kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 AO Kaspersky Lab

جدول المحتويات

تعليمات Kaspersky Security Center 15.1

ما الجديد

حول Kaspersky Security Center

البنية الهندسية

متطلبات الأجهزة والبرامج

متطلبات خادم الإدارة

متطلبات Web Console

متطلبات الخوادم المتنقلة

متطلبات وحدة تحكم الإدارة

متطلبات عميل الشبكة

تطبيقات وحلول Kaspersky المتوافقة

تراخيص وميزات برنامج Kaspersky Security Center 15.1

عن توافق مكونات Kaspersky Security Center

مقارنة Kaspersky Security Center: المستندة إلى Windows مقابل المستندة إلى Linux

حول Kaspersky Security Center Cloud Console

Kaspersky Security Center 15.1

المفاهيم الأساسية

خادم الإدارة

التسلسل الهرمي لخوادم الإدارة

خادم الإدارة الافتراضي

خادم الجهاز المحمول

خادم الويب

عميل الشبكة

مجموعات الإدارة

الجهاز المُدار

جهاز غير مخصص

محطة عمل المسؤول

مكون الإدارة الإضافي

مكون الإدارة الإضافي للويب

السياسات

ملفات تعريف السياسة

المهام

نطاق المهمة

كيفية ارتباط إعدادات التطبيق المحلية بالسياسات

نقطة توزيع

بوابة الاتصال

سيناريو التثبيت الرئيسي

المنافذ المستخدمة بواسطة Kaspersky Security Center

شهادات للعمل مع Kaspersky Security Center

حول شهادات Kaspersky Security Center

حول شهادة خادم الإدارة

متطلبات الشهادات المخصصة المستخدمة في Kaspersky Security Center

السيناريو: تحديد شهادة خادم الإدارة المخصصة

استبدال شهادة خادم الإدارة باستخدام الأداة المساعدة klsetsrvcert
توصيل عملاء الشبكة بخادم الإدارة باستخدام الأداة المساعدة klmover
إعادة إصدار شهادة خادم الويب
المخططات لحركة البيانات واستخدام المنفذ
خادم الإدارة والأجهزة المدارة في شبكة الاتصال المحلية (LAN)
خادم الإدارة الرئيسي في شبكة الاتصال المحلية (LAN) وخادما إدارة تابعان
خادم الإدارة في شبكة الاتصال المحلية (LAN)، الأجهزة المدارة على الإنترنت، الخادم الوكيل العكسي قيد الاستخدام
خادم الإدارة في شبكة الاتصال المحلية (LAN)، الأجهزة المدارة متصلة بالإنترنت، بوابة الاتصال قيد الاستخدام
خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، الأجهزة المدارة متصلة بالإنترنت
التفاعل مع مكونات Kaspersky Security Center وتطبيقات الأمان: مزيد من المعلومات
الاصطلاحات المستخدمة في مخططات التفاعل
خادم الإدارة ونظام إدارة قواعد البيانات
خادم الإدارة ووحدة تحكم الإدارة
خادم الإدارة والجهاز العميل: إدارة تطبيق الأمان
ترقية البرنامج على جهاز عميل خلال نقطة توزيع
التسلسل الهرمي لخوادم الإدارة: خادم الإدارة الرئيسي وخادم الإدارة الثانوي
التسلسل الهرمي لخوادم الإدارة مع خادم إدارة تابع في منطقة الأجهزة الموصلة مباشرة بالإنترنت
خادم الإدارة وبوابة اتصال في قطاع شبكة وجهاز عميل
خادم الإدارة وجهازان في منطقة الأجهزة الموصلة مباشرة بالإنترنت: بوابة الاتصال وجهاز عميل
خادم الإدارة و Kaspersky Security Center Web Console
تفعيل وإدارة تطبيق الأمان على جهاز محمول
أفضل ممارسات النشر
دليل التقوية
موقع خادم الإدارة
سلامة الاتصال
الحسابات والمصادقة
إدارة حماية خادم الإدارة
إدارة حماية الأجهزة العميلة
تكوين الحماية للتطبيقات المدارة
صيانة خادم الإدارة
نقل الحدث إلى أنظمة الطرف الثالث
توصيات الأمان لأنظمة معلومات الجهات الخارجية
توصيات لاستخدام تطبيقات الأمان من Kaspersky
التحضير للنشر
التخطيط لنشر Kaspersky Security Center
الأنظمة التقليدية لنشر نظام الحماية
حول تخطيط نشر Kaspersky Security Center على شبكة مؤسسة
تحديد بنية لحماية مؤسسة ما
التكوينات القياسية لـ Kaspersky Security Center
التكوين القياسي: مكتب واحد
التكوين القياسي: عدد قليل من المكاتب واسعة النطاق تُدار بواسطة مسؤوليها
التكوين القياسي: مكاتب صغيرة متعددة بعيدة
تحديد نظام إدارة قواعد البيانات (DBMS) لخادم الإدارة
تطبيق التصحيح التراكمي CU12 عند استخدام SQL Server 2019 كنظام لإدارة قاعدة البيانات
تكوين خادم MariaDB x64 للعمل مع Kaspersky Security Center 15.1
تكوين خادم MySQL x64 للعمل مع Kaspersky Security Center 15.1
تكوين خادم PostgreSQL أو Postgres Pro للعمل مع Kaspersky Security Center 15.1

إدارة الأجهزة المحمولة باستخدام Kaspersky Endpoint Security for Android
توفير الوصول عبر الإنترنت إلى خادم الإدارة
الوصول إلى الإنترنت: خادم الإدارة في شبكة محلية
الوصول إلى الإنترنت: خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت
الوصول إلى الإنترنت: عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت
حول نقاط التوزيع
زيادة حد واصفات الملفات لخدمة klnagent
حساب عدد نقاط التوزيع وتكوينهم
التسلسل الهرمي لخوادم الإدارة
خوادم الإدارة الافتراضية
معلومات حول قيود Kaspersky Security Center
تحميل الشبكة
النشر الأولي للحماية ضد الفيروسات
التحديث المبدئي لقواعد بيانات مكافحة الفيروسات
مزامنة عميل مع خادم الإدارة
التحديث الإضافي لقواعد بيانات مكافحة الفيروسات
معالجة الأحداث الخاصة بالعملاء بواسطة خادم الإدارة
حركة المرور كل 24 ساعة
التحضير لإدارة الجهاز المحمول
خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
التكوين القياسي: Kaspersky Device Management for iOS في منطقة الأجهزة الموصلة مباشرة بالإنترنت
التكوين القياسي: خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الشبكة المحلية لمؤسسة ما
إدارة الأجهزة المحمولة باستخدام Kaspersky Endpoint Security for Android
معلومات حول أداء خادم الإدارة
قيود على الاتصال بخادم إدارة
نتائج اختبار أداء خادم الإدارة
نتائج اختبار أداء خادم وكيل KSN
إعدادات الشبكة للتفاعل مع الخدمات الخارجية
نشر عميل الشبكة وتطبيق الأمان
النشر الأولي
تكوين أدوات التثبيت
حزم التثبيت
خصائص MSI وملفات التحويل
النشر باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد.
معلومات حول مهام التثبيت عن بُعد في Kaspersky Security Center
النشر عن طريق التقاط صورة جهاز ونسخها
النسخ غير الصحيح لصورة القرص الثابت
النشر باستخدام سياسات المجموعة الخاصة بـ Microsoft Windows
النشر الإجباري عبر مهمة تثبيت عن بُعد من Kaspersky Security Center
تشغيل الحزم المستقلة التي أنشأها Kaspersky Security Center
خيارات التثبيت اليدوي للتطبيقات
إنشاء ملف MST
تثبيت التطبيقات عن بُعد على الأجهزة المثبت عليها عميل الشبكة.
إدارة عمليات إعادة تشغيل الجهاز في مهمة التثبيت عن بُعد
ملاءمة تحديث قواعد البيانات في حزمة تثبيت ما خاصة بتطبيق أمان
استخدام الأدوات لتثبيت التطبيقات عن بُعد في Kaspersky Security Center لتشغيل الملفات التنفيذية ذات الصلة على الأجهزة المدارة
مراقبة النشر

تكوين أدوات التثبيت
معلومات عامة
التثبيت في الوضع الصامت (مع ملف الاستجابة)
تثبيت عميل الشبكة في الوضع الصامت (دون ملف استجابة)
تكوين التثبيت الجزئي عبر setup.exe
معلمات تثبيت خادم الإدارة
معلمات تثبيت عميل الشبكة
البنية التحتية الافتراضية
نصائح لتقليل الحمل على الأجهزة الظاهرية
دعم الأجهزة الظاهرية الديناميكية
دعم نسخ الأجهزة الظاهرية
دعم عودة نظام الملفات الخاص بالأجهزة المثبّت عليها عميل الشبكة إلى حالته السابقة
التثبيت المحلي للتطبيقات
التثبيت المحلي لعميل الشبكة
تثبيت عميل الشبكة في الوضع الصامت
تثبيت عميل الشبكة لنظام Linux في الوضع الصامت (مع ملف إجابات)
تجهيز جهاز يعمل بنظام التشغيل Astra Linux في وضع بيئة البرامج المغلقة لتثبيت عميل الشبكة
تثبيت عميل الشبكة لنظام التشغيل Linux في الوضع التفاعلي
التثبيت المحلي لمكون الإدارة الإضافي للتطبيق
تثبيت التطبيقات في الوضع الصامت
تثبيت التطبيقات باستخدام الحزم المستقلة
إعدادات حزمة تثبيت عميل الشبكة
عرض سياسة الخصوصية
نشر نظم إدارة الأجهزة المحمولة
نشر نظام للإدارة باستخدام بروتوكول iOS MDM
تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الوضع الصامت
سيناريوهات نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
نظام النشر المبسّط
نظام النشر الذي يتضمن تفويض Kerberos مقيّد (KCD)
تلقي شهادة أسماء نقاط الوصول (APNs)
تجديد شهادة أسماء نقاط الوصول (APNs)
تكوين شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM احتياطية
تثبيت شهادة APN على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
تكوين الوصول إلى خدمة Apple Push Notification
إصدار وتثبيت شهادة مشتركة على جهاز محمول
إضافة جهاز KES إلى قائمة الأجهزة المدارة
توصيل أجهزة KES بخادم الإدارة
الاتصال المباشر للأجهزة بخادم الإدارة
نظام توصيل أجهزة KES بالخادم الذي يتضمن تفويض Kerberos المقيّد (KCD)
استخدام مراسلة Firebase Cloud
التكامل مع البنية الأساسية للمفاتيح العامة
Kaspersky Security Center Web Server

تثبيت Kaspersky Security Center
الإعداد للتثبيت
حسابات للعمل باستخدام نظام إدارة قواعد البيانات (DBMS)
تكوين الحسابات للعمل مع SQL Server (مصادقة Windows)
تكوين الحسابات للعمل مع SQL Server (مصادقة SQL Server)
تكوين الحسابات للعمل مع MySQL و MariaDB
نقل البيانات من مساحة جدول مشتركة إلى مساحة جدول لكل ملف في MySQL و MariaDB DBMS
تكوين الحسابات للعمل مع PostgreSQL و Postgres Pro
السيناريو: مصادقة خادم Microsoft SQL
السيناريو: مصادقة MySQL Server
السيناريو: مصادقة خادم PostgreSQL
توصيات حول تثبيت خادم الإدارة
إنشاء حسابات لخدمات خادم الإدارة على مجموعة تجاوز الفشل
تحديد مجلد مشترك
التثبيت عن بُعد باستخدام أدوات خادم الإدارة عبر سياسات مجموعة Active Directory
التثبيت عن بُعد من خلال تسليم مسار UNC إلى حزمة مستقلة
التحديث من المجلد المشترك لخادم الإدارة
تثبيت صور أنظمة التشغيل
تحديد عنوان خادم الإدارة
التثبيت القياسي
الخطوة 1. مراجعة اتفاقية الترخيص وسياسة الخصوصية
الخطوة 2. تحديد طريقة التثبيت
الخطوة 3. تثبيت Kaspersky Security Center Web Console
الخطوة 4. اختيار حجم الشبكة
الخطوة 5. تحديد قاعدة البيانات
الخطوة 6. تكوين خادم SQL Server
الخطوة 7. تحديد وضع مصادقة
الخطوة 8. فك وتثبيت الملفات على القرص الثابت
التثبيت المخصص
الخطوة 1. مراجعة اتفاقية الترخيص وسياسة الخصوصية
الخطوة 2. تحديد طريقة التثبيت
الخطوة 3. تحديد المكونات المراد تثبيتها
الخطوة 4. تثبيت Kaspersky Security Center Web Console
الخطوة 5. اختيار حجم الشبكة
الخطوة 6. تحديد قاعدة البيانات
الخطوة 7. تكوين خادم SQL Server
الخطوة 8. تحديد وضع مصادقة
الخطوة 9. تحديد الحساب لتشغيل خادم الإدارة
الخطوة 10. تحديد الحساب لتشغيل خدمات Kaspersky Security Center
الخطوة 11. تحديد مجلد مشترك
الخطوة 12. تكوين الاتصال بخادم الإدارة
الخطوة 13. تعريف عنوان خادم الإدارة
الخطوة 14. عنوان خادم الإدارة للاتصال بالأجهزة المحمولة
الخطوة 15. تحديد مكونات الإدارة الإضافية للتطبيق
الخطوة 16. فك وتثبيت الملفات على القرص الثابت

نشر مجموعة تجاوز الفشل من Kaspersky Security Center
السيناريو: نشر مجموعة تجاوز الفشل من Kaspersky Security Center
حول مجموعة تجاوز الفشل من Kaspersky Security Center
تحضير خادم ملف لمجموعة تجاوز الفشل من Kaspersky Security Center
تحضير العقد لنظام مجموعة تجاوز الفشل من Kaspersky Security Center
تثبيت Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky Security Center
بدء تشغيل مهمة وإيقافها يدويًا
تثبيت خادم الإدارة على مجموعة تجاوز الفشل في Windows Server
الخطوة 1. مراجعة اتفاقية الترخيص وسياسة الخصوصية
الخطوة 2. تحديد نوع التثبيت على نظام المجموعة
الخطوة 3. تحديد اسم خادم الإدارة الافتراضي
الخطوة 4. تحديد تفاصيل الشبكة الخاصة بخادم الإدارة الافتراضي
الخطوة 5. تحديد مجموعة الكتلة
الخطوة 6. تحديد تخزين بيانات نظام المجموعة:
الخطوة 7. تحديد حساب للتثبيت عن بُعد
الخطوة 8. تحديد المكونات المراد تثبيتها
الخطوة 9. اختيار حجم الشبكة
الخطوة 10. تحديد قاعدة البيانات
الخطوة 11. تكوين خادم SQL Server
الخطوة 12. تحديد وضع مصادقة
الخطوة 13. تحديد الحساب لتشغيل خادم الإدارة
الخطوة 14. تحديد الحساب لتشغيل خدمات Kaspersky Security Center
الخطوة 15. تحديد مجلد مشترك
الخطوة 16. تكوين الاتصال بخادم الإدارة
الخطوة 17. تعريف عنوان خادم الإدارة
الخطوة 18. عنوان خادم الإدارة للاتصال بالأجهزة المحمولة
الخطوة 19. فك وتثبيت الملفات على القرص الثابت
تثبيت خادم الإدارة في الوضع الصامت
تثبيت وحدة تحكم الإدارة على محطة عمل المسؤول
التغييرات في النظام بعد تثبيت Kaspersky Security Center
إزالة التطبيق
حول ترقية Kaspersky Security Center
ترقية Kaspersky Security Center من إصدار سابق
ترقية Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky Security Center
ترقية Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Microsoft
الإعداد الأولي لـ Kaspersky Security Center
دليل التقوية
معالج البدء السريع لخادم الإدارة
حول معالج البدء السريع
بدء معالج البدء السريع لخادم الإدارة
الخطوة 1. تكوين خادم وكيل
الخطوة 2. تحديد طريقة تفعيل التطبيق
الخطوة 3. تحديد مناطق الحماية وأنظمة التشغيل
الخطوة 4. تحديد المكونات الإضافية للتطبيقات المُدارة
الخطوة 5. تنزيل حزم التوزيع وإنشاء حزم التثبيت
الخطوة 6. تكوين استخدام Kaspersky Security Network
الخطوة 7. تكوين إشعارات البريد الإلكتروني

الخطوة 8. تكوين إعدادات التحديث
الخطوة 9. إنشاء تكوين حماية أولية
الخطوة 10. توصيل الأجهزة المحمولة
الخطوة 11. تنزيل التحديثات
الخطوة 12. اكتشاف الأجهزة
الخطوة 13. إغلاق معالج البدء السريع
تكوين اتصال وحدة تحكم الإدارة بخادم الإدارة
تكوين إعدادات الوصول إلى الإنترنت لخادم الإدارة
توصيل الأجهزة خارج المكتب
السيناريو: توصيل الأجهزة الموجودة خارج المكتب عن طريق بوابة الاتصال
السيناريو: توصيل الأجهزة خارج المكتب من خلال خادم إدارة ثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)
حول توصيل الأجهزة خارج المكتب
توصيل الأجهزة المكتبية الخارجية بخادم الإدارة
حول ملفات التعريف الخاصة باتصال المستخدمين المتواجدين خارج المكتب
إنشاء ملف تعريف خاص باتصال المستخدمين المتواجدين خارج المكتب
حول تبديل عميل الشبكة إلى خوادم إدارة أخرى
إنشاء قاعدة تبديل عميل شبكة حسب موقع الشبكة
إخطارات الأحداث
تكوين إخطار الحدث
إخطارات الاختبار
إخطارات الحدث التي يتم عرضها بواسطة الملف التنفيذي
تشفير الاتصال باستخدام بروتوكول TLS
تكوين الواجهة
اكتشاف الأجهزة المتصلة بالشبكة
سيناريو: اكتشاف الأجهزة المتصلة بالشبكة
الأجهزة غير المخصصة
اكتشاف الأجهزة
استقصاء شبكة Windows
استقصاء Active Directory
استقصاء نطاق IP
استطلاع شبكة لا تتطلب تكوينًا
العمل مع مجالات Windows. عرض وتغيير إعدادات المجال
تكوين قواعد الاستبقاء للأجهزة غير المخصصة
العمل مع نطاقات IP
إنشاء نطاق IP
عرض إعدادات نطاق IP وتغييرها
العمل مع مجموعات Active Directory. عرض وتعديل إعدادات المجموعة
إنشاء قواعد لنقل الأجهزة إلى مجموعات الإدارة تلقائيًا
استخدام الوضع الديناميكي VDI على الأجهزة العميلة
تمكين وضع VDI الديناميكي في خصائص حزمة تثبيت عميل الشبكة
البحث عن الأجهزة التي تُعد جزءًا من VDI
نقل الأجهزة من VDI إلى مجموعة إدارة
مخزون المعدات
إضافة معلومات حول الأجهزة الجديدة
تكوين المعايير المستخدمة لتحديد أجهزة المؤسسة
تكوين الحقول المخصصة

الترخيص
تم تجاوز حد أحداث الترخيص
حول الترخيص
حول الترخيص
حول اتفاقية ترخيص المستخدم النهائي
حول شهادة الترخيص
حول مفتاح الترخيص
حول ملف المفتاح
حول الاشتراك
حول رمز التنشيط
إلغاء الموافقة على اتفاقية ترخيص المستخدم النهائي
بخصوص تزويد البيانات
خيارات ترخيص Kaspersky Security Center
ميزات الترخيص الخاصة بـ Kaspersky Security Center والتطبيقات المدارة
تطبيقات Kaspersky. النشر المركزي
استبدال تطبيقات الأمان من جهة خارجية
تثبيت التطبيقات باستخدام مهمة التثبيت عن بُعد
تثبيت تطبيق على الأجهزة المحددة
تثبيت تطبيق على الأجهزة العميلة في مجموعة الإدارة
تثبيت تطبيق من خلال سياسات مجموعة Active Directory
تثبيت التطبيقات عن بُعد على الأجهزة
تثبيت التطبيقات على خوادم الإدارة الثانوية
تثبيت التطبيقات باستخدام معالج التثبيت عن بُعد
العمل مع المكونات الإضافية للإدارة
عرض تقرير نشر الحماية
إزالة التطبيقات عن بُعد
الإزالة عن بُعد لتطبيق من الأجهزة العميلة الخاصة بمجموعة الإدارة
الإزالة عن بُعد للتطبيق من الأجهزة المحددة
العمل باستخدام حزم التثبيت
إنشاء حزمة توزيع
إنشاء حزم تثبيت مستقلة
انشاء حزمة توزيع مخصصة
عرض خصائص حزم التثبيت المخصصة وتحريرها
الحصول على حزمة تثبيت عميل الشبكة من مجموعة توزيع Kaspersky Security Center
توزيع حزم التثبيت على خوادم الإدارة الثانوية
توزيع حزم التثبيت بواسطة نقاط التوزيع
نقل نتائج تثبيت التطبيق إلى Kaspersky Security Center
تحديد عنوان خادم وكيل KSN لحزم التثبيت
تلقي إصدارات التطبيقات المُحدَّثة
تحضير جهاز يعمل بنظام Windows للتثبيت عن بُعد
تحضير جهاز Linux وتثبيت عميل الشبكة على جهاز Linux عن بُعد
تحضير جهاز يقوم بتشغيل SUSE Linux Enterprise Server 15 لتثبيت عميل الشبكة
إعداد جهاز macOS يعمل لتثبيت عميل الشبكة عن بُعد
تطبيقات Kaspersky: الترخيص والتنشيط
ترخيص التطبيقات المُدارة
عرض معلومات حول مفاتيح التراخيص قيد الاستخدام
إضافة مفتاح ترخيص إلى مستودع خادم الإدارة

إزالة مفتاح ترخيص خادم الإدارة
نشر مفتاح ترخيص على الأجهزة العميلة
التوزيع التلقائي لمفتاح الترخيص
إنشاء تقرير حول استخدام مفتاح الترخيص وعرضه
عرض معلومات حول مفاتيح ترخيص التطبيق
تصدير ملف مفتاح الترخيص
تكوين حماية الشبكة
السيناريو: تكوين حماية الشبكة
نشر وإعداد السياسة: نهج مرتكز على الجهاز
حول نُهج إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم
الإعداد اليدوي لسياسة Kaspersky Endpoint Security
تكوين السياسة في قسم الحماية من التهديدات المتقدمة
تكوين السياسة في قسم الحماية من التهديدات الأساسية
تكوين السياسة في قسم الإعدادات العامة
تكوين السياسة في القسم تكوين الحدث
الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security
الإعداد اليدوي للمهمة الجماعية لفحص جهاز باستخدام Kaspersky Endpoint Security
جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
الإعداد اليدوي للمهمة الجماعية لتثبيت التحديثات وإصلاح الثغرات الأمنية
تعيين الحد الأقصى لعدد الأحداث في مستودع الأحداث
تحديد فترة التخزين القصوى للمعلومات حول الثغرات الأمنية الثابتة
إدارة المهام
إنشاء مهمة
إنشاء مهمة خادم الإدارة
إنشاء مهمة لأجهزة محددة
إنشاء مهمة محلية
عرض مهمة جماعية موروثة في مساحة عمل لمجموعة متداخلة
تشغيل الأجهزة تلقائيًا قبل بدء المهمة
إيقاف تشغيل جهاز تلقائيًا بعد اكتمال مهمة
تحديد وقت تشغيل المهمة
تصدير مهمة
استيراد مهمة
تحويل المهام
بدء تشغيل مهمة وإيقافها يدويًا
إيقاف المهمة مؤقتًا واستئنافها يدويًا
مراقبة تنفيذ المهمة
عرض نتائج تشغيل المهمة المخزنة على خادم الإدارة
تكوين تصفية المعلومات بشأن نتائج تشغيل المهمة
تعديل مهمة. التراجع عن التغييرات
مقارنة المهام
الحسابات التي ستقوم ببدء المهام
تصدير سجل تنفيذ المهمة
معالج تغيير كلمة مرور المهام
الخطوة 1. تحديد أوراق الاعتماد
الخطوة 2. تحديد إجراء لاتخاذه
الخطوة 3. عرض النتائج
إنشاء تسلسل هرمي لمجموعات الإدارة التابعة لخادم إدارة افتراضي

السياسات وملفات تعريف السياسة
التسلسل الهرمي للسياسات، واستخدام ملفات تعريف السياسة
التسلسل الهرمي للسياسات
ملفات تعريف السياسة
توريث إعدادات السياسة
إدارة السياسات
إنشاء سياسة
عرض سياسة موروثة في مجموعة فرعية
تنشيط سياسة
تنشيط سياسة تلقائيًا بعد حدث انتشار الفيروسات
تطبيق سياسة الوجود خارج المكتب
تعديل سياسة. التراجع عن التغييرات
مقارنة السياسات
عرض مخطط حالة توزيع السياسة
حذف سياسة
نسخ سياسة
تصدير سياسة
استيراد سياسة
تحويل السياسات
إدارة ملفات تعريف السياسة
إنشاء ملف تعريف سياسة
تعديل ملف تعريف سياسة
إزالة ملف تعريف سياسة
إنشاء قاعدة تفعيل ملف تعريف سياسة
قواعد نقل الجهاز
نسخ قواعد نقل الجهاز
تصنيف البرنامج
المتطلبات الأساسية لتثبيت التطبيقات على أجهزة المؤسسة العميلة
عرض الإعدادات المحلية للتطبيق وتحريرها
تحديث Kaspersky Security Center والتطبيقات التطبيقات المدارة
السيناريو: تحديث منتظم لقواعد بيانات Kaspersky وتطبيقاتها
حول تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات
حول استخدام ملفات diff لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج
تمكين ميزة تنزيل ملفات diff
إنشاء مهمة لتنزيل التحديثات إلى مستودع خادم الإدارة
إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع
تكوين تنزيل التحديثات إلى مستودع مهمة خادم الإدارة
التحقق من التحديثات المُنزّلة
تكوين سياسات الاختبار والمهام الإضافية
عرض التحديثات المُنزّلة
التثبيت التلقائي لتحديثات Kaspersky Endpoint Security على الأجهزة
النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات
تمكين النموذج غير متصل بالإنترنت لتنزيل التحديثات وتعطيله
التحديث والتصحيح التلقائيان لمكونات Kaspersky Security Center
تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center.

التوزيع التلقائي للتحديثات
توزيع التحديثات تلقائيًا على الأجهزة العميلة
توزيع التحديثات تلقائيًا على خوادم الإدارة الثانوية
تعيين نقاط التوزيع تلقائيًا
تعيين نقطة توزيع لجهاز يدويًا
إزالة جهاز من قائمة نقاط التوزيع
تنزيل التحديثات عن طريق نقاط التوزيع
حذف تحديثات البرامج من المستودع
تثبيت تصحيح خاص بتطبيق Kaspersky في وضع المجموعة
إدارة تطبيقات الجهات الخارجية على أجهزة العميل
حول تطبيقات الجهات الخارجية
تثبيت تحديثات برامج الجهات الخارجية
السيناريو: تحديث برامج الجهات الخارجية
عرض معلومات حول التحديثات المتوفرة لتطبيقات الطرف الثالث
اعتماد ورفض تحديثات البرنامج
مزامنة التحديثات من Windows Update مع خادم الإدارة
الخطوة 1. تحديد ما إذا كان سيتم تقليل حركة المرور
الخطوة 2. التطبيقات
الخطوة 3. تحديث الفئات
الخطوة 4. تحديثات اللغات
الخطوة 5. تحديد الحساب لبدء المهمة
الخطوة 6. تكوين جدول بدء المهمة
الخطوة 7. تحديد اسم المهمة
الخطوة 8. إكمال إنشاء المهمة
تثبيت التحديثات على الأجهزة يدويًا
تكوين تحديثات Windows في سياسة عميل الشبكة
إصلاح الثغرات الأمنية ببرامج الجهات الخارجية
السيناريو: البحث عن الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها
حول البحث عن الثغرات الأمنية بالبرامج وإصلاحها
عرض معلومات حول الثغرات الأمنية بالبرنامج
عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة
فحص التطبيقات بحثًا عن ثغرات أمنية
إصلاح الثغرات الأمنية في التطبيقات
إصلاح الثغرات الأمنية في شبكة معزولة
السيناريو: إصلاح الثغرات الأمنية لبرامج الجهات الخارجية في شبكة معزولة
السيناريو: إصلاح الثغرات الأمنية لبرامج الجهات الخارجية في شبكة معزولة
تكوين خادم الإدارة مع الوصول إلى الإنترنت لإصلاح الثغرات الأمنية في شبكة معزولة
تكوين خوادم الإدارة المعزولة لإصلاح الثغرات الأمنية في شبكة معزولة
جارٍ إرسال التصحيحات وتثبيت التحديثات في شبكة معزولة
جارٍ تعطيل خيار إرسال التصحيحات وتثبيت التحديثات في شبكة معزولة
تجاهل الثغرات الأمنية في البرامج
تحديد إصلاحات المستخدم للثغرات الأمنية في برامج الجهات الخارجية
قواعد لتثبيت التحديثات
مجموعات التطبيقات
استخدام التحكم في التطبيقات لإدارة الملفات القابلة للتنفيذ
الحصول على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل وعرضها
إنشاء فئات التطبيق من أجل سياسات Kaspersky Endpoint Security for Windows

إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا
إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة
إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد
إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق
تكوين إدارة بدء تشغيل التطبيق على الأجهزة العميلة
عرض نتائج التحليل الإحصائي لقواعد بدء التشغيل المطبقة على الملفات التنفيذية
عرض سجل التطبيقات
تغيير وقت بدء تخزين البرامج
حول إدارة مفتاح الترخيص لتطبيقات الطرف الثالث
إنشاء مجموعات التطبيقات المرخصة
إدارة مفاتيح الترخيص لمجموعات التطبيقات المرخصة
مخزون الملفات التنفيذية
عرض معلومات حول الملفات التنفيذية
المراقبة وإعداد التقارير
السيناريو: المراقبة وإعداد التقارير
مراقبة إشارات المرور والأحداث المسجلة في وحدة تحكم الإدارة
التعامل مع التقارير والإحصائيات والإخطارات
التعامل مع التقارير
إنشاء قالب تقرير
عرض وتحرير خصائص قالب التقرير
تنسيق عامل التصفية الموسع في قوالب التقرير
تحويل عامل التصفية إلى التنسيق الممتد
تكوين عامل التصفية الموسع
إنشاء تقرير وعرضه
حفظ تقرير
إنشاء مهمة تسليم تقرير
الخطوة 1. تحديد نوع المهمة
الخطوة 2. تحديد نوع التقرير
الخطوة 3. إجراءات على التقرير
الخطوة 4. تحديد الحساب لبدء المهمة
الخطوة 5. تكوين جدول مهمة
الخطوة 6. تحديد اسم المهمة
الخطوة 7. إكمال إنشاء المهمة
إدارة الإحصائيات
تكوين إخطار الحدث
إنشاء شهادة لخادم STMP
مجموعات الأحداث المحددة
عرض تحديد حدث
تخصيص تحديد حدث
إنشاء تحديد حدث
تصدير تحديد حدث إلى ملف نصي
حذف أحداث من الاختيار
إضافة تطبيقات لاستثناءات بواسطة طلبات المستخدم
تحديدات الأجهزة
عرض تحديد جهاز
تكوين تحديد جهاز
تصدير إعدادات تحديد جهاز إلى ملف

إنشاء تحديد جهاز
إنشاء تحديد جهاز وفقًا لإعدادات مستوردة
إزالة أجهزة من مجموعات الإدارة في تحديد
مراقبة تثبيت التطبيقات وإلغاء تثبيتها
أحداث مكونات Kaspersky Security Center
بنية البيانات لوصف نوع الحدث
أحداث خادم الإدارة
الأحداث الحرجة لخادم الإدارة
أحداث الخلل الوظيفي الخاصة بخادم الإدارة
أحداث التحذير لخادم الإدارة
الأحداث المعلوماتية لخادم الإدارة
أحداث عميل الشبكة
أحداث الخلل الوظيفي لعميل الشبكة
أحداث تحذير عميل الشبكة
الأحداث المعلوماتية لعميل الشبكة
أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
أحداث التحذير لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
الأحداث المعلوماتية لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
حظر الأحداث المتكررة
حول حظر الأحداث المتكررة
إدارة حظر الأحداث المتكررة
إزالة حظر الأحداث المتكررة
تصدير قائمة بالأحداث المتكررة إلى ملف
التحكم في التغييرات في حالة الأجهزة الظاهرية
مراقبة حالة الحماية ضد الفيروسات باستخدام معلومات من سجل النظام
عرض وتكوين الإجراءات عندما تكون حالة الأجهزة غير نشطة
تعطيل أخبار Kaspersky
تعديل نقاط التوزيع وبوابات الاتصال
التكوين القياسي لنقاط التوزيع: مكتب واحد
التكوين القياسي لنقاط التوزيع: مكاتب صغيرة متعددة بعيدة
تعيين جهاز مُدار يعمل كنقطة توزيع
توصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصولة مباشرة بالإنترنت
اتصال جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال
إضافة بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت للعمل كنقطة توزيع
تعيين نقاط التوزيع تلقائيًا
حول التثبيت المحلي لعميل الشبكة على جهاز مُحدد للعمل كنقطة توزيع
حول استخدام نقطة توزيع كبوابة اتصال
إضافة نطاقات IP إلى قائمة النطاقات التي تم استقصاؤها بواسطة نقطة توزيع
استخدام نقطة توزيع كخادم إرسال
عمل روتيني آخر
إدارة خوادم الإدارة
إنشاء تسلسل هرمي من خوادم الإدارة: إضافة خادم إدارة تابع
الاتصال بخادم الإدارة والتبديل بين خوادم الإدارة
حقوق الوصول إلى خادم الإدارة وكائناته
شروط الاتصال بخادم إدارة عبر الإنترنت

اتصال مشفر بخادم إدارة
مصادقة خادم الإدارة عند اتصال جهاز
مصادقة خادم الإدارة أثناء توصيل وحدة تحكم الإدارة
تكوين قائمة السماح بعناوين IP للاتصال بخادم الإدارة
استخدام الأداة المساعدة klscflag لإغلاق المنفذ 13291
قطع الاتصال من خادم إدارة
إضافة خادم إدارة إلى شجرة وحدة التحكم
إزالة خادم إدارة من شجرة وحدة التحكم
إضافة خادم إدارة افتراضي إلى شجرة وحدة التحكم
تغيير حساب خدمة خادم الإدارة. الأداة المساعدة klsrvswch
تغيير بيانات اعتماد DBMS
تغيير المجلد المشترك لخادم الإدارة
إيجاد الحلول لمشكلات عقد خادم الإدارة
عرض وتعديل إعدادات خادم إدارة
ضبط الإعدادات العامة لخادم الإدارة
إعدادات واجهة وحدة تحكم الإدارة
معالجة الحدث وتخزينه على خادم الإدارة
عرض سجل الاتصالات بخادم الإدارة
التحكم في انتشار الفيروسات
تقييد حركة المرور
تكوين خادم الويب
التعامل مع المستخدمين الداخليين
النسخ الاحتياطي والاستعادة لإعدادات خادم الإدارة
استخدام لقطة نظام الملفات لتقليل مدة النسخ الاحتياطي
تعذر تشغيل جهاز يحتوي على خادم الإدارة
إعدادات خادم الإدارة أو قاعدة البيانات تالفة
النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة
مهمة النسخ الاحتياطي لبيانات خادم الإدارة
الأداة المساعدة لنسخ البيانات احتياطيًا واستعادتها (klbackup)
النسخ الاحتياطي للبيانات واستعادتها في الوضع التفاعلي
النسخ الاحتياطي للبيانات واستعادتها في الوضع الصامت
استخدام الأداة المساعدة klbackup لتبديل الأجهزة المدارة تحت إدارة خادم إدارة آخر
النسخ الاحتياطي واستعادة بيانات خادم الإدارة عند استخدام MySQL أو MariaDB
تحسين النسخ الاحتياطي واستعادة بيانات خادم الإدارة
نقل خادم إدارة إلى جهاز آخر
تجنب التعارض بين العديد من خوادم الإدارة
إدارة مجموعات الإدارة
إنشاء مجموعات إدارة
نقل مجموعات الإدارة
حذف مجموعات الإدارة
الإنشاء التلقائي لبنية مجموعات الإدارة
التثبيت التلقائي للتطبيقات على الأجهزة الموجودة في مجموعة إدارة
إدارة الأجهزة العميلة
توصيل الأجهزة العميلة بخادم الإدارة
اتصال جهاز عميل بخادم الإدارة يدويًا. الأداة المساعدة Klmover
نفق اتصال أحد الأجهزة العميلة بخادم الإدارة

