في الوقت الذي يناسبك.
- **Automatically**. وضع التشغيل الذي يقوم فيه Kaspersky Endpoint Security بتشغيل مهمة IOC Scan تلقائيًا بعد 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.

8. تكوين إعدادات المهام المتقدمة لمهمة فحص IOC.

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

دليل الترحيل من KEA إلى KES لحل EDR (KATA)

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 EDR (KATA). 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 5.0 أو أحدث.
- الإصدار 14.2 من Kaspersky Security Center 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 المضمن] 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 نافذة Web Console الرئيسية، 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

قم بإنهاء 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>. تكون 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 **Connection settings** ("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`.

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم.

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 EDR (KATA)

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 Kaspersky Endpoint Detection and Response (KATA).

يتضمن ترخيص الوظيفة الإضافية لحل Kaspersky Endpoint Detection and Response (KATA) 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 إضافة مفتاح منفصل للوظيفة الإضافية لحل Kaspersky Endpoint Detection and Response (KATA). 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 إضافة الوظيفة الإضافية لحل Kaspersky Endpoint Detection and Response (KATA).

- إذا كنت تستخدم رمز تفعيل للترخيص، سيعيد خادم تفعيل Kaspersky إصدار المفاتيح تلقائيًا، وستصبح ميزات EDR (KATA) 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 EDR (KATA) أثناء تثبيت تطبيق أو ترقيته، يوصى باستخدام مهمة التثبيت عن بعد. وعند إنشاء مهمة تثبيت عن بُعد، تحتاج إلى تحديد مكون EDR (KATA) 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 EDR (KATA)، يقوم مُثبّت Kaspersky Endpoint Security تلقائيًا بتكوين مجموعة المكونات ويحدد مكون EDR (KATA). 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 العميل المدمج عن طريق عرض Report on status of application components. 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 EDR Expert 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.

Endpoint Detection and Response Expert (on-premises)

يدعم Kaspersky Endpoint Security for Windows التكامل مع حل Kaspersky Endpoint Detection and Response Expert (on-premises). ويعد Kaspersky Endpoint Detection and Response Expert (on-premises) حلاً للأمن الإلكتروني للمؤسسات يتضمن تطبيقات Kaspersky التي تسمح للمؤسسة بصد معظم أنواع المخاطر الإلكترونية وتغطية أهم سيناريوهات انتشار التهديدات. ويتم نشر مكونات EDR Expert (on-premises) على Open Single Management Platform (OSMP). وتقوم هذه المنصة بتشغيل سيناريوهات عبر الأنظمة الأساسية في واجهة واحدة وتسمح بدمج تطبيقات Kaspersky مع تطبيقات الجهات الخارجية في نظام أمان شامل.

يمثل SIEM أحد العناصر المركزية للحل. ويتتبع SIEM الأحداث القادمة من جميع المكونات ويربط هذه الأحداث ببعضها البعض باستخدام قواعد محددة من قبل البائع والمستخدم. ويبحث EDR Expert (on-premises) في السجلات والقياس عن بُعد الواردة من البنية التحتية للشركة لاكتشاف الهجمات تلقائيًا والسماح بالتحقيق في الحوادث باستخدام رسم بياني لتحقيق موحد يجمع كل الأحداث التي تم جمعها في EDR Expert (on-premises)، بما في ذلك الأحداث من تطبيقات Kaspersky و منتجات أمان المعلومات من جهات خارجية.

للاستجابة للحوادث المتقدمة، يستخدم EDR Expert (on-premises) سيناريوهات معدة مسبقًا ومحددة بواسطة المستخدم. ويمكنك أيضًا استخدام إجراءات الاستجابة من تطبيقات الجهات الخارجية وسيناريوهات الاستجابة التي تتضمن تطبيقات متعددة.

أدوات معلومات التهديدات

يستخدم Kaspersky Endpoint Detection and Response أدوات Threat Intelligence التالية:

- التكامل مع Kaspersky Threat Intelligence Portal، التي تحتوي على معلومات عن سمعة الملفات وعناوين الويب وتعرضها.
- قاعدة بيانات التهديدات الخاصة بشركة Kaspersky.
- 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.

مبدأ تشغيل الحل

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.

عند تثبيته في الوضع القياسي في البنية التحتية لجهاز VDI، يدعم Kaspersky Endpoint Security التكامل مع EDR Expert (on-premises). ومع ذلك، فإن قابلية تشغيل الوظائف الأخرى للتطبيق ليست مضمونة. ولحماية الأجهزة الافتراضية في البنية التحتية لجهاز VDI، نوصي باستخدام Kaspersky Endpoint Security في وضع Light Agent.

يتم إرسال المعلومات عن الأحداث على الكمبيوتر (القياس عن بُعد) إلى خادم EDR Expert (on-premises). وفي هذه الحالة، يرسل Kaspersky Endpoint Security أيضًا معلومات عن التهديدات التي اكتشفتها Kaspersky بالإضافة إلى معلومات عن نتائج معالجة هذه التهديدات.

تم تكوين تكامل EDR Expert (on-premises) في وحدة تحكم Kaspersky Security Center. وبعد ذلك تتم إدارة العامل المضمن باستخدام منصة الإدارة الواحدة المفتوحة (OSMP)، بما في ذلك مهام التشغيل وإدارة الكائنات المعزولة وعرض التقارير والإجراءات الأخرى.

تكوينات Kaspersky Endpoint Security للعمل مع EDR Expert (on-premises)

يمكن استخدام التكوينات التالية للعمل مع EDR Expert (on-premises):

- **[KES+العميل المدمج]**. في هذا التكوين، يعمل Kaspersky Endpoint Security كتطبيق يضمن أمان الكمبيوتر وتطبيق للعمل مع EDR Expert (on-premises). ويتوفر العميل المدمج لحل EDR Expert (on-premises) في Kaspersky Endpoint Security 12.11 for Windows أو أحدث.
- **[EPP التابع لجهة خارجية+EDR Agent]**. في هذا التكوين، يتم توفير أمان البنية التحتية لتكنولوجيا المعلومات من خلال Endpoint Protection Platform (EPP). التابعة لطرف خارجي. ويتم توفير التفاعل مع EDR Expert (on-premises) بواسطة Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent (EDR Agent). وفي هذا التكوين، يكون EDR Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية. يتوفر EDR Agent لحل EDR Expert (on-premises) في Kaspersky Endpoint Security 12.11 for Windows أو أحدث.

تكامل العميل المدمج مع EDR Expert (on-premises)

للتكامل مع حلول Kaspersky Endpoint Detection and Response Expert (on-premises)، يجب عليك إضافة مكون Endpoint Detection and Response Expert (on-premises)، وتكوين Kaspersky Endpoint Security.

لا تتوافق مكونات Endpoint Detection and Response Optimum وEndpoint Detection and Response Expert (cloud) وEndpoint Detection and Response Expert (on-premises) مع بعضها البعض.

يجب استيفاء الشروط التالية لكي يعمل Endpoint Detection and Response Expert (on-premises):

- تم تثبيت OSMP (Open Single Management Platform).
- تم تفعيل التطبيق ويغطي الترخيص الوظيفة.
- تم تشغيل مكون Endpoint Detection and Response Expert (on-premises).
- يتم تمكين وتشغيل مكونات التطبيق التي تضمن تشغيل EDR Expert (on-premises). وتضمن المكونات التالية تشغيل EDR Expert (on-premises):
  - الحماية من تهديدات الملفات.
  - الحماية من تهديدات الويب.
  - الحماية من تهديدات البريد.
  - منع الاستغلال.
  - اكتشاف السلوك.
  - منع اختراق المضيف.
  - محرك المعالجة.
  - مراقبة عيوب التكيف.

يتضمن إعداد تكامل EDR Expert (on-premises) الخطوات التالية:

1. **تثبيت مكون EDR Expert (on-premises)**

   يمكنك تحديد مكون EDR Expert (on-premises) أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

   يجب إعادة تشغيل الكمبيوتر لإنهاء ترقية التطبيق بالمكون الجديد.

2. **تفعيل Kaspersky Endpoint Detection and Response Expert (on-premises)**

   تحتاج إلى شراء ترخيص منفصل لمكون EDR Expert (on-premises) (الوظيفة الإضافية لمكون Kaspersky Endpoint Detection and Response Expert (on-premises)).

   ستتوفر الوظيفة بعد إضافة مفتاح منفصل لبرنامج Kaspersky Endpoint Detection and Response Expert (on-premises). ونتيجة لذلك، تتم إضافة مفتاحين على الكمبيوتر: مفتاح لحل Kaspersky Endpoint Security ومفتاح لحل Kaspersky Endpoint Detection and Response Expert (on-premises).

   الترخيص لوظيفة Endpoint Detection and Response Expert (on-premises) المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

   تأكد من تضمين وظيفة EDR Expert (on-premises) في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

3. **الاتصال بخادم جمع القياس عن بُعد وخادم الاستجابة**

   يتطلب Kaspersky Endpoint Detection and Response Expert (on-premises) اتصالاً موثوقًا به بين Kaspersky Endpoint Security وخادمين:

   - خادم جمع القياس عن بعد هو خادم يعد جزءًا من حل SIEM الذي يجمع المعلومات عن الأحداث التي تحدث على الكمبيوتر وتوحيدها وربطها وتحليلها وتخزينها.
   - خادم الاستجابة هو خادم لاستلام البيانات وفحصها ودراسة سلوك الكائنات ونشر نتائج هذه الدراسات.

   لتكوين اتصال موثوق، يجب عليك استخدام شهادة TLS. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد ذلك يجب عليك إضافة شهادة TLS إلى Kaspersky Endpoint Security (انظر الإرشادات أدناه).

   بشكل افتراضي، يتحقق Kaspersky Endpoint Security فقط من شهادة TLS للخوادم. ولجعل الاتصال أكثر أمانًا، يمكنك أيضًا تمكين التحقق من الكمبيوتر على الخادم (المصادقة ثنائية الاتجاه). ولتمكين هذا التحقق، يجب عليك تشغيل المصادقة ثنائية الاتجاه في إعدادات الخادم وKaspersky Endpoint Security. ولاستخدام المصادقة ثنائية الاتجاه، ستحتاج أيضًا إلى حاوية تشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)).

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون EDR Expert (on-premises) باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (on-premises)**.
5. قم بتشغيل مفتاح **Endpoint Detection and Response Expert (on-premises) ENABLED**.
6. لتكوين EDR Expert (on-premises)، حدد **Endpoint Detection and Response Expert (version 8.0 or later)** من قائمة الحلول.

7. تكوين اتصال خوادم جمع القياس عن بعد:

a. في القسم **Connection to telemetry collection servers**، انقر على الرابط **Connection settings**.

b. تكوين اتصال خوادم جمع القياس عن بعد:

- **Timeout (sec)**. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف.
- **Server certificate**. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security والخادم. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات الخادم، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد تكوين إعدادات الخادم، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

c. انقر على **OK**.

d. أضف خوادم جمع القياس عن بعد. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

يمكنك إضافة عناوين متعددة لخادم جمع القياس عن بعد. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

e. إذا لزم الأمر، كوّن القياس عن بعد.

8. تكوين اتصال خوادم الاستجابة:

a. في القسم **Connection to response servers**، كوّن إعداد **Send sync request to server every (min)**. عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يتلقى Kaspersky Endpoint Security مهام الاستجابة للتهديدات ويرسل نتائج المهام.

b. انقر على رابط **Connection settings**.

c. تكوين اتصال خوادم الاستجابة:

- **Timeout (sec)**. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف.
- **Server certificate**. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)).
- **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security والخادم. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات الخادم، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد تكوين إعدادات الخادم، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

d. انقر على **OK**.

e. أضف خوادم الاستجابة. ولفعل ذلك، حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالخادم.

يمكنك إضافة عناوين متعددة لخادم الاستجابة. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

يمكنك التحقق من حالة المكون باستخدام Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Endpoint Detection and Response Expert (on-premises)** إلى قائمة مكونات Kaspersky Endpoint Security.

تكوين إعدادات القياس عن بُعد لحل EDR Expert (on-premises)

القياس عن بعد عبارة عن قائمة الأحداث التي وقعت على الكمبيوتر المحمي. ويحلل Kaspersky Endpoint Security بيانات القياس عن بُعد ويرسلها إلى خوادم جمع القياس عن بُعد أثناء المزامنة. وللمزيد من المعلومات عن أحداث القياس عن بُعد المنقولة، انظر تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises).

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).

لتكوين إعدادات القياس عن بُعد، اتبع الخطوات التالية:

1. في نافذة Web Console الرئيسية، حدد علامة التبويب **Policies** ← **Asset management**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (on-premises)**.

5. لتكوين EDR Expert (on-premises)، حدد **Endpoint Detection and Response Expert (version 8.0 or later)** من قائمة الحلول.

6. تأكد من تحديد خانة الاختيار **Send telemetry to telemetry collection servers** في القسم **Data transmission settings**.

7. وإذا لزم الأمر، حدد خانة الاختيار **Send telemetry with IOA only**. مؤشر الهجوم (IOA) هو قاعدة تحتوي على وصف لسلوك مشبوه في النظام مما قد يشير إلى هجوم موجه. ويقارن التطبيق السلوك الجاري في النظام مع هذه القواعد ويسجل الأحداث التي تشير إلى هجوم موجه. ويستخدم التطبيق تقنية فحص البث التي تتيح تتبع مثل هذه الأحداث في الوقت الحقيقي.

8. إذا لزم الأمر، قم بتكوين المزامنة مع إعدادات الخادم في القسم **Data transmission settings**:

- **Maximum event transmission delay (sec)**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
- **Maximum number of event packages**. يتزامن التطبيق مع الخادم عندما يمتلئ المخزن المؤقت بالأحداث. الإعداد الافتراضي هو 1024 حدثًا.

9. إذا لزم الأمر ، امسح تحديد خانة الاختيار **Enable request throttling** في القسم **Request throttling**.

تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث. ويتم تمكين هذا الخيار بشكل افتراضي.

10. 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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 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%.

11. في القسم **Connection to response servers**، أدخل قيمة لمعلمة **Send sync request to server every (min)**.

12. عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.

13. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

استثناءات القياس عن بُعد لحل EDR Expert (on-premises)

لتحسين الأداء وتحسين إرسال البيانات إلى خادم جمع القياس عن بُعد، يمكنك إضافة استثناءات القياس عن بعد. على سبيل المثال، يمكنك اختيار عدم إرسال بيانات اتصالات الشبكة لتطبيقات فردية.

يمكن أن يؤدي استخدام الكثير من القواعد إلى زيادة الحمل على خادم جمع القياس عن بُعد وتقليل أداء الكمبيوتر. ونوصي بإضافة القواعد الضرورية فقط.

لإنشاء استثناء للقياس عن بعد في Web Console وCloud Console:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Telemetry Settings**.
5. حدد علامة التبويب **EDR Expert (on-premises) telemetry**.
6. في القسم **General exclusions**، انقر على الزر **Add**.
تفتح النافذة **Add exclusion rule**.

7. إذا لزم الأمر، قم بتغيير حالة القاعدة. بشكل افتراضي، يتم تمكين القاعدة.

8. أدخل اسمًا للقاعدة.

9. حدد الإجراء الذي سيتم تنفيذه عند تشغيل القاعدة:

- **Do not collect**. سيتم استثناء الحدث الذي تمت تصفيته من القياس عن بُعد الذي تم إرساله.
- **Exclude IOA**. سيتم استثناء حدث مشغل قاعدة مؤشر الهجوم (IOA) من القياس عن بُعد الذي تم إرساله.

10. في حالة تحديد الخيار **Exclude IOA**، حدد قواعد مؤشر الهجوم (IOA) لإضافتها إلى الاستثناءات:

- **Exclude all**. عند تلبية الشرط المحدد، سيستثني التطبيق الأحداث التي تم إنشاؤها بناءً على جميع قواعد مؤشر الهجوم (IOA) من القياس عن بُعد.
- **Exclude by GUID**. حدد المعرّف الفريد العام (GUID) الخاص بقاعدة مؤشر الهجوم (IOA). ويمكنك تحديد عدة معرّفات فريدة عامة (GUID) باستخدام `,`. وللمزيد من التفاصيل عن قواعد مؤشر الهجوم (IOA)، يرجى الرجوع إلى تعليمات EDR Expert (on-premises).

11. حدد شرط التصفية:

a. حدد اسم الحقل الذي سيتم استخدامه للتصفية.

b. حدد معاملاً (انظر الجدول أدناه) وحدد القيمة التي ستتم مقارنة قيمة الحقل من الحدث بها.

قائمة المعاملات الشرطية

المعامل	الوصف
<	إذا كانت قيمة الحقل أقل من القيمة المحددة في الشرط، فسيتم تصفية الحدث.
≤	إذا كانت قيمة الحقل أقل من القيمة المحددة في الشرط أو مساوية لها، فسيتم تصفية الحدث.
=	إذا كانت قيمة الحقل مساوية للقيمة المحددة في الشرط، فسيتم تصفية الحدث.
≥	إذا كانت قيمة الحقل أكبر من أو تساوي القيمة المحددة في الشرط، فسيتم تصفية الحدث.
>	إذا كانت قيمة الحقل أكبر من القيمة المحددة في الشرط، فسيتم تصفية الحدث.
≠	إذا كانت قيمة الحقل لا تساوي القيمة المحددة في الشرط، فسيتم تصفية الحدث.
is like	إذا كانت قيمة الحقل تطابق القناع المحدد في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي `*` و `?` عند إدخال قناع.
is not like	إذا كانت قيمة الحقل لا تتطابق مع القناع المحدد في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي `*` و `?` عند إدخال قناع.
one of	إذا كانت قيمة الحقل تتطابق مع إحدى القيم الموجودة في القائمة المحددة في الشرط، فسيتم اعتبار الحدث قد تمت تصفيته.
none of	إذا كانت قيمة الحقل لا تطابق أيًا من القيم الموجودة في القائمة المحددة في الشرط، فسيتم اعتبار الحدث قد تمت تصفيته.
is like one of	إذا كانت قيمة الحقل تتطابق مع أحد الأقنعة المحددة في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي * و? عند إدخال قناع.
is not like one of	إذا كانت قيمة الحقل لا تتطابق مع أي من الأقنعة المحددة في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي * و? عند إدخال قناع.
exists	إذا كان الحقل المحدد في الشرط موجودًا في الحدث، فسيتم تصفية الحدث.
not exists	إذا لم يكن الحقل المحدد في الشرط موجودًا في الحدث، فسيتم تصفية الحدث.
contains	إذا كانت القيمة المحددة في الشرط موجودة في قيمة الحقل، فسيتم تصفية الحدث.
is equal to	إذا كانت قيمة الحقل مساوية للقيمة المحددة في الشرط، فسيتم تصفية الحدث. الفحص غير حساس لحالة الأحرف.
bitwise AND	إذا كانت نتيجة عملية Bitwise AND (&) بين قيمة الحقل والقيمة المحددة في الشرط هي 1، فسيتم تصفية الحدث.

12. إذا لزم الأمر، يمكنك إنشاء معايير تصفية معقدة عن طريق إضافة شروط عامل التصفية المتعددة ومجموعات الشروط. ويمكنك أيضًا إضافة شروط متداخلة ومجموعات شروط إلى مجموعة شروط. ويمكنك استخدام المعاملات التالية:

- يعني **AND** أن عامل التصفية يحدد الأحداث التي تلبي جميع الشروط المحددة.
- يعني **OR** أن عامل التصفية يحدد الأحداث التي تلبي أحد الشروط المحددة.
- يعني **NOT** (لاستخدام هذا المعامل، حدد الخيار **Add NOT before**) أن عامل التصفية يحدد الأحداث التي لا تلبي أيًا من الشروط المحددة.

يتم دمج الشروط ومجموعات الشروط من المستوى الأول مع معامل **AND**.

13. إذا كان جهازك يعمل بنظام المنصة الواحدة للإدارة المفتوحة (OSMP)، فيمكنك إجراء فحص لقاعدة التصفية التي أنشأتها. لتشغيل الفحص، انقر فوق الزر **Check rule**.

في النافذة التي تفتح، سيتم عرض جدول بالأحداث التي تمت تصفيتها حسب القاعدة التي تم إنشاؤها. وللمزيد من التفاصيل، يرجى الرجوع إلى تعليمات EDR Expert (on-premises).

14. إذا لزم الأمر، تحت **All event types**، أضف استثناءات القياس عن بُعد حسب نوع الحدث.

a. انقر فوق اسم نوع الحدث.

b. في النافذة التي تفتح، انقر فوق الزر **Set up manually**.

c. إذا لزم الأمر، قم بتكوين إرسال القياس عن بُعد لنوع الحدث المحدد باستخدام زر التبديل **Send event**. وبشكل افتراضي، يتم تمكين إرسال القياس عن بُعد لجميع أنواع الأحداث.

d. في القسم **Exclusion rules**، انقر على الزر **Add**.

تفتح النافذة **Add exclusion rule**.

e. نفذ الإجراءات الموضحة في الخطوات من 7 إلى 13 لكل قاعدة تضيفها.

15. بالنسبة لبعض أنواع الأحداث، يمكنك أيضًا إضافة قواعد التضمين لتوسيع القياس عن بُعد الذي تم جمعه:

a. في القسم **Inclusion rules**، انقر على الزر **Add**.

تفتح النافذة **Add inclusion rules**.

b. أدخل اسمًا للقاعدة.

c. تحت **Condition**، أدخل قيم الحقول المعروضة. ويعتمد نوع الحقول المتاحة على الحدث المحدد.

يتم إعطاء الأولوية لقواعد الاستثناء على قواعد التضمين.

16. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

تصدير واستيراد عوامل تصفية حدث EDR Expert (on-premises)

يمكنك تصدير قائمة الاستثناءات إلى ملف JSON. وبعد ذلك يمكنك تعديل الملف، على سبيل المثال، إضافة عدد كبير من معرفات الأحداث. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من عوامل تصفية الأحداث أو لترحيل القائمة إلى خادم مختلف.

يمكن أن يؤدي استخدام الكثير من القواعد إلى زيادة الحمل على خادم جمع القياس عن بُعد وتقليل أداء الكمبيوتر. ونوصي بإضافة القواعد الضرورية فقط.

كيفية تصدير واستيراد عوامل تصفية الأحداث في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.

5. في القسم **إعدادات القياس عن بعد** ← **القياس عن بعد لحل EDR Expert (on-premises)**، انقر على الزر **الإعدادات**.

6. لتصدير عوامل تصفية الحدث:

   a. انقر على **تصدير**.
   في النافذة التي تفتح، حدد اسم ملف JSON الذي تريد تصدير عوامل تصفية الأحداث إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   b. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير عوامل تصفية الأحداث إلى ملف JSON.

7. لاستيراد عوامل تصفية الأحداث:

   a. انقر على **استيراد**.

   b. في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد عوامل تصفية الأحداث منه.

   c. افتح الملف.
   في حالة وجود قواعد تصفية الأحداث بالفعل على جهاز الكمبيوتر، يقوم Kaspersky Endpoint Security باستبدالها عند الاستيراد.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تصدير واستيراد عوامل تصفية الأحداث في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **General Settings** ← **Telemetry Settings**.

5. حدد علامة التبويب **EDR Expert (on-premises) telemetry**.

6. لتصدير عوامل تصفية الحدث:

   a. انقر على **Export**.

   b. في النافذة التي تفتح، حدد اسم ملف JSON الذي تريد تصدير عوامل تصفية الأحداث إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   c. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير عوامل تصفية الأحداث إلى ملف JSON.

7. لاستيراد عوامل تصفية الأحداث:

a. انقر على **Import**.

b. في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد عوامل تصفية الأحداث منه.

c. حدد الطريقة التي تريد بها استيراد قواعد تصفية الأحداث: عن طريق الإضافة إلى القواعد الموجودة أو عن طريق تجاهل القواعد الموجودة والاستعاضة عنها بقواعد جديدة.

d. افتح الملف.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

يمكنك أيضًا تصدير أو استيراد عوامل تصفية الأحداث في سطر الأوامر.

اعتبارات خاصة عند استخدام ملفات تعريف السياسة لتكوين التكامل مع EDR Expert (on-premises) وEDR (KATA)

لتكوين التكامل مع EDR (KATA) لمجموعات إدارة معينة ومع EDR Expert (on-premises) للآخرين كجزء من سياسة واحدة، سوف تحتاج إلى استخدام ملفات تعريف السياسة. ويجب تكوين إعدادات تكامل EDR (KATA) في خصائص السياسة، ويجب تكوين تكامل EDR Expert (EDR Expert (on-premises)) لمجموعات الإدارة المحددة في خصائص ملف تعريف السياسة.

يتضمن استخدام ملفات تعريف السياسة لتكوين التكامل مع EDR Expert (on-premises) القيود التالية:

- إذا قمت بتكوين التكامل مع EDR Expert (on-premises) في خصائص السياسة، فسوف يتم تطبيق هذه الإعدادات على جميع مجموعات الإدارة؛ ولن يتم تطبيق إعدادات التكامل من ملفات تعريف السياسة.
- عند استخدام ملفات تعريف السياسة لتكوين التكامل مع EDR Expert (on-premises)، لا يمكنك استخدام وحدة تحكم الإدارة (MMC) لإدارة السياسات. وعند فتح خصائص السياسة في وحدة تحكم الإدارة، سيتم تجاوز إعدادات تكامل EDR Expert (on-premises) في ملفات تعريف السياسة من خلال الإعدادات من السياسة، مما يتسبب في عمل المكون بشكل غير صحيح. وسوف تحتاج إلى إعادة تعيين إعدادات مكون Endpoint Detection and Response Expert (on-premises) وفقًا للتعليمات التالية.
- عند استخدام ملفات تعريف السياسة لتكوين التكامل مع EDR Expert (on-premises)، لا يمكنك استخدام السياسات الفرعية.

إذا كان لديك بالفعل سياسة تم تكوينها في إصدار سابق من المكون الإضافي للويب، فيجب عليك إعادة تعيين إعدادات مكون Endpoint Detection and Response Expert (on-premises) لتطبيق إعدادات تكامل EDR Expert (on-premises) على الأجهزة المدارة من ملفات تعريف السياسة.

لإعادة تعيين إعدادات المكون:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (on-premises)**.

5. قم بتغيير وضع التشغيل من **Endpoint Detection and Response Expert (version 7.1 or earlier)** إلى **وضع Endpoint Detection and Response Expert (الإصدار 8.0 أو أحدث)**.

6. ارجع إلى **Endpoint Detection and Response Expert (version 7.1 or earlier)**.

7. احفظ تغييراتك.

Endpoint Detection and Response Expert (cloud)

تكامل Kaspersky Endpoint Security مع Kaspersky Endpoint Detection and Response Expert (cloud) غير متاح مؤقتًا.
ومن المقرر دعم هذه الوظيفة بحلول نهاية عام 2026. تابع ملاحظات الإصدار الخاصة بنا لتكون على دراية بترقيات التطبيق والمزايا الجديدة.



يدعم Kaspersky Endpoint Security التكامل مع حل Kaspersky Endpoint Detection and Response Expert (cloud). ويعد Kaspersky Endpoint Detection and Response Expert (cloud) حلاً سحابيًا للأمن الإلكتروني للمؤسسات يتضمن تطبيقات Kaspersky التي تسمح للمؤسسة بصد معظم أنواع المخاطر الإلكترونية وتغطية أهم سيناريوهات انتشار التهديدات. يتم نشر مكونات EDR Expert (cloud) على Open Single Management Platform (OSMP). وتقوم هذه المنصة بتشغيل سيناريوهات عبر الأنظمة الأساسية في واجهة واحدة وتسمح بدمج تطبيقات Kaspersky مع تطبيقات الجهات الخارجية في نظام أمان شامل.

يمثل SIEM أحد العناصر المركزية للحل. ويتتبع SIEM الأحداث القادمة من جميع المكونات ويربط هذه الأحداث ببعضها البعض باستخدام قواعد محددة من قبل البائع والمستخدم. ويبحث EDR Expert (cloud) في السجلات والقياس عن بُعد الواردة من البنية التحتية للشركة لاكتشاف الهجمات تلقائيًا والسماح بالتحقيق في الحوادث باستخدام رسم بياني لتحقيق موحد يجمع كل الأحداث التي تم جمعها في EDR Expert (cloud)، بما في ذلك الأحداث من تطبيقات Kaspersky و منتجات أمان المعلومات من جهات خارجية.

للاستجابة للحوادث المتقدمة، يستخدم EDR Expert (cloud) سيناريوهات معدة مسبقًا ومحددة بواسطة المستخدم. ويمكنك أيضًا استخدام إجراءات الاستجابة من تطبيقات الجهات الخارجية وسيناريوهات الاستجابة التي تتضمن تطبيقات متعددة.

أدوات معلومات التهديدات

يستخدم Kaspersky Endpoint Detection and Response أدوات Threat Intelligence التالية:

- التكامل مع Kaspersky Threat Intelligence Portal، التي تحتوي على معلومات عن سمعة الملفات وعناوين الويب وتعرضها.
- قاعدة بيانات التهديدات الخاصة بشركة Kaspersky.
- 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.

مبدأ تشغيل الحل

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.

يتم إرسال المعلومات عن الأحداث على الكمبيوتر (القياس عن بُعد) إلى خادم EDR Expert (cloud). وفي هذه الحالة، يرسل Kaspersky Endpoint Security أيضًا معلومات عن التهديدات التي اكتشفتها Kaspersky بالإضافة إلى معلومات عن نتائج معالجة هذه التهديدات.

تم تكوين تكامل EDR Expert (cloud) في وحدة تحكم Kaspersky Security Center. وبعد ذلك تتم إدارة العامل المضمن باستخدام منصة الإدارة الواحدة المفتوحة (OSMP)، بما في ذلك مهام التشغيل وإدارة الكائنات المعزولة وعرض التقارير والإجراءات الأخرى.

تكامل العميل المدمج مع EDR Expert (cloud)

لإعداد التكامل مع حل Kaspersky Endpoint Detection and Response (cloud)، يجب عليك تثبيت مكون Endpoint Detection and Response Expert (cloud) وتكوين Kaspersky Endpoint Security.

لا تتوافق مكونات Endpoint Detection and Response Optimum و Endpoint Detection and Response Expert (cloud) و Endpoint Detection and Response Expert (on-premises) مع بعضها البعض.

ظروف تشغيل EDR Expert (cloud)

لكي يعمل EDR Expert (cloud)، يجب استيفاء الشروط التالية:

- تتوفر البنية التحتية لحل Kaspersky Endpoint Detection and Response Expert (cloud) في منطقتك. وللحصول على معلومات عن مدى توفر البنية التحتية لحل EDR Expert (cloud) في منطقتك، يرجى الاتصال بالدعم الفني.
- تم تثبيت OSMP (Open Single Management Platform).
- تم تثبيت Kaspersky Endpoint Security في الوضع القياسي.
- تم تفعيل تطبيق Kaspersky Endpoint Security ويغطي الترخيص الوظائف.
- لقد قبلت شروط اتفاقية معالجة البيانات لحل Kaspersky Endpoint Detection and Response Expert (cloud).
- تم تمكين مكون Endpoint Detection and Response Expert (cloud).
- يتم تمكين وتشغيل مكونات التطبيق التي تضمن تشغيل EDR Expert (cloud):
  - الحماية من تهديدات الملفات.
  - الحماية من تهديدات الويب.
  - الحماية من تهديدات البريد.
  - منع الاستغلال.
  - اكتشاف السلوك.
  - منع اختراق المضيف.
  - محرك المعالجة.
  - مراقبة عيوب التكيف.

خطوات التكامل مع EDR Expert (cloud)

يتضمن إعداد تكامل EDR Expert (cloud) الخطوات التالية:

1. **تثبيت مكون Endpoint Detection and Response Expert (cloud)**

يمكنك تحديد مكون Endpoint Detection and Response Expert (cloud) أثناء التثبيت أو الترقية، وكذلك استخدام مهمة تغيير مكونات التطبيق.

يجب إعادة تشغيل الكمبيوتر لإنهاء ترقية التطبيق بالمكون الجديد.

2. **تفعيل Kaspersky Endpoint Detection and Response Expert (cloud)**

تحتاج إلى شراء ترخيص منفصل لحل Kaspersky Endpoint Detection and Response Expert (cloud).

ستتوفر الوظيفة بعد إضافة مفتاح منفصل لحل Kaspersky Endpoint Detection and Response Expert (cloud). ونتيجة لذلك، تتم إضافة مفتاحين على الكمبيوتر: مفتاح لحل Kaspersky Endpoint Security ومفتاح لحل Kaspersky Endpoint Detection and Response Expert (cloud).

الترخيص لوظيفة Endpoint Detection and Response Expert (cloud) المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

تأكد من تضمين وظيفة EDR Expert (cloud) في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

3. **الاتصال بخادم جمع القياس عن بُعد وخادم الاستجابة**

يتطلب Kaspersky Endpoint Detection and Response Expert (cloud) اتصالاً موثوقًا به بين Kaspersky Endpoint Security وخادمين:

- خادم جمع القياس عن بعد هو خادم يعد جزءًا من حل SIEM الذي يجمع المعلومات عن الأحداث التي تحدث على الكمبيوتر وتوحيدها وربطها وتحليلها وتخزينها.
- خادم الاستجابة هو خادم لاستلام البيانات وفحصها ودراسة سلوك الكائنات ونشر نتائج هذه الدراسات.

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون EDR Expert (cloud) باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (cloud)**.
5. قم بتمكين المكون باستخدام مفتاح التبديل **Endpoint Detection and Response Expert (cloud) DISABLED**.
6. إذا كانت السياسة الحالية عبارة عن سياسة فرعية وتمنع السياسة الرئيسية إجراء تغييرات على إعدادات تكامل EDR Expert (cloud) ("قفل" مغلق)، فيمكنك تكوين وراثة الإعداد في قسم **Inheritance**:

- **Inherit connection settings from the policy** (القيمة الافتراضية). سيتم توريث إعدادات الاتصال من السياسة الرئيسية. ولن تتمكن من تحرير الإعدادات.
- **Use custom connection settings**. يمكنك تكوين إعدادات الاتصال يدويًا.

7. تعرض علامة التبويب **Response server** اسم المجال المؤهل بالكامل ومنفذ خادم الاستجابة، اللذين يتم استردادهما تلقائيًا. وإذا كانت سياسة الأمان في بنيتك التحتية لا تسمح لك بالاتصال مباشرة بخوادم EDR Expert (cloud)، فيمكنك إعداد اتصال عبر قناة TCP:

a. حدد خانة الاختيار **Use a TCP tunnel for response**.

b. حدد عنوان الخادم (IPv4، IPv6) والمنفذ للاتصال بالقناة.

8. إذا لزم الأمر، قم بتعيين تكرار إرسال طلبات المزامنة إلى الخادم في الحقل **Send sync request to server every (min)**. أثناء المزامنة، يتلقى Kaspersky Endpoint Security مهام الاستجابة للتهديدات ويرسل نتائج المهام.

9. انتقل إلى علامة التبويب **Telemetry collection server**.

10. تكوين إعدادات اتصال خادم مجموعة القياس عن بعد:

a. انقر على رابط **Edit**.

b. في النافذة التي تفتح، حدد خادم مجموعة القياس عن بعد من القائمة. ويعمل مُجمع KUMA كخادم تجميع للقياس عن بُعد في EDR Expert (cloud). وللحصول على المزيد من التفاصيل، يرجى الرجوع إلى تعليمات Kaspersky Unified Monitoring and Analysis Platform.

في حالة حدوث خطأ أثناء الاتصال بخادم مجموعة القياس عن بُعد، حدد خادمًا مختلفًا. وإذا كنت غير قادر على الاتصال بخادم جمع القياس عن بعد، يرجى الاتصال بالدعم الفني.

c. إذا لزم الأمر، يمكنك تكوين اتصال بخادم مجموعة القياس عن بُعد عبر قناة TCP، تمامًا كما تفعل مع خادم الاستجابة.

11. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

يمكنك التحقق من حالة المكون باستخدام Report on status of application components. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **Endpoint Detection and Response Expert (cloud)** إلى قائمة مكونات Kaspersky Endpoint Security.

تكوين إعدادات القياس عن بُعد لحل EDR Expert (cloud)

القياس عن بعد عبارة عن قائمة الأحداث التي وقعت على الكمبيوتر المحمي. ويحلل Kaspersky Endpoint Security بيانات القياس عن بُعد ويرسلها إلى خوادم جمع القياس عن بُعد 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).

لتكوين إعدادات القياس عن بُعد، اتبع الخطوات التالية:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** ← **Endpoint Detection and Response Expert (cloud)**.

5. في النافذة التي تفتح، حدد القسم **Data transmission settings**.

6. تأكد من تحديد خانة الاختيار **Sending telemetry ENABLED**.

7. إذا لزم الأمر، قم بتمكين وظائف **Send telemetry with IOA only**. مؤشر الهجوم (IOA) هو قاعدة تحتوي على وصف لسلوك مشبوه في النظام مما قد يشير إلى هجوم موجه. ويقارن التطبيق السلوك الجاري في النظام مع هذه القواعد ويسجل الأحداث التي تشير إلى هجوم موجه. ويستخدم التطبيق تقنية فحص البث التي تتيح تتبع مثل هذه الأحداث في الوقت الحقيقي. وبشكل افتراضي، يتم تعطيل الوظيفة.

8. إذا لزم الأمر، قم بتكوين إعدادات مزامنة الخادم:

- **Maximum event transmission delay (sec)**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
- **Maximum number of event packages**. يتزامن التطبيق مع الخادم عندما يمتلئ المخزن المؤقت بالأحداث. الإعداد الافتراضي هو 1024 حدثًا.

9. انتقل إلى علامة التبويب **Request throttling**.

10. إذا لزم الأمر، قم بتعطيل تقييد الطلب باستخدام مفتاح التبديل **Request throttling ENABLED**.

تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث. ويتم تمكين هذا الخيار بشكل افتراضي.

11. 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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 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%.

12. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

استثناءات القياس عن بُعد لحل EDR Expert (cloud)

لتحسين الأداء وتحسين إرسال البيانات إلى خادم جمع القياس عن بُعد، يمكنك إضافة استثناءات القياس عن بعد. على سبيل المثال، يمكنك اختيار عدم إرسال بيانات اتصالات الشبكة لتطبيقات فردية.

يمكن أن يؤدي استخدام الكثير من القواعد إلى زيادة الحمل على خادم جمع القياس عن بُعد وتقليل أداء الكمبيوتر. ونوصي بإضافة القواعد الضرورية فقط.

لإنشاء استثناء للقياس عن بعد في Web Console وCloud Console:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **General Settings** ← **Telemetry Settings**.

5. حدد علامة التبويب **EDR Expert (cloud) telemetry**.

6. في القسم **General exclusions**، انقر على الزر **Add**.
تفتح النافذة **Add exclusion rule**.

7. إذا لزم الأمر، قم بتغيير حالة القاعدة. بشكل افتراضي، يتم تمكين القاعدة.

8. أدخل اسمًا للقاعدة.

9. حدد الإجراء الذي سيتم تنفيذه عند تشغيل القاعدة:

- **Do not collect**. سيتم استثناء الحدث الذي تمت تصفيته من القياس عن بُعد الذي تم إرساله.
- **Exclude IOA**. سيتم استثناء حدث مشغل قاعدة مؤشر الهجوم (IOA) من القياس عن بُعد الذي تم إرساله.

10. في حالة تحديد الخيار **Exclude IOA**، حدد قواعد مؤشر الهجوم (IOA) لإضافتها إلى الاستثناءات:

- **Exclude all**. عند تلبية الشرط المحدد، سيستثني التطبيق الأحداث التي تم إنشاؤها بناءً على جميع قواعد مؤشر الهجوم (IOA) من القياس عن بُعد.
- **Exclude by GUID**. حدد المعرّف الفريد العام (GUID) الخاص بقاعدة مؤشر الهجوم (IOA). ويمكنك تحديد عدة معرّفات فريدة عامة (GUID) باستخدام `,`. وللمزيد من التفاصيل عن قواعد مؤشر الهجوم (IOA)، يرجى الرجوع إلى تعليمات EDR Expert (cloud).

11. حدد شرط التصفية:

a. حدد اسم الحقل الذي سيتم استخدامه للتصفية.

b. حدد معاملاً (انظر الجدول أدناه) وحدد القيمة التي ستتم مقارنة قيمة الحقل من الحدث بها.

قائمة المعاملات الشرطية

المعامل	الوصف
>	إذا كانت قيمة الحقل أقل من القيمة المحددة في الشرط، فسيتم تصفية الحدث.
≥	إذا كانت قيمة الحقل أقل من القيمة المحددة في الشرط أو مساوية لها، فسيتم تصفية الحدث.
=	إذا كانت قيمة الحقل مساوية للقيمة المحددة في الشرط، فسيتم تصفية الحدث.
≤	إذا كانت قيمة الحقل أكبر من أو تساوي القيمة المحددة في الشرط، فسيتم تصفية الحدث.
<	إذا كانت قيمة الحقل أكبر من القيمة المحددة في الشرط، فسيتم تصفية الحدث.
≠	إذا كانت قيمة الحقل لا تساوي القيمة المحددة في الشرط، فسيتم تصفية الحدث.
is like	إذا كانت قيمة الحقل تطابق القناع المحدد في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي `*` و `?` عند إدخال قناع:
is not like	إذا كانت قيمة الحقل لا تتطابق مع القناع المحدد في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي `*` و `?` عند إدخال قناع:
one of	إذا كانت قيمة الحقل تتطابق مع إحدى القيم الموجودة في القائمة المحددة في الشرط، فسيتم اعتبار الحدث قد تمت تصفيته.
none of	إذا كانت قيمة الحقل لا تطابق أيًا من القيم الموجودة في القائمة المحددة في الشرط، فسيتم اعتبار الحدث قد تمت تصفيته.
is like one of	إذا كانت قيمة الحقل تتطابق مع أحد الأقنعة المحددة في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي * و? عند إدخال قناع.
is not like one of	إذا كانت قيمة الحقل لا تتطابق مع أي من الأقنعة المحددة في الشرط، فسيتم تصفية الحدث. يدعم التطبيق حرفي * و? عند إدخال قناع.
exists	إذا كان الحقل المحدد في الشرط موجودًا في الحدث، فسيتم تصفية الحدث.
not exists	إذا لم يكن الحقل المحدد في الشرط موجودًا في الحدث، فسيتم تصفية الحدث.
contains	إذا كانت القيمة المحددة في الشرط موجودة في قيمة الحقل، فسيتم تصفية الحدث.

المعامل	الوصف
is equal to	إذا كانت قيمة الحقل مساوية للقيمة المحددة في الشرط، فسيتم تصفية الحدث. الفحص غير حساس لحالة الأحرف.
bitwise AND	إذا كانت نتيجة عملية Bitwise AND (&) بين قيمة الحقل والقيمة المحددة في الشرط هي 1، فسيتم تصفية الحدث.

12. إذا لزم الأمر، يمكنك إنشاء معايير تصفية معقدة عن طريق إضافة شروط عامل التصفية المتعددة ومجموعات الشروط. ويمكنك أيضًا إضافة شروط متداخلة ومجموعات شروط إلى مجموعة شروط. ويمكنك استخدام المعاملات التالية:

- يعني **AND** أن عامل التصفية يحدد الأحداث التي تلبي جميع الشروط المحددة.
- يعني **OR** أن عامل التصفية يحدد الأحداث التي تلبي أحد الشروط المحددة.
- يعني **NOT** (لاستخدام هذا المعامل، حدد الخيار **Add NOT before**) أن عامل التصفية يحدد الأحداث التي لا تلبي أيًا من الشروط المحددة.

يتم دمج الشروط ومجموعات الشروط من المستوى الأول مع معامل **AND**.

13. لفحص قاعدة التصفية التي أنشأتها، انقر فوق الزر **Check rule**.

في النافذة التي تفتح، سيتم عرض جدول بالأحداث التي تمت تصفيتها حسب القاعدة التي تم إنشاؤها. وللمزيد من التفاصيل، يرجى الرجوع إلى تعليمات EDR Expert (cloud).

14. إذا لزم الأمر، تحت **All event types**، أضف استثناءات القياس عن بُعد حسب نوع الحدث.

a. انقر فوق اسم نوع الحدث.

b. في النافذة التي تفتح، انقر فوق الزر **Set up manually**.

c. إذا لزم الأمر، قم بتكوين إرسال القياس عن بُعد لنوع الحدث المحدد باستخدام زر التبديل **Send event**. وبشكل افتراضي، يتم تمكين إرسال القياس عن بُعد لجميع أنواع الأحداث.

d. في القسم **Exclusion rules**، انقر على الزر **Add**.

تفتح النافذة **Add exclusion rule**.

e. نفذ الإجراءات الموضحة في الخطوات من 7 إلى 13 لكل قاعدة تضيفها.

15. بالنسبة لبعض أنواع الأحداث، يمكنك أيضًا إضافة قواعد التضمين لتوسيع القياس عن بُعد الذي تم جمعه:

a. في القسم **Inclusion rules**، انقر على الزر **Add**.

تفتح النافذة **Add inclusion rules**.

b. أدخل اسمًا للقاعدة.

c. تحت **Condition**، أدخل قيم الحقول المعروضة. ويعتمد نوع الحقول المتاحة على الحدث المحدد.

يتم إعطاء الأولوية لقواعد الاستثناء على قواعد التضمين.

16. لتطبيق السياسة على أجهزة الكمبيوتر، تأكد من أن الأقفال مغلقة (🔒) واحفظ تغييراتك.

كيفية تصدير أو استيراد عوامل تصفية أحداث EDR Expert (cloud).

يمكنك تصدير قائمة الاستثناءات إلى ملف JSON. وبعد ذلك يمكنك تعديل الملف، على سبيل المثال، إضافة عدد كبير من معرفات الأحداث. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من عوامل تصفية الأحداث أو لترحيل القائمة إلى خادم مختلف.

يمكن أن يؤدي استخدام الكثير من القواعد إلى زيادة الحمل على خادم جمع القياس عن بُعد وتقليل أداء الكمبيوتر. ونوصي بإضافة القواعد الضرورية فقط.

لتصدير أو استيراد عوامل تصفية الأحداث في Web Console:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Telemetry Settings**.
5. حدد علامة التبويب **EDR Expert (cloud) telemetry**.
6. لتصدير عوامل تصفية الحدث:
   a. انقر على **Export**.
   b. في النافذة التي تفتح، حدد اسم ملف JSON الذي تريد تصدير عوامل تصفية الأحداث إليه وحدد المجلد الذي تريد حفظ هذا الملف به.
   c. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير عوامل تصفية الأحداث إلى ملف JSON.
7. لاستيراد عوامل تصفية الأحداث:
   a. انقر على **Import**.
   b. في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد عوامل تصفية الأحداث منه.
   c. حدد الطريقة التي تريد بها استيراد قواعد تصفية الأحداث: عن طريق الإضافة إلى القواعد الموجودة أو عن طريق تجاهل القواعد الموجودة والاستعاضة عنها بقواعد جديدة.
   d. افتح الملف.
8. لتطبيق السياسة على أجهزة الكمبيوتر، تأكد من أن الأقفال مغلقة (🔒) واحفظ تغييراتك.
   1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
   2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
      فتح نافذة خصائص السياسة.
   3. حدد علامة التبويب **Application settings**.
   4. انتقل إلى **General Settings** ← **Telemetry Settings**.

5. حدد علامة التبويب **EDR Expert (cloud) telemetry**.

6. لتصدير عوامل تصفية الحدث:

   a. انقر على **Export**.

   b. في النافذة التي تفتح، حدد اسم ملف JSON الذي تريد تصدير عوامل تصفية الأحداث إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

   c. احفظ الملف.

   يقوم Kaspersky Endpoint Security بتصدير عوامل تصفية الأحداث إلى ملف JSON.

7. لاستيراد عوامل تصفية الأحداث:

   a. انقر على **Import**.

   b. في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد عوامل تصفية الأحداث منه.

   c. حدد الطريقة التي تريد بها استيراد قواعد تصفية الأحداث: عن طريق الإضافة إلى القواعد الموجودة أو عن طريق تجاهل القواعد الموجودة والاستعاضة عنها بقواعد جديدة.

   d. افتح الملف.

8. لتطبيق السياسة على أجهزة الكمبيوتر، تأكد من أن الأقفال مغلقة (🔒) واحفظ تغييراتك.

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 تكامله مع حلول Kaspersky Detection and Response. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل عن 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 وتعليمات Kaspersky Endpoint Detection and Response Expert (on-premises).

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

بشكل افتراضي، يقتصر حجم العزل على 1024 ميجابايت. وعندما يصل العزل إلى الحد الأقصى للحجم، يتوقف Kaspersky Endpoint Security عن إرسال الملفات وينشئ الحدث لا تتوفر مساحة كافية في مخزن العزل. ولمنع نفاد مساحة القرص في العزل، يمكنك تعيين حد ينشئ عنده Kaspersky Endpoint Security الحدث مساحة تخزين العزل على وشك النفاد. ولا يمكنك تكوين فترة احتفاظ للملفات المعزولة لإزالتها تلقائيًا.

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 (RAM) على الكمبيوتر (على سبيل المثال، 8 جيجا بايت) أو تعطيل حد حجم العزل.

كيفية تكوين الحد الأقصى لحجم العزل في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **التقارير والمخزن**.

4. في قسم **العزل**، قم بتكوين حجم العزل:

- **تقييد حجم العزل إلى N م ب**. إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لحجم العزل ليكون بالقيمة المُحددة. والإعداد الافتراضي لهذا الخيار هو 1024 ميجا بايت. وعندما يصل العزل إلى الحجم الأقصى، يرسل Kaspersky Endpoint Security حدث لا تتوفر مساحة كافية في مخزن العزل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يوقف التطبيق عزل الكائنات الجديدة. ويجب إفراغ العزل يدويًا.

  إذا تم إلغاء تحديد خانة الاختيار، فسيتم تحديد حجم العزل على حسب المساحة الخالية المتوفرة على القرص.

- **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.

  إذا تم إلغاء تحديد خانة الاختيار هذه، فلن ينشئ التطبيق أحداثًا عند الوصول إلى حد العزل.

5. احفظ تغييراتك.

كيفية تكوين الحد الأقصى لحجم العزل في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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**. إذا تم تحديد خانة الاختيار، فإن حجم العزل يقتصر على القيمة المحددة. إذا تم إلغاء تحديد خانة الاختيار، فسيتم تحديد حجم العزل على حسب المساحة الخالية المتوفرة على القرص. وقد يكون هذا ضروريًا لفحص YARA لأن التطبيق يمكنه حفظ ملف تفريغ ذاكرة كبير.

- **Maximum size of Quarantine (MB)**. إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لحجم العزل ليكون بالقيمة المُحددة. والإعداد الافتراضي لهذا الخيار هو 1024 ميجا بايت. وعندما يصل العزل إلى الحجم الأقصى، يرسل Kaspersky Endpoint Security حدث لا تتوفر مساحة كافية في مخزن العزل إلى Kaspersky Security Center وينشر الحدث في Windows Event Log. وفي الوقت نفسه، يوقف التطبيق عزل الكائنات الجديدة. ويجب إفراغ العزل يدويًا.

  إذا تم إلغاء تحديد خانة الاختيار، فسيتم تحديد حجم العزل على حسب المساحة الخالية المتوفرة على القرص.

- **Notify when the Quarantine storage reaches (%)**. 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.

كيفية تمكين نقل بيانات الملفات المعزولة في وحدة التحكم في الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **التقارير والمخزن**.
4. في القسم **نقل البيانات إلى خادم الإدارة**، انقر على الزر **الإعدادات**.
5. في النافذة التي تفتح، حدد خانة الاختيار **عزل الملفات**.
6. احفظ تغييراتك.

كيفية تمكين نقل بيانات الملفات المعزولة في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **KSC Integration**.
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. يحفظ التطبيق نسخة من الملف في العزل بعد استعادة الملف. ولحذف الملف، يجب عليك مسح العزل يدويًا.

مراقبة إجراءات EDR

يقدم Kaspersky Endpoint Security for Windows 12.9 مركز مراقبة إجراءات EDR. مركز مراقبة إجراءات EDR هو وحدة تحكم يمكنك من خلالها عرض محفوظات الاستجابة للتهديدات لجميع حلول Kaspersky Detection and Response. وإذا كانت مؤسستك لديها العديد من عمليات الاكتشاف والاستجابة التي تم نشرها (على سبيل المثال، EDR Optimum وMDR)، فسيعرض Kaspersky Endpoint Security محفوظات الاستجابة للتهديدات لجميع الحلول. ويتيح لك ذلك تحليل أداء حلول الاكتشاف والاستجابة على كمبيوتر منفصل وتحسين إعدادات هذه الحلول.

يوفر مركز المراقبة المعلومات التالية:

- معلومات عن مهام الاستجابة للتهديدات (على سبيل المثال، مهمة إنهاء العملية)
- التغييرات في عزل شبكة الاتصال وقواعد منع التنفيذ

إذا واجهت الاستجابة للتهديدات خطأً يتعلق بالوصول إلى مشاركة شبكة اتصال، فسيتم حذف هذا الخطأ من محفوظات الاستجابة للتهديدات المعروضة.

للانتقال إلى مركز مراقبة إجراءات EDR:

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Assets (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 14.2**.

   تقوم هذه الخطوة بفتح الإعدادات الخاصة بالتطبيق المحلي.

5. حدد علامة التبويب **Application settings**.

6. انتقل إلى **Detection and Response** ← **Response history**.

يؤدي ذلك إلى فتح وحدة تحكم مركز مراقبة إجراءات EDR. ويمكنك استخدام وحدة التحكم لعرض حالات مهمة الاستجابة للتهديدات ومدة المهمة وتغييرات القواعد وتفاصيل المُنشئ.

Kaspersky Unified Monitoring and Analysis Platform (KUMA)



يدعم Kaspersky Endpoint Security for Windows حل Kaspersky Unified Monitoring and Analysis Platform. وKaspersky Unified Monitoring and Analysis Platform (KUMA) هو حل إدارة معلومات الأمان والأحداث (SIEM) للبنية التحتية لتكنولوجيا المعلومات في المؤسسات. ويسمح KUMA باكتشاف التهديدات الأمنية وتحليلها والتخفيف من حدتها قبل أن تتسبب في ضرر.

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 Unified Monitoring and Analysis Platform (KUMA). وفي وحدة التحكم الخاصة به، يعرض KUMA الأحداث في شكل قائمة بدون علامات، مشابه لسجل أحداث Windows.

لا يوفر Kaspersky Endpoint Security كل وظائف عميل KUMA. ويرسل التطبيق الأحداث فقط إلى KUMA بدون ترميز. وللوصول إلى كل وظائف KUMA، تحتاج إلى شراء ترخيص ونشر الحل وفقًا لدليل مسؤول KUMA.

تكامل Kaspersky Endpoint Security مع KUMA

يتضمن إعداد تكامل KES مع KUMA الخطوات التالية:

1. في وحدة تحكم KUMA، أضف مُجمعًا.
2. في وحدة تحكم KUMA، كوّن موصلاً للمُجمع لاستلام الأحداث من KES.
3. في وحدة تحكم KUMA، قم بتمكين المصادقة ثنائية الاتجاه (اختياري).
4. في سياسة Kaspersky Endpoint Security for Windows، كوّن الإعدادات لتوصيل KES بمنصة KUMA.
5. في وحدة تحكم KUMA، تأكد من وصول الأحداث الواردة من KES إلى المستأجر الصحيح ومعالجتها بواسطة قواعد الربط الصحيحة.

التحضير لدمج KES مع KUMA

لاستخدام KUMA، يجب استيفاء الشروط التالية:

- Kaspersky Security Center الإصدار 14.2 أو أحدث. وفي الإصدارات السابقة من Kaspersky Security Center، من المستحيل تفعيل وظيفة تكامل KUMA.
- تم تفعيل التطبيق ويغطي الترخيص الوظيفة.
- تم تمكين مكون تكامل KUMA.

يتضمن التحضير لتكامل KES مع KUMA الخطوات التالية:

1. **تثبيت مكون تكامل KUMA**

ويمكنك تحديد مكون تكامل KUMA أثناء تثبيت أو ترقية التطبيق، وكذلك استخدام مهمة تغيير مكونات التطبيق.

يجب إعادة تشغيل الكمبيوتر لإنهاء ترقية التطبيق بالمكون الجديد.

2. **تفعيل KUMA**

بالإضافة إلى ترخيص تطبيق Kaspersky Endpoint Security (على سبيل المثال، Kaspersky Endpoint Security for Business Standard)، تحتاج إلى ترخيص منفصل لتكامل Kaspersky Endpoint Security مع KUMA (الوظيفة الإضافية لتكامل Kaspersky Endpoint Security for Windows KUMA).

إذا كنت تقوم بتثبيت التطبيق في وضع عميل EDR، فأنت بحاجة إلى ترخيص لدمج Kaspersky Endpoint Security مع KUMA وترخيص Kaspersky Anti Targeted Attack Platform (KATA) أو ترخيص Kaspersky Managed Detection and Response (MDR). ولا يمكنك نشر عميل EDR لحل KUMA فقط.

تصبح الوظيفة متاحة بعد إضافة مفتاح KUMA المنفصل. ونتيجة لذلك، سيكون هناك مفتاح نشط آخر على الكمبيوتر لتكامل Kaspersky Endpoint Security مع KUMA.

الترخيص لوظيفة KUMA المستقلة هو ترخيص Kaspersky Endpoint Security نفسه.

تأكد من تضمين وظيفة KUMA في الترخيص وتشغيلها في الواجهة المحلية للتطبيق.

ربط KES مع KUMA

لتوصيل الكمبيوتر الذي يحتوي على تطبيق Kaspersky Endpoint Security بحل KUMA:

1. في وحدة تحكم KUMA، أضف مجمّعًا بموصلات من نوع **tcp** أو **udp** أو **http** وحدد إعدادات الشبكة الأساسية للاتصال. وللحصول على تفاصيل عن إدارة المجمعات، يرجى الرجوع إلى تعليمات Kaspersky Unified Monitoring and Analysis Platform.

2. في سياسة Kaspersky Endpoint Security، أضف عناوين مُجمع KUMA وحدد إعدادات الشبكة الخاصة بالاتصال.

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون KUMA باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة، حدد **تكامل KUMA**.

5. حدد خانة الاختيار **تكامل KUMA**.

6. في القسم **إعدادات التكامل**، حدد خانة الاختيار **"تمكين نقل أحداث Windows إلى خادم KUMA": $IsKUMATelemetry ? "تمكين نقل أحداث Windows إلى خادم SIEM"**.

7. إضافة خوادم KUMA:

a. انقر على **إضافة**.

يؤدي هذا إلى فتح النموذج الذي يمكنك من خلاله إضافة خوادم KUMA.

b. حدد بروتوكول الاتصال بخادم KUMA: **HTTP / HTTPS**، **TCP**، **UDP**.