الاتصال البعيد بسطح مكتب جهاز عميل
الاتصال بنظام التشغيل Windows الأجهزة العميلة
الاتصال بنظام macOS الأجهزة العميلة
الاتصال بالأجهزة من خلال مشاركة سطح المكتب لـ Windows
تكوين إعادة تشغيل الجهاز العميل
مراجعة الإجراءات على جهاز عميل
التحقق من اتصال جهاز عميل بخادم الإدارة
التحقق من اتصال جهاز عميل بخادم الإدارة تلقائيًا
التحقق يدويًا من اتصال جهاز عميل بخادم الإدارة الأداة المساعدة Klnagchk
حول التحقق من وقت الاتصال بين جهاز ما وخادم الإدارة
تحديد الأجهزة العميلة على خادم الإدارة
نقل أجهزة إلى مجموعة إدارة
تغيير خادم الإدارة للأجهزة العميلة
نقل الأجهزة المتصلة بخادم الإدارة عبر بوابات الاتصال إلى خادم إدارة آخر
مصفوفات المجموعات والخوادم
تشغيل الأجهزة العميلة وإيقاف تشغيلها وإعادة تشغيلها عن بُعد
حول استخدام الاتصال المستمر بين جهاز مُدار وخادم الإدارة
حول المزامنة المفروضة
حول جدول الاتصال
إرسال رسائل إلى مستخدمي الجهاز
إدارة Kaspersky Security for Virtualization
تكوين تبديل حالات الجهاز
وضع العلامات على الأجهزة وعرض العلامات المعينة
وضع علامات على الجهاز تلقائيًا
عرض العلامات المعينة إلى جهاز وتكوينها
التشخيصات عن بُعد للأجهزة العميلة. أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center
توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل
إنشاء ملف تفريغ لتطبيق
تمكين وتعطيل التتبع، تنزيل ملف التتبع
تنزيل إعدادات التطبيق
تنزيل سجلات الأحداث
تنزيل عناصر معلومات التشخيص المتعددة
بدء التشخيصات وتنزيل النتائج
تشغيل التطبيقات وإيقافها وإعادة تشغيلها
أجهزة الحماية UEFI
إعدادات جهاز مدار
إعدادات السياسة العامة
إعدادات سياسة عميل الشبكة
إدارة حسابات المستخدمين
العمل باستخدام حسابات المستخدمين
إضافة حساب خاص بمستخدم داخلي
تحرير حساب خاص بمستخدم داخلي
تغيير عدد محاولات إدخال كلمة المرور المسموح بها
تكوين التحقق من تميز اسم أحد المستخدمين الداخليين
إضافة مجموعة أمان
إضافة مستخدم إلى مجموعة

تكوين حقوق الوصول إلى ميزات التطبيق. التحكم في الوصول على أساس الدور
حقوق الوصول إلى ميزات التطبيق
أدوار المستخدم المحددة مسبقًا
إضافة دور للمستخدم
تعيين دور لمستخدم أو لمجموعة أمان
تعيين أذونات للمستخدمين والمجموعات
نشر أدوار المستخدم على خوادم الإدارة الثانوية
تعيين المستخدم كمالك للجهاز
تسليم الرسائل للمستخدمين
عرض قائمة الأجهزة المحمولة للمستخدم
تثبيت شهادة لمستخدم
عرض قائمة الشهادات التي تم إصدارها لمستخدم
حول مسؤول خادم الإدارة الافتراضي
التثبيت عن بُعد لنظم التشغيل والتطبيقات
إنشاء صور لأنظمة التشغيل
تثبيت صور أنظمة التشغيل
تكوين عنوان الخادم الوكيل لشبكة KSN
إضافة برامج تشغيل بيئة التثبيت المسبق من Windows (WinPE)
إضافة برامج تشغيل إلى حزمة تثبيت مع صورة نظام تشغيل
تكوين الأداة المساعدة sysprep.exe
نشر أنظمة التشغيل على الأجهزة الجديدة المتصلة بالشبكة
نشر أنظمة التشغيل على الأجهزة العميلة
إنشاء حزم تثبيت التطبيقات
إصدار شهادة لحزم تثبيت التطبيقات
تثبيت التطبيقات على الأجهزة العميلة
إدارة مراجعات الكائن
حول مراجعات الكائن
عرض قسم محفوظات المراجعة
مقارنة مراجعات الكائن
إعداد فترة التخزين لمراجعات الكائن وللمعلومات حول الكائن المحذوف
عرض مراجعة كائن
حفظ مراجعة كائن في ملف
التراجع عن التغييرات
إضافة وصف للمراجعة
حذف الكائنات
حذف كائن
عرض معلومات حول الكائنات المحذوفة
حذف الكائنات بصورة دائمة من قائمة الكائنات المحذوفة
إدارة الأجهزة المحمولة
السيناريو: نشر إدارة الجهاز المحمول
حول سياسة المجموعة لإدارة أجهزة iOS MDM
تمكين إدارة الجهاز المحمول
تعديل إعدادات إدارة جهاز المحمول
تعطيل إدارة جهاز المحمول
العمل مع الأوامر للأجهزة المحمولة
الأوامر لإدارة الجهاز المحمول
استخدام مراسلة Firebase Cloud

إرسال أوامر
عرض حالات الأوامر في سجل الأمر
جارٍ العمل بشهادات الأجهزة المحمولة
بدء معالج تثبيت الشهادة
الخطوة 1. تحديد نوع الشهادة
الخطوة 2. تحديد نوع الجهاز المحمول
الخطوة 3. تحديد مستخدم
الخطوة 4. تحديد مصدر الشهادة
الخطوة 5. تخصيص علامة للشهادة
الخطوة 6. تحديد إعدادات نشر الشهادة
الخطوة 7. تحديد طريقة إخطار المستخدم
الخطوة 8. إنشاء الشهادة
تكوين قواعد إصدار الشهادة
التكامل مع البنية الأساسية للمفاتيح العامة
تمكين دعم تفويض Kerberos المقيد
إضافة أجهزة محمولة iOS إلى قائمة الأجهزة المُدارة
إضافة أجهزة محمولة تعمل بنظام Android إلى قائمة الأجهزة المُدارة
إدارة أجهزة iOS MDM
توقيع ملف تعريف iOS MDM بشهادة
إضافة ملف تعريف التكوين
تثبيت ملف تعريف تكوين إلى جهاز
إزالة ملف تعريف التكوين من جهاز
إضافة جهاز جديد بواسطة نشر رابط على ملف تعريف
إضافة جهاز جديد من خلال تثبيت ملف التعريف بواسطة المسؤول
إضافة ملف تعريف التزويد
تثبيت ملف تعريف التزويد إلى جهاز
إزالة ملف تعريف التزويد إلى جهاز
إضافة تطبيق مدار
تثبيت تطبيق على جهاز محمول:
إزالة تطبيق من جهاز
تكوين التجوال على جهاز محمول iOS MDM
عرض معلومات حول جهاز iOS MDM
قطع اتصال جهاز iOS MDM من الإدارة
إرسال الأوامر إلى جهاز
التحقق من حالة تنفيذ الأوامر التي تم إرسالها
إدارة أجهزة KES
إنشاء حزمة تطبيقات محمولة لأجهزة KES
تمكين المصادقة القائمة على الشهادة لأجهزة KES
عرض معلومات حول جهاز KES
قطع اتصال جهاز KES بالإدارة
تشفير البيانات وحمايتها
عرض قائمة بالأجهزة المشفرة
عرض قائمة بأحداث التشفير
تصدير قائمة بأحداث التشفير إلى ملف نص
إنشاء تقارير التشفير وعرضها
نقل مفاتيح التشفير بين خوادم الإدارة

مستودعات البيانات
تصدير قائمة كائنات المستودع إلى ملف نص
حزم التثبيت
الحالات الرئيسية للملفات الموجودة في المستودع
تفعيل القواعد في وضع التدريب الذكي
عرض قائمة بعمليات الكشف التي تم إجراؤها باستخدام قواعد مراقبة عيوب التكيف
إضافة استثناءات من قواعد مراقبة عيوب التكيف
الخطوة 1. تحديد التطبيق
الخطوة 2. تحديد السياسة (السياسات)
الخطوة 3. معالجة السياسة (السياسات)
العزل والنسخ الاحتياطي
تمكين إدارة الملفات الموجودة في المستودعات عن بُعد
عرض خصائص ملف موجود في المستودع
حذف الملفات من المستودعات
استعادة الملفات من المستودعات
حفظ ملف من المستودعات إلى القرص
فحص الملفات في العزل
تهديدات نشطة
تنظيف ملف غير معالج
حفظ ملف لم تتم معالجته إلى القرص
حذف ملفات من المجلد "التهديدات المفعلة"
(KSN) Kaspersky Security Network
حول KSN
إعداد الوصول إلى Kaspersky Security Network
تمكين وتعطيل KSN
عرض بيان KSN المقبول
عرض إحصائيات خادم وكيل KSN
قبول بيان KSN محدث
حماية مُحسنة باستخدام Kaspersky Security Network
التحقق مما إذا كانت نقطة التوزيع تعمل كخادم وكيل لشبكة KSN
التبديل بين التعليمات عبر الإنترنت والتعليمات دون الاتصال به
تصدير الأحداث إلى أنظمة SIEM
تكوين تصدير الحدث إلى أنظمة SIEM
قبل البدء
حول الأحداث في Kaspersky Security Center
حول تصدير الحدث
حول تكوين تصدير الحدث في نظام SIEM
وضع علامة على الأحداث للتصدير إلى أنظمة SIEM بتنسيق Syslog
وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog
وضع علامة على الأحداث العامة للتصدير بتنسيق Syslog
حول تصدير الأحداث باستخدام تنسيق Syslog
تصدير الأحداث باستخدام تنسيقات CEF و LEEF
تكوين Kaspersky Security Center لتصدير الأحداث إلى نظام SIEM

تصدير الأحداث مباشرة من قاعدة البيانات
تنفيذ استعلام SQL باستخدام أداة klsql2 المساعدة
مثال على استعلام SQL في الأداة المساعدة klsql2
عرض اسم قاعدة بيانات Kaspersky Security Center
عرض نتائج التصدير
استخدام SNMP في إرسال الإحصاءات إلى تطبيقات الأطراف الخارجية
تكوين خدمة SNMP للاستخدام مع Kaspersky Security Center
عميل SNMP ومعرفات الكائنات
الحصول على عداد سلاسل من معرف كائن
قيم معرفات الكائنات لـ SNMP
استكشاف الأخطاء وحلها
العمل في بيئة السحابة
حول العمل في بيئة السحابة
سيناريو: النشر لسيناريو بيئة السحابة
المتطلبات الأساسية لنشر Kaspersky Security Center في بيئة السحابة
متطلبات الأجهزة لخادم الإدارة في بيئة السحابة
خيارات الترخيص في بيئة السحابة
خيارات قاعدة البيانات للعمل في بيئة السحابة
العمل في بيئة سحابة Amazon Web Services
حول العمل في بيئة سحابة Amazon Web Services
إنشاء أدوار IAM وحسابات مستخدمي IAM لمثيلات Amazon EC2
التأكد من أن خادم إدارة Kaspersky Security Center لديه الأذونات للعمل مع خدمات AWS
إنشاء دور IAM لخادم الإدارة
إنشاء حساب مستخدم IAM للعمل مع Kaspersky Security Center
إنشاء دور IAM لتثبيت التطبيقات على مثيلات Amazon EC2
استخدام Amazon RDS
إنشاء مثيل Amazon RDS
إنشاء مجموعة خيارات لمثيل Amazon RDS
تعديل مجموعة الخيارات
تعديل الأذونات لدور IAM لمثيل قاعدة بيانات Amazon RDS
تحضير مستودع خدمة Amazon S3 لقاعدة البيانات
ترحيل قاعدة البيانات إلى Amazon RDS
العمل في بيئة السحابة لـ Microsoft Azure
حول العمل في Microsoft Azure
إنشاء اشتراك ومعرف تطبيق وكلمة مرور
تعيين دور لمعرف تطبيق Azure
نشر خادم الإدارة في Microsoft Azure وتحديد قاعدة البيانات
العمل مع Azure SQL
إنشاء حساب تخزين Azure
إنشاء قاعدة بيانات Azure SQL وخادم SQL Server
ترحيل قاعدة البيانات إلى Azure SQL
العمل في Google Cloud
إنشاء بريد إلكتروني للعميل ومعرف المشروع ومفتاح خاص
العمل مع Google Cloud SQL لمثيل MySQL
المتطلبات الأساسية للأجهزة العميلة في بيئة السحابة والتي تكون لازمة للعمل مع Kaspersky Security Center
إنشاء حزم التثبيت المطلوبة لتكوين بيئة السحابة

تكوين بيئة السحابة
حول معالج تكوين بيئة السحابة
الخطوة 1. تحديد طريقة تفعيل التطبيق
الخطوة 2. تحديد بيئة السحابة
الخطوة 3. التخويل في بيئة السحابة
الخطوة 4. تكوين المزامنة مع السحابة واختيار إجراءات إضافية
الخطوة 5. تكوين Kaspersky Security Network في بيئة السحابة
الخطوة 6. تكوين إشعارات البريد الإلكتروني في بيئة السحابة
الخطوة 7. إنشاء تكوين أولي لحماية البيئة السحابية
الخطوة 8. تحديد الإجراء عندما يتعين إعادة تشغيل نظام التشغيل أثناء التثبيت (لبيئة السحابة)
الخطوة 9. تلقي التحديثات بواسطة خادم الإدارة
التحقق من التكوين
مجموعة جهاز السحابة
استقصاء قطاع الشبكة
إضافة اتصالات لاستقصاء قطاع السحابة
حذف اتصالات خاصة باستقصاء قطاع السحابة
تكوين جدول الاستقصاء
تثبيت تطبيقات على الأجهزة في بيئة السحابة
عرض خصائص أجهزة السحابة
المزامنة مع السحابة
نشر Kaspersky Security Center في Yandex.Cloud
الملاحق
الميزات المتقدمة
التشغيل التلقائي لعمليات Kaspersky Security Center. الأداة المساعدة klakaut
الأدوات المخصصة
وضع استنساخ قرص عميل الشبكة
إعداد جهاز مرجعي مع تثبيت وكلاء الشبكة لإنشاء صورة لنظام التشغيل
تكوين استلام الرسائل من مراقبة سلامة الملف
صيانة خادم الإدارة
الوصول إلى خوادم DNS العامة
نافذة طريقة إخطار المستخدم
نافذة تحديد الجهاز
نافذة تحديد اسم الكائن الجديد
ميزات استخدام واجهة الإدارة
شجرة وحدة التحكم
كيفية تحديث البيانات في مساحة العمل
كيفية التنقل في شجرة وحدة التحكم
كيفية فتح نافذة خصائص الكائن في مساحة العمل
كيفية تحديد مجموعة من الكائنات في مساحة العمل
كيفية تغيير مجموعة من الأعمدة في مساحة العمل
معلومات مرجعية
أوامر قائمة السياق
قائمة بالأجهزة المُدارة. وصف الأعمدة
حالات الأجهزة والمهام والسياسات
رموز حالة الملف في وحدة تحكم الإدارة

البحث عن البيانات وتصديرها
العثور على أجهزة
إعدادات البحث عن الجهاز
استخدام الأقنعة في متغيرات السلسلة
استخدام تعبيرات عادية في حقل البحث
تصدير القوائم من مربعات الحوار
إعدادات المهام
إعدادات المهمة العامة
تنزيل التحديثات إلى إعدادات مهمة مستودع خادم الإدارة
إعدادات مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع
البحث عن الثغرات الأمنية والإعدادات المطلوبة لمهمة التحديثات
قم بتثبيت التحديثات المطلوبة وضبط إعدادات مهمة إصلاح الثغرات الأمنية
القائمة العمومية للشبكات الفرعية
إضافة شبكات فرعية إلى القائمة العمومية للشبكات الفرعية
عرض وتعديل خصائص الشبكة الفرعية في القائمة العمومية للشبكات الفرعية
استخدام عميل الشبكة لأنظمة التشغيل Windows و Linux و macOS: المقارنة
Kaspersky Security Center Web Console
نشر مخطط خادم إدارة Kaspersky Security Center و Kaspersky Security Center Web Console
المنافذ التي يستخدمها Kaspersky Security Center Web Console
واجهة Kaspersky Security Center Web Console
تثبيت أقسام القائمة الرئيسية وإلغاء تثبيتها
السيناريو: تثبيت وإعداد مبدئي لـ Kaspersky Security Center Web Console
التثبيت:
تثبيت Kaspersky Security Center (تثبيت قياسي)
تثبيت Kaspersky Security Center Web Console
تثبيت Kaspersky Security Center Web Console المتصل بخادم الإدارة المُثبت على عقد مجموعة تجاوز الفشل
ترقية Kaspersky Security Center Web Console
شهادات للعمل مع Kaspersky Security Center Web Console
إعادة إصدار شهادة Kaspersky Security Center Web Console
استبدال شهادة Kaspersky Security Center Web Console
يتم تحديد الشهادات لخوادم الإدارة الموثوقة فيKaspersky Security Center Web Console
تحويل شهادة PFX إلى تنسيق PEM
الترحيل من Kaspersky Security Center Windows
الترحيل إلى Kaspersky Security Center Cloud Console
الترحيل إلى Kaspersky Next XDR Expert
الترحيل إلى Kaspersky Security Center Linux
الترحيل إلى Kaspersky Security Center Linux باستخدام النسخ الاحتياطي للبيانات في خادم الإدارة
الترحيل إلى Kaspersky Security Center Linux باستخدام معالج الترحيل
تصدير كائنات المجموعة من Kaspersky Security Center Windows
استيراد ملف التصدير إلى Kaspersky Security Center Linux
تبديل الأجهزة المدارة لتكون تحت إدارة Kaspersky Security Center Linux
تسجيل الدخول إلى Kaspersky Security Center Web Console وتسجيل الخروج منها
إدارة الهوية والوصول في Kaspersky Security Center Web Console
حول إدارة الهوية والوصول
تمكين إدارة الهوية والوصول: سيناريو
تكوين إدارة الهوية والوصول في Kaspersky Security Center Web Console
تسجيل تطبيق Kaspersky Industrial CyberSecurity for Networks في Kaspersky Security Center Web Console

مدة صلاحية الرموز المميزة ومهلة التفويض لإدارة الهوية والوصول
تحميل وتوزيع شهادات IAM
تعطيل إدارة الهوية والوصول
تكوين مصادقة المجال باستخدام بروتوكولات NTLM و Kerberos
تكوين خادم الإدارة
تكوين اتصال Kaspersky Security Center Web Console بخادم الإدارة
تكوين تسجيل أحداث الاتصال بخادم الإدارة
تكوين إعدادات الوصول إلى الإنترنت لخادم الإدارة
تعيين الحد الأقصى لعدد الأحداث في مستودع الأحداث
إعدادات الاتصال لأجهزة حماية UEFI
إنشاء تسلسل هرمي من خوادم الإدارة: إضافة خادم إدارة تابع
عرض قائمة خوادم الإدارة الثانوية
حذف تسلسل هرمي لخوادم الإدارة
صيانة خادم الإدارة
تكوين الواجهة
إدارة خوادم الإدارة الافتراضية
إنشاء خادم إدارة افتراضي
تمكين وتعطيل خادم إدارة افتراضي
تعيين مسؤول عن خادم إدارة افتراضي
تغيير خادم الإدارة للأجهزة العميلة
حذف خادم إدارة افتراضي
تمكين حماية الحساب من تعديل غير مصرح به
النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة
إنشاء مهمة نسخ احتياطي للبيانات
نقل خادم إدارة إلى جهاز آخر
التحقق من سلامة الوحدات باستخدام أداتي klscmodchk و integrity_checker
الإعداد الأولي لتطبيق Kaspersky Security Center Web Console
معالج البدء السريع (Kaspersky Security Center Web Console)
الخطوة 1. تحديد إعدادات اتصال الإنترنت
الخطوة 2. جارٍ تنزيل التحديثات المطلوبة
الخطوة 3. تحديد الأصول التي سيتم حمايتها
الخطوة 4. تحديد التشفير في الحلول
الخطوة 5. تكوين تثبيت المكونات الإضافية للتطبيقات المُدارة
الخطوة 6. تثبيت المكونات الإضافية المحددة
الخطوة 7. تنزيل حزم التوزيع وإنشاء حزم التثبيت
الخطوة 8. تكوين Kaspersky Security Network
الخطوة 9. تحديد طريقة تفعيل التطبيق
الخطوة 10. تحديد إعدادات إدارة التحديث من جهة خارجية
الخطوة 11. إنشاء تكوين أساسي لحماية الشبكة
الخطوة 12. تكوين إشعارات البريد الإلكتروني
الخطوة 13. إجراء استطلاع على الشبكة
الخطوة 14. إغلاق معالج البدء السريع
توصيل الأجهزة خارج المكتب
السيناريو: توصيل الأجهزة الموجودة خارج المكتب عن طريق بوابة الاتصال
السيناريو: توصيل الأجهزة خارج المكتب من خلال خادم إدارة ثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)
حول توصيل الأجهزة خارج المكتب
توصيل الأجهزة المكتبية الخارجية بخادم الإدارة

حول ملفات التعريف الخاصة باتصال المستخدمين المتواجدين خارج المكتب
إنشاء ملف تعريف خاص باتصال المستخدمين المتواجدين خارج المكتب
حول تبديل عميل الشبكة إلى خوادم إدارة أخرى
إنشاء قاعدة تبديل عميل شبكة حسب موقع الشبكة
معالج نشر الحماية
الخطوة 1. بدء معالج نشر الحماية
الخطوة 2. تحديد حزمة التثبيت
الخطوة 3. تحديد طريقة لتوزيع ملف المفتاح أو رمز التفعيل
الخطوة 4. تحديد إصدار عميل الشبكة
الخطوة 5. تحديد الأجهزة
الخطوة 6. تحديد إعدادات مهمة التثبيت عن بُعد
الخطوة 7. إدارة إعادة التشغيل
الخطوة 8. إزالة التطبيقات غير المتوافقة قبل التثبيت
الخطوة 9. نقل الأجهزة إلى الأجهزة المُدارة
الخطوة 10. تحديد الحسابات للوصول إلى الأجهزة
الخطوة 11. بدء التثبيت
نشر تطبيقات Kaspersky من خلال Kaspersky Security Center Web Console
السيناريو: نشر تطبيقات Kaspersky من خلال Kaspersky Security Center Web Console
الحصول على المكونات الإضافية لتطبيقات Kaspersky
تنزيل حزم التثبيت وإنشائها لتطبيقات Kaspersky
تغيير حد حجم بيانات حزمة التثبيت المخصصة
تنزيل حزم التوزيع لتطبيقات Kaspersky
التحقق من نشر Kaspersky Endpoint Security بنجاح
إنشاء حزم تثبيت مستقلة
عرض قائمة حزم التثبيت المستقلة
إنشاء حزمة توزيع مخصصة
توزيع حزم التثبيت على خوادم الإدارة الثانوية
تثبيت التطبيقات باستخدام مهمة التثبيت عن بُعد
تثبيت تطبيق عن بُعد
تثبيت تطبيق من خلال سياسات مجموعة Active Directory
تثبيت التطبيقات على خوادم الإدارة الثانوية
تحديد إعدادات التثبيت عن بُعد على أجهزة Unix
تشغيل وإيقاف تطبيقات Kaspersky
إدارة الأجهزة المحمولة
استبدال تطبيقات الأمان من جهة خارجية
اكتشاف الأجهزة المتصلة بالشبكة
سيناريو: اكتشاف الأجهزة المتصلة بالشبكة
اكتشاف الأجهزة
استقصاء شبكة Windows
استقصاء نطاق IP
إضافة نطاق IP وتعديله
استطلاع شبكة لا تتطلب تكوينًا
استقصاء وحدة تحكم المجال
المصادقة والاتصال بوحدة تحكم المجال
تكوين وحدة تحكم مجال Samba
تكوين قواعد الاستبقاء للأجهزة غير المخصصة

مخزون المعدات
إضافة معلومات حول الأجهزة الجديدة
تكوين المعايير المستخدمة لتحديد أجهزة المؤسسة
تطبيقات Kaspersky: الترخيص والتنشيط
ترخيص التطبيقات المُدارة
إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
إضافة مفتاح ترخيص خادم الإدارة
نشر مفتاح ترخيص على الأجهزة العميلة
التوزيع التلقائي لمفتاح الترخيص
عرض معلومات حول مفاتيح التراخيص قيد الاستخدام
إزالة مفتاح ترخيص من المستودع
إلغاء الموافقة على اتفاقية ترخيص المستخدم النهائي
تجديد تراخيص تطبيقات Kaspersky
استخدام Kaspersky Marketplace لاختيار حلول أعمال Kaspersky
تكوين حماية الشبكة
السيناريو: تكوين حماية الشبكة
حول نُهج إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم
نشر وإعداد السياسة: نهج مرتكز على الجهاز
إعداد السياسة ونشرها: نهج مرتكز على المستخدم
إعدادات سياسة عميل الشبكة
مقارنة إعدادات نهج عميل الشبكة حسب أنظمة التشغيل
تمكين وتعطيل وضع الاستهلاك منخفض الموارد لعميل الشبكة
تكوين إعدادات الحماية للتطبيقات المدارة
الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security
إزالة تحديثات تطبيقات أو برامج عن بُعد
المهام
حول المهام
حول نطاق المهمة
إنشاء مهمة
بدء مهمة يدويًا
عرض قائمة المهام
إعدادات المهمة العامة
تصدير مهمة
استيراد مهمة
بدء معالج تغيير كلمة مرور المهام
الخطوة 1. تحديد أوراق الاعتماد
الخطوة 2. تحديد إجراء لاتخاذه
الخطوة 3. عرض النتائج
إنشاء مهمة تنفيذ البرامج النصية عن بعد
تثبيت التطبيقات عن بعد على الأجهزة باستخدام مهمة تنفيذ البرامج النصية عن بعد
تكوين الإخطارات والمراقبة لمهمة تنفيذ البرامج النصية عن بُعد
تحضير أرشيف لمهمة تنفيذ البرامج النصية عن بُعد
إنشاء حزمة تثبيت بناءً على ملف بيان
إدارة الأجهزة العميلة
إعدادات جهاز مدار
إنشاء مجموعات إدارة
إضافة أجهزة إلى مجموعة إدارة يدويًا

نقل أجهزة أو مجموعات إلى مجموعة إدارة يدويًا
إنشاء قواعد نقل الجهاز
نسخ قواعد نقل الجهاز
شروط قاعدة نقل الجهاز
حول مصفوفات المجموعات والخادم
خصائص مجموعة أو مصفوفة خادم
عرض وتكوين الإجراءات عندما تكون حالة الأجهزة غير نشطة
حول حالات الجهاز
تكوين تبديل حالات الجهاز
الاتصال البعيد بسطح مكتب جهاز عميل
الاتصال بالأجهزة من خلال مشاركة سطح المكتب لـ Windows
تحديدات الأجهزة
عرض قائمة الأجهزة من تحديد جهاز
إنشاء تحديد جهاز
تكوين تحديد جهاز
تصدير قائمة الأجهزة من تحديد جهاز
إزالة أجهزة من مجموعات الإدارة في تحديد
علامات الجهاز
إنشاء علامة لجهاز
إعادة تسمية علامة جهاز
حذف علامة جهاز
عرض الأجهزة التي تم تعيين علامة لها
عرض العلامات المعينة إلى جهاز
وضع علامة على جهاز يدويًا
إزالة علامة معينة من جهاز
عرض قواعد وضع العلامات على الأجهزة تلقائيًا
تحرير قاعدة لوضع علامات على الأجهزة تلقائيًا
إنشاء قاعدة لوضع علامات على الأجهزة تلقائيًا
قواعد التشغيل لوضع العلامات على الأجهزة تلقائيًا
حذف قاعدة لوضع علامات على الأجهزة تلقائيًا
إدارة علامات الجهاز باستخدام الأداة المساعدة klscflag
السياسات وملفات تعريف السياسة
حول السياسات وملفات تعريف السياسة
حول القفل والإعدادات المقفولة
التسلسل الهرمي للسياسات، واستخدام ملفات تعريف السياسة
التسلسل الهرمي للسياسات
ملفات تعريف السياسة في التسلسل الهرمي للسياسات
كيفية تنفيذ الإعدادات على جهاز مُدار
إدارة السياسات
عرض قائمة السياسات
إنشاء سياسة
تعديل سياسة
إعدادات السياسة العامة
تمكين خيار توريث سياسة وتعطيله
نسخ سياسة
نقل سياسة
تصدير سياسة

استيراد سياسة
عرض مخطط حالة توزيع السياسة
حذف سياسة
إدارة ملفات تعريف السياسة
عرض ملفات تعريف سياسة
تغيير أولوية ملف تعريف سياسة
إنشاء ملف تعريف سياسة
تعديل ملف تعريف سياسة
إزالة ملف تعريف سياسة
إنشاء قاعدة تفعيل ملف تعريف سياسة
إزالة ملف تعريف سياسة
تشفير البيانات وحمايتها
عرض قائمة ببرامج التشغيل المشفرة
عرض قائمة بأحداث التشفير
إنشاء تقارير التشفير وعرضها
منح حق الوصول إلى محرك أقراص مشفر في وضع عدم الاتصال
المستخدمين وأدوار المستخدمين
حول أدوار المستخدم
عرض حسابات المستخدمين والجلسات
تكوين حقوق الوصول إلى ميزات التطبيق. التحكم في الوصول على أساس الدور
حقوق الوصول إلى ميزات التطبيق
أدوار المستخدم المحددة مسبقًا
تعيين حقوق الوصول إلى كائنات محددة
تعيين حقوق الوصول للمستخدمين ومجموعات الأمان
إضافة حساب خاص بمستخدم داخلي
إنشاء مجموعة أمان
تحرير حساب خاص بمستخدم داخلي
تحرير مجموعة أمان
تعيين دور لمستخدم أو لمجموعة أمان
إضافة حسابات المستخدمين إلى مجموعة أمان داخلية
تعيين مستخدم كمالك للجهاز
تكوين التحقق بخطوتين لجميع المستخدمين
عن المصادقة الثنائية
تمكين التحقق بخطوتين لحسابك الخاص (Web Console)
تمكين التحقق بخطوتين لحسابك الخاص (القائم على MMC)
تمكين التحقق بخطوتين المطلوب لجميع المستخدمين (Web Console)
تمكين التحقق بخطوتين لجميع المستخدمين (القائم على MMC)
تعطيل التحقق بخطوتين لحساب مستخدم (Web Console)
تعطيل التحقق بخطوتين لحساب مستخدم (القائم على MMC)
تعطيل التحقق بخطوتين المطلوب لجميع المستخدمين (Web Console)
تمكين التحقق بخطوتين المطلوب لجميع المستخدمين (القائم على MMC)
استثناء الحسابات من التحقق بخطوتين (Web Console)
استثناء الحسابات من التحقق بخطوتين (القائم على MMC)
تحرير اسم مُصدِر رمز الأمان (Web Console)
تحرير اسم مُصدِر رمز الأمان (القائم على MMC)
تكوين التحقق بخطوتين لحسابك الخاص (Web Console)
تكوين التحقق بخطوتين لحسابك الخاص (القائم على MMC)

إنشاء مفتاح سري جديد
منع المستخدمين الجدد من إعداد التحقق ثنائي الخطوات لأنفسهم
تعيين مستخدم كمالك لجهاز Linux بعد تثبيت عميل الشبكة
حذف مستخدم أو مجموعة أمان
تغيير كلمة المرور لحساب مستخدم
إنشاء دور للمستخدم
تحرير دور المستخدم
تحرير نطاق دور المستخدم
حذف دور مستخدم
ربط ملفات تعريف السياسة بأدوار
نشر أدوار المستخدم على خوادم الإدارة الثانوية
تغيير كلمة مرور الحساب
إلغاء حقوق المسؤول المحلي
إدارة مراجعات الكائن
التراجع عن كائن إلى مراجعة سابقة
إضافة وصف للمراجعة
عرض وحفظ مراجعة سياسة
حذف الكائنات
(KSN) Kaspersky Security Network
حول KSN
تعيين الوصول إلى KSN
تمكين وتعطيل استخدام KSN
عرض بيان KSN المقبول
قبول بيان KSN محدث
التحقق مما إذا كانت نقطة التوزيع تعمل كخادم وكيل لشبكة KSN
سيناريو: ترقية Kaspersky Security Center وتطبيقات الأمان المُدارة
تحديث قواعد بيانات Kaspersky وتطبيقاته
السيناريو: تحديث منتظم لقواعد بيانات Kaspersky وتطبيقاتها
حول تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات
إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة
التحقق من التحديثات المُنزّلة
إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع
تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center.
التثبيت التلقائي لتحديثات Kaspersky Endpoint Security for Windows
اعتماد ورفض تحديثات البرنامج
تحديث خادم الإدارة
تمكين النموذج غير متصل بالإنترنت لتنزيل التحديثات وتعطيله
تحديث قواعد بيانات Kaspersky ووحدات البرامج على الأجهزة غير المتصلة بالإنترنت
النسخ الاحتياطي واستعادة المكونات الإضافية للويب
تعديل نقاط التوزيع وبوابات الاتصال
التكوين القياسي لنقاط التوزيع: مكتب واحد
التكوين القياسي لنقاط التوزيع: مكاتب صغيرة متعددة بعيدة
عن تعيين نقاط التوزيع
تعيين نقاط التوزيع تلقائيًا
تعيين نقاط التوزيع يدويًا
تعديل قائمة نقاط التوزيع لمجموعة إدارة

المزامنة المفروضة
تمكين خادم الإرسال
إدارة تطبيقات الجهات الخارجية على أجهزة العميل
تثبيت تحديثات برامج الجهات الخارجية
السيناريو: تحديث برامج الجهات الخارجية
تثبيت تحديثات برامج الجهات الخارجية
إنشاء مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
البحث عن الثغرات الأمنية والإعدادات المطلوبة لمهمة التحديثات
إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية
حدد قواعد لتثبيت التحديثات
إنشاء مهمة تثبيت تحديثات Windows Update
عرض معلومات حول تحديثات برامج الجهات الخارجية المتوفرة
تصدير قائمة تحديثات البرامج المتوفرة إلى ملف
الموافقة على تحديثات برامج الجهات الخارجية ورفضها
إنشاء مهمة إجراء مزامنة Windows Update.
تحديث تطبيقات الجهات الخارجية تلقائيًا
إصلاح الثغرات الأمنية ببرامج الجهات الخارجية
السيناريو: البحث عن الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها
حول البحث عن الثغرات الأمنية بالبرامج وإصلاحها
إصلاح الثغرات الأمنية ببرامج الجهات الخارجية
إنشاء مهمة إصلاح الثغرات الأمنية
إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية
حدد قواعد لتثبيت التحديثات
تحديد إصلاحات المستخدم للثغرات الأمنية في برامج الجهات الخارجية
عرض معلومات حول ثغرات البرامج المكتشفة على جميع الأجهزة المدارة
عرض معلومات حول ثغرات البرامج المكتشفة على الجهاز المُدار المحدد
عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة
تصدير قائمة بأحداث التشفير إلى ملف نص
تجاهل الثغرات الأمنية في البرامج
إدارة التطبيقات المشغلة على أجهزة العميل
استخدام التحكم في التطبيقات لإدارة الملفات القابلة للتنفيذ
أوضاع وفئات التحكم في التطبيق
الحصول على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل وعرضها
إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا
إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة
إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد
عرض قائمة فئات التطبيق
إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق
تكوين التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows
الحصول على قائمة بالتطبيقات المثبتة على أجهزة العميل وعرضها
إنشاء حزمة تثبيت لتطبيق جهة خارجية من قاعدة بيانات Kaspersky
عرض وتعديل إعدادات حزمة تثبيت لتطبيق جهة خارجية من قاعدة بيانات Kaspersky
إعدادات حزمة تثبيت تطبيق جهة خارجية من قاعدة بيانات Kaspersky
علامات التطبيقات
إنشاء علامة تطبيق
إعادة تسمية علامة تطبيق
تعيين علامات لتطبيق

إزالة علامات معينة من تطبيق
حذف علامة تطبيق
المراقبة وإعداد التقارير
السيناريو: المراقبة وإعداد التقارير
حول أنواع المراقبة وإعداد التقارير
لوحة القيادة والبرامج المصغرة
باستخدام لوحة القيادة
إضافة عناصر واجهة إلى جزء المعلومات
إخفاء عنصر واجهة من لوحة القيادة
تحريك عنصر واجهة مستخدم على لوحة القيادة
تغيير حجم عنصر الواجهة أو مظهره
تغيير إعدادات عنصر الواجهة
حول وضع لوحة القيادة فقط
جارٍ تكوين وضع لوحة المعلومات فقط
تقارير الإدارة والحماية
استخدام التقارير
إنشاء قالب تقرير
عرض وتحرير خصائص قالب التقرير
تصدير تقرير إلى ملف
إنشاء تقرير وعرضه
إنشاء مهمة تسليم تقرير
حذف قوالب التقارير
الفعاليات واختيارات الفعالية
عن أحداث Kaspersky Security Center
استخدام تحديدات الحدث
إنشاء تحديد حدث
إنشاء تحديد حدث
عرض قائمة تحديد الحدث
تصدير مجموعة حدث
استيراد مجموعة حدث
عرض تفاصيل حدث
تصدير الأحداث إلى ملف
عرض تاريخ كائن من حدث
حذف الأحداث
حذف تحديدات الحدث
تعيين مدة التخزين لحدث
أحداث مكونات Kaspersky Security Center
بنية البيانات لوصف نوع الحدث
أحداث خادم الإدارة
الأحداث الحرجة لخادم الإدارة
أحداث الخلل الوظيفي الخاصة بخادم الإدارة
أحداث التحذير لخادم الإدارة
الأحداث المعلوماتية لخادم الإدارة
أحداث عميل الشبكة
أحداث الخلل الوظيفي لعميل الشبكة
أحداث تحذير عميل الشبكة
الأحداث المعلوماتية لعميل الشبكة

أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
أحداث التحذير لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
الأحداث المعلوماتية لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
حظر الأحداث المتكررة
حول حظر الأحداث المتكررة
إدارة حظر الأحداث المتكررة
إزالة حظر الأحداث المتكررة
الإخطارات وحالات الجهاز
استخدام الإخطارات
عرض الإخطارات التي تظهر على الشاشة
حول حالات الجهاز
تكوين تبديل حالات الجهاز
تكوين تسليم الإخطار
إخطارات الحدث التي يتم عرضها بواسطة الملف التنفيذي
إعلامات Kaspersky
حول أخبار Kaspersky
تحديد إعدادات أخبار Kaspersky
تعطيل أخبار Kaspersky
عرض معلومات حول اكتشافات التهديدات
اكتشاف السحابة
تمكين Cloud Discovery باستخدام الأداة
إضافة أداة Cloud Discovery إلى لوحة المعلومات
عرض معلومات عن استخدام الخدمات السحابية
مستوى خطر خدمة سحابية
حظر الوصول إلى الخدمات السحابية غير المرغوب فيها
تسجيل نشاط Kaspersky Security Center Web Console
التكامل بين Kaspersky Security Center والحلول الأخرى
جارٍ إنشاء اتصال في الخلفية
تصدير الأحداث إلى أنظمة SIEM
تكوين تصدير الحدث إلى أنظمة SIEM
قبل البدء
حول الأحداث في Kaspersky Security Center
حول تصدير الحدث
حول تكوين تصدير الحدث في نظام SIEM
وضع علامة على الأحداث للتصدير إلى أنظمة SIEM بتنسيق Syslog
حول وضع علامة على الأحداث لتصديرها إلى نظام SIEM بتنسيق Syslog
وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog
وضع علامة على الأحداث العامة للتصدير بتنسيق Syslog
تصدير الأحداث باستخدام تنسيقات CEF و LEEF
تحويل الأحداث إلى تنسيق CEF أو LEEF
حول تصدير الأحداث باستخدام تنسيق Syslog
تكوين Kaspersky Security Center لتصدير الأحداث إلى نظام SIEM

تصدير الأحداث مباشرة من قاعدة البيانات
تنفيذ استعلام SQL باستخدام أداة klsql2 المساعدة
مثال على استعلام SQL في الأداة المساعدة klsql2
عرض اسم قاعدة بيانات Kaspersky Security Center
عرض نتائج التصدير
العمل باستخدام Kaspersky Security Center Web Console في بيئة السحابة
تكوين بيئة السحابة في Kaspersky Security Center Web Console
الخطوة 1. تحقق من حزم التثبيت والمكونات الإضافية
الخطوة 2. ترخيص التطبيق
الخطوة 3. تحديد بيئة السحابة والمصادقة
الخطوة 4. استقصاء القطاع، تكوين المزامنة مع السحابة واختيار إجراءات إضافية
الخطوة 5. اختيار تطبيق لإنشاء سياسة ومهام لـ
الخطوة 6. تكوين Kaspersky Security Network لأجل Kaspersky Security Center
الخطوة 7. إنشاء تكوين أولي للحماية
استقصاء مقطع الشبكة عبر Kaspersky Security Center Web Console
إضافة اتصالات لاستقصاء قطاع السحابة
حذف اتصال خاص باستقصاء قطاع السحابة
تكوين جدول الاستقصاء عبر Kaspersky Security Center Web Console
عرض نتائج استقصاء قطاع السحابة عبر Kaspersky Security Center Web Console
عرض خصائص الأجهزة السحابية عبر Kaspersky Security Center Web Console
التزامن مع السحابة: تكوين قاعدة النقل
التثبيت عن بُعد للتطبيقات لأجهزة Azure الافتراضية
إنشاء نسخة احتياطية من مهمة بيانات خادم الإدارة باستخدام سحابة DBMS
التشخيصات عن بُعد لأجهزة العميل
فتح نافذة التشخيص عن بُعد
تمكين التتبع للتطبيقات وتعطيله
تنزيل ملفات التتبع لتطبيق
حذف ملفات التتبع
تنزيل إعدادات التطبيق
تنزيل سجلات الأحداث
بدء التطبيق وإيقافه وإعادة تشغيله
تشغيل التشخيصات عن بُعد لعميل شبكة Kaspersky Security Center وتنزيل النتائج
تشغيل تطبيق على جهاز عميل
إنشاء ملف تفريغ لتطبيق
تشغيل التشخيصات عن بُعد على جهاز عميل يعمل بنظام التشغيل Linux
تنزيل وحذف الملفات من العزل والنسخ الاحتياطي
تنزيل الملفات من العزل والنسخ الاحتياطي
تغيير لغة واجهة Kaspersky Security Center Web Console
الدليل المرجعي لـ API
أفضل ممارسات موفري الخدمات
التخطيط لنشر Kaspersky Security Center
توفير الوصول عبر الإنترنت إلى خادم الإدارة
التكوين القياسي لـ Kaspersky Security Center
حول نقاط التوزيع
التسلسل الهرمي لخوادم الإدارة
خوادم الإدارة الافتراضية
إدارة الأجهزة المحمولة باستخدام Kaspersky Endpoint Security for Android

النشر والإعداد الأولي
توصيات حول تثبيت خادم الإدارة
إنشاء حسابات لخدمات خادم الإدارة على مجموعة تجاوز الفشل
تحديد نظام إدارة قواعد البيانات
تحديد عنوان خادم الإدارة
تكوين الحماية في شبكة المؤسسة العميلة
الإعداد اليدوي لسياسة Kaspersky Endpoint Security
تكوين السياسة في قسم الحماية من التهديدات المتقدمة
تكوين السياسة في قسم الحماية من التهديدات الأساسية
تكوين السياسة في قسم الإعدادات العامة
تكوين السياسة في القسم تكوين الحدث
الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security
الإعداد اليدوي للمهمة الجماعية لفحص جهاز باستخدام Kaspersky Endpoint Security
جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
الإعداد اليدوي للمهمة الجماعية لتثبيت التحديثات وإصلاح الثغرات الأمنية
بناء بنية مجموعات الإدارة وتعيين نقاط التوزيع
التكوين القياسي لعميل MSP: مكتب واحد
التكوين القياسي لعميل MSP: مكاتب صغيرة متعددة بعيدة
التسلسل الهرمي للسياسات، واستخدام ملفات تعريف السياسة
التسلسل الهرمي للسياسات
ملفات تعريف السياسة
المهام
قواعد نقل الجهاز
تصنيف البرنامج
معلومات عن التطبيقات متعددة المستأجرين
النسخ الاحتياطي والاستعادة لإعدادات خادم الإدارة
تعذر تشغيل جهاز يحتوي على خادم الإدارة
إعدادات خادم الإدارة أو قاعدة البيانات تالفة
نشر عميل الشبكة وتطبيق الأمان
النشر الأولي
تكوين أدوات التثبيت
حزم التثبيت
خصائص MSI وملفات التحويل
النشر باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد
معلومات عامة حول مهام التثبيت عن بُعد في Kaspersky Security Center
النشر باستخدام سياسات المجموعة الخاصة بـ Microsoft Windows
النشر الإجباري عبر مهمة تثبيت عن بُعد من Kaspersky Security Center
تشغيل الحزم المستقلة التي أنشأها Kaspersky Security Center
خيارات التثبيت اليدوي للتطبيقات
تثبيت التطبيقات عن بُعد على الأجهزة المثبت عليها عميل الشبكة
إدارة عمليات إعادة تشغيل الجهاز في مهمة التثبيت عن بُعد
ملاءمة تحديث قواعد البيانات في حزمة تثبيت ما خاصة بتطبيق مكافحة الفيروسات
استبدال تطبيقات الأمان من جهة خارجية غير المتوافقة
إزالة عميل الشبكة المحمي بكلمة مرور باستخدام موجه الأوامر
استخدام الأدوات لتثبيت التطبيقات عن بُعد في Kaspersky Security Center لتشغيل الملفات التنفيذية ذات الصلة على الأجهزة المدارة
مراقبة النشر

تكوين أدوات التثبيت
معلومات عامة
التثبيت في الوضع الصامت (مع ملف الاستجابة)
تثبيت عميل الشبكة في الوضع الصامت (دون ملف استجابة)
تكوين التثبيت الجزئي عبر setup.exe
معلمات تثبيت خادم الإدارة
إعدادات تثبيت عميل الشبكة
البنية التحتية الافتراضية
نصائح لتقليل الحمل على الأجهزة الظاهرية
دعم الأجهزة الظاهرية الديناميكية
دعم نسخ الأجهزة الظاهرية
دعم عودة نظام الملفات الخاص بالأجهزة المثبّت عليها عميل الشبكة إلى حالته السابقة
حول ملفات التعريف الخاصة باتصال المستخدمين المتواجدين خارج المكتب
نشر ميزة إدارة الجهاز المحمول
توصيل أجهزة KES بخادم الإدارة
الاتصال المباشر للأجهزة بخادم الإدارة
نظام توصيل أجهزة KES بالخادم الذي يتضمن تفويض Kerberos المقيّد (KCD)
استخدام مراسلة Firebase Cloud
التكامل مع البنية الأساسية للمفاتيح العامة
Kaspersky Security Center Web Server
عمل روتيني آخر
مراقبة إشارات المرور والأحداث المسجلة في وحدة تحكم الإدارة
الوصول عن بُعد للأجهزة المدارة
استخدام خيار "عدم قطع الاتصال بخادم الإدارة" لتوفير اتصال مستمر بين جهاز مُدار وخادم الإدارة
حول التحقق من وقت الاتصال بين جهاز ما وخادم الإدارة
حول المزامنة المفروضة
حول النفق
دليل القياس
حول هذا الدليل
معلومات حول قيود Kaspersky Security Center
حسابات خوادم الإدارة
حساب موارد الأجهزة لخادم الإدارة
متطلبات الأجهزة الخاصة بنظام إدارة قواعد البيانات وخادم الإدارة
حساب مساحة قاعدة البيانات
حساب مساحة القرص (مع أو بدون استخدام ميزة إدارة الثغرات الأمنية والتصحيحات)
حساب رقم وتكوين خوادم الإدارة
توصيات لتوصيل الأجهزة الافتراضية الديناميكية بـ Kaspersky Security Center
حسابات نقاط التوزيع وبوابات الاتصال
المتطلبات لنقطة توزيع
حساب عدد نقاط التوزيع وتكوينهم
حساب عدد بوابات الاتصال
تسجيل المعلومات حول أحداث المهام والسياسات
الاعتبارات الخاصة والإعدادات المثالية الخاصة بمهام محددة
معدل تكرار اكتشاف الأجهزة
مهمة النسخ الاحتياطي لبيانات خادم الإدارة ومهمة صيانة خادم الإدارة
مهام جماعية لتحديث Kaspersky Endpoint Security
مهمة الجرد

تفاصيل حول انتشار حمل الشبكة بين خادم الإدارة والأجهزة المحمية
استهلاك حركة المرور بموجب السيناريوهات المختلفة
متوسط استخدام حركة المرور كل 24 ساعة
الاتصال بالدعم الفني
كيفية الحصول على الدعم الفني
الدعم الفني من خلال Kaspersky CompanyAccount
الحصول على ملفات تفريغ خادم الإدارة
مصادر المعلومات المتعلقة بالتطبيق
مسرد المصطلحات
(AWS API) AWS Application Program Interface
HTTPS
JavaScript
(KPSN) Kaspersky Private Security Network
Kaspersky Security Center Operator
Kaspersky Security Center Web Server
(KSN) Kaspersky Security Network
(LWNGT) Lightweight Nagent
SSL
أداة التحقق من سلامة نظام (SHV) Kaspersky Security Center
إعدادات البرنامج
إعدادات المهمة
استعادة بيانات خادم الإدارة
اكتشاف السحابة
الأجهزة المدارة
الإدارة المباشرة للتطبيق
الإدارة المركزية للتطبيق
الاستعادة
التثبيت الإجباري
التثبيت المحلي
التثبيت اليدوي
التثبيت عن بُعد
التحديث المتوفر
التطبيق غير متوافق
الثغرات الأمنية
الحماية ضد فيروسات الشبكة
الشهادة المشتركة
المهمة
الهوية وإدارة الوصول (IAM)
الوعي بموقع الشبكة (NLA)
انتشار الفيروس
بوابة الاتصال
بيئة السحابة
تحديث
ترقية Kaspersky Security Center
جهاز iOS MDM
جهاز KES
جهاز حماية UEFI

حالة الحماية
حالة حماية الشبكة
حزمة التثبيت
حقوق المسؤول
خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
خادم الإدارة
خادم الإدارة الافتراضي
خادم الإدارة الرئيسي
خادم الجهاز المحمول
خدمات تحديث خادم Windows (WSUS)
خطورة الحدث
خوادم تحديث Kaspersky
دليل التقوية
دور IAM
سياسة
شهادة خادم الإدارة
صورة جهاز Amazon (AMI)
عتبة نشاط الفيروس
عميل الشبكة
عميل خادم الإدارة (الجهاز العميل)
فترة الترخيص
قواعد بيانات مكافحة الفيروسات
مالك الجهاز
متجر التطبيقات
مثيل Amazon EC2
مجال البث
مجلد النسخ الاحتياطي
مجموعة الإدارة
مجموعة التطبيقات المرخصة
محطة عمل المسؤول
مسؤول Kaspersky Security Center
مسؤول العميل
مسؤول موفر الخدمة
مستخدم IAM
مستخدمين داخليين
مستودع الأحداث
مستوى أهمية التصحيح
مفتاح الترخيص الإضافي (أو الاحتياطي)
مفتاح مفعل
مفتاح وصول AWS IAM
مكون الإدارة الإضافي
ملف المفتاح
ملف تعريف iOS MDM
ملف تعريف التزويد
ملف تعريف التكوين
منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)
مهمة جماعية

مهمة لأجهزة محددة
مهمة محلية
موفر خدمة الحماية ضد الفيروسات
نسخ احتياطي لبيانات خادم الإدارة
نقطة توزيع
هجوم الوسيط
وحدة التحكم الخاصة بإدارة AWS
وحدة تحكم الإدارة
وكيل المصادقة
معلومات حول التعليمات البرمجية الخاصة بطرف ثالث
إشعارات العلامة التجارية
المشكلات المعروفة

تعليمات Kaspersky Security Center 15.1

	ما الجديد اكتشف كل ما هو جديد في أحدث إصدار للتطبيق.		**تكوين حماية الشبكة** إدارة أمان المؤسسة
	متطلبات الأجهزة والبرامج تحقق أيًا من أنظمة التشغيل وإصدارات التطبيق مدعومة.		**تطبيقات Kaspersky. تحديث قواعد البيانات والوحدات النمطية للبرامج** الحفاظ على موثوقية نظام الحماية.
	النشر والإعداد الأولي تخطيط استخدام الموارد، وتثبيت خادم الإدارة، وتثبيت عميل الشبكة، وتطبيقات الأمان على الأجهزة العميلة وجمع الأجهزة في مجموعات الإدارة.		**المراقبة وإعداد التقارير** عرض البنية الأساسية الخاصة بك، وحالات الحماية والإحصائيات. وقم إدارة الوصول إلى الخدمات السحابية باستخدام Cloud Discovery.
	اكتشاف الأجهزة المتصلة بالشبكة اكتشف الأجهزة الجديدة والموجودة على شبكة مؤسستك.		**استبدال تطبيقات الأمان من جهة خارجية** تعرف على طرق لإلغاء تثبيت التطبيقات غير المتوافقة.
	تطبيقات Kaspersky. النشر المركزي نشر تطبيقات Kaspersky.		**تعديل نقاط التوزيع وبوابات الاتصال** تكوين نقاط التوزيع.
	ترقية Kaspersky Security Center من إصدار سابق ترقية Kaspersky Security Center 15.1 من إصدار سابق.		**أفضل ممارسات موفري الخدمة (التعليمات عبر الإنترنت فقط)** تعرف على التوصيات حول كيفية نشر التطبيق وتكوينه واستخدامه، بالإضافة إلى شرح طرق حل المشكلات النمطية عند عمل التطبيق.
	تطبيقات Kaspersky. الترخيص والتفعيل تفعيل تطبيقات Kaspersky في بضع خطوات.		**دليل القياس (التعليمات عبر الإنترنت فقط)** للحصول على أداء مثالي والحفاظ عليه تحت ظروف مختلفة، ضع في اعتبارك عدد الأجهزة المتصلة بالشبكة ومخطط الشبكة ومجموعة ميزات Kaspersky Security Center التي تطلبها.
	تصدير الأحداث إلى أنظمة SIEM قم بتكوين تصدير الأحداث إلى أنظمة SIEM لتحليلها.		**إدارة الثغرات الأمنية والتصحيحات** ابحث عن الثغرات الأمنية وأصلحها في برامج الجهات الخارجية.
	العمل في بيئة السحابة انشر Kaspersky Security Center في البيئات السحابية: كمنصة Amazon Web Services ™ ومنصة Microsoft Azure ™ ومنصة Google Cloud ™.		**الأسئلة الشائعة (الإنجليزية فقط)** ابحث عن إرشادات حول كيفية حل المشكلات الشائعة.
	دليل البدء السريع لـ Kaspersky Endpoint Security for Business ابدأ باستخدام Kaspersky Endpoint Security for Business: ثبّت هذا الحل وتكوينه. يمكنك أيضًا فحص مقارنة ميزات Kaspersky Security Center، لاختيار الطريقة الأنسب لإدارة أمان الشبكة.		

ما الجديد

التحديث 2 لتطبيق Kaspersky Security Center 15.1

يركز التحديث 2 لتطبيق Kaspersky Security Center 15.1 على إصلاح المشكلات التي أبلغ عنها المستخدمون وفريق الاختبار:

- أصبحت المهام تُنفّذ بشكل صحيح على نطاق الأجهزة المدارة التي تعمل بنظام التشغيل Linux، وذلك عند تحديدها عن طريق استيراد ملف نصي (TXT).
- الآن، عند تثبيت تطبيق Kaspersky باستخدام مهمة تثبيت عن بُعد تم إنشاؤها على خادم إدارة افتراضي، يتم إرسال حزم التثبيت إلى الأجهزة المدارة باستخدام أدوات نظام التشغيل فقط من خلال نقطة التوزيع التي يديرها المُشغل الافتراضي لهذا الخادم.
- تم حل المشكلة التي تحدث عند فشل خادم إدارة ثانوي في إعادة الاتصال بخادم الإدارة الأساسي بعد تدوير شهادة الخادم الثانوي.
- تم حل المشكلات التي تؤثر على اتصالات TLS.
- تم حل مشكلة تسببت في العديد من أخطاء "تحويل نوع غير صالح" أثناء تسجيل دخول المستخدم.
- يرسل Kaspersky Security Center الآن إخطارات الأحداث عبر البريد الإلكتروني بشكل صحيح.
- تم إصلاح مشكلة إضافة مجلد التحديثات إلى النسخة الاحتياطية عند ترقية Kaspersky Security Center من الإصدار 14.2 إلى الإصدار 15.1.
- يتم الآن عرض تاريخ انتهاء صلاحية ترخيص تطبيق Kaspersky بشكل صحيح في Kaspersky Security Center Web Console.
- يعمل الآن أمرا **تحديد موقع الجهاز المحمول والحصول على محفوظات موقع الجهاز** بشكل صحيح.
- تم إصلاح المشكلة التي كانت تتسبب في عدم حذف حزم التثبيت التي تحتوي على شهادات أجهزة محمولة تلقائيًا بعد ساعة واحدة من التنزيل أو بعد 24 ساعة من عدم استخدامها.
- أصبح الآن ملف تعريف السياسة الذي يتم تفعيله بعلامة محددة يُطبّق بشكل صحيح على الأجهزة التي تحتوي أوصافها على تلك العلامة.
- تم إصلاح مشكلة كانت تتسبب في ظهور رسائل خطأ قاعدة بيانات PostgreSQL في سجل الأحداث.
- أصبحت الآن عملية استثناء حساب من التحقق بخطوتين تعمل بشكل صحيح.
- تم حل مشكلة كانت تمنع تسجيل الخروج من Kaspersky Security Center Web Console من العمل بشكل صحيح عند استخدام المصادقة عبر النطاق مع تفعيل ميزة مدير الهوية والوصول.
- الآن، عند تحديث مكون إضافي للويب للإدارة، يؤدي الضغط على الرابط الذي يحتوي على إصدار المكون الإضافي إلى بدء التنزيل.
- المشكلات التي تم إصلاحها في التقارير:
  - عند إنشاء مهمة تسليم للتقارير عن التهديدات والتحديثات، وتعيين جدول المهام إلى **شهريًا**، يتم تعبئة التقارير بالبيانات بشكل صحيح.
  - في التقرير عن حالة قالب مكونات التطبيق، يتم تطبيق عوامل التصفية حسب اسم المكون بشكل صحيح.
  - يمكن الآن تصفية تقرير نشر الحماية لعرض الأجهزة التي لم يتم تثبيت تطبيقات Kaspersky عليها. ويساعد هذا في تصور عدد الأجهزة التي سيتم تثبيت التطبيقات عليها.
- يتم عرض أداة **Cloud Discovery** بشكل صحيح سواء كان لديك حق **التنفيذ** في منطقة **الميزات العامة: الوظائف الأساسية** أم لا.
- تم تحسين أداء الإجراءات المخزنة وعمليات قاعدة البيانات.

- تم إصلاح مشكلة كانت تتسبب فيها الشهادات منتهية الصلاحية والمرتبطة بمستخدمين غير موجودين، في توقف عملية التجديد لجميع المستخدمين.

- تم حل المشكلات التي تؤثر على التعامل الصحيح مع الشهادات.

- بعد ترقية Kaspersky Security Center من الإصدار 14.2 إلى 15.1، أصبح الآن تنزيل حزمة تثبيت مستقلة من خادم إدارة افتراضي ثانوي في وحدة تحكم الإدارة يعمل بشكل صحيح.

- تم إصلاح مشكلة في Kaspersky Security Center Web Console، حيث عند تمكين استخدام Kaspersky Security Network (KSN) في سياسة تطبيق Kaspersky، لم يكن خيار قبول بيان KSN متاحًا للتطبيقات التالية: Kaspersky Endpoint Security for Linux الإصدار 12.2 أو أقدم، وKaspersky Industrial CyberSecurity for Linux Nodes الإصدار 1.5 أو أقدم، وKaspersky Security for Virtualization Light Agent، الإصدار 6.0 و6.1، وKaspersky Embedded Systems Security for Linux الإصدار 3.3، وKaspersky Security for Windows Server الإصدار 11.0.1.897.

- تم إصلاح مشكلة كانت تمنع تطبيق ملف تعريف السياسة على الأجهزة التي تعمل بنظام Linux والتي يتم تضمينها في مجموعة نطاق Active Directory.

- تم إصلاح مشكلة حدثت أثناء محاولات الاتصال من عدة خوادم إدارة ثانوية من المستوى الثاني إلى خادم الإدارة الرئيسي.

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 له العديد من الميزات والتحسينات الجديدة:

- Cloud Discovery. هذه ميزة جديدة تسمح لك بمراقبة محاولات استخدام الخدمات السحابية على الأجهزة المُدارة التي تعمل بنظام التشغيل Windows، ومنع الوصول إلى الخدمات السحابية التي تعتبرها غير مرغوب فيها. هذه الميزة متاحة فقط في Kaspersky Security Center Web Console.

- يتيح لك استقصاء وحدة تحكم المجال الآن استطلاع وحدة تحكم مجال Samba من خلال نقطة توزيع تعتمد على Linux. تم إجراء تحسينات إضافية لدعم استقصاء المجالات الكبيرة.

- تم تحسين التشخيص عن بعد للأجهزة المُدارة المستندة إلى Linux.

- مخزون أجهزة موسع لنظام التشغيل macOS. يرسل عميل الشبكة على جهاز macOS عنوان MAC والرقم التسلسلي للجهاز إلى خادم الإدارة.

- يمكنك الآن التحقق من الاتصال بنظام SIEM.

- تم زيادة الحد الأقصى لطول كلمة المرور للمستخدم الداخلي إلى 256 حرفًا.

- عند الترحيل من Kaspersky Security Center Windows إلى Kaspersky Security Center Linux، يمكنك الآن تبديل الأجهزة المُدارة لتكون تحت إدارة Kaspersky Security Center Linux من خلال استعادة الشهادة والمفتاح الخاص لخادم الإدارة من نسخة احتياطية.

- عند تشغيل أداة Cleaner أو أداة klmover لإزالة عميل الشبكة المحمي بكلمة مرور، سيُطلب منك إدخال كلمة مرور إلغاء التثبيت.

- لم تعد الترقية من Kaspersky Security for Windows Server إلى Kaspersky Security for Windows Server تتطلب إعادة تشغيل الجهاز المستهدف.

- يمكن تعيين مستخدم كمالك للجهاز أثناء تثبيت عميل الشبكة على جهاز عميل على Linux أو بعد تثبيته.

- يمكنك الآن تلقي تقرير عن التثبيت عن بُعد عند تثبيت البرنامج على الأجهزة المُدارة من خلال البرامج النصية المخصصة.

- عند تنفيذ عدة نصوص مخصصة على جهاز مُدار، يمكنك تعيين أولوية لكل نص لتحديد ترتيب التنفيذ. وسيتم تنفيذ البرامج النصية بدءًا من البرنامج النصي ذي الأولوية الأعلى إلى البرنامج النصي ذي الأولوية الأقل.

- التدقيق الموسع للسياسة. يمكنك الآن عرض محتويات مراجعة سياسة وحفظ مراجعة سياسة في ملف. وفي الوقت الحالي، تتوفر هذه الميزات فقط لسياسة خادم الإدارة وسياسة عميل الشبكة.

- تحسينات تجربة المستخدم، بما في ذلك:
  - تخصيص القائمة الرئيسية من خلال تثبيت أقسام في Kaspersky Security Center Web Console للوصول السريع من القسم **Pinned**.
  - تحسين العمل باستخدام الجداول. ويحتوي الآن العرض الافتراضي لكل جدول على الأعمدة الأكثر استخدامًا. بالإضافة إلى ذلك، يمكنك الآن تحديد كل العناصر الموجودة في الصفحة الحالية أو في الجدول بأكمله، بالإضافة إلى فرز العناصر في الجدول بأكمله.
  - تم تحسين تكوين تسليم التقارير. ويمكنك الآن تحديد ما يصل إلى 20 عنوان بريد إلكتروني لإرسال التقارير إليها، وجدول تسليم التقارير.
- يمكنك إلغاء حقوق المسؤول المحلي من الحسابات الموجودة على الأجهزة المُدارة المستندة إلى Linux. ويتيح لك هذا طبقة إضافية من التحكم في حسابات المستخدم. على سبيل المثال، يمكنك إلغاء حقوق المسؤول المحلي بعد اكتمال التعيين لمرة واحدة.
- يمكنك تغيير كلمة مرور الحساب المحلي على الأجهزة المُدارة المستندة إلى Linux، على سبيل المثال، عندما ينسى المستخدم كلمة مرور الحساب المحلي أو لإجراء تغيير كلمة مرور مجدول.
- في القسم الفرعي **إدارة شهادات المستخدم**، يمكنك تحديد شهادات الجذر التي تريد تثبيتها. ويمكن استخدام هذه الشهادات، على سبيل المثال، للتحقق من صحة مواقع الويب أو خوادم الويب.
- يتضمن Report on network attacks الآن عنوان MAC ومنفذ الجهاز المهاجم.
- خيار جديد لإجبار المستخدم الداخلي على تغيير كلمة المرور عند المحاولة التالية لتسجيل الدخول إلى Kaspersky Security Center Web Console.
- لم يعد يتم التحقق من ترخيص تجاري عند تصدير الأحداث إلى نظام SIEM بتنسيقات CEF أو LEEF.
- عند الانتقال من تطبيق Kaspersky إلى تطبيق آخر وكان تطبيقك الحالي محميًا بكلمة مرور، يمكنك الآن تحديد كلمة مرور إلغاء التثبيت في مهمة التثبيت عن بُعد.
- لم يعد Exchange ActiveSync مدعومًا.

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 له العديد من الميزات والتحسينات الجديدة:

- تم إصدار دليل تقوية جديد. نوصي بشدة بقراءة الدليل بعناية واتباع توصيات الأمان لتهيئة Kaspersky Security Center والبنية التحتية لشبكتك.

  يرجى أيضًا تثبيت آخر تحديث لبرنامج Kaspersky Security Center. يتضمن هذا التحديث ميزات حماية البنية التحتية مثل التحقق بخطوتين من حسابات المستخدمين وتحسينات أخرى.
- يتم الآن التحقق من الوصول إلى خوادم Kaspersky تلقائيًا. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم DNS العام.
- حقوق المستخدم على خادم إدارة افتراضي متاحة للتكوين في أي وقت بشكل مستقل عن خادم الإدارة الأساسي. يمكنك أيضًا تعيين حقوق مستخدمي الخادم الأساسيين لإدارة خادم افتراضي.
- يدعم الآن العمل Kaspersky Security Center مع DBMSs التالية:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (جميع الإصدارات)

- Postgres Pro 14.x (جميع الإصدارات)
- MariaDB 10.1، 10.4، 10.5

- يمكنك استخدام Kaspersky Security Center Web Console لتصدير السياسات والمهام إلى ملف، ثم استيراد السياسات والمهام إلى Kaspersky Security Center Windows أو Kaspersky Security Center Linux.
- تمت إزالة خيار **لا تستخدم الخادم الوكيل** من المهام التالية:
  - تنزيل التحديثات إلى مستودع خادم الإدارة
  - تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع
- لحماية أجهزة العميل في بيئة سحابية، يمكنك نشر Kaspersky Endpoint Security for Windows بدلاً من Kaspersky Security for Windows Server. هذه الميزة متاحة الآن بعد إصدار Kaspersky Endpoint Security 12.0 for Windows.
- أصبح العمل باستخدام مفاتيح التشفير مقيدًا الآن بحقوق الوصول **General features** : منطقة وظيفة **Encryption Key Management**. ويستطيع مستخدمو Kaspersky Security Center الآن تصدير مفاتيح التشفير إذا كان لديهم حق **القراءة**، ويمكنهم استيراد مفاتيح التشفير إذا كان لديهم حق **الكتابة**.

Kaspersky Security Center 14

Kaspersky Security Center 14 له العديد من الميزات والتحسينات الجديدة:

- يمكنك تثبيت التحديثات وإصلاح الثغرات الأمنية لبرامج الجهات الخارجية (باستثناء برامج Microsoft) في شبكة معزولة . تتضمن هذه الشبكات خوادم الإدارة والأجهزة المدارة التي ليس لها وصول إلى الإنترنت. لإصلاح الثغرات الأمنية في هذا النوع من الشبكات، تحتاج إلى تنزيل التحديثات المطلوبة عن طريق خادم الإدارة مع الوصول إلى الإنترنت، ثم إرسال التصحيحات إلى خوادم الإدارة المعزولة.
- تمت إضافة ملفات تعريف اتصال المستخدمين الموجودين خارج المكتب الخاصة بأجهزة macOS. باستخدام ملفات تعريف الاتصال، يمكنك تكوين قواعد عملاء الشبكة على أجهزة macOS للاتصال بخوادم الإدارة نفسها أو خوادم الإدارة المختلفة، بناءً على موقع الجهاز.
- يمكن الآن تثبيت عميل الشبكة على الأجهزة التي تعمل بنظام التشغيل Windows 10 IoT EnterpriseMicrosoft
- في **تقرير التهديدات**، يمكنك الآن تصفية قائمة التهديدات لعرض التهديدات التي تم اكتشافها بواسطة Cloud Sandbox.
- يدعم Kaspersky Security Center الآن ملفات Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 كتطبيق مُدار.

يتضمن Kaspersky Security Center Web Console العديد من الميزات والتحسينات الجديدة:

- يمكنك تكوين وضع لوحة المعلومات فقط للموظفين الذين لا يديرون الشبكة ولكنهم يرغبون في الاطلاع على إحصائيات حماية الشبكة في Kaspersky Security Center (على سبيل المثال، أحد كبار المديرين). عندما يقوم مستخدم بتمكين هذا الوضع، تُعرض لوحة معلومات تتضمن مجموعة محددة مسبقًا من التطبيقات المصغرة فقط. وبالتالي، يمكنه مراقبة الإحصائيات المحددة في التطبيقات المصغرة، على سبيل المثال، حالة الحماية لجميع الأجهزة المدارة، أو عدد التهديدات المكتشفة مؤخرًا، أو قائمة التهديدات الأكثر شيوعًا في الشبكة.
- يدعم Kaspersky Security Center Web Console الآن Kaspersky Security for iOS كتطبيق أمان.
- في خصائص المهمة، يمكنك تحديد ما إذا كنت تريد تطبيق المهمة على المجموعات الفرعية وخوادم الإدارة الثانوية (بما في ذلك الافتراضية) أم لا.
- يدعم Kaspersky Security Center الآن ملفات Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 كتطبيق مُدار.