يجب أن يتطابق بروتوكول الاتصال بالمُجمع في Kaspersky Endpoint Security مع نوع الموصل في KUMA: **http** أو **tcp**، أو **udp**.

عند استخدام بروتوكول UDP، قد تُفقد البيانات بسبب فقدان حزم البيانات المتأصل في طبيعة هذا البروتوكول.

c. أدخل عنوان الخادم (IPv4، Ipv6، FQDN) والمنفذ للاتصال بالخادم (بشكل افتراضي، يتم تحديد المنفذ 443).

عند إدخال عنوان الخادم، ضع في اعتبارك ما يلي:

- **TCP**:
  - **بدون TLS**. يمكنك تحديد عنوان IP أو FQDN للخادم.
  - **مع TLS**. يجب تحديد FQDN للخادم فقط.
- **HTTP / HTTPS**:
  - **بدون TLS**. يجب عليك تحديد بروتوكول HTTP بشكل صريح في عنوان الخادم (على سبيل المثال، `http://server.com` أو `http://10.10.10.100`).
  - **مع TLS**. لا يلزمك تحديد البروتوكول (على سبيل المثال، `https://server.com` أو `server.com`).
- **UDP**. لا يدعم بروتوكول UDP تشفير TLS. يمكنك تحديد عنوان IP أو FQDN للخادم.

يمكنك عرض عنوان الخادم في خصائص الموصل في وحدة تحكم KUMA. وللمزيد من المعلومات عن موصلات KUMA، انظر تعليمات Kaspersky Unified Monitoring and Analysis Platform.

d. انقر على **موافق**.

يتصل Kaspersky Endpoint Security بخادم KUMA الأول في القائمة. وفي حالة فشل الاتصال، يتصل Kaspersky Endpoint Security بخادم KUMA الثاني في القائمة وهكذا.

8. إذا لزم الأمر، كوّن إعداد **الحد الأقصى لتأخير إرسال الحدث (ثانية)** في القسم **إعدادات نقل البيانات**. وعند نفاد الوقت المحدد، يحاول Kaspersky Endpoint Security الاتصال بالمُجمع نفسه أو الاتصال بالمُجمع التالي في القائمة في حالة وجود مُجمعات متعددة. الإعداد الافتراضي هو 30 ثانية.

9. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية توصيل كمبيوتر Kaspersky Endpoint Security بمكون KUMA باستخدام Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← **Policies**.

2. انقر فوق اسم سياسة Kaspersky Endpoint Security.

فتح نافذة خصائص السياسة.

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

4. انتقل إلى **Built-in Agents Configuration** ← **KUMA Integration**.

5. قم بتشغيل مفتاح **KUMA Integration ENABLED**.

6. إضافة خوادم KUMA:

a. انقر على **Add**.

يؤدي هذا إلى فتح النموذج الذي يمكنك من خلاله إضافة خوادم KUMA.

b. حدد بروتوكول الاتصال بخادم KUMA: **HTTP/HTTPS**، **TCP**، **UDP**.

يجب أن يتطابق بروتوكول الاتصال بالمُجمع في Kaspersky Endpoint Security مع نوع الموصل في KUMA: **http** أو **tcp**، أو **udp**.

عند استخدام بروتوكول UDP، قد تُفقد البيانات بسبب فقدان حزم البيانات المتأصل في طبيعة هذا البروتوكول.

c. أدخل عنوان الخادم (IPv4، Ipv6، FQDN) والمنفذ للاتصال بالخادم (بشكل افتراضي، يتم تحديد المنفذ 443).

عند إدخال عنوان الخادم، ضع في اعتبارك ما يلي:

- **TCP**:
  - **بدون TLS**. يمكنك تحديد عنوان IP أو FQDN للخادم.
  - **مع TLS**. يجب تحديد FQDN للخادم فقط.
- **HTTP/HTTPS**:
  - **بدون TLS**. يجب عليك تحديد بروتوكول HTTP بشكل صريح في عنوان الخادم (على سبيل المثال، `http://server.com` أو `http://10.10.10.100`).
  - **مع TLS**. لا يلزمك تحديد البروتوكول (على سبيل المثال، `https://server.com` أو `server.com`).
- **UDP**. لا يدعم بروتوكول UDP تشفير TLS. يمكنك تحديد عنوان IP أو FQDN للخادم.

يمكنك عرض عنوان الخادم في خصائص الموصل في وحدة تحكم KUMA. وللمزيد من المعلومات عن موصلات KUMA، انظر تعليمات Kaspersky Unified Monitoring and Analysis Platform.

d. انقر على **OK**.

يتصل Kaspersky Endpoint Security بخادم KUMA الأول في القائمة. وفي حالة فشل الاتصال، يتصل Kaspersky Endpoint Security بخادم KUMA الثاني في القائمة وهكذا.

7. إذا لزم الأمر، كوّن إعداد **Maximum delay when sending events (sec)** في القسم **Server connection settings**. وعند نفاد الوقت المحدد، يحاول Kaspersky Endpoint Security الاتصال بالمُجمع نفسه أو الاتصال بالمُجمع التالي في القائمة في حالة وجود مُجمعات متعددة. الإعداد الافتراضي هو 30 ثانية.

8. احفظ تغييراتك.

يمكنك التحقق من تكوين تكامل KUMA بشكل صحيح في وحدة تحكم KUMA (للمزيد من التفاصيل، راجع تعليمات Kaspersky Unified Monitoring and Analysis Platform). تحقق من حالة تشغيل المكون من خلال عرض Report on status of application components في وحدة تحكم Kaspersky Security Center. ويمكنك أيضًا عرض حالة تشغيل أحد المكونات في التقارير في الواجهة المحلية لتطبيق Kaspersky Endpoint Security. وستتم إضافة مكون **تكامل KUMA** إلى قائمة مكونات Kaspersky Endpoint Security.

إنشاء اتصال موثوق بين KES وKUMA

يمكنك إنشاء اتصال موثوق بين Kaspersky Endpoint Security ومُجمع KUMA باستخدام موصل من نوع tcp أو http. ولا يمكن إنشاء اتصال موثوق مع موصل من نوع udp.

لإنشاء اتصال موثوق، يلزم تكوين وضع TLS في إعدادات الموصل. وتكون أوضاع TLS التالية ممكنة:

- **Disabled**: عدم استخدام تشفير TLS. ويتم تحديد هذا الخيار بشكل افتراضي.
- **Enabled**: استخدام تشفير TLS، لكن بدون التحقق من الشهادة.
- **Custom PFX with client authentication**: استخدام تشفير TLS مع كلمة سر PFX. في هذا الوضع، يتم مصادقة العميل باستخدام شهادة.

لا يدعم Kaspersky Endpoint Security وضع TLS **Custom PFX**. وعند دمج KES مع KUMA مع PFX، يلزم مصادقة المستخدم بكلمة مرور.

لتكوين اتصال موثوق، تحتاج إلى شهادة TLS — شهادة سلطة التصديق للخدمة المصغرة. ويمكنك الحصول على شهادة TLS في وحدة تحكم KUMA. وللحصول على تفاصيل عن تنزيل شهادات TLS، يرجى الرجوع إلى تعليمات Kaspersky Unified Monitoring and Analysis Platform. وبعد ذلك يجب عليك إضافة شهادة TLS إلى Kaspersky Endpoint Security (انظر الإرشادات أدناه).

لجعل الاتصال أكثر أمانًا، يمكنك تمكين مصادقة إضافية لجهاز الكمبيوتر في KUMA (المصادقة ثنائية الاتجاه). ولتمكين هذه المصادقة، تحتاج إلى إنشاء حاوية تشفير في هيئة تصديق خارجية. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص بتنسيق PKCS#12. وبعد ذلك، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات KUMA (**Custom PFX with client authentication** لوضع TLS) وتمكين المصادقة ثنائية الاتجاه في Kaspersky Endpoint Security، وإضافة أرشيف PFX إلى وحدة تحكم KUMA وإلى Kaspersky Endpoint Security.

كيفية تكوين اتصال موثوق بين KES وKUMA في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **تكامل KUMA**.
5. حدد خانة الاختيار **تكامل KUMA**.
6. في القسم **إعدادات الاتصال بخوادم KUMA**، حدد خانة الاختيار **استخدام تشفير TLS**.
7. تكوين الاتصال الموثوق:
   a. انقر على **إعدادات الاتصال بخوادم KUMA**.
   b. تكوين اتصال الخادم:
   - **المهلة (ثانية)**. الحد الأقصى لوقت انتظار استجابة من خادم KUMA (القيمة الافتراضية 5 ثوانٍ). عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم KUMA مختلف.
   - **شهادة TLS للخادم**. شهادة TLS لإنشاء اتصال موثوق مع خادم KUMA. ويمكنك الحصول على شهادة TLS في وحدة تحكم Kaspersky Unified Monitoring and Analysis Platform (راجع التعليمات في تعليمات Kaspersky Unified Monitoring and Analysis Platform).

   لإنشاء اتصال موثوق، يتعين عليك تحديد **Enabled** وضع TLS في وحدة تحكم KUMA.

- **استخدام المصادقة ثنائية الاتجاه**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين KES وKUMA. لاستخدام المصادقة ثنائية الاتجاه، في وحدة تحكم KUMA، في إعدادات الموصل، يجب عليك تحديد وضع TLS **Custom PFX with client authentication** (راجع إعدادات الموصل في تعليمات Kaspersky Unified Monitoring and Analysis Platform). ثم يجب عليك تنزيل شهادة خادم وتعيين كلمة مرور لحماية حاوية التشفير.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

c. انقر على **موافق**.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين اتصال موثوق بين KES و KUMA في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **Built-in Agents Configuration** ← **KUMA Integration**.

5. قم بتشغيل مفتاح **KUMA Integration ENABLED**.

6. تحت **Server connection settings**، قم بتشغيل مفتاح **Use TLS encryption**.

7. تكوين الاتصال الموثوق:

a. انقر على **Connection settings**.

b. تكوين اتصال الخادم:

- **Timeout (sec)**. الحد الأقصى لوقت انتظار استجابة من خادم KUMA (القيمة الافتراضية 5 ثوانٍ). عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم KUMA مختلف.
- **Server TLS certificate**. شهادة TLS لإنشاء اتصال موثوق مع خادم KUMA. ويمكنك الحصول على شهادة TLS في وحدة تحكم Kaspersky Unified Monitoring and Analysis Platform (راجع التعليمات في تعليمات Kaspersky Unified Monitoring and Analysis Platform).
لإنشاء اتصال موثوق، يتعين عليك تحديد **Enabled** وضع TLS في وحدة تحكم KUMA.
- **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين KES وKUMA. لاستخدام المصادقة ثنائية الاتجاه، في وحدة تحكم KUMA، في إعدادات الموصل، يجب عليك تحديد وضع TLS **Custom PFX with client authentication** (راجع إعدادات الموصل في تعليمات Kaspersky Unified Monitoring and Analysis Platform). ثم يجب عليك تنزيل شهادة خادم وتعيين كلمة مرور لحماية حاوية التشفير.

يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.

c. انقر على **OK**.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

تمكين إرسال القياس عن بعد إلى خادم KUMA

بشكل افتراضي، يتم تعطيل إرسال الأحداث إلى خادم KUMA. وللتأكد من عمل KUMA بشكل صحيح، يجب تمكين إرسال القياس عن بُعد. ويمكنك تحديد مصدر حدث من بين السجلات القياسية: Application أو Security أو System.

كيفية تمكين إرسال القياس عن بُعد إلى KUMA في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.
5. في القسم **إعدادات القياس عن بعد** ← **القياس عن بعد في KUMA**، انقر على الزر **الإعدادات**.
6. حدد سجلات الأحداث التي تريد استخدامها كمصادر للأحداث: Application أو Security أو System.
   بالإضافة إلى السجلات القياسية، يمكنك تحديد سجل تطبيق جهة خارجية.
7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تمكين إرسال القياس عن بُعد إلى KUMA في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Telemetry Settings**.
5. حدد علامة التبويب **KUMA telemetry**.
6. حدد سجلات الأحداث التي تريد استخدامها كمصادر للأحداث: Application أو Security أو System.
   بالإضافة إلى السجلات القياسية، يمكنك تحديد سجل تطبيق جهة خارجية.
7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

يتم إرسال أحداث التصفية إلى KUMA

بشكل افتراضي، يتم تعطيل إرسال الأحداث إلى خادم KUMA. وللتأكد من عمل KUMA بشكل صحيح، يجب تمكين إرسال القياس عن بُعد. ويمكنك تحديد مصدر حدث من بين السجلات القياسية: Application أو Security أو System. ولتحسين الأداء وزيادة كفاءة إرسال البيانات إلى خادم KUMA، يمكنك إضافة أو استبعاد الأحداث الفردية يدويًا من بيانات القياس عن بعد. على سبيل المثال، يمكنك استبعاد أحداث Sysmon.

كيفية إنشاء قائمة بالأحداث التي سيتم إرسالها إلى KUMA في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.

5. في القسم **إعدادات القياس عن بعد** ← **القياس عن بعد في KUMA**، انقر على الزر **الإعدادات**.

6. في النافذة التي يتم عرضها، قم بتكوين عوامل تصفية الأحداث التي سيتم إرسالها إلى KUMA.
يمكنك تكوين تصفية الأحداث للسجلات المعيارية مثل سجلات Application وSecurity وSystem أو إضافة سجل آخر يدويًا:

   a. افتح خصائص السجل أو انقر فوق الزر **إضافة** وأدخل اسم السجل.

   b. حدد وضع إرسال الحدث:

   - **إرسال كل الأحداث**. في هذا الوضع ، يرسل التطبيق جميع الأحداث من سجل Windows باستثناء الأحداث المضافة إلى قواعد الاستثناء.
   - **إرسال الأحداث المحددة فقط**. في هذا الوضع، يرسل التطبيق الأحداث المضافة في قواعد التضمين فقط.

   c. أنشئ قوائم بقواعد الاستثناء أو قواعد التضمين لوضع إرسال الحدث المناسب.
   لإضافة قواعد، تحتاج إلى تحديد معرف الحدث في سجل أحداث Windows. ويمكنك سرد معرفات أحداث متعددة في القاعدة. ولتحديد معرّفات أحداث متعددة، استخدم حرف الفاصلة (,).

   d. إذا لزم الأمر، قم بتمكين تسجيل الأحداث باستخدام خانة الاختيار المجاورة لاسم السجل.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية إنشاء قائمة بالأحداث التي سيتم إرسالها إلى KUMA في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.

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

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

4. انتقل إلى **General Settings** ← **Telemetry Settings**.

5. حدد علامة التبويب **KUMA telemetry**.

6. في النافذة التي يتم عرضها، قم بتكوين عوامل تصفية الأحداث التي سيتم إرسالها إلى KUMA.
يمكنك تكوين تصفية الأحداث للسجلات المعيارية مثل سجلات Application وSecurity وSystem أو إضافة سجل آخر يدويًا:

   a. افتح خصائص السجل أو انقر فوق الزر **Add** وأدخل اسم السجل.

   b. حدد وضع إرسال الحدث:

   - **Send all events**. في هذا الوضع ، يرسل التطبيق جميع الأحداث من سجل Windows باستثناء الأحداث المضافة إلى قواعد الاستثناء.
   - **Send only selected events**. في هذا الوضع، يرسل التطبيق الأحداث المضافة في قواعد التضمين فقط.

c. أنشئ قوائم بقواعد الاستثناء أو قواعد التضمين لوضع إرسال الحدث المناسب.

لإضافة قواعد، تحتاج إلى تحديد معرف الحدث في سجل أحداث Windows. ويمكنك سرد معرفات أحداث متعددة في القاعدة. ولتحديد معرّفات أحداث متعددة، استخدم حرف الفاصلة (,).

d. إذا لزم الأمر، قم بتمكين تسجيل الأحداث باستخدام مفتاح التبديل الموجود بجوار اسم السجل.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

تصدير واستيراد عوامل تصفية حدث KUMA

يمكنك تصدير قائمة الاستثناءات إلى ملف JSON. وبعد ذلك يمكنك تعديل الملف، على سبيل المثال، إضافة عدد كبير من معرفات الأحداث. ويمكنك أيضًا استخدام وظيفة التصدير/الاستيراد لإنشاء نسخة احتياطية من عوامل تصفية الأحداث أو لترحيل القائمة إلى خادم مختلف.

يمكن أن يؤدي استخدام الكثير من القواعد إلى زيادة الحمل على خادم KUMA وتقليل أداء الكمبيوتر. ونوصي بإضافة القواعد الضرورية فقط.

كيفية تصدير واستيراد عوامل تصفية الأحداث في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

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

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

4. في نافذة السياسة، حدد **الإعدادات العامة** ← **الاستثناءات وأنواع الكائنات**.

5. في القسم **إعدادات القياس عن بعد** ← **القياس عن بعد في KUMA**، انقر على الزر **الإعدادات**.

6. لتصدير عوامل تصفية الحدث:

a. حدد سجلات الأحداث التي تتضمن عوامل التصفية التي تريد تصديرها.

b. انقر على الزر ← **تصدير**.

c. في النافذة التي تفتح، حدد اسم ملف JSON الذي تريد تصدير عوامل تصفية الأحداث إليه وحدد المجلد الذي تريد حفظ هذا الملف به.

d. احفظ الملف.

يقوم Kaspersky Endpoint Security بتصدير عوامل تصفية الأحداث إلى ملف JSON.

7. لاستيراد عوامل تصفية الأحداث:

a. انقر على الزر ← **استيراد**.

b. في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد عوامل تصفية الأحداث منه.

c. افتح الملف.

في حالة وجود قواعد تصفية الأحداث بالفعل على جهاز الكمبيوتر، يقوم Kaspersky Endpoint Security باستبدالها عند الاستيراد.

8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تصدير واستيراد عوامل تصفية الأحداث في Web Console

1. في نافذة Web Console الرئيسية، حدد **Asset management** ← علامة التبويب **Policies**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Telemetry Settings**.
5. حدد علامة التبويب **KUMA telemetry**.
6. لتصدير عوامل تصفية الحدث:
   a. حدد سجلات الأحداث التي تتضمن عوامل التصفية التي تريد تصديرها.
   b. انقر على الزر ← **Export**.
   c. في النافذة التي تفتح، حدد اسم ملف JSON الذي تريد تصدير عوامل تصفية الأحداث إليه وحدد المجلد الذي تريد حفظ هذا الملف به.
   d. احفظ الملف.
   يقوم Kaspersky Endpoint Security بتصدير عوامل تصفية الأحداث إلى ملف JSON.
7. لاستيراد عوامل تصفية الأحداث:
   a. انقر على الزر ← **Import**.
   b. في النافذة التي تفتح، حدد ملف JSON الذي ترغب في استيراد عوامل تصفية الأحداث منه.
   c. افتح الملف.
   في حالة وجود قواعد تصفية الأحداث بالفعل على جهاز الكمبيوتر، يقوم Kaspersky Endpoint Security باستبدالها عند الاستيراد.
8. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

يمكنك أيضًا تصدير أو استيراد عوامل تصفية الأحداث في سطر الأوامر.

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).

     لا تدعم الأداة المساعدة kavremover إدارة KSWS.

   - 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.

مكون Kaspersky Security for Windows Server	مكون Kaspersky Endpoint Security for Windows
Basic functionality	نواة التطبيق
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 النظام
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 التطبيق
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 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 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 قواعد البيانات والوحدات النمطية للتطبيق 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. يجب تكوين الاستثناءات كمناطق محددة مسبقًا في إعدادات مهمة فحص البرامج الضارة. يجب إضافة الاستثناءات كعناوين ويب نصية إلى عناوين الويب الموثوقة للحماية من تهديدات الويب.
Apply also to subfolders (Exclusions)	**تضمين المجلدات الفرعية** (استثناءات الفحص)
Objects to detect (Exclusions)	**نوع الكائن المكتَشف** (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)

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Trusted process (Trusted process)	**التطبيقات الموثوقة** تختلف طرق اختبار 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 تجزئة ملف، 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:** • **الحد الأقصى من الحماية**. • **مستحسن**. تتوافق مستويات أمان KSWS مع أوضاع فحص KES على النحو التالي: • Maximum protection – الحد الأقصى من الحماية • Recommended – مستحسن • Maximum performance – مستحسن

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 Server	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.14.2\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%.

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
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.14.2\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 لمدة 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.

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
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 خادم الإدارة كخادم وكيل لشبكة 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.

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
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	**العنوان** (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)	**تكوين العناوين الموثوقة** (القسم الفرعي **إعدادات الشبكة**)
Exclude processes (Interception area)	**تكوين 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**. • **إعلام**.
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)

فئات Kaspersky Security for Windows Server	فئات Kaspersky Endpoint Security for Windows
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 والموضوعات العسكرية
For children	(عدم الترحيل)
Discrimination	العنف، التعصب
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، التعصب
Discontent	(عدم الترحيل)
Illegal drugs	الكحول والتبغ والمخدرات
Hate and discrimination	العنف، التعصب
Obscene vocabulary	الألفاظ النابية والفحش
Lingerie	محتوى البالغين
News	وسائل الإعلام

فئات Kaspersky Security for Windows Server	فئات Kaspersky Endpoint Security for Windows
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 والموضوعات العسكرية
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، التعصب
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، التعصب
E-commerce	المتاجر على الإنترنت

فئات Kaspersky Security for Windows Server	فئات Kaspersky Endpoint Security for Windows
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 تشغيل 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	**مراقبة 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 باسم **برامج أخرى\التطبيقات، الموثوقة وفقًا للسمعة في شبكة KSN** كشرط لبدء تشغيل القاعدة.
Users and / or user groups allowed to run applications trusted by KSN	يسمح خيار **المستخدمون وحقوقهم** في التحكم في التطبيقات بالقاعدة التي تتضمن فئة KL category**برامج 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	يعمل التحكم في توزيع البرامج في KSWS وKES بشكل مختلف. وأثناء الترحيل، يضيف KES قواعد السماح الجديدة للتطبيقات التي يُسمح عليها بالتوزيع التلقائي للبرامج (**Software distribution applications and packages allowed**). ويتم تحديد تجزئة الملف كشرط لبدء تشغيل القاعدة. وفي خصائص الحساب يتم تحديد خانة الاختيار **برامج التحديث الموثوقة**.

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
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. وفي خصائص الحساب يتم تحديد خانة الاختيار **برامج التحديث الموثوقة**.
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**: • **إعلام**. • **منع**.
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 النظام**.

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** ← **الملف** (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	**المستخدمون و/أو مجموعات المستخدمين الموثوقة**
File operation markers	**علامات عملية الملف**

إعدادات KSWS	إعدادات KES
Calculate checksum for the file if possible	**التجزئة**
Exclusions	**الاستثناءات ← الملف**

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.14.2\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.
SIEM Integration	(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	**عزل الملفات**
Backed up files	**ملفات النسخ الاحتياطي**
Blocked hosts	(عدم الترحيل) يرسل Kaspersky Endpoint Security تلقائيًا بيانات حول المضيفين الممنوعين.

Tasks

Activating 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 قواعد البيانات والوحدات النمطية للتطبيق (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

يتم ترحيل إعدادات مهمة Baseline File Integrity Monitor (KSWS) إلى مهمة التحقق من سلامة النظام وإلى قسم السياسة **ضوابط الأمان**، القسم الفرعي **مراقبة سلامة النظام**.

إعدادات مهمة مراقبة سلامة الملفات الأساسية

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
Hash calculation algorithm: • MD5 • SHA256.	(عدم الترحيل) يستخدم Kaspersky Endpoint Security خوارزمية SHA256 لحساب المجموع الاختباري.
Scan scope	**نطاق المراقبة** (القسم الفرعي **مراقبة سلامة النظام**)

Database Update

يتم ترحيل إعدادات مهمة Database Update (KSWS) إلى مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق (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.

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
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 قواعد البيانات والوحدات النمطية للتطبيق (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). الجديد تراجع عن التحديث مهمة (KES) لها جدول بدء مهمة - Manually.

On-Demand Scan

يتم ترحيل إعدادات مهمة On-Demand Scan (KSWS) إلى مهمة فحص البرامج الضارة (KES).

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 ملفات تنسيق البريد الإلكتروني**. • **فحص الملفات بتنسيقات Microsoft Office**.
Action to perform on infected and other objects: • Disinfect • Disinfect. Remove if disinfection fails • Remove • Perform recommended action • Notify only	**الإجراء المطلوب اتخاذه عند اكتشاف تهديد**: • **تنظيف؛ حذف إذا فشل التنظيف**. • **تنظيف؛ إبلاغ إذا فشل التنظيف**. • **إعلام**.
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 Check

يتم ترحيل إعدادات مهمة Application Integrity Control (KSWS) إلى مهمة التحقق من سلامة التطبيق (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 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 **All tasks ← Policies and tasks batch conversion wizard**.

   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

قم بإنهاء 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 **Managed devices** 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 **Policies**.
4. انقر فوق **New policy**.

   بدء تشغيل معالج السياسة.
5. اتبع تعليمات "معالج السياسات".

الخطوة 1. تحديد التطبيق لإنشاء سياسة المجموعة

حدد تطبيق **Kaspersky Endpoint Security for Windows (14.2)**.

الخطوة 2. تسمية سياسة المجموعة

أدخل اسمًا لسياسة المجموعة، على سبيل المثال، السياسة الخاصة بالمكتب.

حدد خانة الاختيار **Use policy settings for an earlier version of the application**. انقر فوق **Browse** وحدد سياسة KSWS.

الخطوة 3. المشاركة في شبكة Kaspersky Security Network

يرجى قراءة شروط بيان Kaspersky Security Network (KSN) والموافقة عليها.

الخطوة 4. تحديد وضع استخدام التطبيق على أجهزة الكمبيوتر

حدد **الوضع القياسي لحماية المضيفين**. يوفر Kaspersky Endpoint Security سياسة مشتركة لجميع أوضاع التطبيقات وأنواع أنظمة التشغيل.

نوصي باستخدام سياسات مختلفة للأوضاع وأنواع أنظمة التشغيل المختلفة.

الخطوة 5. استيراد الإعدادات

تتوفر هذه الخطوة إذا حددت تكوين السياسة اليدوي في الخطوة 4.

يمكنك إنشاء سياسة بناءً على إعدادات Kaspersky Endpoint Security من ملف تكوين CFG. لا يدعم معالج السياسة الجديد ملفات التكوين المشفرة. وعند تصدير ملف التكوين، تخط خطوة تشفير الملف.

عند استيراد ملف تكوين CFG لتطبيق، لا تتوفر جميع إعدادات السياسة للمعالج. على سبيل المثال، ملفات تعريف السياسة مفقودة من إعدادات التطبيق. وإذا كنت ترغب في نقل جميع الإعدادات وملفات التعريف إلى السياسة، فيمكنك استيراد سياسة أخرى من ملف KLP.

عند استيراد ملف تكوين، لا ينقل Kaspersky Endpoint Security كلمات مرور حاوية التشفير. وإذا كنت تستخدم المصادقة ثنائية الاتجاه عند الاتصال بالخوادم، فستحتاج إلى تحديد كلمات مرور حاوية التشفير من البداية.

الخطوة 6 - 10. تكوين إعدادات السياسة

تتوفر هذه الخطوة إذا حددت تكوين السياسة اليدوي في الخطوة 4.

اتبع الخطوات لإدارة إعدادات السياسة.

الخطوة 11. تكوين المنطقة الموثوقة

تكوين المنطقة الموثوقة. يمكنك إضافة استثناءات الفحص محددة مسبقًا وتطبيقات موثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم. ويمكن أن تساعدك أيضًا استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في وضع Light Agent في البيئات الافتراضية في Citrix وVMware.

الخطوة 12. تحديد حالة السياسة

- **Active**. بعد إجراء المزامنة التالية، سيتم استخدام السياسة باعتبارها السياسة النشطة على جهاز الكمبيوتر.

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.

- **Inactive**. سياسة النسخ الاحتياطي. إذا لزم الأمر يمكن تحويل حالة السياسة من غير نشطة إلى نشطة.

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.

- **Out-of-office**. يتم تفعيل السياسة عندما يترك جهاز الكمبيوتر شبكة المؤسسة المحيطة.

قم بإنهاء المعالج.

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`.

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم.

- 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 (Industrial CyberSecurity)** 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 قواعد البيانات والوحدات النمطية للتطبيق. تأكد أن إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تم ترحيلها بشكل صحيح. وبدلاً من مهام KSWS الثلاث، تستخدم KES مهمة KES واحدة. ويمكنك تحسين مهام تحديث قواعد البيانات والوحدات النمطية للتطبيق 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.

ترحيل المنطقة الموثوقة في KSWS

تُعد المنطقة الموثوقة بمثابة قائمة يتم تكوينها بواسطة مسؤول النظام تضم كائنات وتطبيقات لا يقوم Kaspersky Endpoint Security بمراقبتها عندما يكون نشطًا. ويمكنك ترحيل كائنات المنطقة الموثوقة من KSWS إلى KES باستخدام معالج تحويل مجموعة السياسات والمهام أو معالج إنشاء سياسة KES جديدة بناءً على سياسة KSWS. يحتوي KSWS وKES على مجموعات مختلفة من المكونات والميزات، لذا بعد الترحيل، يجب عليك التحقق من أن الاستثناءات تفي بمتطلبات الأمان الخاصة بشركتك. وتختلف أيضًا طرق إضافة الاستثناءات إلى المنطقة الموثوقة بين KES وKSWS. ولا يحتوي معالج الترحيل على أدوات لترحيل جميع استثناءات KSWS. ويعني هذا أنه بعد الترحيل، يجب عليك إضافة بعض استثناءات KSWS 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`.

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم.

طرق إنشاء المنطقة الموثوقة في KES وKSWS.

KSWS		KES
Object to scan		
• Predefined scope	(عدم الترحيل)	
• Disk, folder or network location	←	**الملف أو المجلد**
• File	←	**الملف أو المجلد**
• Script file or web address	(عدم الترحيل)	
Detected object	←	**نوع الكائن المكتَشف**
Trusted processes	←	**التطبيقات الموثوقة**

ترحيل الكائنات التي تم فحصها

يتم ترحيل استثناءات KSWS التي تم تحديد طريقة **Object to scan** لها في خصائصها إلى استثناءات KES التي تم تحديد طريقة **الملف أو المجلد** لها في خصائصها مع بعض القيود. ويعتمد ترحيل الاستثناء على طريقة تحديد الكائن:

- Predefined scope – عدم الترحيل.

  وبعد الترحيل، يجب إضافة هذه الاستثناءات يدويًا. يجب تكوين الاستثناءات كمناطق محددة مسبقًا في إعدادات مهمة فحص البرامج الضارة.

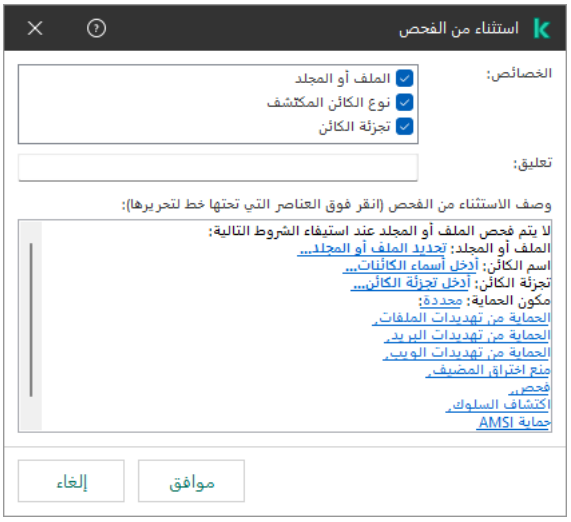
- Disk, folder or network location – الترحيل إلى استثناءات KES التي تم تحديد طريقة "ملف أو مجلد" لها في الخصائص.

- File – الترحيل إلى استثناءات KES التي تم تحديد طريقة "ملف أو مجلد" لها في الخصائص.

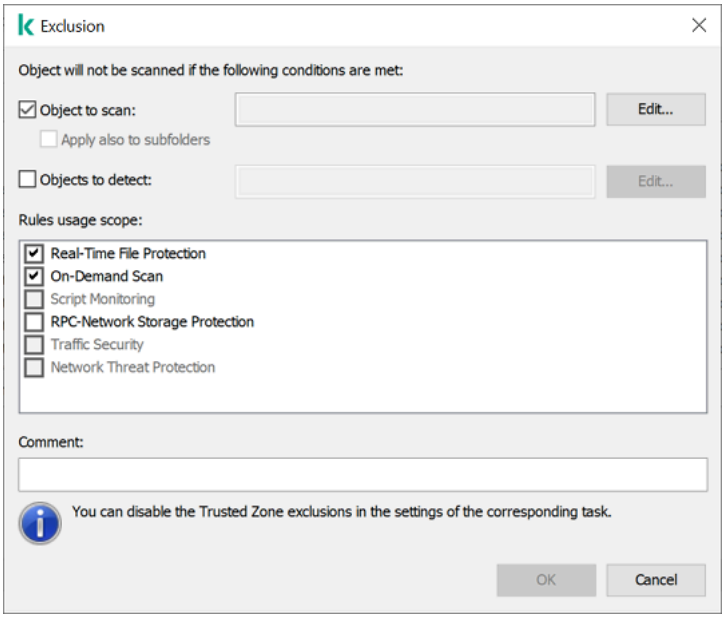
- Script file or web address – عدم الترحيل.

  وبعد الترحيل، يجب إضافة هذه الاستثناءات يدويًا. يجب إضافة الاستثناءات كعناوين ويب نصية إلى عناوين الويب الموثوقة للحماية من تهديدات الويب.

في خالة تحديد خانة الاختيار **Apply also to subfolders** للكائن الذي تم فحصه، يتم ترحيل هذا الإعداد إلى استثناءات KES (خانة الاختيار **تضمين المجلدات الفرعية**).



إعدادات استثناء KES



إعدادات استثناء KSWS

ترحيل الكائنات المكتشفة

يتم ترحيل استثناءات KSWS التي تم تحديد طريقة **Detected object** لها في خصائصها إلى استثناءات KES التي تم تحديد طريقة **نوع الكائن المكتَشف** لها في خصائصها. يتوافق اسم الكائن المكتشف مع تصنيف موسوعة Kaspersky (على سبيل المثال، `Email-Worm` أو `Rootkit` أو `RemoteAdmin`). يدعم Kaspersky Endpoint Security الأقنعة التي تحمل علامة الاستفهام `?` (يطابق أي حرف واحد) وعلامة النجمة `*` (يطابق أي تسلسل من الأحرف).

ترحيل نطاق استخدام الاستثناء

نطاق استخدام الاستثناء هو مجموعة من المكونات التي ينطبق عليها الاستثناء. يتضمن KES وKSWS مجموعات مختلفة من المكونات، لذا لا يستطيع معالج الترحيل ترحيل نطاق استخدام الاستثناء. لذلك، في حالة تحديد مكون واحد على الأقل في KSWS، فإن KES يطبق الاستثناء على جميع مكونات التطبيق.

يمكنك تكوين نطاق استخدام KSWS في إعدادات المنطقة الموثوقة وأيضًا في إعدادات مكونات حماية KSWS. ولفعل ذلك، يمكنك تحديد أو مسح خانة الاختيار **Apply Trusted Zone** في القسم المقابل من السياسة. ولا تتضمن إعدادات مكونات حماية KES خانة الاختيار هذه. ويعني هذا فقدان حالة المنطقة الموثوقة في إعدادات المكونات الفردية عند الترحيل. وبعد إكمال الترحيل، حدد المكونات التي ينطبق عليها الاستثناء في إعدادات المنطقة الموثوقة في سياسة KES.

تعليقات الترحيل

يتم ترحيل التعليقات من منطقة KSWS الموثوقة إلى تعليقات استثناء KES دون تعديل.

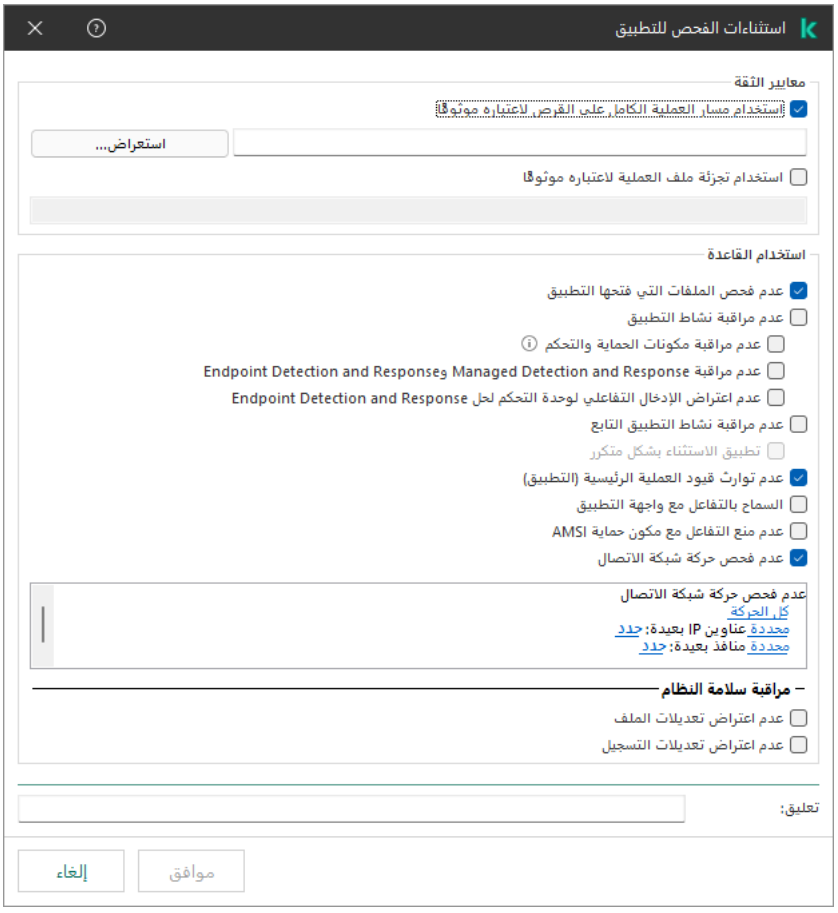
ترحيل العمليات الموثوقة

يتم ترحيل عمليات KSWS الموثوقة إلى عمليات KES الموثوقة مع بعض القيود. ويعتمد ترحيل العمليات الموثوقة على طريقة اختيار الكائن:

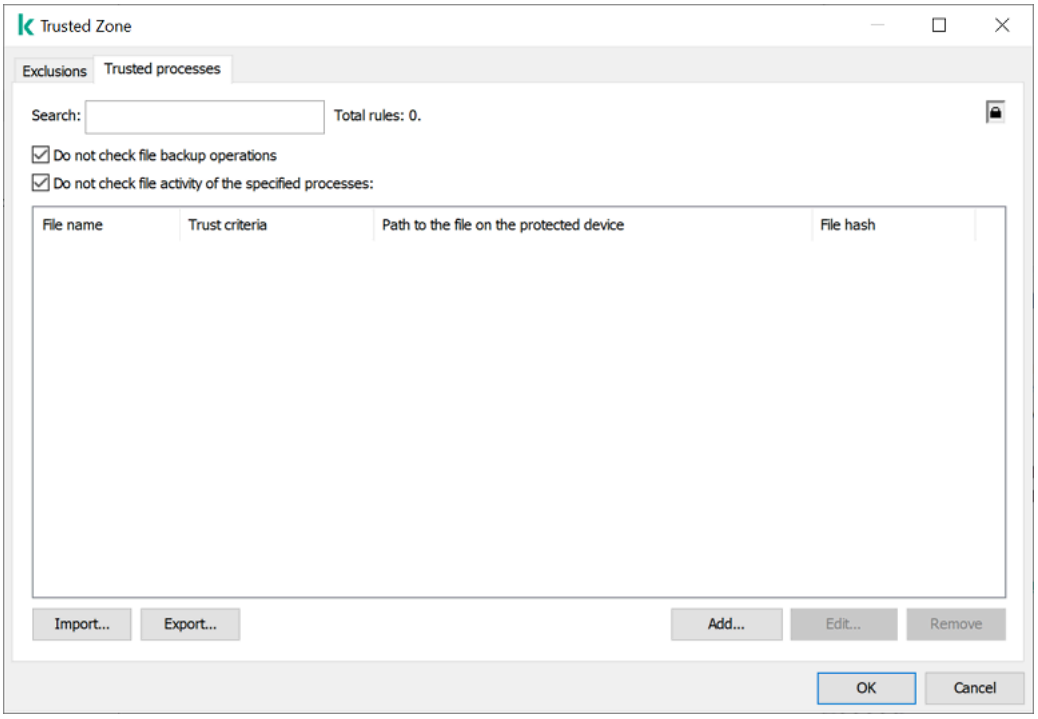
- Path to the file on the protected device – الترحيل إلى تطبيقات KES الموثوقة.
- File hash – عدم الترحيل.

وإذا كان KSWS يتضمن عمليات موثوقة تم تكوينها كملف تجزئة ملف، فلن يتم ترحيل هذه العمليات الموثوقة. وبعد الترحيل، يجب إضافة هذه العمليات الموثوقة يدويًا.

في حالة تحديد خانة الاختيار **Do not check file backup operations** في إعدادات العملية الموثوقة، يتم ترحيل هذا الإعداد إلى تطبيقات KES الموثوقة (خانة الاختيار **عدم مراقبة نشاط التطبيق**).



إعدادات التطبيق الموثوقة في KES



إعدادات العملية الموثوقة في KSWS

ترحيل قواعد التحكم في تشغيل تطبيقات KSWS

يتم حظر التحكم في تشغيل تطبيقات KSWS بشكل افتراضي. بمعنى أن التحكم في تشغيل التطبيقات يحظر تلقائيًا جميع التطبيقات غير المحددة في القواعد كتطبيقات مسموح بها. لذلك يضبط معالج الترحيل الخاص بالتحكم في تطبيق KES تلقائيًا وضع التحكم **قائمة السماح**، الذي يتوافق مع مبدأ محظور بشكل افتراضي.

يمكنك ترحيل قواعد من KSWS إلى KES باستخدام معالج تحويل مجموعة السياسات والمهام أو معالج إنشاء سياسة KES جديدة بناءً على سياسة KSWS.

ترحيل وضع التحكم في تشغيل التطبيقات

ينتقل وضع التحكم في تشغيل تطبيقات KSWS إلى التحكم في تطبيق KES على النحو التالي:

- **Statistics only** ← **اختبار القواعد**؛
- **Active** ← **تطبيق القواعد**.

ترحيل القواعد المحددة مسبقًا للتحكم في تشغيل تطبيقات KSWS

وبشكل افتراضي، يتضمن التحكم في تشغيل تطبيقات KSWS قاعدتين:

- **Allow scripts and MSI by OS-trusted certificate**
- **Allow executable by OS-trusted certificate**

تسمح القواعد المحددة مسبقًا بتشغيل البرامج النصية وحزم MSI والملفات القابلة للتنفيذ الموقعة بشهادة جذر موثوق بها. وإذا كان هناك على الأقل قاعدة KSWS محددة مسبقًا تتضمن نوع **Allow**، ينشئ معالج الترحيل 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.

إذا كانت كل من قواعد KSWS المحددة مسبقًا تتضمن نوع **Deny**، يتجاهل KES القواعد المحددة مسبقًا.

ترحيل القواعد المخصصة للتحكم في تشغيل تطبيقات KSWS

تنظيم قواعد التحكم في تشغيل تطبيقات KSWS عملية تنفيذ الملفات وفقًا للمعايير التالية:

- التوقيع بشهادة رقمية؛
- تجزئة SHA256؛
- مسار الملف.

يتم إنشاء القواعد بشكل مختلف في KSWS و KES، وبالتالي ينشئ معالج الترحيل فئات التطبيق، التي تتضمن الشروط والاستثناءات من قواعد KSWS، ويضيف فئات التطبيق هذه إلى قواعد KES. يستخدم المعالج شروط **الشهادة** و**مسار المجلد** و**رمز تجزئة الملف** في فئات التطبيق. وتتوفر فئات التطبيق الجديدة في وحدة تحكم الإدارة في Kaspersky Security Center في قسم **Application categories** ← **Application management**.

يجمع معالج الترحيل قواعد KSWS حسب النوع والمستخدم. وبعد ذلك، ينشئ المعالج فئات تطبيق تتضمن شروطًا واستثناءات من قواعد KSWS، ويضيف فئات التطبيق إلى قواعد KES الجديدة. ويحدد المعالج أسماء قواعد KSWS في الحقل **الوصف** لقواعد KES.

ترحيل الإعدادات المتقدمة للتحكم في تشغيل تطبيقات KSWS

يختلف مبدأ تشغيل التحكم في تشغيل تطبيقات KSWS والتحكم في تطبيق KES، لذا قد يقوم معالج الترحيل بترحيل مجموعة فرعية من الإعدادات.

إعدادات التحكم في تشغيل التطبيقات

إعدادات Kaspersky Security for Windows Server	إعدادات Kaspersky Endpoint Security for Windows
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.
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	**مراقبة 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 باسم **برامج أخرى\التطبيقات، الموثوقة وفقًا للسمعة في شبكة KSN** كشرط لبدء تشغيل القاعدة.
Users and / or user groups allowed to run applications trusted by KSN	يسمح خيار **المستخدمون وحقوقهم** في التحكم في التطبيقات بالقاعدة التي تتضمن فئة KL category**برامج 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	يعمل التحكم في توزيع البرامج في KSWS وKES بشكل مختلف. وأثناء الترحيل، يضيف KES قواعد السماح الجديدة للتطبيقات التي يُسمح عليها بالتوزيع التلقائي للبرامج (**Software distribution applications and packages allowed**). ويتم تحديد تجزئة الملف كشرط لبدء تشغيل القاعدة. وفي خصائص الحساب يتم تحديد خانة الاختيار **برامج التحديث الموثوقة**.
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. وفي خصائص الحساب يتم تحديد خانة الاختيار **برامج التحديث الموثوقة**.
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.

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 Uninstall application remotely 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.

إذا تم تمكين الحماية بكلمة مرور لتقييد الوصول إلى KSWS ، فأدخل كلمة مرور إلغاء التثبيت في الإعدادات الخاصة بحزمة تثبيت KES.

بعد إزالة KSWS، قم بتثبيت Kaspersky Endpoint Security for Windows باستخدام أي طريقة متاحة.

تثبيت Kaspersky Endpoint Security

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 وKUMA 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 وKUMA وMDR في العمل مع العامل المُضمن لتطبيق Kaspersky Endpoint Security. بالإضافة إلى ذلك، ستتم 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.

يقوم المسؤولون عادةً بتمكين الحماية بكلمة مرور لتقييد الوصول إلى KSWS وKEA. بدءًا من Kaspersky Security Center Linux 15.1، يمكنك إدخال كلمة مرور لإلغاء تثبيت التطبيق في إعدادات مهمة Install application remotely. وتسمح المهمة بإدخال كلمة مرور واحدة فقط لإلغاء التثبيت. أي إذا تم تعيين كلمة المرور نفسها لتطبيقي KSWS وKEA، تتم إزالة تطبيقي KSWS وKEA بنجاح. وإذا كانت كلمات المرور مختلفة، تفشل إزالة أحد التطبيقات بسبب خطأ في الوصول. ولإكمال الترحيل، يجب عليك تعطيل الحماية بكلمة مرور للتطبيق الذي لم تتمكن من إدخال كلمة المرور الخاصة به في إعدادات مهمة Install application remotely.

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 UpgradedFromKSWS <اسم سياسة 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 في 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 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 الوظيفة الإضافية لحل Kaspersky Endpoint Detection and Response Optimum مستقلاً لتفعيل وظيفة EDR Optimum، فيجب عليك التأكد من إضافة مفتاح الوظيفة الإضافية لحل 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 and 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 الإصدار 13.2 أو أحدث من عميل الشبكة على الكمبيوتر.
- تحقق من حالة تشغيل العميل المدمج عن طريق عرض Report on status of application components. 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 Report on status of application components. 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:

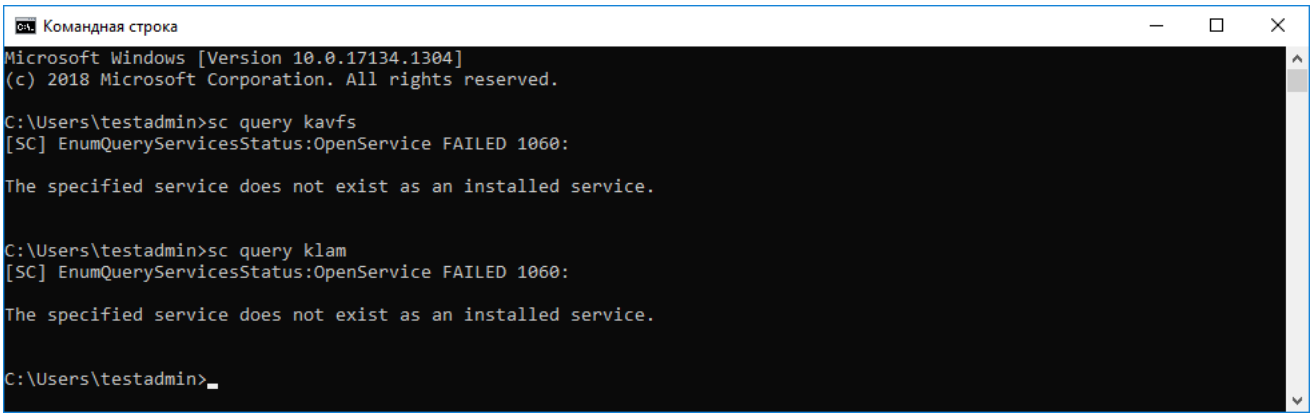
- المجلد `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` غير موجود.
- تكون الخدمات التالية غير موجودة:
  - Kaspersky Security Service (KAVFS)
  - خدمة Kaspersky Security Management (KAVFSGT)
  - خدمة Kaspersky Security Exploit Prevention (KAVFSSLP)
  - خدمة Kaspersky Security Script 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.

طريقة تفعيل Kaspersky Security for Windows Server	ترحيل المفتاح إلى 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.

إدارة التطبيق على خادم في وضع Server Core

لا يحتوي خادم في وضع Server Core 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 في وضع Server Core، لا تتوفر مكونات التطبيق التالية: الحماية من تهديدات الويب، والحماية من تهديدات البريد، والتحكم في الويب، ومنع هجمات BadUSB، 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 في وضع Server Core عن إدارة الكمبيوتر. ويمكنك استخدام السياسات والمهام لتكوين التطبيق.

تتضمن إدارة التطبيق على خادم في وضع Server Core الاعتبارات الخاصة التالية:

- لا يحتوي خادم في وضع Server Core 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 في وضع Server Core، 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
```

الترحيل من [KSWS+KEA] إلى [KES+العميل المدمج]

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 SQL_Policy(1) و SQL_Policy(2) 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 Install application remotely 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 Report on status of application components.

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.

وضع Light Agent لحماية الأجهزة الافتراضية

بدءًا من الإصدار 12.8، يمكنك استخدام Kaspersky Endpoint Security for Windows كجزء من Kaspersky Security for Virtualization Light Agent. Kaspersky Security for Virtualization Light Agent هو حل متكامل يوفر حماية شاملة للأجهزة الافتراضية ضد أنواع مختلفة من تهديدات أمان المعلومات وهجمات شبكة الاتصال وهجمات التصيد الاحتيالي. ولاستخدام هذا الحل، يجب تثبيت التطبيق في وضع Light Agent.

لا يتم دعم تثبيت Kaspersky Endpoint Security في وضع Light Agent على الأجهزة الافتراضية القائمة على Arm.

يمكنك استخدام Kaspersky Endpoint Security في Light Agent كجزء من Kaspersky Security for Virtualization Light Agent بدءًا من الإصدار 6.2.

عند بدء تشغيل Light Agent، فإنه ينشئ ويحافظ على اتصال بجهاز SVM الافتراضي (Secure Virtual Machine). ويتم نشر خادم حماية على SVM. وخادم الحماية هو مكون في حل Kaspersky Security for Virtualization Light Agent يفحص الملفات للبحث عن الفيروسات والبرامج الضارة الأخرى، ويقوم بتحديث قواعد بيانات مكافحة الفيروسات وإدارة مفاتيح الترخيص. ويرسل Light Agent الملفات أو أجزاءها التي تحتاج إلى الفحص إلى SVM. وتتوفر نتائج الفحص لجميع الأجهزة الافتراضية التي تم تثبيت Light Agent عليها (تقنية SharedCache). وتُزيد هذه التقنية كفاءة الحل وتوفر استجابة أسرع للتهديدات.

قد تحتوي البنية التحتية للمؤسسة على العديد من الأجهزة الافتراضية المُثبت عليها Light Agent والعديد من أجهزة SVM. يعالج خادم التكامل التفاعل بين الأجهزة الافتراضية وأجهزة SVM. خادم التكامل هو أحد مكونات حل Kaspersky Security for Virtualization Light Agent الذي ينشئ قائمة من أجهزة SVM المتاحة وينقل هذه البيانات إلى أجهزة Light Agent، ويشارك في اكتشاف أجهزة SVM بواسطة أجهزة Light Agent، ويحمي الاتصال بين أجهزة Light Agent وSVM، ويؤدي وظائف أخرى.

اعتبارات خاصة لوضع Light Agent

يمكنك إدارة Kaspersky Endpoint Security في الوضع القياسي ووضع Light Agent باستخدام سياسات ومهام Kaspersky Endpoint Security. وفي وضع Light Agent، لا تتوفر بعض مكونات وميزات التطبيق.

تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق

يستخدم Kaspersky Endpoint Security في وضع Light Agent قواعد بيانات البرامج الضارة الخاصة التي يحتاجها التطبيق عند العمل كجزء من حل Kaspersky Security for Virtualization Light Agent . ويحصل Kaspersky Endpoint Security على تحديثات قواعد البيانات والوحدة النمطية للتطبيق من خادم الحماية.

يتم تحديث قواعد البيانات والوحدات النمطية على الأجهزة الافتراضية المحمية باستخدام مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق خاصة، حيث يتم تحديد مجلد على SVM كمصدر للتحديث. يقوم Light Agent بتشغيل مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق تلقائيًا. ولا يمكنك تحديد مصدر تحديث مختلف أو تكوين جدول المهام أو إزالة المهمة.

يتم أيضًا التعامل مع التراجع عن آخر تحديث لقاعدة بيانات البرامج الضارة من جانب خادم الحماية. وبعد التراجع عن تحديث قواعد البيانات والوحدات النمطية للتطبيق على SVM، تبدأ مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق المحلية الخاصة على الجهاز الافتراضي المحمي. وتؤدي هذه المهمة إلى عودة Light Agent إلى استخدام المجموعة السابقة من قواعد بيانات البرامج الضارة.

لا يدعم Kaspersky Endpoint Security في وضع Light Agent مهمة تراجع عن التحديث.

تفعيل Light Agent

لتفعيل التطبيق، يجب عليك إضافة مفتاح ترخيص إلى SVM الذي يتصل به Light Agent. وليست هناك حاجة لتفعيل التطبيق بشكل منفصل.

اعتبارات خاصة أخرى لوضع Light Agent

- عند إنشاء سياسة للتطبيق، نوصي بتحديد وضع Light Agent. وفي هذا الوضع، يطالبك معالج السياسة الجديدة بتكوين اتصال SVM. وتكون هذه الإعدادات مطلوبة لكي يعمل التطبيق في وضع Light Agent.
- لا يمكنك تثبيت مكونات "تشفير البيانات" و"مراقبة عيوب التكيف" في وضع Light Agent. وتعتمد مجموعة المكونات أيضًا على نوع نظام تشغيل الضيف: محطة عمل أو خادم.
- لا يدعم Light Agent التكامل مع حلي Kaspersky Endpoint Detection and Response Expert وKaspersky Endpoint Detection and Response Expert (cloud).
- يمكنك إدارة Light Agent في وحدة تحكم الإدارة (MMC) وKaspersky Security Center Web Console. ولا يمكن إدارة Light Agent في Kaspersky Security Center Cloud Console.
- لا يتم دعم تغيير مجموعة مكونات التطبيق على أجهزة VDI الافتراضية.
- ويتصل Kaspersky Endpoint Security بخوادم KSN من خلال خادم وكيل KSN. الاتصال المباشر مع KSN غير مدعوم.
- لا يتم دعم الوضع السحابي في Kaspersky Security Network.
- لا يتم دعم استخدام الخادم الوكيل للتطبيق عند الاتصال بخادم التكامل (VIIS) وخادم الحماية (SVM) وخوادم KSN.

التكوين الأولي للجهاز الافتراضي

يمكنك تثبيت Kaspersky Endpoint Security على جهاز افتراضي يستخدم تقنية المنصة الافتراضية. ويدعم Kaspersky Endpoint Security منصات VMware وMicrosoft Hyper-V وCitrix الافتراضية. وقبل التثبيت، يجب عليك إجراء التكوين الأولي للأجهزة الافتراضية.

التوافق مع تقنية Citrix App Layering

إذا كنت تنوي استخدام Full User Layer لحفظ حالة الأجهزة الافتراضية المؤقتة، فيجب عليك تنفيذ ما يلي قبل التثبيت على قالب الجهاز الافتراضي:

1. أنشئ ملف C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt وأضف الاستثناءات التالية إليه:
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`
2. في سجل نظام التشغيل في مفتاح HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr، أنشئ قيمة DWORD جديدة باسم MiniFilterBypass واضبطها على 1.

3. في سجل نظام التشغيل في المفتاح HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd، أنشئ قيمة MULTI_SZ جديدة باسم ExcludeKey واضبطها على \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab.

4. أعد تشغيل الجهاز الافتراضي.

للتثبيت على الأجهزة الافتراضية في بنية تحتية تستخدم طبقات تطبيق Citrix ، يجب عليك فعل ما يلي:

1. قم بتثبيت Kaspersky Security Center Administration Agent وKaspersky Endpoint Security for Windows على قالب الجهاز الافتراضي في طبقة التطبيق.

2. أنشئ صورة جهاز افتراضي تتكون من طبقات متعددة.

3. انشر الصورة التي تم إنشاؤها على برامج Hypervisor التي تدعم حل Citrix App Layering.

4. قم بتكوين إنشاء أجهزة افتراضية مؤقتة من الصورة التي تم إنشاؤها.

للحصول على تفاصيل عن تثبيت برنامج مكافحة الفيروسات جنبًا إلى جنب مع Citrix App Layering، يرجى الرجوع إلى وثائق Citrix App Layering.

التوافق مع تقنية Citrix Provisioning (Citrix Provisioning Services)

للتأكد من توافق التطبيق مع تقنية Citrix Provisioning (Citrix Provisioning Services):

- إذا تم تثبيت برنامج Citrix Provisioning Target Device على الجهاز الافتراضي، فيجب عليك إزالته قبل تثبيت تطبيق Kaspersky Endpoint Security (للحصول على التفاصيل، يرجى زيارة موقع ويب الدعم الفني لدى Citrix). وبعد تثبيت التطبيق، يجب عليك إعادة تثبيت Citrix Provisioning Target Device. وتحتاج أيضًا إلى إعادة تثبيت Citrix Provisioning Target Device عند استعادة التطبيق، بما في ذلك عند ترقية نظام التشغيل.

  تتضمن ترقية نظام التشغيل الخطوات التالية:

  1. حذف Citrix Provisioning Target Device.

  2. ترقية نظام التشغيل.

  3. بعد بدء تشغيل الجهاز الافتراضي، تأكد من تشغيل تطبيق Kaspersky Endpoint Security وعمله بشكل صحيح.

  4. إعادة تثبيت Citrix Provisioning Target Device.

- عند تثبيت التطبيق باستخدام معالج الإعداد أو عن بُعد باستخدام Kaspersky Security Center، يجب عليك تحديد خانة الاختيار **تأكيد التوافق مع Citrix PVS**.

التوافق مع تقنية Omnissa App Volumes

قبل تثبيت الأجهزة الافتراضية على القالب، يجب عليك إنشاء ملف %SVAgent%\Config\Custom\snapvol.cfg وإضافة الاستثناءات التالية إليه:

- `exclude_path=\ProgramData\Kaspersky Lab`
- `exclude_path=\ProgramData\KasperskyLab`
- `exclude_path=\Program Files\Kaspersky Lab`

- exclude_path=\Program Files\Common Files\Kaspersky Lab
- exclude_path=\Program Files\Kaspersky Lab
- exclude_path=\Program Files (x86)\Kaspersky Lab
- exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files (x86)\Kaspersky Lab
- exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files\Common Files\Kaspersky Lab
- exclude_process_path=\Program Files\Kaspersky Lab
- exclude_process_name=avp.exe
- exclude_process_name=klnagent.exe
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark
- exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon

للحصول على التفاصيل، يرجى الرجوع إلى وثائق Omnissa.

تثبيت Light Agent

لا يتم دعم تثبيت Kaspersky Endpoint Security في وضع Light Agent على الأجهزة الافتراضية القائمة على Arm.

تثبيت التطبيق في وضع Light Agent كما لو كان في الوضع القياسي. قبل تثبيت Light Agent على جهاز افتراضي، يجب التأكد من تثبيت Kaspersky Security Center Network Agent. ويسهل Network Agent التفاعل بين خادم الإدارة وجهاز افتراضي.

يمكن تثبيت Light Agent على جهاز افتراضي بإحدى الطرق التالية:

- عن بُعد باستخدام Kaspersky Security Center.
- محليًا، باستخدام معالج الإعداد.
- محليًا، باستخدام سطر الأوامر.

لتثبيت Light Agent، يجب عليك تحديد التكوين المناسب في إعدادات حزمة التثبيت أو في معالج الاعداد.

عند تثبيت Light Agent على خادم، يتم استبعاد مكونات الحماية المتقدمة (اكتشاف السلوك، ومنع الاستغلال، ومحرك المعالجة) من التكوين الافتراضي للتطبيق. وتوفر إعدادات التطبيق الافتراضية مستوى الحماية الموصى به والاستخدام الأمثل لموارد الخادم. عند تثبيت Light Agent على محطة عمل، يتم تضمين مكونات حماية متقدمة في التكوين الافتراضي للتطبيق.

عند تثبيت Light Agent، نوصي بتحديد الاستثناءات المحددة مسبقًا والتطبيقات الموثوقة للبيئة الافتراضية ذات الصلة. وتساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في إعداد التطبيق بسرعة وتجنب مشاكل توافق البيئة الافتراضية. ويمكنك أيضًا تكوين استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة بعد التثبيت، في السياسة.

كيفية تثبيت Light Agent باستخدام معالج الإعداد

1. انسخ مجلد حزمة التوزيع إلى جهاز افتراضي.
2. قم بتشغيل setup_kes.exe.

يبدأ معالج الإعداد.

تكوين Kaspersky Endpoint Security



اختيار تكوين التطبيق

حدد تكوين **Light Agent لحماية البيئات الافتراضية**. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. وفي هذا التكوين، لا يمكنك استخدام مكونات تشفير البيانات أو مراقبة عيوب التكيف. وإذا كنت تقوم بتثبيت Light Agent على قالب جهاز افتراضي سيتم استخدامه لإنشاء أجهزة افتراضية غير ثابتة، حدد خانة الاختيار **حماية البنية التحتية لسطح المكتب الافتراضي** (VDI يعني Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية.

مكونات برنامج Kaspersky Endpoint Security

حدد المكونات التي تريد تثبيتها (انظر الشكل أدناه). يمكنك تغيير مكونات التطبيقات المتاحة بعد تثبيت التطبيق. لفعل ذلك، سوف تحتاج إلى تشغيل معالج الإعداد مرة أخرى واختيار تغيير المكونات المتاحة.

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. يمكنك تمكين دعم Citrix Provisioning Services لتثبيت برنامج Kaspersky Endpoint Security إلى جهاز افتراضي.

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

كيفية تثبيت Light Agent باستخدام سطر الأوامر

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 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
```

أو

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
```

يمكّن الخيار `VDI` وضع حماية VDI (Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية. ويتم تمكين وضع حماية VDI افتراضيًا.

نتيجة لذلك، يتم تثبيت Light Agent على الجهاز الافتراضي مع مجموعة المكونات الافتراضية. ويمكنك تحرير مجموعة المكونات وتحديد الإعداد المتقدم باستخدام ملف setup.ini. ويمكنك أيضًا تحديد إعدادات التثبيت في سطر الأوامر.

كيفية تثبيت Light Agent باستخدام وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.

2. في شجرة وحدة التحكم، حدد **Remote installation** ← **Advanced** ← مجلد **Installation packages**.

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

3. افتح خصائص حزمة تثبيت Kaspersky Endpoint Security for Windows.

   اذا كان ضروريًا، أنشئ حزمة تثبيت جديدة.

4. انتقل إلى القسم **الإعدادات**.

5. حدد تكوين **Light Agent لحماية البيئات الافتراضية**. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. وفي هذا التكوين، لا يمكنك استخدام مكونات تشفير البيانات أو مراقبة عيوب التكيف. وإذا كنت تقوم بتثبيت Light Agent على قالب جهاز افتراضي سيتم استخدامه لإنشاء أجهزة افتراضية غير ثابتة، حدد خانة الاختيار **حماية البنية التحتية لسطح المكتب الافتراضي** (VDI يعني Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية.

6. حدد المكونات التي تريد تثبيتها.

   يمكنك تغيير مكونات التطبيقات المتاحة بعد تثبيت التطبيق.

7. تكوين المنطقة الموثوقة. حدد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة للبيئة الافتراضية التي تقوم بتثبيت التطبيق فيها.

   وتساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في إعداد التطبيق بسرعة وتجنب مشاكل توافق البيئة الافتراضية.

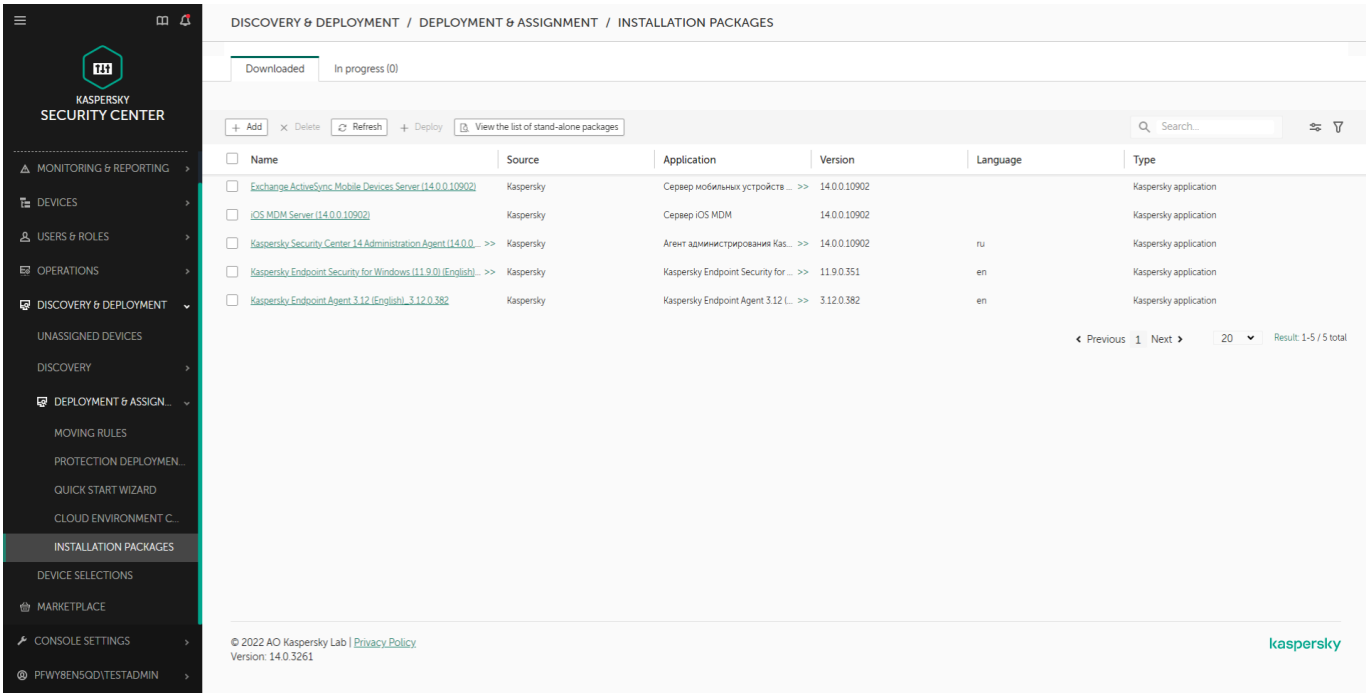
8. احفظ تغييراتك.

9. أنشئ مهمة التثبيت عن بعد. في خصائص المهمة، حدد حزمة التثبيت التي أنشأتها.

كيفية تثبيت Light Agent باستخدام Web Console

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

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



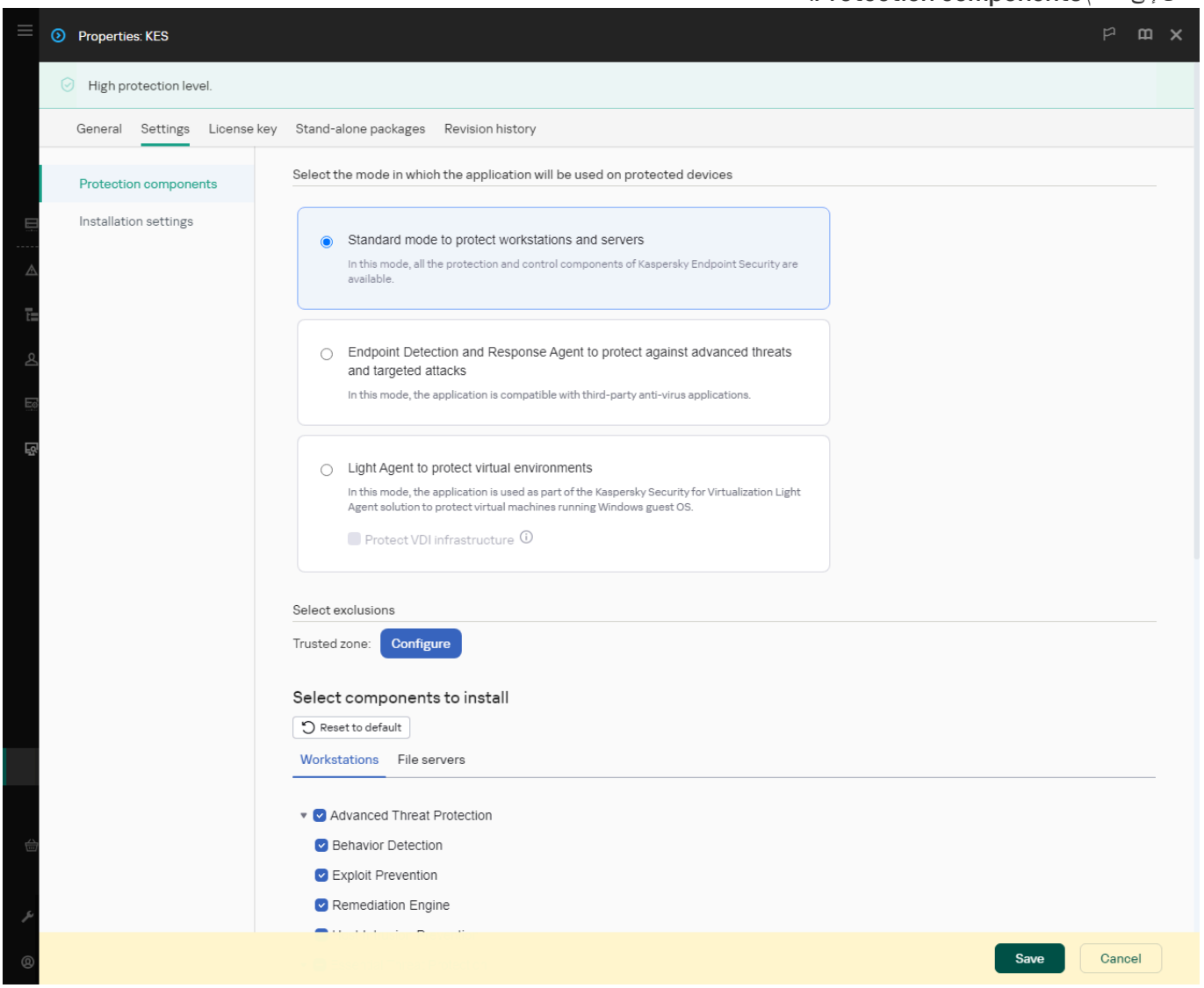
قائمة حزم التثبيت

2. افتح خصائص حزمة تثبيت Kaspersky Endpoint Security for Windows.

اذا كان ضروريًا، أنشئ حزمة تثبيت جديدة.

3. حدد علامة التبويب **Settings**.

4. انتقل إلى القسم **Protection components**.



المكونات المضمنة في حزمة التثبيت

5. حدد تكوين **Light Agent to protect virtual environments**. هذا التكوين مخصص للتطبيق الذي يتم استخدامه كجزء من حل Kaspersky Security for Virtualization Light Agent. ويجب تثبيت Light Agent على كل جهاز افتراضي يحتاج إلى الحماية باستخدام الحل. وفي هذا التكوين، لا يمكنك استخدام مكونات تشفير البيانات أو مراقبة عيوب التكيف. وإذا كنت تقوم بتثبيت Light Agent على قالب جهاز افتراضي سيتم استخدامه لإنشاء أجهزة افتراضية غير ثابتة، حدد خانة الاختيار **Protect VDI infrastructure** (VDI يعني Virtual Desktop Infrastructure). يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. وفي هذا الوضع، يرفض Light Agent تحديثات التطبيق التي تتطلب إعادة تشغيل الجهاز الافتراضي وعند تلقي تحديثات التطبيق التي تتطلب إعادة التشغيل، ينشئ Light Agent حدثًا حول الحاجة إلى تحديث قالب الأجهزة الافتراضية المحمية.

6. حدد المكونات التي تريد تثبيتها.

يمكنك تغيير مكونات التطبيقات المتاحة بعد تثبيت التطبيق.

7. تكوين المنطقة الموثوقة. حدد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة للبيئة الافتراضية التي تقوم بتثبيت التطبيق فيها.

وتساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في إعداد التطبيق بسرعة وتجنب مشاكل توافق البيئة الافتراضية.

8. احفظ تغييراتك.

9. أنشئ مهمة التثبيت عن بعد. في خصائص المهمة، حدد حزمة التثبيت التي أنشأتها.

نتيجة لذلك، يتم تثبيت Light Agent على جهاز افتراضي. ويمكنك استخدام واجهة التطبيق ويتم عرض أيقونة التطبيق في منطقة الإخطارات . أنت الآن بحاجة إلى تكوين اتصال Light Agent بجهاز SVM.



النافذة الرئيسية لوضع Light Agent

ربط Light Agent بجهاز SVM

يتطلب حل Kaspersky Security for Virtualization Light Agent اتصالاً مستمراً لوضع Light Agent وSVM. ويعد ذلك ضروريًا لفحص الملفات المرسلة بواسطة Light Agent للبحث عن الفيروسات والبرامج الضارة الأخرى. وبدون اتصال SVM، لا يمكن لوضع Light Agent إرسال ملفات للفحص، وإذا تعذر إنشاء الاتصال لأكثر من خمس دقائق، فسينتهي الفحص بوجود خطأ.

يتضمن توصيل Light Agent بجهاز SVM الخطوات التالية:

1. يحصل Light Agent على قائمة أجهزة SVM المتاحة.
2. يحدد Light Agent خادم الحماية (SVM) المتاح الذي يعتبر مثاليًا للاتصال وفقًا لخوارزمية اختيار SVM.
3. يتحقق Light Agent من إعدادات اتصال SVM الإضافية: العلامات وحالة حماية الاتصال ويغطي الترخيص وظائف التطبيق.
4. توصيل Light Agent بجهاز SVM.

يمكنك الحصول على معلومات عن حالة اتصال Light Agent بجهاز SVM في Kaspersky Endpoint Security أو باستخدام أمر التطبيق. وينشئ التطبيق حدثًا متى تم فقد اتصال SVM بوضع Light Agent أو تأسيسه، ويرسل هذه الأحداث إلى Kaspersky Security Center. وإذا كنت تستخدم خادم التكامل لاكتشاف SVM، فيمكنك الحصول على معلومات عن حالة SVM وعدد أوضاع Light Agent المتصلة في وحدة تحكم خادم التكامل. وللحصول على تفاصيل عن مراقبة حالة SVM، راجع تعليمات Kaspersky Security for Virtualization Light Agent.

اكتشاف SVM

يمكنك تحديد إحدى طرق اكتشاف SVM لوضع Light Agent:

- استخدام خادم التكامل (VIIS).

خادم التكامل هو مكون الحل الذي يتيح تفاعل Kaspersky Security for Virtualization Light Agent مع البنية التحتية الافتراضية وينشئ قائمة بأجهزة SVM المتاحة للاتصال. ويؤسس Light Agent اتصالاً بخادم التكامل ويحصل على قائمة بعناوين SVM.

يعد خادم التكامل مفيدًا للغاية في البنى التحتية الافتراضية الكبيرة لأنه يقوم تلقائيًا بموازنة التحميل بين SVMs، ويحصل على معلومات عن أجهزة SVM المتاحة، ويحلل هذه المعلومات، ويزود Light Agent بقائمة من خوادم الحماية (SVMs) المثالية للاتصال.

لكي يتمكن Light Agent من الحصول على قائمة من الأجهزة الافتراضية الخاصة، تحتاج فقط إلى إدخال عنوان خادم التكامل.

- استخدام مجموعة خوادم تكامل عالية التوافر.

يتوفر نشر استخدام مجموعة خوادم تكامل عالية التوافر. في Kaspersky Security for Virtualization Light Agent 6.4 بدءًا من الإصدار 6.4. توفر مجموعة خوادم التكامل عالية التوفر حماية دون انقطاع للبيئة الافتراضية بفضل تجاوز فشل أجهزة SVM وعملاء Light Agent إلى خادم تكامل احتياطي كلما تعطل خادم التكامل الأساسي. يتولى مكوّن خاص في المجموعة، وهو موازن التحميل، مسؤولية تجاوز فشل الخادم. وللحصول على تفاصيل عن مجموعة خوادم التكامل عالية التوافر، راجع تعليمات Kaspersky Security for Virtualization Light Agent.

لكي يحصل Light Agent على قائمة بأجهزة SVM، يتعين عليك إدخال عنوان الجهاز المثبت عليه موازن التحميل.

- استخدام قائمة عناوين SVM.

إذا كنت بحاجة إلى تحديد اجهزة افتراضية منفصلة فردية ترغب أن يتصل بها Light Agent، فيمكنك تحضير قائمة يدويًا.

تحتاج إلى سرد عناوين أجهزة SVM المتاحة التي يمكن لوضع Light Agent الاتصال بها.

كيفية تكوين اكتشاف SVM بواسطة Light Agent في وحدة تحكم الإدارة (MMC)

1. افتح Kaspersky Security Center Administration Console.
2. في شجرة وحدة التحكم، حدد **Policies**.
3. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
4. في نافذة السياسة، حدد **وضع Light Agent** ← **إعدادات اكتشاف SVM**.
5. حدد طريقة لاكتشاف SVM.
   - **خادم التكامل**. أدخل إعدادات الاتصال بخادم التكامل وفقًا للبنية التحتية الخاصة بك:
     - **خادم تكامل فردي**. أدخل إعدادات اتصال خادم التكامل: عنوان IPv4 أو اسم المجال المؤهل بالكامل (FQDN) الخاص بالجهاز.
     - **مجموعة خوادم تكامل عالية التوافر**. أدخل عنوان IP ومنفذ موازن التحميل الذي يعد جزءًا من المجموعة.
   - **استخدام قائمة مخصصة لعناوين جهاز متجهات الدعم (SVM)**. أنشئ قائمة بالأجهزة الافتراضية المنفصلة التي يمكن لوضع Light Agent الاتصال بها. وحدد عنوان IP بتنسيق IPv4 أو اسم المجال المؤهل بالكامل (FQDN) لجهاز SVM. يجب إدخال كل عنصر في القائمة في سطر جديد أو فصله عن العنصر السابق بحرف فاصلة منقوطة (;).

في قائمة عناوين SVM، حدد فقط أسماء مجالات كاملة (FQDN) مطابقة لعنوان IP واحد. وقد يؤدي استخدام اسم نطاق مؤهل بالكامل يتوافق مع عناوين IP متعددة إلى حدوث أخطاء في الحل.

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين اكتشاف SVM بواسطة Light Agent في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Asset management** ← **Policies**.

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

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

4. انتقل إلى **Light Agent Mode** ← **SVM discovery settings**.

5. حدد طريقة لاكتشاف SVM.

- **Use Integration Server**. أدخل إعدادات الاتصال بخادم التكامل وفقًا للبنية التحتية الخاصة بك:
  - **خادم تكامل فردي**. أدخل إعدادات اتصال خادم التكامل: عنوان IPv4 أو اسم المجال المؤهل بالكامل (FQDN) الخاص بالجهاز.
  - **مجموعة خوادم تكامل عالية التوافر**. أدخل عنوان IP ومنفذ موازن التحميل الذي يعد جزءًا من المجموعة.
- **Use a custom list of SVM addresses**. أنشئ قائمة بالأجهزة الافتراضية المنفصلة التي يمكن لوضع Light Agent الاتصال بها. وحدد عنوان IP بتنسيق IPv4 أو اسم المجال المؤهل بالكامل (FQDN) لجهاز SVM. يجب إدخال كل عنصر في القائمة في سطر جديد أو فصله عن العنصر السابق بحرف فاصلة منقوطة (;).

في قائمة عناوين SVM، حدد فقط أسماء مجالات كاملة (FQDN) مطابقة لعنوان IP واحد. وقد يؤدي استخدام اسم نطاق مؤهل بالكامل يتوافق مع عناوين IP متعددة إلى حدوث أخطاء في الحل.

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين اكتشاف SVM بواسطة Light Agent في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، تحت **وضع Light Agent** انقر فوق لوحة **إعدادات اكتشاف SVM**.

3. حدد طريقة لاكتشاف SVM.

- **استخدام خادم التكامل**. أدخل إعدادات الاتصال بخادم التكامل وفقًا للبنية التحتية الخاصة بك:
  - **خادم تكامل فردي**. أدخل إعدادات اتصال خادم التكامل: عنوان IPv4 أو اسم المجال المؤهل بالكامل (FQDN) الخاص بالجهاز.
  - **مجموعة خوادم تكامل عالية التوافر**. أدخل عنوان IP ومنفذ موازن التحميل الذي يعد جزءًا من المجموعة.
- **استخدام قائمة مخصصة لعناوين جهاز متجهات الدعم (SVM)**. أنشئ قائمة بالأجهزة الافتراضية المنفصلة التي يمكن لوضع Light Agent الاتصال بها. وحدد عنوان IP بتنسيق IPv4 أو اسم المجال المؤهل بالكامل (FQDN) لجهاز SVM. يجب إدخال كل عنصر في القائمة في سطر جديد أو فصله عن العنصر السابق بحرف فاصلة منقوطة (;).

في قائمة عناوين SVM، حدد فقط أسماء مجالات كاملة (FQDN) مطابقة لعنوان IP واحد. وقد يؤدي استخدام اسم نطاق مؤهل بالكامل يتوافق مع عناوين IP متعددة إلى حدوث أخطاء في الحل.

4. احفظ تغييراتك.

تكوين خوارزمية اختيار SVM لوضع Light Agent

قد تحتوي البنية التحتية للمؤسسة على العديد من أجهزة SVM التي تم نشرها التي يمكن لأوضاع Light Agent الاتصال بها. ولتحقيق التوازن في الحمل على الشبكة وموارد البنية التحتية الافتراضية، تحتاج إلى توزيع أوضاع Light Agent بين أجهزة SVM.

خوارزميات تحديد SVM

يمكن لعملاء Light Agent تطبيق خوارزميات تحديد خادم SVM التالية للاتصال: الخوارزمية القياسية (افتراضيًا) والخوارزمية الموسعة.

خوارزميات تحديد SVM

الخوارزمية القياسية	الخوارزمية الموسعة
في حالة استخدام هذه الخوارزمية، بعد التثبيت وبدء التشغيل، يختار Light Agent على الجهاز الافتراضي الاتصال بجهاز SVM محلي بالنسبة إلى Light Agent. إذا تعذر العثور على أجهزة SVM محلية مناسبة للاتصال، يحدد Light Agent جهاز SVM المتصل به أقل عدد من عملاء Light Agent، بغض النظر عن موضع جهاز SVM في البنية التحتية الافتراضية. لا يحدد التطبيق ما إذا كان جهاز SVM محليًا بالنسبة إلى Light Agent في حالة تمكين وضع حماية البنية التحتية الكبيرة لخادم الحماية على جهاز SVM. وفي هذه الحالة، يوصى باستخدام خوارزمية تحديد SVM الموسعة وتحديد خادم التكامل كطريقة اكتشاف SVM. يعتمد ما إذا كان جهاز SVM محليًا بالنسبة إلى Light Agent على نوع البنية التحتية الافتراضية.	إذا تم تطبيق هذه الخوارزمية، يمكنك تحديد إعدادات تحديد SVM التالية: • ما إذا كان يجب مراعاة أو تجاهل موقع جهاز SVM في البنية التحتية عند اختيار أجهزة SVM للاتصال بها • في حالة مراعاة موقع جهاز SVM، طَريقة تحديد محليّة جهاز SVM بالنسبة إلى Light Agent إذا تجاهل عملاء Light Agents موقع أجهزة SVM في البنية التحتية، فسيتمكن عملاء Light Agent من الاتصال بأي أجهزة SVM متاحة للاتصال. إذا كان يجب على عملاء Light Agent مراعاة موقع جهاز SVM في البنية التحتية، فستحتاج إلى تحديد نوع مسار SVM الذي سيتم وضعه في الاعتبار عند تحديد منطقة SVM ذات الصلة بعميل Light Agent. يعتمد ما إذا كان جهاز SVM محليًا بالنسبة إلى Light Agent على نوع البنية التحتية الافتراضية. إذا أخذ عملاء Light Agent في الاعتبار موقع أجهزة SVM في البنية التحتية عند اختيار جهاز SVM الذي تريد الاتصال به، فيمكن فقط لعملاء Light Agent الاتصال بأجهزة SVM المحلية. على سبيل المثال، إذا حددت مجموعة برنامج محاكاة افتراضية كنوع لمسار SVM، فستُعتبر جميع أجهزة SVM المنشورة على مجموعة برنامج المحاكاة الافتراضية هذه محليّة بالنسبة إلى Light Agent، ولن يتسنى لعميل Light Agent الاتصال إلا بأحد أجهزة SVM هذه. في حالة عدم توفر أجهزة SVM متاحة للاتصال ضمن المجموعة نفسها التي يعمل فيها Light Agent، فإن Light Agent لن يتصل بأي جهاز SVM. عند تحديد أجهزة SVM، يأخذ عملاء Light Agent أيضًا في الاعتبار عدد عملاء Light Agent المتصلين لضمان توزيع عملاء Light Agent بالتساوي بين أجهزة SVM المتاحة للاتصال بها. في حالة استخدام Light Agent لخوارزمية تحديد جهاز SVM الممتدة، وتعيين طريقة اكتشاف جهاز SVM على قائمة عناوين أجهزة SVM، وتمكين وضع حماية البنى التحتية الكبيرة على جهاز SVM، فإن اتصال Light Agent بجهاز SVM هذا لن يكون ممكنًا إلا إذا تم تجاهل مسار جهاز SVM.
Basis Dynamix Enterprise	
في بنية تحتية افتراضية تستند إلى Basis Dynamix Enterprise، فإن جهاز SVM الذي يتم اعتباره محليًا بالنسبة إلى Light Agent هو جهاز SVM يتم نشره على العقدة نفسها التي تحتوي على الجهاز الافتراضي المثبت عليه Light Agent.	في البنية التحتية الافتراضية القائمة على Basis Dynamix Enterprise، يمكن اعتبار SVM محليًا بالنسبة إلى Light Agent في أي من الحالات التالية: • يتم نشر SVM على العقدة نفسها التي تحتوي على الجهاز الافتراضي المثبت عليه Light Agent. • يتم نشر SVM في المنطقة نفس التي تحتوي على الجهاز الظاهري المثبت عليه Light Agent. • يتم نشر SVM في مركز البيانات الذي يحتوي على الجهاز الافتراضي المثبت عليه Light Agent.
Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis وALT Virtualization Server وAstra Linux وNuma vServer وBasis Dynamix Standard	

الخوارزمية القياسية	الخوارزمية الموسعة
في البنية التحتية الافتراضية القائمة على Microsoft Hyper-V أو XenServer أو VMware vSphere أو KVM أو Proxmox VE أو Basis أو HUAWEI FusionSphere أو Nutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard، يُعتبر جهاز SVM محليًّا بالنسبة إلى Light Agent إذا كان منشورًا على برنامج المحاكاة الافتراضية نفسه الذي يحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent.	في البنية التحتية الافتراضية القائمة على Microsoft Hyper-V أو XenServer أو VMware vSphere أو KVM أو Proxmox VE أو Basis أو HUAWEI FusionSphere أو Nutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard، يمكن اعتبار جهاز SVM محليًا بالنسبة إلى Light Agent في أي من الحالات التالية: • يتم نشر SVM على برنامج المحاكاة الافتراضية نفسه الذي تحتوي على الجهاز الافتراضي المثبت عليه Light Agent. • يتم نشر SVM على مجموعة برنامج المحاكاة الافتراضية التي تحتوي على الجهاز الافتراضي المثبت عليه Light Agent. • يتم نشر SVM في مركز البيانات الذي يحتوي على الجهاز الافتراضي المثبت عليه Light Agent.
OpenStack وVK Private Cloud SVM	
في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud، يمكنك تحديد كيفية قياس محلية جهاز SVM بالنسبة إلى Light Agent باستخدام المعامل `StandardAlgorithmSvmLocality` في قسم `HypervisorSpecificSettings:Openstack` في ملف تكوين خادم التكامل appsettings.json. ووفقًا لإصدار خادم التكامل، يوجد الملف في أحد المسارات التالية: • /var/opt/kaspersky/viis/common/ لخادم التكامل المستند إلى Linux • %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ لخادم التكامل المستند إلى Windows يمكن أن تأخذ معلمة `StandardAlgorithmSvmLocality` القيم التالية: • `ServerGroup` - في حالة تحديد هذه القيمة، يُعتبر جهاز SVM محليًّا بالنسبة إلى Light Agent إذا كانت يقع ضمن مجموعة الخوادم نفسها التي تحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent. ويتم استخدام هذه القيمة بشكل افتراضي. • `Project` - في حالة تحديد هذه القيمة، يُعتبر جهاز SVM محليًّا بالنسبة إلى Light Agent إذا تم نشره في مشروع OpenStack نفسه الذي يحتوي على الجهاز الافتراضي المثبت عليه Light Agent. • `AvailabilityZone` - في حالة تحديد هذه القيمة، يُعتبر جهاز SVM محليًّا بالنسبة إلى Light Agent إذا كانت يقع ضمن منطقة التوافر نفسها التي تحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent.	في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud، يمكن اعتبار جهاز SVM محليًّا بالنسبة إلى Light Agent في أي من الحالات التالية: • يوجد جهاز SVM في مجموعة الخوادم نفسها التي تحتوي على الجهاز الافتراضي المثبت عليه Light Agent. • يتم نشر جهاز SVM في مشروع OpenStack نفسه الذي يحتوي على الجهاز الافتراضي المثبت عليه Light Agent. • يوجد جهاز SVM في منطقة الإتاحة نفس التي تحتوي على الجهاز الافتراضي المثبت عليه Light Agent.

بالإضافة إلى خوارزميات اتصال SVM، يمكنك تنظيم اتصال Light Agent بأجهزة SVM باستخدام العلامات.

تكوين خوارزمية تحديد SVM

كيفية تكوين خوارزمية تحديد SVM لوضع Light Agent في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **وضع Light Agent ← خوارزمية تحديد SVM**.
4. حدد الخوارزمية:
   - **استخدام خوارزمية تحديد SVM القياسية**. يحدد Light Agent اجهزة SVM، التي يتم نشرها على مراقب الأجهزة الافتراضية نفسه.
   - **استخدام خوارزمية تحديد SVM الموسعة**. يحدد Light Agent أجهزة SVM التي تم نشرها في نوع مسار SVM المحدد (بشكل افتراضي، **Hypervisor**).

5. إذا لزم الأمر، حدد مسار SVM لخوارزمية تحديد SVM الموسعة:

- **Hypervisor**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

- يتم نشر جهاز SVM في برنامج محاكاة الأجهزة الافتراضية نفسه المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

- يوجد جهاز SVM في مجموعة الخوادم نفسها التي تحتوي على الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية تعمل على منصة OpenStack أو منصة VK Private Cloud).

- يوجد جهاز SVM على العقدة نفسها التي تحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

في حالة عدم توفر أجهزة SVM للاتصال بها في برنامج المحاكاة الافتراضية نفسه أو ضمن مجموعة الخوادم نفسها التي يوجد فيها الجهاز الافتراضي الذي يحتوي على Light Agent، فإن Light Agent لن يتصل بجهاز SVM.

- **Cluster**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

- يتم نشر أجهزة SVM في مجموعة برنامج محاكاة الأجهزة الافتراضية نفسها التي يوجد عليها الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

- يتم نشر أجهزة SVM ضمن مشروع OpenStack نفسه الذي يحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent (في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud.

- يوجد جهاز SVM في المنطقة نفسها التي تحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

في حالة عدم توفر أجهزة SVM للاتصال بها في مجموعة برنامج المحاكاة الافتراضية نفسه أو ضمن مشروع OpenStack نفسه الذي يوجد فيه الجهاز الافتراضي الذي يحتوي على Light Agent، فإن Light Agent لن يتصل بجهاز SVM.

- **مركز البيانات**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

- يتم نشر أجهزة SVM في مركز البيانات نفسه الذي يوجد عليه الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

- توجد أجهزة SVM ضمن منطقة التوفر نفسها التي تحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent (في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud.

- يوجد جهاز SVM في مركز البيانات نفسه الذي يحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

إذا لم تكن هناك أجهزة SVM متاحة للاتصال في مركز البيانات نفسه أو منطقة توافر الخدمات نفسها حيث يوجد الجهاز الافتراضي المُثبت عليه Light Agent، فلن يتصل Light Agent بجهاز SVM.

- **تجاهل**. يتجاهل Light Agent مسار SVM للاتصال بخادم الحماية. يضع Light Agents في الاعتبار معايير أخرى: العلامات وعدد أوضاع Light Agent المتصلة بجهاز SVM، وما إلى ذلك.

6. احفظ تغييراتك.

كيفية تكوين خوارزمية تحديد SVM لوضع Light Agent في Web Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **Light Agent Mode** ← **SVM selection algorithm**.

5. حدد الخوارزمية:

- **Use the standard SVM selection algorithm**. يحدد Light Agent اجهزة SVM، التي يتم نشرها على مراقب الأجهزة الافتراضية نفسه.
- **Use the extended SVM selection algorithm**. يحدد Light Agent أجهزة SVM التي تم نشرها في نوع مسار SVM المحدد (بشكل افتراضي، **Hypervisor**).

6. إذا لزم الأمر، حدد مسار SVM لخوارزمية تحديد SVM الموسعة:

- **Hypervisor**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

- يتم نشر جهاز SVM في برنامج محاكاة الأجهزة الافتراضية نفسه المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

- يوجد جهاز SVM في مجموعة الخوادم نفسها التي تحتوي على الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية تعمل على منصة OpenStack أو منصة VK Private Cloud).

- يوجد جهاز SVM على العقدة نفسها التي تحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

في حالة عدم توفر أجهزة SVM للاتصال بها في برنامج المحاكاة الافتراضية نفسه أو ضمن مجموعة الخوادم نفسها التي يوجد فيها الجهاز الافتراضي الذي يحتوي على Light Agent، فإن Light Agent لن يتصل بجهاز SVM.

- **Cluster**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

- يتم نشر أجهزة SVM في مجموعة برنامج محاكاة الأجهزة الافتراضية نفسها التي يوجد عليها الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

- يتم نشر أجهزة SVM ضمن مشروع OpenStack نفسه الذي يحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent (في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud.

- يوجد جهاز SVM في المنطقة نفسها التي تحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

في حالة عدم توفر أجهزة SVM للاتصال بها في مجموعة برنامج المحاكاة الافتراضية نفسه أو ضمن مشروع OpenStack نفسه الذي يوجد فيه الجهاز الافتراضي الذي يحتوي على Light Agent، فإن Light Agent لن يتصل بجهاز SVM.

- **Data center**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

- يتم نشر أجهزة SVM في مركز البيانات نفسه الذي يوجد عليه الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

- توجد أجهزة SVM ضمن منطقة التوفر نفسها التي تحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent (في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud.

- يوجد جهاز SVM في مركز البيانات نفسه الذي يحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

إذا لم تكن هناك أجهزة SVM متاحة للاتصال في مركز البيانات نفسه أو منطقة توافر الخدمات نفسها حيث يوجد الجهاز الافتراضي المُثبت عليه Light Agent، فلن يتصل Light Agent بجهاز SVM.

- **Ignore**. يتجاهل Light Agent مسار SVM للاتصال بخادم الحماية. يضع Light Agents في الاعتبار معايير أخرى: العلامات وعدد أوضاع Light Agent المتصلة بجهاز SVM، وما إلى ذلك.

7. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين خوارزمية تحديد SVM لوضع Light Agent في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، تحت **وضع Light Agent** انقر فوق لوحة **إعدادات اكتشاف SVM**.

3. حدد الخوارزمية:

- **استخدام خوارزمية تحديد جهاز متجهات الدعم (SVM) القياسية**. يحدد Light Agent اجهزة SVM، التي يتم نشرها على مراقب الأجهزة الافتراضية نفسه.

- **استخدام خوارزمية تحديد SVM الموسعة**. يحدد Light Agent أجهزة SVM التي تم نشرها في نوع مسار SVM المحدد (بشكل افتراضي، **Hypervisor**).

4. إذا لزم الأمر، حدد مسار SVM لخوارزمية تحديد SVM الموسعة:

- **Hypervisor**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

- يتم نشر جهاز SVM في برنامج محاكاة الأجهزة الافتراضية نفسه المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

- يوجد جهاز SVM في مجموعة الخوادم نفسها التي تحتوي على الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية تعمل على منصة OpenStack أو منصة VK Private Cloud).

- يوجد جهاز SVM على العقدة نفسها التي تحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

في حالة عدم توفر أجهزة SVM للاتصال بها في برنامج المحاكاة الافتراضية نفسه أو ضمن مجموعة الخوادم نفسها التي يوجد فيها الجهاز الافتراضي الذي يحتوي على Light Agent، فإن Light Agent لن يتصل بجهاز SVM.

- **Cluster**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

  - يتم نشر أجهزة SVM في مجموعة برنامج محاكاة الأجهزة الافتراضية نفسها التي يوجد عليها الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

  - يتم نشر أجهزة SVM ضمن مشروع OpenStack نفسه الذي يحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent (في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud.

  - يوجد جهاز SVM في المنطقة نفسها التي تحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

  في حالة عدم توفر أجهزة SVM للاتصال بها في مجموعة برنامج المحاكاة الافتراضية نفسه أو ضمن مشروع OpenStack نفسه الذي يوجد فيه الجهاز الافتراضي الذي يحتوي على Light Agent، فإن Light Agent لن يتصل بجهاز SVM.

- **مركز البيانات**. يحدد Light Agent جهاز SVM للاتصال به والذي يلبي المعايير (اعتمادًا على نوع البنية التحتية الافتراضية):

  - يتم نشر أجهزة SVM في مركز البيانات نفسه الذي يوجد عليه الجهاز الافتراضي المُثبت عليه Light Agent (في بنية تحتية افتراضية قائمة على Microsoft Hyper-V وXenServer وVMware vSphere وKVM وProxmox VE وBasis وHUAWEI FusionSphere وNutanix Acropolis أو ALT Virtualization Server أو Astra Linux أو Numa vServer أو Basis Dynamix Standard).

  - توجد أجهزة SVM ضمن منطقة التوفر نفسها التي تحتوي على الجهاز الافتراضي المُثبّت عليه Light Agent (في البنية التحتية الافتراضية التي تعمل على منصة OpenStack أو VK Private Cloud.

  - يوجد جهاز SVM في مركز البيانات نفسه الذي يحتوي على الجهاز الافتراضي المثبت علي Light Agent (في بنية تحتية افتراضية قائمة على Basis Dynamix Enterprise).

  إذا لم تكن هناك أجهزة SVM متاحة للاتصال في مركز البيانات نفسه أو منطقة توافر الخدمات نفسها حيث يوجد الجهاز الافتراضي المُثبت عليه Light Agent، فلن يتصل Light Agent بجهاز SVM.

- **تجاهل**. يتجاهل Light Agent مسار SVM للاتصال بخادم الحماية. يضع Light Agents في الاعتبار معايير أخرى: العلامات وعدد أوضاع Light Agent المتصلة بجهاز SVM، وما إلى ذلك.

5. احفظ تغييراتك.

توزيع اتصالات Light Agent على أجهزة SVM (العلامات)

يمكن لتطبيقات Light Agent متعددة الاتصال بجهاز SVM. ويمكنك تحقيق التوازن في اتصالات Light Agent تحديد قائمة منفصلة من أجهزة SVM. وإذا كنت تستخدم وحدة خدمة تكامل لاكتشاف SVM، فيمكنك استخدام العلامات لتحقيق التوازن في اتصالات Light Agent بأجهزة SVM. وهذا يعني، بالنسبة لوضع Light Agent، أنه يمكنك تعيين قائمة من أجهزة SVM للاتصال باستخدام علامة. ولفعل ذلك، يجب عليك تعيين علامة إلى Light Agent وتحديد هذه العلامة في إعدادات SVM. وللحصول على تفاصيل عن تحديد العلامات في إعدادات SVM، راجع تعليمات Kaspersky Security for Virtualization Light Agent.

مثال: يتم نشر حل Kaspersky Endpoint Detection and Response Optimum في بنيتك التحتية لمضيفي الجهاز الافتراضي المعينين. وفي هذه الحالة، يمكنك تعيين العلامة `[EDROptimum]` لوضع Light Agent ليتصل بالأجهزة الافتراضية المنفصلة المضاف بها مفتاح ترخيص EDR Optimum (EDR Optimum Add-on). ونتيجة لذلك، يمكنك استخدام وظيفة EDR Optimum على الجهاز الافتراضي المثبت عليه Light Agent. وعند توصيل Light Agent بجهاز SVM بدون مفتاح ترخيص EDR Optimum، لن تتوفر وظائف Kaspersky Endpoint Detection and Response Optimum.

كيفية تعيين علامة اتصال SVM إلى Light Agent في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **وضع Light Agent** ← **علامة اتصال SVM**.

4. حدد خانة الاختيار **استخدام علامة الاتصال** وأدخل علامة الاتصال بجهاز SVM.
بالنسبة للعلامة، يمكنك إدخال سلسلة نصية يصل طولها إلى 255 حرفًا. ويمكنك استخدام أي حرف باستثناء ;.

5. احفظ تغييراتك.

كيفية تعيين علامة اتصال SVM إلى Light Agent في Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies** ← **Asset management**.

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

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

4. انتقل إلى **Light Agent Mode** ← **SVM connection tag**.

5. حدد خانة الاختيار **Use connection tag** وأدخل علامة الاتصال بجهاز SVM.
بالنسبة للعلامة، يمكنك إدخال سلسلة نصية يصل طولها إلى 255 حرفًا. ويمكنك استخدام أي حرف باستثناء ;.

6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تعيين علامة اتصال SVM لوضع Light Agent في واجهة التطبيق

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

2. في نافذة إعدادات التطبيق، تحت **وضع Light Agent** انقر فوق لوحة **علامة اتصال SVM**.

3. حدد خانة الاختيار **استخدام علامة الاتصال** وأدخل علامة الاتصال بجهاز SVM.
بالنسبة للعلامة، يمكنك إدخال سلسلة نصية يصل طولها إلى 255 حرفًا. ويمكنك استخدام أي حرف باستثناء ;.

4. احفظ تغييراتك.

حماية الاتصال بين Light Agent وSVM

يمكنك تكوين تشفير الاتصال بين أوضاع Light Agent وخادم الحماية. ولفعل ذلك، تحتاج إلى تمكين تشفير قناة البيانات بين Light Agent وخادم الحماية في إعدادات خادم الحماية على SVM وفي إعدادات Light Agent.

يستطيع Light Agent الذي تم تمكين حماية الاتصال له فقط الاتصال بالأجهزة الافتراضية المنفصلة التي يتم تمكين تشفير قناة البيانات بين Light Agent وخادم الحماية لها. ولا يمكن لوضع Light Agent الذي تم تعطيل حماية الاتصال له الاتصال إلا بالأجهزة الافتراضية المنفصلة التي تم تعطيل تشفير القناة لها أو يُسمح لها بالاتصال غير الآمن بين خادم الحماية وLight Agent.

للحصول على تفاصيل عن تكوين حماية الاتصال على خادم الحماية، راجع تعليمات Kaspersky Security for Virtualization Light Agent.

قد تقلل حماية الاتصال باستخدام التشفير أداء Kaspersky Security for Virtualization Light Agent.

كيفية تكوين حماية الاتصال في Light Agent في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **وضع Light Agent** ← **حماية الاتصال**.
4. حدد خانة الاختيار **تشفير قناة البيانات بين Light Agent وخادم الحماية**.
5. احفظ تغييراتك.

كيفية تكوين حماية الاتصال في Light Agent في وحدة Web Console

1. في النافذة الرئيسية لـ Web Console، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **Light Agent Mode** ← **Connection protection**.
5. حدد خانة الاختيار **Encrypt data channel between Light Agent and the Protection Server**.
6. لتطبيق السياسة على أجهزة الكمبيوتر، أغلق أيقونات القفل واحفظ تغييراتك.

كيفية تكوين حماية الاتصال في Light Agent في واجهة التطبيق

1. في نافذة التطبيق الرئيسية، انقر فوق الزر ⚙.
2. في نافذة إعدادات التطبيق، تحت **وضع Light Agent** انقر فوق لوحة **حماية الاتصال**.
3. حدد خانة الاختيار **تشفير قناة البيانات بين Light Agent وخادم الحماية**.
4. احفظ تغييراتك.

تفعيل Light Agent

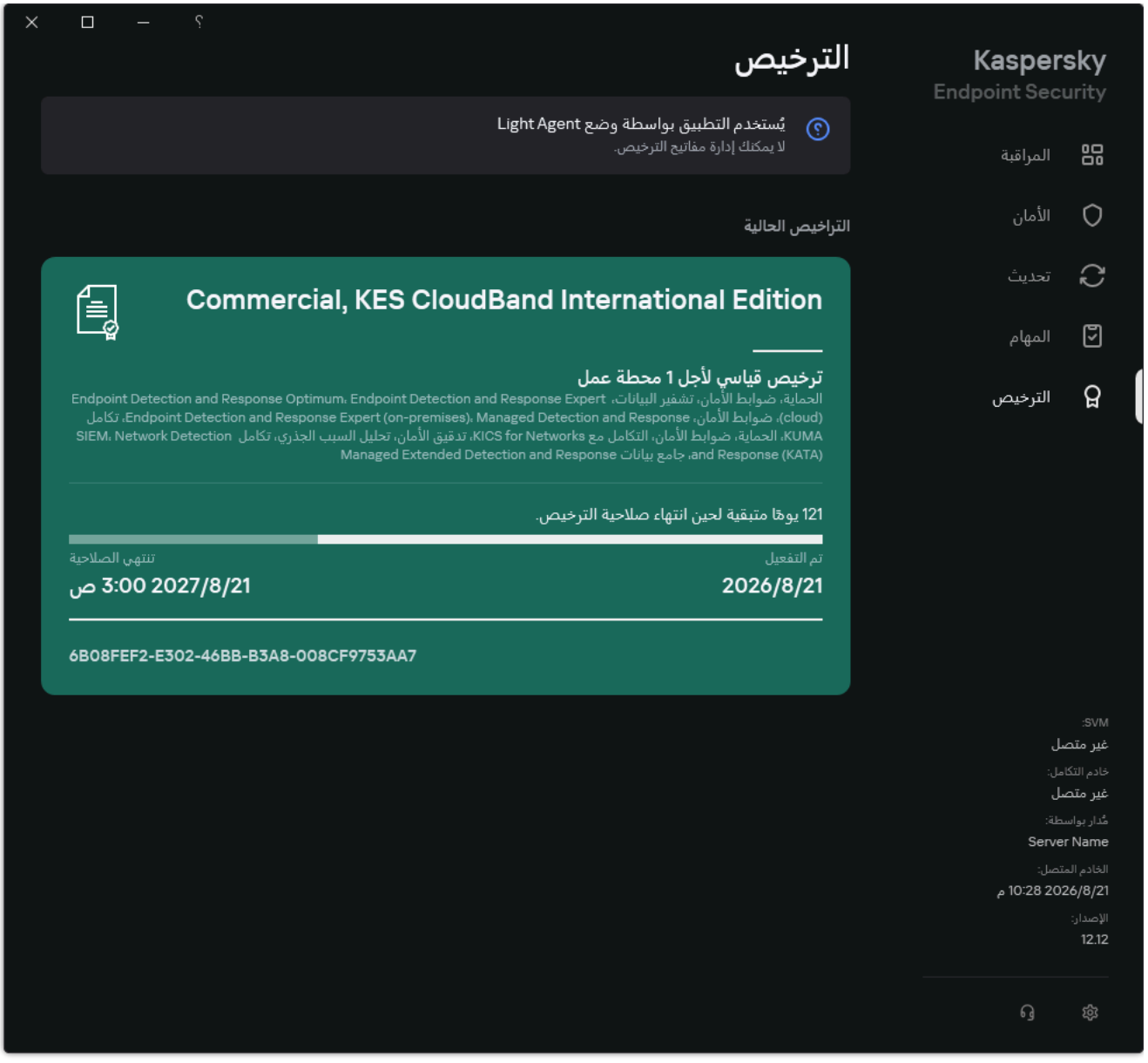
إذا تم استخدام Kaspersky Endpoint Security في وضع Light Agent لحماية البيئات الافتراضية، فلن تحتاج إلى تفعيل التطبيق بشكل منفصل. ولتفعيل التطبيق، يجب عليك إضافة مفتاح ترخيص إلى SVM. ويمكنك إضافة مفتاح ترخيص إلى SVM باستخدام المهمة الخاصة في وحدة تحكم Kaspersky Security Center. ولا يمكنك إدارة مفاتيح الترخيص في واجهة Light Agent، ومع ذلك، يمكنك عرض معلومات الترخيص (انظر الشكل أدناه). ويمكنك أيضًا عرض معلومات ترخيص Light Agent في سطر الأوامر (انظر التعليمات أدناه). ويحصل Light Agent على هذه المعلومات من SVM. وللحصول على تفاصيل عن تفعيل الحل وإدارة مفاتيح الترخيص، راجع تعليمات Kaspersky Security for Virtualization Light Agent.

لعرض معلومات ترخيص Light Agent:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd) كمسؤول.
2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.
3. قم بتشغيل الأمر التالي:

```
avp.com LICENSE /CHECK
```

نتيجةً لذلك، يعرض Kaspersky Endpoint Security معلومات الترخيص: عنوان SVM الذي يتصل به Light Agent، وعدد الأيام المتبقية حتى انتهاء صلاحية الترخيص، ومعلومات أخرى. وإذا واجهت أي مشاكل عند تفعيل Light Agent، فيرجى الرجوع إلى قاعدة معارف الدعم الفني.



نافذة الترخيص

دليل ترحيل KSVLA Light Agent إلى KES Light Agent

يحتوي Kaspersky Security for Virtualization 5.2 Light Agent على مكون Light Agent for Windows 5.2 (يشار إليه فيما يلي أيضًا باسم "KSVLA Light Agent"). وفي الإصدار 6.2 من Kaspersky Security for Virtualization Light Agent، يتم استخدام Kaspersky Endpoint Security في وضع Light Agent كمكون Light Agent. ولتحديث الحل إلى الإصدار 6.2، يجب عليك الترحيل من KSVLA Light Agent 5.2 إلى Kaspersky Endpoint Security في وضع Light Agent (يشار إليه فيما يلي أيضًا باسم "KES Light Agent"). وللحصول على تفاصيل عن تحديث إصدار Kaspersky Security for Virtualization Light Agent، راجع تعليمات Kaspersky Security for Virtualization Light Agent.

متطلبات البرنامج

قبل أن تبدأ الترحيل من KSVLA Light Agent إلى KES Light Agent، تأكد أن جهازك الافتراضي 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 KSVLA Light Agent إلى KES Light Agent:

- Kaspersky Endpoint Security for Windows 12.8.
- Kaspersky Security for Virtualization Light Agent 6.2 (بما في ذلك مكونات خادم الحماية وخادم التكامل).
- 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.

خطوات الترحيل

يتم تنفيذ الترحيل من KSVLA Light Agent إلى KES Light Agent بشكل شبه تلقائي. وهذا ضروري بسبب اختلاف بنيات التطبيقات.

قم بالترحيل من KSVLA Light Agent إلى KES Light Agent بالترتيب التالي:

1 ترحيل مهام وسياسات KSVLA Light Agent

لترحيل 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 تحديث قاعدة البيانات). وبعد الترحيل، يوصى أيضًا بالتحقق مما إذا كان معالج الترحيل قد قام بترحيل جميع الإعدادات بشكل صحيح.

إذا تم تمكين الحماية بكلمة مرور لتقييد الوصول إلى KSVLA Light Agent، فإنك تحتاج قبل تثبيت KES Light Agent إلى تعطيل الحماية بكلمة مرور في سياسة KSVLA Light Agent. ولا يمكنك إدخال كلمة مرور لإلغاء التثبيت في إعدادات حزمة تثبيت KES Light Agent. وبعد الانتهاء من تثبيت KES Light Agent أعلى KSVLA Light Agent، يجب عليك تمكين الحماية بكلمة مرور في سياسة KES.

2 تثبيت Kaspersky Endpoint Security في وضع Light Agent

يمكنك تثبيت KES Light Agent بالطرق التالية:

- تثبيت KES Light Agent بعد إزالة KSVLA Light Agent (مستحسن)
- تثبيت KES Light Agent فوق KSVLA Light Agent

3 تأكد أن التطبيق في حالة عمل بعد الترحيل

بعد الترحيل من KSVLA Light Agent إلى KES Light Agent، تأكد أن التطبيق يعمل بشكل صحيح. وقم بتفعيل السياسة المحولة. وتحقق من حالة الجهاز الافتراضي في وحدة تحكم Kaspersky Security Center (يجب أن تكون جيدة). تأكد من عدم الإبلاغ عن أي أخطاء للتطبيق، وتحقق أيضًا من وقت آخر اتصال بجهاز SVM وحالة حماية الجهاز الافتراضي. ولا تحتاج إلى تفعيل Light Agent لأن مفتاح الترخيص تمت إضافته إلى SVM.

تثبيت KES Light Agent بدلاً من KSVLA Light Agent

يمكنك تثبيت KES Light Agent بالطرق التالية:

- تثبيت KES Light Agent بعد إزالة KSVLA Light Agent (مستحسن)
- تثبيت KES Light Agent فوق KSVLA Light Agent

إزالة KSVLA Light Agent

يمكنك إزالة التطبيق عن بُعد باستخدام ملحق مهمة Install application remotely، محليًا على الجهاز الافتراضي أو في قالب الجهاز الافتراضي. بعد إزالة KSVLA Light Agent، قد تحتاج إلى إعادة تشغيل الجهاز الافتراضي.

بعد إزالة KSVLA Light Agent، قم بتثبيت KES Light Agent باستخدام أي طريقة مناسبة.

تثبيت Kaspersky Endpoint Security

إذا تم تمكين الحماية بكلمة مرور لتقييد الوصول إلى KSVLA Light Agent، فإنك تحتاج قبل تثبيت KES Light Agent إلى تعطيل الحماية بكلمة مرور في سياسة KSVLA Light Agent. ولا يمكنك إدخال كلمة مرور لإلغاء التثبيت في إعدادات حزمة تثبيت KES Light Agent. وبعد الانتهاء من تثبيت KES Light Agent فوق KSVLA Light Agent، يجب عليك تمكين الحماية بكلمة مرور في سياسة KES.

عند تثبيت Kaspersky Endpoint Security، يجب عليك تحديد وضع **Light Agent لحماية البيئات الافتراضية**. وقبل تثبيت KES Light Agent على جهاز افتراضي، يكتشف المثبت KSVLA Light Agent كبرنامج غير متوافق ويقوم بإزالته. ولا يتم دعم ترحيل تكوين KSVLA Light Agent. أي عند تثبيت KES Light Agent، يتم تحديد مجموعة المكونات المراد تثبيتها من خلال اختيارك في خصائص حزمة التثبيت أو في معالج التثبيت. وبعد إزالة KSVLA Light Agent، يجب إعادة تشغيل الجهاز الافتراضي.

لا يتم ترحيل إعدادات ومهام KSVLA Light Agent عند تثبيت KES Light Agent. 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.

التطابق بين مكونات KSVLA Light Agent وKES Light Agent

مجموعات مكونات KSVLA Light Agent وKES Light Agent متماثلتان تقريبًا. ويحتوي KES Light Agent على إعدادات أكثر من KSVLA Light Agent. وبعد الترحيل، تحتوي الإعدادات الجديدة على قيم افتراضية.

التطابق بين مكونات KSVLA Light Agent وKES Light Agent

Light Agent 5.2	KES Light Agent
Scan kernel	نواة التطبيق
File Anti-Virus	الحماية من تهديدات الملفات
Mail Anti-Virus	الحماية من تهديدات البريد
Web Anti-Virus	الحماية من تهديدات الويب
Firewall	جدار الحماية
Network Attack Blocker	الحماية من تهديدات الشبكة
Application Privilege Control	منع اختراق المضيف
Applications Launch Control	التحكم في التطبيقات
Web Control	التحكم في الويب
Device Control	التحكم في الجهاز
System Watcher	في Kaspersky Endpoint Security، يتم تقسيم هذا المكون إلى المكونات التالية: • منع الاستغلال • اكتشاف السلوك • محرك المعالجة
System Integrity Monitoring	مراقبة سلامة النظام
Integration with Kaspersky Endpoint Agent	(غير مدعوم) في Kaspersky Endpoint Security for Windows 11.9.0، لم تعد حزمة توزيع Kaspersky Endpoint Agent جزءًا من مجموعة التوزيع.
AMSI Protection	حماية AMSI

ترحيل مهام وسياسات KSVLA Light Agent

يمكنك ترحيل إعدادات سياسات ومهام KSVLA Light Agent باستخدام "معالج تحويل مجموعة السياسات والمهام" (المشار إليه فيما يلي أيضًا باسم "معالج الترحيل").

يتوفر معالج الترحيل لتطبيق KSVLA Light Agent فقط في وحدة تحكم الإدارة (MMC). ولا يمكن ترحيل إعدادات السياسة والمهام في Web Console وCloud Console.

يتم تضمين الاعتبارات الخاصة التالية في سياسات ومهام الترحيل:

- سياسة جديدة باسم <Policy> (تم التحويل).
- وتكون حالة السياسة الجديدة Inactive policy.
- لم يتم ترحيل حظر تعديل الإعدادات ("القفل"). ويعين "معالج الترحيل" القيم الافتراضية.
- لا يتم ترحيل ملفات تعريف السياسة. ويجب عليك إضافة ملفات تعريف السياسة يدويًا.

- تحسين إدارة المنطقة الموثوقة. في KSVLA Light Agent، لا يمكنك إضافة استثناءات محددة مسبقًا إلا عند إنشاء سياسة. وبالتالي، في خصائص السياسة، يمكنك تكوين الاستثناءات المضافة مسبقًا أو إضافة الاستثناءات يدويًا. ولا يمكنك إضافة استثناءات محددة مسبقًا في خصائص السياسة. وفي KES Light Agent، تتوفر الاستثناءات المحددة مسبقًا أثناء إنشاء السياسة وفي خصائص السياسة التي تم إنشاؤها. ويمكنك أيضًا تحديد الاستثناءات المحددة مسبقًا في حزمة التثبيت.

- تم نقل تكوين واجهة مستخدم التطبيق في Kaspersky Endpoint Security من المُثبت إلى السياسة. وإذا كنت بحاجة، على سبيل المثال، إلى إخفاء واجهة مستخدم التطبيق، يمكنك إدارة إعدادات السياسة.

- تختلف مجموعات الوظائف الخاصة بتكوين التحكم في الوصول المستند الموجود على اليمين (RBAC) في Kaspersky Endpoint Security وKSVLA Light Agent. ويجب عليك تكوين حقوق وصول المستخدم إلى المناطق الوظيفية من البداية.

كيفية استخدام معالج تحويل تصحيح المهام والسياسات لترحيل إعدادات سياسة KSVLA Light Agent

1. في وحدة تحكم الإدارة ، حدد خادم الإدارة وانقر بزر الماوس الأيمن لفتح قائمة السياق.

2. حدد **All tasks ← Policies and tasks batch conversion wizard**.

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

حدد سياسة Kaspersky Security for Virtualization 5.2 Light Agent for Windows التي تريد تحويلها. انتقل إلى الخطوة التالية.

سيبدأ معالج الترحيل بعد ذلك في تحويل السياسات. وأثناء تحويل السياسة، يطالبك معالج الترحيل بقبول شروط بيان KSN. سياسة جديدة باسم <Policy> (تم التحويل).

الخطوة 3. تحويل المهام

ينشئ معالج الترحيل مهام جديدة لبرنامج Kaspersky Endpoint Security for Windows. في قائمة المهام، حدد مهام KSVLA Light Agent التي تريد إنشاءها لتطبيق Kaspersky Endpoint Security. وسيتم تسمية المهام الجديدة Task name>> (تم التحويل). انتقل إلى الخطوة التالية.

الخطوة 4. اكتمال المعالج

قم بإنهاء المعالج.

بعد ترحيل السياسة، يجب عليك فتح خصائص السياسة، والتحقق من إعداداتها وحفظ السياسة. وإذا لم تكمل هذه الخطوات، فقد يتجاهل KES Light Agent السياسة المحولة.

انتبه بشكل خاص إلى ترحيل إعدادات اتصال SVM لتطبيق Light Agent وقوائم الاستثناء والتطبيقات الموثوقة وعناوين الويب الموثوقة وقواعد التحكم في التطبيقات.

ترحيل تكوين [KSVLA Light Agent+KEA] إلى تكوين [KES Light Agent+العامل المُضمن]

لدعم استخدام Kaspersky Endpoint Security for Windows كجزء من EDR (KATA) وEDR Optimum وKaspersky Sandbox، تمت إضافة عامل مُضمن إلى التطبيق. ولم تعد بحاجة إلى تطبيق Kaspersky Endpoint Agent منفصل للعمل مع هذين الحلين.

عند الترحيل من KSVLA Light Agent إلى KES Light Agent، تستمر حلول EDR (KATA) وEDR Optimum وKaspersky Sandbox في العمل مع العملاء المُضمنين لتطبيق Kaspersky Endpoint Security. بالإضافة إلى ذلك، ستتم إزالة Kaspersky Endpoint Agent من الكمبيوتر.

قبل الترحيل من KSVLA Light Agent إلى KES Light Agent، يجب عليك تحديث جميع مكونات Kaspersky Security for Virtualization إلى الإصدار 6.2، بما في ذلك خادم الحماية وخادم التكامل. وللحصول على تفاصيل عن تحديث إصدار Kaspersky Security for Virtualization Light Agent، راجع تعليمات Kaspersky Security for Virtualization Light Agent.

يتضمن ترحيل تكوين [KSVLA Light Agent+KEA] إلى تكوين [KES Light Agent+العامل المدمج] الخطوات التالية:

1. **ترحيل السياسة والمهام**

   يتضمن ترحيل سياسات ومهام [KSVLA Light Agent+KEA] إلى [KES Light Agent+العامل المُضمن] الخطوات التالية:

   1. ترحيل السياسات والمهام من KSVLA Light Agent إلى KES Light Agent باستخدام معالج تحويل تصحيح المهام والسياسات (متاح فقط في وحدة تحكم الإدارة (MMC)).

      نتيجة لذلك، يتم إنشاء سياسة جديدة بالاسم <السياسة> (محولة). ويتم أيضًا إنشاء مهام KES الجديدة مع أسماء <اسم المهمة> (محولة).

   2. ترحيل السياسات والمهام من KEA إلى KES باستخدام المعالج للترحيل من Kaspersky Endpoint Agent (متاح فقط في 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.

2. **الترحيل من KSVLA Light Agent إلى KES Light Agent**

   يتضمن الترحيل من KSVLA Light Agent إلى KES Light Agent تثبيت KES Light Agent بدلاً من KSVLA Light Agent.

يقوم المسؤولون عادةً بتمكين الحماية بكلمة مرور لتقييد الوصول إلى KSVLA Light Agent وKEA. ويمكنك فقط إدخال كلمة مرور إلغاء تثبيت KEA في خصائص مهمة Install application remotely. وللترحيل، يجب عليك تعطيل الحماية بكلمة مرور لتطبيق KSVLA Light Agent.

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.

3. **وظيفة الترخيص**

إذا تم استخدام التطبيق في وضع Light Agent، فلن تحتاج إلى تفعيل التطبيق. ولتفعيل التطبيق، يجب عليك إضافة مفتاح ترخيص إلى SVM. ويجب عليك أيضًا إضافة مفتاح الترخيص لتفعيل الوظائف الإضافية (على سبيل المثال، EDR Optimum) إلى SVM. وهذا يعني أنه يتم إجراء ترخيص الوظائف تلقائيًا كجزء من عملية الترحيل.

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 الإصدار 13.2 أو أحدث من عميل الشبكة على الكمبيوتر.
- تحقق من حالة تشغيل العميل المدمج عن طريق عرض Report on status of application components. 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 Report on status of application components. وإذا كانت حالة مكون ما غير مشمول بالترخيص ، فتأكد من تشغيل وظيفة توزيع مفتاح الترخيص التلقائي لمكون EDR Optimum.
- تحقق من حالة اتصال الجهاز الافتراضي بجهاز SVM. يمكنك الحصول على معلومات عن حالة اتصال Light Agent بجهاز SVM في Kaspersky Endpoint Security أو باستخدام أمر التطبيق.

لإدارة التطبيق من سطر الأوامر

يمكنك إدارة Kaspersky Endpoint Security من سطر الأوامر. يمكنك استعراض قائمة الأوامر لإدارة التطبيق من خلال تشغيل الأمر `avp.com HELP`. للقراءة عن بناء الأمر لأمر محدد، قم بإدخال `avp.com 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 `%%`.

بدائل القيمة `1` هي القيم `yes` و `on` و `enable` و `enabled` و `true`. بدائل القيمة `0` هي القيم `no` و `off` و `disable` و `disabled` و `false`.

Setup. تثبيت التطبيق

يتضمن تثبيت التطبيق من سطر الأوامر الخطوات التالية:

1. **اختيار حزمة توزيع**

   توفر Kaspersky حزم توزيع لعمليات الترجمة المختلفة التي تتوافق مع بنيات وحدة المعالجة المركزية المختلفة وتتضمن وحدات تشفير مختلفة.

   تتضمن مجموعة التوزيع حزم التوزيع التالية:

   - **AES256**

     حزمة التوزيع هذه مخصصة للتثبيت على أجهزة الكمبيوتر ذات بنية x86/x64. تحتوي حزمة التوزيع هذه على أدوات التشفير التي تنفذ خوارزمية التشفير AES (Advanced Encryption Standard) باستخدام طول مفتاح فعال 256 بت.

   - **AES56**

     حزمة التوزيع هذه مخصصة للتثبيت على أجهزة الكمبيوتر ذات بنية x86/x64. تحتوي حزمة التوزيع هذه على أدوات التشفير التي تقوم بتنفيذ خوارزمية التشفير AES باستخدام طول مفتاح فعال 56 بت.

   - **Arm64**

     حزمة التوزيع هذه مخصصة للتثبيت على أجهزة الكمبيوتر القائمة على Arm. حزمة التوزيع هذه غير مخصصة للتثبيت على الخوادم.

2. **نقل حزمة توزيع التطبيق إلى التخزين بالكمبيوتر**

   حزمة التوزيع هي أرشيف ذاتي الاستخراج بتنسيق EXE. ولعرض محتويات حزمة التوزيع، تحتاج إلى استخراج الأرشيف إلى مجلد منفصل. لتثبيت التطبيق، تحتاج إلى جميع الملفات من حزمة التوزيع، بما في ذلك ملف bases.cab.

3. **تشغيل أمر التثبيت**

   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 التثبيت في الوضع الصامت، لا يلزم مشاركتك في عملية التثبيت (التثبيت الصامت). 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 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 تشغيل 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).



وصف خيارات أمر التثبيت

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] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

أو

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/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.
`CONFIGPATH=<path to the configuration file>`	تثبيت التطبيق بإعدادات محددة مسبقًا. ولفعل هذا، تحتاج إلى تحميل ملف يحدد إعدادات برنامج Kaspersky Endpoint Security. يمكنك إنشاء ملف تكويني في الواجهة المحلية للتطبيق.
`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`	قم بتعطيل التحقق من البرامج المُثبتة. تتوفر قائمة البرامج التي قد تسبب مشكلات في التوافق في ملف incompatible.txt المضمن في حزمة التوزيع. إذا لم يتم تعيين قيمة لهذه المعلمة وتم اكتشاف برنامج من القائمة، فسيتم إنهاء تثبيت Kaspersky Endpoint Security.
`SKIPPRODUCTUNINSTALL=1`	قم بتعطيل الإزالة التلقائية للبرامج المكتشفة من قائمة incompatible.txt. إذا لم يتم تعيين قيمة لهذه المعلمة، فسيحاول Kaspersky Endpoint Security إزالة البرنامج الذي قد يسبب مشكلات في التوافق. لا يمكن تمكين الإزالة التلقائية للبرنامج عند تثبيت Kaspersky Endpoint Security باستخدام مثبت msiexec. لإزالة البرنامج الذي قد يتسبب في حدوث مشكلات في التوافق تلقائيًا، استخدم ملف setup_kes.exe.
`CLEANERSIGNCHECK=0|1`	التحقق من التوقيعات الرقمية لملفات البرامج المكتشفة من قائمة incompatible.txt. لإزالة البرنامج، يقوم Kaspersky Endpoint Security بتشغيل ملف مُثبت البرنامج. وإذا لم يكن ملف التثبيت يحتوي على توقيع رقمي، فإن Kaspersky Endpoint Security يعتبر الملف غير موثوق به ويوقف عملية إزالة البرنامج لتجنب تشغيل تعليمات برمجية ضارة محتملة. وإذا لم يتمكن التطبيق من التحقق من التوقيع الرقمي لملف البرنامج المكتشف، فسيتم إيقاف تثبيت Kaspersky Endpoint Security بسبب حدوث 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).

STANDALONEMODE=1	تثبيت التطبيق في تكوين Endpoint Detection and Response Agent (EDR Agent) للتكامل مع حلي Kaspersky Endpoint Detection and Response (KATA) أو Kaspersky Endpoint Detection and Response Expert (on-premises). وهذا التكوين مطلوب إذا تم نشر منصة حماية نقطة النهاية (EPP) التابعة لجهة خارجية في مؤسستك جنبًا إلى جنب مع حل Kaspersky Endpoint Detection and Response. وهذا يجعل Kaspersky Endpoint Security في تكوين Endpoint Detection and Response Agent متوافقًا مع تطبيقات EPP التابعة لجهات خارجية.
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 ببيانات اعتماد حساب المستخدم (معلمتا 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. • EXPORT – تصدير إعدادات التطبيق. على سبيل المثال، KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT. لحساب KLAdmin الحق في اتخاذ أي إجراء محمي بكلمة مرور. لذلك، من المستحيل تكوين نطاق كلمة المرور لحساب KLAdmin. وإذا حاولت تكوين نطاق كلمة المرور لحساب KLAdmin، فإن التطبيق يمنع الإجراءات المحددة لمجموعة "الكل".
PROTECTOSSERVICES	حماية وظائف خدمات نظام التشغيل. تمنع حماية خدمات نظام التشغيل تطبيقات الطرف الثالث من التدخل في تشغيل خدمات نظام التشغيل. وتشمل هذه الخدمات، على سبيل المثال، خدمة التشغيل التلقائي للتطبيق. • 1 يعني أنه تم تمكين حماية خدمات نظام التشغيل (القيمة الافتراضية). • 0 يعني أن حماية خدمات نظام التشغيل معطلة.
ENABLETRACES	تمكين أو تعطيل تتبع التطبيق. بعد بدء تشغيل Kaspersky Endpoint Security، فإنه يحفظ ملفات التتبع في المجلد %ProgramData%\Kaspersky Lab\KES.14.2\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). تضمن هذه الميزة العرض الصحيح لحالة الجهاز الافتراضي في Azure في وحدة تحكم 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 (Sensor ID). ويسمح وضع التوافق مع Azure WVD بتعيين Sensor ID فريد دائم لهذه الأجهزة الظاهرية. وفي حالة إيقاف تشغيل وضع التوافق، Sensor ID 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: • Seamless يعني ترقية التطبيق مع إعادة تشغيل الكمبيوتر (القيمة الافتراضية). • Force 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 إعدادات التطبيق 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 (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.
EnableUniqueSensorID	إنشاء معرف كمبيوتر فريد (Sensor ID) أثناء تثبيت أو تحديث التطبيق. يتم استخدام Sensor ID في حل Kaspersky Anti Targeted Attack Platform لتحديد أجهزة الكمبيوتر التي ترسل القياس عن بُعد إلى الخادم. وعند إنشاء Sensor ID، يستخدم التطبيق خوارزمية تضع في الاعتبار تكوين الكمبيوتر، مثل الرقم التسلسلي للوحة الأم. وفي بعض الحالات، على سبيل المثال، عند استخدام التطبيق في بيئة افتراضية، قد يتم تكرار Sensor ID. ونتيجة لذلك، يتعذر على Kaspersky Anti Targeted Attack Platform تحديد الكمبيوتر الذي يتم إرسال القياس عن بُعد منه. ولإنشاء Sensor ID فريد، تحتاج إلى ضبط المعلمة EnableUniqueSensorID=1. ونتيجة لذلك، سيستخدم التطبيق خوارزمية مختلفة لإنشاء Sensor ID، والذي يضع في الاعتبار البيانات الأخرى حول الكمبيوتر. ويضمن هذا وجود Sensor ID فريد. بشكل افتراضي، لا يتم تعيين المعلمة. ويرث التطبيق Sensor ID في الحالات التالية: • تحديث إصدار التطبيق؛ • ترحيل تكوين [KES+KEA] إلى تكوين [KES+العامل المضمن] كجزء من إصلاح التطبيق، يحاول المثبت وراثة Sensor ID. إذا كان من غير الممكن استعادة Sensor ID، فإن التطبيق ينشئ Sensor ID.
SKIPKB5007186CHECK=1	تعطيل التحقق من تحديث نظام التشغيل المثبت KB5007186. قبل تثبيت التطبيق، يتحقق المثبت من تحديثات نظام التشغيل المثبتة. يكون تحديث KB5007186 موجودًا في قائمة تحديثات نظام التشغيل التي يمكن أن تسبب مشاكل للتطبيق. وللحصول على معلومات مفصلة، ارجع إلى قاعدة معارف الدعم الفني. لذلك، يوقف المثبت التثبيت في حالة اكتشاف هذا التحديث. ولمتابعة التثبيت، عيّن SKIPKB5007186CHECK=1.

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 setup.ini ملف. 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.

  لتطبيق الإعدادات من ملف setup.ini، ضع هذا الملف في المجلد الذي يحتوي على حزمة توزيع Kaspersky Endpoint Security.

- install.cfg - إعدادات عملية Kaspersky Endpoint Security

  لتطبيق الإعدادات من ملف التكوين install.cfg، تحتاج إلى تحديد المسار إلى الملف في أمر تثبيت التطبيق التالي: `CONFIGPATH=<path to the configuration file>`.

- 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 ملف setup.reg، ضع هذا الملف 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>`.

Setup /x. 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 (إلغاء التثبيت في الوضع الصامت). 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 المعرّف الفريد العام (GUID) للتطبيق في قاعدة معارف الدعم الفني أو باستخدام الأمر التالي:

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

- إذا كانت عملية الإزالة محمية بكلمة مرور:

```
setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

أو

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

يمكنك أيضًا استخدام معلمة SAVEQB لحفظ الملفات التي تم فحصها بواسطة التطبيق ووضعها في النسخة الاحتياطية. يتم تخزين النسخ الاحتياطية للملفات في المجلد C:\ProgramData\Kaspersky Lab\KES.14.2\QB. وبشكل افتراضي، يتم تعطيل حفظ الملفات في النسخة الاحتياطية (SAVEQB=0).

مثال

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i. استعادة التطبيق

عند الاسترداد، يفحص التطبيق ويستعيد سلامة جميع الوحدات النمطية للتطبيق ومفاتيح تسجيل النظام التالفة التي تم إنشاؤها كجزء من عملية تثبيت التطبيق.

يمكن استرداد برنامج Kaspersky Endpoint Security من سطر الأوامر في أحد الأوضاع التالية:

- في الوضع التفاعلي باستخدام معالج إعداد التطبيق.
- في الوضع الصامت. بعد بدء الاسترداد في الوضع الصامت، لا يلزم تدخلك في عملية الاسترداد.

إذا كان مُثبِّت Kaspersky Endpoint Security يعمل في وضع الاسترداد، ولا يحتاج التطبيق إلى الاسترداد، فلن يقوم المُثبِّت بإجراء أي تغييرات.

إذا كان مُثبِّت Kaspersky Endpoint Security يعمل في وضع الاسترداد، ولم يتم تثبيت التطبيق، يبدأ المثبت عملية التثبيت.

لإلغاء استرداد 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 الاسترداد غير محمية بكلمة مرور:

```
msiexec.exe /i <GUID> REINSTALL=ALL /qn
```

<GUID> هو المعرف الفريد للتطبيق. يمكنك معرفة المعرّف الفريد العام (GUID) للتطبيق في قاعدة معارف الدعم الفني أو باستخدام الأمر التالي:

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

- إذا كانت عملية الاسترداد محمية بكلمة مرور:

```
msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
```

مثال

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

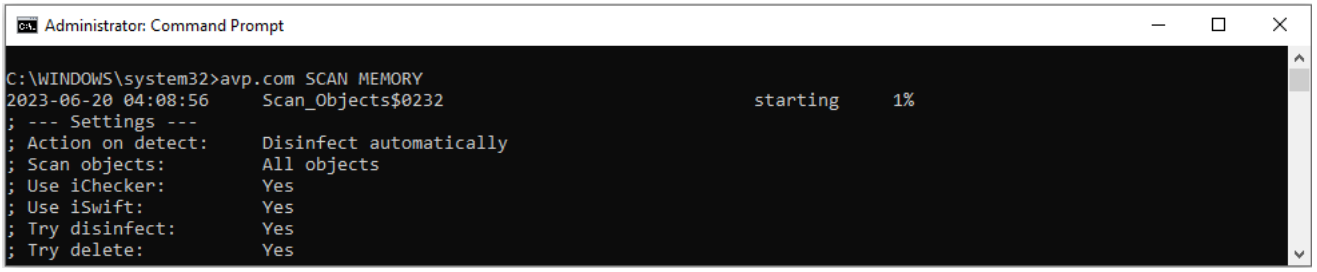
أوامر AVP

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.
   يمكنك إضافة مسار إلى الملف القابل للتنفيذ إلى متغير النظام %PATH% أثناء تثبيت التطبيق.
3. استخدم القالب التالي لتنفيذ الأمر:

```
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

تشغيل مهمة فحص البرامج الضارة.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

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 في Kaspersky Endpoint Security for Windows 12.12، يتم استثناء البريد الإلكتروني من نطاق فحص التطبيق. ويتم فحص رسائل البريد الإلكتروني الواردة والصادرة بواسطة مكون الحماية من تهديدات البريد. وإذا كنت تستخدم إصدارًا سابقًا من المكون الإضافي للإدارة، فإن التطبيق يستثني البريد الإلكتروني من نطاق الفحص، حتى إذا كانت السياسة تتضمنه.
/MEMORY	فحص ذاكرة Kernel
/STARTUP	فحص الكائنات التي يتم تحميلها عند بدء تشغيل نظام التشغيل
/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	**إعلام**. في حالة تحديد هذا الخيار، يضيف Kaspersky Endpoint Security المعلومات حول الملفات المصابة إلى قائمة التهديدات النشطة عند اكتشاف هذه الملفات.
/i1	**تنظيف؛ إبلاغ إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول Kaspersky Endpoint Security تلقائيًا تنظيف كل ما تم اكتشافه من ملفات مصابة. وإذا فشل التنظيف، يضيف Kaspersky Endpoint Security معلومات عن الملفات المصابة المكتشفة إلى قائمة التهديدات النشطة.
/i2	**تنظيف؛ حذف إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف. ويتم تحديد هذا الإجراء بصورة افتراضية.
/i3	**الحذف في حالة فشل التنظيف**. وأيضًا قم بحذف الملفات المركبة (على سبيل، الأرشيفات) إذا تعذر تنظيف الملف المصاب أو حذفه.
/i4	**حذف**. 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:<file mask>	يتم استثناء الملفات التي تتطابق قناع الملف من نطاق الفحص. على سبيل المثال: • سيشمل القناع `*.exe` كافة المسارات إلى 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 الملفات من عمليات 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:<file with scan settings>	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 "C:\Documents and Settings\All Users\My Documents" "C:\Program Files
```

UPDATE. تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق

تشغيل مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

لا يمكن تشغيل هذا الأمر في حالة تثبيت التطبيق في وضع Light Agent.

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 قواعد البيانات والوحدات النمطية للتطبيق التي تم إنشاؤها تلقائيًا بعد تثبيت التطبيق. يمكنك تغيير إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق في واجهة التطبيق المحلية أو في وحدة التحكم على Kaspersky Security Center. إذا لم يتم تكوين هذا الإعداد، يبدأ Kaspersky Endpoint Security مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق بالإعدادات الافتراضية أو بالإعدادات المحددة في الأمر. يمكنك تكوين إعدادات مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق على النحو التالي: • يبدأ `UPDATE` مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق بالإعدادات الافتراضية: مصدر التحديث هو خوادم تحديث Kaspersky والحساب هو النظام والإعدادات الافتراضية الأخرى. • يبدأ `UPDATE local` مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق الذي تم إنشاؤه تلقائيًا بعد التثبيت (مهمة محددة مسبقًا). • يبدأ `UPDATE <update settings>` مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق بالإعدادات المحددة يدويًا (انظر أدناه).

مصدر التحديث	
`"<update source>"`	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.

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 قواعد البيانات والوحدات النمطية للتطبيق. 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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

لا يمكن تشغيل هذا الأمر في حالة تثبيت التطبيق في وضع Light Agent.

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

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.14.2\Traces. وبشكل افتراضي، يتم تعطيل عملية التتبع.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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 معلمتي file و mem.
file	احفظ ملف تتبع واحد (لا يوجد حد للحجم).

rot	احفظ عمليات التتبع لعدد محدود من مجموعات الملفات التي لها حجم محدود واستبدل الملفات الأقدم عند الوصول إلى الحد الأقصى للحجم.
mem	احفظ عمليات التتبع في ملفات التفريغ.

مثال

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START. بدء ملف تعريف

بدء ملف تعريف (على سبيل المثال، بدء تحديث قاعدة البيانات أو تمكين مكون الحماية).

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
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 عرض قائمة ملفات التعريف المتاحة عن طريق تشغيل 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 تنفيذ ملف التعريف (على سبيل المثال، إيقاف فحص محركات الأقراص القابلة للإزالة أو تعطيل مكون حماية).

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم أذونات **تعطيل مكونات الحماية** و**تعطيل مكونات التحكم**.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
<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 عرض قائمة ملفات التعريف المتاحة عن طريق تشغيل الأمر HELP STOP.

المصادقة	
/login=<user name> /password=<password>	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

STATUS. حالة ملف التعريف

عرض معلومات الحالة لملفات تعريف التطبيق (على سبيل المثال، running أو completed). يمكنك عرض قائمة ملفات التعريف المتاحة عن طريق تشغيل 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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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 إحصائيات لملف 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`.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
<avp.com STATISTICS <profile
```

RESTORE. استعادة الملفات من النسخ الاحتياطي

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.14.2\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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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=samplePassword
```

EXPORT. تصدير إعدادات التطبيق

تصدير إعدادات Kaspersky Endpoint Security في ملف. إذا كان الأمر يحتوي فقط على اسم الملف الذي تريد تصدير الإعدادات إليه، فإن التطبيق يضع الملف كما يلي:

- إذا تمت إضافة المسار إلى avp.com إلى متغير النظام %PATH%، يضع التطبيق الملف في المجلد C:\Windows\SysWOW64.
- إذا قمت بتشغيل الأمر من مجلد تثبيت التطبيق، فسيفشل التصدير لأن الحماية الذاتية للتطبيق تمنع إنشاء ملف جديد في مجلد التطبيق. ولتصدير إعدادات التطبيق إلى ملف، أدخل مسار الملف.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **تصدير الإعدادات**.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
<avp.com EXPORT <profile> <file name> /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 عرض قائمة ملفات التعريف المتاحة عن طريق تشغيل الأمر HELP EXPORT.

ملف للتصدير	
<file name>	اسم الملف الذي سيتم تصدير إعدادات التطبيق إليه. ويمكنك أيضًا إدخال مسار الملف. يمكنك تصدير إعدادات برنامج Kaspersky Endpoint Security إلى ملف تكوين DAT أو CFG أو ملف النص TXT أو إلى مستند XML.

المصادقة	
`/login=<user name> /password=<password>`	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT. استيراد إعدادات التطبيق

استيراد إعدادات Kaspersky Endpoint Security من ملف تم إنشاؤه باستخدام الأمر `EXPORT`.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة. يجب أن يكون لدى المستخدم إذن **تكوين إعدادات التطبيق**.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد 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=samplePassword
```

ADDKEY. تطبيق ملف المفتاح

تفعيل Kaspersky Endpoint Security باستخدام ملف مفتاح. إذا كان التطبيق مفعلًا بالفعل، فستتم إضافة المفتاح كمفتاح احتياطي.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

لا يمكن تشغيل هذا الأمر في حالة تثبيت التطبيق في وضع Light Agent.

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=<password>	بيانات اعتماد حساب المستخدم. يجب إدخال بيانات الاعتماد هذه فقط إذا تم تمكين الحماية بكلمة المرور.

مثال

```
avp.com ADDKEY file.key
```

LICENSE. الترخيص

إدارة مفاتيح ترخيص Kaspersky Endpoint Security أو 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**.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

لا يمكن تشغيل هذا الأمر في حالة تثبيت التطبيق في وضع Light Agent.

بناء جملة الأمر

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

العملية	
/ADD <file name>	تفعيل Kaspersky Endpoint Security باستخدام ملف مفتاح. 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 <license ID>	تحديث حالة التراخيص باستخدام معرف الترخيص. باستخدام هذا الأمر، يمكنك تحديث حالة الوظيفة الإضافية لحل EDR أو الوظيفة الإضافية لحل MDR أو الوظيفة الإضافية لحل KUMA أو التراخيص الأخرى. ويمكنك الحصول على معرف الترخيص من شهادة الترخيص. ونتيجة لذلك، يتلقى التطبيق معلومات محدثة عن حالة الترخيص من خوادم تنشيط Kaspersky.
/CHECK	الحصول على معلومات الترخيص. يعرض Kaspersky Endpoint Security معلومات عن جميع مفاتيح الترخيص المضافة بما في ذلك المفاتيح الاحتياطية ووظيفة EDR الإضافية ووظيفة MDR الإضافية ووظيفة KUMA الإضافية والمفاتيح الأخرى. يعرض Kaspersky Endpoint Security معلومات الترخيص التالية: • اسم الترخيص؛ • معرّف الترخيص؛ • عنوان خادم الحماية (SVM) الذي يتصل به الجهاز الافتراضي الذي تم تثبيت التطبيق عليه في وضع Light Agent؛ • نوع الترخيص: تجريبي، تجاري، بيتا، اشتراك؛ • تاريخ ووقت تفعيل التطبيق؛ • تاريخ ووقت انتهاء صلاحية الترخيص؛ • عدد الأيام حتى انتهاء صلاحية الترخيص.
/CHECK <license ID>	الحصول على معلومات الترخيص عن طريق الهوية. يمكنك استخدام هذا الأمر للحصول على معلومات الترخيص. ويمكنك الحصول على معرف الترخيص من شهادة الترخيص.
/DEL /login=<user name> /password=<password>	إزالة مفتاح الترخيص الخاص بالتطبيق. وكذلك ستتم إزالة المفتاح الاحتياطي.
/DEL <license ID> /login= <user name> /password= <password>	حذف المفتاح باستخدام معرف الترخيص. باستخدام هذا الأمر، يمكنك حذف مفتاح الوظيفة الإضافية لحل EDR أو الوظيفة الإضافية لحل MDR أو الوظيفة الإضافية لحل KUMA أو التراخيص الأخرى. ويمكنك الحصول على معرف الترخيص من شهادة الترخيص.

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 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

مثال

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW. شراء الترخيص

فتح موقع ويب Kaspersky لشراء الترخيص أو لتجديد الترخيص الخاص بك.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

لا يمكن تشغيل هذا الأمر في حالة تثبيت التطبيق في وضع Light Agent.

PBATESTRESET. إعادة تعيين 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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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**.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد 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**.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

SPYWARE. الكشف عن برامج التجسس

إدارة اكتشاف برامج التجسس. افتراضيًا، يتم تمكين الكشف عن برامج التجسس.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com SPYWARE on|off
```

KSN. التبديل بين KPSN / KSN

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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

لا يمكن تشغيل هذا الأمر في حالة تثبيت التطبيق في وضع Light Agent.

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
```

مثال

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE. تعطيل حماية الاتصال بالخادم

تشغيل مهمة حماية الاتصال بخادم الإدارة، التي تزيل كلمة المرور الخاصة باتصال الكمبيوتر بخادم الإدارة. وبهذه الطريقة، تعمل المهمة على تعطيل حماية الاتصال بخادم الإدارة.

لتنفيذ هذا الأمر، يجب أن تكون الحماية بكلمة المرور ممكنة.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

كلمة المرور	
/password=<password>	كلمة مرور حساب مستخدم KLAdmin أو كلمة المرور من مهمة حماية الاتصال بخادم الإدارة. وإذا لم يتم تحديد المعلمة، فسيطالبك Kaspersky Endpoint Security بإدخال كلمة مرور في السطر التالي.

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 قواعد البيانات والوحدات النمطية للتطبيق.

يمكنك عرض قائمة أوامر KESCLI باستخدام أمر `kescli --help` أو باستخدام الأمر المختصر `kescli -h`.

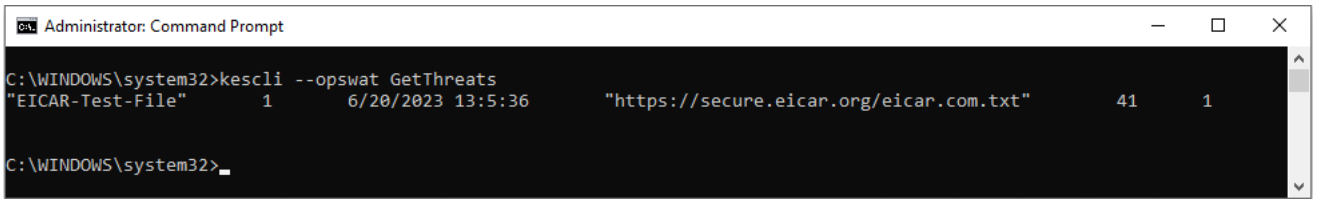
لإدارة برنامج Kaspersky Endpoint Security من سطر الأوامر:

1. قم بتشغيل سطر الأوامر الخاص بالمفسر (cmd.exe) كمسؤول.
2. انتقل إلى المجلد الذي يحتوي على الملف التنفيذي الخاص ببرنامج Kaspersky Endpoint Security.
   يمكنك إضافة مسار إلى الملف القابل للتنفيذ إلى متغير النظام %PATH% أثناء تثبيت التطبيق.

3. استخدم القالب التالي لتنفيذ الأمر:

```
kescli <command> [options]
```

وكنتيجة لذلك، سيقوم برنامج Kaspersky Endpoint Security بتنفيذ الأمر (اطلع على الشكل أدناه).



لإدارة التطبيق من سطر الأوامر

Scan. فحص البرامج الضارة

تشغيل مهمة فحص البرامج الضارة (فحص كامل).

لتشغيل المهمة، يجب على المسؤول السماح باستخدام المهام المحلية في السياسة.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

بناء جملة الأمر

```
<kescli --opswat Scan "<scan scope>" <action on threat detection
```

يمكنك التحقق من اكتمال حالة مهمة فحص البرامج الضارة باستخدام الأمر `GetScanState` وعرض التاريخ والوقت عند اكتمال الفحص الأخير باستخدام الأمر `GetLastScanTime`.

نطاق الفحص	
`<scan scope>`	قائمة مفصولة بمسافة من الملفات والمجلدات. على سبيل المثال، `"C:\Program Files (x86)\Example Folder"`.

الإجراء المطلوب اتخاذه عند اكتشاف تهديد	
`0`	**إعلام**. 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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف. 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

عرض معلومات عن حالة اكتمال مهمة فحص البرامج الضارة (فحص كامل):

- `1` – الفحص قيد التقدم.
- `0` – الفحص لا يعمل.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

بناء جملة الأمر

```
kescli --opswat GetScanState
```

GetLastScanTime. تحديد وقت إكمال الفحص

عرض معلومات عن تاريخ ووقت اكتمال مهمة فحص البرامج الضارة (فحص كامل) الأخيرة.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

بناء جملة الأمر

```
kescli --opswat GetLastScanTime
```

GetThreats. الحصول على بيانات عن التهديدات المكتشفة

عرض قائمة بالتهديدات المكتشفة (Report on threats). يحتوي هذا التقرير على معلومات عن التهديدات ونشاط الفيروسات خلال 30 يومًا الماضية قبل إنشاء التقرير.

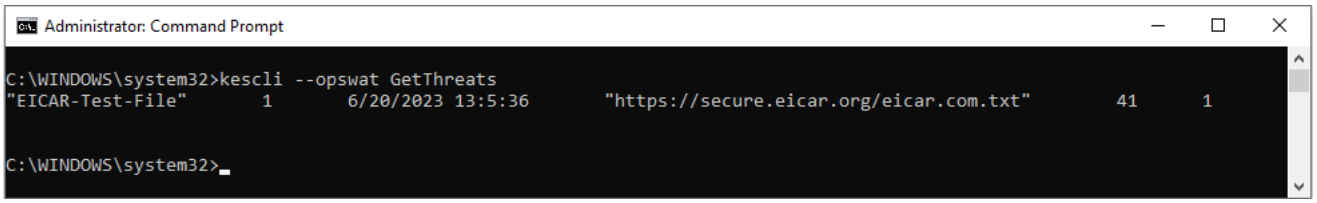
لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

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 (Phishing).
80	مرفق بريد إلكتروني غير مرغوب فيه (Attachment).
90	برنامج ضار تم اكتشافه بواسطة (Urgent) Kaspersky Security Network.
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

تشغيل مهمة تحديث قواعد البيانات والوحدات النمطية للتطبيق. يستخدم Kaspersky Endpoint Security المصدر الافتراضي: خوادم تحديث Kaspersky.

لتشغيل المهمة، يجب على المسؤول السماح باستخدام المهام المحلية في السياسة.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

لا يمكن تشغيل هذا الأمر في حالة تثبيت التطبيق في وضع Light Agent.

بناء جملة الأمر

```
kescli --opswat UpdateDefinitions
```

يمكنك عرض تاريخ ووقت إصدار قواعد بيانات مكافحة الفيروسات الحالية باستخدام الأمر `GetDefinitionsetState`.

GetDefinitionState. تحديد تاريخ ووقت آخر تحديث لقواعد البيانات

عرض معلومات عن تاريخ ووقت آخر تحديث لقواعد بيانات مكافحة الفيروسات المستخدمة.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

بناء جملة الأمر

```
kescli --opswat GetDefinitionState
```

EnableRTP. تمكين الحماية

تمكين 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).

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

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

عرض معلومات عن حالة مكون الحماية من تهديدات الملفات:

- `1` – تم تمكين المكون.
- `0` – تم تعطيل المكون.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

بناء جملة الأمر

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState. حالة تشفير القرص

عرض معلومات عن حالة تشفير القرص:

- يعني `1` أن القرص محمي بواسطة تقنية تشفير القرص من Kaspersky أو BitLocker.
- يعني `0` أن القرص غير مشفر.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

بناء جملة الأمر

```
kescli --opswat GetEncryptionState
```

Version. تحديد إصدار التطبيق

عرض إصدار Kaspersky Endpoint Security for Windows.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security.

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 تشغيل 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. استخدم القالب التالي لتنفيذ الأمر:

```
avp.com <command> [options]
```

كنتيجة لذلك، سوف ينفذ برنامج Kaspersky Endpoint Security الأمر.

SANDBOX. إدارة Sandbox

الأوامر لإدارة مكون Sandbox:

- تمكين أو تعطيل مكون Sandbox.

  توفر مكونات Sandbox التفاعل مع حل Kaspersky Sandbox ومكون KATA Sandbox، وهو جزء من Kaspersky Anti Targeted Attack Platform.

- تكوين مكون Kaspersky Sandbox:

  - توصيل الكمبيوتر بخوادم 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. للحصول على تفاصيل حول نشر الصور الافتراضية وتكوين خوادم Sandbox، راجع تعليمات Kaspersky Sandbox وتعليمات Kaspersky Anti Targeted Attack Platform.

  - تكوين مهلة الاتصال للخادم.

    انتهت مهلة الاتصال بخادم الحماية (لتطبيق Kaspersky Sandbox) أو خادم العقدة المركزية (لتطبيق KATA). بعد انقضاء المهلة التي تم تكوينها، يرسل Kaspersky Endpoint Security طلبًا إلى الخادم التالي. ويمكنك زيادة مهلة الاتصال لتطبيق Sandbox إذا كانت سرعة الاتصال لديك منخفضة أو إذا كان الاتصال غير مستقر. مهلة الطلب الموصى بها 0.5 ثانية أو أقل.

  - تكوين اتصال موثوق بين الكمبيوتر والخوادم.

    لتكوين اتصال موثوق به مع خادم الحماية (لتطبيق Kaspersky Sandbox) أو خادم العقدة المركزية (لتطبيق KATA)، يجب عليك إعداد شهادة TLS. ويجب عليك بعد ذلك إضافة الشهادة إلى الكمبيوتر باستخدام سياسة. وتحتاج أيضًا إلى إضافة الشهادة إلى خادم Sandbox (لتطبيق Kaspersky Sandbox) أو خادم العقدة المركزية (لتطبيق KATA).

  - تكوين وضع التكامل.

تحتاج إلى تحديد حل يمثل Sandbox جزءًا منه، أي Kaspersky Sandbox أو KATA Sandbox. Kaspersky Sandbox هو حل اكتشاف واستجابة مستقل بواسطة Kaspersky. KATA Sandbox هو مكون في حل Kaspersky Anti Targeted Attack Platform. وعند التكامل مع KATA Sandbox، يمكن أن يعمل المكون في الأوضاع التالية:

- **Manually**. يرسل المستخدم الملف يدويًا للفحص من قائمة السياق (**إرسال إلى Sandbox**).
- **Automatically**. يكتشف التطبيق تلقائيًا الكائنات ويرسلها إلى Sandbox للفحص.
- **Combined**.

- عرض الإعدادات الحالية للمكون.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-
   certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server
connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

العميلة	
`stop`	تعطيل مكون Sandbox.
`start`	تمكين مكون Sandbox.

`set`	تكوين مكون Sandbox. يمكنك تكوين الإعدادات التالية:
	• إضافة خوادم Sandbox (`--servers`)
	• إضافة شهادة TLS (`--pinned-certificate`)
	• إضافة حاوية تشفير (`--client-certificate`)
	• تحديد كلمة مرور لحاوية التشفير (`--client-certificate-password`)؛
	• ضبط مهلة اتصال الخادم (`--timeout`)
	• تحديد وضع تكامل (`--mode`):
	  • `KSB` - التكامل مع Kaspersky Sandbox؛
	  • `KATAManual` - التكامل اليدوي مع KATA Sandbox؛
	  • `KATAAuto` - التكامل التلقائي مع KATA Sandbox؛
	  • `KATAFull` - التكامل المشترك مع KATA Sandbox.

show	عرض الإعدادات الحالية للمكون. تحصل على الرد التالي: sandbox.timeout=<Sandbox server connection timeout (ms)> sandbox.servers=<list of Sandbox servers> sanbox.mode=<integration mode> sandbox.tls=<trusted connection status>

المصادقة	
/login=<user name> /password=<password>	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB
/login=login /password=password
```

PREVENTION. إدارة منع التنفيذ

تعطيل مكون منع التنفيذ أو عرض الإعدادات الحالية للمكون، بما في ذلك قائمة قواعد منع التنفيذ.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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).

ISOLATION. إدارة عزل شبكة الاتصال

تعطيل عزل شبكة الاتصال للكمبيوتر أو عرض الإعدادات الحالية للمكون. وتتضمن إعدادات المكونات أيضًا قائمة باتصالات الشبكة المضافة إلى الاستثناءات.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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

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 تكامله مع حلول Kaspersky Detection and Response. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل عن 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 وتعليمات Kaspersky Endpoint Detection and Response Expert (on-premises).

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 KATA (EDR)، 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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

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=samplePassword
```

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 IOC Scan. 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 IOC Scan العثور على مؤشرات الاختراق على الكمبيوتر واتخاذ إجراءات الاستجابة للتهديدات.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

يتم إلغاء فحص مؤشر الاختراق بعد 128 تطابقًا مع شرح مؤشرات الاختراق في ملفات مؤشر الاختراق. ويعد هذا ضروريًا للحد من عدد الإدخالات في تقرير فحص مؤشر الاختراق لتسهيل التحليل وحماية التقرير من الفائض بسبب مؤشرات الاختراق المصاغة بشكل غير دقيق التي قد تولد عددًا كبيرًا من التطابقات.

بناء جملة الأمر

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
 path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
      [/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
                [/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
            <all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

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 مؤشر الاختراق (IOC) مع معيار OpenIOC. على سبيل المثال، `C:\Users\Admin\Desktop\IOC`

نوع البيانات لفحص مؤشر الاختراق	
`/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 ProcessItem IOC موصوفًا في ملف IOC المتاح للفحص.
`/hint=<full path to the executable file of the process|full path to the file>`	حلل بيانات الملفات عند إجراء فحص مؤشرات الاختراق (ProcessItem وشروط FileItem). يمكنك تحديد ملف بإحدى الطرق التالية: • `<full path to the executable file of the process>` –شرط ProcessItem؛ • `<full path to the file>` – شرط FileItem.
`/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 RegistryItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security تسجيل Windows فقط إذا كان مستند RegistryItem IOC 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. إذا 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 DnsEntryItem IOC 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 ArpEntryItem IOC، فسيتم تجاهلها (يتم اكتشافها على أنها غير متطابقة). إذا لم يتم تحديد الوسيطة، يحلل Kaspersky Endpoint Security جدول ARP فقط إذا كان مستند ArpEntryItem IOC 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 PortItem IOC 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. إذا 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 كان ملف IOC يحتوي 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. بالنسبة لمصطلح IOC source \ EventLogItem ، استخدم القيمة **اسم المزود** من مخطط XML للحدث.
/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 (المعلمة Full Name 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 مؤشرات الاختراق المحدد بواسطة المستخدم عند تحليل البيانات لمستند مؤشرات الاختراق FileItem (`/drives=custom`). يمكنك تحديد مسارات متعددة مفصولة بمسافات.
/retro /<number of days>	فحص مؤشر الاختراق بأثر رجعي هو وضع لمهمة IOC Scan يفحص فيها Kaspersky Endpoint Security مؤشرات الاختراق باستخدام البيانات لفترة زمنية معينة. ويهدف هذا الوضع إلى البحث عن مؤشرات الاختراق عن طريق القياس عن بُعد للكمبيوتر المحمي مثل نشاط الشبكة والعمليات والملفات والقياس عن بُعد الآخر. يمكنك تعيين فترة زمنية من 1 إلى 14 يومًا. وبشكل افتراضي، يفحص التطبيق مؤشرات الاختراق ليوم واحد.
/network=on|off	تحليل بيانات الشبكة (مصطلح NetworkItem).
/url=on|off	تحليل البيانات في سجلات المستعرض (مصطلح UrlHistoryItem). يحلل فحص مؤشر الاختراق الاستعادي سجلات المستعرضات التالية: Google Chrome و Mozilla Firefox و Microsoft Edge (الإصدار 79 أو أحدث).
/email	تحليل كائنات البريد (مصطلح EmailItem).
/route	تحليل جداول التوجيه وإعادة التوجيه (مصطلح RouteEntryItem).

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 اكتشاف 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

إضافة 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 ().

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

`بناء جملة الأمر`

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

العميلة	
`/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=samplePassword
```

مثال

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA. تكامل EDR (KATA)

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.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
   <Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

العميلة	
`stop`	تعطيل مكون EDR (KATA).
`start`	تمكين مكون EDR (KATA).
`set`	تكوين مكون EDR (KATA). يمكنك تكوين الإعدادات التالية: • إضافة خوادم العقدة المركزية (`servers=<server address>:<port>`) • إضافة شهادة TLS (`server-certificate=<path to the TLS certificate>`) • ضبط مهلة اتصال خادم Central Node (`/timeout=<Central Node server connection timeout (s)>`) • تعيين فترة المزامنة مع خادم Central Node (`/sync-period=<Central Node server synchronization period (min)>`)
`show`	عرض الإعدادات الحالية للمكون.

EDRExpertOnPrem. تكامل EDR Expert (on-premises)

أوامر لإدارة العميل المضمن لتكوين تكامل Kaspersky Endpoint Detection and Response Expert (on-premises):

- تمكين أو تعطيل عميل EDR Expert (on-premises) المدمج.
- تكوين إعدادات الاتصال لخوادم EDR Expert (on-premises).
- عرض الإعدادات الحالية للعميل المدمج.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com START EDRExpertOnPrem
```

```
avp.com STOP EDRExpertOnPrem
```

```
avp.com EDRExpertOnPrem /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate>
     [/client-certificate=<path to the PFX archive> /client-certificate-password=<password to the PFX archive>]
   [/timeout=<server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
 /telemetry-servers=<server address:port> /telemetry-server-certificate=<path to the TLS certificat> [telemetry-
client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>]
       [/telemetry-timeout=<server connection timeout (s)>] [/events-send-period=<seconds>] [/events-limit=<0|1>]
  [/events-per-hour=<number of events>] [/max-packet-length=<number of packets>] [/telemetry-only-tagged-events=
                                                                    <<0|1>] login=<user name> password=<password
```

```
avp.com EDRExpertOnPrem /show
```

العملية	الوصف
`stop`	تعطيل عميل EDR Expert (on-premises) المدمج.
`start`	تمكين عميل EDR Expert (on-premises) المدمج.

`set`	تكوين عميل EDR Expert (on-premises) المدمج. يمكنك تكوين إعدادات الاتصال التالية لخوادم الاستجابة: • `servers=<server address>:<port>`. عنوان خادم الاستجابة (FQDN، IPv4، IPv6). • `server-certificate=<path to the TLS certificate>`. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). • `client-certificate=<path to the PFX archive> client-certificate-password=<password to the PFX archive>`. استخدم حاوية تشفير للمصادقة ثنائية الاتجاه. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص بتنسيق PKCS#12. ولتمكين هذه المصادقة، تحتاج إلى إنشاء حاوية تشفير في هيئة تصديق خارجية. • `timeout=<server connection timeout (s)>`. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف. • `sync-period=<server synchronization period (min)>`. عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يتلقى Kaspersky Endpoint Security مهام الاستجابة للتهديدات ويرسل نتائج المهام. يمكنك تكوين إعدادات الاتصال التالية لخوادم جمع القياس عن بُعد: • `telemetry-servers=<server address:port>`. عنوان خادم جمع القياس عن بُعد (FQDN، IPv4، IPv6). • `telemetry-server-certificate=<path to the TLS certificat>`. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). • `telemetry-client-certificate=<path to the PFX archive> telemetry-client-certificate-password=<password to the PFX archive>`. استخدم حاوية تشفير للمصادقة ثنائية الاتجاه. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص بتنسيق PKCS#12. ولتمكين هذه المصادقة، تحتاج إلى إنشاء حاوية تشفير في هيئة تصديق خارجية. • `telemetry-timeout=<server connection timeout (s)>`. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف. • `events-send-period=<seconds>`. الحد الأقصى للتأخير عند إرسال الأحداث. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية. • `events-limit=<0|1>`. تحديدعدد الطلبات. تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث. • `events-per-hour=<number of events>`. 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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 حدث في الساعة. • `max-packet-length=<number of packets>`. أقصى طول للحزمة. يتزامن التطبيق مع الخادم عندما يمتلئ المخزن المؤقت بالأحداث. الإعداد الافتراضي هو 1024 حدثًا. • `telemetry-only-tagged-events=<0|1>`. إرسال القياس عن بُعد باستخدام مؤشر الهجوم (IOA) فقط. مؤشر الهجوم (IOA) هو قاعدة تحتوي على وصف لسلوك مشبوه في النظام مما قد يشير إلى هجوم موجه. ويقارن التطبيق السلوك الجاري في النظام مع هذه القواعد ويسجل الأحداث التي تشير إلى هجوم موجه. ويستخدم التطبيق تقنية فحص البث التي تتيح تتبع مثل هذه الأحداث في الوقت الحقيقي. يمكنك تكوين الإعدادات العامة التالية: • `mode=EDRKATA | EDRExpertOnPrem`. التبديل بين الحلول: • [segment already translated...source not re-sent] • Endpoint Detection and Response Expert (version 8.0 or later). `EDRExpertOnPrem`. القيمة الافتراضية. • `login=<user name> password=<password>`. بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.
`show`	عرض الإعدادات الحالية للمكون.

KUMA. تكامل KUMA

الأوامر الخاصة بإدارة عميل KUMA المدمج:

- تمكين أو تعطيل تكامل KUMA.

  يوفر عميل KUMA المدمج إمكانية التشغيل البيني مع حل Kaspersky Unified Monitoring and Analysis Platform.

- تكوين الاتصال بخوادم Kaspersky Unified Monitoring and Analysis Platform.

- عرض الإعدادات الحالية للمكون.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

العميلة	
stop	تعطيل تكامل KUMA.
start	تمكين تكامل KUMA.
set	تكوين عميل KUMA المدمج. يمكنك تكوين الإعدادات التالية: • إضافة خوادم KUMA (/<servers=<protocol>://<server address>:<port>) يدعم التطبيق بروتوكولات الاتصال بالخادم التالية: tcp و udp و http و https. • إضافة شهادة TLS (/server-certificate=<path to the TLS certificate>) • ضبط مهلة اتصال الخادم (/timeout=<KUMA server connection timeout (s)>) • إضافة حاوية تشفير (/client-certificate=<path to the crypto-container> /client-certificate-password=<password>) • تكوين تأخير إرسال الحدث (/maximum-data-transfer-time=<maximum events transmission delay (sec)>
show	عرض الإعدادات الحالية للمكون.

المصادقة	
/login=<user name> /password=<password>	بيانات اعتماد حساب المستخدم مع أذونات حماية كلمة المرور المطلوبة.

مثال

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA. تشغيل فحص YARA

تشغيل مهمة تشغيل فحص YARA. يفحص التطبيق الملفات والكائنات بحثًا عن مؤشرات للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في الشركة باستخدام قواعد بيانات قواعد YARA. قواعد YARA هي أوصاف لتوقيعات الهجمات المستهدفة وحالات التسلل في البنية التحتية لتكنولوجيا المعلومات للشركة التي يستخدمها Kaspersky Endpoint Security لفحص الكائنات.

لتشغيل فحص YARA، يجب عليك تجهيز ملفات YARA التي تصف القواعد. وعند إنشاء ملفات YARA، ضع في اعتبارك المتطلبات التالية:

- يدعم Kaspersky Endpoint Security ملفات YARA بامتدادات YAR. التي تتبع المعيار المفتوح YARA 4.2.3 لوصف مؤشرات الاختراق.
- يمكن فقط تحديد الملفات التي تحتوي على قواعد YARA للمهمة. ولا تدعم مهمة تشغيل فحص YARA أنواع القواعد الأخرى.
- إذا أضفت ملفات YARA لا يدعمها Kaspersky Endpoint Security، أو إذا كانت القواعد تحتوي على أخطاء في بناء الجملة، فسيتم إنهاء المهمة مع ظهور رسالة الخطأ المقابلة.
- يجب أن تكون معرفات كل ملفات YARA المستخدمة في فحص فردي فريدة. وإذا كانت هناك ملفات YARA بالمعرف نفسه، فقد تؤثر على نتائج تنفيذ المهمة.
- يتم إلغاء فحص YARA بعد 128 تطابقًا مع المؤشرات الموضحة في قواعد YARA. ويعد هذا ضروريًا للحد من عدد الإدخالات في تقرير فحص YARA لتسهيل التحليل وحماية التقرير من الفائض بسبب قواعد YARA المصاغة بشكل غير دقيق التي قد تولد عددًا كبيرًا من التطابقات.

توصي Kaspersky بإنشاء قاعدة واحدة لكل ملف YARA. ويجعل هذا نتائج الفحص أكثر قابلية للقراءة.

قد يستغرق فحص YARA قدرًا كبيرًا من الوقت. وبناءً على حجم محرك الأقراص وإعدادات المهمة وعدد الكائنات الموجودة على القرص، يمكن أن يستمر فحص YARA في أي مكان من عدة دقائق إلى عدة ساعات. ولا يعرض التطبيق مؤشر تقدم. ولا يمكن إيقاف أو إلغاء فحص YARA. ويُنصح بالانتظار حتى تتوفر نتائج فحص YARA.

بناء جملة الأمر

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

ملفات YARA	
<full path to the YARA file>	المسار الكامل إلى ملف YARA الذي تريد استخدامه للفحص. يمكنك تحديد المسارات إلى ملفات YARA متعددة مفصولة بمسافات. الوسيطة المطلوبة في حالة عدم تحديد القيمة /path=<path to the folder with YARA files>. مثال: C:\Users\Admin\Desktop\YARA\file1.yar C:\Users\Admin\Desktop\YARA\file2.yar
/path=<path to the folder with YARA files>	المسار الكامل إلى مجلد يحتوي على ملفات YARA التي تريد استخدامها للفحص. الوسيطة المطلوبة في حالة عدم تحديد القيمة <full path to the YARA file>. مثال: /path=C:\Users\Admin\Desktop\YARA

إعدادات متقدمة	
/fastScan=<on|off>	فحص YARA السريع. لكل كائن، يسجل التطبيق تكرارًا واحدًا للمؤشر المكتشف. ويخفي التطبيق أيضًا تكرارات المؤشرات المكتشفة في السجل. ويتيح فحص YARA السريع فحص الملفات الكبيرة بشكل أسرع. إذا لم يتم تحديد هذا الإعداد، فسوف يُجري التطبيق فحص YARA قياسيًا. وفي هذا الوضع، يسجل التطبيق تكرارات المؤشرات المكتشفة.
/maxRules=<maximum number of scan rules>	حد عدد القواعد الفريدة التي يتم تشغيلها التي تجعل التطبيق يوقف فحص YARA عند الوصول إليه. إذا لم يتم تحديد قيمة هذا الإعداد أو في حالة تحديد 0، يُجري التطبيق فحص YARA بدون قيود.
/timeOut=<stop scan after the specified time in seconds>	ما المدة التي يمكن أن يستغرقها فحص YARA، بالثواني. عند نفاد هذا الوقت، يوقف التطبيق فحص YARA. إذا لم يتم تحديد قيمة هذا الإعداد أو في حالة تحديد 0، يُجري التطبيق فحص YARA بدون قيود.
/recursive=<on|off>	تبدأ هذه الوسيطة فحصًا تكراريًا للمجلدات الفرعية داخل مسار الفحص المخصص /scanFolders.
/scanFolders=<list of folders to be scanned>	تبدأ هذه الوسيطة فحص YARA للملفات الموجودة في قائمة المجلدات المحددة. يمكنك تحديد قيم متعددة مفصولة بمسافات. يدعم Kaspersky Endpoint Security حرفي * و ? عند إدخال قناع مسار مجلد. إذا لم يتم تحديد هذا الإعداد، فسوف يُجري التطبيق فحص YARA لجميع الأقراص المحلية باستثناء المجلدات المشتركة على الشبكة ومحركات الأقراص السحابية والوسائط القابلة للإزالة.
/scanMemory=<on|off>	فحص ذاكرة كل العمليات الجارية.
/scanProcess=<process name>	فحص الذاكرة فقط لعمليات محددة. حدد مسارات كاملة مفصولة بمسافات لملفات العمليات القابلة للتنفيذ. ويمكنك أيضًا استخدام حرفي * و ? لإدخال قناع.
/maxSize=<file size in bytes>	تقييد حجم الملف لفحص YARA. يتخطى التطبيق الملفات الأكبر حجمًا.
includes=<list of objects to be scanned>/	تحرير نطاق الفحص. يمكنك تحديد قيم متعددة مفصولة بمسافات. تتوافر القيم التالية: • اسم الملف • ملحق الملف يجب تحديد نطاق الفحص بمعلمة /scanFolders. مثال: /scanFolders C:*.* /includes=*.exe *.dll – يفحص التطبيق جميع الملفات بامتدادات EXE وDLL على القرص C.
/excludes=<list of objects to be scanned>	استثناء الملفات من فحص YARA. يمكنك تحديد قيم متعددة مفصولة بمسافات. تتوافر القيم التالية: • مسار الملف • قناع مسار الملف يجب تحديد الاستثناءات بمعلمة /scanFolders. مثال: /scanFolders C:*.* /excludes readme.txt C:\trusted*.* *.xml – يتخطى التطبيق ملف readme.txt، وكل الملفات الموجودة في المجلد C:\trusted، وكل الملفات التي تحمل الامتداد XML. في المجلد الرئيسي للقرص C.
/scanAutoruns=<on|off>	فحص YARA لكائنات نقطة التشغيل التلقائي.
/excludeAutoruns=<list of autorun point areas to skip>	استثناء كائنات نقطة التشغيل التلقائي من نطاق الفحص. حدد مسارات كاملة مفصولة بمسافات لملفات العمليات القابلة للتنفيذ. ويمكنك أيضًا استخدام حرفي * و ? لإدخال قناع.
/logFolder=<path to the folder for saving the scan results in a TXT file>	إذا حددت مسارًا لمجلد ، فإن التطبيق يحفظ نتائج الفحص في المسار المحدد في ملف يسمى yara_<computer name>_<scan completion time>.txt. إذا حددت مسارًا إلى ملف TXT معين، يحفظ التطبيق نتائج الفحص في هذا الملف. علي سبيل المثال: /logFolder=C:\test أو /logFolder=C:\test\abc.txt. يتم إخراج نتائج الفحص إلى سطر الأوامر بغض النظر عما إذا كان خيار /logFolder قد تم تحديده.

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.
- `5` يعني أنه لم يتم العثور على ملف واحد أو أكثر بقواعد YARA المحددة في المعلمة.

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:

`Started at <time>` `Finished at <time>`	وقت البدء ووقت إكمال الفحص.
`Host name: <computer name>`	اسم الكمبيوتر الذي تم اكتشاف الكائن عليه.
`Result: <error>`	رمز الخطأ للخطأ الذي حدث أثناء تشغيل المهمة. إذا لم تكن هناك أخطاء، فسوف يُخرج التطبيق `0x00000000`.
`Comment: <comment text>`	وصف الخطأ للخطأ الذي حدث أثناء تشغيل المهمة. على سبيل المثال، `Operation timeout`.
`Object Name:` أو `Process:` (عند فحص ذاكرة العملية)	اسم الكائن أو العملية التي تم تشغيل قاعدة YARA عليها.
`Md5: <md5 hash>` `Sha256: <sha256 hash>`	تجزئات الكائن الذي يتم تشغيل قاعدة YARA عليه.
`Rule Name`	اسم قاعدة YARA التي تم تشغيلها.

`:Meta`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	البيانات الوصفية المحددة في قاعدة YARA.

`:Detects`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	تم العثور على تطابقات داخل الكائن تلبي شروط قاعدة YARA:
	• الإزاحة في ذاكرة العملية أو الملف حيث تم اكتشاف تطابق (`Offset`).
	• اسم السلسلة المطابقة في قاعدة YARA (`String name`).
	• السلسلة المطابقة في ذاكرة العملية أو الملف (`String data`).

عوامل تصفية القياس عن بُعد. يتم إرسال أحداث التصفية إلى KUMA

بشكل افتراضي، يتم تعطيل إرسال الأحداث إلى خادم KUMA. وللتأكد من عمل KUMA بشكل صحيح، يجب تمكين إرسال القياس عن بُعد. ويمكنك تحديد مصدر حدث من بين السجلات القياسية: Application أو Security أو System. ولتحسين الأداء وزيادة كفاءة إرسال البيانات إلى خادم KUMA، يمكنك إضافة أو استبعاد الأحداث الفردية يدويًا من بيانات القياس عن بعد. على سبيل المثال، يمكنك استبعاد أحداث Sysmon.

يمكنك تصدير قائمة الاستثناءات إلى ملف JSON من سطر الأوامر.

إذا كان الأمر يحتوي فقط على اسم الملف الذي تريد تصدير الإعدادات إليه، فإن التطبيق يضع الملف كما يلي:

- إذا تمت إضافة المسار إلى avp.com إلى متغير النظام %PATH%، يضع التطبيق الملف في المجلد `C:\Windows\SysWOW64`.
- إذا قمت بتشغيل الأمر من مجلد تثبيت التطبيق، فسيفشل التصدير لأن الحماية الذاتية للتطبيق تمنع إنشاء ملف جديد في مجلد التطبيق. ولتصدير إعدادات التطبيق إلى ملف، أدخل مسار الملف.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
<avp.com TELEMETRYFILTERS /export <file name
```

```
<avp.com TELEMETRYFILTERS /import <file name
```

العميلة	
`export`	تصدير عوامل تصفية الأحداث التي سيتم إرسالها إلى KUMA.
`import`	استيراد عوامل تصفية الأحداث التي سيتم إرسالها إلى KUMA. في حالة وجود قواعد تصفية الأحداث بالفعل على جهاز الكمبيوتر، يقوم Kaspersky Endpoint Security باستبدالها عند الاستيراد.