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 له العديد من الميزات والتحسينات الجديدة:

- يمكنك الآن تثبيت خادم الإدارة، ووحدة تحكم الإدارة، و Kaspersky Security Center 13.2 Web Console، وعميل الشبكة على أنظمة التشغيل الجديدة التالية (راجع متطلبات البرنامج للحصول على التفاصيل):
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2 (تحديث أكتوبر 2021)
  - Windows Server 2022
- يمكنك استخدام MySQL 8.0 كقاعدة بيانات.
- يمكنك نشر Kaspersky Security Center على مجموعة تجاوز الفشل من Kaspersky Security Center، لتوفير إتاحة عالية من Kaspersky Security Center.
- يعمل Kaspersky Security Center الآن على عناوين IPv6 بالإضافة إلى عناوين IPv4. يمكن لخادم الإدارة استقصاء الشبكات التي تحتوي على أجهزة بعناوين IPv6.

لدى Kaspersky Security Center 13.2 Web Console العديد من الميزات والتحسينات الجديدة:

- يمكنك الآن إدارة الأجهزة المحمولة التي تعمل بنظام أندرويد عبر Kaspersky Security Center 13.2 Web Console.
- يتوفر سوق Kaspersky كقسم قائمة جديد: يمكنك البحث عن تطبيق Kaspersky عبر Kaspersky Security Center 13.2 Web Console.
- يدعم Kaspersky Security Center الآن تطبيقات Kasperskyالتالية:
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 له العديد من الميزات والتحسينات الجديدة:

- تم تحسين التكامل في أنظمة SIEM. يمكنك الآن تصدير الأحداث إلى أنظمة SIEM عبر القناة المشفرة (TLS). الميزة متاحة لتطبيق Kaspersky Security Center Web Console ووحدة التحكم في الإدارة القائمة على MMC.
- يمكنك الآن تلقي تصحيحات خادم الإدارة كحزمة توزيع، والتي يمكنك استخدامها في التحديثات المستقبلية للإصدارات الأحدث.
- تمت إضافة قسم جديد، و**تنبيهات**، لبرنامج Kaspersky Endpoint Detection and Response Optimum حتى برنامج Kaspersky Security Center 13.1 Web Console. تمت إضافة العديد من التطبيقات المصغّرة الجديدة أيضًا للعمل مع التهديدات التي اكتشفها Kaspersky Endpoint Detection and Response Optimum.

- يمكنك في Kaspersky Security Center 13.1 Web Console تلقي إشعارات حول انتهاء صلاحية التراخيص لتطبيقات Kaspersky.
- تم تقليل وقت استجابة Kaspersky Security Center 13.1 Web Console.

Kaspersky Security Center 13

تمت إضافة الميزات التالية إلى Kaspersky Security Center 13 Web Console:

- المصادقة الثنائية المطبقة. يمكنك تمكين المصادقة الثنائية لتقليل مخاطر الوصول غير المصرح به إلى Kaspersky Security Center 13 Web Console.
- مصادقة المجال المطبقة باستخدام بروتوكولات NTLM و Kerberos (تسجيل دخول أحادي). تتيح ميزة تسجيل الدخول الأحادي لمستخدم نظام Windows تمكين مصادقة آمنة في Kaspersky Security Center 13 Web Console دون أن يتعيّن عليه إعادة إدخال كلمة المرور على شبكة الشركة.
- يمكنك الآن تكوين مكون إضافي للعمل مع Kaspersky Managed Detection and Response. يمكنك استخدام هذا التكامل لعرض الحوادث وإدارة محطات العمل.
- يمكنك الآن تحديد إعدادات Kaspersky Security Center 13 Web Console في معالج تثبيت خادم الإدارة.
- يتم عرض الإخطارات عن الإصدارات الجديدة للتحديثات والتصحيحات. يمكنك تثبيت تحديث على الفور أو لاحقًا في أي وقت. يمكنك الآن تثبيت تصحيحات لخادم الإدارة عبر Kaspersky Security Center 13 Web Console.
- عند العمل مع الجداول، يمكنك الآن تحديد ترتيب وعرض الأعمدة وفرز البيانات وتحديد حجم الصفحة.
- يمكنك الآن فتح أي تقرير بالنقر فوق اسمه.
- Kaspersky Security Center 13 Web Console متاح الآن باللغة الكورية.
- يوجد قسم جديد: أخبار Kaspersky، متوفر الآن في قائمة **Monitoring & reporting**. يبقيك هذا القسم على اطلاع من خلال توفير المعلومات المتعلقة بإصدار Kaspersky Security Center لديك والتطبيقات المدارة المثبتة على الأجهزة المدارة. يقوم Kaspersky Security Center بتحديث المعلومات الواردة في هذا القسم بشكل دوري عن طريق إزالة الأخبار القديمة وإضافة معلومات جديدة. ومع ذلك، يمكنك تعطيل أخبار Kaspersky إذا كنت ترغب في ذلك.
- تم تنفيذ مصادقة إضافية بعد تغيير إعدادات حساب مستخدم. يمكنك تمكين حماية حساب المستخدم من التعديل غير المصرح به. إذا كان هذا الخيار مفعلاً، تعديل إعدادات حساب المستخدم يتطلب ترخيص مستخدم يملك حقوق التعديل.

تمت إضافة الميزات التالية إلى Kaspersky Security Center 13:

- تم تنفيذ المصادقة الثنائية. يمكنك تمكين المصادقة الثنائية لتقليل مخاطر الوصول غير المصرح به إلى وحدة تحكم الإدارة. إذا كان هذا الخيار مفعلاً، تعديل إعدادات حساب المستخدم يتطلب ترخيص المستخدم الذي يملك حقوق التعديل. يمكنك الآن تمكين أو تعطيل المصادقة الثنائية لأجهزة KES.
- يمكنك إرسال رسائل إلى خادم الإدارة عبر بروتوكول HTTP. يتوفر الآن دليل مرجعي ومكتبة Python للعمل مع OpenAPI لخادم الإدارة.
- يمكنك إصدار شهادة احتياطية للاستخدام في ملفات تعريف iOS MDM لضمان التبديل السلس لأجهزة iOS المُدارة بعد انتهاء صلاحية شهادة خادم iOS MDM.
- مجلد التطبيقات متعددة المستأجرين لم يعد معروضًا في وحدة تحكم الإدارة.

حول Kaspersky Security Center

يحتوي القسم على معلومات عن الغرض من Kaspersky Security Center وميزاته ومكوناته الرئيسية وطرق شراء Kaspersky Security Center.

قد تختلف المعلومات المقدمة في التعليمات عبر الإنترنت عن المعلومات المقدمة في المستندات التي يتم شحنها مع التطبيق؛ في هذه الحالة، تعتبر التعليمات عبر الإنترنت محدثة. يمكنك المتابعة إلى "التعليمات عبر الإنترنت" بالنقر فوق الروابط الموجودة في الواجهة أو بالنقر فوق رابط "التعليمات عبر الإنترنت" في المستندات. يمكن تحديث "التعليمات عبر الإنترنت" دون إشعار مسبق. يمكنك التبديل بين المساعدة عبر الإنترنت والمساعدة دون الاتصال بالإنترنت إذا لزم الأمر.

تم تصميم Kaspersky Security Center للتنفيذ المركزي لمهام الإدارة والصيانة الأساسية في شبكة المؤسسة. يُمكّن التطبيق المسؤول من الوصول إلى المعلومات المفصلة حول مستوى أمان شبكة المؤسسة؛ ويسمح بتكوين جميع مكونات الحماية التي تم إنشاؤها باستخدام تطبيقات Kaspersky.

ويستهدف Kaspersky Security Center مسؤولي شبكات الشركات والموظفين المسؤولين عن حماية الأجهزة في نطاق واسع من المؤسسات.

باستخدام Kaspersky Security Center يمكنك القيام بما يلي:

- بإنشاء ترتيب هرمي لخوادم الإدارة لإدارة شبكة المؤسسة، بالإضافة إلى الشبكات الموجودة في المكاتب البعيدة أو مؤسسات العميل.
  المؤسسة العميلة عبارة عن مؤسسة يقوم مزود الخدمة بضمان حمايتها ضد الفيروسات.
- قم بإنشاء ترتيب هرمي لمجموعات الإدارة لإدارة مجموعة محددة من الأجهزة العميلة ككل.
- إدارة نظام الحماية ضد الفيروسات الذي تم إنشاؤه استنادًا إلى تطبيقات Kaspersky.
- إنشاء صور نظام التشغيل ونشرها على الأجهزة العميلة عبر الشبكة، وإجراء تثبيت عن بُعد للتطبيقات بواسطة Kaspersky وبائعي البرامج الآخرين.
- إدارة التطبيقات المثبتة على الأجهزة العميلة عن بُعد بواسطة Kaspersky والموردين الآخرين. تثبيت التحديثات والعثور على الثغرات الأمنية وإصلاحها.
- تنفيذ نشر مركزي لمفاتيح الترخيص لتطبيقات Kaspersky على الأجهزة العميلة ومراقبة استخدامها وإعادة تجديد التراخيص.
- تلقي إحصاءات وتقارير عن تشغيل التطبيقات والأجهزة.
- تلقي إخطارات حول الأحداث الحرجة أثناء تشغيل تطبيقات Kaspersky.
- إدارة الأجهزة المحمولة.
- إدارة تشفير المعلومات المخزنة على محركات الأقراص الثابتة للأجهزة ومحركات الأقراص القابلة للإزالة ووصول المستخدمين إلى البيانات المشفرة.
- بتنفيذ مخزون الأجهزة المتصلة بشبكة المؤسسة.
- قم بإجراء الإدارة المركزية للملفات التي تم نقلها إلى العزل أو النسخ الاحتياطي بواسطة تطبيقات الأمن بالإضافة إلى إدارة الكائنات التي تم تأجيل معالجتها بواسطة تطبيقات الأمن.

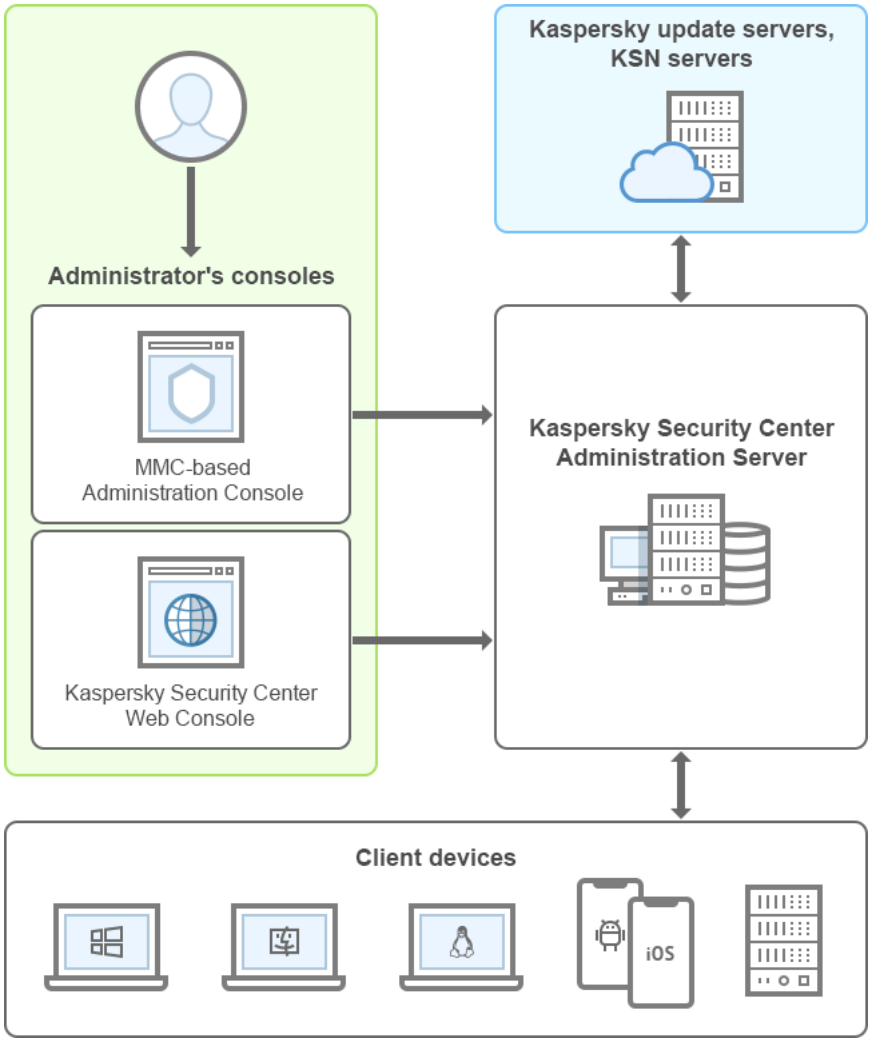
يمكنك شراء Kaspersky Security Center من خلال Kaspersky (على سبيل المثال، على https://www.kaspersky.com) أو من خلال الشركات الشريكة.

إذا اشتريت Kaspersky Security Center من خلال Kaspersky، يمكنك نسخ التطبيق من موقع الويب الخاص بنا. ويتم إرسال المعلومات المطلوبة لتفعيل التطبيق إليك عن طريق البريد الإلكتروني بعد معالجة الدفع.

وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية)، بالإضافة إلى وظيفة KSN التي قد لا تكون متاحة في البرنامج في الولايات المتحدة الأمريكية.

البنية الهندسية

يقدم هذا القسم وصفًا لمكونات Kaspersky Security Center وتفاعلها.



بنية Kaspersky Security Center

يتكون Kaspersky Security Center من المكونات الأساسية التالية:

- وحدة تحكم الإدارة (يشار إليها أيضًا في هذا المستند بـ وحدة التحكم). توفير واجهة مستخدم لخدمات الإدارة الخاصة بخادم الإدارة وعميل الشبكة. يتم تنفيذ وحدة تحكم الإدارة كأداة إضافية لـMicrosoft Management Console (MMC). تتيح لك وحدة تحكم الإدارة الاتصال عن بُعد بخادم الإدارة عبر الإنترنت.
- Kaspersky Security Center Web Console. تقدم واجهة الويب لإنشاء وصيانة نظام حماية شبكة تنظيم العميل التي تتم إدارتها بواسطة Kaspersky Security Center.
- خادم إدارة Kaspersky Security Center (ويُشار إليه كذلك باسم الخادم). يعمل على مركزة تخزين معلومات حول التطبيقات المثبتة على شبكة المؤسسة وحول كيفية إدارتها.

- خوادم تحديث Kaspersky. خوادم (S)HTTP في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق.

- خوادم KSN. الخوادم التي تحتوي على قاعدة بيانات Kaspersky المزودة بمعلومات محدثة باستمرار حول سمعة الملفات وموارد الويب والبرامج. ويضمن استخدام Kaspersky Security Network الحصول على استجابات أسرع للتهديدات من قِبل تطبيقات Kaspersky، ويحسن من أداء بعض مكونات الحماية، ويقلل أيضًا من احتمالية ظهور حالات إيجابية زائفة.

- أجهزة العميل. أجهزة شركة العميل المحمية بواسطة Kaspersky Security Center. يجب أن يكون لكل جهاز يلزم حمايته أحد تطبيقات أمان Kaspersky المثبتة.

متطلبات الأجهزة والبرامج

- متطلبات خادم الإدارة
- متطلبات Web Console
- متطلبات الخوادم المتنقلة
- متطلبات وحدة تحكم الإدارة
- متطلبات عميل الشبكة

للحصول على متطلبات إصدار نظامي Android وiOS لنشر الحماية وإدارة الأجهزة المحمولة، ارجع إلى تعليمات Kaspersky Security for Mobile وتعليمات Kaspersky Secure Mobility Management.

متطلبات خادم الإدارة

الحد الأدنى لمتطلبات الجهاز:

- وحدة معالجة مركزية بتردد تشغيل 1 جيجاهرتز أو أعلى. بالنسبة لنظام تشغيل 64 بت، يكون الحد الأدنى لتردد وحدة المعالجة المركزية هو 1.4 جيجاهرتز.
- ذاكرة الوصول العشوائي: 4 جيجابايت
- مساحة القرص المتاحة: 10 جيجا بايت. عند استخدام إدارة الثغرات الأمنية والتصحيحات، يجب توفير مساحة على القرص بمقدار 100 جيجا بايت على الأقل.

للنشر في البيئات السحابية، تكون متطلبات خادم الإدارة وخادم قاعدة البيانات هي نفسها متطلبات خادم الإدارة الفعلي (اعتمادًا على عدد الأجهزة التي تريد إدارتها).

متطلبات البرامج:

- مكونات الوصول إلى بيانات Microsoft® (MDAC) 2.8
- Microsoft Windows® DAC 6.0.
- Microsoft Windows Installer 4.5

أنظمة التشغيل التالية مدعومة:

للتواصل بين العمليات في نظام التشغيل، يجب أن تكون واجهة الحلقة المرتدة متاحة.

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core إصدار 64 بت
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installation Option) (LTSB) إصدار 64 بت
- Windows Server 2019 Standard/Datacenter/Core 64 بت
- Windows Server 2022 Standard/Datacenter/Core 64 بت
- Windows Server 2025 Standard/Datacenter/Core بنظام 64 بت
- Windows Storage Server 2019 64 بت

يتم دعم الأنظمة الأساسية الظاهرية التالية:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 إصدار 64 بت
- Microsoft Hyper-V Server 2022 إصدار 64 بت
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

خوادم قاعدة البيانات التالية مدعومة (يمكن تثبيتها على جهاز مختلف):

- Microsoft SQL Server 2016 (جميع الإصدارات) إصدار 64 بت
- Microsoft SQL Server 2017 (جميع الإصدارات) على Windows/Linux إصدار 64 بت
- Microsoft SQL Server 2019 (جميع الإصدارات) على Windows/Linux 64 بت (يتطلب إجراءات إضافية)
- Microsoft SQL Server 2022 (جميع الإصدارات) على Windows/Linux إصدار 64 بت
- MySQL 5.7 Community إصدار 32 بت / 64 بت
- MySQL Standard Edition 8.0 (إصدار 8.0.20 وأحدث) إصدار 32 بت / 64 بت
- MySQL Enterprise Edition 8.0 (إصدار 8.0.20 وأحدث) إصدار 32 بت / 64 بت
- MariaDB 10.5 (إصدار 10.5.27 وأحدث) إصدار 32 بت / 64 بت

- MariaDB Galera Cluster 10.3 إصدار 32 بت / 64 بت مع محرك تخزين InnoDB
- PostgreSQL 13.x إصدار 64 بت
- PostgreSQL 14.x إصدار 64 بت
- PostgreSQL 15.x إصدار 64 بت
- Postgres Pro 13.x Windows/Linux 64 بت
- Postgres Pro 14.x Windows/Linux 64 بت

راجع الموضوع التالي للتعرف على التفاصيل والقيود: اختيار نظام إدارة قاعدة البيانات.

SIEM وأنظمة إدارة المعلومات الأخرى:

- HP ArcSight ESM 7.0 (Micro Focus)
- IBM Qradar 7.3
- Splunk 7.1

متطلبات Web Console

Kaspersky Security Center Web Console Server

الحد الأدنى لمتطلبات الجهاز:

- وحدة المعالجة المركزية: 4 مراكز معالجة وتردد تشغيل 2.5 جيجا هرتز
- ذاكرة الوصول العشوائي: 8 جيجا بايت
- مساحة القرص المتوفرة: 40 جيجابايت

الحد الأدنى لمتطلبات شهادة خادم الإدارة:

- خوارزمية توقيع الشهادة SHA-2
- الحد الأدنى لطول المفتاح 2048

إذا كنت بحاجة إلى إعادة إصدار الشهادة، فراجع قاعدة معارف Kaspersky Security Center.

أنظمة التشغيل التي يدعمها Kaspersky Security Center Web Console Server

أنظمة التشغيل. Microsoft Windows (إصدارات 64 بت فقط) للتواصل بين العمليات في نظام التشغيل، يجب أن تكون واجهة الحلقة المرتدة متاحة.	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Installation) Windows Server 2016 Standard/Datacenter/Essentials/Server Core (LTSB) (Option Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019

الأنظمة الأساسية للمحاكاة الافتراضية	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

الأجهزة العميلة

بالنسبة لجهاز عميل، لا يتطلب استخدام Kaspersky Security Center Web Console إلا وجود مستعرض.

الحد الأدنى لدقة الشاشة هو 1366 × 768 بكسل.

تتطابق متطلبات الأجهزة والبرامج في الجهاز مع تلك الخاصة بالمستعرض المستخدم للعمل مع Kaspersky Security Center Web Console.

المستعرضات:

- Google Chrome 128.0.6613.120 أو الإصدارات الأحدث
- Microsoft Edge 128.0.2739.67 أو أحدث
- Safari 17.6 على macOS
- "Yandex" Browser 24.7.3.1081 أو أحدث
- Mozilla Firefox Extended Support Release 115.14.0 أو أحدث

متطلبات الخوادم المتنقلة

خادم إدارة الأجهزة المحمولة التي تعمل بنظام iOS (iOS MDM)

متطلبات الأجهزة:

- وحدة معالجة مركزية بتردد تشغيل 1 جيجاهرتز أو أعلى. بالنسبة لنظام تشغيل 64 بت، يكون الحد الأدنى لتردد وحدة المعالجة المركزية هو 1.4 جيجاهرتز.
- ذاكرة الوصول العشوائي: 2 جيجابايت
- مساحة القرص المتوفرة: 2 جيجابايت.

متطلبات الأجهزة: نظام التشغيل Microsoft Windows (يتم تحديد الإصدار المدعوم لنظام التشغيل حسب متطلبات خادم الإدارة).

متطلبات وحدة تحكم الإدارة

متطلبات الأجهزة:

- وحدة معالجة مركزية بتردد تشغيل 1 جيجاهرتز أو أعلى. بالنسبة لنظام تشغيل 64 بت، يكون الحد الأدنى لتردد وحدة المعالجة المركزية هو 1.4 جيجاهرتز.
- ذاكرة الوصول العشوائي: 512 ميجابايت.
- مساحة القرص المتوفرة: 1 جيجا بايت.

متطلبات البرامج:

- نظام التشغيل Microsoft Windows (يتم تحديد الإصدار المدعوم لنظام التشغيل حسب متطلبات خادم الإدارة):
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64 بت
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) إصدار 64 بت
  - Windows Server 2019 Standard/Datacenter إصدار 64 بت
  - Windows Server 2022 Standard/Datacenter إصدار 64 بت
  - Windows Server 2025 Standard/Datacenter/Core بنظام 64 بت
  - Windows Storage Server 2019 64 بت
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 يعمل على:
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Storage Server 2019
- Microsoft Edge يعمل على Microsoft Windows Server 2022 Standard

متطلبات عميل الشبكة

الحد الأدنى لمتطلبات الجهاز:

- وحدة معالجة مركزية بتردد تشغيل 1 جيجاهرتز أو أعلى. بالنسبة لنظام تشغيل 64 بت، يكون الحد الأدنى لتردد وحدة المعالجة المركزية هو 1.4 جيجاهرتز.
- ذاكرة الوصول العشوائي: 512 ميجابايت.
- مساحة القرص المتوفرة: 1 جيجا بايت.

متطلبات البرامج للأجهزة التي تعمل بنظام Linux: يجب تثبيت مترجم لغة Perl الإصدار 5.10 أو أحدث.

أنظمة التشغيل Microsoft Windows	Windows Embedded POSReady 2009 مع أحدث حزمة خدمة إصدار 32 بت Windows Embedded Standard 7 مع حزمة الخدمة 1 إصدار 32 بت / 64 بت Windows Embedded 8.1 Industry Pro إصدار 32 بت / 64 بت Windows 10 Enterprise 2015 LTSB إصدار 32 بت/64 بت Windows 10 Enterprise 2016 LTSB إصدار 32 بت / 64 بت Windows 10 IoT Enterprise 2015 LTSB إصدار 32 بت / 64 بت Windows 10 IoT Enterprise 2016 LTSB إصدار 32 بت / 64 بت Windows 10 Enterprise 2019 LTSC إصدار 32 بت / 64 بت Windows 10 IoT Enterprise الإصدار 32 1703 بت/64 بت Windows 10 IoT Enterprise الإصدار 1709 إصدار 32 بت / 64 بت Windows 10 IoT Enterprise الإصدار 1803 إصدار 32 بت / 64 بت Windows 10 IoT Enterprise الإصدار 1809 إصدار 32 بت / 64 بت Windows 10 20H2 إصدار 32 بت / 64 بت Windows 10 Enterprise 21H2 إصدار 32 بت / 64 بت Windows 10 IoT Enterprise إصدار 32 بت / 64 بت Windows 10 IoT Enterprise الإصدار 1909 إصدار 32 بت / 64 بت Windows 10 IoT Enterprise 2021 LTSC إصدار 32 بت / 64 بت Windows 10 IoT Enterprise الإصدار 32 1607 بت/64 بت Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 بت/64 بت Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education لأنظمة 32 بت/64 بت Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM لأنظمة 64 بت Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education لأنظمة 64 بت Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 بت Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 بت Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 بت Windows 8 Pro/Enterprise إصدار 32 بت / 64 بت Windows 8.1 Pro/Enterprise 32 بت / 64 بت Windows 7 Home/Pro/Enterprise/Ultimate مع Service Pack 1 إصدار 32 بت / 64 بت Microsoft Windows XP Professional with Service Pack 2 بنظام 32 بت / 64 بت (مدعوم فقط بواسطة عميل الشبكة الإصدار 10.5.1781، الذي يمكنك طلبه من خلال الدعم الفني) نظام التشغيل Windows XP Professional مع حزمة الخدمة Service Pack 3 وإصدارات 32 بت الأحدث (مدعوم بواسطة عميل الشبكة الإصدار 14.0.0.20023) نظام التشغيل Windows XP Professional للأنظمة المضمنة مع حزمة الخدمة Service Pack 3 إصدار 32 بت (مدعوم بواسطة عميل الشبكة الإصدار 14.0.0.20023) Windows MultiPoint Server 2011 Standard/Premium إصدار 64 بت Windows Server 2003 SP1 بنظام 32 بت / 64 بت (معتمد فقط بواسطة عميل الشبكة الإصدار 10.5.1781) Windows Server 2003 SP2 Standard / Enterprise بنظام 32 بت / 64 بت (معتمد فقط بواسطة عميل الشبكة الإصدار 10.5.1781) Windows Server 2003 R2 Standard / Enterprise المزود مع حزمة الخدمة SP2 بنظام 32 بت / 64 بت (مدعوم فقط بواسطة عميل الشبكة الإصدار 10.5.1781) Windows Server 2008 Standard/Enterprise/Datacenter/Foundation مع حزمة الخدمة 2 إصدار 32 بت / 64 بت Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation/ مع حزمة الخدمة 1 وأحدث إصدار 64 بت Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core إصدار 64 بت Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core إصدار 64 بت

	Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installation Option) (LTSB) إصدار 64 بت Windows Server 2019 Standard/Datacenter/Core 64 بت Windows Server 2019 RS5 Standard/Essentials إصدار 64 بت Windows Server 2022 Standard/Datacenter/Core 64 بت Windows Server 2022 21H2 Standard/Datacenter إصدار 64 بت Windows Server 2025 Standard/Datacenter/Core بنظام 64 بت Windows Storage Server 2019 64 بت

أنظمة التشغيل. Linux	Debian GNU/Linux 10.x (Buster) إصدار 32 بت / 64 بت Debian GNU/Linux 11.x (Bullseye) 32 بت/64 بت Debian GNU/Linux 12 (Bookworm) إصدار 32 بت / 64 بت Ubuntu Server 18.04 LTS (Bionic Beaver) 64 بت Ubuntu Server 20.04 LTS (Focal Fossa) 64 بت Ubuntu Server 22.04 LTS (Jammy Jellyfish) إصدار 64 بت Ubuntu Server 22.04 LTS ARM إصدار 64 بت Ubuntu Server 24.04 LTS (Noble Numbat) إصدار 64 بت CentOS 6.7 وأحدث إصدار 32 بت CentOS 6.x (up to 6.6) إصدار 32 بت / 64 بت CentOS 7.x 64 بت CentOS Stream 8 64 بت CentOS Stream 9 64 بت CentOS Stream 9 ARM 64 بت Red Hat Enterprise Linux Server 6.x إصدار 32 بت / 64 بت Red Hat Enterprise Linux Server 7.x إصدار 64 بت Red Hat Enterprise Linux Server 8.x إصدار 64 بت Red Hat Enterprise Linux Server 9.x إصدار 64 بت SUSE Linux Enterprise Server 12 (جميع حزم الخدمة) إصدار 64 بت SUSE Linux Enterprise Server 15 (جميع حزم الخدمة) 64 بت SUSE Linux Enterprise Server 15 (كل حزم الخدمة) ARM إصدار 64 بت openSUSE 15 إصدار 64 بت EulerOS 2.0 SP10 64 بت EulerOS 2.0 SP10 ARM 64 بت Astra Linux Special Edition RUSB.10015-01 (التحديث التشغيلي 1.5) إصدار 64 بت Astra Linux Special Edition RUSB.10015-01 (التحديث التشغيلي 1.6) إصدار 64 بت Astra Linux Special Edition RUSB.10015-16 (الإصدار 1) (التحديث التشغيلي 1.6) إصدار 64 بت Astra Linux Special Edition RUSB.10015-17 (التحديث التشغيلي 1.7.3) إصدار 64 بت Astra Linux Special Edition RUSB.10015-01 (التحديث التشغيلي 1.7) إصدار 64 بت Astra Linux Special Edition RUSB.10015-01 (التحديث التشغيلي 1.8) إصدار 64 بت Astra Linux Special Edition RUSB.10015-37 (التحديث التشغيلي 7.7) إصدار 64 بت Astra Linux Special Edition RUSB.10152-02 (التحديث التشغيلي 4.7) ARM إصدار 64 بت Astra Linux Common Edition (التحديث التشغيلي 2.12) إصدار 64-bit ALT Workstation 10.1 64 بت ALT Server 10.1 64 بت ALT Education 10.1 64 بت ALT SP Server 10 إصدار 32 بت / 64 بت ALT SP Server 10 ARM إصدار 64 بت ALT SP Workstation 10 إصدار 32 بت / 64 بت ALT SP Workstation 10 ARM إصدار 64 بت ALT Server 10 إصدار 64 بت ALT Server 10 ARM إصدار 64 بت ALT Workstation 10 إصدار 32 بت / 64 بت ALT 8 SP Workstation (8.4) 64 ARM بت ALT 8 SP Server (8.4) ARM إصدار 64 بت ALT 8 SP Server (LKNV.11100-01) إصدار 32 بت / 64 بت ALT 8 SP Server (LKNV.11100-02) إصدار 32 بت / 64 بت ALT 8 SP Server (LKNV.11100-03) إصدار 32 بت / 64 بت ALT 8 SP Workstation (LKNV.11100-01) إصدار 32 بت / 64 بت ALT 8 SP Workstation (LKNV.11100-02) إصدار 32 بت / 64 بت ALT 8 SP Workstation (LKNV.11100-03) إصدار 32 بت / 64 بت Mageia 4 إصدار 32 بت Oracle Linux 7 إصدار 64 بت Oracle Linux 8 إصدار 64 بت Oracle Linux 9 64 بت Linux Mint 20.x إصدار 64 بت

	Linux Mint 21.1 وأحدث إصدار 64 بت AlterOS 7.5 وأحدث إصدار 64 بت GosLinux IC6/7.17 إصدار 64 بت GosLinux IC6/7.2 إصدار 64 بت SberOS 3.3.1 إصدار 64 بت Platform V SberLinux OS Server (SLO) 8.8 إصدار 64 بت Platform V SberLinux OS Server (SLO) 8.9.2 إصدار 64 بت RED OS 7.3 ARM إصدار 64 بت RED OS 7.3 Server إصدار 64 بت RED OS 7.3 إصدار معتمد 64 بت RED OS 8 Certified Edition إصدار 64 بت ROSA Enterprise Linux Server 7.9 إصدار 64 بت ROSA Enterprise Linux Desktop 7.9 إصدار 64 بت ROSA COBALT 7.9 إصدار 64 بت ROSA CHROME 12 إصدار 64 بت AlmaLinux 8 and later إصدار 64 بت AlmaLinux 9 وأحدث إصدار 64 بت Rocky Linux 8 وأحدث إصدار 64 بت Rocky Linux 9 وأحدث إصدار 64 بت Atlant، نسخة Alcyone، الإصدار 2022.02 إصدار 64 بت MSVSPHERE 9.2 SERVER إصدار 64 بت MSVSPHERE 9.2 ARM إصدار 64 بت SynthesisM Server 8.6 إصدار 64 بت SynthesisM Client 8.6 إصدار 64 بت OSnova 2.10 إصدار 64 بت Kylin 10 إصدار 64 بت EMIAS 1.0 إصدار 64 بت Amazon Linux 2 إصدار 64 بت MosOS 15.4 Arbat إصدار 64 بت OS MES (Moscow Electronic School) إصدار 64 بت
أنظمة التشغيل macOS.	للحصول على قائمة بأنظمة التشغيل المدعومة، راجع تعليمات Kaspersky Endpoint Security for Mac .

بالنسبة إلى عميل الشبكة، يتم أيضًا دعم بنية Apple Silicon (M1) بالإضافة إلى Intel.

يتم دعم الأنظمة الأساسية الظاهرية التالية:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- KVM (جهاز افتراضية معتمد على النواة).

في إصدارات Windows الأقدم من Microsoft Windows Server 2008 R2 (إصدارات الخادم) و Microsoft Windows 7 (إصدارات سطح المكتب) لا يدعم عميل الشبكة الوظائف التالية:

- إعادة ترجمة التحديثات (المستخدمة بواسطة نقاط التوزيع)
- خادم KSN الوكيل (المستخدم بواسطة نقاط التوزيع)
- مهمة فحص الثغرات الأمنية

على الأجهزة التي تعمل بنظام Microsoft Windows 10 الإصدار RS4 أو الإصدار RS5، قد يتعذر على Kaspersky Security Center اكتشاف بعض الثغرات الأمنية في المجلدات التي تم تمكين الحساسية لحالة الأحرف عليها.

قبل تثبيت عميل الشبكة على الأجهزة التي تعمل بنظام التشغيل Windows 7 أو Windows Server 2008 أو Windows Server 2008 R2، تأكد من تثبيت تحديث الأمان KB3063858 لنظام التشغيل Windows (تحديث الأمان لنظام التشغيل Windows 7 (KB3063858)، وتحديث الأمان لنظام التشغيل Windows 7 للأنظمة المستندة إلى x64 (KB3063858)، وتحديث الأمان لنظام التشغيل Windows Server 2008 (KB3063858)، وتحديث الأمان لنظام التشغيل Windows Server 2008 x64 Edition (KB3063858)، وتحديث الأمان لنظام التشغيل Windows Server 2008 R2 x64 Edition (KB3063858).

في Microsoft Windows XP، قد لا يؤدي عميل الشبكة بعض العمليات بشكل صحيح.

يمكنك تثبيت عميل الشبكة أو تحديثه لنظام التشغيل Windows XP في نظام التشغيل Microsoft Windows XP فقط. وتم سرد الإصدارات المدعومة من Microsoft Windows XP والإصدارات المقابلة لها من عميل الشبكة في قائمة أنظمة التشغيل المدعومة. ويمكنك تنزيل الإصدار المطلوب من عميل الشبكة لنظام التشغيل Microsoft Windows XP من هذه الصفحة.

نوصي بتثبيت الإصدار نفسه من عميل الشبكة مثل Kaspersky Security Center.

يدعم Kaspersky Security Center بشكل كامل عميل الشبكة من الإصدارات نفسها أو الإصدارات الأحدث.

يتوفر عميل الشبكة لنظام macOS معًا مع تطبيقات الأمان الخاصة بـ Kaspersky لأنظمة التشغيل هذه.

تطبيقات وحلول Kaspersky المتوافقة

يدعم Kaspersky Security Center النشر والإدارة المركزيين لجميع تطبيقات وحلول Kaspersky المدعومة حاليًا. يوضح الجدول أدناه تطبيقات وحلول Kaspersky التي تدعمها وحدة تحكم الإدارة المعتمدة على MMC و Kaspersky Security Center Web Console. لمعرفة إصدارات التطبيقات والحلول، ارجع إلى صفحة ويبدورة حياة دعم المنتج .

قائمة تطبيقات وحلول Kaspersky المدعومة بواسطة Kaspersky Security Center Web Console

اسم تطبيق أو حل Kaspersky	مدعومة بوحدة تحكم الإدارة المعتمدة على MMC	مدعوم بواسطة Kaspersky Security Center Web Console
لمحطات العمل		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓

اسم تطبيق أو حل Kaspersky	مدعومة بوحدة تحكم الإدارة المعتمدة على MMC	مدعوم بواسطة Kaspersky Security Center Web Console
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	—	✓
للحلول الصناعية		
الأمن الإلكتروني الصناعي من Kaspersky للعقد	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (النشر المركزي غير مدعوم)	✓	✓
للأجهزة المحمولة		
Kaspersky Endpoint Security for Android:	✓	✓
Kaspersky Security لأجهزة iOS	—	✓
لخوادم الملفات		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
للبيئات الظاهرية		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	—
بالنسبة لاكتشاف هجمات مستهدفة		
خادم Kaspersky Sandbox	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
لأجهزة KasperskyOS		
بوابة Kaspersky IoT الآمنة	—	✓
Thin Client Kaspersky	—	✓
قواعد بيانات السمعة		
Kaspersky Private Security Network	—	✓

تراخيص وميزات برنامج Kaspersky Security Center 15.1

يتطلب برنامج Kaspersky Security Center ترخيصًا لبعض من ميزاته.

الجدول أدناه يوضح الترخيص وما يتناوله من ميزات Kaspersky Security Center.

لتمكين ميزات Kaspersky Security Center، يجب عليك تفعيل خادم الإدارة عن طريق إضافة مفتاح ترخيص خادم الإدارة.

ويجب عليك إضافة مفتاح ترخيص يدويًا لكل خادم إدارة.

ميزات Kaspersky Security Center	إدارة الثغرات الأمنية والتصحيحات من Kaspersky	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
تقييم الثغرات الأمنية	✓	✓	✓	✓	✓	✓	✓
إدارة التصحيح	✓	—	✓	✓	—	✓	✓
التحكم في الوصول على أساس الدور	✓	✓	✓	✓	✓	✓	✓
التثبيت لنظم التشغيل والتطبيقات	✓	—	✓	✓	—	✓	✓
إدارة الأجهزة المحمولة (أي إدارة أجهزة المستخدمين التي تعمل بنظام iOS أو Android)	✓	✓	✓	✓	—	—	✓
قم بتكوين بيئة السحابة للعمل في بيئات السحابة مثل AWS أو Microsoft Azure أو Google Cloud	—	—	—	—	✓	✓	—
تصدير الأحداث إلى أنظمة SIEM: Syslog	✓	✓	✓	✓	✓	✓	✓
تصدير الأحداث إلى أنظمة SIEM: QRadar بواسطة IBM و Micro Focus بواسطة ArcSight	✓	✓	✓	✓	✓	✓	✓

عن توافق مكونات Kaspersky Security Center

في الجدول أدناه، يمكنك العثور على معلومات حول توافق مكونات Kaspersky Security Center.

توافق مكونات Kaspersky Security Center

المكون	متوافق مع
خادم إدارة Kaspersky Security Center 15.1	• Kaspersky Security Center 15.1 Administration Console. • Kaspersky Security Center 15.1 Web Console. • Kaspersky Security Center Network Agent من الإصدارات التالية: 16.3، 16.2، 16.1، 16، 15.4، 15.1، 15، 14.2، 14.
Kaspersky Security Center 15.1 Web Console	Kaspersky Security Center Administration Server من الإصدارات التالية: 15.1 و14.2.
Kaspersky Security Center 15.1 Primary Administration Server	خوادم الإدارة الثانوية: • Kaspersky Security Center 14 Windows. • Kaspersky Security Center 14.2 Windows. • Kaspersky Security Center 15.1 Windows. • Kaspersky Security Center 14.2 Linux. • Kaspersky Security Center 15 Linux. • Kaspersky Security Center 15.1 Linux.

المكون	متوافق مع
Kaspersky Security Center 15.1 Secondary Administration Server	خوادم الإدارة الأساسية: • Kaspersky Security Center 14 Windows. • Kaspersky Security Center 14.2 Windows. • Kaspersky Security Center 15.1 Windows. • Kaspersky Security Center 14.2 Linux. • Kaspersky Security Center 15 Linux. • Kaspersky Security Center 15.1 Linux.

نوصي باستخدام أحدث إصدار من كل من Kaspersky Security Center Administration Server و Kaspersky Security Center Web Console. وبخلاف ذلك، قد تكون وظائف Kaspersky Security Center محدودة. يمكنك تثبيت وترقية خادم إدارة Kaspersky Security Center وكذلك Kaspersky Security Center Web Console بشكل مستقل. يجب عليك التأكد أن إصدار Kaspersky Security Center Web Console المثبت متوافق مع إصدار خادم الإدارة الذي تتصل به.

إذا كان لديك أحدث إصدار من Kaspersky Security Center Web Console والإصدار السابق من Kaspersky Security Center، وحدث خطأ أثناء مصادقة المجال، فسيتضمن نص الخطأ رسالة افتراضية.

مقارنة Kaspersky Security Center: المستندة إلى Windows مقابل المستندة إلى Linux

يوفر Kaspersky Center كحل محلي لمنصتين أساسيتين - Windows و Linux. في الحل المستند إلى Windows، تقوم بتثبيت خادم الإدارة على جهاز يعمل بنظام التشغيل Windows، ويحتوي الحل المستند إلى Linux على إصدار خادم الإدارة المصمم ليتم تثبيته على جهاز Linux. تحتوي هذه التعليمات عبر الإنترنت على معلومات حول Kaspersky Security Center Windows. للحصول على معلومات مفصلة عن الحل المستند إلى Linux، يُرجى الرجوع إلى تعليمات Kaspersky Security Center Linux عبر الإنترنت.

يتيح لك الجدول أدناه مقارنة الميزات الرئيسية لبرنامج Kaspersky Security Center كحل مستند إلى Windows وكحل مستند إلى Linux.

مقارنة ميزات Kaspersky Security Center الذي يعمل كحل مستند إلى Windows والحل المستند إلى Linux

الميزة أو الملكية	Kaspersky Security Center	
	حل قائم على Windows	حل قائم على Linux
خادم الإدارة		
موقع نظام إدارة قواعد البيانات (DBMS)	في أماكن العمل	في أماكن العمل (Microsoft SQL غير مدعوم)
نظام تشغيل لتثبيت خادم الإدارة عليه	Windows	Linux
التسلسل الهرمي لخوادم الإدارة	✓	✓
دعم خوادم الإدارة الافتراضية	✓	✓
استخدام SNMP لإرسال إحصائيات خادم الإدارة إلى تطبيقات الطرف الثالث	✓	سيتم تنفيذه في 2026
خادم الويب لنشر حزم التثبيت والملفات الأخرى	✓	✓
تثبيت خادم الإدارة على مجموعة تجاوز الفشل في موقع واحد في نظام Windows Server	✓	—
نشر مجموعة تجاوز الفشل من Kaspersky Security Center	✓ مجموعة ذات موقع واحد فقط	✓ بدءًا من الإصدار 16.2 لنظام التشغيل Linux من Kaspersky Security Center، أصبحت مجموعة تجاوز الفشل الموزعة جغرافيًا مدعومة.
وحدة تحكم الإدارة		

الميزة أو الملكية	Kaspersky Security Center	
	حل قائم على Windows	حل قائم على Linux
نوع وحدة تحكم الإدارة	المستند إلى MMC والمستند إلى الويب	على شبكة الإنترنت
نظام تشغيل لتثبيت وحدة الإدارة المستندة إلى الويب عليه	نظام التشغيل Windows أو Linux	Linux
سجل الدخول إلى وحدة التحكم باستخدام مصادقة المجال	✓	✓ تسجيل الدخول الأحادي غير مدعوم للإصدارات من 15.1 إلى 15.4 ضمنًا
إدارة أجهزة العملاء ومجموعات الإدارة		
العدد الأقصى للأجهزة المدارة (واحد لكل خادم إدارة)	000,100	000,50 (مع PostgreSQL وPostgres Pro)
استقصاء الشبكة	✓	✓ بدءًا من الإصدار 16، يتم دعم وحدتا تحكم المجال FreelPA وALD Pro
حماية الأجهزة المدارة التي تعمل بأنظمة Windows وmacOS وLinux	✓	✓
حماية الأجهزة المحمولة	✓ الإدارة الأساسية للأجهزة المحمولة	✓ إدارة الأجهزة المحمولة (MDM) واستخدام وظيفة Kaspersky Secure Mobility Management (بموجب ترخيص)
إدارة حماية الأجهزة الافتراضية	✓	✓
حماية البنية التحتية السحابية العامة	✓	—
الاتصال عن بُعد بسطح مكتب جهاز العميل	✓	✓ بدءًا من الإصدار 15.3
تشفير البيانات وحمايتها	✓	✓ على الأجهزة المدارة التي تعمل بنظام التشغيل Windows المُثبت عليها Endpoint Security for Windows أو Kaspersky Endpoint Security for Mac
دعم المجموعات ومصفوفات الخادم في مجموعات الإدارة	✓	✓
التسلسل الهرمي لمجموعة الإدارة	✓	✓
إضافة بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت للعمل كنقطة توزيع	✓ (وحدة تحكم الإدارة المستندة إلى MMC)	سيتم تنفيذه في 2026
التعامل مع المستخدمين		
إنشاء وإدارة حسابات المستخدمين	✓	✓
إدارة تطبيقات Kaspersky		
سياسات التطبيق	✓	✓
مهام تطبيقات Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
وكيل KSN	✓	✓
Kaspersky Private Security Network	✓	✓
النشر المركزي لمفاتيح الترخيص لتطبيقات Kaspersky	✓	✓
التشخيصات عن بُعد لأجهزة العميل	✓	✓
تحديث تطبيقات Kaspersky تلقائيًا	✓	✓
دعم مراقبة عيوب التكيف	✓	✓
إدارة أمان تتمحور حول الجهاز	✓	✓
إدارة الأمان تتمحور حول المستخدم	✓	✓
إدارة النظام		
نشر أنظمة التشغيل على الأجهزة العميلة	✓	—
إدارة تراخيص الطرف الثالث	✓	—

الميزة أو الملكية	Kaspersky Security Center	
	حل قائم على Windows	حل قائم على Linux
باستخدام خادم الإدارة كخادم WSUS	✓	✓ (وضع بحث Windows Update فقط)
إدارة تطبيقات الجهات الخارجية على أجهزة العميل		
تثبيت تحديثات برامج الطرف الثالث وإصلاح الثغرات الأمنية لبرامج الطرف الثالث	✓	✓
المراقبة وإعداد التقارير والتدقيق		
إدارة مراجعات الكائن	✓	✓
مقارنة مراجعات السياسة	✓	سيتم تنفيذه في 2026
عرض والتعامل مع التنبيهات المكتشفة بواسطة Kaspersky Endpoint Detection and Response Optimum	✓	✓
إشعارات عن الأحداث التي وقعت على الأجهزة المدارة	✓	✓
مراقبة حالة السياسات وحالة المهام	✓	✓
التكاملات		
التكامل مع Kaspersky Managed Detection and Response	✓	✓
التكامل مع أنظمة SIEM	✓	✓
تصدير الأحداث باستخدام تنسيقي CEF وLEEF	✓	✓
تجميع التنبيهات وتنفيذ إجراءات الاستجابة عبر Active directory وKASAP وKaspersky TIP Sandbox	—	✓ (بدءًا من الإصدار 15.4) يجب عليك تفعيل خادم الإدارة بموجب ترخيص Kaspersky Next XDR Optimum، ثم نشر مفتاح ترخيص Kaspersky Next XDR Optimum إلى تطبيقاتك المدارة

حول Kaspersky Security Center Cloud Console

يعني استخدام Kaspersky Security Center كتطبيق محلي أنك تقوم بتثبيت Kaspersky Security Center، بما في ذلك خادم الإدارة، على جهاز محلي وإدارة نظام أمان الشبكة من خلال وحدة تحكم الإدارة المستندة إلى Microsoft Management Console (متوفرة فقط في Kaspersky Security Center Windows) أو Kaspersky Security Center Web Console.

ومع ذلك، يمكنك استخدام Kaspersky Security Center كخدمة سحابية بدلاً من ذلك. في هذه الحالة، يتم تثبيت Kaspersky Security Center وصيانته من أجلك بواسطة خبراء Kaspersky في بيئة السحابة، ويمنحك Kaspersky إمكانية الوصول إلى خادم الإدارة كخدمة. يمكنك إدارة نظام أمان الشبكة من خلال وحدة تحكم الإدارة المستندة إلى السحابة والتي تسمى Kaspersky Security Center Cloud Console. تحتوي وحدة التحكم هذه على واجهة مشابهة لواجهة Kaspersky Security Center Web Console.

تتوفر واجهة ووثائق Kaspersky Security Center Cloud Console باللغات التالية:

- الإنجليزية
- الفرنسية
- الألمانية
- الإيطالية
- اليابانية
- البرتغالية (البرازيل)

- الروسية
- الصينية المبسطة
- الإسبانية
- الإسبانية (LATAM)
- الصينية التقليدية

يتوفر المزيد من المعلومات حول Kaspersky Security Center Cloud Console وميزاتها في وثائق Kaspersky Security Center Cloud Console وفي وثائق Kaspersky Endpoint Security for Business.

Kaspersky Security Center 15.1

يقدم هذا القسم معلومات حول تغيير Kaspersky Security Center 15.1.

قد تختلف المعلومات المقدمة في التعليمات عبر الإنترنت عن المعلومات المقدمة في المستندات التي يتم شحنها مع التطبيق؛ في هذه الحالة، تعتبر التعليمات عبر الإنترنت محدثة. يمكنك المتابعة إلى "التعليمات عبر الإنترنت" بالنقر فوق الروابط الموجودة في الواجهة أو بالنقر فوق رابط "التعليمات عبر الإنترنت" في المستندات. يمكن تحديث "التعليمات عبر الإنترنت" دون إشعار مسبق. يمكنك التبديل بين المساعدة عبر الإنترنت والمساعدة دون الاتصال بالإنترنت إذا لزم الأمر.

المفاهيم الأساسية

يوضح هذا القسم المفاهيم الأساسية ذات صلة Kaspersky Security Center.

خادم الإدارة

تتيح مكونات Kaspersky Security Center إدارة تطبيقات Kaspersky المُثبتة على أجهزة العملاء عن بُعد.

ستتم الإشارة إلى الأجهزة المثبت عليها مكون خادم الإدارة باسم خوادم الإدارة (كما يُشار إليها باسم الخوادم). يجب أن تكون خوادم الإدارة محمية، بما في ذلك الحماية الفعلية، وضد أي وصول غير مصرح به.

ويتم تثبيت خادم الإدارة على الجهاز كخدمة لها مجموعة السمات التالية:

- باستخدام الاسم "خادم إدارة Kaspersky Security Center".
- تعيين للبدء تلقائيًا عند بدء تشغيل نظام التشغيل
- من خلال استخدام حساب **النظام المحلي** أو حساب المستخدم المُحدد أثناء تثبيت خادم الإدارة.

ويقوم خادم الإدارة بالوظائف التالية:

- تخزين بنية مجموعات الإدارة
- تخزين معلومات حول تكوين الأجهزة العميلة.
- ترتيب المستودعات لحزم توزيع التطبيقات.
- تثبيت التطبيقات عن بُعد على الأجهزة العميلة وإزالة التطبيقات.
- تحديث قواعد بيانات التطبيقات والوحدات النمطية لبرامج تطبيقات Kaspersky
- إدارة السياسات والمهام على الأجهزة العميلة.
- تخزين معلومات حول الأحداث التي وقعت على الأجهزة العميلة.
- إنشاء تقارير حول تشغيل تطبيقات Kaspersky.

- نشر مفاتيح الترخيص على أجهزة العملاء، وتخزين معلومات حول مفاتيح الترخيص.
- إعادة توجيه الإخطارات حول تقدم المهام (مثل اكتشاف فيروس على جهاز عميل).

تسمية خوادم الإدارة في واجهة التطبيق

في واجهة وحدة تحكم الإدارة المستندة إلى MMC وKaspersky Security Center Web Console، يمكن أن تحمل خوادم الإدارة الأسماء التالية:

- اسم جهاز خادم الإدارة، على سبيل المثال: "اسم_الجهاز" أو "خادم الإدارة: اسم_الجهاز".
- عنوان IP لجهاز خادم الإدارة، على سبيل المثال: "IP_address" أو "خادم الإدارة: IP_address".
- تحتوي خوادم الإدارة الثانوية وخوادم الإدارة الافتراضية على أسماء مخصصة تحددها عند توصيل خادم إدارة افتراضي أو ثانوي بخادم الإدارة الرئيسي.
- إذا كنت تستخدم Kaspersky Security Center Web Console المثبت على جهاز Linux، سيعرض التطبيق أسماء خوادم الإدارة التي حددتها على أنها موثوقة في ملف الاستجابة.

يمكنك الاتصال بخادم الإدارة باستخدام وحدة تحكم الإدارة أو Kaspersky Security Center Web Console.

التسلسل الهرمي لخوادم الإدارة

يمكن ترتيب خوادم الإدارة في تسلسل هرمي. ويمكن أن يحتوي كل خادم إدارة على عدة خوادم إدارة تابع (يُشار إليها باسم خوادم تابعة) على مستويات تداخل مختلفة بالتسلسل الهرمي. مستوى التداخل للخوادم التابعة غير مُقيَّد. ثم ستتضمن مجموعات الإدارة الخاصة بخادم الإدارة الرئيسي الأجهزة العميلة الخاصة بجميع خوادم الإدارة الثانوية. وهكذا، يمكن إدارة الأقسام المنعزلة والمستقلة من الشبكات بواسطة خوادم إدارة مختلفة تتم إدارتها في المقابل بواسطة الخادم الرئيسي.

خوادم الإدارة الافتراضية حالة خاصة من خوادم الإدارة الثانوية.

يمكن استخدام التسلسل الهرمي لخوادم الإدارة للقيام بما يلي:

- تخفيف الحمل على خادم الإدارة (مقارنةً بخادم إدارة منفرد مثبت على الشبكة بالكامل).
- تخفيف حركة مرور الإنترانت وتبسيط التعامل مع المكاتب البعيدة. وليس من الضروري إنشاء اتصالات بين خادم الإدارة الرئيسي وجميع الأجهزة المتصلة بالشبكة، والتي قد توجد في مناطق أخرى على سبيل المثال. ويكفي تثبيت خادم إدارة تابع في كل قطاع شبكة، وتوزيع الأجهزة فيما بين مجموعات إدارة الخوادم التابعة، وإنشاء اتصالات بين الخوادم التابعة والخوادم الرئيسية عبر قنوات اتصال سريعة.
- توزيع المسؤوليات بين مسؤولي أمان مكافحة الفيروسات. جميع إمكانيات الإدارة المركزية ومراقبة حالة أمان مكافحة الفيروسات في شبكات الشركة تظل متوفرة.
- استخدم Kaspersky Security Center من قبل مزودي الخدمة. لا يحتاج موفر الخدمة إلا إلى تثبيت Kaspersky Security Center وKaspersky Security Center Web Console فقط. لإدارة عدد كبير من أجهزة العميل لمؤسسات مختلفة، يمكن لمزود الخدمة إضافة خوادم الإدارة الثانوية (بما في ذلك الخوادم الافتراضية) إلى التسلسل الهرمي لخوادم الإدارة.

ويمكن توصيل كل جهاز مُدرج في التسلسل الهرمي لمجموعات الإدارة بخادم إدارة واحد فقط. يجب عليك مراقبة اتصال الأجهزة بخوادم الإدارة بشكل مستقل. استخدم ميزة البحث عن جهاز في مجموعات إدارة الخوادم المختلفة حسب سمات الشبكة.

خادم الإدارة الافتراضي

خادم الإدارة الافتراضي (المشار إليه فيما يلي أيضًا باسم الخادم الافتراضي) هو أحد مكونات Kaspersky Security Center ومصمم لإدارة الحماية ضد الفيروسات لشبكة منظمة عميلة.

يُعد خادم الإدارة الافتراضي حالة خاصة من خادم الإدارة الثانوي ويشتمل على القيود التالية مقارنةً بخادم الإدارة الفعلي:

- لا يمكن إنشاء خادم إدارة افتراضي إلا على خادم إدارة أساسي.
- يستخدم خادم الإدارة الافتراضي قاعدة بيانات خادم الإدارة الرئيسية في تشغيله. مهام النسخ الاحتياطي للبيانات واستعادتها، بالإضافة إلى مهام البحث عن التحديثات والتنزيل، غير مدعومة على خادم الإدارة الافتراضي.
- لا يدعم خادم الإدارة الافتراضي إنشاء خوادم إدارة ثانوية (بما في ذلك الخوادم الافتراضية).

إضافة إلى ذلك، يشتمل خادم الإدارة الافتراضي على القيود التالية:

- يكون عدد الأقسام في نافذة خصائص خادم الإدارة الافتراضي محدودًا.
- لتثبيت تطبيقات Kaspersky عن بُعد على أجهزة العملاء المُدارة بواسطة خادم الإدارة الافتراضي، يجب عليك التأكد من تثبيت عميل الشبكة على أحد أجهزة العملاء للتأكد من وجود اتصال مع خادم الإدارة الافتراضي. في أول اتصال مع خادم الإدارة الافتراضي، يتم تعيين الجهاز كنقطة توزيع تلقائيًا، لذا فإنه يعمل كبوابة للاتصال بين الأجهزة العميلة وخادم الإدارة الافتراضي.
- يمكن للخادم الظاهري استقصاء الشبكة فقط من خلال نقاط التوزيع.
- لإعادة تشغيل خادم افتراضي به خلل، يعمل Kaspersky Security Center على إعادة تشغيل خادم الإدارة الرئيسي وجميع خوادم الإدارة الافتراضية.
- لا يمكن تعيين دور للمستخدمين الذين تم إنشاؤهم على خادم افتراضي على خادم الإدارة.

يكون لمسؤول خادم الإدارة الافتراضي جميع الامتيازات على هذا الخادم الافتراضي تحديدًا.

خادم الجهاز المحمول

إن خادم الأجهزة المحمولة هو مكون من مكونات Kaspersky Security Center والذي يوفر وصولاً إلى الأجهزة المحمولة ويسمح بإدارتها من خلال وحدة تحكم الإدارة. يقوم خادم الجهاز المحمول بتلقي معلومات حول الأجهزة المحمولة وتخزين ملفات التعريف الخاصة بها.

يتضمن Kaspersky Security Center خادم iOS MDM كخادم للأجهزة المحمولة. يتم استخدام خادم الأجهزة المحمولة لإدارة الأجهزة المحمولة التي تدعم خدمة Apple® Push Notification service (APNs).

تتيح لك خوادم الأجهزة المحمولة الخاصة بـ Kaspersky Security Center إدارة الكائنات التالية:

- جهاز محمول فردي.
- العديد من الأجهزة المحمولة.
- العديد من الأجهزة المحمولة المتصلة بمجموعة من الخوادم، في وقت واحد. بعد الاتصال بمجموعة من الخوادم، يتم عرض خادم الأجهزة المحمولة المثبتة في هذه المجموعة في وحدة تحكم الإدارة كخادم واحد.

خادم الويب

Web Server Kaspersky Security Center (المشار إليه فيما بعد بـ خادم الويب) هو مكون Kaspersky Security Center يتم تثبيته معًا مع خادم الإدارة. تم تصميم خادم الويب لنقل حزم التثبيت المستقلة وملفات تعريف iOS MDM وملفات من المجلد المشترك، عبر أحد الشبكات.

عند إنشاء حزمة تثبيت مستقلة، يتم نشرها تلقائيًا على خادم الويب. يتم عرض رابط تنزيل الحزمة المستقلة في قائمة حزم التثبيت المستقلة التي تم إنشاؤها. إذا لزم الأمر، فيمكنك إلغاء نشر الحزمة المستقلة أو يمكنك نشرها على خادم الويب مرة أخرى.

عند إنشاء ملف تعريف iOS MDM للجهاز المحمول الخاص بالمستخدم، فيتم نشره تلقائيًا على خادم الويب. يتم حذف ملف التعريف الذي تم نشره تلقائيًا من خادم الويب بمجرد تثبيته بنجاح على الجهاز المحمول الخاص بالمستخدم.

يتم استخدام المجلد المشترك لتخزين المعلومات المتوفرة لجميع المستخدمين الذين تتم إدارة الأجهزة الخاصة بهم من خلال خادم الإدارة. إذا كان المستخدم لا يمتلك وصولاً مباشرًا إلى المجلد المشترك، فيمكن تزويده بمعلومات من هذا المجلد باستخدام خادم الويب.

لتزويد المستخدمين بمعلومات من المجلد المشترك باستخدام خادم الويب، يجب أن يقوم المسؤول بإنشاء مجلد فرعي يُسمى "عام" في المجلد المشترك ولصق المعلومات ذات الصلة بداخله.

تكون بنية جملة رابط نقل المعلومات كما يلي:

```
<object>/public/<HTTPS port>:<Web Server name>//:https
```

حيث:

- `<Web Server name>` هو اسم Kaspersky Security Center Web Server.
- `<HTTPS port>` هو منفذ HTTPS لخادم الويب المحدد بواسطة المسؤول. يمكن تعيين منفذ HTTPS في القسم **خادم الويب** بنافذة خصائص خادم الإدارة. رقم المنفذ الافتراضي هو 8061.
- `<object>` هو المجلد الفرعي أو الملف الذي يُمنح المستخدم وصولاً إليه.

ويمكن للمسؤول إرسال الرابط الجديد إلى المستخدم بأي طريقة مناسبة: على سبيل المثال عبر البريد الإلكتروني.

وباستخدام على الرباط، يمكن للمستخدم تنزيل المعلومات المطلوبة على الجهاز المحلي.

عميل الشبكة

يتم التفاعل بين خادم الإدارة والأجهزة من خلال مكون عميل الشبكة التابع لـ Kaspersky Security Center. يجب تثبيت عميل الشبكة على جميع الأجهزة التي يُستخدم عليها Kaspersky Security Center لإدارة تطبيقات Kaspersky.

ويتم تثبيت عميل الشبكة على الجهاز كخدمة تتميز بمجموعة السمات التالية:

- باسم "عميل شبكة Kaspersky Security Center"
- تعيين للبدء تلقائيًا عند بدء تشغيل نظام التشغيل
- باستخدام حساب النظام المحلي

ويُطلق على الجهاز الذي لديه عميل شبكة مثبت به جهاز مُدار أو جهاز.

يمكنك تثبيت عميل الشبكة على جهاز يعمل بنظام التشغيل Windows أو Linux أو Mac. يمكنك الحصول على المكون من أحد المصادر التالية:

- حزمة التثبيت في وحدة تخزين خادم الإدارة (يجب أن يكون لديك خادم إدارة مثبتًا)
- حزمة التثبيت الموجودة على خوادم ويب Kaspersky

لا ينبغي عليك تثبيت عميل الشبكة على الجهاز الذي تقوم بتثبيت خادم الإدارة عليه، لأنه يتم تثبيت إصدار خادم عميل الشبكة تلقائيًا إلى جانب خادم الإدارة.

اسم العملية التي يبدأها عميل الشبكة هو klnagent.exe.

يقوم عميل الشبكة بمزامنة الجهاز المُدار من خلال خادم الإدارة. نوصي أن تقوم بتعيين فترة المزامنة (يُشار إليها أيضًا باسم heartbeat) إلى 15 دقيقة لكل 10 000 جهاز مُدار.

مجموعات الإدارة

إن مجموعة الإدارة (يُشار إليها فيما بعد أيضًا بـ المجموعة) هي مجموعة منطقية من الأجهزة المُدارة التي تم تجميعها على أساس ميزة معينة بغرض إدارة الأجهزة المجمعة كوحدة واحدة ضمن Kaspersky Security Center.

ويتم تكوين جميع الأجهزة المُدارة ضمن مجموعة الإدارة لتنفيذ الإجراءات التالية:

- استخدام نفس إعدادات التطبيق (التي يمكنك تحديدها في سياسات المجموعة).
- استخدم وضع تشغيل شائع لجميع التطبيقات من خلال إنشاء مهام جماعية بإعدادات محددة. تشتمل أمثلة مهام جماعية على إنشاء وتثبيت حزمة تثبيت عامة، وتحديث قواعد البيانات والوحدات النمطية للتطبيقات، وفحص الجهاز حسب الطلب، وتمكين الحماية في الوقت الحقيقي.

لا يمكن لجهاز مُدار أن ينتمي إلا لمجموعة إدارة واحدة فقط.

يمكنك إنشاء تسلسلات هرمية تتمتع بأية درجة من التداخل لخوادم الإدارة والمجموعات. يمكن أن يتضمن مستوى التسلسل الهرمي الفردي خوادم إدارة ثانوية وافتراضية ومجموعات وأجهزة مُدارة. يمكنك تحريك الأجهزة من مجموعة إلى أخرى من دون تحريكها فعليًا. على سبيل المثال، إذا تغير منصب الموظف في المؤسسة من منصب المحاسب إلى المُطوّر، فبإمكانك تحريك جهاز الموظف من مجموعة إدارة المحاسبين إلى مجموعة إدارة المُطوّرين. وبعد ذلك، سوف يتلقى الجهاز تلقائيًا إعدادات التطبيق اللازمة للمُطوّرين.

الجهاز المُدار

الجهاز المُدار هو جهاز يعمل بنظام Windows أو Linux أو macOS المثبت عليه عميل الشبكة، أو جهاز محمول مثبت عليه تطبيق أمان Kaspersky. يمكنك إدارة مثل هذه الأجهزة عن طريق إنشاء مهام وسياسات للتطبيقات المثبتة على هذه الأجهزة. يمكنك كذلك تلقي التقارير من الأجهزة المُدارة.

يمكنك جعل الجهاز المُدار غير المحمول يعمل كنقطة توزيع وكبوابة اتصال.

يمكن إدارة الجهاز بواسطة خادم إدارة واحد فقط. يمكن لخادم إدارة واحد إدارة ما يصل إلى 100 000 جهاز، بما في ذلك الأجهزة المحمولة.

جهاز غير مخصص

الجهاز غير المخصص هو جهاز موجود على الشبكة وهو لم يتم تضمينه في أية مجموعة إدارة. يمكنك تنفيذ بعض الإجراءات على الأجهزة غير المخصصة، على سبيل المثال، نقلها إلى مجموعات الإدارة أو تثبيت التطبيقات عليها.

عند اكتشاف جهاز جديد على شبكتك، يذهب هذا الجهاز إلى مجموعة **Unassigned devices**. يمكنك تكوين القواعد للأجهزة من أجل نقلها تلقائيًا إلى مجموعات الإدارة الأخرى بعد أن يتم اكتشاف الأجهزة.

محطة عمل المسؤول

محطة عمل المسؤول هي جهاز تم تثبيت وحدة تحكم الإدارة عليه أو تستخدمه لفتح Kaspersky Security Center Web Console. يمكن للمسؤولين استخدام هذه الأجهزة في الإدارة المركزية عن بُعد لتطبيقات Kaspersky المُثبتة على أجهزة العملاء.

بعد أن يتم تثبيت وحدة تحكم الإدارة على الجهاز الخاص بك، سيظهر الرمز الخاص بها، الذي يسمح لك ببدء تشغيل وحدة تحكم الإدارة. ابحث عنه في قائمة **بدء** > **البرامج** > **Kaspersky Security Center**.

ولا توجد قيود على عدد محطات عمل المسؤول. من أية محطة عمل مسؤول، يمكنك إدارة مجموعات الإدارة لعدة خوادم إدارة على الشبكة في وقت واحد. يمكنك توصيل محطة عمل المسؤول بخادم إدارة (فعلي أو ظاهري) بأي مستوى من التسلسل الهرمي.

ويمكنك تضمين محطة عمل المسؤول في مجموعة الإدارة كجهاز عميل.

وداخل مجموعات الإدارة لأي خادم إدارة، يمكن أن يعمل نفس الجهاز كعميل خادم إدارة أو خادم إدارة أو محطة عمل مسؤول.

مكون الإدارة الإضافي

تتم إدارة تطبيقات Kaspersky من خلال وحدة تحكم الإدارة باستخدام مكون مخصص يُطلق عليه اسم مكون الإدارة الإضافي. كل تطبيق من تطبيقات Kaspersky التي يمكن إدارتها من خلال Kaspersky Security Center يشمل مكون الإدارة الإضافي.

وباستخدام مكون الإدارة الإضافي للتطبيق، يمكنك القيام بالإجراءات التالية في وحدة تحكم الإدارة:

- إنشاء وتحرير سياسات التطبيقات وإعداداتها، بالإضافة إلى إعدادات مهام التطبيقات.
- الحصول على معلومات حول مهام التطبيقات، وأحداث التطبيقات، بالإضافة إلى إحصاءات تشغيل التطبيق المُستلمة من الأجهزة العميلة.

يمكنك تنزيل المكونات الإضافية للإدارة من صفحة الدعم الفني لـ Kaspersky.

مكون الإدارة الإضافي للويب

يُستخدم مكون خاص—مكون الإدارة الإضافي للويب—لإدارة برنامج Kasperskyعن بُعد من خلال Kaspersky Security Center Web Console. مكون الإدارة الإضافي للويب يُشار إليه هنا فيما بعد باسم مكون الإدارة الإضافي. مكون الإدارة الإضافي هو واجهة بين Kaspersky Security Center Web Console وتطبيق Kaspersky محدد. باستخدام مكون الإدارة الإضافي، يمكنك تكوين المهمات والسياسات المخصصة للتطبيق.

يمكنك تنزيل المكونات الإضافية للإدارة على الويب من موقع Kaspersky الإلكتروني.

يوفر مكون الإدارة الإضافي ما يلي:

- واجهة لإنشاء وتحرير مهمات التطبيقات وإعداداتها
- واجهة لإنشاء وتحرير السياسات وملفات تعريف السياسة للتحكم عن بُعد والتكوين المركزي لتطبيقات Kaspersky والأجهزة.
- يتم إنشاء نقل الأحداث عن طريق التطبيقات
- وظائف Kaspersky Security Center Web Console لعرض البيانات التشغيلية وأحداث التطبيقات والإحصائيات المنقولة من الأجهزة العملية

السياسات

السياسة هي مجموعة من إعدادات تطبيقات Kaspersky التي تنطبق على مجموعة إدارة ومجموعاتها الفرعية. يمكنك تثبيت عدة تطبيقات Kaspersky على أجهزة مجموعة إدارة. Kaspersky Security Center يوفر سياسة واحدة لكل تطبيق من تطبيقات Kaspersky في مجموعة الإدارة. السياسة لها إحدى الحالات التالية (انظر الجدول أدناه):

حالة السياسة

الحالة	الوصف
نشطة	السياسة الحالية المطبقة على الجهاز. يمكن أن تكون سياسة واحدة نشطة لتطبيق Kaspersky في كل مجموعة إدارة. الأجهزة تطبق قيم الإعدادات لسياسة نشطة لتطبيق Kaspersky.
غير نشطة	سياسة غير مطبقة حاليا على جهاز.
خارج المكتب	إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.

تعمل السياسات وفق القواعد التالية:

- يمكن تكوين عدة سياسات بقيم مختلفة لتطبيق واحد.
- يمكن تفعيل سياسة واحدة فقط للتطبيق الحالي.
- يمكنك تفعيل سياسة غير نشطة عند وقوع حدث معين. ويعني ذلك، على سبيل المثال، أنه يمكنك تنفيذ إعدادات مكافحة الفيروسات الأكثر صرامة أثناء انتشار الفيروسات.
- يمكن أن يكون للسياسة سياسات فرعية.