ملف للتصدير أو الاستيراد	
`<file name>`	سيتم إرسال اسم الملف مع عوامل تصفية الأحداث إلى KUMA. ويمكنك أيضًا إدخال مسار الملف. ويمكنك تصدير عوامل التصفية لإرسالها إلى KUMA إلى ملف JSON.

أوامر إدارة Light Agent

يمكنك إدارة التطبيق في Light Agent لحماية البيئات الافتراضية في سطر الأوامر. ويمكنك إدارة التطبيق في وضع Light Agent إذا كانت الإدارة باستخدام وحدة تحكم Kaspersky Security Center غير ممكنة. يمكنك استعراض قائمة الأوامر لإدارة التطبيق من خلال تشغيل الأمر `HELP`. للقراءة عن بناء الأمر لأمر محدد، قم بإدخال `HELP <command>`.

لإدارة التطبيق في وضع Light Agent 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. استخدم القالب التالي لتنفيذ الأمر:

```
avp.com <command> [options]
```

كنتيجة لذلك، سوف ينفذ برنامج Kaspersky Endpoint Security الأمر.

يدعم التطبيق المثبت في وضع Light Agent تقريبًا جميع أوامر AVP للتطبيق المثبت في الوضع القياسي. وفي وضع Light Agent، تكون مهام تحديث قاعدة بيانات مكافحة الفيروسات ومهام إدارة مفتاح الترخيص محدودة.

KSVLAINFO. تحديد وضع Light Agent

تحديد وضع Light Agent.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com KSVLAINFO
```

يؤدي الأمر إلى إخراج المعلومات التالية إلى وحدة التحكم:

- وضع Light Agent لحماية البيئات الافتراضية: تم التمكين أو تم التعطيل.

  في حالة تمكين وضع Light Agent، يتم استخدام التطبيق كجزء من حل Kaspersky Security for Virtualization Light Agent.

- وضع حماية VDI: تم التمكين أو تم التعطيل.

  يساعد وضع حماية VDI على تحسين أداء Kaspersky Endpoint Security على الأجهزة الافتراضية غير الدائمة. إذا تم تمكين وضع حماية VDI، فلن يتم تثبيت التحديثات التي تتطلب إعادة تشغيل الجهاز الافتراضي المحمي على الأجهزة الافتراضية غير الدائمة. وعند تلقي تحديثات تتطلب إعادة تشغيل، يرسل Light Agent المثبت على جهاز افتراضي غير دائم رسالة إلى Kaspersky Security Center لإعلامه بضرورة تحديث قالب الجهاز الافتراضي المحمي.

- نوع الجهاز الافتراضي المحمي: دائم أو غير دائم.

- دور الجهاز الافتراضي المحمي في البنية التحتية الافتراضية: خادم أو محطة عمل.

- المعرف: UUID.

VIISINFO. حالة اتصال Light Agent بخادم التكامل

عرض معلومات عن اتصال Light Agent بخادم التكامل.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com VIISINFO
```

يؤدي الأمر إلى إخراج المعلومات التالية إلى وحدة التحكم:

- عنوان ومنفذ خادم التكامل الذي يتصل به Light Agent.
- حالة اتصال خادم التكامل.
- تاريخ ووقت آخر اتصال لوضع Light Agent بخادم التكامل.

SVMINFO. حالة اتصال Light Agent بخادم الحماية

عرض معلومات حول اتصال Light Agent بخادم الحماية.

لتشغيل الأمر، انتقل إلى المجلد الذي يحتوي على ملف القابل للتنفيذ الخاص ببرنامج Kaspersky Endpoint Security. ويمكنك أيضًا إضافة مسار الملف القابل للتنفيذ إلى متغير النظام %PATH% وتشغيل الأمر دون الانتقال إلى مجلد التطبيق.

بناء جملة الأمر

```
avp.com SVMINFO
```

يؤدي الأمر إلى إخراج المعلومات التالية إلى وحدة التحكم:

- عنوان SVM الذي يتصل به Light Agent، وموقع SVM في البنية التحتية الافتراضية بالنسبة إلى Light Agent: محلي أو غير محلي.
- طريقة اكتشاف SVM التي يستخدمها Light Agent: استخدام خادم تكامل أو استخدام قائمة مخصصة بعناوين SVM.
- قائمة بعناوين SVM في حالة تحديد قائمة عناوين SVM كطريقة اكتشاف SVM.
- علامة لتوصيل Light Agent بجهاز SVM.
- خوارزمية تحديد SVM: قياسية أو موسعة. في حالة استخدام خوارزمية تحديد SVM الموسعة، يتم أيضًا عرض نوع مسار SVM في البنية التحتية الافتراضية.
- حالة حماية الاتصال بين Light Agent وخادم الحماية.

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، `Error: Cannot start task '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

رمز الخطأ	الوصف
89479004	البيانات تالفة
89479005	ملف المفتاح تالف
89479006	انتهت صلاحية الترخيص
89479007	لم يتم تحديد ملف المفتاح
89479008	ملف مفتاح غير صالح
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	المفتاح غير مناسب لهذا 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

رمز الخطأ	الوصف
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

رمز الخطأ	الوصف
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	لا تتوافق أنواع التراخيص مع المفاتيح الفعالة ولا تتطابق المفاتيح الاحتياطية
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 داخلي بالخادم
89479403	لا يتوافر مفتاح لرمز التفعيل الذي تم إدخاله

رمز الخطأ	الوصف
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 مستخدم 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`. 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.
- `AntiCryptor`
- `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` - التراجع عن التحديث (لا يمكن تطبيق ملف التعريف في حالة تثبيت التطبيق في وضع Light Agent)
- `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 (لا يمكن تطبيق ملف التعريف في حالة تثبيت التطبيق في وضع Light Agent)
- `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 وثائق 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:
     `KEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestApi`
  3. أدخل مسار الشهادة، على سبيل المثال، `Certificate = C:\Folder\cert.pem`.
  4. تمكين الدفاع الذاتي لبرنامج Kaspersky Endpoint Security.
  5. 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 وثائق 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

يصف هذا القسم مصادر المعلومات المتعلقة بالتطبيق.

يمكنك اختيار المصدر الأكثر ملاءمة للمعلومات اعتمادًا على أهمية وإلحاح مشكلتك.

صفحة Kaspersky Endpoint Security على موقع ويب Kaspersky

على صفحة Kaspersky Endpoint Security، يمكنك الاطلاع على معلومات عامة عن التطبيق ووظائفه وميزاته.

تحتوي صفحة Kaspersky Endpoint Security على رابط إلى متجر الإنترنت. وهنا يمكنك شراء أو تجديد التطبيق.

صفحة Kaspersky Endpoint Security في قاعدة المعارف

قاعدة المعارف هي قسم علي موقع ويب الدعم الفني.

يمكنك من خلال صفحة Kaspersky Endpoint Security في قاعدة المعارف قراءة المقالات التي توفر معلومات وتوصيات وإجابات مفيدة للأسئلة المتداولة حول كيفية شراء التطبيق وتثبيته واستخدامه.

بإمكان المقالات الموجودة في قاعدة المعارف الإجابة على الأسئلة المتعلقة بتطبيق Kaspersky Endpoint Security وكذلك تطبيقات Kaspersky الأخرى. وأيضًا قد تحتوي المقالات الموجودة في قاعدة المعارف على أخبار من الدعم الفني.

مناقشة عن تطبيقات Kaspersky في منتدى المستخدمين

إذا كان تساؤلك لا يتطلب ردًا عاجلاً، يمكنك مناقشته مع خبراء Kaspersky ومع المستخدمين الآخرين في المنتدى الخاص بنا.

يمكنك استعراض الموضوعات الموجودة في هذا المنتدى وكتابة تعليقاتك الخاصة وإنشاء موضوعات جديدة واستخدام محرك البحث.

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 حذفها نهائيًا عند إزالة التطبيق.

يتم حفظ ملفات التتبع، باستثناء تلك الخاصة بوكيل المصادقة، في المجلد `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

يتم تسمية ملفات التتبع على النحو التالي: `trace file type>.log><.KES<14.2_dateXX.XX_timeXX.XX_pidXXX`.

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.

محتويات ملفات التتبع SRV.log، وGUI.log، وALL.log

قد تُخزن 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: `PERF.HAND.etl<.KES<14.2_dateXX.XX_timeXX.XX_pidXXX`.

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

بالإضافة إلى البيانات العامة، يحتوي ملف التتبع `AMSI.log` على معلومات عن 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 مجلد System Volume Information ويسمى على النحو 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. وأثناء عملية التتبع، ينشئ التطبيق مجموعة من الملفات ذات تتضمن بيانات حول تشغيل مكونات التطبيق المختلفة (على سبيل المثال، SRV.log وWD.log وغيرهما).

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 تقييد الحجم**. احفظ عمليات التتبع لعدد محدود من مجموعات الملفات التي لها حجم محدود واستبدل الملفات الأقدم عند الوصول إلى الحد الأقصى للحجم. في حالة تحديد هذا الوضع، يمكنك تحديد الحد الأقصى من مجموعات الملفات للتدوير والحجم الأقصى لكل مجموعة ملفات.

  بشكل افتراضي ، يحفظ التطبيق خمس مجموعات من ملفات التتبع. ويبلغ حجم كل مجموعة من الملفات 3072 ميجابايت. وبهذه الطريقة، تحتاج إلى 15 جيجا بايت من مساحة القرص الخالية لحفظ ملفات التتبع.

- **بدون قيود**. احفظ ملف تتبع واحد (لا يوجد حد للحجم).

5. في القائمة المنسدلة **المستوى**، حدد مستوى التتبع:

- يعني **عادي** أن ملف التتبع يحفظ الرسائل عن جميع الأخطاء والتحذيرات، بالإضافة إلى المعلومات عن التشغيل العادي للتطبيق (افتراضي).
- يعني **تفصيلي** أن ملف التتبع يحفظ جميع المعلومات عن تشغيل التطبيق.

تتوفر مستويات تتبع إضافية إذا قمت بإدارة إعدادات تتبع التطبيق في سطر الأوامر. يُنصح بتوضيح مستوى التتبع المطلوب لاختصاصي الدعم الفني. في غياب توجيه الدعم الفني، حدد مستوى التتبع إلى **عادي**.

إذا تم تمكين تتبع التطبيق في سطر الأوامر وتم تعيين مستوى تتبع بخلاف **عادي** أو **تفصيلي**، يتم تعيين القائمة المنسدلة **المستوى** على **عادي**.

6. 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 ملفات تتبع تشغيل التطبيق في المجلد `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`. وبعد إنشاء ملفات التتبع، أرسل الملفات 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 وإيقاف 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 تقييد الحجم**. 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.
- **بدون قيود**. 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.14.2\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 كمبيوتر طالما أن التطبيق قيد الاستخدام ويتم خذفها نهائيًا عند إزالة التطبيق. يتم تخزين ملفات التفريغ في المجلد `%ProgramData%\Kaspersky Lab\KES.14.2\Traces`.

كيفية تمكين كتابة التفريغ في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.

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

3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.

4. في القسم **معلومات التصحيح**، انقر على الزر **الإعدادات**.

5. في النافذة التي تفتح، استخدم خانة الاختيار **تمكين كتابة التفريغ** لتمكين أو تعطيل كتابة تفريغ التطبيق.

6. احفظ تغييراتك.

كيفية تمكين كتابة التفريغ في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Technical Support**.
5. في القسم **Debug information**، استخدم خانة الاختيار **Dump writing ENABLED** لتمكين كتابة تفريغ التطبيق أو تعطيله.
6. احفظ تغييراتك.

كيفية تمكين تفريغ الكتابة 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 **معلومات التصحيح**، 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.

كيفية تمكين حماية ملفات التفريغ وملفات التتبع في وحدة تحكم الإدارة (MMC)

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد **Policies**.
2. حدد السياسة اللازمة وانقر نقرًا مزدوجًا لفتح خصائص السياسة.
3. في نافذة السياسة، حدد **الإعدادات العامة** ← **إعدادات التطبيق**.
4. في القسم **معلومات التصحيح**، انقر على الزر **الإعدادات**.
5. في النافذة التي تفتح، استخدم خانة الاختيار **تمكين حماية ملفات التفريغ والتتبع** لتمكين أو تعطيل حماية الملفات.
6. احفظ تغييراتك.

كيفية تمكين حماية ملفات التفريغ وتتبع الملفات في Web Console وCloud Console

1. في نافذة Web Console الرئيسية، حدد **Policies** ← **Asset management**.
2. انقر فوق اسم سياسة Kaspersky Endpoint Security.
   فتح نافذة خصائص السياسة.
3. حدد علامة التبويب **Application settings**.
4. انتقل إلى **General Settings** ← **Technical Support**.
5. في القسم **Debug information**، استخدم خانة الاختيار **Dump and trace files protection ENABLED** لتمكين حماية الملفات أو تعطيلها.
6. احفظ تغييراتك.

كيفية تمكين حماية ملفات التفريغ وتتبع الملفات 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 **معلومات التصحيح**، 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.

الحصول على بيانات نظام التشغيل (الحصول على معلومات النظام من Kaspersky)

بعد تثبيت تطبيق Kaspersky Endpoint Security، قد لا يعمل نظام التشغيل أو التطبيق بشكل صحيح. ويوجد تعارض بين التطبيق والبرامج أو برامج تشغيل مكونات الكمبيوتر.

لتحديد سبب المشكلة، يطلب الدعم الفني من Kaspersky تقريرًا من الأداة المساعدة Kaspersky Get System Info (المشار إليها فيما يلي باسم GSI). وللحصول على معلومات تفصيلية عن استخدام الأداة المساعدة، ارجع إلى قاعدة معارف Kaspersky.

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.
- في خصائص مهمة تغيير مكونات التطبيق عند تبديل وضع التثبيت (**الوضع المنفصل / الوضع المشترك**)، لا يتم دعم مزامنة مجموعة المكونات بين الأوضاع. ويزامن التطبيق مجموعة المكونات بين الأوضاع بعد إعادة فتح خصائص المهمة.
- 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 Kaspersky Endpoint Security، فابدأ استعادة التطبيق 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 Endpoint Security for Windows (KES) على خادم مُثبت عليه Kaspersky 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.

- يتوفر الترحيل من Kaspersky Small Office Security (KSOS) إلى Kaspersky Endpoint Security (KES) مع تمكين الحماية بكلمة مرور بدءًا من الإصدار 21.16 من KSOS. لترحيل الإصدارات السابقة من KSOS، يجب عليك تعطيل الحماية بكلمة مرور أو إزالة KSOS يدويًا. يتم تنفيذ الترحيل من KSOS إلى KES مع تعطيل الحماية بكلمة مرور بشكل صحيح.

- لا يمكنك تثبيت Kaspersky Endpoint Security على محرك أقراص قابل للإزالة قابل للتمهيد. عند التثبيت، يعرض Kaspersky Endpoint Security رسالة خطأ: قمت بتحديد مجلد أو محرك غير صحيح. يجب تثبيت التطبيق على قرص ثابت محلي. وإذا تمكنت من تثبيت التطبيق على محرك أقراص قابل للإزالة باستخدام أدوات خاصة بجهة خارجية، فقد يتسبب ذلك في تعطل نظام التشغيل (BSOD) أثناء عملية التمهيد. وهذا يعني أن Kaspersky Endpoint Security لا يدعم Windows To Go والحلول المماثلة. ولفحص كمبيوتر من محرك أقراص قابل للإزالة، يمكنك استخدام الإصدار المجاني من تطبيق قرص الإنقاذ من Kaspersky.

- يتطلب تثبيت Kaspersky Endpoint Security مع مكونات الشبكة على خادم محطة طرفية يدعم جلسات RDP متعددة المستخدمين مراعاة بعض الأمور الخاصة. وتفرض أنظمة التشغيل على جميع جلسات عمل المستخدم الإنهاء بعد انتهاء جلسة المسؤول. وللاتصال بخادم المحطة الطرفية، يجب إعادة تشغيل الخادم أو تسجيل الدخول إلى النظام محليًا. ويتم تحديد هذا السلوك من خلال خصوصيات كيفية عمل نظام التشغيل Windows.

- في حالة تثبيت المكونات الإضافية للويب لتطبيق Kaspersky Endpoint Security for Windows (الإصدار 12.11.0.2004) وKaspersky Endpoint Security for Linux (الإصدار 12.4.0.1354) في Kaspersky Security Center 16.0 أو Kaspersky Security Center 16.1، فإن تحديث المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security for Windows إلى الإصدار 12.11.0.6004 قد يؤدي إلى حدوث أعطال في سياسات Kaspersky Endpoint Security for Linux.

  الحل المحتمل: انتقل إلى **Settings** ← **Web plug-ins**، وقم بإزالة المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security for Windows والمكوّن الإضافي للويب لتطبيق Kaspersky Endpoint Security for Linux وKaspersky Unified Protection and Management Plug-in من القائمة. وبعد ذلك، قم بتثبيت المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security for Linux أولاً، متبوعًا بالمكون الإضافي للويب لتطبيق Kaspersky Endpoint Security for Windows .

- في Web Console، يتم عرض قائمة المكونات بشكل غير صحيح في خصائص حزمة تثبيت Kaspersky Endpoint Security 12.11 for Windows. ولا يتوفر مكون منفصل، مكافحة التشفير، في هذا الإصدار من التطبيق. ويتم تضمين حماية المجلدات المشتركة ضد وظيفة التشفير الخارجي في مكون اكتشاف السلوك. وفي Kaspersky Endpoint Security 12.12 for Windows، تعد هذه الوظيفة مكونًا منفصلاً. وفي الوقت نفسه، في وحدة تحكم الإدارة (MMC)، يتم عرض قائمة المكونات بشكل صحيح.

- عند استخدام المكون الإضافي للويب، الإصدار 7.0 أو أحدث، تظهر قائمة المكونات المحددة للتثبيت افتراضيًا بشكل غير صحيح في خصائص حزمة التثبيت الخاصة ببرنامج Kaspersky Endpoint Security 14.1 والإصدارات السابقة. وإذا لم يتم تعديل هذه القائمة عند إنشاء حزمة التثبيت، فسيتم تثبيت التطبيق باستخدام مجموعة المكونات الافتراضية المحددة لإصدار التطبيق المقابل.

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 تحديث قواعد البيانات والوحدات النمطية للتطبيق وفحص المناطق الحرجة وفحص مخصص والتحقق من سلامة التطبيق

- على أجهزة الكمبيوتر التي تعمل بنظام Windows 10 الإصدار 1903 و1909، قد تنتهي الترقيات من Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (الإصدار 10.3.3.275) و4 Service Pack 2 Maintenance Release (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.

- 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 Critical في Kaspersky Security Center؛ ويتم استلام الحدث خوادم KSN 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 Kaspersky Endpoint Security على جهاز كمبيوتر يعمل بنظام التشغيل Microsoft Windows 11، قد تعرض قائمة سياق الملف عناصر لكل من إصداري التطبيق السابق والجديد. أعد تشغيل الكمبيوتر الخاص بك مرتين لضمان التشغيل الصحيح لقائمة سياق الملف.

- إذا تم إيقاف تشغيل الدفاع الذاتي للتطبيق وتوقفت كافة محولات الشبكة، فلن تعمل مكونات الشبكة الخاصة بالتطبيق بين نهاية ترقية التطبيق وإعادة تشغيل الكمبيوتر. وتتضمن مكونات الشبكة الخاصة بالتطبيق الحماية من تهديدات الويب، والحماية من تهديدات البريد، والحماية من تهديدات الشبكة، وجدار الحماية، ومنع اختراق المضيف، والتحكم في الويب. أعد تشغيل الكمبيوتر حتى يعمل التطبيق بشكل صحيح.

- لا يعمل مكون منع هجوم BadUSB بين نهاية ترقية التطبيق وإعادة تشغيل الكمبيوتر. أعد تشغيل الكمبيوتر حتى يعمل التطبيق بشكل صحيح.

- لا يمكن ترقية التطبيق إذا لم تكتمل عملية الترقية السابقة. أعد تشغيل الكمبيوتر حتى يعمل التطبيق بشكل صحيح.

- بعد ترقية التطبيق من إصدارات أقدم من Kaspersky Endpoint Security 11 for Windows، يجب إعادة تشغيل الكمبيوتر.

- إذا كنت تدير Kaspersky Endpoint Security باستخدام Kaspersky Security Center Cloud Console، فلن يُسمح بتحديث التطبيق محليًا. وعند تحديث التطبيق محليًا، لا يمكن قبول اتفاقية معالجة بيانات Kaspersky Security Center Cloud Console.

دعم بنية Arm

- لا يتم دعم تثبيت Kaspersky Endpoint Security في وضع Light Agent على الأجهزة الافتراضية القائمة على Arm.

- لا يتم دعم تشفير القرص من Kaspersky في أجهزة الكمبيوتر القائمة على Arm.

- لا يتم دعم تشفير الملفات على أجهزة الكمبيوتر القائمة على Arm.

- لا يتم دعم تشفير محركات الأقراص القابلة للإزالة على أجهزة الكمبيوتر القائمة على Arm.

- على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 11 ببنية Arm64 ، لا يتوافق EDR Agent مع Bitdefender Endpoint Security Tools.

- لا يتم دعم وظيفة حماية الإشارة الصوتية ووظيفة حماية الوصول إلى كاميرا الويب على أجهزة الكمبيوتر القائمة على بنية Arm.

- وعلى أجهزة الكمبيوتر المستندة إلى بنية Arm، يدعم ملحق الحماية من تهديدات البريد إصدارات 32 بت و64 بت من Outlook 2016 وOutlook 2021 وOutlook 2024 وOutlook 365 for Arm64.

- لا يرسل Kaspersky Endpoint Security كائنات مخصصة لبنية Arm إلى Kaspersky Sandbox.

- لا يتم دعم التحكم في الطباعة على أجهزة الكمبيوتر القائمة على بنية Arm.

- على أجهزة الكمبيوتر القائمة على بنية Arm، تدعم مهمة IOC Scan ملفات البريد الإلكتروني من عملاء البريد التاليين فقط: إصدارات 32 بت و 64 بت من Outlook 2016 وOutlook 2021 و2024 و365 لبنية Arm64.

- على أجهزة الكمبيوتر التي تعمل بنظام Windows 11 لمعالجات Arm64، قد لا تتوفر المصادقة المستندة إلى الرمز المميز لتعذر اكتشاف نظام التشغيل شهادة صالحة على الرمز المميز. ويحدث هذا السلوك بسبب الطريقة التي يتفاعل بها نظام التشغيل مع برنامج الرمز المميز. على سبيل المثال، قد لا يحتوي نظام التشغيل على برامج التشغيل المطلوبة لعمل الرمز المميز. وفي هذه الحالة، لا يدعم Kaspersky Endpoint Security أيضًا المصادقة المستندة إلى الرمز المميز (الحماية بكلمة مرور). ويمكنك استخدام طرق المصادقة الأخرى، مثل بيانات اعتماد المستخدم.

الدعم للأنظمة الأساسية للخادم

- على الخوادم التي تم تمكين البيانات المكررة عليها، تحتاج إلى إضافة ملف fsdmhost.exe إلى قائمة التطبيقات الموثوقة. ويساعد ذلك على تحسين أداء التطبيق ومنع الحمل الزائد على وحدة المعالجة المركزية.

- 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 .

- وضع Server Core 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.
- نظاما التشغيل Windows 10 Enterprise multi-session وWindows 11 Enterprise multi-session مدعومان مع وجود 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 الخيار **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 VMware ESXi Hypervisor. حاول فصل الجهاز بأمان مرة أخرى.
- يتوافق Kaspersky Endpoint Security مع برنامج VMware ESXi Hypervisor مع القيود التالية:
  - قد يكون Kaspersky Endpoint Security غير متوافق مع برامج تشغيل Guest Introspection (vnetWFP.sys وvnetFLT.sys وغيرها). لإصلاح مشكلة عدم التوافق، قم بتحديث برامج التشغيل إلى أحدث إصدار أو إزالة تثبيت برامج التشغيل.
  - في بعض الحالات، قد تفشل محاولة إزالة قرص قابل للإزالة بأمان على جهاز افتراضي. حاول فصل الجهاز بأمان مرة أخرى.

- قد يؤدي تثبيت Kaspersky Endpoint Security على الأجهزة الافتراضية التي تحتوي على عميل Citrix VDA إلى ظهور خطأ في التوافق. ويحدث هذا بسبب توافق Citrix Provisioning Services المحدود مع حلول مكافحة الفيروسات. وللتعرف على أفضل ممارسات استخدام حلول مكافحة الفيروسات مع Citrix Provisioning Services، ارجع غلى موقع ويب دعم Citrix.

- يتخطى Kaspersky Endpoint Security فحص محرك الأقراص القابل للإزالة إذا كان محرك الأقراص متصلاً بجهاز افتراضي موجود في Citrix hypervisor (مهمة فحص محركات الأقراص القابلة للإزالة). وفي هذه الأجهزة، يكتشف نظام التشغيل محرك الأقراص القابل للإزالة المتصل كمحرك أقراص شبكة. وفي مثل هذه الحالات، يمكنك استخدام مهمة فحص مخصص. ويتطابق سلوك التطبيق في الوضع القياسي وفي وضع Light Agent.

- في حالة تثبيت Kaspersky Endpoint Security على جهاز افتراضي في بنية تحتية تستخدم تكنولوجيا Citrix App Layering، فلن تتم إزالة الملفات التي يكتشفها التطبيق كملفات مصابة بالحالة سيتم حذف الكائن عند إعادة التشغيل تلقائيًا عند إعادة تشغيل الجهاز الافتراضي.

  لحذف هذه الملفات، يجب عليك تحميل ملف VHDX الذي يحتوي على User Layer على كمبيوتر مسؤول Citrix App Layering وتشغيل فحص البرامج الضارة على القرص الذي تم تحميله.

- قبل إنشاء لقطة صورة ذهبية لجهاز افتراضي مُثبت عليه Kaspersky Endpoint Security، يوصى بإيقاف تشغيل الجهاز الافتراضي وإنشاء لقطة "ساكنة". وفي حال إنشاء لقطة أثناء تشغيل الجهاز الافتراضي (لقطة "حية")، فلا يمكن ضمان عمل التطبيق بصورة صحيحة.

التوافق مع Kaspersky Security Center

- 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.

- بعد إصلاح التطبيق، يتم تعطيل حماية اتصال الكمبيوتر بخادم الإدارة. بعد إصلاح التطبيق، قم بتشغيل مهمة حماية الاتصال بخادم الإدارة مرة أخرى.

- في Kaspersky Security Center Administration Console، تعرض نافذة **حدد مستخدمًا أو مجموعة من المستخدمين** أول 50000 مستخدم فقط من قائمة مستخدمي Kaspersky Security Center. انظر تعليمات Kaspersky Security Center للمزيد من التفاصيل.

- عند البحث عن الأجهزة المدارة في وحدة تحكم الإدارة في Kaspersky Security Center، فإن علامة التبويب **Application components** قد تعرض متغيرات متعددة لاسم مكون التطبيق نفسه، بما في ذلك الأسماء المقابلة للإصدارات الأقدم من Kaspersky Endpoint Security. وقد يتم أيضًا تكرار أسماء بعض المكونات.

  للبحث حسب المكون، ما عليك سوى تحديد أحد المتغيرات المعروضة. وللمزيد من التفاصيل عن اكتشاف الجهاز، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

- في Kaspersky Security Center Web Console 15.1 Update 2 مع الإصدار 12.11 من مكون الويب الإضافي لتطبيق Kaspersky Endpoint Security for Windows أو إصدار أحدث وUnified Protection and Management Plug-in، لا تعمل شروط تفعيل ملف التعريف الخاصة بالسياسة. ولا يضيف Kaspersky Security Center أجهزة جديدة تلبي شروط تفعيل ملف التعريف إلى وحدة التحكم.

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.

- 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. ويرجع ذلك إلى حقيقة أن التطبيق يقوم أولاً بتفعيل الترخيص التجريبي المضمن أثناء عملية التثبيت. ويتطلب الوصول إلى الإنترنت.

- 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. ويرجع ذلك إلى حقيقة أن التطبيق يقوم أولاً بتفعيل الترخيص التجريبي المضمن أثناء عملية تثبيت التحديث. ويتطلب الوصول إلى الإنترنت.

- 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 14.2 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 الإلكتروني باستخدام ملحق الحماية من تهديدات البريد لبرنامج Microsoft Outlook، نوصي باستخدام وضع التخزين المؤقت في خادم Exchange (Use Cached Exchange Mode).

- لا يدعم Kaspersky Endpoint Security إصدار 64 بت من عميل البريد Microsoft Outlook. وهذا يعني أن Kaspersky Endpoint Security لا يفحص ملفات Microsoft Outlook (ملفات PST وOST) في حالة تثبيت إصدار 64 بت من Microsoft Outlook على الكمبيوتر، حتى إذا كان البريد مضمنًا في نطاق الفحص.

- لا يدعم Kaspersky Endpoint Security عميل بريد Microsoft Outlook الجديد.

- إذا عطلت تنظيف التهديدات التي اكتشفها مكون الحماية من تهديدات البريد وتلقيت رسالة بريد إلكتروني مصابة في صندوق بريد Outlook، فقد يحظر مكون الحماية من تهديدات الويب الاتصال بخادم Exchange عبر بروتوكول MAPI. ينشئ مكون الحماية من تهديدات الويب حينئذٍ حدثًا لاكتشاف التهديدات ويرسله إلى Kaspersky Security Center. ولاستعادة الاتصال بين الكمبيوتر وخادم Exchange، يجب حذف البريد الإلكتروني المصاب يدويًا من صندوق بريد Outlook.

  عند تحديث إصدار التطبيق دون إعادة تشغيل الكمبيوتر، ينخفض مستوى أمان مكون الحماية من تهديدات البريد مؤقتًا (لمدة تصل إلى دقيقة واحدة). وإذا تلقيت رسالة بريد إلكتروني مصابة في صندوق بريد Outlook أثناء تحديث التطبيق، فسيحظر مكون الحماية من تهديدات الويب أيضًا الاتصال بخادم Exchange عبر بروتوكول MAPI. ولاستعادة الاتصال، احذف رسالة البريد الإلكتروني المصابة من صندوق بريد Outlook.

محرك المعالجة

- يقوم التطبيق باستعادة الملفات في الأجهزة التي تحتوي على نظام الملف NTFS أو FAT32 فقط.

- يستعيد التطبيق ملفات يصل حجمها إلى 100 ميجابايت.

- 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.

جدار الحماية

- إذا كانت قاعدة حزمة شبكة الاتصال أو قاعدة شبكة التطبيق تحدد أسماء DNS، فقد يرسل Kaspersky Endpoint Security طلبات إلى خادم DNS لتحديد عناوين IP لهذه الموارد. ويستخدم جدار الحماية عناوين IP لمراقبة نشاط شبكة الاتصال. لذلك يحلل التطبيق أسماء DNS إلى عناوين IP. ويوصى باستخدام أسماء DNS في القواعد فقط لأجهزة كمبيوتر الشبكة المحلية أو الخدمات الداخلية.

- لتحديد قاعدة لجميع عناوين IPv6، أضف نطاق العنوان ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. لا يدعم جدار الحماية قناع ::/0.

- 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.
- 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 موثوق. 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. وتمت إضافة العمود **نوع القاعدة** إلى تقرير جدار الحماية. وعند تشغيل قاعدة حزمة الشبكة، تظل القيمة الموجودة في عمود **اسم التطبيق** فارغة.
- إذا حظرت كل نشاط الشبكة باستخدام جدار الحماية، فقد يكتشف مكون الحماية من تهديدات الشبكة هجومًا من نوع فحص المنافذ. ويمكن أن يحدث هذا لأن التطبيق يبدأ الحماية من تهديدات الشبكة قبل جدار الحماية لاكتشاف النشاط المشبوه في الشبكة.

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.

Kaspersky Security Network

- لا يدعم Kaspersky Endpoint Security بروتوكول HTTPS عند الاتصال بالخادم الوكيل لشبكة KSN (تم تحديد خانة الاختيار **استخدام HTTPS** في إعدادات اتصال الخادم الوكيل لشبكة KSN) إذا كان عنوان الخادم يتضمن أحرفًا غير لاتينية (رموز غير ASCII).
- في Kaspersky Security Center، عند التبديل من استخدام شبكة Kaspersky Security Network العالمية إلى استخدام شبكة Kaspersky Security Network (KPSN) 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.

- بدءًا من الإصدار Kaspersky Endpoint Security 12.9 for Windows، عند التبديل من شبكة KPSN إلى شبكة KSN العالمية، تحتاج إلى إعادة تأكيد اتفاقيتك مع بيان Kaspersky Security Network. ولفعل ذلك، تحتاج إلى تمكين استخدام Kaspersky Security Network في خصائص السياسة أو في واجهة التطبيق وتأكيد اتفاقيتك مع بيان Kaspersky Security Network. وإذا كنت قد استخدمت بالفعل شبكة KSN العالمية، فيجب عليك أولاً تعطيل استخدام شبكة KSN، ثم إعادة تمكينها وتأكيد اتفاقيتك مع بيان Kaspersky Security Network. وإذا كنت لا توافق على بيان Kaspersky Security Network، فلن يتمكن التطبيق من الوصول إلى بيانات Kaspersky Security Network.

- لا يرسل Kaspersky Endpoint Security ملفات نصية (مثل ملفات TXT وCSV وLOG وDOCX بدون وحدات ماكرو) إلى Kaspersky Security Network لفحصها. ويرسل التطبيق الملفات التي قد تشكل تهديدًا إلى KSN لفحصها. وتتضمن هذه الملفات ملفات قابلة للتنفيذ أو ملفات قد تحتوي على تعليمات برمجية قابلة للتنفيذ (مثل وحدات الماكرو في ملفات DOCX). وتكون المكونات الأخرى للتطبيق مسؤولة عن فحص الملفات النصية. ويمكنك أيضًا التحقق يدويًا من سمعة ملف نصي من قائمة سياق الملف. وإذا كانت سمعة الملف النصي غير موثوق به (Kaspersky Security Network)، فإن التطبيق يتجاهل الإجراء المحدد للتهديدات المكتشفة.

التحكم في التطبيقات

- عند العمل باستخدام قواعد التحكم في التطبيقات، لا يوصى بإضافة أكثر من 100000 من شروط التضمين والاستثناء الإجمالية للتطبيقات عبر الفئات المختلفة، بشرط أن يتم تشغيل Kaspersky Endpoint Security على جهاز كمبيوتر يلبي الحد الأدنى من متطلبات الأجهزة ويعمل على Microsoft Windows 10.

- يتم دعم الأرشيفات بتنسيق ZIP فقط عند العمل مع 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 باستخدام قواعد التحكم في التطبيقات في Kaspersky Security Center Web Console، يبلغ الحد الأقصى للحجم المدعوم للملف الذي تم تحميله 104 ميجابايت. 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.

- إذا قمت بإضافة قواعد التحكم في التطبيق المحددة مسبقًا جديدة عند ترقية Kaspersky Endpoint Security، فلا يمكنك تطبيق هذه القواعد على الإصدارات السابقة من التطبيق.

- 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.exe`
  - `C:\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.

- عند ترحيل سياسة KSWS إلى ملف تعريف سياسة KES، يعيد معالج تحويل تصحيح المهام والسياسات (معالج الترحيل) تسمية فئات التطبيق إذا كانت أسماء الفئات تحتوي على أحرف ممنوعة: `"` `*` `<` `>` `?` `\` `:` `|`. يستبدل "معالج الترحيل" هذه الأحرف ويضع مكانها أحرف `_`. على سبيل المثال، تتم إعادة تسمية فئة التطبيق `KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` إلى `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`.

- من الممكن أن يسجل تطبيق Kaspersky Endpoint Security أحداث اتصال وقطع اتصال الجهاز الخارجي. تستخدم خدمات Windows حساب مستخدم النظام لتوصيل الأجهزة أو قطع اتصالها. وهذا يجعل من المستحيل معرفة المستخدم الذي يقوم بتوصيل أو قطع اتصال الجهاز. ويحدد Kaspersky Endpoint Security حساب مستخدم النظام في الحدث.

- 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.

- عند ترقية التطبيق دون إعادة تشغيل الكمبيوتر، لا يطبق التحكم في الجهاز قواعد الوصول على الأجهزة التي يتم إعادة توصيلها. ومع ذلك، إذا كان الجهاز متصلاً قبل الترقية، فسيطبق التحكم في الجهاز القواعد بشكل صحيح. أعد تشغيل الكمبيوتر حتى يعمل التطبيق بشكل صحيح مع الأجهزة التي تم إعادة توصيلها.

- على أجهزة الكمبيوتر المُثبت عليها Kaspersky Endpoint Security الإصدار 12.0، فإن وضع الوصول إلى الطابعة **السماح وعدم التسجيل** لنوع الجهاز **طابعات الشبكة** يسمى **يعتمد على ناقل الاتصال**، إذا تم تطبيق سياسة Kaspersky Endpoint Security الإصدار 12.1 على الكمبيوتر. وفي هذه الأوضاع، ينفذ التطبيق الإجراءات نفسها. وفي Kaspersky Endpoint Security الإصدار 12.1، 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). لا يتم دعم التحكم في الطباعة على أجهزة الكمبيوتر القائمة على بنية Arm.

- بدءًا من Kaspersky Endpoint Security 12.0 for Windows، أصبح بروتوكول WPA3 مدعومًا من قبل التطبيق للأجهزة من نوع **Wi-Fi**. وفي حالة تطبيق سياسة Kaspersky Endpoint Security الإصدار 12.2 على جهاز كمبيوتر، سيتم تحديد بروتوكول WPA2 على أجهزة الكمبيوتر التي يعمل عليها تطبيق Kaspersky Endpoint Security الإصدار 11.11.0 والإصدارات الأقدم؛ وتم تحديد WPA2 / WPA3 للإصدارات من 12.0 إلى 12.1؛ وتم تحديد WPA3 للإصدار 12.2 والإصدارات الأحدث.

- 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.

- في Kaspersky Endpoint Security 12.3 for Windows، تختلف إعدادات الوصول لنوع الجهاز **تقنية Bluetooth**. إذا حددت قيمة **يعتمد على ناقل الاتصال** في الإصدار السابق من التطبيق، ثم بعد ترقية التطبيق إلى الإصدار 12.3، تتغير القيمة التي تم تكوينها إلى **السماح وعدم التسجيل**. وهذا لا يغير سلوك الجهاز.

- يدعم التحكم في الجهاز أجهزة Bluetooth فقط من خلال حزمة Microsoft Windows Bluetooth. وقد يعمل التحكم في الجهاز بشكل غير صحيح مع مكدسات Bluetooth التابعة لجهة خارجية.

- إذا أخفى جهاز Bluetooth فئة الجهاز (COD) الخاصة به أو قلدها، فقد يعمل التحكم في الجهاز بشكل غير صحيح.
- على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows 7 أو Windows 8 والمزودة ببرامج تشغيل Realtek Bluetooth dongle معينة، قد لا يكون من الممكن السماح فقط بتوصيل أجهزة Bluetooth كأجهزة إدخال (الفئة HID). أي أنه إذا حظرت الوصول إلى أجهزة Bluetooth في إعدادات التطبيق وأضفت أجهزة الإدخال إلى الاستثناءات، فقد يمنع التحكم في الجهاز الوصول إلى جميع أجهزة Bluetooth بدلاً من ذلك.

التحكم في الويب

- لا يتم دعم تنسيقات OGV وWEBM.
- لا يتم دعم بروتوكول RTMP.
- Web Control يدعم فقط WSL1. ولا يتحكم التطبيق في حركة مرور WSL2.

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 حول قواعد مراقبة عيوب التكيف التي تم تشغيلها** إذا كانت العينة تتضمن ولو 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.
- يتعذر على Kaspersky Security Center 15.1 إنشاء تقرير **تقرير حول حالة قواعد مراقبة عيوب التكيف** عن قاعدة محددة.
- تتوفر قواعد مراقبة عيوب التكيف فقط باللغة التي تطابق لغة تثبيت المكون الإضافي للويب. وإذا قمت بتغيير لغة الواجهة، تعرض وحدة تحكم الويب قائمة قواعد فارغة. وللوصول إلى القواعد، قم بتغيير لغة الواجهة مرة أخرى إلى لغة تثبيت المكون الإضافي للويب.

تشفير محرك الأقراص (FDE)

- لا يتم دعم تشفير القرص من Kaspersky في أجهزة الكمبيوتر القائمة على Arm.
- لا يتم دعم تشفير محرك BitLocker على أجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows Home.
- باستخدام تشفير محرك الأقراص من BitLocker، يمكن للمستخدم تغيير كلمة مرور المصادقة يدويًا باستخدام واجهة برمجة تطبيقات Windows. وفي مثل هذه الحالات، يتجاهل BitLocker متطلبات كلمة المرور المحددة في سياسة Kaspersky Endpoint Security. بمعنى آخر، يمكن للمستخدم تعيين أي كلمة مرور على الإطلاق.
- 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 Intel Advanced Encryption AES-NI Standard New Instructions 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.

- لا يمكن أن تتواجد عوامل تنزيل متعددة على جهاز كمبيوتر مشفر واحد.

- محاولة لاستعادة صورة لقرص GPT قابل للتمهيد في حالة غير مشفرة، ويمكن لنظام التشغيل جعل نظام التشغيل غير صالح للعمل. ولتجنب ذلك، اتبع هذه التوصيات:

  - قم بفك تشفير القرص بالكامل قبل استعادة الصورة من النسخة الاحتياطية.

  - استخدم النسخ قطاعًا تلو الآخر عند إنشاء الصورة.

  - احذف البيانات من القطاعات الأولى للقرص المشفر قبل استعادة الصورة وإعادة تهيئة القرص.

- 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 <domain>/<Windows account name>، 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 Web Console، 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 على أجهزة الكمبيوتر القائمة على Arm.

- لا يتم دعم تشفير الملفات والمجلدات على أنظمة تشغيل Microsoft Windows Embedded.

- بمجرد تثبيت التطبيق، يجب إعادة تشغيل نظام التشغيل لكي يعمل تشفير الملفات والمجلدات بشكل صحيح.

- يدعم التطبيق تشفير الملفات فقط على الأجهزة التي تعمل بأنظمة ملفات NTFS وFAT32. وفي حالة نقل ملف مشفر إلى جهاز يتضمن نظام ملفات غير مدعوم (على سبيل المثال، exFAT)، فلن يتم تشفير الملف الموجود على هذا الجهاز وسيكون متاحًا للتعديل.

- 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 Encrypting File System 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.

- عند نسخ الملف الذي تم فك تشفيره، على سبيل المثال، إلى وسائط قابلة للإزالة، قد يظل الملف مشفرًا. ويمكن أن يحدث هذا لأنه عندما يحاول مدير الملفات (على سبيل المثال، explorer.exe) الوصول إلى الملف المشفر، فإنه يحفظ تجزئة الملف في قائمة خاصة بالعملية. وبعد فك تشفير الملف، عندما يحاول مدير الملفات الوصول إلى الملف، تبحث العملية عن تجزئة الملف في القائمة. وإذا تم العثور على التجزئة، يترك Kaspersky Endpoint Security الملف مشفرًا. ولتجنب ذلك، تحتاج إلى مسح قائمة العملية. ويمسح نظام التشغيل تلقائيًا قائمة العملية عند امتلائها. ويمكنك أيضًا مسح القائمة يدويًا. ولفعل ذلك، يمكنك إعادة تشغيل الكمبيوتر، وإعادة تشغيل العملية التي تستخدمها للوصول إلى الملف (على سبيل المثال ، explorer.exe)، أو يمكنك استخدام مدير ملفات مختلف لم تستخدمه للوصول إلى الملف المشفر.

- 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 Client-Side Caching (CSC). ولا يتم دعم تشفير الملفات غير المتصلة بالإنترنت أو تقنية Branch Caching عبر SMB للخوادم أيضًا. 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.

- 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 (Windows Subsystem for Linux).

- عند تثبيت مكون التشفير على مستوى الملفات، لا يتم دعم POSIX (Portable Operating System Interface) 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.

Detection and Response (EDR) وNDR وMDR وXDR Sandbox)

- لا يمكنك فحص كائن تم عزله نتيجة مهمة Move file to Quarantine.

- لا يمكن عزل Alternate Data Stream (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 IOC Scan على محركات أقراص الشبكة إذا كان مسار المجلد في خصائص المهمة يبدأ بحرف محرك أقراص. ويدعم Kaspersky Endpoint Security تنسيق مسار UNC فقط لمهام IOC Scan على محركات أقراص الشبكة. على سبيل المثال، `\\server\shared_folder`.

- للتأكد من أن مهمة IOC Scan باستخدام شروط EmailItem تعمل بشكل صحيح، يجب تحديث المكون الإضافي للويب لتطبيق Kaspersky Endpoint Security إلى أحدث إصدار.

- على أجهزة الكمبيوتر القائمة على بنية Arm، تدعم مهمة IOC Scan ملفات البريد الإلكتروني من عملاء البريد التاليين فقط: إصدارات 32 بت و 64 بت من Outlook 2016 وOutlook 2021 وOutlook 2024 و365 لبنية Arm64.

- 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 استيراد سياسة من ملف KLP، لا يتم تطبيق قيمة المعلمة التي تحدد قبول شروط وأحكام اتفاقية Kaspersky Detection and Response Expert. ونتيجة لذلك، بعد استيراد السياسة، لا ينفذ Kaspersky Endpoint Security وظائف وكيل EDR. ولكي يعمل وكيل EDR، افتح السياسة وقم بتغيير أي معلمة واحفظ إعدادات السياسة.

- عند اكتشاف مؤشر على حدوث اختراق أثناء مهمة IOC Scan، 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 Uninstall application remotely).

  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.

- عند إنشاء تفاصيل التنبيه، يوفر التطبيق معلومات عن التهديد المكتشف، بما في ذلك تجزئات الملفات المعدلة. ويحسب Kaspersky Endpoint Security تجزئة الملف أثناء إنشاء تفاصيل التنبيه. ضع في اعتبارك أن التجزئة الأصلية للملف عند إنشاء حدث تعديل الملف قد لا تكون هي نفسها التجزئة التي تم حسابها عند إنشاء تفاصيل التنبيه.

- 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 إذا قمت بتفعيل 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 $Secure:$SDH:$INDEX_ROOT؛ NTFS: $Secure:$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. تمت إضافة الدعم لملفات التعريف هذه إلى Kaspersky Endpoint Security الإصدار 12.2.

- 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 **Connection settings** ("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).

- يتم عرض حالة تفعيل التطبيق بشكل غير صحيح عند تثبيت التطبيق في وضع Endpoint Detection and Response Agent لدعم حل Kaspersky Managed Detection and Response بدون اتصال بحل Kaspersky Security Center. بعد تحميل ملف BLOB، تعرض منطقة الإخطارات في شريط مهام Windows حالة غير صحيحة: لم يتم تفعيل التطبيق. ومع ذلك، تعرض واجهة التطبيق حالة التفعيل بشكل صحيح. أعد تشغيل الكمبيوتر حتى يعمل التطبيق بشكل صحيح.

- يسمح Kaspersky Endpoint Security بالتكامل مع حل Kaspersky Anti Targeted Attack Platform باستخدام مكون EDR (KATA) أو Endpoint Sensor (غير مدعوم). ولاحظ أنه يمكنك فقط استخدام أحد المكونات للتفاعل مع Kaspersky Anti Targeted Attack Platform. لعرض حالة المكون، افتح خصائص الكمبيوتر في وحدة تحكم الإدارة (MMC)، في قسم **Applications**، وافتح خصائص Kaspersky Endpoint Security for Windows، وانتقل إلى قسم **Components**. ونطبق الاعتبارات الخاصة التالية على عرض حالة المكون للتفاعل مع Kaspersky Anti Targeted Attack Platform:

  - بالنسبة للمكون الإضافي للإدارة 12.0 والإصدارات السابقة، يعرض التطبيق الحالة الحالية لمكون **Endpoint Sensor**. وفي Kaspersky Endpoint Security 12.0 والإصدارات الأقدم، لا يتوفر مكون EDR (KATA). وتم تقديم مكون EDR (KATA) في الإصدار 12.1.

  - بالنسبة للمكون الإضافي للإدارة 12.1 والإصدارات الأحدث، يعرض التطبيق الحالة العامة لمكون **Endpoint Detection and Response (KATA)**، التي يمكن أن تعني إما حالة Endpoint Sensor، أو حالة مكون EDR (KATA). يعتمد هذا على إصدار التطبيق المُثبت على كمبيوتر المستخدم والمكونات المتوفرة التي يمكنك استخدامها للتفاعل مع Kaspersky Anti Targeted Attack Platform.

- بدءًا من الإصدار 12.6 من Kaspersky Endpoint Security والإصدارات الأحدث، لا يعرض الإصدار 14.2 من Kaspersky Security Center Web Console والإصدارات الأقل اسم مكون **Endpoint Detection and Response (KATA)** في خصائص الكمبيوتر. وبدلاً من مكون **Endpoint Detection and Response (KATA) Expert (KATA EDR)**. لعرض قائمة المكونات، افتح خصائص الكمبيوتر في Web Console، وفي قسم **Applications**، افتح خصائص Kaspersky Endpoint Security for Windows، وانتقل إلى قسم **Components**. بدءًا من الإصدار 15.1 من Kaspersky Security Center Web Console والإصدارات الأحدث، يعرض التطبيق اسم المكون بشكل صحيح.

- عند تحديث المكون الإضافي لإدارة Kaspersky Endpoint Detection and Response إلى الإصدار 15.3 المثبت في إصدارات Web Console من 14.0 إلى 14.2، يتم عرض تفاصيل التنبيه بشكل غير صحيح. ولكي تعمل تفاصيل التنبيه بشكل صحيح، أعد تشغيل خادم إدارة Kaspersky Security Center .

- لا يدعم الإصدار 15.4 من المكوّن الإضافي لإدارة Kaspersky Endpoint Detection and Response الإصدار 14.0 من Kaspersky Security Center. وبعد تحديث المكون الإضافي للإدارة، يتم عرض تفاصيل التنبيه بشكل غير صحيح.

- لا تدعم حلول فئة الإصدار 1.4 من Kaspersky Extended Detection and Response (XDR) الإصدار 12.12 أو الإصدارات الأحدث من مكون الويب الإضافي لتطبيق Kaspersky Endpoint Security for Windows. ويمكنك إما ترك إصدار المكون الإضافي للويب الحالي أو تحديث حل XDR إلى الإصدار 2.0 أو إصدار أحدث.

- لا يرسل Kaspersky Endpoint Security كائنات مخصصة لبنية Arm إلى Kaspersky Sandbox.

- يدعم Kaspersky Endpoint Security حتى 10000 قاعدة من قواعد التضمين والاستثناء الخاصة بحل EDR Expert (on-premises) في المجمل.

- لن يتم تمرير قواعد تصفية أحداث EDR Expert (on-premises) من السياسة إلى الأجهزة المدارة التي تعمل بالإصدار 14.0 من Kaspersky Endpoint Security أو أقدم في حالة تجاوز الحد المدعوم لقواعد التصفية المخزنة. وسيعرض التطبيق تحذيرًا مطابقًا.

- لا يدعم Kaspersky Endpoint Security for Windows الإصدارات من 12.11 إلى 14.1 أحداث القياس عن بعد EDR Expert (on-premises) التالية:

  - LDAP Attribute Change
  - GPO Change
  - SCCM Local Config Mismatch
  - SCCM Config Change

- SCCM Deployment Task
- Smb Connection Open

بدءًا من الإصدار 14.2، يدعم Kaspersky Endpoint Security كل أحداث التتبع عن بُعد الخاصة بتطبيق EDR Expert (on-premises) باستثناء LDAP Attribute Change.