بشكل عام، يمكنك استخدام السياسات كاستعدادات لحالات الطوارئ، مثل هجمات الفيروسات. على سبيل المثال: في حال وجود هجمة عبر محركات الفلاش، يمكنك تنشيط سياسة تحجب الوصول إلى محركات أقراص الفلاش. في هذه الحالة، تصير السياسة المفعلة الحالية غير نشطة تلقائيًا.

من أجل منع الاحتفاظ بسياسات متعددة (على سبيل المثال عندما تفترض مناسبات مختلفة تغيير عدة إعدادات فقط)، يمكنك استخدام ملفات تعريف السياسة.

ملف السياسة التعريفي عبارة عن مجموعة فرعية من قيم إعدادات السياسة لها اسم، والتي تحل محل قيم إعدادات السياسة. ملف تعريف السياسة يؤثر على فاعلية تكوين الإعدادات على جهاز مُدار. الإعدادات الفعالة هي مجموعة من إعدادات السياسة وإعدادات ملفات تعريف السياسة وإعدادات التطبيق المحلية المطبقة حاليا للجهاز.

تعمل ملفات التعريفية للسياسة وفقًا للقواعد التالية:

- يسري ملف السياسة التعريفي عند حدوث حالة تفعيل معينة.
- ملفات تعريف السياسة تحتوي على قيم الإعدادات التي تختلف من إعدادات السياسة.
- تنشيط ملف تعريف السياسة يغير الإعدادات الفعالة للجهاز المُدار.
- يمكن أن تتضمن سياسة ما على 100 ملف تعريف سياسة بحد أقصى.

ملفات تعريف السياسة

قد يكون من الضروري في بعض الأحيان إنشاء مثيلات متعددة لسياسة واحدة مخصصة لمجموعات إدارة مختلفة؛ قد ترغب كذلك في تعديل إعدادات تلك السياسات على نحوٍ مركزي. يمكن لهذه المثيلات الاختلاف وفقًا لإعداد واحد أو إعدادين فقط. على سبيل المثال، يعمل جميع المحاسبين في مؤسسة ما ويخضعون لنفس السياسة—ولكن كبار المحاسبين مسموح لهم باستخدام محركات الفلاش، بينما هذا الأمر ليس مسموح به للمحاسبين حديثي الخبرة. في هذه الحالة، قد يكون تطبيق السياسات على الأجهزة فقط من خلال الترتيب الهرمي لمجموعات الإدارة غير ملائم.

لمساعدتك على تجنب إنشاء مثيلات عديدة لسياسة واحدة، يتيح لك Kaspersky Security Center إنشاء ملفات تعريف السياسة. إن ملفات تعريف السياسة تعد ضرورية إذا كنت تريد تشغيل الأجهزة الموجودة ضمن مجموعة إدارة واحدة بموجب إعدادات سياسة مختلفة.

ملف تعريف السياسة هو مجموعة فرعية مسمّاة لإعدادات السياسة. يتم توزيع هذه المجموعة الفرعية على الأجهزة المستهدفة بالإضافة إلى السياسة، وتلحقها في حالة خاصة تُسمى شرط تفعيل ملف التعريف. تحتوي ملفات التعريف فقط على الإعدادات التي تختلف عن السياسة "الأساسية"، والتي تكون نشطة على الجهاز المُدار. يؤدي تنشيط ملف التعريف إلى تعديل إعدادات السياسة "الأساسية" التي كانت نشطة في البداية على الجهاز. تأخذ الإعدادات المعدلة القيم التي تم تحديدها في ملف التعريف.

المهام

يقوم Kaspersky Security Center بإدارة تطبيقات Kaspersky security المثبتة على الأجهزة عن طريق إنشاء المهام وتشغيلها. يلزم وجود المهام من أجل تثبيت التطبيقات، وبدء تشغيلها، وإيقافها، وفحص الملفات، وتحديث قواعد البيانات والوحدات النمطية للبرامج، واتخاذ إجراءات أخرى بشأن التطبيقات.

يمكن إنشاء مهام لتطبيق محدد فقط في حالة تثبيت مكونات الإدارة لهذا التطبيق.

يمكن إجراء المهام على خادم الإدارة وعلى الأجهزة.

يتم إجراء المهام التالية على خادم الإدارة:

- التوزيع التلقائي للتقارير
- تنزيل التحديثات إلى مستودع خادم الإدارة
- النسخ الاحتياطي لبيانات خادم الإدارة
- صيانة قاعدة البيانات
- مزامنة Windows Update
- إنشاء حزمة تثبيت بناءً على صورة نظام التشغيل (OS) للجهاز المرجعي

يتم إجراء أنواع المهام التالية على الأجهزة:

- المهام المحلية—هي المهام التي يتم إجراؤها على جهاز محدد

  يمكن تعديل المهام المحلية إما بواسطة المسؤول باستخدام أدوات وحدة تحكم الإدارة أو بواسطة مستخدم جهاز بعيد (على سبيل المثال، عبر واجهة تطبيق الأمان). في حالة تعديل مهمة محلية بواسطة المسؤول ومستخدم الجهاز المُدار في الوقت نفسه، فستسري التغييرات التي يقوم بها المسؤول حيث أنه يملك أولوية أعلى.

- المهام الجماعية—هي المهام التي يتم إجرائها على كافة الأجهزة الخاصة بمجموعة محددة

  ما لم يتم تحديد خلاف ذلك في خصائص المهمة، تؤثر أيضًا المهمة الجماعية على كافة المجموعات الفرعية الخاصة بالمجموعة المحددة. كما تؤثر المهام الجماعية (بشكل اختياري) على الأجهزة المتصلة بخوادم الإدارة الثانوية والافتراضية التي تم نشرها في هذه المجموعة أو أيٍ من مجموعاتها الفرعية.

- المهام العالمية—هي المهام التي تنفذ على مجموعة من الأجهزة محددة بصرف النظر عما إذا كانت مضمنة في أية مجموعة إدارة أم لا

يمكنك إنشاء أي عدد من المهام الجماعية أو المهام العالمية أو المهام المحلية، وذلك لكل تطبيق.

ويمكنك إجراء تغييرات على إعدادات المهام، وعرض مستوى تقدمها، ونسخها، وتصديرها، واستيرادها، وحذفها.

لا يتم بدء تشغيل المهمة على جهاز إلا إذا كان التطبيق الذي تم إنشاء المهمة له قيد التشغيل.

يتم حفظ نتائج المهام في سجل أحداث Microsoft Windows وسجل أحداث Kaspersky Security Center، بشكل مركزي على حد سواء على خادم الإدارة ومحليًا على كل جهاز.

لا تقم بتضمين بيانات خاصة في إعدادات المهمة. على سبيل المثال، تجنّب تخصيص كلمة مرور مسؤول المجال.

نطاق المهمة

نطاق المهمة هو مجموعة الأجهزة التي يتم تنفيذ المهمة عليها. أنواع النطاق هي التالية:

- لتنفيذ مهمة في الجهاز، يكون الجهاز نفسه هو النطاق.
- لتنفيذ مهمة في خادم الإدارة، يكون خادم الإدارة هو النطاق.
- لتنفيذ مهمة جماعية، تكون قائمة الأجهزة المشمولة في المجموعة هي النطاق.

عند إنشاء مهمة شاملة، يمكنك استخدام الوسائل التالية لتحديد نطاقها:

- تحديد أجهزة معينة يدويًا.

  يمكنك استخدام عنوان IP (أو نطاق IP)، أو اسم NetBIOS أو اسم DNS كعنوان الجهاز.

- استيراد قائمة بالأجهزة من ملف TXT يحتوي على عناوين الأجهزة المراد إضافتها (يجب وضع كل عنوان في سطر منفرد).

  إذا قمت باستيراد قائمة بالأجهزة من ملف أو قمت بإنشاء قائمة يدويًا، وإذا تم تحديد الأجهزة بأسمائها، فيمكن فقط أن تحتوي القائمة على الأجهزة التي تم إدخال معلوماتها في قاعدة بيانات خادم الإدارة. علاوة على ذلك، لا بد أن المعلومات قد تم إدخالها عند اتصال هذه الأجهزة أو أثناء اكتشاف الأجهزة.

- تعيين تحديد جهاز.

  بمرور الوقت، يتغير نطاق المهمة بتغير مجموعة الأجهزة المضمنة في التحديد. يمكن القيام بتحديد أجهزة على أساس سمات الجهاز، بما في ذلك البرنامج المثبت على جهاز ما، وعلى أساس العلامات المعيّنة إلى الأجهزة. تحديد الجهاز هو الطريقة الأكثر مرونة لتحديد نطاق مهمة ما.

  تعمل المهام المخصصة لتحديدات الأجهزة دائمًا وفق جدول بواسطة خادم الإدارة. لا يمكن أن تعمل هذه المهام على أجهزة غير متصلة بخادم الإدارة. إن المهام التي تم تحديد نطاقها باستخدام وسائل أخرى يتم تنفيذها مباشرةً على الأجهزة ولذلك لا تعتمد على اتصال الجهاز بخادم الإدارة.

  لا يتم تنفيذ المهام المخصصة لتحديدات الجهاز في الوقت المحلي لجهاز ما؛ وبدلاً من ذلك، يتم تنفيذها في الوقت المحلي لخادم الإدارة. إن المهام التي تم تحديد نطاقها باستخدام وسائل أخرى يتم تنفيذها في الوقت المحلي لجهاز ما.

كيفية ارتباط إعدادات التطبيق المحلية بالسياسات

يمكنك استخدام السياسات لتعيين القيم المماثلة لإعدادات التطبيق بجميع الأجهزة الموجودة بالمجموعة.

يمكن إعادة تحديد قيم الإعدادات المحددة بواسطة سياسة الأجهزة المنفردة في إحدى المجموعات باستخدام إعدادات التطبيق المحلية. يمكنك فقط تعيين قيم الإعدادات التي تسمح السياسة بتعديلها، أي الإعدادات غير المقفلة.

يتم تحديد قيمة إعداد يستخدمها التطبيق على جهاز عميل بواسطة موضع القفل (🔒) لهذا الإعداد في السياسة:

- في حالة قفل تعديل الإعداد، تُستخدم نفس القيمة (المحددة في السياسة) على جميع الأجهزة العميلة.
- وفي حالة عدم تأمين تعديل إعداد، فإن التطبيق يستخدم قيمة الإعداد المحلية على كل جهاز عميل بدلاً من القيمة المحددة في السياسة. ويمكن بعدها تغيير الإعداد في إعدادات التطبيق المحلية.

هذا يعني أنه عند تشغيل المهمة على جهاز عميل، يقوم التطبيق بتطبيق الإعدادات المحددة بطريقتين مختلفتين:

- بواسطة إعدادات المهمة وإعدادات التطبيق المحلية إذا كان الإعداد غير مؤمَّن ضد التغييرات في السياسة.
- بواسطة سياسة المجموعة إذا كان الإعداد مؤمَّنًا ضد التغييرات

يتم تغيير إعدادات التطبيق المحلية بعد تطبيق السياسة أولاً وفقًا لإعدادات السياسة.

نقطة توزيع

نقطة توزيع (كانت تُعرَف فيما سبق بوكيل التحديث) هي جهاز مثبت عليه عميل الشبكة يتم استخدامه لتوزيع التحديثات، وتثبيت التطبيقات عن بُعد، واسترداد معلومات حول الأجهزة المتصلة بالشبكة. تعمل نقاط التوزيع على تسريع توزيع التحديثات وتحرير مساحة موارد خادم الإدارة.

تختلف ميزات وحالات استخدام عميل الشبكة المثبت على جهاز يُستخدم كنقطة توزيع حسب نظام التشغيل.

يمكن لنقطة التوزيع إجراء الوظائف التالية:

- وزع الملفات المستلمة من خادم الإدارة إلى أجهزة العميل داخل المجموعة (بما في ذلك التوزيع من خلال البث المتعدد باستخدام UDP).

  تتضمن قائمة الملفات التي يمكن نقلها عن طريق نقاط التوزيع ما يلي:

  - تحديثات قواعد بيانات Kaspersky والوحدات النمطية للبرنامج
  - تحديثات برامج الجهات الخارجية
  - حزم التثبيت
  - تحديثات Windows عندما تستخدم خادم الإدارة كخادم WSUS

  يمكن تلقي التحديثات سواء من خادم الإدارة أو من خوادم تحديث Kaspersky. في الحالة الأخيرة، يجب إنشاء مهمة تحديث لنقطة التوزيع. لا يمكن لأجهزة نقاط التوزيع التي تعمل بنظام macOS تنزيل التحديثات من خوادم تحديث Kaspersky.

  في حالة وجود جهاز أو أكثر من الأجهزة التي تعمل بنظام macOS داخل نطاق مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع ، تكون المهمة مكتملة مع إظهار حالة فشل ، حتى إذا تم إكمالها بنجاح على جميع أجهزة Windows.

  عندما تكون جميع نقاط التوزيع المخصصة للجهاز معطلة، فلن يتمكن الجهاز من تلقي التحديثات (قواعد بيانات مكافحة الفيروسات والتصحيحات وحزم التثبيت.

- توزيع سياسات المجموعة ومهامها من خلال الإرسال المتعدد باستخدام UDP.
- تعمل كبوابة اتصال إلى خادم الإدارة للأجهزة المتواجدة في مجموعة الإدارة.

  إذا تعذر إنشاء اتصال مباشر بين الأجهزة المدارة في المجموعة وخادم الإدارة، يمكن استخدام نقطة التوزيع كبوابة اتصال إلى خادم الإدارة لهذه المجموعة. في هذه الحالة، سوف يتم توصيل الأجهزة المدارة إلى بوابة الاتصال، التي بدورها، سوف يتم توصيلها بخادم الإدارة.

  وجود نقطة توزيع تعمل كبوابة اتصال لا يحجب خيار الاتصال المباشر بين الأجهزة المدارة وخادم الإدارة. إذا لم تتوافر بوابة الاتصال، ولكن هناك إمكانية تقنية للاتصال المباشر مع خادم الإدارة، فسيتم توصيل الأجهزة المدارة بخادم الإدارة مباشرة.

- قم باستقصاء الشبكة لاكتشاف الأجهزة الجديدة وتحديث المعلومات حول الأجهزة الموجودة بالفعل. يمكن لنقطة التوزيع تطبيق نفس وسائل اكتشاف الأجهزة كخادم الإدارة.

- قم بإجراء التثبيت عن بُعد لبرامج الجهات الخارجية وتطبيقات Kaspersky باستخدام أدوات نظام تشغيل نقطة التوزيع. لاحظ أن نقطة التوزيع يمكنها إجراء التثبيت على أجهزة العميل بدون عميل الشبكة.

  تتيح هذه الميزة نقل حزم تثبيت عميل الشبكة عن بُعد إلى الأجهزة العميلة التي توجد في الشبكات التي يتعذر على خادم الإدارة الوصول إليها.

- العمل كخادم وكيل مشارك في Kaspersky Security Network (KSN).

  يمكنك تمكين الخادم الوكيل لشبكة KSN على جانب نقطة التوزيع لجعل الجهاز يعمل كخادم وكيل لشبكة KSN. في هذه الحالة، يتم تشغيل خدمة وكيل (ksnproxy) على الجهاز.

يتم نقل الملفات من خادم الإدارة إلى نقطة توزيع عبر HTTP أو عبر HTTPS، إذا ما كان اتصال SSL ممكّنا. يتم استخدام نتائج HTTP أو HTTPS في مستوى الأداء الأعلى، بالمقارنة بـ SOAP، من خلال قطع حركة المرور.

يمكن تعيين الأجهزة المثبت عليها عميل الشبكة لتعمل كنقاط توزيع سواء يدويًا (بواسطة المسؤول)، أو تلقائيًا (بواسطة خادم الإدارة). يتم عرض قائمة نقاط التوزيع بأكملها لمجموعات إدارة محددة في تقرير حول قائمة نقاط التوزيع.

نطاق نقطة توزيع هو مجموعة الإدارة التي تم تعيينها إليها بواسطة المسؤول، وكذلك مجموعاتها الفرعية لجميع مستويات التضمين. إذا تم تعيين العديد من نقاط التوزيع في التسلسل الهرمي لمجموعات الإدارة، فسيتصل عميل الشبكة في الجهاز المدار بنقطة التوزيع الأقرب في التسلسل الهرمي.

يمكن أيضًا أن يكون موقع الشبكة نطاق نقاط التوزيع. يتم استخدام موقع الشبكة في الإنشاء اليدوي لمجموعة الأجهزة التي ستقوم نقطة التوزيع بتوزيع التحديثات عليها. يمكن تحديد موقع الشبكة للأجهزة التي تعمل بنظام تشغيل Windows فقط.

إذا تم تعيين نقاط التوزيع تلقائيًا بواسطة خادم الإدارة، فيتم تعيينهم حسب مجالات البث، وليس بحسب مجموعات الإدارة. يحث ذلك إذا كانت كل مجالات البث معروفة. يتبادل عميل الشبكة الرسائل مع عملاء الشبكة الآخرين في نفس الشبكة الفرعية ثم يرسل معلومات حوله وحول غيره من عملاء الشبكة إلى خادم الإدارة. بإمكان خادم الإدارة استخدام هذه المعلومات لتجميع وكلاء التحديث حسب مجالات البث. تكون مجالات البث معروفة لخادم الإدارة عقب إجراء استقصاء لأكثر من 70% من وكلاء التحديث في مجموعات الإدارة. يقوم خادم الإدارة باستقصاء مجالات البث كل ساعتين. بعد تعيين نقاط التوزيع حسب مجالات البث، فلا يمكن إعادة تعيينها حسب مجموعات الإدارة.

إذا قام المسؤول بتعيين نقاط التوزيع يدويًا، فيمكن تعيينها إلى مجموعات الإدارة أو مواقع الشبكة.

لا يشارك وكلاء التحديث ذوي ملف تعريف اتصال فعال في اكتشاف مجال البث.

يعين Kaspersky Security Center لكل عميل شبكة عنوان IP للإرسال المتعدد فريد من نوعه يختلف عن كل عنوان أخر. يتيح لك ذلك تجنب الحمل الزائد على الشبكة الذي يمكن أن يحدث نظرًا إلى تراكب IP.

إذا تم تعيين أثنين أو أكثر من نقاط التوزيع إلى منطقة شبكة واحدة أو إلى مجموعة إدارة واحدة، فستصبح أحداهما نقطة التوزيع المفعلة، وستصبح الباقية نقاط التوزيع في وضع الاستعداد. تقوم نقطة التوزيع المفعلة بتنزيل التحديثات وحزم التثبيت مباشرة من خادم الإدارة، بينما تقوم نقاط التوزيع في وضع الاستعداد بتلقي التحديثات من نقطة التوزيع المفعلة فقط. في هذه الحالة، يتم تنزيل الملفات من خادم الإدارة لمرة واحدة ثم يتم توزيعهم بين نقاط التوزيع. إذا أصبحت نقطة التوزيع المفعلة غير متوفرة لأي سبب، فستصبح إحدى نقاط التوزيع في وضع الاستعداد نشطةً. يقوم خادم الإدارة بتعيين نقطة توزيع للعمل في وضع الاستعداد تلقائيًا.

تظهر حالة نقطة التوزيع (نشطة / في وضع الاستعداد) مع خانة اختيار في التقرير klnagchk.

تتطلب نقطة التوزيع توفر 4 جيجابايت على الأقل كمساحة خالية على القرص. إذا كانت مساحة القرص الخالية لنقطة التوزيع أقل من 2 جيجابايت، يقوم Kaspersky Security Center بإنشاء مشكلة أمان بمستوى الأهمية تحذير. سيتم نشر مشكلة الأمان في خصائص الجهاز، في قسم **Security issues**.

يتطلب تشغيل مهام التثبيت عن بُعد على جهاز المعيّن كنقطة توزيع مساحة خالية إضافية على القرص. يجب أن تتجاوز مساحة القرص الفارغة الحجم الإجمالي لجميع حزم التثبيت التي سيتم تثبيتها.

يتطلب تشغيل أي من مهام التحديث (التصحيح) ومهام إصلاح الثغرات الأمنية على جهاز المعيّن كنقطة توزيع وجود مساحة خالية إضافية على القرص. يجب أن تكون مساحة القرص الفارغة على الأقل ضعف الحجم الإجمالي لجميع التصحيحات التي سيتم تثبيتها.

يجب أن تكون الأجهزة التي تعمل كنقاط توزيع محمية، بما في ذلك الحماية الفعلية، وضد أي وصول غير مصرح به.

بوابة الاتصال

بوابة الاتصال هي عميل شبكة يعمل في وضع خاص. تقبل بوابة الاتصال الاتصالات من عملاء الشبكة الآخرين وتقوم بنقلها إلى خادم الإدارة من خلال اتصالها الخاص بالخادم. على عكس عميل الشبكة العادي، تنتظر بوابة الاتصال الاتصالات من خادم الإدارة بدلاً من إنشاء اتصالات بخادم الإدارة.

يمكن لبوابة الاتصال تلقي اتصالات ما يصل إلى 10 000 جهاز.

لديك خياران عند استخدام بوابات الاتصال:

- نوصي بتثبيت بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ). بالنسبة لوكلاء الشبكة الآخرين المثبتين على أجهزة موجودة خارج المكتب، أنت بحاجة إلى تكوين اتصال بخادم الإدارة بشكل خاص من خلال بوابة الاتصال.

  لا تقوم بوابة الاتصال بتعديل البيانات إرسالها من وكلاء الشبكة إلى خادم الإدارة أو معالجتها بأي شكل من الأشكال. بالإضافة إلى ذلك، لا تسجل هذه البيانات في أي مخزن مؤقت وبالتالي لا يمكنها قبول البيانات من عميل الشبكة وإعادة توجيهها لاحقًا إلى خادم الإدارة. إذا حاول عميل الشبكة الاتصال بخادم الإدارة من خلال بوابة الاتصال، ولكن بوابة الاتصال لا يمكنها الاتصال بخادم الإدارة، فإن عميل الشبكة يدرك ذلك بأن خادم الإدارة لا يمكن الوصول إليه. تظل جميع البيانات موجودة على عميل الشبكة (وليس على بوابة الاتصال).

  لا يمكن لبوابة الاتصال أن تتصل بخادم الإدارة من خلال بوابة اتصال أخرى. وهذا يعني أن عميل الشبكة لا يمكن أن يعمل كبوابة اتصال بشكل متزامن ويستخدم بوابة اتصال ليتصل بخادم الإدارة.

  يتم إدراج جميع بوابات الاتصال في قائمة نقاط التوزيع الموجودة في خصائص خادم الإدارة.

- يمكنك أيضًا استخدام بوابات الاتصال داخل نطاق الشبكة. على سبيل المثال، تصبح أيضًا نقاط التوزيع المعينة تلقائيًا بوابات اتصال داخل النطاق الخاص بها. لا تعد بوابات الاتصال التي تقع، ضمن نطاق الشبكة الداخلية، ذو فائدة معتبرة. فهي تحد من عدد اتصالات الشبكة التي يتلقاها خادم الإدارة، ولكنها لا تقلل من حجم البيانات الواردة. حتى دون توفر بوابات الاتصال، ما يزال بإمكان جميع الأجهزة الاتصال بخادم الإدارة.

سيناريو التثبيت الرئيسي

عند اتباع هذا السيناريو، يمكنك نشر خادم الإدارة بالإضافة إلى تثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة المتصلة بالشبكة. يمكنك استخدام هذا السيناريو للحصول لإلقاء نظرة فاحصة على التطبيق ولتثبيت التطبيقات للعمل في المستقبل.

يتألف تثبيت Kaspersky Security Center من الخطوات التالية:

1. عمل تحضيري
2. تثبيت Kaspersky Security Center وتطبيق الأمان من Kaspersky على جهاز خادم الإدارة
3. النشر المركزي لتطبيقات الأمان من Kaspersky على أجهزة العملاء

تم وصف نشر Kaspersky Security Center في البيئات السحابية و نشر Kaspersky Security Center لموفري الخدمات" في أقسام المساعدة الأخرى.

نوصي بتعيين ساعة واحدة على الأقل لتثبيت خادم الإدارة، ويوم عمل واحد على الأقل لإكمال السيناريو. كما نوصي بتثبيت تطبيق الأمان، مثل Kaspersky Security for Windows Server أو Kaspersky Endpoint Security على الجهاز الذي سيعمل بوصفه خادم إدارة Kaspersky Security Center.

عند إكمال السيناريو، سيتم نشر الحماية في شبكة المؤسسة بالطريقة التالية:

- سيتم تثبيت DBMS لخادم الإدارة.
- سيتم تثبيت خادم إدارة Kaspersky Security Center.

- سيتم إنشاء جميع السياسات والمهام المطلوبة؛ وسيتم تحديد الإعدادات الافتراضية للسياسات والمهام.
- سيتم تثبيت تطبيقات الأمان (على سبيل المثال Kaspersky Endpoint Security for Windows) وعميل الشبكة على الأجهزة المُدارة.
- سيتم إنشاء مجموعات الإدارة (من المحتمل أن تكون مُجمَّعة في تسلسل هرمي).
- سيتم نشر حماية الأجهزة المحمولة، عند الضرورة.
- يتم تعيين نقاط التوزيع عند اللزوم.

يتم تثبيت Kaspersky Security Center من خلال المراحل التالية:

عمل تحضيري

1. **الحصول على الملفات المهمة**

تأكد من توفر مفتاح ترخيص (رمز تنشيط) برنامج Kaspersky Security Center أو مفاتيح ترخيص (رموز تنشيط) تطبيقات الأمان من Kaspersky.

فك ضغط الأرشيف الذي استلمته من البائع. يحتوي هذا الأرشيف على مفاتيح الترخيص (ملفات المفتاح)، رموز التنشيط، وقائمة تطبيقات Kaspersky التي يمكن تفعيلها بواسطة كل مفتاح ترخيص.

إذا كنت تريد تجربة برنامج Kaspersky Security Center أولاً، فيمكنك الحصول على نسخة تجريبية مجانية لمدة 30 يومًا على موقع ويب Kaspersky.

للحصول على معلومات مفصلة حول ترخيص الأمان الخاص بـ Kaspersky غير المضمنة في برنامج Kaspersky Security Center، يمكنك الرجوع إلى وثائق تلك التطبيقات.

2. **تحديد هيكل لحماية المؤسسة**

تعرف على المزيد حول مكونات Kaspersky Security Center. حدد هيكل الحماية وتكوين الشبكة الأنسب لمؤسستك. وبناءً على تكوين الشبكة ومعدل نقل قنوات الاتصال، حدد عدد خوادم الإدارة التي ستُستخدم وكيفية توزيعها على مكاتبك إذا كنت تقوم بتشغيل شبكة موزّعة.

للحصول على أداء مثالي والحفاظ عليه تحت ظروف التشغيل المختلفة، يرجى مراعاة عدد الأجهزة المتصلة بالشبكة ومخطط الشبكة ومجموعة ميزات Kaspersky Security Center التي تطلبها (لمزيد من التفاصيل، يرجى الرجوع إلى دليل قياس Kaspersky Security Center).

حدد ما إذا كان سيتم استخدام التسلسل الهرمي لخوادم الإدارة في مؤسستك أم لا. للقيام بذلك، يجب عليك تقييم ما إذا كان من الممكن ومن الملائم تغطية جميع الأجهزة العميلة التي تحتوي على خادم إدارة واحد أو كان من الضروري إنشاء تسلسل هرمي لخوادم الإدارة. قد يتعين عليك أيضًا إنشاء تسلسل هرمي لخوادم الإدارة مطابق للهيكل التنظيمي للمؤسسة التي تريد حماية شبكتها.

إذا كان من الضروري ضمان حماية الأجهزة المحمولة، قم بتنفيذ جميع الإجراءات الأساسية المطلوبة لتكوين خادم iOS MDM.

تأكد أن جميع الأجهزة التي حددتها كخوادم إدارة، بالإضافة إلى الأجهزة المحددة لتثبيت وحدة تحكم الإدارة، مستوفية لجميع متطلبات الأجهزة والبرامج.

3. **التحضير لاستخدام الشهادات المخصصة**

إذا كانت البنية التحتية للمفتاح العام (PKI) لمؤسستك تتطلب منك استخدام شهادات مخصصة صادرة عن الجهة المحددة المعتمدة (CA)، فقم بإعداد هذه الشهادات وتأكد من أنها تفي بجميع المتطلبات.

4. **التحضير لتثبيت ترخيص Kaspersky Security Center**

إذا كنت تخطط لاستخدام إصدار Kaspersky Security Center المزود بإدارة جهاز المحمول، و/أو المتكامل مع أنظمة SIEM، و/المزود بإدارة الثغرات الأمنية والتصحيحات، فتأكد من أن لديك ملف مفتاح أو رمز تنشيط لترخيص التطبيق.

5. **التحضير لتثبيت ترخيص تطبيقات الأمان المُدارة**

أثناء نشر الحماية، يتعين عليك تزويد Kaspersky Security Center بمفاتيح الترخيص المفعلة للتطبيقات التي تنوي إدارتها من خلال Kaspersky Security Center (راجع قائمة تطبيقات الأمان القابلة للإدارة). للحصول على مزيد من التفاصيل حول ترخيص أي تطبيق أمان، يمكنك الرجوع إلى وثائق هذا التطبيق.

6 **تحديد تكوين الجهاز لخادم الإدارة ونظام إدارة قواعد البيانات.**

خطط لتكوين الجهاز لنظام إدارة قواعد البيانات وخادم الإدارة، مع أخذ عدد الأجهزة في شبكتك في الاعتبار.

7 **تحديد نظام إدارة قواعد البيانات**

عند تحديد نظام إدارة قواعد البيانات (DBMS)، ضع في اعتبارك عدد الأجهزة المدارة التي ستتم تغطيتها بواسطة خادم الإدارة هذا. إذا كانت شبكتك تشمل أقل من 10 000 جهاز ولا تخطط لزيادة هذا العدد، يمكنك اختيار نظام مجاني لإدارة قواعد البيانات مثل SQL Express أو MySQL أو MariaDB وتثبيته على الجهاز الذي يعمل كخادم إدارة. بدلاً من ذلك، يمكنك اختيار MariaDB DBMS التي تسمح لك بإدارة ما يصل إلى 20 ألف جهاز. إذا كانت شبكتك تحتوي على أكثر من 10 000 جهاز (أو إذا كنت تخطط لتوسيع شبكتك لتصل إلى هذا العدد من الأجهزة)، فنوصيك باختيار نظام إدارة قواعد بيانات SQL مدفوعة وتثبيتها على جهاز مخصص. يمكن أن يعمل نظام إدارة قواعد البيانات المدفوع مع خوادم إدارة متعددة، بينما يعمل نظام إدارة قواعد البيانات المجاني مع خادم واحد فقط.

إذا حددت SQL Server DBMS، فيُرجى ملاحظة أنه يمكنك ترحيل البيانات المخزنة في قاعدة البيانات إلى MySQL أو MariaDB أو Azure SQL أو DBMS. لإجراء الترحيل، انسخ بياناتك احتياطيًا واستعدها إلى نظام DBMS الجديد .

إذا حددت MSSQL 2019، فيجب عليك استخدام التصحيح التراكمي CU12 أو إصدار أحدث. ويتيح لك ذلك تجنب الأخطاء والعبء الزائد على النظام الذي قد يحدث.

8 **تثبيت نظام إدارة قواعد البيانات وإنشاء قاعدة بيانات**

تعرف على المزيد حول حسابات استخدام DBMS وتثبيت DBMS.

قبل التثبيت، اختر نظام إدارة قواعد البيانات المدعوم. يمكنك تحديد، على سبيل المثال، PostgreSQL أو Postgres Pro أو Microsoft SQL Server أو MySQL أو MariaDB.

لمزيد من المعلومات عن كيفية تثبيت نظام إدارة قاعدة البيانات المحدد، يُرجى الرجوع إلى مستنداته.

إذا قمت بتثبيت MariaDB و MySQL و PostgreSQL ، أو Postgres Pro ، استخدم الإعدادات الموصى بها للتأكد من أن نظام إدارة قواعد البيانات يعمل بشكل صحيح.

اكتب إعدادات نظام إدارة قواعد البيانات (DBMS) واحفظها لأنك ستحتاج إليها أثناء تثبيت خادم الإدارة. تشمل هذه الإعدادات اسم خادم SQL Server ورقم المنفذ المُستخدم للاتصال بخادم SQL Server واسم الحساب وكلمة المرور للوصول إلى خادم SQL Server.

إذا قررت تثبيت PostgreSQL أو Postgres Pro DBMS، فتأكد من تحديد كلمة مرور للمستخدم المتميز. إذا لم يتم تحديد كلمة المرور، فقد يتعذر على خادم الإدارة الاتصال بقاعدة البيانات.

بشكل افتراضي، يقوم مثبّت Kaspersky Security Center بإنشاء قاعدة بيانات لتخزين معلومات خادم الإدارة، ولكن يمكنك إلغاء الاشتراك في إنشاء قاعدة البيانات هذه واستخدام قاعدة بيانات مختلفة بدلاً منها. في هذه الحالة، تأكد من أنه تم إنشاء قاعدة البيانات وأنك تعرف اسمها وأن الحساب الموجود ضمن خادم الإدارة وسيصل إلى قاعدة البيانات هذه يتمتع بالدور db_owner من أجلها.

إذا لزم الأمر، اتصل بنظام إدارة قواعد البيانات الخاص بك للحصول على مزيد من المعلومات.

9 **تكوين منافذ**

تأكد من أن كل المنافذ الضرورية مفتوحة للتفاعل بين المكونات وفقًا لبنية الأمان المحددة الخاصة بك.

إذا كان يتعين عليك توفير الوصول عبر الإنترنت إلى خادم الإدارة، قم بتكوين المنافذ وحدد إعدادات الاتصال، بناء على تكوين الشبكة.

10 **التحقق من الحسابات**

تأكد أن لديك جميع حقوق المسؤول المحلية المطلوبة لتثبيت خادم إدارة Kaspersky Security Center بنجاح ولنشر الحماية بعد ذلك على الجهاز. حقوق المسؤول المحلية على الأجهزة العميلة مطلوبة لتثبيت عميل الشبكة على هذه الأجهزة. بعد تثبيت عميل الشبكة، يمكنك استخدامه لتثبيت تطبيقات على الأجهزة عن بُعد، بدون استخدام الحساب الذي يمتلك حقوق مسؤول الجهاز.

بشكل افتراضي، على الجهاز المحدد لتثبيت خادم الإدارة، يقوم مثبّت Kaspersky Security Center بإنشاء ثلاثة حسابات محلية سيتم تشغيل خادم الإدارة وخدمات Kaspersky Security Center بموجبها:

- KL-AK-*: حساب خدمة خادم إدارة
- خدمة NT / KSC *: حساب للخدمات الأخرى من مجموعة خادم الإدارة
- KlPxeUser: حساب لنشر أنظمة التشغيل

يمكنك إلغاء الاشتراك في إنشاء حسابات لخدمات خادم الإدارة والخدمات الأخرى. وبدلاً من ذلك، يمكنك استخدام حساباتك الحالية مثل حسابات المجال، إذا كنت تخطط لتثبيت خادم الإدارة على مجموعة تجاوز الفشل أو كنت تخطط لاستخدام حسابات المجال بدلاً من الحسابات المحلية لأي سبب آخر. في هذه الحالة، تأكد من أن الحسابات المخصصة لتشغيل خادم الإدارة وخدمات Kaspersky Security Center التي تم إنشاؤها، وأنها ليست ذات امتيازات ولديها جميع الأذونات المطلوبة للوصول إلى نظام إدارة قواعد البيانات. (إذا كنت تخطط لمزيد من نشر أنظمة التشغيل على الأجهزة من خلال Kaspersky Security Center، فلا تقم بإلغاء الاشتراك في إنشاء الحسابات.)

تثبيت Kaspersky Security Center وتطبيق الأمان من Kaspersky على جهاز خادم الإدارة

1. **تثبيت خادم الإدارة، ووحدة تحكم الإدارة، وKaspersky Security Center Web Console، ومكونات الإدارة الإضافية لتطبيقات الأمان**

قم بتنزيل Kaspersky Security Center من موقع ويب Kaspersky. يمكنك تنزيل الحزمة الكاملة أو Web Console فقط أو وحدة تحكم الإدارة فقط.