قيود أخرى

- تدعم أنظمة تشغيل Windows، بدءًا من الإصدار 11 و24H2، تقنية UDP Receive Segment Coalescing Offload (URO). ويتم تمكين التقنية بشكل افتراضي في حالة تثبيت بطاقة شبكة وبرامج تشغيل متوافقة على الكمبيوتر. ويمكن أن يؤدي تعطيل استلام تفريغ اندماج القسم (URO) على كمبيوتر المستخدم إلى تقليل أداء التطبيق بشكل كبير.
- يدعم Kaspersky Endpoint Security نظام WSL الفرعي (Windows Subsystem for Linux) مع قيود:
  - WSL 1. يراقب التطبيق حركة مرور الشبكة ويكتشف التهديدات عبر HTTP / HTTPS. ونظرًا لحقيقة أن Kaspersky Endpoint Security يستخدم شهادته الخاصة لفحص اتصالات HTTPS الآمنة، فقد يتم مقاطعة تشغيل بعض تطبيقات الجهات الخارجية.
  - WSL 2. لا يدعم التطبيق WSL 2.
- 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 **Repositories** ← **Advanced** ← مجلد **Active threats**. ولحفظ الملف، يجب عليك تنظيف الملف المصاب. وعند التنظيف، يحفظ التطبيق نسخة من الملف في النسخة الاحتياطية. ويمكنك الآن حفظ الملف على القرص من **Repositories** ← **Advanced** ← مجلد **Backup**.
- 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.
- قد تحدث أخطاء في اتصال TLS عندما يعمل برنامج طرف ثالث مع مكتبة Libcurl. ويمكن أن يكون هذا مرتبطًا بشهادة Kaspersky التي يستخدمها Kaspersky Endpoint Security لغرض فحص الاتصالات المشفرة. ولمواصلة العمل، يمكنك تعطيل التحقق من صحة الشهادة لبرامج الأطراف الخارجية (غير مستحسن) أو إضافة نص شهادة Kaspersky إلى مخزن شهادات cURL. وللحصول على معلومات مفصلة، راجع قاعدة معارف Kaspersky.
- 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.
- 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.

- 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 Ready Boot أو قم بزيادة مهلة نظام التشغيل لبدء الخدمات.

- لا يمكن للتطبيق العمل في Safe Mode في نظام Windows.

- 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.

- 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\`.

- إذا كنت تستخدم سياسات تقييد البرامج (Software Restriction Policies، 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**). يوجد الملف في مجلد `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.2\klhk\klhk_x64\`. إذا حددت هذه الطريقة، ستحتاج أيضًا إلى مسح خانة الاختيار **تنزيل تحديثات الوحدات النمطية للتطبيق** 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 مجموعة Windows (Group Policy Object، GPO) مع تعيين معلمة DriverLoadPolicy على 8 (Good only)، فإن إعادة تشغيل الكمبيوتر المثبت عليه Kaspersky Endpoint Security تؤدي إلى ظهور شاشة الموت الزرقاء. ولمنع الفشل، يجب تعيين معلمة Early Launch Antimalware (ELAM) في "نهج المجموعة" على 1 (Good and unknown). توجد إعدادات ELAM في السياسة أسفل: **Computer Configuration** ← **Administrative Templates** ← **System** ← **Early Launch Antimalware**.

- 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).

- إذا تم تثبيت Kaspersky Endpoint Security على خادم لنظام إدارة قاعدة البيانات SQL Server، يرسل التطبيق طلبات إلى مثيل الخادم. وهذا ضروري لفحص وظائف عميل SQL Server ومنع تشغيل الوظائف الضارة. يستخدم Kaspersky Endpoint Security حساب مستخدم SQL Server لفحص الوظائف. ويرسل التطبيق الطلبات إلى الخادم عند فحص ذاكرة النظام وبعد تحديث قواعد بيانات مكافحة الفيروسات.

- 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 حماية القرص وتشفير البيانات في برنامج Secret Net Studio.

    ولا يمكن تثبيت التطبيق على جهاز كمبيوتر حيث يتم نشر Secret Net Studio مع مكون حماية القرص وتشفير البيانات. ولجعل التشغيل البيني ممكنًا، يجب إزالة مكون حماية القرص وتشفير البيانات 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.

- عند استيراد قواعد مراقبة سلامة النظام، يتحقق التطبيق من معرف القاعدة واسمها. وإذا كانت معرفات القاعدة واحدة، فإن Kaspersky Endpoint Security يستبدل القواعد الموجودة ويستخدم بدلاً منها القاعدة الجديدة. وعند تصدير القواعد، يقوم التطبيق تلقائيًا بتعيين معرفات. ويمكن أن توجد قاعدة بمعرفات متطابقة، على سبيل المثال، إذا قمت يدويًا بتحرير ملفات XML للقاعدة التي تم تصديرها. وإذا كانت معرفات القاعدة فريدة، لكن أسماء القواعد واحدة، يضيف Kaspersky Endpoint Security (1) وهكذا إلى اسم القاعدة.

- بدءًا من الإصدار 12.11 من Kaspersky Endpoint Security for Windows، لا يمكن عرض إعدادات سياسة رئيسية مفتوحة في مجموعة فرعية في Web Console. ويعرض Web Console أيضًا تحذيرًا: This policy is inherited. You can edit the policy settings only in the administration group in which it was created.

- لا يتم عرض الإخطارات المنبثقة التي يزيد طولها عن 256 حرفًا في وحدة تحكم الإدارة (MMC).

- وقد تكون أسماء المكونات في السياسة وحزمة التثبيت مختلفة. على سبيل المثال، قد يتم تسمية Endpoint Detection and Response Expert (on-premises) باسم Endpoint Detection and Response (KATA)، و-Endpoint Detection and Response Expert (on-premises)، وKaspersky Anti Targeted Attack Platform Integration. وقد تختلف أسماء المكونات أيضًا وفقًا لإصدار التطبيق.

المصطلحات

Cloud Discovery

ويدير Cloud Discovery وصول المستخدم إلى الخدمات السحابية. وتشمل الخدمات السحابية، على سبيل المثال، Microsoft Teams وSalesforce وMicrosoft Office 365. ويتم تجميع الخدمات السحابية في فئات، على سبيل المثال، مشاركة الملفات وبرامج المراسلة والبريد الإلكتروني.

IOC

مؤشر الاختراق. مجموعة من البيانات حول كائن أو نشاط خبيث.

Light Agent

مكون Kaspersky Security for Virtualization Light Agent. يتم تثبيته على كل جهاز افتراضي يحتاج إلى حماية.

OpenIOC

المعيار المفتوح لوصف مؤشر الاختراق (IOC) المستند إلى XML ويتضمن أكثر من 500 مؤشر مختلف للاختراق.

SVM

جهاز افتراضي آمن - جهاز افتراضي خاص يتم تثبيت خدمة خادم الفحص عليه (خادم الحماية، وهو أحد مكونات Kaspersky Endpoint Security for Virtualization Light Agent).

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.

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.

خادم التكامل

مكون Kaspersky Security for Virtualization Light Agent. يتفاعل بين مكونات Kaspersky Endpoint Security والبنية التحتية الافتراضية.

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.

مصادقة Kerberos

آلية مصادقة متبادلة بين العميل والخادم قبل إنشاء اتصال بينهما، مما يسمح بالاتصال عبر الشبكات غير الآمنة. وتعتمد الآلية على بطاقة يحصل عليها المستخدم من مركز مصادقة موثوق به.

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 ملفات الكمبيوتر. وبشكل افتراضي، يوجد مكون الحماية من تهديدات الملفات بشكل دائم في ذاكرة الوصول العشوائي للكمبيوتر ويفحص جميع الملفات التي يتم فتحها وحفظها وبدء تشغيلها، في الوقت الحقيقي. ويفحص هذا المكون الملفات الموجودة على جميع محركات أقراص الكمبيوتر، بما في ذلك محركات الأقراص المتصلة. يوفر المكون حماية للكمبيوتر بمساعدة قواعد بيانات مكافحة الفيروسات وخدمة السحابة الإلكترونية Kaspersky Security Network وكذلك التحليل المساعد على الاكتشاف.

يفحص المكون الملفات التي تم الوصول إليها بواسطة مستخدم أو تطبيق. 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 توجد محتوياته في وحدة تخزين سحابية في 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**. يوصى 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 فقط استثناء 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.

المعلمة	الوصف
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 الملف المصاب المكتشف. وفي حالة فشل التنظيف، يحذف التطبيق الملف. **تنظيف؛ منع إذا فشل التنظيف**. في حالة تحديد هذا الخيار، يحاول التطبيق تلقائيًا تنظيف الملف المصاب المكتشف. وفي حالة فشل التنظيف، يمنع التطبيق هذا الملف. **منع**. إذا تم تحديد هذا الخيار، فسيحظر التطبيق تلقائيًا الملف المصاب دون محاولة تنظيفه أو حذفه. 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	فحص حزم توزيع تطبيقات الجهات الخارجية.
فحص الملفات بتنسيقات Microsoft Office	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. ويفحص التطبيق الملفات بتنسيق Office التي يقل حجمها عن 1 ميجا بايت، بغض النظر عما إذا كانت خانة الاختيار محددة أم لا.
فحص ملفات تنسيق البريد الإلكتروني	يفحص ملفات تنسيق البريد الإلكتروني. يفحص التطبيق ملفات MSG وEML. وتتضمن ملفات تنسيق البريد الإلكتروني كائنات OLE وملفات MHT كذلك. ويفحص تطبيق Kaspersky Endpoint Security ملفات البريد الإلكتروني 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 ضغط 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 الملفات من عمليات 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).

المعلمة	الوصف
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.
فحص عمليات الملفات المنفذة في حاويات Windows	إذا تم اكتشاف تهديد داخل حاوية، فسيطبق التطبيق الإجراء المحدد لمكون الحماية من تهديدات الملفات. **إيقاف الحاوية إذا فشل التنظيف**. قد لا يمتلك التطبيق حقوق قراءة وكتابة كافية للكائن المكتشف. وفي هذه الحالة، يستحيل تنظيف أو حذف الكائن المكتشف. وإذا تم تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف ويوقف الحاوية. وإذا تم إلغاء تحديد خانة الاختيار هذه، فسيحظر التطبيق الكائن المكتشف فقط. **لا تفحص عمليات الملفات المنفذة في حاويات Windows**. في حالة تحديد خانة الاختيار، سيفحص التطبيق الحاوية فقط عند بدء تشغيل الحاوية. وإذا تم إلغاء تحديد خانة الاختيار، سيفحص التطبيق الحاوية باستمرار في الوقت الحقيقي.

الحماية من تهديدات الويب

يمنع مكون الحماية من تهديدات الويب تنزيلات الملفات الضارة عبر الإنترنت، ويحظر أيضًا الاتصال بمواقع الويب الضارة والخاصة بالتصيد الاحتيالي. 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.

لاستخدام الحماية من تهديدات الويب، يجب عليك إكمال التكوين الأولي للتطبيق:

- لمراقبة حركة مرور HTTPS، قم بتمكين فحص الاتصالات المشفرة (يتم التمكين بشكل افتراضي).
- حدد المنافذ التي يجب أن يراقبها Kaspersky Endpoint Security (بشكل افتراضي، يراقب التطبيق كل المنافذ).
- حدد التطبيقات التي تريد أن يراقب Kaspersky Endpoint Security حركة البيانات الخاصة بها. وتوجد معظم المستعرضات بالفعل في قائمة التطبيقات التي أوصت بها Kaspersky. وإذا كان المستعرض الخاص بك مفقودًا من القائمة، فقم بإضافته يدويًا.
- نوصي بإدخال برنامج نصي لتفاعل صفحة الويب في حركة مرور الويب (بشكل افتراضي، يتم تعطيل إدخال البرنامج النصي). يتيح هذا البرنامج النصي تسجيل أحداث الحماية من تهديدات الويب لسجل أحداث التطبيق، وسجل أحداث نظام التشغيل والتقارير.

عندما يحاول مستخدم فتح موقع إلكتروني ضار أو احتيالي، فإن Kaspersky Endpoint Security سوف يحجب الوصول إلى ذلك الموقع ويعرض تحذيرًا.

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 كمبيوتر عبر 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 التطبيق 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 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. **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.

المعلمة	الوصف
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 هذا الخيار، 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 وWeb Control 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
- MyOffice Mail
- R7-Office Organizer

لفحص حركة البيانات في عملاء بريد Mozilla Thunderbird وMyOffice Mail وR7-Office Organizer، فإنك تحتاج إلى إضافة شهادة Kaspersky إلى مخزن الشهادات وتحديد مخزن الشهادات الخاص.

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 إصدارات 32 بت و64 بت من Outlook 2010 و2013 و2016 و2019 و2021 و2024 و365. وعلى أجهزة الكمبيوتر المستندة إلى بنية Arm، يدعم ملحق الحماية من تهديدات البريد إصدارات 32 بت و64 بت من Outlook 2016 وOutlook 2021 وOutlook 2024 وOutlook 365 for Arm64.

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	للحماية من تهديدات البريد، فإن التطبيق باستطاعته تطبيق 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 التطبيق 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 التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. إذا تعذّر تنظيف الكائن، يحذف التطبيق الكائن المصاب. ويضيف التطبيق 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 التطبيق تنظيف الكائن المُكتشف. سيتمكن المستخدم من الوصول إلى الرسالة ومعها مرفق آمن. وإذا تعذّر تنظيف الكائن، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. عند اكتشاف كائن مصاب في رسالة صادرة، يحاول التطبيق تنظيف الكائن المُكتشف. إذا تعذّر تنظيف الكائن، يحظر التطبيق إرسال الرسالة ويظهر عميل البريد خطأ. **منع**. في حالة اكتشاف كائن مصاب في رسالة واردة، يضيف التطبيق تحذيرًا إلى موضوع الرسالة. سيتمكن المستخدم من الوصول إلى الرسالة مع المرفق الأصلي. إذا تم اكتشاف كائن مصاب في رسالة صادرة، يحظر التطبيق 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	يتم نقل الفحص حسب مكون الحماية من تهديدات البريد للحركة 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 Cached Exchange Mode. 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 التطبيق 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. ويفحص التطبيق 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.

المعلمة	الوصف
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 المحدد.
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 Intrusion Detection System، IDS) حركة شبكة الاتصال الواردة للبحث عن خاصية النشاط لهجمات الشبكة. عندما يكتشف التطبيق محاولة هجوم على الشبكة على كمبيوتر مستخدم، فإنه يحظر اتصال الشبكة مع الكمبيوتر المهاجم. وتتوفر أوصاف لأنواع هجمات الشبكة المعروفة حاليًا وطرق إبطالها في قواعد بيانات التطبيق. 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 أجهزة الهجوم لمدة N دقيقة	في حالة تمكين هذا الخيار، 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. يمكنك إضافة عنوان IP مع المنفذ والبروتوكول المحدد. 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

يمنع مكون جدار الحماية الاتصالات غير المصرح بها لجهاز كمبيوتر 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.

أنواع اتصال الشبكة

يسمح لك جدار الحماية بالتحكم في نشاط الشبكة اعتمادًا على نوع اتصال الشبكة. يتلقى Kaspersky Endpoint Security نوع اتصال الشبكة من نظام تشغيل الكمبيوتر. يقوم المستخدم بتعيين نوع اتصال الشبكة في نظام التشغيل عند إعداد الاتصال. يمكنك تغيير نوع اتصال الشبكة في إعدادات Kaspersky Endpoint Security. سيراقب جدار الحماية نشاط الشبكة اعتمادًا على نوع الشبكة المحدد في إعدادات Kaspersky Endpoint Security وليس في نظام التشغيل.

تتوفر أنواع اتصال الشبكة 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.

  يُعين جدار الحماية نوع الشبكة العامة إلى الإنترنت بشكل افتراضي. لا يمكنك تغيير نوع 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 جهاز كمبيوتر للهجمات أو محاولات الوصول للبيانات غير المسموح بها. ويسمح جدار الحماية بأي نشاط للشبكة ضمن الشبكات التي تتمتع بهذه الحالة.

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 المتاحة	يحتوي هذا الجدول على معلومات حول اتصالات الشبكة التي يكتشفها جدار الحماية على الكمبيوتر. 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 بكمبيوتر ويتم 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.

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.



مصادقة لوحة المفاتيح

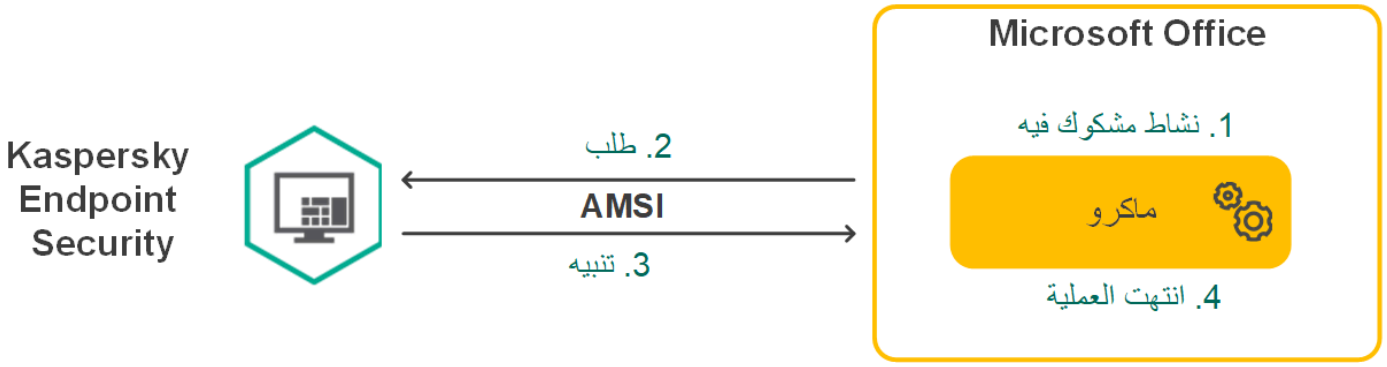
إعدادات مكون منع هجمات BadUSB

المعلمة	الوصف
منع استخدام لوحة المفاتيح على الشاشة لمصادقة أجهزة USB	في حالة تبديل زر التبديل، يمنع التطبيق استخدام لوحة المفاتيح على الشاشة للحصول على تصريح لجهاز USB الذي يتعذر إدخال رمز تصريح من خلاله.
حظر استخدام رمز شريطي لمصادقة أجهزة USB	في حالة تمكين مفتاح التبديل، لن يعرض التطبيق الرمز الشريطي في إخطار المصادقة على الماسح الضوئي للرمز الشريطي.
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، يحظر التطبيق جهاز USB بعد المحاولة الخامسة غير الناجحة. ويعرض Kaspersky Endpoint Security مدة الحظر لجهاز USB. وبعد انقضاء هذا الوقت، سيصبح لديك مرة أخرى خمس محاولات لإدخال رمز المصادقة.
المهلة عند الوصول إلى الحد الأقصى لعدد المحاولات	مدة حظر جهاز USB بعد العدد المحدد من المحاولات غير الناجحة 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.

يستطيع مكون حماية AMSI فقط اكتشاف التهديدات وإخطار تطبيق خارجي بالتهديد المكتشف. لا يسمح التطبيق الخارجي بعد استلام الإخطار بوجود تهديد بإجراءات مشكوك فيها (على سبيل المثال، ينهي الإجراء).



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 / Enterprise متعدد الجلسات؛
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise متعدد الجلسات؛
- Windows Server 2016 Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)
- Windows Server 2019 Essentials / Standard / Datacenter (بما في ذلك وضع Server Core)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (بما في ذلك وضع Server Core)
- Windows Server 2025 Standard / Datacenter

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	فحص حزم توزيع تطبيقات الجهات الخارجية.
فحص الملفات بتنسيقات Microsoft Office	يفحص ملفات Microsoft Office (DOC وDOCX وXLS وPPT وملحقات Microsoft الأخرى). وتتضمن الملفات بتنسيقات Office كائنات OLE كذلك. ويفحص التطبيق 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

يكتشف مكون منع الاستغلال 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.

بالإضافة إلى ذلك، يراقب مكون منع الاستغلال منافذ الشبكة لعمليات التطبيق التي قد تهدد أمان الكمبيوتر. ويحصل التطبيق على معلومات عن هذه العمليات مع قواعد بيانات مكافحة الفيروسات.

إعدادات مكون منع الاستغلال

المعلمة	الوصف
عند اكتشاف استغلال	**منع**. في حالة تحديد هذا العنصر، عند اكتشاف استغلال، يمنع Kaspersky Endpoint Security عمليات هذا الاستغلال ويدون إدخال سجل بالمعلومات حول هذا الاستغلال. **إعلام**. 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. وتعتمد وظيفة Kaspersky Endpoint Security على توقيعات تدفق السلوك وتوفر دفاعًا استباقيًا للكمبيوتر.

بالإضافة إلى ذلك، يراقب مكون اكتشاف السلوك منافذ الشبكة لعمليات التطبيق التي قد تهدد أمان الكمبيوتر. ويحصل التطبيق على معلومات عن هذه العمليات مع قواعد بيانات مكافحة الفيروسات.

إعدادات مكون اكتشاف السلوك

المعلمة	الوصف
الإجراء عند اكتشاف نشاط برنامج ضار	**حذف**. 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. **منع**. في حالة تحديد هذا الخيار، فإنKaspersky Endpoint Security يقوم بإنهاء هذا التطبيق عند اكتشاف وجود أي نشاط ضار. **إعلام**. 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.

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 (على سبيل المثال، الملفات والتطبيقات)

يتم التحكم في نشاط الشبكة للتطبيقات بواسطة مكون 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**. جدول حقوق الوصول لموارد نظام التشغيل والبيانات الشخصية للتطبيقات التي تنتمي إلى مجموعة الثقة. • **الحقوق**. جدول حقوق الوصول للعمليات والموارد الخاصة بنظام التشغيل للتطبيقات التي تنتمي إلى مجموعة الثقة. • **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.
مجموعة الثقة للتطبيقات التي يتم بدء تشغيلها قبل Kaspersky Endpoint Security	مجموعة ثقة سيضع فيها Kaspersky Endpoint Security التطبيقات التي بدأت قبل Kaspersky Endpoint Security.
تحديث القواعد للتطبيقات التي لم تكن معروفة سابقًا من KSN	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.

المعلمة	الوصف
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 غير المدرجة في مجموعات أخرى	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 مكون 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.

قد لا تكون وظيفة KSN متاحة في التطبيق في الولايات المتحدة.

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. في حال مشاركتك في Kaspersky Security Network (KSN)، فإن خدمات KSN تزود Kaspersky Endpoint Security بمعلومات عن سمعة عناوين الويب المفحوصة، بالإضافة إلى معلومات عن فئة وسمعة الملفات التي يتم فحصها. وللمزيد من التفاصيل عن تكوين الوصول إلى KSN، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.

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.

إعدادات Kaspersky Security Network

المعلمة	الوصف
تمكين وضع KSN الموسع	إن وضع KSN الموسع هو وضع يقوم فيه Kaspersky Endpoint Security بإرسال بيانات إضافية إلى Kaspersky. 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 خادم الإدارة كخادم وكيل لشبكة 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 Kaspersky Security Network عندما يكون الخادم الوكيل لشبكة KSN غير متاح (متوفر فقط في Kaspersky Security Center Console)	إذا تم تحديد خانة الاختيار، سيستخدم Kaspersky Endpoint Security خوادم شبكة KSN عند عدم توافر خدمة KSN Proxy. 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.

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 ما، ينشئ التطبيق حدثًا بحالة Critical (انظر الشكل أدناه).

إذا كنت ترغب في استخدام فحص السجل، تأكد من تكوين إعدادات 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.

مكافحة التشفير

يحلل مكون مكافحة التشفير 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.

المعلمة	الوصف
الاستثناءات حسب الاسم أو عنوان IP	**الاستثناءات حسب الاسم أو عنوان IP**. 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. **الاستثناءات حسب القناع**. استثناءات نطاق الحماية. ومن الممكن أن يؤدي استثناء مجلد من نطاق الحماية 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. 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.
الإجراء المطلوب اتخاذه عند اكتشاف تهديد	• **إعلام**. في حالة تحديد هذا الخيار، عند اكتشاف محاولة لتعديل الملفات في المجلدات المشتركة، يضيف Kaspersky Endpoint Security معلومات عن هذه المحاولة إلى قائمة التهديدات النشطة، ويضيف إدخالاً إلى تقارير واجهة التطبيق المحلية ويرسل معلومات عن النشاط الخبيث المكتشف إلى Kaspersky Security Center. • **منع الاتصال لمدة (دقيقة) N min**. في حالة تحديد هذا الخيار، عندما يكتشف Kaspersky Endpoint Security محاولة لتعديل الملفات في المجلدات المشتركة، فإنه يمنع الوصول إلى تعديل الملف للجلسة التي بدأت النشاط الضار وينشئ نسخًا احتياطية من الملفات المعدلة. في حالة تمكين مكون محرك المعالجة وتحديد الخيار **منع الاتصال لمدة (دقيقة)**، سيتم استعادة الملفات المعدلة من النسخ الاحتياطية.
نطاق الحماية	نطاق الحماية هو قائمة بمسارات المجلدات المشتركة التي يراقب فيها Kaspersky Endpoint Security نشاط الملفات. يدعم Kaspersky Endpoint Security متغيرات البيئة وحروف `*` و `?` عند إدخال قناع. وبشكل افتراضي، يحدد التطبيق تلقائيًا المجلدات المشتركة ويراقب نشاط الملفات في جميع المجلدات.

التحكم في الويب

يقوم المكون التحكم في الويب بإدارة وصول المستخدم 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).

لاستخدام التحكم في الويب، يجب عليك إكمال التكوين الأولي للتطبيق:

- لمراقبة حركة مرور HTTPS، قم بتمكين فحص الاتصالات المشفرة (يتم التمكين بشكل افتراضي).
- حدد المنافذ التي يجب أن يراقبها Kaspersky Endpoint Security (بشكل افتراضي، يراقب التطبيق كل المنافذ).
- حدد التطبيقات التي تريد أن يراقب Kaspersky Endpoint Security حركة البيانات الخاصة بها. وتوجد معظم المستعرضات بالفعل في قائمة التطبيقات التي أوصت بها Kaspersky. وإذا كان المستعرض الخاص بك مفقودًا من القائمة، فقم بإضافته يدويًا.
- نوصي بإدخال برنامج نصي لتفاعل صفحة الويب في حركة مرور الويب (بشكل افتراضي، يتم تعطيل إدخال البرنامج النصي). يتيح هذا البرنامج النصي تسجيل أحداث التحكم في الويب لسجل أحداث التطبيق، وسجل أحداث نظام التشغيل، والتقارير.

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 المستخدم إلى البيانات الموجودة على موقع الويب، وإخفاء الصور، 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 تطبيقات Office فقط لفئة 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.

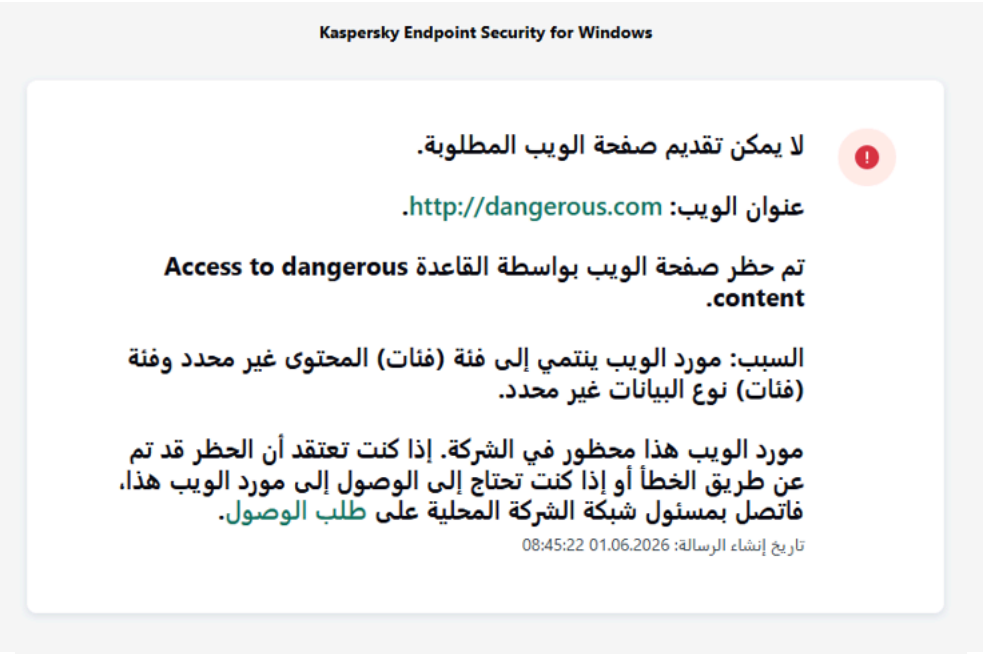
  على سبيل المثال، يمكنك تقييد وصول جميع مستخدمي الشركة إلى الإنترنت من خلال المستعرض باستثناء قسم تكنولوجيا المعلومات.

- 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.
إنهاء جلسات مستعرض المستخدم النشطة بعد تطبيق القاعدة	في حالة تحديد خانة الاختيار، ينهي Web Control الاتصال بموارد الويب المحظورة فورًا بعد تطبيق السياسة. ويتوقف المستعرض على الفور عن تنزيل البيانات من صفحة الويب. وعندما تقوم بتحديث صفحة الويب أو الانتقال إلى صفحة ويب أخرى محظورة، يعرض التطبيق تحذيرًا. يسمح Web Control بفصل موارد الويب على الفور فقط في مستعرضات الويب. وبالنسبة للتطبيقات الأخرى، يقيد Web Control الاتصالات الجديدة فقط. إذا تم إلغاء تحديد خانة الاختيار، يُقيد مكون Web Control الاتصالات الجديدة فقط بموارد الويب المحظورة. ولا ينهي Web Control الاتصالات النشطة.

المعلمة	الوصف
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 **User requests**. 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. يتم توفير متغيرات خاصة لإدارة قوالب الرسائل (على سبيل المثال، `%USER_NAME%`). وتسمح المتغيرات باستخدام قالب رسالة واحدة لأجهزة الكمبيوتر المختلفة.
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 كمبيوتر (على سبيل المثال، الأقراص الصلبة أو الكاميرات أو وحدات شبكة Wi-Fi). ويتيح لك هذا حماية جهاز الكمبيوتر من الإصابة بالفيروسات عند اتصال مثل هذه الأجهزة به، ومنع فقدان البيانات أو تسريباتها.

في حالة تمكين التحكم في الأجهزة، ينقل التطبيق معلومات عن الأجهزة المتصلة إلى Kaspersky Security Center. يمكنك عرض قائمة الأجهزة المتصلة في Kaspersky Security Center في المجلد **Hardware** ← **Repositories** ← **Advanced**.

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). إذا تم تحديد وضع **يعتمد على ناقل الاتصال** لنوع الجهاز، يسمح التطبيق أو يرفض الوصول إلى الجهاز وفقًا لواجهة الاتصال (مثل 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 (Hardware ID 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**. لكل جهاز Vendor ID (VID) وProduct ID (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.

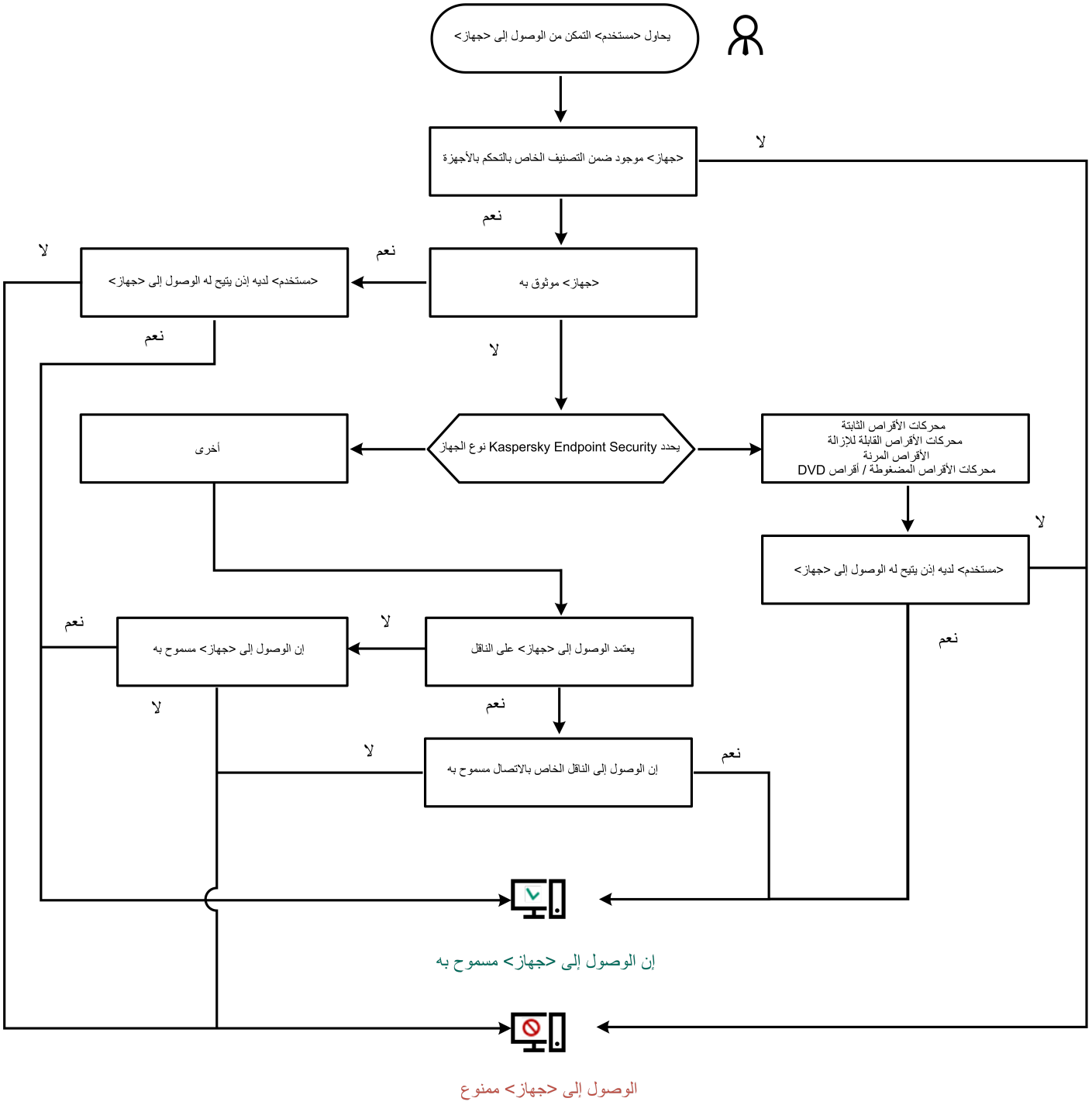
عند حظر جهاز متصل بجهاز كومبيوتر بواسطة التحكم في الجهاز، فإن برنامج Kaspersky Endpoint Security سيقوم بحظر الوصول وإظهار إخطار (انظر الشكل أدناه).



إخطار التحكم في الجهاز

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.

المعلمة	الوصف
السماح بطلبات للوصول المؤقت (متوفر فقط في Kaspersky Security Center (Console	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.
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. يسمح Kaspersky Endpoint Security أو يرفض الوصول إلى الأجهزة بناءً على نوع ناقل الاتصال إذا تم تحديد الوضع **يعتمد على ناقل الاتصال**.
الأجهزة الموثوقة	قائمة الأجهزة الموثوقة والمستخدمين الذين تم منحهم حق الوصول إلى هذه الأجهزة.
دمج القيم عند التوريث (متوفر فقط في Kaspersky Security Center (Console	يدمج هذا قائمة الأجهزة 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 بالأجهزة الموثوقة للمؤسسة بأكملها. لا يمكن حذف عناصر القائمة الموروثة في السياسات الفرعية أو تحريرها. ويمكن حذف قائمة الأجهزة 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. تسمح هذه الوظيفة أيضًا بدمج القوائم في ملفات تعريف السياسة. ولدمج القوائم، في ملف التعريف ذي الأولوية القصوى، قم بتمكين وراثة الإعدادات من ملف تعريف ذي أولوية منخفضة. وللمزيد من التفاصيل عن أولويات ملف تعريف السياسة، يُرجى الرجوع إلى تعليمات Kaspersky Security Center.
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. ولإنشاء فئة، يمكنك استخدام المعايير التالية: فئة KL (على سبيل المثال المستعرضات او فئة أخرى)، وتجزئة الملف وبائع التطبيق ومعايير أخرى.

2. إنشاء قواعد التحكم في التطبيقات.

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. ويمكن للمسؤول إنشاء العديد من القواعد. وقد يتطابق تطبيق واحد مع معايير القواعد المتعددة. تكون أولوية أية قاعدة منع أعلى من أولوية أية قاعدة سماح. ويتحقق Kaspersky Endpoint Security مما إذا كان التطبيق يتطابق مع قاعدة في كل مرة يتم تشغيلها فيها. ويطابق Kaspersky Endpoint Security بشكل تسلسلي التطبيق مقابل جميع قواعد التحكم في التطبيق.

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.

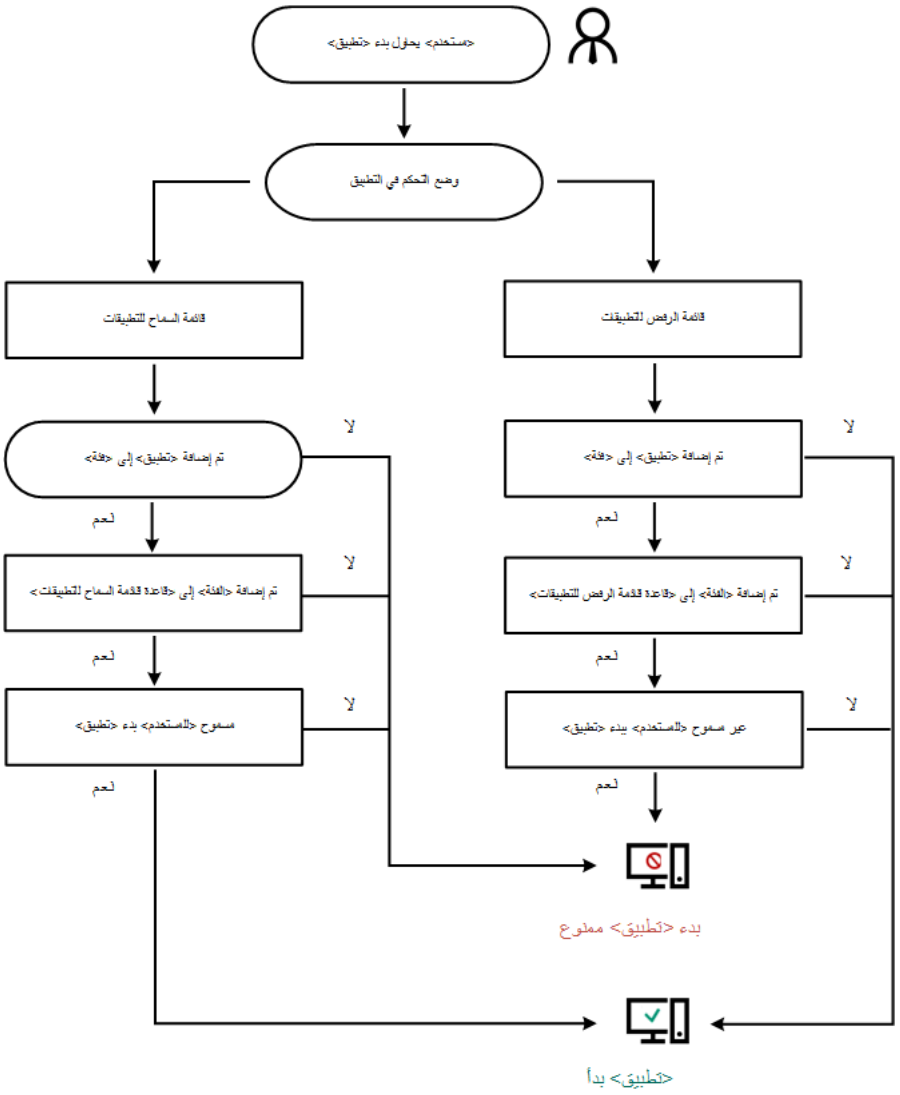
تستند قواعد التحكم في التطبيقات التي تم إنشاؤها في وحدة تحكم إدارة Kaspersky Security Center إلى فئات التطبيقات المخصصة وليس على شروط التضمين والاستبعاد كما هو الحال في الواجهة المحلية لـ Kaspersky Endpoint Security.

- استلام معلومات حول التطبيقات المثبَّتة 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

المعلمة	الوصف
الإجراء عند بدء تشغيل التطبيقات الممنوعة بواسطة القواعد	**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 تطبيق، 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 تطبيق، 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.
مراقبة 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 "**صورة ذهبية\الشهادات 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.
استخدام التحقق الصارم من التوقيع الرقمي	يمكنك تحديد شهادة كشرط تشغيل لقاعدة التحكم في التطبيق. وفي حالة تحديد خانة الاختيار هذه، يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بشهادات فقط من مخزن شهادات نظام موثوق. وتعتبر التطبيقات الموقعة بمثل هذه الشهادة موثوقة أيضًا بواسطة مكونات الحماية ، على سبيل المثال المهمة فحص البرامج الضارة. ومع ذلك، إذا حددت شهادة من متجر مختلف في قاعدة التحكم في التطبيقات، فلن يطبق Kaspersky Endpoint Security هذه القاعدة. إذا تم إلغاء تحديد خانة الاختيار، فسوف يطبق Kaspersky Endpoint Security القواعد على التطبيقات الموقعة بواسطة شهادة من Windows Trusted Root Certificate Store. ولا تعد مثل هذه التطبيقات جزءًا من المنطقة الموثوقة. وتراقب مكونات الحماية نشاط هذه التطبيقات.
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 **User requests**. 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 الأحداث في تقرير تشغيل القاعدة ومستودع **Rule triggers in Smart Training state**.

2. تحليل تقرير تشغيل القاعدة.

يحلل المسؤول تقرير تشغيل القاعدة أو محتويات مستودع **Rule triggers in Smart Training state**. 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 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 **Rule triggers in Smart Training state**. ونوصي بالتحقق من التقرير عن تشغيل القواعد ومحتويات تخزين **Rule triggers in Smart Training state**.

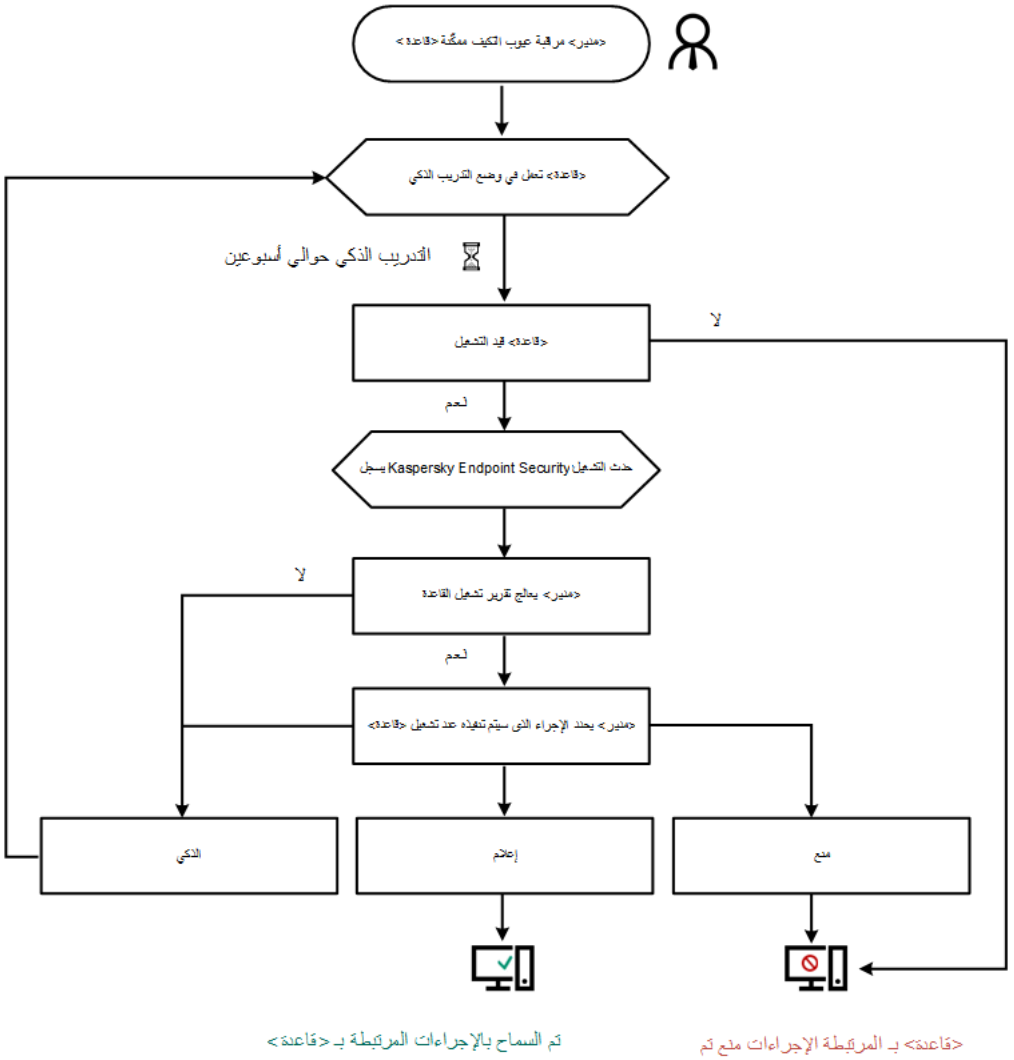
عندما يحاول تطبيق ضار تنفيذ إجراء ما، سيحظر Kaspersky Endpoint Security الإجراء ويعرض إخطارًا (انظر الشكل أدناه).



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.

المعلمة	الوصف
القواعد	جدول قواعد مراقبة عيوب التكيف. تم إنشاء القواعد من قِبل متخصصي Kaspersky استنادًا إلى سيناريوهات نموذجية للنشاط الضار.
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 **User requests**. 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 النظام

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.

بدءًا من الإصدار 12.6، يتضمن Kaspersky Endpoint Security for Windows مكون مراقبة سلامة النظام بدلاً من مكون مراقبة سلامة الملفات. يتضمن مكون مراقبة سلامة النظام كل وظائف مراقبة سلامة الملفات ويسمح بالإضافة إلى ذلك بمراقبة تغييرات السجل واتصال الأجهزة الخارجية.

يراقب مكون مراقبة سلامة النظام التغييرات في نظام التشغيل التي قد تشير إلى خروقات أمان الكمبيوتر. وعند اكتشاف هذه التغييرات، ينشئ Kaspersky Endpoint Security الأحداث المقابلة وينبه المسؤول. يمكن أن تعمل مراقبة سلامة النظام في وضع الوقت الحقيقي ويمكنها أيضًا إجراء التحقق من سلامة النظام عند الطلب.

مراقبة سلامة النظام في الوقت الحقيقي

في وضع الوقت الحقيقي، يتبع مكون مراقبة سلامة النظام التغييرات في الكائنات التي قمت بتضمينها في نطاق المكون (نطاق المراقبة). وتسمح مراقبة سلامة النظام أيضًا بمنع الوصول غير المصرح به إلى هذه الكائنات في الوقت الحقيقي.

التحقق من سلامة النظام عند الحاجة

يعد التحقق من سلامة النظام عند الحاجة مهمة يمكنك تشغيلها يدويًا أو وفقًا لجدول زمني. ولتشغيل مهمة التحقق من سلامة النظام، يجب عليك تكوين نطاق المكون (نطاق المراقبة) وإنشاء خط أساس. ويعد خط الأساس بمثابة حالة مسجلة للكائنات في النظام، التي يستخدمها التطبيق كمرجع عند مقارنتها بالحالة الحالية.

إعدادات مراقبة سلامة النظام

المعلمة	الوصف
وضع التشغيل لقواعد الحظر	• **منع**. وفي هذا الوضع، تمنع مراقبة سلامة النظام الإجراءات باستخدام الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا. • **إعلام**. وفي هذا الوضع، تسمح مراقبة سلامة النظام باتخاذ إجراءات مع الملفات ومفاتيح السجل من نطاق المراقبة، وتنشئ حدثًا مطابقًا.
مراقبة سلامة النظام في الوقت الحقيقي	في وضع الوقت الحقيقي، يتبع مكون مراقبة سلامة النظام التغييرات في الكائنات التي قمت بتضمينها في نطاق المكون (نطاق المراقبة). وتسمح مراقبة سلامة النظام أيضًا بمنع الوصول غير المصرح به إلى هذه الكائنات في الوقت الحقيقي.
مراقبة الأجهزة	تراقب مراقبة سلامة النظام اتصال وفصل الأجهزة الخارجية.
مراقبة الملفات والسجل	تراقب مراقبة سلامة النظام التغييرات على الملفات والمجلدات والسجل.
التحقق من سلامة النظام	يعد التحقق من سلامة النظام عند الحاجة مهمة يمكنك تشغيلها يدويًا أو وفقًا لجدول زمني. ولتشغيل مهمة التحقق من سلامة النظام، يجب عليك تكوين نطاق المكون (نطاق المراقبة) وإنشاء خط أساس. ويعد خط الأساس بمثابة حالة مسجلة للكائنات في النظام، التي يستخدمها التطبيق كمرجع عند مقارنتها بالحالة الحالية.

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 Kaspersky Anti Targeted Attack Platform. Kaspersky Anti Targeted Attack Platform عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدِفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. تتضمن Kaspersky Anti Targeted Attack Platform ثلاث وحدات وظيفية:

- Kaspersky Anti Targeted Attack Platform (KATA)
- Kaspersky Endpoint Detection and Response (EDR (KATA))
- Network Detection and Response (NDR (KATA))

يمكنك شراء جميع الوحدات الوظيفية أو الوحدات الوظيفية الفردية 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.

Sandbox

يتضمن Kaspersky Endpoint Security for Windows عاملاً مضمنًا للتكامل مع حل Kaspersky Sandbox. ويكتشف مكون Sandbox ويمنع تلقائيًا التهديدات المتقدمة على أجهزة الكمبيوتر. ويحلل Sandbox سلوك الكائن لاكتشاف النشاط الخبيث وخصائص النشاط للهجمات المستهدفة على البنية التحتية لتكنولوجيا المعلومات في المؤسسة. ويحلل Sandbox الكائنات ويفحصها على خوادم خاصة باستخدام صور افتراضية منشورة لأنظمة تشغيل Microsoft Windows (خوادم Sandbox). وللحصول على التفاصيل عن الحل، يُرجى الرجوع إلى تعليمات Kaspersky Sandbox وتعليمات Kaspersky Anti Targeted Attack Platform.

بدءًا من الإصدار 12.7، يدعم Kaspersky Endpoint Security for Windows مكون Sandbox الذي يعد جزءًا من حل Kaspersky Anti Targeted Attack Platform. وعلى عكس حل Kaspersky Sandbox، يسمح مكون KATA Sandbox بفحص الملفات ليس فقط تلقائيًا، لكن أيضًا يدويًا من قائمة سياق الملف.

يتطلب KATA Sandbox نشر Kaspersky Anti Targeted Attack Platform 7.0 أو أحدث.

يمكن إدارة المكون فقط باستخدام Kaspersky Security Center Web Console. لا يمكنك إدارة هذا المكون باستخدام وحدة تحكم الإدارة (MMC).

إعدادات مكون Sandbox

المعلمة	الوصف
Integration mode	**Kaspersky Sandbox**. التكامل مع حل Kaspersky Sandbox. ويرسل التطبيق الملفات المراد فحصها في Kaspersky Sandbox في الوضع التلقائي فقط. **KATA Sandbox**. التكامل مع مكون Sandbox في حل Kaspersky Anti Targeted Attack Platform. ويمكنك تحديد وضع إرسال الملف للفحص: • **Manually**. يرسل المستخدم الملف يدويًا للفحص من قائمة السياق (**إرسال إلى Sandbox**). • **Automatically**. يكتشف التطبيق تلقائيًا الكائنات ويرسلها إلى Sandbox للفحص. • **Combined**.
Server connection settings	**Timeout (msec)**. انتهت مهلة الاتصال بخادم الحماية (لتطبيق Kaspersky Sandbox) أو خادم العقدة المركزية (لتطبيق KATA). بعد انقضاء المهلة التي تم تكوينها، يرسل Kaspersky Endpoint Security طلبًا إلى الخادم التالي. ويمكنك زيادة مهلة الاتصال لتطبيق Sandbox إذا كانت سرعة الاتصال لديك منخفضة أو إذا كان الاتصال غير مستقر. مهلة الطلب الموصى بها 0.5 ثانية أو أقل. **Request queue**. حجم مجلد قائمة انتظار الطلبات. عند إرسال كائنات متعددة للفحص في Sandbox، ينشئ Kaspersky Endpoint Security قائمة انتظار للطلبات. وافتراضيًا، يقتصر حجم مجلد قائمة انتظار الطلبات على 100 ميجابايت. وبعد الوصول إلى الحد الأقصى للحجم، يتوقف 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. **Server TLS certificate**. لتكوين اتصال موثوق به مع خادم الحماية (لتطبيق Kaspersky Sandbox) أو خادم العقدة المركزية (لتطبيق KATA)، يجب عليك إعداد شهادة TLS. ويجب عليك بعد ذلك إضافة الشهادة إلى الكمبيوتر باستخدام سياسة. وتحتاج أيضًا إلى إضافة الشهادة إلى خادم Sandbox (لتطبيق Kaspersky Sandbox) أو خادم العقدة المركزية (لتطبيق KATA). **Use two-way authentication** (فقط لتطبيق KATA Sandbox). المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.
Connection to Sandbox servers	**Kaspersky Sandbox**. إعدادات اتصال خادم 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. **KATA Sandbox**. إعدادات اتصال خادم العقدة المركزية. تختار العقدة المركزية الإعدادات المثلى للفحص وتحميل التوازنات بين خوادم Sandbox.

المعلمة	الوصف
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 Critical Areas Scan**. في حالة تحديد هذا الخيار، يُشغل Kaspersky Endpoint Security مهمة Critical Areas Scan. 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 IOC Scan (مهمة مستقلة لفحص مؤشر الاختراق). ولهذه المهمة، يمكنك تكوين وضع التشغيل ونطاق الفحص والإجراء عند اكتشاف مؤشر الاختراق (Move copy to Quarantine, delete object أو Run Critical Areas Scan). ولتعديل الإعدادات الأخرى لمهمة IOC Scan، 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 drive 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 فيه بدء مهمة IOC Scan يدويًا في الوقت الذي يناسبك. **Automatically**. وضع التشغيل الذي يقوم فيه Kaspersky Endpoint Security بتشغيل مهمة IOC Scan تلقائيًا بعد 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.

Managed Detection and Response

يدعم Kaspersky Endpoint Security for Windows التكامل مع حل 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.

إعدادات Managed Detection and Response

المعلمة	الوصف
ملف تكوين MDR	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.

Endpoint Detection and Response

يتضمن Kaspersky Endpoint Security for Windows عميلاً مضمنًا لحل Kaspersky Endpoint Detection and Response Optimum (المشار 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. ويعد التنبيه حدثًا في البنية التحتية لتكنولوجيا المعلومات للشركة حدده التطبيق على أنه غير عادي أو مشكوك فيه ويمكن أن يشكل تهديدًا أمنيًا للبنية التحتية لتكنولوجيا المعلومات الخاصة بالشركة. 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 Endpoint Detection and Response Optimum في Web Console وCloud Console. تتوفر إعدادات مكون Endpoint Detection and Response Expert (cloud) فقط في Cloud Console.

إعدادات Endpoint Detection and Response

المعلمة	الوصف
Enable advanced system activity logging	تعمل ميزة القياس عن بُعد على تحسين دقة اكتشاف مؤشر الاختراق، لكنها تستخدم المزيد من موارد الكمبيوتر. ونوصي بتمكين القياس عن بُعد الموسع على الكمبيوتر بغرض فحص مؤشر الاختراق بأثر رجعي. فحص مؤشر الاختراق بأثر رجعي هو وضع لمهمة IOC Scan يفحص فيها Kaspersky Endpoint Security مؤشرات الاختراق باستخدام البيانات لفترة زمنية معينة. ويهدف هذا الوضع إلى البحث عن مؤشرات الاختراق عن طريق القياس عن بُعد للكمبيوتر المحمي مثل نشاط الشبكة والعمليات والملفات والقياس عن بُعد الآخر. في حالة تعطيل القياس عن بُعد الموسع، فقد يقوم Kaspersky Endpoint Security بتدوير المعلومات عن مؤشرات الاختراق التي تم اكتشافها.
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 device in (hours)	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 add to event log**. 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. **Add to event log**. 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.
Execution prevention rules	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.

المعلمة	الوصف
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 Report on threats في وحدة تحكم Kaspersky Security Center.

Endpoint Detection and Response Expert (on-premises)

Endpoint Detection and Response Expert (on-premises)

يدعم Kaspersky Endpoint Security for Windows التكامل مع حل Kaspersky Endpoint Detection and Response Expert (on-premises). ويعد Kaspersky Endpoint Detection and Response Expert (on-premises) حلاً للأمن الإلكتروني للمؤسسات يتضمن تطبيقات Kaspersky التي تسمح للمؤسسة بصد معظم أنواع المخاطر الإلكترونية وتغطية أهم سيناريوهات انتشار التهديدات. ويتم نشر مكونات EDR Expert (on-premises) على Open Single Management Platform (OSMP). وتقوم هذه المنصة بتشغيل سيناريوهات عبر الأنظمة الأساسية في واجهة واحدة وتسمح بدمج تطبيقات Kaspersky مع تطبيقات الجهات الخارجية في نظام أمان شامل.

يمثل SIEM أحد العناصر المركزية للحل. ويتتبع SIEM الأحداث القادمة من جميع المكونات ويربط هذه الأحداث ببعضها البعض باستخدام قواعد محددة من قبل البائع والمستخدم. ويبحث EDR Expert (on-premises) في السجلات والقياس عن بُعد الواردة من البنية التحتية للشركة لاكتشاف الهجمات تلقائيًا والسماح بالتحقيق في الحوادث باستخدام رسم بياني لتحقيق موحد يجمع كل الأحداث التي تم جمعها في EDR Expert (on-premises)، بما في ذلك الأحداث من تطبيقات Kaspersky و منتجات أمان المعلومات من جهات خارجية.

للاستجابة للحوادث المتقدمة، يستخدم EDR Expert (on-premises) سيناريوهات معدة مسبقًا ومحددة بواسطة المستخدم. ويمكنك أيضًا استخدام إجراءات الاستجابة من تطبيقات الجهات الخارجية وسيناريوهات الاستجابة التي تتضمن تطبيقات متعددة.

Endpoint Detection and Response (KATA)

يدعم Kaspersky Endpoint Security for Windows العمل مع مكون Kaspersky Endpoint Detection and Response كجزء من حل Kaspersky Anti Targeted Attack Platform (EDR (KATA)). Kaspersky Anti Targeted Attack Platform عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدِفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. تتضمن Kaspersky Anti Targeted Attack Platform ثلاث وحدات وظيفية:

- Kaspersky Anti Targeted Attack Platform (KATA)
- Kaspersky Endpoint Detection and Response (EDR (KATA))
- Network Detection and Response (NDR (KATA))

يمكنك شراء جميع الوحدات الوظيفية أو الوحدات الوظيفية الفردية 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) وNDR (KATA) في 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 Expert (on-premises)

المعلمة	الوصف
Connection to telemetry collection servers	خادم جمع القياس عن بعد هو خادم يعد جزءًا من حل SIEM الذي يجمع المعلومات عن الأحداث التي تحدث على الكمبيوتر وتوحيدها وربطها وتحليلها وتخزينها. قم تكوين ما يلي للاتصال بخوادم مجموعة القياس عن بُعد (KUMA): • **Timeout (sec)**. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف. • **Server certificate**. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security والخادم. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات الخادم، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد تكوين إعدادات الخادم، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور. يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.
Address و**Port** (خوادم جمع القياس عن بُعد)	إعدادات الاتصال بخوادم جمع القياس عن بُعد. يمكنك إدخال عنوان IP (IPv4 أو IPv6). يمكنك إضافة عناوين متعددة لخادم جمع القياس عن بعد. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.
Send telemetry to telemetry collection servers	تتيح لك هذه الوظيفة إيقاف تشغيل إرسال القياس عن بُعد إلى خادم KATA تمامًا. على سبيل المثال، إذا كنت تستخدم Kaspersky Anti Targeted Attack Platform جنبًا إلى جنب مع حل آخر يستخدم أيضًا القياس عن بُعد، يمكنك إيقاف تشغيل إرسال القياس عن بُعد لحل KATA (EDR). ويتيح لك هذا تحسين حمل الخادم لهذه الحلول. وإذا 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). • **Send telemetry with IOA only**. يتيح ذلك تحسين القياس عن بُعد وإرسال القياس عن بُعد فقط مع IOA. مؤشر الهجوم (IOA) هو قاعدة تحتوي على وصف لسلوك مشبوه في النظام مما قد يشير إلى هجوم موجه. ويقارن التطبيق السلوك الجاري في النظام مع هذه القواعد ويسجل الأحداث التي تشير إلى هجوم موجه. ويستخدم التطبيق تقنية فحص البث التي تتيح تتبع مثل هذه الأحداث في الوقت الحقيقي. • **Maximum event transmission delay (sec)**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية. • **Limit the number of event packets per transmission**. يتزامن التطبيق مع الخادم عندما يمتلئ المخزن المؤقت بالأحداث. الإعداد الافتراضي هو 1024 حدثًا. تسمح هذه الوظيفة بتعطيل التخزين المؤقت للأحداث قبل المزامنة مع الخادم.
Enable request throttling	تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث. تكوين إعدادات القياس عن بعد: • **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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 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%.
Send sync request to server every (min)	عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.

المعلمة	الوصف
Connection to response servers	خادم الاستجابة هو خادم لاستلام البيانات وفحصها ودراسة سلوك الكائنات ونشر نتائج هذه الدراسات. قم بتكوين ما يلي للاتصال بخادم الاستجابة: • **Timeout (sec)**. الحد الأقصى لمهلة استجابة الخادم. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم مختلف. • **Server certificate**. شهادة TLS لإنشاء اتصال موثوق مع الخادم. يمكنك الحصول على شهادة TLS على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). • **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security والخادم. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات الخادم، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. وحاوية التشفير هي أرشيف PFX مع شهادة ومفتاح خاص. يمكنك الحصول على حاوية تشفير على منصة الإدارة الواحدة المفتوحة (راجع التعليمات في تعليمات Kaspersky Endpoint Detection and Response Expert (on-premises)). وبعد تكوين إعدادات الخادم، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور.
Address و Port (خوادم الاستجابة)	إعدادات الاتصال بخوادم الاستجابة. يمكنك إدخال عنوان IP (IPv4 أو IPv6). يمكنك إضافة عناوين متعددة لخادم جمع القياس عن بعد. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

إعدادات Endpoint Detection and Response (KATA)

المعلمة	الوصف
Send sync request to server every (min)	عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.
Connection to KATA servers	قم بتكوين ما يلي للاتصال بخادم العقدة المركزية: • **Timeout (sec)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف. • **Server 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**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور. يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.
Address و Port (خوادم KATA)	إعدادات الاتصال بخوادم Kaspersky Anti Targeted Attack Platform. أدخل عنوان IP (IPv4 أو IPv6) ومنفذ خادم Central Node للاتصال. يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.
Send telemetry to KATA	تتيح لك هذه الوظيفة إيقاف تشغيل إرسال القياس عن بُعد إلى خادم KATA تمامًا. على سبيل المثال، إذا كنت تستخدم Kaspersky Anti Targeted Attack Platform جنبًا إلى جنب مع حل آخر يستخدم أيضًا القياس عن بُعد، يمكنك إيقاف تشغيل إرسال القياس عن بُعد لحل KATA (EDR). ويتيح لك هذا تحسين حمل الخادم لهذه الحلول. وإذا 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). تكوين إعدادات القياس عن بعد: • **Maximum event transmission delay (sec)**. يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية. • **Maximum number of event packages**. يتزامن التطبيق مع الخادم عندما يمتلئ المخزن المؤقت بالأحداث. الإعداد الافتراضي هو 1024 حدثًا.
Enable request throttling	تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث. تكوين إعدادات القياس عن بعد: • **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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 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%.

Network Detection and Response (KATA)

يدعم Kaspersky Endpoint Security for Windows العمل مع مكون Kaspersky Network Detection and Response كجزء من حل Kaspersky Anti Targeted Attack Platform (EDR (KATA)). Kaspersky Anti Targeted Attack Platform عبارة عن حل تم تصميمه لاكتشاف التهديدات المتطورة في الوقت المناسب، مثل الهجمات المستهدِفة، والتهديدات المستمرة المتقدمة (APT)، وهجمات يوم الصفر، وغير ذلك. تتضمن Kaspersky Anti Targeted Attack Platform ثلاث وحدات وظيفية:

- Kaspersky Anti Targeted Attack Platform (KATA)
- Kaspersky Endpoint Detection and Response (EDR (KATA))
- Network Detection and Response (NDR (KATA))

يمكنك شراء جميع الوحدات الوظيفية أو الوحدات الوظيفية الفردية 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) وNDR (KATA) في 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.

معلمات Networkt Detection and Response (KATA)

المعلمة	الوصف
إعدادات اتصال الخادم	**المهلة (ثانية)**. الحد الأقصى لمهلة استجابة خادم Central Node. عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم Central Node مختلف. **شهادة TLS للخادم**. 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). **استخدام المصادقة ثنائية الاتجاه**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين Kaspersky Endpoint Security وخادم Central Node. لاستخدام المصادقة ثنائية الاتجاه، تحتاج إلى تمكين المصادقة ثنائية الاتجاه في إعدادات خادم Central Node، ثم الحصول على حاوية تشفير وتعيين كلمة مرور لحماية حاوية التشفير. 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). وبعد تكوين إعدادات Central Node، تحتاج أيضًا إلى تمكين المصادقة ثنائية الاتجاه في إعدادات Kaspersky Endpoint Security وتحميل حاوية تشفير محمية بكلمة مرور. يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.
العنوان والمنفذ	إعدادات الاتصال بخوادم Kaspersky Anti Targeted Attack Platform. أدخل عنوان IP (IPv4 أو IPv6) ومنفذ خادم Central Node للاتصال. يمكنك إضافة عناوين متعددة لخادم العقدة المركزية. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.
إرسال طلب مزامنة إلى خادم NDR كل (دقيقة)	عدد مرات إرسال طلبات المزامنة إلى الخادم. أثناء المزامنة، يرسل Kaspersky Endpoint Security معلومات عن إعدادات ومهام التطبيق المعدلة.
الحد الأقصى لتأخير إرسال الحدث (ثانية)	يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
تمكين تقييد الطلب	تساعد هذه الميزة في تحسين الحمل على الخادم. وفي حالة تمكين هذه الوظيفة، يقيد التطبيق إرسال الحدث. وإذا تجاوز عدد الأحداث الحدود التي تم تكوينها، يتوقف Kaspersky Endpoint Security عن إرسال الأحداث.
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. إذا تم تثبيت التطبيق على خادم، يكون تدفق بيانات القياس عن بُعد أعلى. وبالنسبة للخوادم، يوصى بزيادة القيمة إلى 60,000 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%.

تكامل KUMA

يدعم Kaspersky Endpoint Security for Windows حل Kaspersky Unified Monitoring and Analysis Platform. وKaspersky Unified Monitoring and Analysis Platform (KUMA) هو حل إدارة معلومات الأمان والأحداث (SIEM) للبنية التحتية لتكنولوجيا المعلومات في المؤسسات. ويسمح KUMA باكتشاف التهديدات الأمنية وتحليلها والتخفيف من حدتها قبل أن تتسبب في ضرر.

إعدادات تكامل KUMA

المعلمة	الوصف
Maximum delay when sending events (sec)	يتزامن التطبيق مع الخادم لإرسال الأحداث بعد انتهاء صلاحية الفاصل الزمني للمزامنة. الإعداد الافتراضي هو 30 ثانية.
Connection to KUMA servers	**Timeout (sec)**. الحد الأقصى لوقت انتظار استجابة من خادم KUMA (القيمة الافتراضية 5 ثوانٍ). عندما تنتهي المهلة، يحاول Kaspersky Endpoint Security الاتصال بخادم KUMA مختلف. **Server certificate**. شهادة TLS لإنشاء اتصال موثوق مع خادم KUMA. ويمكنك الحصول على شهادة TLS في وحدة تحكم Kaspersky Unified Monitoring and Analysis Platform (راجع التعليمات في تعليمات Kaspersky Unified Monitoring and Analysis Platform). لإنشاء اتصال موثوق، في وحدة تحكم KUMA، في إعدادات موصل tcp، يجب عليك تحديد وضع TLS **With verification** (راجع إعدادات الموصل من نوع tcp في تعليمات Kaspersky Unified Monitoring and Analysis Platform). **Use two-way authentication**. المصادقة ثنائية الاتجاه عند إنشاء اتصال آمن بين KES وKUMA. لاستخدام المصادقة ثنائية الاتجاه، في وحدة تحكم KUMA، في إعدادات الموصل، يجب عليك تحديد وضع TLS **Custom PFX with client authentication** (راجع إعدادات الموصل في تعليمات Kaspersky Unified Monitoring and Analysis Platform). ثم يجب عليك تنزيل شهادة خادم وتعيين كلمة مرور لحماية حاوية التشفير. يجب أن تكون حاوية التشفير محمية بكلمة مرور. ولا يمكن إضافة حاوية تشفير بكلمة مرور فارغة.
خوادم KUMA	إعدادات الاتصال بخوادم Kaspersky Unified Monitoring and Analysis Platform. يمكنك إدخال عنوان IP (IPv4 أو IPv6). يمكنك إضافة عناوين متعددة لخادم KUMA. ويحاول Kaspersky Endpoint Security الاتصال بالخادم باستخدام أول عنوان IP. وإذا تعذّر إنشاء اتصال، يُحاول Kaspersky Endpoint Security الاتصال باستخدام عنوان IP الثاني في القائمة وهكذا.

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

لا يتم دعم تشفير القرص من Kaspersky في أجهزة الكمبيوتر القائمة على Arm.

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. ويمكنك أيضًا استخدام تقنية Single Sign-On (SSO) التي تتيح لك تسجيل الدخول 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. يسمح لك Kaspersky Endpoint Security بالتحكم في تقنية Bitlocker وإدارتها باستخدام البنية التحتية لتطبيق Kaspersky Next. 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.

عند تشفير القرص، يضع BitLocker أداة تحميل التمهيد والملفات المساعدة الأخرى في system partition. ويكون هذا القسم غير مشفر. وينشئ نظام التشغيل قسم النظام تلقائيًا أثناء تثبيت Windows. وإذا كان القرص مقسمًا بشكل كامل قبل تثبيت Windows، فلن يتمكن نظام التشغيل من إنشاء قسم للنظام. وفي هذه الحالة، عند بدء تشغيل تشفير القرص باستخدام BitLocker، يطالبك نظام التشغيل بإعادة تقسيم القرص وإنشاء قسم للنظام. وبعد إنشاء قسم النظام، يبدأ نظام التشغيل تشفير BitLocker.

توفر تقنية BitLocker تخزينًا آمنًا لمفاتيح الوصول باستخدام وحدة نمطية للنظام الأساسي الموثوق به. Trusted Platform Module (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 النظام، يحتاج المستخدم إلى تجاوز مصادقة BitLocker لإقلاع نظام التشغيل. وبعد المصادقة، يسمح BitLocker للمستخدم بتسجيل الدخول. ولا تدعم BitLocker تقنية تسجيل الدخول الأحادي (SSO).

بعد تشفير محرك أقراص، ينشئ BitLocker مفتاح استرداد. ويرسل Kaspersky Endpoint Security مفتاح الاسترداد إلى Kaspersky Security Center حتى يمكنك استعادة الوصول إلى القرص، على سبيل المثال، إذا نسي مستخدم كلمة مروره.

إذا قام مستخدم بتشفير قرص باستخدام BitLocker، فسوف يرسل Kaspersky Endpoint Security مفتاح الاسترداد ومعلومات عن تشفير القرص إلى Kaspersky Security Center.

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.

المعلمة	الوصف
وضع التشفير	**تشفير جميع محركات الأقراص الصلبة**. إذا تم تحديد هذا الخيار، يشفر التطبيق 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 الخيار، يفك التطبيق 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 وكيل المصادقة تلقائيًا لمستخدمي Windows	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.
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. بشكل افتراضي، يتم إلغاء تحديد خانة الاختيار.
استخدام دعم USB القديم (غير موصى به)	تقوم خانة الاختيار هذه بتمكين أو تعطيل وظائف Legacy USB Support. 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). لا يؤثر Legacy USB Support 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 تمكين وظيفة Legacy USB Support، 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.

المعلمة	الوصف
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 الخيار، يشفر التطبيق 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 الخيار، يفك التطبيق 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	باستخدام المصادقة التي تتطلب إدخال بيانات في بيئة ما قبل 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. نوصي باستخدام 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 (بحد 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. بشكل افتراضي، يتم إلغاء تحديد خانة الاختيار.

المعلمة	الوصف
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). Trusted Platform Module (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. • **وحدة النظام الأساسي الموثوق بها (TPM) أو كلمة المرور إذا لم تكن وحدة النظام الأساسي الموثوق بها متاحة**. في حالة تحديد هذا الخيار، يستطيع 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. يجب تكوين طريقة المصادقة المحددة عن طريق تحديد متطلبات كلمة المرور أو رقم التعريف الشخصي: • **الحد الأدنى لطول رمز PIN (الأحرف)** (القيمة الافتراضية هي 6). • **الحد الأدنى لطول كلمة المرور (الأحرف)** (القيمة الافتراضية هي 8). • **الحد الأقصى لعدد كلمات المرور / أرقام التعريف الشخصية المخزنة** (القيمة الافتراضية هي 5). • **الحد من فترة صلاحية كلمة المرور / رمز PIN لأجل TPM (بالأيام)** (معطل بشكل افتراضي). • **استخدام رمز PIN المُحسن (حروف وأرقام)**. يسمح رمز PIN المحسّن باستخدام أحرف أخرى بالإضافة إلى الأحرف الرقمية: الأحرف اللاتينية الكبيرة والصغيرة والأحرف الخاصة والمسافات. معطل بشكل افتراضي.
إعادة إنشاء كلمة مفتاح الاسترداد تلقائيًا (بالأيام)	قم بتحديث كلمة المرور تلقائيًا لاستعادة الوصول إلى محرك الأقراص المحمي بواسطة BitLocker. وفي حالة تحديد خانة الاختيار، حدد فترة صلاحية كلمة مرور مفتاح الاسترداد. ويساعد هذا في منع إعادة استخدام كلمة مرور مفتاح الاسترداد.

التشفير على مستوى الملف

لا يتم دعم تشفير الملفات على أجهزة الكمبيوتر القائمة على Arm.

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.

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.

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 التشفير	**عدم التغيير**. إذا تم تحديد هذا العنصر، فيترك Kaspersky Endpoint Security الملفات والمجلدات بدون تغيير دون تشفيرها أو 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

لا يتم دعم تشفير محركات الأقراص القابلة للإزالة على أجهزة الكمبيوتر القائمة على Arm.

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:

- Full Disk Encryption (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").

- File Level Encryption (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.

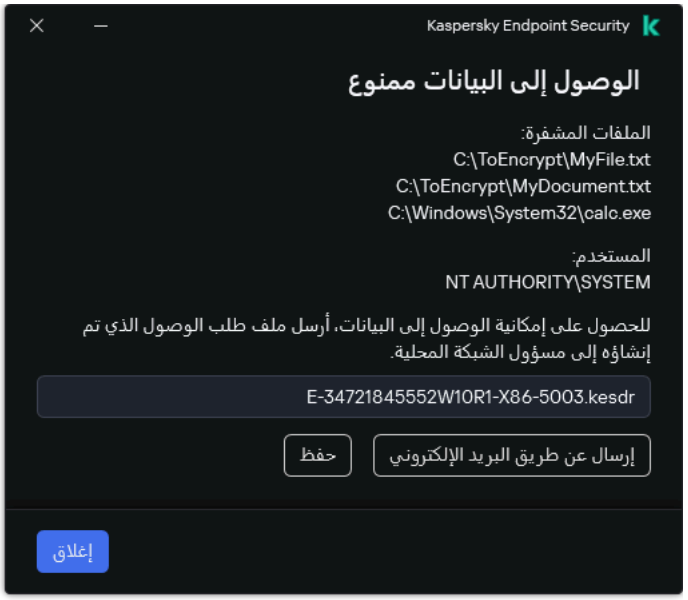
المعلمة	الوصف
الوضع المحمول	تقوم خانة الاختيار هذه بتمكين / تعطيل إعداد القرص القابل للإزالة مما يسهل من الوصول إلى الملفات المخزنة علىمحرك الأقراص القابل للإزالة هذا على أجهزة الكمبيوتر خارج شبكة الشركة. إذا تم تحديد خانة الاختيار هذه، فيُطالب Kaspersky Endpoint Security المستخدم بتحديد كلمة مرور قبل 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:
	  • حسب معرف الجهاز (Hardware ID أو HWID)
	  • حسب طراز الجهاز: Vendor ID (VID) وProduct ID (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.

بدءًا من Kaspersky Endpoint Security 12.5 for Windows، يمكنك إضافة قياس EDR عن بُعد إلى المنطقة الموثوقة. ويسمح ذلك بتحسين البيانات التي يرسلها التطبيق إلى خادم جمع القياس عن بُعد لحل Kaspersky Anti Targeted Attack Platform (EDR).

بدءًا من Kaspersky Endpoint Security 12.6 for Windows، تتم إضافة استثناءات الفحص والتطبيقات الموثوقة إلى المنطقة الموثوقة. وتساعد استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة على تكوين Kaspersky Endpoint Security بسرعة على خوادم SQL وخوادم Microsoft Exchange وإدارة تكوين مركز النظام. ويعني هذا أنك لست بحاجة إلى إعداد منطقة موثوقة يدويًا للتطبيق على الخوادم.

بدءًا من الإصدار Kaspersky Endpoint Security 12.8 for Windows، يمكنك تثبيت التطبيق في وضع Light Agent لحماية البيئات الافتراضية. ويمكن أن تساعدك استثناءات الفحص المحددة مسبقًا والتطبيقات الموثوقة في تكوين Kaspersky Endpoint Security بسرعة في البيئات الافتراضية في Citrix و VMware

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. تتيح استثناءات الفحص إمكانية الاستخدام الآمن للبرامج الشرعية التي يمكن للمجرمين استغلالها لإتلاف جهاز الكمبيوتر أو بيانات المستخدم. وليس بالضرورة أن يكون لمثل هذه التطبيقات أغراض ضارة، لكن يمكن للقراصنة استغلالها. وللحصول على معلومات مفصلة عن التطبيقات المشروعة التي يمكن أن يستخدمها الدخلاء لاختراق الكمبيوتر أو بيانات المستخدم، يرجى زيارة موقع ويب موسوعة 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.
- مهمة 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. وبشكل افتراضي، يراقب 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.

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 بجهاز كمبيوتر.

- **الفيروسات والفيروسات المتنقلة**

الفئة الفرعية: الفيروسات والفيروسات المتنقلة (Viruses_and_Worms)

مستوى الخطر: مرتفع

تقوم الفيروسات التقليدية والفيروسات المتنقلة بإجراءات غير مسموح بها من قبل المستخدم. فيمكنها إنشاء نسخ من أنفسها كما تتمكن هذه النسخ من نسخ نفسها.

فيروس تقليدي

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. تكتب فيروسات Overwriting رمزها الخاص فوق رمز الملف المصاب، ثم تمسح محتوى الملف. ولذا، يتوقف ملف مصاب عن العمل ويتعذر استعادته. تقوم فيروسات Parasitic بتعديل الملفات مع تركها تعمل كليًا أو جزئيًا. تقوم فيروسات Companion بتعديل الملفات، لكنها تنشئ نُسخًا 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 Link وفيروسات OBJ وفيروسات LIB وفيروسات التعليمات البرمجية المصدرية والعديد من الفيروسات الأخرى.

الفيروس المتنقل

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 ما 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 Internet Relay Chats، وهي أنظمة خدمة تتيح التواصل مع الآخرين 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 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.
الفيروس المتنقل	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 الخطر: مرتفع

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.

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	أدوات النقر لفيروس 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 دون 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 (IM) (Trojan-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 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 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 قِبل 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. فيروسات الاستغلال عبارة عن حزم شبكة تقوم بتعطيل أجهزة الكمبيوتر.
FileCryptor	مشفرون	تقوم بترميز التطبيقات الضارة الأخرى لإخفائها من تطبيق مكافحة الفيروسات.
Flooder	برامج "تلويث" 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: برامج إعلانية (Adware)

مستوى الخطر: 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: تم اكتشاف برامج قانونية يمكن أن يستخدمها المجرمون لإتلاف جهازك 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.
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 فيروسات 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 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 لمكافحة الفيروسات تعرض عن حول اكتشاف البرامج الضارة. برغم ذلك، فإنها لا تكتشف في الواقع أي شيء أو تنظفه.

- **برامج قانونية يمكن أن يستخدمها المجرمون لإتلاف جهازك أو بياناتك الشخصية**

الفئة الفرعية: تم اكتشاف برامج قانونية يمكن أن يستخدمها المجرمون لإتلاف جهازك 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.
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 فيروسات 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 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 لمكافحة الفيروسات تعرض عن حول اكتشاف البرامج الضارة. برغم ذلك، فإنها لا تكتشف في الواقع أي شيء أو تنظفه.

- **كائنات مضغوطة قد يُستخدم الضغط الخاص بها لحماية التعليمات البرمجية الخبيثة**

الفئة الفرعية: الملفات المحزومة التي قد تتسبب في حدوث أضرار

مستوى الخطر: متوسط.

يتم حزم الملف باستخدام أداة حزم خاصة يتم استخدامها لحزم البرامج الضارة: الفيروسات والفيروسات المتنقلة وفيروسات حصان طروادة. يفحص Kaspersky Endpoint Security الوحدة النمطية لفك الحزمة داخل الأرشيفات ذاتية الاستخراج (SFX).

لإخفاء البرامج الضارة من الاكتشاف بواسطة برنامج مكافحة الفيروسات، يقوم المتسللون بحزمها باستخدام برامج حزم خاصة. حدد خبراء Kaspersky برامج الحزم الأكثر شيوعًا بين القراصنة.

- **الكائنات متعددة الضغط**

الفئة الفرعية: الملفات المحزومة التي قد تتسبب في حدوث أضرار

مستوى الخطر: متوسط.

يتم حزم الملف باستخدام أداة حزم خاصة يتم استخدامها لحزم البرامج الضارة: الفيروسات والفيروسات المتنقلة وفيروسات حصان طروادة. يفحص Kaspersky Endpoint Security الوحدة النمطية لفك الحزمة داخل الأرشيفات ذاتية الاستخراج (SFX).

لإخفاء البرامج الضارة من الاكتشاف بواسطة برنامج مكافحة الفيروسات، يقوم المتسللون بحزمها باستخدام برامج حزم خاصة. حدد خبراء Kaspersky برامج الحزم الأكثر شيوعًا بين القراصنة.

الاستثناءات	يحتوي هذا الجدول على معلومات حول استثناءات من الفحص. نوصي بتحديد المسارات النسبية بدلاً من المسارات المطلقة. ولا يسمح هذا باستثناء كائنات نظام الملفات فحسب، بل يسمح أيضًا باستثناء الكائنات التي ليس لها ملفات. على سبيل المثال، `*\Program Files (x86)\Folder\Subfolder`. 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. يخفي Kaspersky Endpoint Security قائمة استثناءات الفحص في واجهة المستخدم الخاصة بالتطبيق إذا تم حظر تكوين استثناءات الفحص بواسطة المسؤول في وحدة التحكم (رمز "القفل المغلق") وتم حظر استثناءات الفحص المحلية (تم إلغاء تحديد خانة الاختيار **السماح باستخدام الاستثناءات المحلية**).
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 في 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. يخفي Kaspersky Endpoint Security القائمة الموحدة للتطبيقات الموثوقة في واجهة المستخدم الخاصة بالتطبيق إذا تم حظر تكوين التطبيقات الموثوقة بواسطة المسؤول في وحدة التحكم (رمز "القفل المغلق") وتم حظر التطبيقات الموثوقة المحلية (تم إلغاء تحديد خانة الاختيار **السماح باستخدام التطبيقات الموثوقة المحلية**).

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. تسمح هذه الوظيفة أيضًا بدمج القوائم في ملفات تعريف السياسة. ولدمج القوائم، في ملف التعريف ذي الأولوية القصوى، قم بتمكين وراثة الإعدادات من ملف تعريف ذي أولوية منخفضة. وللمزيد من التفاصيل عن أولويات ملف تعريف السياسة، يُرجى الرجوع إلى تعليمات 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.
القياس عن بعد لحل EDR (KATA) / NDR (KATA) (متوفر فقط في Kaspersky Security Center Console)	يحتوي هذا الجدول على معلومات حول استثناءات القياس عن بعد لحل EDR.
القياس عن بعد في KUMA (متوفر فقط في Kaspersky Security Center Console)	قائمة الأحداث التي سيتم إرسالها إلى Kaspersky Unified Monitoring and Analysis Platform (KUMA). ويعمل Kaspersky Endpoint Security في الأوضاع التالية: • **إرسال كل الأحداث**. في هذا الوضع ، يرسل التطبيق جميع الأحداث من سجل Windows باستثناء الأحداث المضافة إلى قواعد الاستثناء. • **إرسال الأحداث المحددة فقط**. في هذا الوضع، يرسل التطبيق الأحداث المضافة في قواعد التضمين فقط.
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

المعلمة	الوصف
بدء التطبيق عند بدء تشغيل الكمبيوتر (موصى به)	عند تحديد هذا الخيار، يبدأ Kaspersky Endpoint Security بعد تحميل نظام التشغيل لحماية الكمبيوتر أثناء الجلسة بأكملها. عند إلغاء تحديد هذا الخيار، 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)	ينهي Kaspersky Endpoint Security عادةً البرامج الضارة المكتشفة قبل إصابة الكمبيوتر. وتحمي تقنية التنظيف المتقدمة الكمبيوتر من البرامج الضارة النشطة بالفعل (الإصابة النشطة)، وبالتالي تقليل مخاطر فقدان البيانات وانتشار التهديد. إذا تم تمكين هذه التقنية، فعند اكتشاف نشاط ضار، يعرض Kaspersky Endpoint Security إخطارًا منبثقًا. في الإخطار الخاص به، يعرض Kaspersky Endpoint Security على المستخدم خيار إجراء تنظيف متقدم للكمبيوتر. بعد موافقة المستخدم على هذا الإجراء، يُبطل Kaspersky Endpoint Security التهديد ثم يعيد 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، يمكنك 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	في حالة تحديد خانة الاختيار هذه، يستخدم التطبيق خادم إدارة Kaspersky Security Center كخادم وكيل للاتصال بخوادم التفعيل. ويعد ذلك ضروريًا عند استخدام رمز تفعيل لتفعيل التطبيق في جزء شبكة منعزل بدون اتصال بالإنترنت. وإذا كنت تقوم بتفعيل التطبيق باستخدام ملف مفتاح، فلن يكون الوصول إلى الإنترنت ضروريًا.
تمكين الدفاع الذاتي	في حالة تمكين هذه الوظيفة، يمنع Kaspersky Endpoint Security أي تغيير أو حذف لملفات التطبيق على محرك القرص الثابت وعمليات الذاكرة وإدخالات تسجيل النظام.
منع الإدارة الخارجية لخدمات التطبيق	في حالة تمكين هذه الوظيفة، فلن يسمح Kaspersky Endpoint Security بإدارة خدمات التطبيق باستخدام تطبيقات الجهات الخارجية (مثل CMD). وعند إجراء محاولة لإدارة خدمات التطبيقات باستخدام تطبيقات الجهات الخارجية، يتم عرض إشعار في شريط مهام Microsoft Windows، أعلى أيقونة التطبيق (ما لم يتم تعطيل خدمة الإخطار من قبل المستخدم). يمكنك السماح بالإدارة الخارجية لخدمات التطبيق فقط على أجهزة الكمبيوتر التي لا تدعم تقنية AM-PPL أو أجهزة الكمبيوتر التي تم تعطيل التقنية عليها.
تأجيل تشغيل المهام المجدولة أثناء التشغيل على طاقة البطارية	في حالة تحديد خانة الاختيار هذه، يتم تمكين وضع توفير الطاقة عند تشغيل الكمبيوتر على طاقة البطارية. يؤجل Kaspersky Endpoint Security المهام المجدولة. يمكن بدء مهام الفحص والتحديث يدويًا، إذا لزم الأمر. عند تمكين وضع توفير الطاقة وتشغيل الكمبيوتر باستخدام طاقة البطارية، لا يتم تشغيل المهام التالية حتى وإن كانت مجدولة: • فحص كامل. • فحص المناطق الحرجة. • فحص مخصص. • التحقق من سلامة التطبيق. • فحص IOC. • تحديث قواعد البيانات والوحدات النمطية للتطبيق (الإصلاحات فقط) يتخطى التطبيق تحديثات قاعدة البيانات المجدولة فقط عندما يعمل الكمبيوتر المحمول على طاقة البطارية ومستوى البطارية أقل من 30% (القيمة الافتراضية). ويمكنك تغيير الحد الأدنى لمستوى شحن البطارية الذي يبدأ عنده التطبيق في تخطي تحديثات قاعدة بيانات مكافحة الفيروسات المجدولة عن طريق تحرير السجل. وفي جميع الحالات الأخرى، يقوم Kaspersky Endpoint Security بتحديث قواعد البيانات وفقًا للجدول الزمني، بغض النظر عما إذا كان الكمبيوتر المحمول متصلاً بالتيار الكهربائي أو يعمل بطاقة البطارية، أو ما إذا كان التطبيق في وضع توفير الطاقة.
التنازل عن الموارد 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 لمنح الموارد للتطبيقات الأخرى.
تقييد استخدام وحدة المعالجة المركزية لمهام الفحص	لتحسين أداء Kaspersky Endpoint Security، يمكنك تقييد استخدام وحدة المعالجة المركزية عبر مهمة فحص البرامج الضارة. إذا تم تحديد خانة الاختيار، فإن متوسط الحمل على جميع مراكز وحدة المعالجة المركزية من مهمة فحص البرامج الضارة يُقرب القيمة المحددة. بشكل افتراضي، يتم إلغاء تحديد خانة الاختيار.

المعلمة	الوصف
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.
التوافق مع برامج الإدارة عن بعد (متوفر فقط في Kaspersky Security Center (Console	إذا تسبب استخدام Kaspersky Endpoint Security إلى جانب أدوات الإدارة عن بعد (RAT) في حدوث مشكلات، يمكنك تمكين وضع التوافق. وقد تكون المشاكل مرتبطة بعدم توافق أدوات الإدارة عن بُعد مع وظيفة Secure Desktop في التطبيق. ويكون الغرض من هذه الوظيفة تأكيد الإجراءات التي من المحتمل أن تؤدي إلى خفض مستوى أمان الكمبيوتر. وتتيح هذه الوظيفة للتطبيق عرض مربع حوار التأكيد المعزول عن العمليات الأخرى. وتستخدم هذه الوظيفة حقوقًا مرتفعة لتأمين الطلب. وبهذه الطريقة، يستطيع المستخدم فقط تأكيد الإجراء وليس البرامج الضارة. في حالة تحديد هذا الخيار، سيتم تمكين وضع توافق أداة الإدارة عن بُعد. ويعرض التطبيق مربع حوار تأكيد بدون هذه الوظيفة. وقد يقلل هذا من مستوى الأمان للكمبيوتر. لا نوصي بتمكين وضع التوافق إذا كان Kaspersky Endpoint Security لا يسبب مشاكل في أداة الإدارة عن بُعد الخاصة بك. إذا تم إلغاء تحديد هذا الخيار، فسيتم تعطيل وضع التوافق مع أداة الإدارة بُعد. بشكل افتراضي، يتم إلغاء تحديد خانة الاختيار. مثال: عند استخدام المستعرض في وضع RemoteApp، قد لا يعرض Kaspersky Endpoint Security نافذة تأكيد عند زيارة موقع ويب بشهادة غير موثوقة لأن RemoteApp لا يدعم وظيفة Secure Desktop الخاصة بالتطبيق. ويمكن أن يتسبب هذا في عدم استجابة المستعرض. ولكي يعمل المستعرض بشكل صحيح في وضع RemoteApp، يجب عليك تمكين وضع التوافق. يمكنك أيضًا محاولة تمكين وضع التوافق إذا واجهت مشاكل في وظيفة Secure Desktop عند استخدام برامج خاصة بجهات خارجية أخرى.

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.14.2\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.14.2\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 تكامله مع حلول Kaspersky Detection and Response. وفي حالات أخرى، يضع Kaspersky Endpoint Security الملف ذي الصلة في النسخ الاحتياطي. وللحصول على تفاصيل عن 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 وتعليمات Kaspersky Endpoint Detection and Response Expert (on-premises).

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
Delete reports after (days)	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.
Limit the size of report file to (MB)	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.
Delete objects after (days)	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.
Limit the size of Backup to (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.
Limit the size of Quarantine	إذا تم تحديد خانة الاختيار، يتم تحديد الحد الأقصى لحجم العزل ليكون بالقيمة المُحددة. والإعداد الافتراضي لهذا الخيار هو 1024 ميجا بايت. وعندما يصل العزل إلى الحجم الأقصى، يرسل Kaspersky Endpoint Security حدث لا تتوفر مساحة كافية في مخزن العزل 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	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.

المعلمة	الوصف
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. ويمكنك تعطيل نقل بعض البيانات لتحسين مساحة القرص على خادم الإدارة. يرسل التطبيق أحداث الفئات التالية: • **About Quarantine files**. ويمكنك عرض قائمة الملفات المعزولة في لوحة تحكم Kaspersky Security Center في المجلد **Advanced** ← **Repositories** ← **Quarantine**. ولا يستخدم Kaspersky Endpoint Security العزل إلا عند تكامله مع حلول Kaspersky Detection and Response. • **About files in Backup**. ويمكنك عرض قائمة الملفات في النسخ الاحتياطي في لوحة تحكم Kaspersky Security Center في المجلد **Advanced** ← **Repositories** ← **Backup**. • **About unprocessed files**. يمكنك عرض قائمة الملفات المدعومة في وحدة تحكم Kaspersky Security Center في المجلد **Advanced** ← **Repositories** ← **Active threats**. • **About installed devices**. يمكنك عرض قائمة الأجهزة المتصلة في لوحة تحكم Kaspersky Security Center في المجلد **Advanced** ← **Repositories** ← **Hardware**. وتتوفر قائمة الأجهزة أيضًا في خصائص الكمبيوتر وفي سياسة Kaspersky Endpoint Security for Windows (قسم **التحكم في الجهاز**). • **About started applications**. يمكنك عرض قائمة الملفات القابلة للتنفيذ في وحدة تحكم Kaspersky Security Center في المجلد **Advanced** ← **Executable files** ← **Application management**. وتتوفر قائمة الملفات القابلة للتنفيذ أيضًا في خصائص الكمبيوتر. • **About file encryption errors**. يمكنك عرض قائمة بأخطاء تشفير الملفات في وحدة تحكم Kaspersky Security Center في المجلد **Advanced** ← **Data encryption and protection** ← **Encryption events**. وتتوفر قائمة الأخطاء أيضًا في خصائص الكمبيوتر. • **Report on Adaptive Anomaly Control rules state**. يمكنك عرض التقرير في لوحة تحكم Kaspersky Security Center في عقدة **Administration Server** في علامة التبويب **Reports**. ويتوفر هذا التقرير أيضًا في خصائص سياسة Kaspersky Endpoint Security for Windows (قسم **مراقبة عيوب التكيف**). • **Report on triggered Adaptive Anomaly Control rules**. يمكنك عرض التقرير في لوحة تحكم Kaspersky Security Center في عقدة **Administration Server** في علامة التبويب **Reports**. ويتوفر هذا التقرير أيضًا في خصائص سياسة Kaspersky Endpoint Security for Windows (قسم **مراقبة عيوب التكيف**). • **About a threat development chain**. ويمكنك عرض تفاصيل الاكتشاف في Kaspersky Security Center Web Console في قسم **Monitoring** ← **Alerts**. ويتم استخدام المعلومات عن سلسلة تطوير التهديد بواسطة حلول Kaspersky Endpoint Detection and Response.

إعدادات الشبكة

يمكنك تكوين الخادم الوكيل الذي يتم استخدامه للاتصال بالإنترنت وتحديث قواعد بيانات مكافحة الفيروسات، قم بتحديد وضع مراقبة منافذ الشبكة وإعداد 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.
إعدادات 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 الوكيل للعناوين المحلية	إذا تم تحديد خانة الاختيار هذه، فلن يستخدم Kaspersky Endpoint Security الخادم الوكيل عند إجراء تحديث من مجلد مشارك.

المعلمة	الوصف
إعدادات مصادقة الخادم الوكيل	لمصادقة التطبيق على الخادم الوكيل للوصول إلى الإنترنت، يجب إدخال بيانات اعتماد المستخدم. ويدعم Kaspersky Endpoint Security المصادقة التلقائية على الخادم الوكيل. وإذا فشلت المصادقة التلقائية، سيطالبك التطبيق بإدخال بيانات الاعتماد. **عدم استخدام المصادقة**. **مصادقة NTLM**. مصادقة NTLM باستخدام حساب المستخدم الحالي (افتراضي). **مصادقة NTLM باستخدام اسم المستخدم وكلمة المرور**. مصادقة NTLM باستخدام بيانات اعتماد محددة يدويًا. **اسم المستخدم وكلمة المرور**. المصادقة باستخدام بيانات اعتماد محددة يدويًا. **المصادقة التلقائية**. **مصادقة Kerberos**. مصادقة Kerberos باستخدام حساب المستخدم الحالي. للتأكد من أن مصادقة Kerberos تعمل بشكل صحيح عند استخدام سجلات CNAME لعنوان الخادم الوكيل، يجب عليك تسجيل اسم الخدمة الرئيسي (SPN) لكل سجل CNAME. **مصادقة Kerberos مع اسم المستخدم وكلمة المرور**. مصادقة Kerberos باستخدام بيانات اعتماد محددة يدويًا. إذا تم تحديد مصادقة Kerberos، فإن Kaspersky Endpoint Security يستطيع، بناءً على إعدادات الخادم الوكيل، إجراء المصادقة باستخدام إما بروتوكول Kerberos أو NTLM.
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.
زيارة مجال بشهادة 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**. 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.
زيارة مجال يتضمن خطأ في فحص الاتصالات المشفرة	• **منع**. في حالة ظهور خطأ في فحص الاتصالات المشفرة، يحظر Kaspersky Endpoint Security اتصال الشبكة. • **السماح بالمجال وإضافته إلى الاستثناءات**. في حالة 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**. ينشئ Kaspersky Endpoint Security أيضًا حدثًا لخطأ فحص الاتصال المشفر.
منع اتصالات SSL 2.0	في حالة تحديد خانة الاختيار، يراقب التطبيق ويحظر 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. ومع ذلك، لا يراقب التطبيق حركة شبكة الاتصال عبر هذا البروتوكول.

المعلمة	الوصف
منع اتصالات SSL 3.0	في حالة تحديد خانة الاختيار، لن يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 3.0. في حالة إلغاء تحديد خانة الاختيار، لا يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول SSL 3.0. ويراقب التطبيق حركة شبكة الاتصال عبر هذا البروتوكول. وتعمل جميع مكونات التطبيق دون قيود.
منع اتصالات TLS 1.0	في حالة تحديد خانة الاختيار، لن يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول TLS 1.0. في حالة إلغاء تحديد خانة الاختيار، لا يحظر التطبيق اتصالات شبكة الاتصال التي يتم إنشاؤها عبر بروتوكول TLS 1.0. ويراقب التطبيق حركة شبكة الاتصال عبر هذا البروتوكول. وتعمل جميع مكونات التطبيق دون قيود.
فك تشفير اتصال مشفر بموقع الويب الذي يستخدم شهادات تحقق من الصحة موسعة	تؤكد شهادات EV (Extended Validation Certificate) 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.
تكوين 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 وWeb Control 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`.
تكوين 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.
لفحص الاتصالات المشفرة في التطبيقات باستخدام مخزن الشهادات الخاص بها، استخدم (متوفر فقط في واجهة Kaspersky (Endpoint Security	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. يستخدم التطبيق شهادة جذر Kaspersky لفك تشفير البيانات المشفرة وتحليلها. يمكنك تحديد مخزن الشهادات الذي سيحتوي على شهادة جذر Kaspersky. • **مخزن شهادات Windows (مستحسن)**. تتم إضافة شهادة جذر Kaspersky إلى هذا المخزن أثناء تثبيت Kaspersky Endpoint Security. • **مخزن الشهادات الخاص**. 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.

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. ويعرض Kaspersky Endpoint Security أيضًا الإخطارات التي تتطلب إجراءً من المستخدم أعلى أيقونة 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 عرض واجهة المستخدم**. على جهاز كمبيوتر عميل، لا يتم عرض أي علامات لعملية تشغيل برنامج Kaspersky Endpoint Security. الرمز الموجود في منطقة إخطار Windows والإخطارات غير متاحين.
Access to 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. في حالة إلغاء تحديد خانة الاختيار هذه، يتم إخفاء المهام المحلية في واجهة التطبيق. 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.
View group tasks	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.
Manage group tasks	في حالة تحديد خانة الاختيار، يمكن للمستخدمين بدء وإيقاف المهام الجماعية المحددة في وحدة تحكم 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 يبدأ المسؤول المهام يدويًا في وحدة تحكم Kaspersky Security Center.
تكوين الإخطارات	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.
تكوين الإخطارات عبر البريد الإلكتروني	إعدادات خادم SMTP لتسليم الإخطارات الخاصة بالأحداث المسجلة خلال تشغيل التطبيق. بشكل افتراضي، يستخدم Kaspersky Endpoint Security إعدادات إخطارات البريد الإلكتروني من Kaspersky Security Center. وللمزيد من التفاصيل عن إعدادات إخطارات البريد الإلكتروني، يُرجى الرجوع إلى تعليمات Kaspersky Security Center. إذا كنت بحاجة إلى تكوين إخطار بريد إلكتروني فردي، يمكنك تحرير الإعدادات التالية: • **عنوان المرسل**. عنوان البريد الإلكتروني للمرسل. لا ينصح باستخدام عنوان غير موجود. • **خادم SMTP**. عنوان واحد أو أكثر من عناوين خوادم البريد الإلكتروني لمؤسستك (على سبيل المثال، `mail.company.com`). يمكنك إدخال عنوان IP (IPv4 أو IPv6). لمصادقة المستخدم على خادم SMTP، أدخل بيانات اعتماد المرسل في الحقول المقابلة. ولاختبار إخطارات البريد الإلكتروني، يمكنك إرسال رسالة اختبار. • **عنوان المستلم**. عناوين البريد الإلكتروني للمستلمين الذين سيرسل لهم التطبيق إخطارات. • **وضع الإرسال**. وضع إرسال إخطارات البريد الإلكتروني. قد يرسل Kaspersky Endpoint Security رسائل على الفور عند وقوع حدث ما ؛ أو بدلاً من ذلك، يمكنه اتباع جدولة معدة مسبقًا.
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 لحساب KLAdmin.
دعم المستخدم / الروابط الخاصة بالموارد على الويب (متوفر فقط في Kaspersky Security Center (Console	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.
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.

قد لا تكون وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية) متاحة في التطبيق في الولايات المتحدة.

تحتاج التحديثات المنتظمة ترخيص ساريًا. في حالة عدم وجود ترخيص موجود، سيكون بإمكانك إجراء تحديث لمرة واحدة فقط.

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.

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.

إذا كان التطبيق يعمل في وضع Light Agent، يتم تضمين اعتبارات خاصة في تحديث قواعد بيانات التطبيق والوحدات النمطية.

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. **Manually**. يتيح لك وضع تشغيل مهمة التحديث هذا ببدء مهمة التحديث يدويًا. **By schedule**. 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.
Run missed tasks	في حالة تحديد خانة الاختيار، يبدأ Kaspersky Endpoint Security في تشغيل المهمة التي تم تخطيها بمجرد أن يكون هذا ممكنًا. ويمكن تخطي المهمة، على سبيل المثال، إذا كان الكمبيوتر مغلقًا في وقت بدء المهمة المجدولة. وعندما يحصل التطبيق على فرصة لتنفيذ المهام الفائتة، يقوم بتشغيل المهام بشكل عشوائي خلال فترة زمنية معينة لتوزيع الحمل على الكمبيوتر. في حالة إلغاء تحديد خانة الاختيار هذه، لن يبدأ Kaspersky Endpoint Security في تشغيل المهام التي تم تخطيها. وكبديل، سيقوم بتشغيل المهمة 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. إذا كانت خوادم تحديث Kaspersky غير متوفرة، فيمكن أن يستخدم Kaspersky Endpoint Security مجالات بديلة لتحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق الخاصة به. وللحصول على معلومات مفصلة، ارجع إلى قاعدة معارف الدعم الفني. 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. بشكل افتراضي، يستخدم Kaspersky Endpoint Security خادم Kaspersky Security Center كأول مصدر تحديث. ويساعد هذا في الحفاظ على حركة المرور عند التحديث. وإذا لم يتم تطبيق سياسة على الكمبيوتر، سيتم تحديد خوادم Kaspersky كأول مصدر تحديث في إعدادات المهمة المحلية تحديث قواعد البيانات والوحدات النمطية للتطبيق لأن التطبيق قد لا يتمكن من الوصول إلى خادم Kaspersky Security Center. إذا كان التطبيق يعمل في وضع Light Agent، يتم تحديد مجلد على SVM كمصدر للتحديث.
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.

المعلمة	الوصف
تنزيل تحديثات الوحدات النمطية للتطبيق	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. يتم تحديد خانة الاختيار 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.14.2\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 للتكوين التلقائي للخادم الوكيل يستخدم Kaspersky Endpoint Security بروتوكول WPAD (Web Proxy Auto-Discovery Protocol). إذا تعذر تحديد عنوان IP الخاص بالخادم الوكيل باستخدام هذا البروتوكول، فسوف يستخدم Kaspersky Endpoint Security عنوان الخادم الوكيل الذي تم تحديده في إعدادات مستعرض 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 موثوق.

  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.
  - وضع المستخدم التطبيق في المجموعة مقيد 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 مقيد بشكل عالٍ.

  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 موثوق.

  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 و Windows 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 - لمستندMicrosoft 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 XML)، xltx – 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 XML)، xltx – 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 وKaspersky Security Center قناة اتصال مشفرة مع TLS (أمن طبقة النقل) للعمل مع الخدمات الخارجية من Kaspersky.

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.

العنوان	الوصف
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.

العنوان	الوصف
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 cm.k.kaspersky-labs.com البروتوكول: HTTP المنفذ: 80	تحديث قواعد البيانات والوحدات النمطية لبرامج التطبيق.
ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.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: KSN المنفذ: 1443، 443	استخدام Kaspersky Security Network.
click.kaspersky.com redirect.kaspersky.com البروتوكول: HTTPS المنفذ: 443	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` – Critical، `4` – Functional failure، `3` – Warning، `2` – Info.
- `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.

ما مدة تخزين الأحداث على الخادم

حرج

انتهت صلاحية الترخيص

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)	✓

الترخيص على وشك انتهاء صلاحيته

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	203
معرف حدث Kaspersky Security Center	000000cb

سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

قواعد البيانات مفقودة أو تالفة

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	206
معرف حدث Kaspersky Security Center	000000ce
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	–

قواعد البيانات قديمة للغاية

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	207
معرف حدث Kaspersky Security Center	000000cf
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تم تعطيل التشغيل التلقائي للتطبيق

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	209
معرف حدث Kaspersky Security Center	000000d1
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

خطأ في التفعيل

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	229
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تم اكتشاف تهديد نشط. يجب بدء التنظيف المتقدم

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	231
معرف حدث Kaspersky Security Center	000000e7
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

خوادم KSN غير متاحة

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	2023
معرف حدث Kaspersky Security Center	000007e7
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لا تتوفر مساحة كافية في مخزن العزل

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	343
معرف حدث Kaspersky Security Center	00000157
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لم تتم استعادة الكائن من العزل

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	346
معرف حدث Kaspersky Security Center	0000015a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لم يتم حذف الكائن من العزل

الحالة	⚠
المكون	تدقيق النظام
معرف حدث Windows	348

معرف حدث Kaspersky Security Center	0000015c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

أنشأ التطبيق اتصالاً بموقع ويب لديه شهادة غير موثوق بها

الحالة	!
المكون	تدقيق النظام
معرف حدث Windows	57
معرف حدث Kaspersky Security Center	00000039
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

فشل التحقق من اتصال مشفر. تمت إضافة المجال إلى قائمة الاستثناءات

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 مكافحة أداة التشفير 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): 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 مكافحة أداة التشفير 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

يتعذر التنظيف

الحالة	!
المكون	الحماية من تهديدات الملفات الحماية من تهديدات البريد منع اختراق المضيف اكتشاف السلوك مكافحة أداة التشفير 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): 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 مكافحة أداة التشفير 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة شبكة KSN الخاصة (blacklist): true أو 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة شبكة KSN الخاصة (blacklist): true أو 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة شبكة KSN الخاصة (blacklist): true أو 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: المجاميع الاختبارية للعملية / الكائن المصدر والعملية / الكائن الهدف. تم منع العملية (verdict_type): true أو false. معرف أمان المستخدم (SID).
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لم تتم مصادقة لوحة المفاتيح

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)	✓

تم اكتشاف هجوم عبر الشبكة

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)	✓

تم حظر بدء تشغيل التطبيق

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)	✓

يتم حظر التشغيل مع الجهاز حتى يتم بدء Kaspersky Endpoint Security

الحالة	⚠
المكون	التحكم في الجهاز
معرف حدث Windows	816
معرف حدث Kaspersky Security Center	00000330
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

يتم حظر اتصال الجهاز حتى يتم بدء تشغيل Kaspersky Endpoint Security

الحالة	⚠
المكون	التحكم في الجهاز
معرف حدث Windows	817
معرف حدث Kaspersky Security Center	00000331
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Error updating component

الحالة	⚠
المكون	تحديث
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
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
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
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

معرف حدث Windows	1017
معرف حدث Kaspersky Security Center	000003f9
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

حدث خطأ أثناء التحقق من قواعد بيانات التطبيق والوحدات النمطية

الحالة	!
المكون	تحديث
معرف حدث Windows	1018
معرف حدث Kaspersky Security Center	000003fa
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

حدث خطأ في التفاعل مع Kaspersky Security Center

الحالة	!
المكون	تحديث
معرف حدث Windows	1019
معرف حدث Kaspersky Security Center	000003fb
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لم يتم تحديث كافة المكونات

الحالة	!
المكون	تحديث
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
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
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
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)	–

خطأ في تمكين الوضع المحمول

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	Sandbox

معرف حدث Windows	2252
معرف حدث Kaspersky Security Center	000008cc
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object not quarantined (Sandbox)

الحالة	⚠
المكون	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	Sandbox
معرف حدث Windows	2607
معرف حدث Kaspersky Security Center	00000a2f
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid Sandbox server certificate

الحالة	⚠
المكون	Sandbox
معرف حدث Windows	2613
معرف حدث Kaspersky Security Center	00000a35
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The Sandbox node is unavailable

الحالة	⚠
المكون	Sandbox
معرف حدث Windows	2614
معرف حدث Kaspersky Security Center	00000a36
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Failed to process the object in Sandbox

الحالة	⚠
المكون	Sandbox
معرف حدث Windows	2617
معرف حدث Kaspersky Security Center	00000a39
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Maximum load to Sandbox is exceeded

الحالة	⚠
المكون	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)	✓

Sandbox license verification failed

الحالة	⚠
المكون	Sandbox
معرف حدث Windows	2620
معرف حدث Kaspersky Security Center	00000a3c
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

فشل إرسال مهمة الفحص إلى Sandbox بواسطة مستخدم

الحالة	⚠
المكون	Sandbox
معرف حدث Windows	2623
معرف حدث Kaspersky Security Center	00000a3e
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

حدث خطأ في إنشاء مهمة Sandbox

الحالة	⚠
المكون	Sandbox
معرف حدث Windows	2621
معرف حدث Kaspersky Security Center	00000a3d
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 EDR Expert server

الحالة	⚠
المكون	Endpoint Detection and Response Expert (on-premises)
معرف حدث Windows	2850
معرف حدث Kaspersky Security Center	00000b22
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid certificate of the EDR Expert server

الحالة	⚠
المكون	Endpoint Detection and Response Expert (on-premises)
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 EDR Expert server

الحالة	ⓘ
المكون	Endpoint Detection and Response Expert (on-premises)
معرف حدث Windows	2852
معرف حدث Kaspersky Security Center	00000b24
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

خطأ في الاتصال بخادم الاستجابة لأداة EDR Expert

الحالة	ⓘ
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2858
معرف حدث Kaspersky Security Center	00000b22
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة خادم غير صالحة لخادم الاستجابة لأداة EDR Expert

الحالة	ⓘ
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2859
معرف حدث Kaspersky Security Center	00000b23
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة غير صالحة للعميل على خادم الاستجابة لأداة EDR Expert

الحالة	ⓘ
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2860
معرف حدث Kaspersky Security Center	00000b24
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

خطأ في الاتصال بخادم جمع القياس عن بعد لأداة EDR Expert

الحالة	!
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2854
معرف حدث Kaspersky Security Center	00000b22
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة خادم غير صالحة لخادم جمع القياس عن بعد لأداة EDR Expert

الحالة	!
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2855
معرف حدث Kaspersky Security Center	00000b23
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة غير صالحة للعميل على خادم جمع القياس عن بعد لأداة EDR Expert

الحالة	!
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2856
معرف حدث Kaspersky Security Center	00000b24
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

خطأ في الاتصال بخادم NDR

الحالة	!
المكون	Network Detection and Response (KATA)
معرف حدث Windows	3080
معرف حدث Kaspersky Security Center	00000c08
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة خادم NDR غير صالحة

الحالة	⊗
المكون	Network Detection and Response (KATA)
معرف حدث Windows	3081
معرف حدث Kaspersky Security Center	00000c09
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة غير صالحة للعميل على خادم NDR

الحالة	⊗
المكون	Network Detection and Response (KATA)
معرف حدث Windows	3082
معرف حدث Kaspersky Security Center	00000c0a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

جهازك متصل بخادم الإدارة غير الموثوق به. اتصل بالمسؤول

الحالة	⊗
المكون	حماية الاتصال بخادم الإدارة
معرف حدث Windows	3301
معرف حدث Kaspersky Security Center	00000ce5
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File or folder change was detected

الحالة	⊗ / ⚠ / ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2950
معرف حدث Kaspersky Security Center	00000b86
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاحتفاظ للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Event aggregation started .Object changes too often

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2955
معرف حدث Kaspersky Security Center	00000b8b
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Report on object modification for the aggregation period

الحالة	
المكون	مراقبة سلامة النظام
معرف حدث Windows	2953
معرف حدث Kaspersky Security Center	00000b89
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2956
معرف حدث Kaspersky Security Center	00000b8c
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاحتفاظ للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Registry change was detected

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2951

معرف حدث Kaspersky Security Center	00000b87
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاحتفاظ للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Device connection / disconnection is detected

الحالة	ⓘ / ⚠ / ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2952
معرف حدث Kaspersky Security Center	00000b88
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاحتفاظ للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

يتضمن نطاق المراقبة كائنات غير صحيحة

الحالة	ⓘ / ⚠ / ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2903
معرف حدث Kaspersky Security Center	00000b89
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاحتفاظ للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Event aggregation started .Attempts to perform the restricted operations with the object is too many

الحالة	ⓘ
المكون	مراقبة سلامة النظام

معرف حدث Windows	2963
معرف حدث Kaspersky Security Center	00000b93
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

An operation with the files of the monitoring scope was blocked

الحالة	⚠
المكون	مراقبة سلامة النظام
معرف حدث Windows	2959
معرف حدث Kaspersky Security Center	00000b8f
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاحتفاظ للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Registry modification blocked

الحالة	⚠
المكون	مراقبة سلامة النظام
معرف حدث Windows	2960
معرف حدث Kaspersky Security Center	00000b90
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاحتفاظ للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Processing error

الحالة	⚠
المكون	مراقبة سلامة النظام
معرف حدث Windows	2954
معرف حدث Kaspersky Security Center	00000b8a

سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

System Integrity Monitoring: rule triggering disabled for user accounts without matching security identifier (SID)

الحالة	⊗
المكون	مراقبة سلامة النظام
معرف حدث Windows	2964
معرف حدث Kaspersky Security Center	00000b94
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Application Control: rule triggering disabled for user accounts without matching security identifier (SID)

الحالة	⊗
المكون	التحكم في التطبيقات
معرف حدث Windows	711
معرف حدث Kaspersky Security Center	000002c7
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Device Control: rule triggering disabled for user accounts without matching security identifier (SID)

الحالة	⊗
المكون	التحكم في الجهاز
معرف حدث Windows	810
معرف حدث Kaspersky Security Center	0000032a
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Web Control: rule triggering disabled for user accounts without matching security identifier (SID)

الحالة	⚠
المكون	التحكم في الويب
معرف حدث Windows	757
معرف حدث Kaspersky Security Center	000002f5
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Adaptive Anomaly Control: rule triggering disabled for user accounts without matching security identifier (SID)

الحالة	⚠
المكون	مراقبة عيوب التكيف
معرف حدث Windows	504
معرف حدث Kaspersky Security Center	000001f8
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Log Inspection: rule triggering disabled for user accounts without matching security identifier (SID)