تثبيت خادم الإدارة على الجهاز الذي حددته (أو أجهزة متعددة، إذا كنت تخطط لاستخدام خوادم إدارة متعددة). يمكنك تحديد تثبيت قياسي أو تثبيت مخصص لخادم الإدارة. يتم تثبيت وحدة تحكم الإدارة مع خادم الإدارة. يوصى بتثبيت خادم الإدارة على خادم مخصص بدلاً من وحدة التحكم بالمجال.

من المستحسن استخدام التثبيت القياسي إذا كنت ترغب في تجربة Kaspersky Security Center، على سبيل المثال، عن طريق اختبار تشغيله في منطقة صغيرة ضمن شبكتك. أثناء التثبيت القياسي، تقوم فقط بتكوين قاعدة البيانات. ويمكنك أيضًا تثبيت مجموعة المكونات الإضافية الافتراضية فقط الخاصة بإدارة تطبيقات Kaspersky. كما يمكنك أيضًا استخدام عملية التثبيت القياسي إذا كانت لديك خبرة في استخدام Kaspersky Security Center ويمكنك تحديد كل الإعدادات ذات الصلة بعد إجراء عملية التثبيت القياسي.

من المستحسن استخدام التثبيت المخصص إذا كنت تخطط لتعديل إعدادات Kaspersky Security Center، مثل المسار إلى المجلد المشترك والحسابات ومنافذ الاتصال بخادم الإدارة وإعدادات قاعدة البيانات. يمكّنك التثبيت المخصص من تحديد مكونات الإدارة الإضافية لـ Kaspersky المراد تثبيتها. إذا لزم الأمر، يمكنك بدء تثبيت مخطط في الوضع الصامت.

يتم تثبيت وحدة تحكم الإدارة وإصدار خادم عميل الشبكة مع خادم الإدارة. يمكنك أيضًا اختيار تثبيت Kaspersky Security Center Web Console أثناء التثبيت.

إذا كنت ترغب في تثبيت وحدة تحكم الإدارة و/أو Kaspersky Security Center Web Console على محطة عمل المسؤول بشكل منفصل لإدارة خادم الإدارة من خلال الشبكة.

2. **الإعداد الأولي والترخيص**

عند اكتمال تثبيت خادم الإدارة، يبدأ تشغيل معالج البدء السريع تلقائيًا عند أول اتصال خادم الإدارة. قم بتنفيذ التكوين الأولي لخادم الإدارة وفقًا للمتطلبات الحالية. أثناء مرحلة التكوين الأولي، يستخدم المعالج الإعدادات الافتراضية لإنشاء السياسات والمهام المطلوبة لنشر الحماية. ومع ذلك، قد لا تكون الإعدادات الافتراضية مثالية لاحتياجات مؤسستك. إذا لزم الأمر، يمكنك تحرير إعدادات السياسات والمهام (تكوين الحماية في شبكة تنظيم العميل، السيناريو: تكوين حماية الشبكة).

إذا كنت تخطط لاستخدام الميزات الموجودة خارج نطاق الوظائف الأساسية، يمكنك ترخيص التطبيق. يمكنك إجراء ذلك بإحدى الخطوات المذكورة في معالج البدء السريع.

3. **التحقق من نجاح تثبيت خادم الإدارة**

عند إكمال كل الخطوات السابقة، يتم تثبيت خادم الإدارة ويكون جاهزًا للاستخدام المستقبلي.

تأكد من أن وحدة تحكم الإدارة تعمل ويمكنك الاتصال بخادم الإدارة عبر وحدة تحكم الإدارة. وتأكد أيضًا من أن تنزيل التحديثات إلى مستودع مهمة خادم الإدارة متاحة في خادم الإدارة (في المجلد **المهام** الخاص بشجرة وحدة التحكم)، بالإضافة إلى سياسة Kaspersky Endpoint Security (في المجلد **السياسات** الخاص بشجرة وحدة التحكم).

عند اكتمال عملية التحقق، فتابع إجراء الخطوات أدناه.

النشر المركزي لتطبيقات الأمان من Kaspersky على أجهزة العملاء

1 **اكتشاف الأجهزة المتصلة بالشبكة**

هذه الخطوة جزء من معالج البدء السريع. كما يمكنك أيضًا بدء اكتشاف الأجهزة يدويًا. يتلقى Kaspersky Security Center عناوين وأسماء جميع الأجهزة التي تم اكتشافها في الشبكة. بعد ذلك يمكنك استخدام Kaspersky Security Center لتثبيت تطبيقات وبرامج Kaspersky المتوفرة من موردين آخرين في الأجهزة المكتشفة. يبدأ Kaspersky Security Center اكتشاف الأجهزة بشكل منتظم، مما يعني أنه في حالة ظهور أي مثيلات جديدة في الشبكة، سيتم اكتشافها تلقائيًا.

2 **تثبيت عميل الشبكة وتطبيقات أمان على أجهزة متصلة بالشبكة.**

يشمل نشر الحماية (تكوين الحماية في شبكة تنظيم عميل، السيناريو: تكوين حماية الشبكة) لشبكة المؤسسة على تثبيت عميل الشبكة وتطبيقات الأمان (على سبيل المثال، Kaspersky Endpoint Security) على الأجهزة التي تم اكتشافها بواسطة خادم الإدارة من خلال اكتشاف الأجهزة.

تحمي تطبيقات الأمان الأجهزة ضد الفيروسات و / أو البرامج الأخرى التي تشكّل تهديدًا. يضمن عميل الشبكة الاتصال بين الجهاز وخادم الإدارة. يتم تكوين إعدادات عميل الشبكة تلقائيًا بشكل افتراضي.

إذا كنت تريد ذلك، يمكنك تثبيت عملاء الشبكة في الوضع الصامت بملف استجابة أو بدون ملف استجابة.

قبل أن تبدأ في تثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة المتصلة بالشبكة، تأكد من إمكانية الوصول إلى هذه الأجهزة (أي قيد التشغيل). يمكنك تثبيت عميل الشبكة على الأجهزة الافتراضية وكذلك على الأجهزة الفعلية.

يمكن تثبيت تطبيقات الأمان وعميل الشبكة عند بعد أو محليًا.

التثبيت عن بُعد—باستخدام معالج نشر الحماية، يمكنك تثبيت تطبيق الأمان عن بُعد (على سبيل المثال، Kaspersky Endpoint Security for Windows) وعميل الشبكة على الأجهزة التي تم اكتشافها بواسطة خادم الإدارة في شبكة المؤسسة. وفي المعتاد، تقوم مهمة التثبيت عن بُعد بنشر الحماية بنجاح على معظم الأجهزة المتصلة بالشبكة. ولكن، قد تُرجع خطأ على بعض الأجهزة إذا، على سبيل المثال، تم إيقاف تشغيل جهاز أو عدم التمكن من الوصول إليه لأي سبب آخر. في هذه الحالة، ننصحك بالاتصال بالجهاز يدويًا واستخدام التثبيت المحلي.

يُستخدم التثبيت المحلي على أجهزة الشبكة التي يتعذر نشر الحماية عليها باستخدام مهمة التثبيت عن بُعد. لتثبيت الحماية على هذه الأجهزة، قم بإنشاء حزمة تثبيت مستقلة يمكنك تشغيلها محليًا على هذه الأجهزة.

يتم وصف تثبيت عميل الشبكة على الأجهزة التي تستخدم نظامي التشغيل Linux وMacOS في الوثائق الخاصة بـ Kaspersky Endpoint Security for Linux و Kaspersky Endpoint Security for Mac على التوالي. على الرغم من أن الأجهزة التي تعمل بأنظمة التشغيل Linux وmacOS تعد أقل عرضة للثغرات الأمنية مقارنةً بأجهزة الكمبيوتر التي تعمل بنظام التشغيل Windows، مع ذلك نقترح أن تثبت تطبيقات الأمان على هذه الأجهزة.

بعد التثبيت، تأكد من أن تطبيق الأمان مثبّت على الأجهزة المدارة. قم بتشغيل تقرير إصدار برنامج Kaspersky واستعراض نتائجه.

3 **نشر مفاتيح الترخيص على الأجهزة العميلة**

قم بنشر مفاتيح الترخيص على الأجهزة العميلة لتفعيل تطبيقات الأمان المُدارة على هذه الأجهزة.

4 **تكوين حماية الأجهزة المحمولة**

هذه الخطوة جزء من معالج البدء السريع.

إذا أردت إدارة الأجهزة المحمولة للمؤسسة، فاتخاذ الخطوات اللازمة لتحضير ونشر إدارة الأجهزة المحمولة.

5 **إنشاء بنية مجموعة الإدارة**

في بعض الحالات، قد يتطلب نشر الحماية على الأجهزة المتصلة بالشبكة بأنسب طريقة أن تقسم مجموعة الأجهزة بالكامل في مجموعات الإدارة مع أخذ بنية المؤسسة في الاعتبار. يمكنك إنشاء قواعد نقل لتوزيع الأجهزة بين المجموعات، أو يمكنك توزيع الأجهزة يدويًا. يمكنك تعيين مهام جماعية لمجموعات الإدارة، وتحديد نطاق السياسات، وتعيين نقاط التوزيع.

تأكد أن جميع الأجهزة المدارة تم تعيينها بشكل صحيح في مجموعات الإدارة المناسبة، وأنه لم يعد هناك أجهزة غير معينة في الشبكة.

6 **تعيين نقاط التوزيع**

يعين Kaspersky Security Center ملفات نقاط التوزيع لمجموعات الإدارة تلقائيًا، ولكن يمكنك تعيينها يدويًا، عند اللزوم. نوصيك باستخدام نقاط التوزيع في الشبكات واسعة النطاق لتقليل التحميل على خادم الإدارة وفي الشبكات المشتملة لبنية موزعة لتوفير وصول خادم الإدارة إلى الأجهزة (أو مجموعات الأجهزة) المتصلة من خلال قنوات ذات معدلات نقل منخفضة. يمكنك استخدام الأجهزة التي تعمل بنظام Linux كنقاط توزيع، بالإضافة إلى الأجهزة التي تعمل بنظام Windows.

المنافذ المستخدمة بواسطة Kaspersky Security Center

تعرض الجداول أدناه المنافذ الافتراضية التي تستخدمها خوادم الإدارة وأجهزة العميل. يمكنك إذا كنت ترغب في ذلك أن تغير أرقام المنافذ الافتراضية.

إذا قمت بتثبيت خادم الإدارة وقاعدة البيانات على أجهزة مختلفة، فيجب عليك إتاحة المنافذ الضرورية على الجهاز الموجود به قاعدة البيانات (على سبيل المثال، المنفذ 3306 لخادم MySQL Server أو المنفذ 1433 لخادم Microsoft SQL Server أو المنفذ 5432 لبرنامج PostgreSQL وPostgres Pro). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

المنافذ المستخدمة بواسطة خادم الإدارة

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
8060	klcsweb	TCP	نقل حزم التثبيت التي تم نشرها إلى أجهزة عميلة	نشر حزم التثبيت. يمكنك تغيير رقم المنفذ الافتراضي **في القسم خادم الويب** في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console. هذا المنفذ اختياري. لأسباب أمنية نوصي باستخدام المنفذ TCP 8061.
8061	klcsweb	TCP (TLS)	نقل حزم التثبيت التي تم نشرها إلى أجهزة عميلة	نشر حزم التثبيت. يمكنك تغيير رقم المنفذ الافتراضي في القسم خادم الويب في نافذة خصائص **خادم الإدارة** في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
13000	klserver	TCP (TLS)	تلقي اتصالات من عملاء الشبكة وكذلك خوادم الإدارة الثانوية؛ بالإضافة إلى استخدامه على الخوادم التابعة لتلقي اتصالات من خادم الإدارة الرئيسي (على سبيل المثال في حالة وجود خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت)	إدارة أجهزة العملاء وخوادم الإدارة الثانوية. يمكنك تغيير رقم المنفذ الافتراضي لتلقي الاتصالات من عملاء الشبكة عند تكوين منافذ الاتصال. يمكنك تغيير رقم المنفذ الافتراضي لتلقي الاتصالات من خوادم الإدارة الثانوية عند إنشاء تسلسل هرمي لخوادم الإدارة في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
13000	klserver	UDP	تلقي معلومات حول الأجهزة التي تم إيقاف تشغيلها من عملاء الشبكة	إدارة الأجهزة العميلة. يمكنك تغيير رقم المنفذ الافتراضي في إعدادات سياسة عميل الشبكة في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	تلقي اتصالات من وحدة تحكم الإدارة إلى خادم الإدارة	إدارة خادم الإدارة. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة.
13299	klserver	TCP (TLS)	تلقي اتصالات من Kaspersky Security Center Web Console إلى خادم الإدارة؛ تلقي اتصالات إلى خادم الإدارة عبر OpenAPI	Kaspersky Security Center Web Console، OpenAPI. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة (القسم **إعدادات اتصال خادم الإدارة** ← القسم الفرعي **منافذ الاتصال**) في وحدة تحكم الإدارة، أو عند إنشاء تسلسل هرمي لخوادم الإدارة في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
14000	klserver	TCP	تلقي اتصالات من عملاء الشبكة	إدارة الأجهزة العميلة. يمكنك تغيير رقم المنفذ الافتراضي عند تكوين منافذ الاتصال أثناء تثبيت Kaspersky Security Center أو عند توصيل جهاز عميل بخادم الإدارة يدويًا. هذا المنفذ اختياري. لأسباب أمنية نوصي باستخدام المنفذ TCP 13000.
13111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	TCP	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة.
15111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	UDP	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة.
17000	klactprx	TCP (TLS)	تلقي اتصالات لتفعيل التطبيق من الأجهزة المُدارة (باستثناء الأجهزة المحمولة)	خادم عميل التنشيط الذي تستخدمه الأجهزة غير المحمولة لتنشيط تطبيقات Kaspersky برموز التنشيط. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة.
17100 (فقط إذا كنت تدير أجهزة محمولة)	klactprx	TCP (TLS)	تلقي اتصالات لتفعيل التطبيق من الأجهزة المحمولة	خادم وكيل التفعيل للأجهزة المحمولة. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة.

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
19170	klserver	HTTPS (TLS)	نفق الاتصالات إلى الأجهزة المُدارة باستخدام الأداة المساعدة klsctunnel	الاتصال عن بُعد بالأجهزة المدارة باستخدام Kaspersky Security Center Web Console. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة فقط (القسم **إعدادات اتصال خادم الإدارة** ← القسم الفرعي **منافذ الاتصال** ← الخيار **افتح منفذ بروتوكول سطح المكتب البعيد (RDP) الخاص بـ Web Console**).
13292 (فقط إذا كنت تدير أجهزة محمولة)	klserver	TCP (TLS)	تلقي اتصالات من الأجهزة المحمولة	إدارة جهاز المحمول. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
13294 (فقط إذا كنت تدير أجهزة محمولة)	klserver	TCP (TLS)	تلقي اتصالات من أجهزة حماية UEFI	إدارة أجهزة العملاء لحماية UEFI. يمكنك تغيير رقم المنفذ الافتراضي عند توصيل أجهزة محمولة، أو لاحقًا في نافذة خصائص خادم الإدارة (القسم **إعدادات اتصال خادم الإدارة** ← القسم الفرعي **منافذ الاتصال**) في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
13296	klserver	TCP (TLS)	نشر مقاييس Kaspersky Security Center لنظام Prometheus	نشر مقاييس Kaspersky Security Center التي سيحصل عليها نظام Prometheus أيضًا. يمكنك عرض المقاييس عبر الرابط التالي: https://<server_address>:13296/metrics في <server_address>، حدد عنوان IP أو اسم المجال لخادم الإدارة الخاص بك. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة.
30522، 30523 (المنافذ الموجودة على واجهة المضيف المحلي)	klnagent	TCP	تلقي تحديثات تطبيق Kaspersky من خادم الإدارة باستخدام مكون FileTransferBridge	جهاز خادم الإدارة الذي يتلقى تحديثات تطبيق Kaspersky.

يوضح الجدول أدناه المنفذ الذي يستخدمه خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM (فقط إذا كنت تدير الأجهزة المحمولة).

المنفذ المستخدم بواسطة خادم iOS MDM

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
443	kliosmdmservicesrv	TCP (TLS)	تلقي اتصالات من الأجهزة المحمولة iOS	إدارة جهاز المحمول. يمكنك تغيير رقم المنفذ الافتراضي عند تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

يوضح الجدول أدناه المنفذ الذي يستخدمه Kaspersky Security Center Web Console Server. يمكن أن يكون نفس الجهاز المثبت عليه خادم الإدارة أو جهاز مختلف.

المنفذ الذي يستخدمه Kaspersky Security Center Web Console Server

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
8080	Node.js: جافا سكريبت من جانب الخادم	TCP (TLS)	تلقي اتصالات من مستعرض الويب إلى Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. يمكنك تغيير رقم المنفذ الافتراضي عند تثبيت Kaspersky Security Center Web Console على جهاز يعمل بنظام Windows أو على منصة Linux. إذا قمت بتثبيت Kaspersky Security Center Web Console على نظام التشغيل Linux ALT، فيجب عليك تحديد رقم منفذ بخلاف 8080، لأن المنفذ 8080 يستخدمه نظام التشغيل.

يوضح الجدول أدناه المنفذ الذي تستخدمه الأجهزة المدارة المثبت عليها عميل الشبكة.

المنافذ التي يستخدمها عميل الشبكة

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
15000	klnagent	UDP	إشارات الإدارة من خادم الإدارة أو نقطة التوزيع إلى عملاء الشبكة	إدارة الأجهزة العميلة. يمكنك تغيير رقم المنفذ الافتراضي في إعدادات سياسة عميل الشبكة في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
15000	klnagent	بث بروتوكول حزم بيانات المستخدم (UDP)	الحصول على بيانات حول وكلاء الشبكة الآخرين ضمن مجال البث نفسه (ثم يتم إرسال البيانات إلى خادم الإدارة)	تسليم التحديثات وحزم التثبيت.

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
15001	klnagent	UDP	استقبال طلبات البث المتعدد من نقطة توزيع (إذا كانت قيد الاستخدام)	استلام التحديثات وحزم التثبيت من نقطة التوزيع. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
30522، 30523 (المنافذ الموجودة على واجهة المضيف المحلي)	klnagent	TCP	تلقي تحديثات تطبيق Kaspersky من خادم الإدارة باستخدام مكون FileTransferBridge	الأجهزة المدارة التي تتلقى تحديثات تطبيق Kaspersky من خادم الإدارة المحدد كمصدر لتحديث قاعدة البيانات.
161	klnagent	SNMP	مراقبة واكتشاف الأجهزة المتصلة بالشبكة.	قابلية اكتشاف الجهاز.

يرجى ملاحظة أن عملية klnagent يمكنها أيضًا طلب منافذ مجانية من نطاق المنفذ الديناميكي لنظام تشغيل نقطة النهاية. يتم تخصيص هذه المنافذ لعملية klnagent تلقائيًا بواسطة نظام التشغيل، لذلك يمكن لعملية klnagent استخدام بعض المنافذ التي يستخدمها برنامج آخر. إذا كانت عملية klnagent تؤثر على عمليات البرنامج، فقم بتغيير إعدادات المنفذ في هذا البرنامج، أو قم بتغيير نطاق المنفذ الديناميكي الافتراضي في نظام التشغيل الخاص بك لاستبعاد المنفذ المستخدم بواسطة البرنامج المتأثر.

ضع في الاعتبار أيضًا أن التوصيات المتعلقة بتوافق Kaspersky Security Center مع برامج الأطراف الخارجية موصوفة كمرجع فقط وقد لا تنطبق على الإصدارات الجديدة من برامج الأطراف الخارجية. وتستند التوصيات الموضحة لتكوين المنافذ على تجارب الدعم الفني وأفضل الممارسات الخاصة بنا.

يوضح الجدول الموجود أدناه المنافذ التي يستخدمها جهاز مدار مثبت عليه عميل شبكة والذي يعمل كنقطة توزيع. تُستخدم المنافذ المدرجة بواسطة أجهزة نقطة التوزيع بالإضافة إلى المنافذ التي يستخدمها عملاء الشبكة (انظر الجدول أعلاه).

المنافذ التي يستخدمها عميل الشبكة وتعمل كنقطة توزيع

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
13000	klnagent	TCP (TLS)	استلام الاتصالات من عملاء الشبكة ومن Kaspersky Security Center عندما تعمل نقطة التوزيع كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ). إذا تم تحديد جهاز مُثبت عليه خادم الإدارة كنقطة توزيع، سيتم استخدام المنفذ 13001 لاتصال SSL بشكل افتراضي بدلاً من المنفذ 13000.	إدارة الأجهزة العميلة وتسليم التحديثات وحزم التثبيت. يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: خادم الإدارة وبوابة اتصال في مقطع شبكة اتصال وجهاز عميل. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
13111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	TCP	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
15111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	UDP	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
17111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	HTTPS	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.
13295 (إذا كنت تستخدم نقطة التوزيع كخادم إرسال فقط)	klnagent	TCP (TLS)	استلام اتصالات من الأجهزة العميلة	قم بإرسال خادم. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console.

يوضح الجدول أدناه المنافذ المستخدمة على جهاز وحدة تحكم المجال.

المنافذ المستخدمة على جهاز وحدة تحكم المجال

رقم المنفذ	البروتوكول	غرض المنفذ	النطاق
389	LDAP عبر TCP أو UDP	الاتصال بخادم LDAP	استقصاء وحدة تحكم المجال
636	LDAP عبر TLS	الاتصال بخادم LDAP	استقصاء وحدة تحكم المجال

يحتوي الجدول أدناه على المنفذ الذي يجب أن يكون مفتوحًا على الأجهزة العميلة التي لم يتم تثبيت عميل الشبكة عليها.

المنفذ المستخدم على جهاز العميل غير المُعين

رقم المنفذ	البروتوكول	غرض المنفذ	النطاق
22	SSH	الاتصال بجهاز عميل عبر SSH	لأجهزة العميل المستندة إلى Linux فقط. التثبيت عن بُعد لتطبيقات Kaspersky من خلال نقطة توزيع Linux.

شهادات للعمل مع Kaspersky Security Center

يحتوي هذا القسم على معلومات حول شهادات Kaspersky Security Center ويصف كيفية إصدار شهادة مخصصة لخادم الإدارة.

حول شهادات Kaspersky Security Center

يستخدم Kaspersky Security Center الأنواع التالية من الشهادات لتمكين التفاعل الآمن بين مكونات التطبيق:

- شهادة خادم الإدارة
- شهادة المحمول
- شهادة خادم الأجهزة التي تعمل بنظام iOS MDM
- شهادة خادم الويب Kaspersky Security Center
- شهادة Kaspersky Security Center Web Console

بشكل افتراضي، يستخدم Kaspersky Security Center الشهادات الموقعة ذاتيًا (أي الصادرة عن Kaspersky Security Center نفسه)، ولكن يمكنك استبدالها بشهادات مخصصة لتفي بمتطلبات شبكة مؤسستك بشكل أفضل والامتثال لمعايير الأمان. بعد أن يتحقق خادم الإدارة مما إذا كانت الشهادة المخصصة تفي بجميع المتطلبات المعمول بها، تفترض هذه الشهادة نفس النطاق الوظيفي للشهادة الموقعة ذاتيًا. الاختلاف الوحيد هو أن الشهادة المخصصة لا يتم إعادة إصدارها تلقائيًا عند انتهاء الصلاحية. يمكنك استبدال الشهادات بشهادات مخصصة عن طريق الأداة المساعدة klsetsrvcert أو من خلال قسم خصائص خادم الإدارة في وحدة تحكم الإدارة بناءً على نوع الشهادة. عند استخدام الأداة المساعدة klsetsrvcert، فعليك تحديد نوع الشهادة باستخدام إحدى القيم التالية:

- C—الشهادة العامة للمنفذين 13000 و13291.
- CR—شهادة الاحتياطي المشترك للمنفذين 13000 و13291.
- M—شهادة الجوال للمنفذ 13292.
- MR—شهادة حجز الهاتف المحمول للمنفذ 13292.
- MCA—مرجع تصديق الجوال لشهادات المستخدم المُنشأة تلقائيًا.

لا تحتاج إلى تنزيل الأداة المساعدة klsetsrvcert. يتم تضمين الأداة المساعدة في مجموعة توزيع Kaspersky Security Center. الأداة المساعدة غير متوافقة مع إصدارات Kaspersky Security Center السابقة.

يجب أن تكون فترة الصلاحية القصوى لأي من شهادات خادم الإدارة 397 يومًا أو أقل.

شهادات خادم الإدارة

مطلوب شهادة خادم الإدارة لمصادقة خادم الإدارة، وكذلك للتفاعل الآمن بين خادم الإدارة وعميل الشبكة على الأجهزة المُدارة أو بين خادم الإدارة الأساسي وخوادم الإدارة الثانوية. عند توصيل وحدة تحكم الإدارة بخادم الإدارة لأول مرة، تتم مطالبتك بتأكيد استخدام شهادة خادم الإدارة الحالية. هذا التأكيد مطلوب أيضًا في كل مرة يتم فيها استبدال شهادة خادم الإدارة، بعد كل مرة تعيد تثبيت خادم الإدارة، وعند توصيل خادم الإدارة الثانوي بخادم الإدارة الرئيسي. تسمى هذه الشهادة بالمشتركة ("C").

يتم إنشاء الشهادة العامة ("C") تلقائيًا عند تثبيت مكون خادم الإدارة. وتتكون الشهادة من جزأين:

- ملف klserver.cer؛ ويوجد بشكل افتراضي على الجهاز حيث تم تثبيت مكون خادم الإدارة في المجلد C:\ProgramData\KasperskyLab\adminkit\1093\cert.
- المفتاح السري الموجود في وحدة التخزين المحمية لنظام Windows.

كما توجد شهادة احتياطية مشتركة ("CR"). يُنشئ Kaspersky Security Center هذه الشهادة تلقائيًا قبل 90 يومًا من انتهاء صلاحية الشهادة المشتركة. تُستخدم الشهادة الاحتياطية المشتركة لاحقًا في الاستبدال السلس لشهادة خادم الإدارة. عندما توشك الشهادة المشتركة على الانتهاء، يتم استخدام الشهادة الاحتياطية المشتركة للحفاظ على الاتصال مع مثيلات عميل الشبكة المثبتة على الأجهزة المدارة. بهذا الغرض، تصبح الشهادة الاحتياطية المشتركة تلقائيًا الشهادة المشتركة الجديدة قبل 24 ساعة من انتهاء صلاحية الشهادة المشتركة القديمة.

يمكنك أيضًا إجراء نسخ احتياطي لشهادة خادم الإدارة بشكل منفصل عن إعدادات خادم الإدارة الأخرى من أجل نقل خادم الإدارة من جهاز إلى آخر دون فقدان البيانات.

شهادات المحمول

مطلوب شهادة المحمول ("M") لمصادقة خادم الإدارة على الأجهزة المحمولة. يمكنك تكوين استخدام شهادة المحمول في الخطوة المخصصة لمعالج البدء السريع.

كما توجد شهادة احتياطية للمحمول ("MR"): يتم استخدامها لاستبدال شهادة خادم الإدارة بسهولة. يُنشئ Kaspersky Security Center هذه الشهادة تلقائيًا قبل 60 يومًا من انتهاء صلاحية الشهادة المشتركة. عندما توشك شهادة المحمول أن تنتهي صلاحيتها، يتم استخدام الشهادة الاحتياطية للمحمول من أجل الحفاظ على الاتصال مع مثيلات عميل الشبكة المثبتة على الأجهزة المحمولة المدارة. بهذا الغرض، تصبح الشهادة الاحتياطية للمحمول بشكلٍ تلقائي الشهادة المشتركة الجديدة قبل 24 ساعة من انتهاء صلاحية الشهادة المشتركة القديمة.

إذا كان سيناريو الاتصال يتطلب استخدام شهادة العميل على الأجهزة المحمولة (اتصال يتضمن مصادقة SSL ثنائية الاتجاه)، فيمكنك إنشاء هذه الشهادات عن طريق الجهة المعتمدة لشهادات المستخدم التي يتم إنشاؤها تلقائيًا ("MCA"). يمكّنك أيضًا معالج البدء السريع من بدء استخدام شهادات العميل المخصصة الصادرة عن جهة معتمدة مختلفة، بينما يتيح لك التكامل مع مجال البنية التحتية للمفتاح العام (PKI) لمؤسستك إصدار شهادات العميل عن طريق جهة معتمدة للمجال الخاص بك.

شهادة خادم الأجهزة التي تعمل بنظام iOS MDM

مطلوب شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لمصادقة خادم الإدارة على الأجهزة المحمولة التي تعمل بنظام التشغيل iOS. يتم إجراء التفاعل مع هذه الأجهزة عبر بروتوكول إدارة الأجهزة المحمولة من Apple (MDM) الذي لا يتضمن أي عميل شبكة. بدلاً من ذلك، تقوم بتثبيت ملف تعريف iOS MDM خاص يحتوي على شهادة العميل على كل جهاز لضمان مصادقة SSL ثنائي الاتجاه.

يمكّنك أيضًا معالج البدء السريع من بدء استخدام شهادات العميل المخصصة الصادرة عن جهة معتمدة مختلفة، بينما يتيح لك التكامل مع مجال البنية التحتية للمفتاح العام (PKI) لمؤسستك إصدار شهادات العميل عن طريق جهة معتمدة للمجال الخاص بك.

يتم إرسال شهادات العميل إلى أجهزة iOS عند تنزيل ملفات تعريف iOS MDM هذه. شهادة عميل خادم iOS MDM فريدة لكل جهاز iOS مُدار. يمكنك إنشاء جميع شهادات العميل لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عن طريق الجهة المعتمدة لشهادات المستخدم المُنشأة تلقائيًا ("MCA").

شهادة خادم الويب Kaspersky Security Center

يستخدم Kaspersky Security Center Web Server (المشار إليه فيما يلي باسم خادم الويب)، وهو أحد مكونات خادم إدارة Kaspersky Security Center، نوعًا خاصًا من الشهادات. هذه الشهادة مطلوبة لنشر حزم تثبيت عميل الشبكة التي تقوم بتنزيلها بشكل متتابع على الأجهزة المُدارة، وهي مطلوبة كذلك لنشر ملفات تعريف iOS MDM وتطبيقات iOS وحزم تثبيت Kaspersky Security for Mobile. بالنسبة لهذا الغرض، يمكن لخادم الويب استخدام شهادات مختلفة.

إذا تم تعطيل دعم الجهاز المحمول، فسيستخدم خادم الويب إحدى الشهادات التالية حسب ترتيب الأولوية:

1. شهادة خادم الويب المخصصة التي حددتها يدويًا عن طريق وحدة تحكم الإدارة
2. شهادة خادم الإدارة المشتركة ("C")

إذا تم تمكين دعم الجهاز المحمول، فسيستخدم خادم الويب إحدى الشهادات التالية حسب ترتيب الأولوية:

1. شهادة خادم الويب المخصصة التي حددتها يدويًا عن طريق وحدة تحكم الإدارة
2. شهادة المحمول المخصصة
3. شهادة المحمول الموقعة ذاتيًا ("M")
4. شهادة خادم الإدارة المشتركة ("C")

شهادة Kaspersky Security Center Web Console

يمتلك Kaspersky Security Center Web Console Server (المشار إليه فيما يلي باسم Web Console) شهادته الخاصة. عند فتح موقع ويب، يتحقق المستعرض مما إذا كان اتصالك موثوقًا به أم لا. تسمح لك شهادة Web Console بمصادقة Web Console وتُستخدم لتشفير حركة المرور بين المستعرض وWeb Console.

عند فتح وحدة تحكم الويب، قد يخبرك المستعرض أن الاتصال بوحدة تحكم الويب ليس خاصًا وأن شهادة وحدة تحكم الويب غير صالحة. يظهر هذا التحذير لأن شهادة Web Console موقعة ذاتيًا ويتم إنشاؤها تلقائيًا بواسطة Kaspersky Security Center. لإزالة هذا التحذير، يمكنك القيام بأحد الإجراءات التالية:

- استبدل شهادة Kaspersky Security Center Web Console بشهادة مخصصة (خيار موصى به). قم بإنشاء شهادة موثوق بها في بنيتك الأساسية وتفي بمتطلبات الشهادات المخصصة.
- أضف شهادة Kaspersky Security Center Web Console إلى قائمة شهادات المستعرض الموثوق بها. نوصي باستخدام هذا الخيار فقط إذا لم تتمكن من إنشاء شهادة مخصصة.

حول شهادة خادم الإدارة

يتم إجراء عمليتين على أساس شهادة خادم الإدارة: مصادقة خادم الإدارة أثناء الاتصال عن طريق وحدة تحكم الإدارة وتبادل البيانات مع الأجهزة. تستخدم الشهادة كذلك للمصادقة عندما تكون خوادم الإدارة الأساسية متصلة بخوادم الإدارة الثانوية.

شهادة صادرة من Kaspersky

يتم إنشاء شهادة خادم الإدارة تلقائيًا أثناء تثبيت مكون خادم الإدارة ويتم تخزينها في المجلد ٪ALLUSERSPROFILE٪ \ Application Data \ KasperskyLab \ adminkit \ 1093 \ cert.

تكون شهادة خادم الإدارة صالحة لمدة خمس سنوات، إذا تم إنشاء الشهادة بواسطة خادم الإدارة الإصدار 12.2 أو إصدار أقدم. بخلاف ذلك، فإن مدة صلاحية الشهادة تقتصر على 397 يومًا. يتم إنشاء شهادة جديدة بواسطة خادم الإدارة كشهادة احتياطية قبل 90 يومًا من تاريخ انتهاء صلاحية الشهادة الحالية. وبالتالي، تستبدل الشهادة الجديدة تلقائيًا الشهادة الحالية قبل يوم واحد من تاريخ انتهاء الصلاحية. تتم إعادة تكوين جميع الأجهزة العميلة تلقائيًا لمصادقة خادم الإدارة بالشهادة الجديدة.

الشهادات المخصصة

إذا لزم الأمر، فيمكنك تعيين شهادة مخصص لخادم الإدارة. على سبيل المثال، قد يكون هذا الأمر ضروريًا لتحقيق تكامل أفضل مع PKI الموجود لمؤسستك أو للتكوين المخصص لحقول الشهادة.

يجب أن تكون فترة الصلاحية القصوى لأي من شهادات خادم الإدارة 397 يومًا أو أقل.

عند استبدال الشهادة، سيفقد كل عملاء الشبكة الذين تم توصيلهم بخادم الإدارة من قبل عبر SSL اتصالهم، وسيتم إرجاع خطأ "مصادقة خادم الإدارة". لإزالة هذا الخطأ، سوف يتعين عليك استعادة الاتصال بعد استبدال الشهادة.

في حال فقدان شهادة خادم الإدارة، يجب عليك إعادة تثبيت مكون خادم الإدارة ومن ثم استعادة البيانات للحصول عليها.

إذا فتحت Kaspersky Security Center Web Console في مستعرضات مختلفة وقمت بتنزيل ملف شهادة خادم الإدارة في نافذة خصائص خادم الإدارة، فإن الملفات التي يتم تنزيلها يكون لها أسماء مختلفة.

متطلبات الشهادات المخصصة المستخدمة في Kaspersky Security Center

يوضح الجدول أدناه متطلبات الشهادات المخصصة المحددة لمكونات مختلفة من Kaspersky Security Center.