الحالة	⚠
المكون	فحص السجل
معرف حدث Windows	2810
معرف حدث Kaspersky Security Center	00000afa
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

SVM is unavailable

الحالة	⚠
المكون	Light Agent
معرف حدث Windows	3151
معرف حدث Kaspersky Security Center	00000c4f
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Advanced Disinfection should be started on a virtual machine template .Malicious object detected

الحالة	ⓘ
المكون	Light Agent
معرف حدث Windows	3182
معرف حدث Kaspersky Security Center	00000c6e
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تم حظر اتصال الشبكة الذي تم إنشاؤه عبر البروتوكول القديم

الحالة	ⓘ
المكون	الحماية
معرف حدث Windows	75
معرف حدث Kaspersky Security Center	0000004b
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

خطأ في الاتصال بخادم KUMA

الحالة	ⓘ
المكون	تكامل KUMA
معرف حدث Windows	2854
معرف حدث Kaspersky Security Center	00000b26
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة خادم KUMA غير صالحة

الحالة	ⓘ
المكون	تكامل KUMA
معرف حدث Windows	2855
معرف حدث Kaspersky Security Center	00000b27
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

شهادة غير صالحة للعميل على خادم KUMA

الحالة	!
المكون	تكامل KUMA
معرف حدث Windows	2856
معرف حدث Kaspersky Security Center	00000b28
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

SIEM server connection error

الحالة	!
المكون	تكامل KUMA
معرف حدث Windows	3250
معرف حدث Kaspersky Security Center	00000cb2
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid certificate of the SIEM server

الحالة	!
المكون	تكامل KUMA
معرف حدث Windows	3251
معرف حدث Kaspersky Security Center	00000cb3
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Invalid certificate of the agent on the SIEM server

الحالة	!
المكون	تكامل KUMA
معرف حدث Windows	3252
معرف حدث Kaspersky Security Center	00000cb4
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)	✓

Settings not applied .Invalid task settings

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 مكافحة أداة التشفير 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): true أو false. إصدار EDR. معرف التهديد في EDR. تجزئة MD5 للكائن.
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

The operating system settings do not allow to control access to Wi-Fi networks

الحالة	⚠
المكون	التحكم في الجهاز
معرف حدث Windows	249
معرف حدث Kaspersky Security Center	000000f9
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Object not restored 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 مكافحة أداة التشفير 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	0000013a
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 مكافحة أداة التشفير مكافحة أداة التشفير فحص البرامج الضارة
معرف حدث Windows	303
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. • 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 (type).
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 مكافحة أداة التشفير مكافحة أداة التشفير فحص البرامج الضارة
معرف حدث Windows	303
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 (type).
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 مكافحة أداة التشفير 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): true 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 مكافحة أداة التشفير 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 مكافحة أداة التشفير 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)	✓

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)	✓

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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): 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 (type). • GNRL_EA_PARAM_9 هي معلومات إضافية حول الكائن المكتشف: مكون التطبيق (engine). تقنية اكتشاف التهديدات (method). تم اكتشاف تهديد بواسطة Kaspersky Private Security Network (blacklist): 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 canceled by the user

الحالة	⚠
المكون	تحديث
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 سلامة النظام
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	Endpoint Sensor
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	Endpoint Sensor
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 the administrator

الحالة	⚠
المكون	Endpoint Sensor
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
Endpoint Sensor	المكون
2107	معرف حدث Windows
0000083b	معرف حدث Kaspersky Security Center
✓	سجل أحداث Windows (افتراضي)
✓	سجل أحداث Kaspersky Security Center (افتراضي)

Network activity of all third-party applications is unblocked

⚠	الحالة
Endpoint Sensor	المكون
2108	معرف حدث Windows
0000083c	معرف حدث Kaspersky Security Center
✓	سجل أحداث Windows (افتراضي)
✓	سجل أحداث Kaspersky Security Center (افتراضي)

Object will be deleted after restart (Sandbox)

⚠	الحالة
Sandbox	المكون
2605	معرف حدث Windows
00000a2d	معرف حدث Kaspersky Security Center
✓	سجل أحداث Windows (افتراضي)
✓	سجل أحداث Kaspersky Security Center (افتراضي)

Total size of scan tasks exceeded the limit

⚠	الحالة
Sandbox	المكون
2612	معرف حدث Windows
00000a34	معرف حدث Kaspersky Security Center

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)	✓

Connection to a website with an untrusted certificate is established by user decision

الحالة	⚠
المكون	Network Detection and Response (KATA)
معرف حدث Windows	70
معرف حدث Kaspersky Security Center	00000046
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)	✓

Starting the cloud service client application is blocked

الحالة	⚠
المكون	Cloud Discovery
معرف حدث Windows	2212
معرف حدث Kaspersky Security Center	000008a4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Access to the cloud service is blocked

الحالة	⚠
المكون	Cloud Discovery
معرف حدث Windows	2213
معرف حدث Kaspersky Security Center	000008a5
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File or folder change was detected

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2950
معرف حدث Kaspersky Security Center	00000b86
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Event aggregation started .Object changes too often

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2955
معرف حدث Kaspersky Security Center	00000b8b
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Report on object modification for the aggregation period

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2956
معرف حدث Kaspersky Security Center	00000b8c
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Registry change was detected

الحالة	/ /
المكون	مراقبة سلامة النظام

معرف حدث Windows	2951
معرف حدث Kaspersky Security Center	00000b87
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Device connection / disconnection is detected

الحالة	ⓘ / ⚠ / ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2952
معرف حدث Kaspersky Security Center	00000b88
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

يتضمن نطاق المراقبة كائنات غير صحيحة

الحالة	ⓘ / ⚠ / ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2903
معرف حدث Kaspersky Security Center	00000b89
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

The prohibited operation was allowed in test mode

الحالة	⚠
المكون	مراقبة سلامة النظام
معرف حدث Windows	2961
معرف حدث Kaspersky Security Center	00000b91
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تعذر الاتصال بخادم التكامل لأكثر من 30 دقيقة. تحقق من حالة خادم التكامل وإعدادات الشبكة

الحالة	⚠
المكون	Light Agent
معرف حدث Windows	3102
معرف حدث Kaspersky Security Center	00000c1e
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Check Integration Server status and .Unable to connect to the Integration Server for more than 6 hours network settings

الحالة	⚠
المكون	Light Agent
معرف حدث Windows	3103
معرف حدث Kaspersky Security Center	00000c1f
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

يتعذر الاتصال بخادم التكامل. تحقق من حالة خادم التكامل وإعدادات الشبكة

الحالة	⚠
المكون	Light Agent
معرف حدث Windows	3101
معرف حدث Kaspersky Security Center	00000c1d
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

قالب الجهاز الافتراضي بحاجة إلى تحديث

الحالة	⚠
المكون	Light Agent
معرف حدث Windows	3181
معرف حدث Kaspersky Security Center	00000c6d
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

The application is running under the Enterprise license .The Standard license is terminated

الحالة	⚠
المكون	Light Agent
معرف حدث Windows	3171
معرف حدث Kaspersky Security Center	00000c64
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

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)	✓

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)	✓

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 مكافحة أداة التشفير منع اختراق المضيف 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 مكافحة أداة التشفير 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
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
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 مكافحة أداة التشفير 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
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
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
معرف حدث Windows	1003
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File downloaded

الحالة	
المكون	تحديث
معرف حدث Windows	1004
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File installed

الحالة	
المكون	تحديث
معرف حدث Windows	1005
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

File updated

الحالة	ⓘ
المكون	تحديث
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
معرف حدث Windows	1007
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Updating files

الحالة	ⓘ
المكون	تحديث
معرف حدث Windows	1008
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Distributing updates

الحالة	ⓘ
المكون	تحديث
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
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
معرف حدث Windows	1013
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Downloading patches

الحالة	
المكون	تحديث
معرف حدث Windows	2150
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Installing patch

الحالة	
المكون	تحديث
معرف حدث Windows	2151
معرف حدث Kaspersky Security Center	–

سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

Patch installed

الحالة	ⓘ
المكون	تحديث
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
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
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	Endpoint Sensor
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	Endpoint Detection and Response Expert (on-premises)
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 (Sandbox)

الحالة	ⓘ
المكون	Sandbox
معرف حدث Windows	2602
معرف حدث Kaspersky Security Center	00000a2a
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Object deleted (Sandbox)

الحالة	
المكون	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	Sandbox
معرف حدث Windows	2606
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

الحالة	ⓘ
المكون	Sandbox
معرف حدث Windows	2609
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

الحالة	
المكون	Sandbox
معرف حدث Windows	2610
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

الحالة	
المكون	Sandbox
معرف حدث Windows	2616
معرف حدث Kaspersky Security Center	–
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	–

تم تعيين خادم الإدارة الذي يتصل به جهازك كخادم موثوق به

الحالة	
المكون	حماية الاتصال بخادم الإدارة
معرف حدث Windows	3300
معرف حدث Kaspersky Security Center	00000ce4
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

جهازك متصل بخادم الإدارة الموثوق به الجديد

الحالة	
المكون	حماية الاتصال بخادم الإدارة
معرف حدث Windows	3302
معرف حدث Kaspersky Security Center	00000ce6

سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لم يعد خادم الإدارة الذي يتصل به جهازك معينًا كخادم موثوق به

الحالة	ⓘ
المكون	حماية الاتصال بخادم الإدارة
معرف حدث Windows	3303
معرف حدث Kaspersky Security Center	00000ce7
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Asynchronous Sandbox detection

الحالة	ⓘ
المكون	Sandbox
معرف حدث Windows	2619
معرف حدث Kaspersky Security Center	GNRL_EV_APP_INCIDENT_OCCURED
معلمات الحدث	• GNRL_EA_PARAM_1 هي معلمات مكونات 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)	✓

The scan task has been successfully sent to Sandbox by a user

الحالة	ⓘ
المكون	Sandbox
معرف حدث Windows	2622
معرف حدث Kaspersky Security Center	00000a3e
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)	✓

Successful connection to the EDR Expert server

الحالة	ⓘ
المكون	Endpoint Detection and Response Expert (on-premises)
معرف حدث Windows	2853
معرف حدث Kaspersky Security Center	00000b25
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تم الاتصال بنجاح بخادم الاستجابة لأداة EDR Expert

الحالة	ⓘ
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2853
معرف حدث Kaspersky Security Center	00000b25
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تم الاتصال بنجاح بخادم جمع القياس عن بعد لأداة EDR Expert

الحالة	
المكون	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
معرف حدث Windows	2857
معرف حدث Kaspersky Security Center	00000b26
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تم الاتصال بنجاح بخادم NDR

الحالة	
المكون	Network Detection and Response (KATA)
معرف حدث Windows	3083
معرف حدث Kaspersky Security Center	00000c0b
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Starting the cloud service client application is allowed

الحالة	
المكون	Cloud Discovery
معرف حدث Windows	2210
معرف حدث Kaspersky Security Center	000008a2
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Access to the cloud service is allowed

الحالة	
المكون	Cloud Discovery
معرف حدث Windows	2211
معرف حدث Kaspersky Security Center	000008a3
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

الوصول إلى المنطقة المحمية

الحالة	
المكون	تدقيق النظام
معرف حدث Windows	2004
معرف حدث Kaspersky Security Center	000007d4
سجل أحداث Windows (افتراضي)	✓
سجل أحداث Kaspersky Security Center (افتراضي)	✓

File or folder change was detected

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2950
معرف حدث Kaspersky Security Center	00000b86
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Event aggregation started .Object changes too often

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2955
معرف حدث Kaspersky Security Center	00000b8b
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Report on object modification for the aggregation period

الحالة	/ /
المكون	مراقبة سلامة النظام
معرف حدث Windows	2956
معرف حدث Kaspersky Security Center	00000b8c

سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Registry change was detected

الحالة	ⓘ / ⚠ / ⓧ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2951
معرف حدث Kaspersky Security Center	00000b87
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Device connection / disconnection is detected

الحالة	ⓘ / ⚠ / ⓧ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2952
معرف حدث Kaspersky Security Center	00000b88
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

يتضمن نطاق المراقبة كائنات غير صحيحة

الحالة	ⓘ / ⚠ / ⓧ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2903

معرف حدث Kaspersky Security Center	00000b89
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Baseline created

الحالة	ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2957
معرف حدث Kaspersky Security Center	00000b8d
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Baseline updated

الحالة	ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2958
معرف حدث Kaspersky Security Center	00000b8e
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

An operation is performed by the trusted user

الحالة	ⓘ
المكون	مراقبة سلامة النظام
معرف حدث Windows	2962
معرف حدث Kaspersky Security Center	00000b92
سجل أحداث Windows (افتراضي)	–

سجل أحداث Kaspersky Security Center (افتراضي)	✓

لتكوين فترة الاحتفاظ لهذا الحدث، انتقل إلى قسم **Event configuration** في السياسة وقم بتعيين فترة الاستبقاء للحدث العام لمراقبة سلامة النظام - File or folder change was detected.

Connected to SVM

الحالة	ⓘ
المكون	Light Agent
معرف حدث Windows	3152
معرف حدث Kaspersky Security Center	00000c50
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

A new temporary password was created

الحالة	ⓘ
المكون	تدقيق النظام
معرف حدث Windows	265
معرف حدث Kaspersky Security Center	00000109
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Connected to the Integration Server

الحالة	ⓘ
المكون	Light Agent
معرف حدث Windows	3105
معرف حدث Kaspersky Security Center	00000c21
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

Restoring connection to the Integration Server

الحالة	
المكون	Light Agent
معرف حدث Windows	3104
معرف حدث Kaspersky Security Center	00000c20
سجل أحداث Windows (افتراضي)	–
سجل أحداث Kaspersky Security Center (افتراضي)	✓

تم الاتصال بنجاح بخادم KUMA

الحالة	
المكون	تكامل KUMA
معرف حدث Windows	2857
معرف حدث Kaspersky Security Center	00000b29
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.

امتدادات الملفات المدعومة لمنع التنفيذ

اسم التطبيق	الملف القابل للتنفيذ	ملحق الملف
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf

اسم التطبيق	الملف القابل للتنفيذ	ملحق الملف
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 مستعرض Yandex Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

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 و javaw.exe).

الملحق رقم 9. نطاق فحص IOC في التسجيل (RegistryItem)

عندما تضيف نوع البيانات **Windows registry - RegistryItem** إلى نطاق فحص مؤشرات الاختراق، 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 وXML في إصدارات OpenIOC القياسية المفتوحة 1.0 و1.1 لوصف مؤشرات الاختراق.
- بعد تحميل ملفات مؤشرات الاختراق، يمكنك تحرير الملفات يدويًا في المحرر المدمج مباشرة في خصائص المهمة. ويدعم Kaspersky Endpoint Security تحرير ملفات مؤشرات الاختراق المتوافقة مع معيار OpenIOC 1.1. ولا يمكن تعديل محتوى ملفات مؤشر الاختراق المتوافقة مع الإصدار 1.0 من OpenIOC.
- إذا قمت أثناء إنشاء مهمة IOC Scan 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 IOC Scan في سطر الأوامر أن جميع ملفات فحص الاختراق التي قمت بتحميلها غير مدعومة، فمن الممكن مواصلة تشغيل المهمة، لكنها لن تكتشف أي مؤشرات للاختراق. 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 IOC Scan.

يحتوي الملف الذي يمكنك تنزيله بالنقر فوق الارتباط أدناه على جدول يحتوي على قائمة كاملة بشروط IOC لمعيار OpenIOC.

تنزيل ملف IOC_TERMS.XLSX

يوضح الجدول التالي ميزات وقيود دعم التطبيق لمعيار OpenIOC.

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`
	
	بالنسبة لشروط Email/*، يتم دعم شرطي `contains` و`is` فقط. ولكي يعمل فحص مؤشر الاختراق (IOC) بأثر رجعي بشكل صحيح، عند استخدام شرط `is`، يجب تحديد عناوين البريد الإلكتروني في ملفات مؤشر الاختراق بالتنسيق التالي: `"name@example.org>" <SMTP:name@example.org;`. عند تشغيل مهمة فحص IOC بشكل عادي، يكفي تحديد عنوان البريد الإلكتروني بالتنسيق التالي: `name@example.org`.

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: `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 `Content` 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 البيانات `date` و`duration` في حالة تعيين المؤشرات بتنسيق `ISO 8601, Zulu time zone, UTC`.

الملحق رقم 11. واجهة برمجة التطبيقات للاستجابة لتهديدات EDR

يقدم Kaspersky Endpoint Security 12.9 for Windows دعمًا لإجراءات الاستجابة لتهديدات EDR (EDR responses) باستخدام Kaspersky Security Center OpenAPI. أي أنه يمكنك استدعاء طرق OpenAPI لأتمتة الاستجابة للتهديدات EDR باستخدام Python. ويمكنك استدعاء هذه الطرق عند دمجها مع حلول SIEM. تدعم Kaspersky Unified Monitoring and Analysis Platform، وهي حل نظام إدارة معلومات الأمان والأحداث (SIEM) من Kaspersky، واجهة OpenAPI لتهديدات EDR بدءًا من الإصدار 3.4.1. وللحصول على أمثلة للبرامج النصية، يرجى الرجوع إلى وثائق KUMA.

لتنفيذ إجراءات الاستجابة لتهديدات EDR، تحتاج إلى إنشاء طلب وإرساله باستخدام KSC Open API (AddIncident). وبعد معالجة الطلب، يتم إنشاء مهمة خاصة في وحدة تحكم Kaspersky Security Center.

لإنشاء مهام عند الاستجابة لتهديدات EDR، يجب عليك إنشاء اتصال في الخلفية بين خادم الإدارة وKaspersky Security Center Web Console. وتتوفر خدمة الاتصال في الخلفية في Kaspersky Security Center Windows 14.2 أو أحدث وفي Kaspersky Security Center Linux 15.2 أو أحدث. ولا يتم دعم وحدات التحكم الأخرى، بما في ذلك وحدات التحكم لحلول Kaspersky Detection and Response.

بالنسبة للاستجابة لتهديدات EDR، تحتاج إلى تحديد معلمات الطلب الأساسية، على سبيل المثال، بتنسيق JSON:

- `task` هو نوع المهمة (انظر أدناه).
- `targetHost` هو معرف الكمبيوتر الذي يجب تشغيل البرنامج النصي عليه. الوسيطة المطلوبة. يحصل البرنامج النصي على هذه الوسيطة من الحدث.
- `responseEventIncidentArea` هو اسم التطبيق الذي قام بتشغيل البرنامج النصي (على سبيل المثال، `KUMA`). ويتم إضافة هذه المعلمة إلى اسم المهمة التي تم إنشاؤها.

لتكوين الاستجابة لتهديدات EDR، تحتاج إلى تحديد إعدادات المهمة بتنسيق JSON في المعلمة `"KLINCDT_BODY": json.dumps(data)`. ونتيجة لذلك، ينشئ التطبيق `[Response][KUMA] <task type> - <Date> <Time> - <ID>` في وحدة تحكم Kaspersky Security Center.

الاتصال مع Kaspersky Security Center OpenAPI

كجزء من الاستجابة لتهديدات EDR، ينشئ التطبيق مهام خاصة في وحدة تحكم Kaspersky Security Center. ويتطلب إنشاء هذه المهام إنشاء اتصال بين الكمبيوتر وKaspersky Security Center. ولتحقيق ذلك، يجب تحديد معلمات اتصال Kaspersky Security Center في الطلب.

في الإصدار 2.1 من Kaspersky XDR، تغيرت طريقة منح الإذن للطلبات. ويستخدم Kaspersky XDR رموز PAT المميزة بدلاً من المصادقة على اسم المستخدم وكلمة المرور. لذلك، لا يمكن تشغيل البرامج النصية في Kaspersky XDR. وللمزيد من المعلومات عن مصادقة الطلب، يُرجى الرجوع إلى تعليمات Kaspersky XDR.

معلمات اتصال Kaspersky Security Center

المعلمة	النوع	الوصف
`kscHost`	`string`	عنوان خادم إدارة Kaspersky Security Center. المعلمة المطلوبة.
`kscPort`	`int`	منفذ اتصال خادم الإدارة. المعلمة المطلوبة.
`kscCert`	`string`	مسار إلى ملف شهادة للاتصال بخادم إدارة Kaspersky Security Center. بشكل افتراضي، يتم تعيين المعلمة إلى `False`.
`kscUser`	`string`	اسم حساب المستخدم. المعلمة المطلوبة.
`kscPassword`	`string`	كلمة مرور حساب المستخدم. المعلمة المطلوبة.

مثال

```
KSC connection info #
reads Environment variables by default, change with corresponding values #
KSC host, string, required #
"kscHost = "kscHost
"KSC port, required, default is "13299 #
"kscPort = "13299
KSC certificate file path, default is False #
kscCert = False
KSC user, string, required #
"kscUser = "kscUser
```

```
KSC password, string, required #
"kscPassword = "kscPassword

server_url = 'https://' + kscHost + ':' + str(kscPort)
)server = KlAkAdmServer.Create
(server_url, kscUser, kscPassword, verify=kscCert

params = validate(args)

,<data = {"targetHost": <MyHost
,task": task"
,params": params"
,responseEventIncident": True"
{"responseEventIncidentArea":"Kuma"

oHostGroup = KlAkHostGroup(server)

,incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2
,KLINCDT_ADDED": paramDateTime(datetime.datetime.now())"
,KLINCDT_BODY": json.dumps(data)"
()KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal"

,oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False
({KLHST_WKS_HOSTNAME":  args.targetHost"
```

لا يتم حماية بيانات حساب المستخدم، لذلك تحتاج إلى تخصيص مستخدم منفصل سيتم استخدامه لتنفيذ هذه الإجراءات فقط.

الحصول على الملف – getFile

إعدادات مهمة الحصول على الملف

المعلمة	النوع	الوصف
md5hash	`string`	تجزئة MD5 للملف الذي تريد الحصول عليه.
sha256hash	`string`	تجزئة SHA256 للملف الذي تريد الحصول عليه.
path	`string`	مسار الملف الذي تريد الحصول عليه.

مثال

```
} = type getFile
;'task: 'getFile
;targetHost: string
} :params
an empty string or a valid md5 hash of the file //
;md5hash: string
an empty string or a valid sha256 hash of the file //
;sha256hash: string
the path to the file //
;path: string
;{
;responseEventIncidentArea: string
;{
```

حذف الملف – deleteFile

إعدادات مهمة حذف الملف

المعلمة	النوع	الوصف
md5hash	`string`	تجزئة MD5 للملف الذي تريد حذفه.
sha256hash	`string`	تجزئة SHA256 للملف الذي تريد حذفه.
path	`string`	مسار الملف الذي تريد حذفه.
searchInSubfolders?	`boolean`	ابحث عن الملف الذي تريد حذفه في المجلدات الفرعية.

مثال

```
} = type deleteFile
;'task: 'deleteFile
;targetHost: string
} :params
an empty string or a valid md5 hash of the file //
;md5hash: string
an empty string or a valid sha256 hash of the file //
;sha256hash: string
the path to the file //
;path: string
recursive search for a file (subfolder), optional //
;searchInSubfolders?: boolean
;{
;responseEventIncidentArea: string
;{
```

نقل الملف إلى العزل – quarantineFile

إعدادات مهمة نقل الملف إلى العزل

المعلمة	النوع	الوصف
md5hash	`string`	تجزئة MD5 للملف الذي تريد عزله.
sha256hash	`string`	تجزئة SHA256 للملف الذي تريد عزله.
path	`string`	مسار الملف الذي تريد عزله.

مثال

```
} = type quarantineFile
;'task: 'quarantineFile
;targetHost: string
} :params
an empty string or a valid md5 hash of the file //
;md5hash: string
an empty string or a valid sha256 hash of the file //
;sha256hash: string
the path to the file //
;path: string
;{
;responseEventIncidentArea: string
;{
```

فحص IOC – iocScan

إعدادات مهمة فحص IOC

المعلمة	النوع	الوصف
ioc	`string`	المسار إلى أرشيف ZIP الذي يحتوي على ملف مؤشرات الاختراق الذي تريد استخدامه للفحص.
isolateHost	`boolean`	اعزل الكمبيوتر عن الشبكة عند اكتشاف مؤشر اختراق لمنع انتشار التهديد.
scanCriticalAreas	`boolean`	قم بتشغيل مهمة فحص المناطق الحرجة عند اكتشاف مؤشر اختراق.
quarantineObject	`boolean`	احذف الكائن الضار عند اكتشاف مؤشر اختراق. قبل حذف الكائن، يُنشئ Kaspersky Endpoint Security نسخة احتياطية في حالة الحاجة إلى استعادة الكائن لاحقًا. ينقل Kaspersky Endpoint Security النسخة الاحتياطية إلى العزل.

مـثـال

```
} = type iocScan
;'task: 'iocScan
;targetHost: string
} :params
the path to the zip archive with ioc files in base64 encoding //
;ioc: string
isolation of the computer from the network //
;isolateHost: boolean
critical areas scan //
;scanCriticalAreas: boolean
quarantine the file //
;quarantineObject: boolean
;{
;responseEventIncidentArea: string
;{
```

بدء العملية – startProcess

إعدادات مهمة بدء العملية

المعلمة	النوع	الوصف
executablePath	`string`	المسار إلى الملف القابل للتنفيذ الذي يتم استخدامه لبدء العملية.
arguments?	`string`	وسيطات سطر الأوامر الإضافية لبدء العملية.
workingFolder?	`string`	المسار إلى مجلد العمل الخاص بالعملية.

مـثـال

```
} = type startProcess
;'task: 'startProcess
;targetHost: string
} :params
the path to the file //
;executablePath: string
command line arguments, optional //
;arguments?: string
a working folder, optional //
;workingFolder?: string
;{
;responseEventIncidentArea: string
;{
```

إنهاء العملية – terminateProcess

إعدادات مهمة إنهاء العملية

المعلمة	النوع	الوصف
`md5hash`	`string`	تجزئة MD5 للملف الذي تريد إنهاء عمليته.
`sha256hash`	`string`	تجزئة SHA256 للملف الذي تريد إنهاء عمليته.
`path`	`string`	مسار الملف الذي تريد حذفه.
`caseSensitive`	`boolean`	حساسية حالة الأحرف عند البحث عن الملف.

مـثـال

```
} = type terminateProcess
;'task: 'terminateProcess
;targetHost: string
} :params
an empty string or a valid md5 hash of the file //
;md5hash: string
an empty string or a valid sha256 hash of the file //
;sha256hash: string
the path to the file //
;path: string
case sensitive of the file name //
;caseSensitive: boolean
;{
;responseEventIncidentArea: string
;{
```

عزل شبكة الكمبيوتر – isolateHost

إعدادات عزل شبكة الكمبيوتر

المعلمة	النوع	الوصف
`action`	`string`	وضع التشغيل عزل الشبكة.

مـثـال

```
} = type isolateHost
;'task: 'isolateHost
;targetHost: string
} :params
turning off network isolation, 1 - turning on network isolation - 0 //
;action: number
;{
;responseEventIncidentArea: string
;{
```

منع التنفيذ – preventExecution

إعدادات منع التنفيذ

المعلمة	النوع	الوصف
hash	`string`	تجزئة MD5 للملف الذي تريد منع تشغيله.
path	`string`	مسار الملف الذي تريد منع تشغيله.
caseSensitive	`boolean`	حساسية حالة الأحرف عند البحث عن الملف.

مثال

```
} = type preventExecution
;'task: 'preventExecution
;targetHost: string
} :params
a valid md5 hash of the file //
;hash: string
the path to the file //
;path: string
case sensitive of the file name //
;caseSensitive: boolean
;{
;responseEventIncidentArea: string
;{
```

فحص البرامج الضارة – onDemandScan

إعدادات مهمة فحص البرامج الضارة

المعلمة	النوع	الوصف
path	`string`	قائمة بالملفات والمجلدات محددة بمسافات للفحص المخصص.
recursive	`boolean`	وضع الفحص التكراري.
type	`number`	نطاق الفحص.

```
,"ScanObjectType = Enum("ScanObjectType
]
,(SystemMemory", 14")
,(StartupObjectsAndRunningProcesses", 15")
,(DiskBootSectors", 16")
,(SystemBackupStorage", 17")
,(Email", 18")
,(Folder", 22")
,(AllRemovableDrives", 23")
,(AllNetworkDrives", 24")
([(AllFixedDrives", 25")
```

مثال

```
} = type onDemandScan
;'task: 'onDemandScan
;targetHost: string
please note, this is an array //
array of scan object //
}] :params
enabling the scan object //
;enabled: boolean
an empty string or the path to the folder to scan //
;path: string
recursive scan mode //
;recursive: boolean
ID scan object //
;type: number
;[{
```

```
;responseEventIncidentArea: string
;{
```

الملحق رقم 12. حسابات المستخدمين في قواعد مكونات التطبيق

لتكوين بعض مكونات التطبيق، يجب إضافة قواعد خاصة. على سبيل المثال، للتحكم في الويب، يجب إضافة قاعدة تحتوي على قائمة بعناوين الويب التي تريد أن يحظرها التطبيق. وفي قواعد مكون التطبيق، يمكنك أيضًا تكوين جدول للمكون أو تحديد المستخدمين الذين يجب على التطبيق تطبيق القاعدة عليهم.

يجب إضافة القواعد لتكوين مكونات التطبيق التالية:

- التحكم في التطبيقات.
- Web Control.
- التحكم في الجهاز.
- فحص السجل.
- مراقبة عيوب التكيف.
- مراقبة سلامة النظام.

بدءًا من Kaspersky Endpoint Security for Windows 12.5، يمكنك الآن تحديد المستخدمين ليس فقط من Active Directory، لكن أيضًا من قائمة المستخدمين في Kaspersky Security Center. ويمكنك أيضًا إدخال بيانات حساب المستخدم المحلي يدويًا. ويعني هذا أنه يمكنك إضافة مستخدمين بالطرق التالية:

- Active Directory (موصى به)
- قائمة المستخدمين في Kaspersky Security Center
- حساب المستخدم المحلي

لتوظيف جميع أساليب اختيار المستخدم بشكل صحيح، تحتاج إلى تحديث تطبيق Kaspersky Endpoint Security والمكون الإضافي للإدارة إلى الإصدار 12.5 أو أحدث.

توصي Kaspersky باستخدام حسابات المستخدمين المحليين فقط في حالات خاصة عندما لا يكون من الممكن استخدام حسابات مستخدمي المجال. وللحصول على تفاصيل عن مخاطر الأمان لاستخدام الحسابات المحلية، راجع قاعدة معارف Microsoft. وتتحمل المسؤولية الكاملة عن أمان الكمبيوتر إذا تم استخدام حسابات المستخدمين المحلية؛ ويتضمن ذلك على وجه الخصوص مسؤولية التحكم في الوصول إلى إعدادات Kaspersky Endpoint Security وتقييدها.

يستخدم التطبيق SID (معرف الأمان) للمستخدم لتحديد المستخدمين. وعند استخدام حسابات المستخدمين من Active Directory أو من قائمة مستخدمي Kaspersky Security Center، يحدد التطبيق معرف الأمان (SID) على خادم الإدارة. ويعني هذا أن التطبيق لا يضع عبئًا إضافيًا على الكمبيوتر لتحديد المستخدم. وإذا أضفت أكثر من 1000 حساب مستخدم محلي إلى قاعدة تطبيق، تتصل التطبيقات بوحدة تحكم المجال لتحديد المستخدم. ويعني هذا زيادة الحمل على الكمبيوتر. ولتحسين تأثير الأداء على الكمبيوتر، نوصي باستخدام حسابات المستخدمين من Active Directory أو قائمة مستخدمي Kaspersky Security Center.

يستخدم التطبيق أسماء NetBIOS لتحديد حسابات المستخدمين المضافة يدويًا بتنسيقي `<username>` و`<hostname>\<username>`. ويمكن أن يصل طول اسم NetBIOS إلى 16 بايت (15 حرفًا). وإذا كان اسم الكمبيوتر يزيد عن 15 حرفًا، فلن يتمكن التطبيق من التعرف على المستخدم. وبعد ذلك يُعطل التطبيق القاعدة ويُولد خطأ، على سبيل المثال، Web Control: rule triggering disabled for user accounts without matching security identifier (SID). ولكي تعمل القاعدة، يجب عليك تقصير اسم الكمبيوتر يدويًا. ويمكنك إضافة حسابات مستخدمين من Active Directory أو Kaspersky Security Center. وفي هذه الحالة، يقوم التطبيق تلقائيًا بتقصير اسم الكمبيوتر.

يدعم Kaspersky Endpoint Security أيضًا المستخدمين المضمنين والمجموعات (مثل مجموعة "الكل") في القواعد. ونظرًا لكيفية تحديد معرف الأمان (SID) للمستخدم، يسمح التطبيق باستخدام حسابات المستخدمين المضمنة فقط التي تمت إضافتها من Active Directory أو قائمة المستخدمين في Kaspersky Security Center. ولا تعمل القواعد التي يتم فيها إضافة حساب مستخدم مضمن محليًا.

المعلومات القانونية

توفير البيانات

يحتوي هذا القسم على معلومات عن البيانات التي قد يخزنها تطبيق Kaspersky Endpoint Security على الجهاز ويرسلها تلقائيًا إلى Kaspersky أثناء تشغيله.

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.

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)؛
- معرف الطلب الفريد لخدمات صاحب الحق؛
- 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، موردي أحداث Microsoft Windows Kernel Process / Process Power Processor Windows Kernel 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 IOC Scan (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
- المعرف الفريد للعملية التي أجرت استعلام 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 IOC Scan (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
- المعرف الفريد للعملية التي أجرت استعلام HTTP

Kaspersky Endpoint Detection and Response Expert (on-premises)

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:

- البيانات المطلوبة للتكامل مع مكون EDR Expert (on-premises):
  - عنوان ومنفذ الاتصال بخادم KATA Central Node
  - عنوان ومنفذ للاتصال بخادم القياس عن بُعد

- عنوان ومنفذ الاتصال بخادم الاستجابة
- معلومات عن الشهادات المستخدمة للتكامل مع KATA Central Node
- معلومات عن الشهادات المستخدمة للتكامل مع خادم إرسال القياس عن بُعد
- معلومات عن الشهادات المستخدمة للتكامل مع خادم الاستجابة
- الملفات المعزولة

البيانات من أحداث القياس عن بُعد المرسلة

- **بيانات القياس عن بعد**
  - البيانات الموجودة في الملفات:
    - المعرفات الفريدة للملف
    - نوع الملف
    - مسار الملف الكامل
    - حجم الملف
    - سمات الملف
    - معرف المنطقة
    - تاريخ ووقت إنشاء الملف
    - تاريخ ووقت آخر تعديل للملف
    - اسم الملف الأصلي
    - اسم التطبيق
    - إصدار التطبيق.
    - بائع التطبيق
    - وصف الملف
    - إصدار الملف.
    - تجزئات MD5 وSHA256 للكائن
    - نتيجة التحقق من توقيع الملف
    - اسم جهة إصدار الشهادة

- اسم صاحب الشهادة
- الرقم التسلسلي للشهادة

- بيانات عن فحص AMSI:
  - المعرف الفريد للعملية التي بدأت النشاط
  - نوع محتوى الكائن الذي تم تمريره إلى AMSI
  - محتوى الكائن الذي تم تمريره إلى AMSI
  - اسم الكائن
  - تجزئات MD5 وSHA256 للكائن
- بيانات عن حظر التطبيق:
  - المعرف الفريد للعملية التي بدأت حظر التطبيق
  - المعرّف الفريد للعملية الأصل
  - معرّف النظام الفريد للعملية
  - الأمر المستخدم لبدء عملية
  - معرف جلسة تسجيل الدخول
  - مستوى سلامة العملية
  - حالة العملية
  - المعرّف الفريد لملف العملية
  - سطر أوامر العملية
  - قائمة المعرفات الفريدة للملفات المُفسَّرة
- بيانات عن عمليات فتح الملفات المحظورة:
  - المعرف الفريد للعملية التي بدأت فتح الملف
  - المعرفات الفريدة للملف
- بيانات عن تحميل برنامج التشغيل:
  - المعرّف الفريد لبرنامج التشغيل الذي تم تحميله
- بيانات عن الأحداث:
  - المعرّف الفريد للحدث
  - تاريخ ووقت الحدث

- بيانات عن تعديل الملف:
  - المعرف الفريد للعملية التي بدأت تعديل الملف
  - المعرفات الفريدة للملف
  - نوع عملية التعديل
  - علامة تشير إلى أنه سيتم حذف الملف بعد إعادة تشغيل الكمبيوتر
  - المعرّف الفريد للملف المُعدّل
  - المعرّف الفريد للملف قبل التعديل
  - مجموعة علامات البت التي تحدد كيفية فتح الملف
  - بيانات عن العمليات في قائمة التحكم في الوصول
  - بيانات عن التغييرات التي تم إجراؤها على الملكية أو المجموعة الرئيسية للملف
- بيانات عن جلسة تسجيل الدخول:
  - معرف جلسة تسجيل الدخول
  - اسم المستخدم الذي سجل الدخول
  - نوع حساب المستخدم
  - نوع الجلسة
- بيانات عن اتصالات الشبكة:
  - المعرف الفريد للعملية التي بدأت الاتصال
  - عنوان IP المحلي المستخدم لبدء الاتصال
  - عنوان IP البعيد لنقطة نهاية الاتصال
  - اتجاه الاتصال
  - بروتوكول نقل البيانات
  - طريقة HTTP
  - المسار بدون اسم المضيف
  - اسم المضيف
  - حالة العملية الديناميكية في لحظة الاتصال
  - علامة تشير إلى أن الاتصال مفتوح على مستوى المقبس الأولي
  - إصدار TLS المستخدم في جلسة الاتصال
  - اسم خادم TLS

- تجزئات MD5 وSHA1 لشهادة خادم TLS
- قائمة الأسماء البديلة للموضوع (SAN) الخاصة بالشهادة
- اسم جهة إصدار شهادة TLS
- الرقم التسلسلي للشهادة
- خوارزمية التشفير المستخدمة
- تاريخا بدء وانتهاء الشهادة
- بصمة JA3 لعميل TLS
- بصمة JA3S للخادم

- البيانات الملتقطة أثناء الاستماع على منفذ شبكة:
  - المعرف الفريد للعملية التي بدأت الاتصال
- بيانات إدخال سطر الأوامر:
  - المعرف الفريد للعملية التي بدأت إدخال وحدة التحكم
  - نوع إدخال وحدة التحكم
  - النص الذي تم إدخاله بواسطة مستخدم أو عملية
- بيانات عن إنشاء العملية:
  - المعرّف الفريد للعملية
  - المعرّف الفريد للعملية الأصل
  - معرّف النظام الفريد للعملية
  - الأمر المستخدم لبدء عملية
  - معرف جلسة تسجيل الدخول
  - مستوى سلامة العملية
  - المعرّف الفريد لملف العملية
  - قائمة المعرفات الفريدة للملفات المُفسَّرة
  - نوع العملية
- بيانات عن الوحدة التي تم تحميلها بواسطة العملية:
  - المعرف الفريد للعملية التي بدأت التنزيل
  - المسار الكامل للملف الذي تم تحميله إلى العملية
  - المعرّف الفريد لملف الوحدة

- الاسم المؤهل الكامل لتجميع NET.، إذا كان الملف الذي تم تحميله عبارة عن وحدة NET.
- علامات تجميع NET. المحددة في بيانها

- بيانات عن إنهاء العملية:
  - المعرّف الفريد للعملية التي تم إنهاؤها
- بيانات عن تعديل التسجيل:
  - المعرف الفريد للعملية التي بدأت تعديل التسجيل
  - نوع عملية التسجيل
  - المسار الكامل إلى مفتاح التسجيل
  - اسم القيمة داخل مفتاح التسجيل
  - نوع البيانات المخزنة في قيمة مفتاح التسجيل
  - البيانات المحددة في قيمة مفتاح التسجيل
  - اسم المفتاح قبل إعادة التسمية
  - معلومات تتعلق بتغيير في ملكية المفتاح أو مجموعة المفاتيح الأساسية
  - قائمة بالتغييرات التي تم إجراؤها على قائمة التحكم في الوصول (ACL) الخاصة بالمفتاح
- بيانات عن التهديد المكتشف ومعالجته:
  - علامة تشير إلى أن اكتشاف التهديد يعمل في الخلفية
  - قرار التهديد
  - اسم الحكم
  - المعرف الفريد لسجل قاعدة البيانات
  - الوقت الذي تم فيه حفظ سجل التهديد في قاعدة البيانات
  - وضع معالجة التهديد
  - نوع الكائن المصاب
  - اسم الكائن المصاب
  - تجزئات MD5 وSHA256 للكائن
  - المعرف الفريد للكائن المصاب
  - المعرّف الفريد للعملية التي قامت بتنزيل الكائن المصاب من الإنترنت
  - عنوان URL الذي تم تنزيل الكائن المصاب منه
  - عنوان البريد الإلكتروني الخاص بالمرسل الذي أرسل الكائن المصاب

- بروتوكول الشبكة الذي تم من خلاله استلام الكائن المصاب
- العنوان المحلي الذي تم استلام الكائن المصاب منه
- العنوان الخارجي الذي تم استلام الكائن المصاب منه
- نوع محتوى الكائن
- محتوى الكائن

- بيانات عن الوصول إلى العمليات:
  - المعرف الفريد للعملية التي حاولت الوصول
  - المعرف الفريد للعملية المستهدفة التي تم الوصول إليها
  - مجموعة الحقوق المطلوبة من العملية الهدف
  - نوع العملية
  - مجموعة الاستدعاءات عند لحظة الوصول إلى إحدى العمليات
  - واصف عملية المصدر
  - واصف العملية الهدف
- بيانات عن DNS:
  - المعرف الفريد للعملية التي بدأت استعلام DNS
  - عنوان IP لخادم DNS
  - العلامات التي تدير سلوك استعلام DNS
  - حالة اكتمال الفحص
  - اسم المجال المؤهل بالكامل المحدد في استعلام DNS
  - نوع البيانات في استعلام DNS
  - استجابات خادم DNS
- بيانات عن حقن التعليمات البرمجية:
  - المعرّف الفريد للعملية التي حاولت حقن التعليمات البرمجية
  - طريقة الوصول المستخدمة
  - مجموعة الاستدعاءات في وقت اكتشاف التعليمات البرمجية المحقونة
  - المعرّف الفريد للعملية الهدف التي تم تحميل التعليمات البرمجية إليها
  - بيانات عن التغييرات في تسلسل الأوامر للعملية الهدف
  - عنوان العملية الهدف

- اسم مكتبة DLL التي تم تحميلها إلى العملية الهدف
- المسار الكامل لملف DDL
- بيانات عن العمليات مع القنوات المسماة:
  - المعرف الفريد للعملية التي أنشأت القناة أو اتصلت بها
  - الاسم الكامل للقناة المسماة
  - نوع العملية (إنشاء أو اتصال)
- بيانات عن استعلامات WMI:
  - المعرف الفريد للعملية التي بدأت عملية WMI
  - نوع عملية WMI
  - اسم الجهاز الهدف لاستعلام WMI
  - حساب المستخدم الذي بدأ استعلام WMI
  - نص استعلام WMI
  - مساحة الاسم التي يتم تنفيذ استعلام WMI فيها
  - اسم عامل تصفية WMI
  - اسم كائن المستهلك
  - نص يصف إجراء كائن المستهلك
- بيانات عن استعلامات LDAP:
  - المعرف الفريد للعملية التي أجرت استعلام LDAP
  - نطاق البحث لاستعلامات LDAP
  - عامل تصفية LDAP
  - المعلمة التي تحدد قسم Active Directory الذي تم توجيه الاستعلام إليه
  - سمات بحث LDAP
- بيانات عن أجهزة USB المتصلة:
  - نوع عملية جهاز USB
  - نوع جهاز USB
  - معرّف جهاز USB
  - اسم جهاز USB

- المسار إلى جهاز USB
- علامة تشير إلى أن جهاز USB هو محرك أقراص نظام
- بيانات عن إنشاء مهمة مجدولة وحذفها وتعديلها
- بيانات عن إنشاء وحذف وتعديل الخدمات
- بيانات عن تركيب / إلغاء تركيب نظام الملفات
- بيانات عن تشغيل مكون EDR Expert المحلي:
  - معلومات عن بدء / إيقاف العميل
  - معلومات عن تثبيت / إلغاء تثبيت العميل
  - المعرّف فريد لبدء العميل
  - معرّف النظام الخاص بعملية العميل
  - المعرّف الفريد لعملية العميل
  - سبب إنهاء العميل
  - رمز إنهاء عملية العميل

- 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 من طلبات مكون EDR Expert إلى العميل المدمج في Kaspersky Endpoint Security:

- إعدادات المهمة العامة:
  - 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

البيانات من الطلبات المرسلة بواسطة Kaspersky Endpoint Security إلى مكون EDR Expert

عند التكامل مع حل EDR Expert (on-premises)، يتم تخزين البيانات التالية محليًا على أجهزة الكمبيوتر.

- 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

- 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

- 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.

  - 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

- البيانات في نتائج فحص IOC:
  - عنوان IP من جدول ARP
  - العنوان الفعلي من جدول ARP
  - اسم سجل DNS
  - نوع سجل DNS
  - اسم المضيف
  - عنوان IP
  - معرف الحدث في السجل
  - اسم مصدر البيانات في السجل

- اسم السجل
- اسم المستخدم
- تاريخ ووقت إنشاء الحدث بتنسيق ISO
- تجزئات MD5 وSHA256 للملف
- الاسم الكامل للملف
- حجم الملف
- عنوان ومنفذ IP البعيد الذي تم إنشاء الاتصال به أثناء الفحص
- عنوان IP ومنفذ المحول المحلي
- البروتوكول
- 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
- المسار إلى مفتاح التسجيل
- اسم مفتاح التسجيل
- القيمة النصية لمفتاح التسجيل
- اسم الخدمة
- وصف الخدمة
- مسار واسم خدمة DLL
- مسار واسم ملف الخدمة القابل للتنفيذ
- معرف Windows (PID) للخدمة
- نوع الخدمة
- حالة الخدمة
- وضع بدء تشغيل الخدمة
- اسم نظام التشغيل

- إصدار نظام التشغيل
- اسم شبكة الكمبيوتر بدون مجال
- المجال أو مجموعة العمل
- اسم المستخدم
- اسم المجلد
- حرف وحدة التخزين
- نوع وحدة التخزين

Kaspersky Network Detection and Response (KATA)

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

بيانات القياس عن بعد

- **البيانات عن الملفات**
- المعرفات الفريدة للملف
- نوع الملف
- مسار الملف الكامل
- حجم الملف
- سمات الملف
- معرف المنطقة
- تاريخ ووقت إنشاء الملف
- تاريخ ووقت آخر تعديل للملف
- اسم الملف الأصلي
- اسم التطبيق
- إصدار التطبيق.
- بائع التطبيق
- وصف الملف

- إصدار الملف.
- تجزئات MD5 وSHA256 للكائن
- نتيجة التحقق من توقيع الملف
- تاريخ ووقت إنشاء توقيع الملف
- سلاسل الشهادات المستخدمة في ملف التوقيع
- نوع سلسلة الشهادة
- الشهادات في السلسلة
- اسم جهة إصدار الشهادة
- اسم صاحب الشهادة
- الرقم التسلسلي للشهادة
- خوارزمية بصمة الإبهام
- بصمة الشهادة
- فترة صلاحية الشهادة

- **بيانات عن جلسة تسجيل الدخول**
- معرف جلسة تسجيل الدخول
- اسم حساب المستخدم الذي سجل الدخول
- نوع حساب المستخدم
- نوع الجلسة
- عنوان IP للجهاز الذي تم إجراء محاولة تسجيل الدخول منه
- عنوان IP للجهاز المحلي الذي أجريت محاولة تسجيل الدخول إليه
- علامة تشير إلى أن الجلسة التي يمثلها هذا الحدث تمتلك امتيازات مرتفعة وامتيازات إدارية
- المعلمة التي تشير إلى ما إذا كانت الجلسات الأخرى مرتبطة بجلسة تسجيل الدخول هذه
- البروتوكول المستخدم للجلسة النهائية
- بروتوكول IPv4 المستخدم للجلسة الطرفية

- **بيانات عن اتصالات الشبكة**
  - بداية ونهاية الفترة الزمنية التي تم جمع البيانات خلالها
  - قائمة الاتصالات
  - عنوان IP المحلي للكمبيوتر
  - عنوان MAC المحلي للكمبيوتر
  - عنوان IP البعيد للكمبيوتر
  - عنوان MAC البعيد للكمبيوتر
  - عنوان IP البوابة
  - عدد حزم البيانات المرسلة
  - عدد حزم البيانات المستلمة
  - إجمالي عدد وحدات البايت المنقولة
  - بروتوكول نقل البيانات
  - حقل نوع الإيثرنت في إطار الإيثرنت
  - بادئة الحمولة لأول حزمة بيانات في الفاصل الزمني
  - عنوان IPv4 لواجهة الشبكة التي تم التقاط الاتصال من خلالها

- **بيانات عن اتصال الشبكة**
  - المعرف الفريد للعملية التي بدأت الاتصال
  - بروتوكول نقل البيانات
  - عنوان IP المحلي المستخدم لبدء الاتصال
  - عنوان IP البعيد لنقطة نهاية الاتصال
  - طريقة HTTP
  - المسار بدون اسم المضيف
  - اسم المضيف
  - حالة العملية الديناميكية في لحظة الاتصال
  - اتجاه الاتصال
  - حالة العملية الديناميكية
  - حقل نوع الإيثرنت في إطار الإيثرنت

- **البيانات الملتقطة أثناء الاستماع على منفذ شبكة**
  - المعرف الفريد للعملية التي بدأت الاتصال
  - بروتوكول نقل البيانات
  - العنوان المحلي
  - حالة العملية الديناميكية في لحظة الاتصال

- **نتيجة التحقق من الاتصال**
  - إعدادات شبكة المضيف
  - وصف واجهة الشبكة
  - اسم مجال DNS
  - عنوان MAC المحلي للكمبيوتر
  - رقم قياس اتصال IP
  - قائمة عناوين IP
  - عنوان IP
  - قناع الشبكة
  - عنوان IP البوابة
  - عنوان MAC البوابة
  - قائمة التصحيحات المُثبتة
  - رقم التصحيح
  - تاريخ تثبيت التصحيح
  - طراز الجهاز
  - بائع الجهاز
  - معرف المضيف في Kaspersky Security Center
  - وصف برنامج مكافحة الفيروسات من Kaspersky
  - اسم مكون برنامج مكافحة الفيروسات من Kaspersky المُثبت
  - إصدار مكون برنامج مكافحة الفيروسات من Kaspersky المُثبت
  - إصدار قاعدة البيانات لمكون مكافحة الفيروسات من Kaspersky المُثبت

- تاريخ آخر تحديث لقاعدة البيانات لمكون مكافحة الفيروسات من Kaspersky
- حالة مكون برنامج مكافحة الفيروسات من Kaspersky المُثبت
- قائمة مفاتيح الترخيص
- الرقم التسلسلي للمفتاح
- نوع المفتاح
- تاريخ انتهاء صلاحية المفتاح
- حالة المفتاح

- **بيانات عن عملية الإنشاء على المضيف**
  - المعرّف الفريد للعملية
  - المعرّف الفريد للعملية الأصل
  - معرّف النظام الفريد للعملية
  - الأمر المستخدم لبدء عملية
  - معرف جلسة تسجيل الدخول
  - معرف الجلسة الطرفية
  - المعرّف الفريد لملف العملية
  - مستوى سلامة العملية
  - قائمة الرموز المميزة لحقوق العملية
  - حقوق السمة
  - قائمة المعرفات الفريدة للملفات المُفسَّرة
  - حالة العملية
  - الأمر المستخدم لبدء عملية

- **بيانات عن إنهاء العملية**
  - المعرّف الفريد للعملية

- **بيانات عن التهديد المكتشف**
  - معلومات التهديد
  - قرار التهديد
  - رقم سجل AMR
  - إصدار قاعدة بيانات مكافحة الفيروسات
  - وضع اكتشاف التهديد
  - المعرّف الفريد للتهديد
  - تكنولوجيا الحماية
  - معلومات عن الكائن المصاب
  - نوع الكائن المصاب
  - اسم الكائن المصاب
  - تجزئات MD5 وSHA256 للكائن
  - المعرّف الفريد للعملية المصابة
  - المعرف الفريد للكائن المصاب
  - المعرّف الفريد للعملية التي قامت بتنزيل الكائن المصاب من الإنترنت
  - عنوان URL الذي تم تنزيل الكائن المصاب منه
  - عنوان البريد الإلكتروني الخاص بالمرسل الذي أرسل الكائن المصاب
  - بروتوكول الشبكة الذي تم من خلاله استلام الكائن المصاب
  - العنوان المحلي الذي تم استلام الكائن المصاب منه
  - العنوان الخارجي الذي تم استلام الكائن المصاب منه
  - نوع محتوى الكائن
  - سياق التهديد المكتشف
  - محتوى الكائن
  - علامة تشير إلى أن اكتشاف التهديد يعمل في الخلفية

- **بيانات عن معالجة التهديدات**
  - معلومات التهديد
  - قرار التهديد

- رقم سجل AMR
- إصدار قاعدة بيانات مكافحة الفيروسات
- وضع اكتشاف التهديد
- اسم الكائن المصاب
- تجزئات MD5 وSHA256 للكائن
- المعرّف الفريد للعملية المصابة
- المعرف الفريد للكائن المصاب
- بروتوكول الشبكة الذي تم من خلاله استلام الكائن المصاب
- العنوان المحلي الذي تم استلام الكائن المصاب منه
- العنوان الخارجي الذي تم استلام الكائن المصاب منه
- حالة معالجة التهديد
- سبب عدم إمكانية معالجة التهديد
- العنوان الفعلي المحلي

- **بيانات عن المستخدمين**
- معرف الأمان الخاص بالمستخدم
- معرف المستخدم
- اسم المستخدم
- الاسم الكامل للمستخدم
- وصف المستخدم
- ما إذا كان الحساب نشطًا أم محظورًا
- ما إذا كانت كلمة المرور قد انتهت صلاحيتها أم لا
- ما إذا كان تغيير كلمة المرور مطلوبًا أم لا
- ما إذا كان تغيير كلمة المرور مسموحًا به أم لا
- نوع حساب المستخدم
- ما إذا كان تسجيل الدخول التلقائي قد تم تمكينه لهذا الحساب أم لا
- قائمة المجموعات التي ينتمي إليها المستخدم

التكامل مع Kaspersky Unified Monitoring and Analysis Platform (KUMA)

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

عند الدمج مع Kaspersky Unified Monitoring and Analysis Platform (KUMA)، يتم نقل بيانات إعدادات الاتصال، بالإضافة إلى جميع الأحداث المسجلة في سجلات Windows.

سجلات أحداث Windows الرئيسية هي System وSecurity وApplication وForwardedEvents وHardwareEvents. ويمكن للمستخدمين أيضًا إنشاء سجلات مخصصة والعمل باستخدامها لتلبية متطلباتهم المحددة.

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.

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.

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 وMac وSafari علامات تجارية مملوكة لشركة Apple Inc.

Arm علامة تجارية مسجلة لشركة Arm Limited (أو الشركات التابعة لها) في الولايات المتحدة و/أو في أي أماكن أخرى.

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.

Cisco وCisco AnyConnect وIOS علامات تجارية مسجلة أو علامات تجارية لشركة Cisco Systems, Inc. و/أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

Citrix وCitrix Provisioning وCitrix Provisioning Services وCitrix Virtual Apps and Desktop وXenDesktop وXenServer هي إما علامات تجارية مسجلة أو علامات تجارية لشركة Cloud Software Group, Inc. و/أو الشركات التابعة لها في الولايات المتحدة و/أو بلدان أخرى.

Cloudflare وCloudflare Workers وشعار Cloudflare علامات تجارية و/أو علامات تجارية مسجلة لشركة Cloudflare، Inc. في الولايات المتحدة وولايات قضائية أخرى.

Core علامة تجارية لشركة Intel Corporation أو الشركات التابعة لها.

dBase هي علامة تجارية مملوكة لمؤسسة dataBased Intelligence, Inc.

Dell Technologies وDell وEMC والعلامات التجارية الأخرى علامات تجارية لشركة Dell Inc. أو الشركات التابعة لها.

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.

ESET علامة تجارية أو علامة تجارية مسجلة لشركة ESET spol. s r.o. أو كيان ESET المعني.

Foxit علامة تجارية مسجلة لشركة Foxit Corporation.

Radmin هي علامة تجارية مسجلة لشركة Famatech.

Google وAndroid وGoogle Public DNS وGoogle Chrome وChrome علامات تجارية لشركة Google, LLC.

HUAWEI وFusionCompute وFusionSphere هي علامات تجارية لشركة Huawei Technologies Co., Ltd.

ICQ علامة تجارية و/أو علامة خدمة لشركة ICQ LLC.

Intel علامة تجارية لشركة Intel Corporation أو الشركات التابعة لها.

IBM علامة تجارية مملوكة لشركة International Business Machines Corporation مسجلة في العديد من المناطق حول العالم.

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 مملوكة 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 وAccess وActive Directory وActiveSync وBing وBitLocker وExcel وHyper-V وInternet Explorer وInternet Explorer وJScript وLifeCam Cinema وMicrosoft Edge وMSDN وMS-DOS وMS-DOS وMultiPoint وOffice 365 وOffice 365 وOutlook وOutlook وPowerPoint وPowerShell وSkype وSQL Server وSurface وVisual Basic وVisual FoxPro وWindows وWindows وWindows Live وWindows PowerShell وWindows Server وWindows Store 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.

OpenSSL علامة تجارية لشركة OpenSSL Software Foundation.

OpenStack علامة تجارية مسجلة لشركة OpenStack في الولايات المتحدة وبلدان أخرى.

Oracle وJava وJavaScript علامات تجارية مسجلة لشركة Oracle و/أو الشركات التابعة لها.

Python علامة تجارية أو علامة تجارية مسجلة لشركة Python Software Foundation.

Realtek علامة تجارية لشركة Realtek Semiconductor Corporation.

SAMSUNG علامة تجارية لشركة SAMSUNG في الولايات المتحدة وبلدان أخرى.

Thawte علامة تجارية أو علامة تجارية مسجلة لشركة Symantec Corporation أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

Trend Micro علامة تجارية أو علامة تجارية مسجلة لشركة Trend Micro Incorporated.

VERISIGN علامة تجارية مسجلة في الولايات المتحدة وأماكن أخرى أو علامة تجارية غير مسجلة لشركة VeriSign, Inc. والشركات التابعة لها.

VMware وVMware ESXi وVMware Horizon وVMware Workstation وVMware Tools وVMware vSphere هي علامات تجارية مسجلة أو علامات تجارية مسجلة لشركة VMware, Inc. في الولايات المتحدة وبلدان أخرى.

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

توجد معلومات حول التعليمات البرمجية الخاصة بالأطراف الخارجية في ملف legal_notices.txt الموجود في مجلد تثبيت التطبيق.