متطلبات شهادات Kaspersky Security Center

نوع الشهادة	المتطلبات	تعليقات
الشهادة المشتركة، الشهادة الاحتياطية المشتركة ("C"، "CR")	الحد الأدنى لطول المفتاح: 2048. القيود الأساسية: • قيد طول المسار: لا شيء استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL استخدام المفتاح الموسع (اختياري): مصادقة الخادم، مصادقة العميل. يجب أن تتضمن الشهادة اسمًا بديلاً للموضوع (SAN) صالحًا يحتوي على عنوان الحلقة المرتدة لخادم الإدارة: • بالنسبة لبروتوكول IPv4 فالعنوان هو: 127.0.0.1 • بالنسبة لبروتوكول IPv6 فالعنوان هو: 0:0:0:0:0:0:0:1	معلمة استخدام المفتاح الموسع اختيارية. يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، ولكنها لا تقل عن "1".

نوع الشهادة	المتطلبات	تعليقات
شهادة المحمول، الشهادة الاحتياطية للمحمول ("M"، "MR")	الحد الأدنى لطول المفتاح: 2048. القيود الأساسية: • مرجع معتمد: صحيح • قيد طول المسار: لا شيء استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL استخدام المفتاح الموسع (اختياري): مصادقة الخادم.	معلمة استخدام المفتاح الموسع اختيارية. يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، إذا كان طول مسار الشهادة المشتركة لا يقل عن "1".
شهادة المرجع المصدق لشهادات المستخدم التي تم إنشاؤها تلقائيًا ("MCA")	الحد الأدنى لطول المفتاح: 2048. القيود الأساسية: • مرجع معتمد: صحيح • قيد طول المسار: لا شيء استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL استخدام المفتاح الموسع (اختياري): مصادقة الخادم، مصادقة العميل.	معلمة استخدام المفتاح الموسع اختيارية. يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، إذا كان طول مسار الشهادة المشتركة لا يقل عن "1".
شهادة خادم الويب	استخدام المفتاح الموسع : مصادقة الخادم. تتضمن حاوية PKCS # PEM / 12 التي تم تحديد الشهادة منها السلسلة الكاملة للمفاتيح العامة. الاسم البديل للموضوع (SAN) للشهادة موجود؛ أي أن قيمة حقل `subjectAltName` صالحة. تفي الشهادة بالمتطلبات الفعالة للمستعرضات المفروضة على شهادات الخادم، فضلاً عن المتطلبات الأساسية الحالية لمنتدى CA/Browser .	—
شهادة Kaspersky Security Center Web Console	تتضمن حاوية PEM التي تم تحديد الشهادة منها السلسلة الكاملة للمفاتيح العامة. الاسم البديل للموضوع (SAN) للشهادة موجود؛ أي أن قيمة حقل `subjectAltName` صالحة. تفي الشهادة بالمتطلبات الفعالة للمستعرضات لشهادات الخادم، بالإضافة إلى المتطلبات الأساسية الحالية لمنتدى CA/Browser .	لا يتم دعم الشهادات المشفرة بواسطة Kaspersky Security Center Web Console.

السيناريو: تحديد شهادة خادم الإدارة المخصصة

يمكنك تعيين شهادة خادم الإدارة المخصصة، على سبيل المثال، من أجل تكامل أفضل مع البنية الأساسية الحالية للمفتاح العام (PKI) لمؤسستك أو للتهيئة المخصصة لحقول الشهادة. من المفيد استبدال الشهادة فورًا بعد تثبيت خادم الإدارة وقبل انتهاء معالج البدء السريع.

يجب أن تكون فترة الصلاحية القصوى لأي من شهادات خادم الإدارة 397 يومًا أو أقل.

المتطلبات الأساسية

يجب استيفاء الشروط التالية:

- يجب إنشاء الشهادة الجديدة بتنسيق PKCS#12 (على سبيل المثال، عن طريق البنية التحتية للمفاتيح العامة (PKI) الخاصة بالمؤسسة).
- بالنسبة للشهادة الجديدة، يجب استيفاء المتطلبات المذكورة في الجدول أدناه.

في الجدول أدناه، انتبه إلى المتطلب "CA: true" الذي يعني أن الشهادة الجديدة يجب أن تكون صادرة عن هيئة تصديق موثوقة (CA). ويجب أن تتضمن الشهادة الجديدة بالمتطلب "CA: true" سلسلة الثقة الكاملة ومفتاحًا خاصًا، والذي يجب تخزينه في ملف بامتداد pfx أو p12.

متطلبات شهادات خادم الإدارة

نوع الشهادة	المتطلبات
الشهادة المشتركة، والشهادة الاحتياطية المشتركة ("C"، "CR")	الحد الأدنى لطول المفتاح: 2048. القيود الأساسية: • قيد طول المسار: لا شيء يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، ولكنها لا تقل عن "1". استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL استخدام المفتاح الموسع (EKU): مصادقة الخادم ومصادقة العميل. يعد EKU اختياريًا، ولكن إذا كانت شهادتك تحتوي عليه، فيجب تحديد بيانات مصادقة الخادم والعميل في EKU. يجب أن تتضمن الشهادة اسمًا بديلاً للموضوع (SAN) صالحًا. يجب أن يحتوي الحقل `subjectAltName` على عنوان الحلقة المرتدة لخادم الإدارة: • بالنسبة لبروتوكول IPv4 فالعنوان هو: 127.0.0.1 • بالنسبة لبروتوكول IPv6 فالعنوان هو: 0:0:0:0:0:0:0:1
شهادة المحمول، والشهادة الاحتياطية للمحمول ("M"، "MR")	الحد الأدنى لطول المفتاح: 2048. القيود الأساسية: • مرجع معتمد: صحيح • قيد طول المسار: لا شيء يمكن لقيمة قيد طول المسار أن تختلف عن "بلا"، إذا كان طول مسار الشهادة المشتركة لا يقل عن "1". استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL استخدام المفتاح الموسع (EKU): مصادقة الخادم. يعد EKU اختياريًا ، ولكن إذا كانت شهادتك تحتوي عليه، فيجب تحديد بيانات مصادقة الخادم في EKU.
شهادة المرجع المصدق لشهادات المستخدم التي تم إنشاؤها تلقائيًا ("MCA")	الحد الأدنى لطول المفتاح: 2048. القيود الأساسية: • مرجع معتمد: صحيح • قيد طول المسار: لا شيء يمكن لقيمة قيد طول المسار أن تختلف عن "بلا"، إذا كان طول مسار الشهادة المشتركة لا يقل عن "1". استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL استخدام المفتاح الموسع (EKU): مصادقة الخادم. يعد EKU اختياريًا، ولكن إذا كانت شهادتك تحتوي عليه، فيجب تحديد بيانات مصادقة العميل في EKU.

الشهادات الصادرة عن مرجع مصدق عام ليس لديها إذن توقيع الشهادة. ولاستخدام هذه الشهادات، تأكد من تثبيت عميل الشبكة إصدار 13 أو أحدث على نقاط التوزيع أو بوابات الاتصال في شبكتك. وإلا فلن تتمكن من استخدام الشهادات بدون إذن التوقيع.

المراحل

يتم تحديد شهادة خادم الإدارة على مراحل:

1 استبدال شهادة خادم الإدارة

استخدم خط الأوامر الأداة المساعدة klsetsrvcert لهذا الغرض.

2 تحديد شهادة جديدة واستعادة اتصال وكلاء الشبكة بخادم الإدارة

عند استبدال الشهادة، يفقد جميع عملاء الشبكة الذين كانوا متصلين سابقًا بخادم الإدارة من خلال SSL اتصالهم وسيظهر "خطأ في مصادقة خادم الإدارة". لتحديد الشهادة الجديدة واسترجاع الاتصال، استخدم خط الأوامر الأداة المساعدة klmover.

3 تحديد شهادة جديدة في إعدادات Kaspersky Security Center Web Console

بعد استبدال الشهادة، حددها في إعدادات Kaspersky Security Center Web Console. وإذا لم يتم فعل ذلك، لن يقدر Kaspersky Security Center Web Console على الاتصال بخادم الإدارة.

النتائج

عند الانتهاء من السيناريو، يتم استبدال شهادة خادم الإدارة والمصادقة على الخادم بواسطة وكلاء الشبكة على الأجهزة المدارة.

استبدال شهادة خادم الإدارة باستخدام الأداة المساعدة klsetsrvcert

لاستبدال شهادة خادم الإدارة:

في موجّه الأوامر، شغل الأداة التالية:

```
klsetsrvcert [-t <نوع الشهادة> {-i <المسار إلى الشهادة الجديدة> | -g <اسم dns>}][-f <وقت الاستبدال>][-r <شهادات الجذر>][-l <مسار ملف السجل>] [-p <كلمة المرور>] [-o <المعلمات>]
```

لا تحتاج إلى تنزيل الأداة المساعدة klsetsrvcert. يتم تضمين الأداة المساعدة في مجموعة توزيع Kaspersky Security Center. إنه غير متوافق مع إصدارات Kaspersky Security Center السابقة.

يتم عرض وصف معلمات الأداة المساعدة klsetsrvcert في الجدول أدناه.

قيم معلمات الأداة المساعدة klsetsrvcert

المعلمة	القيمة
t- certificate > type <	نوع الشهادة المراد استبدالها. القيم المحتملة لمعلمة certificate type >: • C—استبدال الشهادة للمنفذين 13000 و13291؛ • CR—استبدال الشهادة الاحتياطية للمنفذين 13000 و13291؛ • M — استبدال شهادة الأجهزة المحمولة على المنفذ 13292. • MR—استبدال شهادة الجوال الاحتياطية للمنفذ 13292. • MCA—جهة إصدار عميل الجوال لشهادات المستخدم التي يتم إنشاؤها تلقائيًا.
f- replacement > time <	الجدول الزمني لتغيير الشهادة باستخدام تنسيق "mm:DD-MM-YYYY hh" (للمنافذ 13000 و13291). استخدم هذه المعلمة إذا كنت ترغب في استبدال الشهادة المشتركة بالشهادة الاحتياطية المشتركة قبل انتهاء صلاحية الشهادة المشتركة. حدد الوقت الذي يجب أن تتزامن فيه الأجهزة المُدارة مع خادم الإدارة في شهادة جديدة.
i- path to new > certificate <	حاوية تحتوي على الشهادة والمفتاح الخاص بتنسيق PKCS#12 (ملف بامتداد .p12 أو .pfx).
p- password >	كلمة المرور المستخدمة لحماية الحاوية p12. يتم تخزين الشهادة والمفتاح الخاص في الحاوية ، وبالتالي، فإن كلمة المرور مطلوبة لفك تشفير الملف مع الحاوية.
o- validation > parameters <	معلمات التحقق من صحة الشهادة (مفصولة بفاصلة منقوطة). لاستخدام شهادة مخصصة بدون إذن التوقيع، حدد o NoCA- في الأداة المساعدة o NoCA. هذا مفيد للشهادات الصادرة عن مرجع مصدق عام. لتغيير طول مفتاح التشفير لنوعي الشهادات C أو CR، حدد o:RsaKeyLen- طول المفتاح > في الأداة المساعدة klsetsrvcert، حيث معلمة < طول المفتاح > هي قيمة طول المفتاح المطلوبة. وبخلاف ذلك، يتم استخدام طول مفتاح الشهادة الحالي.
g- dns name >	سيتم إنشاء شهادة جديدة لاسم DNS المحدد.

المعلمة	القيمة
root > r- < certificates	قائمة جهة إصدار الشهادة الجذرية الموثوقة، بتنسيق PEM.
< log file path > l-	ملف إخراج النتائج. بشكل افتراضي، يتم إعادة توجيه الإخراج إلى دفق إخراج قياسي.

على سبيل المثال، لتحديد شهادة خادم إدارة مخصصة، استخدم الأمر التالي:

```
klsetsrvcert -t C -i <المسار إلى الشهادة الجديدة> -p <كلمة المرور> -o NoCA
```

بعد استبدال الشهادة، يفقد جميع عملاء الشبكة المتصلين بخادم الإدارة عبر SSL اتصالهم. لاستعادة الاتصال، استخدم موجّه الأوامر أداة klmover.

لتجنب فقد اتصالات عملاء الشبكة، استخدم الأوامر التالية:

1. لتثبيت الشهادة الجديدة،

```
klsetsrvcert.exe -t CR -i <المسار إلى الشهادة الجديدة> -p <كلمة المرور> -o NoCA
```

2. لتحديد التاريخ الذي سيتم تطبيق الشهادة الجديدة فيه،

```
klsetsrvcert.exe -f "mm:DD-MM-YYYY hh"
```

حيث "mm:DD-MM-YYYY hh" هو التاريخ بعد 3-4 أسابيع من التاريخ الحالي. سيسمح التحول الزمني لتغيير الشهادة إلى الشهادة الجديدة بتوزيع الشهادة الجديدة على جميع عملاء الشبكة.

توصيل عملاء الشبكة بخادم الإدارة باستخدام الأداة المساعدة klmover

بعد استبدال شهادة خادم الإدارة باستخدام موجّه الأوامر الأداة المساعدة klsetsrvcert، تحتاج إلى إنشاء اتصال SSL بين عملاء الشبكة وخادم الإدارة لأن الاتصال مقطوع.

لتحديد شهادة خادم الإدارة الجديدة واستعادة الاتصال:

في موجّه الأوامر، شغل الأداة التالية:

```
klmover -address < عنوان الخادم > [-pn < رقم المنفذ >] [-ps < رقم منفذ SSL >] [-nossl]
[-cert < المسار إلى ملف الشهادة >]
```

حقوق المسؤول مطلوبة لتشغيل الأداة.

يتم نسخ هذه الأداة المساعدة تلقائيًا إلى مجلد عميل الشبكة، عند عميل الشبكة على جهاز عميل.

لمنع الدخلاء من نقل الأجهزة بعيدًا عن سيطرة خادم الإدارة، نوصي بشدة بتمكين الحماية بكلمة مرور لتشغيل الأداة المساعدة klmover. لتمكين الحماية بكلمة مرور ، حدد الخيار **Use uninstallation password** في إعدادات سياسة عميل الشبكة.

تتطلب الأداة المساعدة klmover حقوق المسؤول المحلي. ويمكن حذف الحماية بكلمة مرور لتشغيل الأداة المساعدة klmover للأجهزة التي تعمل بدون حقوق المسؤول المحلي.

يؤدي تمكين الخيار **Use uninstallation password** أيضًا إلى تمكين الحماية بكلمة مرور لأداة التنظيف (cleaner.exe).

لا يمكنك استخدام الأداة المساعدة KLMover لأجهزة العميل المتصلة بخادم الإدارة من خلال بوابات الاتصال. وبالنسبة لهذه الأجهزة، يتعين عليك إما إعادة تكوين عميل الشبكة أو إعادة تثبيت عميل الشبكة وتحديد بوابة الاتصال.

يتم عرض وصف معلمات الأداة المساعدة klmover في الجدول أدناه.

قيم معلمات الأداة المساعدة klsetsrvcert

المعلمة	القيمة
`-address <server address>`	عنوان خادم الإدارة للاتصال. يمكنك تحديد عنوان IP أو اسم NetBIOS أو اسم DNS.
`-pn <port number>`	رقم المنفذ الذي سيتم إنشاء اتصال غير مشفر بخادم الإدارة عن طريقه. رقم المنفذ الافتراضي هو 14000.
`-ps <SSL port number>`	رقم منفذ SSL الذي يتم من خلاله إنشاء الاتصال المشفر بخادم الإدارة باستخدام SSL. رقم المنفذ الافتراضي هو 13000.
`-nossl`	استخدام اتصال غير مشفر بخادم الإدارة. إذا لم يكن المفتاح قيد الاستخدام، فسيتم توصيل عميل الشبكة بخادم الإدارة باستخدام بروتوكول SSL المشفر.
`-cert <path to certificate file>`	استخدم ملف الشهادة المحدد لمصادقة الوصول إلى خادم الإدارة.
`-virtserv`	اسم خادم الإدارة الافتراضي
`-cloningmode`	وضع استنساخ قرص عميل الشبكة. استخدم إحدى المعلمات التالية لتكوين وضع استنساخ القرص: • `-cloningmode` — طلب حالة وضع استنساخ القرص. • `-cloningmode 1` — تمكين وضع استنساخ القرص. • `-cloningmode 0` — تعطيل وضع استنساخ القرص.
`-nauninstpwd <password>`	استخدم هذه المعلمة لتحديد كلمة مرور إلغاء تثبيت عميل الشبكة. المعلمة ليست إلزامية.

على سبيل المثال، لتوصيل عميل الشبكة بخادم الإدارة، قم بتشغيل الأمر التالي:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

إعادة إصدار شهادة خادم الويب

شهادة خادم الويب المستخدمة في برنامج Kaspersky Security Center مطلوبة لنشر حزم تثبيت عميل الشبكة التي تقوم بتنزيلها لاحقًا على الأجهزة المدارة وكذلك لنشر ملفات تعريف iOS MDM وتطبيقات iOS وحزم تثبيت برنامج Kaspersky Endpoint Security للجوال. بناءً على التكوين الحالي للتطبيق، يمكن أن تعمل العديد من الشهادات كشهادة خادم الويب (لمزيد من التفاصيل، راجع حول شهادات Kaspersky Security Center).

قد تحتاج إلى إعادة إصدار شهادة خادم الويب لاستيفاء متطلبات الأمان المحددة لمؤسستك أو للحفاظ على الاتصال المستمر بالأجهزة المُدارة قبل البدء في ترقية التطبيق. يقدم برنامج Kaspersky Security Center طريقتين لإعادة إصدار شهادة خادم الويب؛ يعتمد الاختيار المكون من طريقتين على ما إذا كان لديك أجهزة محمولة متصلة ومدارة من خلال بروتوكول الجوال (أي باستخدام شهادة الجوال).

إذا لم تقم مطلقًا بتحديد الشهادة المخصصة الخاصة بك على أنها شهادة خادم الويب في قسم **خادم الويب** في نافذة خصائص خادم الإدارة، ستعمل شهادة الجوال كشهادة خادم الويب. في هذه الحالة، يتم إعادة إصدار شهادة خادم الويب من خلال إعادة إصدار بروتوكول الجوال نفسه.

لإعادة إصدار شهادة خادم الويب عندما لا يكون لديك أجهزة محمولة مُدارة من خلال بروتوكول الجوال:

1. في مركز وحدة التحكم، انقر بزر الماوس الأيمن فوق اسم خادم الإدارة ذي الصلة وحدد من قائمة السياق **خصائص**.

2. في نافذة خصائص خادم الإدارة التي تفتح، حدد القسم **إعدادات اتصال خادم الإدارة**.

3. في قائمة الأقسام الفرعية، حدد القسم الفرعي **الشهادات**.

4. إذا كنت تخطط لمواصلة استخدام الشهادة الصادرة عن Kaspersky Security Center، فقم بما يلي:

a. في الجزء الأيمن، في مجموعة إعدادات **مصادقة خادم الإدارة من خلال الأجهزة المحمولة**، حدد خيار **تم إصدار الشهادة من خلال خادم الإدارة** وانقر فوق زر **جارٍ إعادة الإصدار**.

b. في النافذة **إعادة إصدار الشهادة** التي تفتح، في مجموعة إعدادات **عنوان الاتصال** و**مدة التفعيل**، حدد الخيارات ذات الصلة وانقر فوق **موافق**.

c. في نافذة التأكيد، انقر فوق **نعم**.

بدلاً من ذلك، إذا كنت تخطط لاستخدام شهادتك المخصصة، فقم بما يلي:

a. تحقق مما إذا كانت شهادتك المخصصة تلبي متطلبات Kaspersky Security Center. إذا اقتضى الأمر ذلك، فقم بتعديل الشهادة.

b. حدد خيار **شهادة أخرى** وانقر فوق زر **استعراض**.

c. في نافذة **الشهادة** التي تفتح في حقل **نوع الشهادة**، حدد نوع شهادتك ثم حدد موقع الشهادة والإعدادات:

- إذا كنت قد اخترت **الحاوية PKCS#12**، فانقر على زر **استعراض** بجوار **ملف الشهادة** الحقل وحدد ملف الشهادة على محرك الأقراص الثابتة. إذا كان ملف الشهادة محميًا بكلمة مرور، فأدخل كلمة المرور في حقل **كلمة المرور (إن وجد)**.
- إذا كنت قد اخترت **الشهادة X.509**، فانقر على **استعراض** الموجود بجوار حقل **المفتاح الخاص (.prk, .pem)**، وحدد المفتاح الخاص على محرك الأقراص الثابتة. إذا كان المفتاح الخاص محميًا بكلمة مرور، فأدخل كلمة المرور في حقل **كلمة المرور (إن وجد)**. ثم انقر فوق زر **استعراض** بجوار حقل **المفتاح العام (.cer)**، وحدد المفتاح الخاص على محرك الأقراص الثابتة.

d. في نافذة **الشهادة**، انقر فوق **موافق** .

e. في نافذة التأكيد، انقر فوق **نعم**.

تم إعادة إصدار شهادة الجوال لاستخدامها كشهادة خادم الويب.

لإعادة إصدار شهادة خادم الويب عندما يكون لديك أي أجهزة محمولة مُدارة من خلال بروتوكول الجوال:

1. أنشئ شهادتك المخصصة وجهزها للاستخدام في برنامج Kaspersky Security Center. تحقق مما إذا كانت شهادتك المخصصة تلبي متطلبات Kaspersky Security Center. إذا اقتضى الأمر ذلك، فقم بتعديل الشهادة.

2. في مركز وحدة التحكم، انقر بزر الماوس الأيمن فوق اسم خادم الإدارة ذي الصلة وحدد من قائمة السياق **خصائص**.

3. في نافذة خصائص خادم الإدارة التي تفتح ، في الجزء الأيمن، حدد القسم **خادم الويب**.

4. في قائمة **عبر HTTPS**، حدد خيار **تحديد شهادة أخرى**.

5. في قائمة **عبر HTTPS**، انقر فوق زر **تغيير**.

6. من نافذة **الشهادة** التي تفتح، في حقل **نوع الشهادة**، حدد نوع شهادتك:

- إذا كنت قد اخترت **الحاوية PKCS#12**، فانقر على زر **استعراض** بجوار **ملف الشهادة** الحقل وحدد ملف الشهادة على محرك الأقراص الثابتة. إذا كان ملف الشهادة محميًا بكلمة مرور، فأدخل كلمة المرور في حقل **كلمة المرور (إن وجد)**.
- إذا كنت قد اخترت **الشهادة X.509**، فانقر على **استعراض** الموجود بجوار حقل **المفتاح الخاص (.prk, .pem)**، وحدد المفتاح الخاص على محرك الأقراص الثابتة. إذا كان المفتاح الخاص محميًا بكلمة مرور، فأدخل كلمة المرور في حقل **كلمة المرور (إن وجد)**. ثم انقر فوق زر **استعراض** بجوار حقل **المفتاح العام (.cer)**، وحدد المفتاح الخاص على محرك الأقراص الثابتة.

7. في نافذة **الشهادة**، انقر فوق **موافق**.

8. إذا اقتضى الأمر ذلك، من نافذة خصائص خادم الإدارة، في حقل **منفذ HTTPS لخادم الويب**، غيّر رقم منفذ HTTPS لخادم الويب. انقر فوق **موافق**.

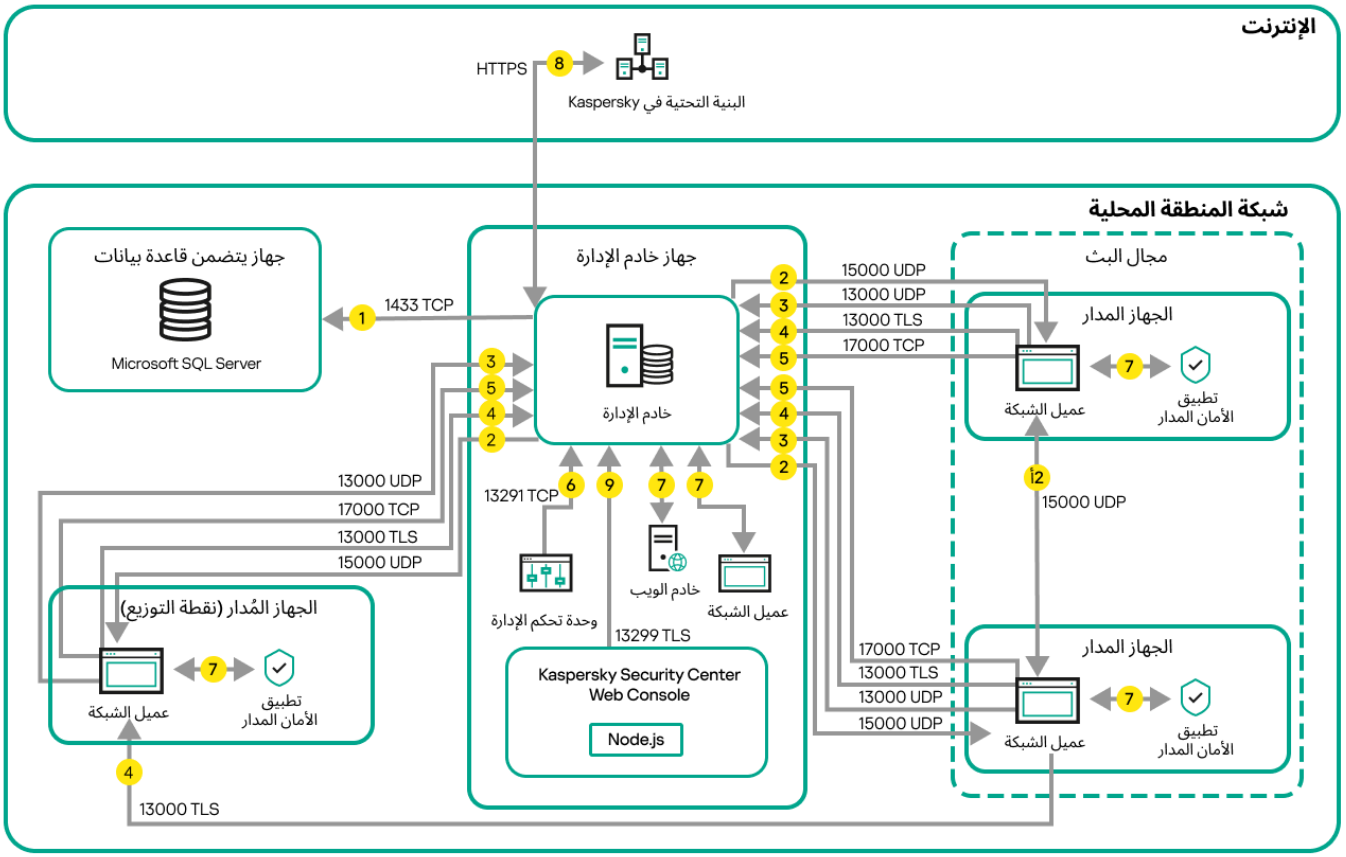
يتم إعادة إصدار شهادة خادم الويب.

المخططات لحركة البيانات واستخدام المنفذ

يوفر هذا القسم مخططات لحركة البيانات بين مكونات Kaspersky Security Center وتطبيقات الأمان المُدارة والخوادم الخارجية تحت تكوينات مختلفة. يتم تزويد المخططات بأرقام للمنافذ التي يجب أن تكون متوفرة على الأجهزة المحلية.

خادم الإدارة والأجهزة المدارة في شبكة الاتصال المحلية (LAN)

يوضح الشكل التالي حالة نقل البيانات عند نشر Kaspersky Security Center في شبكة اتصال محلية (LAN) فقط.



خادم الإدارة والأجهزة المدارة في شبكة الاتصال المحلية (LAN)

يوضح الشكل كيفية اتصال الأجهزة المُدارة المختلفة بخادم الإدارة بطرق مختلفة: مباشرة أو عبر نقطة توزيع. وتعمل نقاط التوزيع على تقليل التحميل على خادم الإدارة أثناء توزيع التحديث، بالإضافة إلى تحسين نقل بيانات الشبكة. ومع ذلك، لن تكون هناك حاجة لنقاط التوزيع إلا إذا كان عدد الأجهزة المدارة كبيرًا بدرجة كافية. إذا كان عدد الأجهزة المُدارة صغيرًا، يمكن لجميع الأجهزة المُدارة تلقي التحديثات من خادم الإدارة مباشرةً.

تشير الأسهم إلى بدء نقل البيانات: يشير كل سهم من جهاز يبدأ الاتصال إلى الجهاز الذي "يرد" على المكالمة. يتم عرض رقم المنفذ واسم البروتوكول المستخدم لنقل البيانات. لكل سهم تسمية رقمية، وتفاصيل عملية نقل البيانات المقابلة كما يلي:

1. خادم الإدارة يُرسل البيانات إلى قاعدة البيانات. إذا قمت بتثبيت خادم الإدارة وقاعدة البيانات على أجهزة مختلفة، فيجب عليك إتاحة المنافذ الضرورية على الجهاز الموجود به قاعدة البيانات (على سبيل المثال، المنفذ 3306 لخادم MySQL Server أو المنفذ 1433 لخادم Microsoft SQL Server). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

2. يتم تحويل طلبات الاتصال الواردة من خادم الإدارة إلى جميع الأجهزة المدارة غير المحمولة عبر منفذ UDP رقم 15000.

يرسل عملاء الشبكة طلبات إلى بعضهم البعض ضمن مجال بث واحد. ثم يتم إرسال البيانات إلى خادم الإدارة وتُستخدم لتحديد حدود مجال البث وللتعيين التلقائي لنقاط التوزيع (إذا تم تمكين هذا الخيار).

إذا لم يكن لدى خادم الإدارة وصول مباشر إلى الأجهزة المدارة، لن يتم إرسال طلبات الاتصال من خادم الإدارة إلى هذه الأجهزة مباشرة.

3. يتم نقل المعلومات عن إيقاف تشغيل الأجهزة المدارة من عميل الشبكة إلى خادم الإدارة عبر منفذ UDP رقم 13000.

4. يستقبل خادم الإدارة الاتصال من عملاء الشبكة ومن خوادم الإدارة الثانوية عبر منفذ TLS رقم 13000.

إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر المنفذ رقم 14000 غير مستند إلى TLS. ويدعم Kaspersky Security Center أيضًا اتصال عملاء الشبكة عبر المنفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ TLS رقم 13000.

كان يُطلق على نقطة التوزيع اسم "وكيل التحديث" في الإصدارات السابقة من Kaspersky Security Center.

5. الأجهزة المدارة (باستثناء الأجهزة المحمولة) تتطلب التفعيل عبر منفذ TCP رقم 17000. لكن هذا غير ضروري إذا كان الجهاز يملك صلاحية الوصول إلى الإنترنت الخاصة به، وفي هذه الحالة يرسل الجهاز البيانات إلى خوادم Kaspersky عبر الإنترنت مباشرةً.

6. يتم نقل البيانات من وحدة تحكم الإدارة المستندة إلى MMC إلى خادم الإدارة عبر المنفذ 13291. (يمكن تثبيت وحدة تحكم الإدارة على نفس الجهاز أو على جهاز مختلف.)

7. تتبادل التطبيقات الموجودة على جهاز واحد حركة البيانات المحليَّة (إما على خادم الإدارة أو على جهاز مدار). ولا يتعين فتح أي موانئ خارجية.

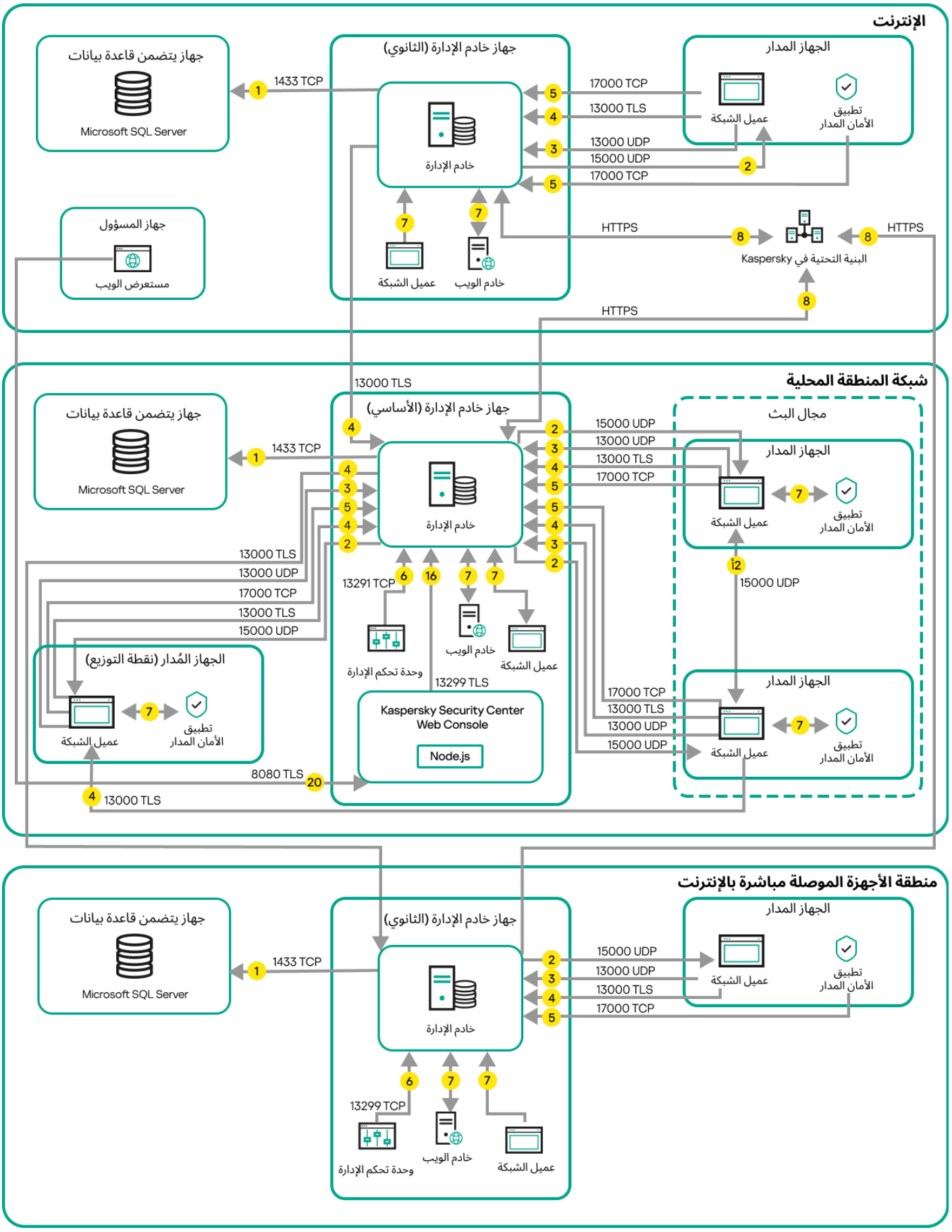
8. يتم نقل البيانات من خادم الإدارة إلى خوادم Kaspersky (مثل: بيانات شبكة KSN أو معلومات عن التراخيص)، والبيانات من خوادم Kaspersky إلى خادم الإدارة (مثل: تحديثات التطبيقات وتحديثات قاعدة بيانات مكافحة الفيروسات) عبر بروتوكول HTTPS.

إذا كنت لا تريد أن يكون لخادم الإدارة الخاص بك اتصالًا بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو على جهاز آخر، عبر منفذ TLS رقم 13299.

خادم الإدارة الرئيسي في شبكة الاتصال المحلية (LAN) وخادما إدارة تابعان

يوضح الشكل أدناه التسلسل الهرمي لخوادم الإدارة: خادم الإدارة الرئيسي في شبكة الاتصال المحلية (LAN). خادم الإدارة الثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)؛ خادم إدارة تابع آخر متصل بالإنترنت.



التسلسل الهرمي لخوادم الإدارة: خادم الإدارة الرئيسي وخادمي إدارة تابعين

تشير الأسهم إلى بدء نقل البيانات: يشير كل سهم من جهاز يبدأ الاتصال إلى الجهاز الذي "يرد" على المكالمة. يتم عرض رقم المنفذ واسم البروتوكول المستخدم لنقل البيانات. لكل سهم تسمية رقمية، وتفاصيل عملية نقل البيانات المقابلة كما يلي:

1. خادم الإدارة يُرسل البيانات إلى قاعدة البيانات. إذا قمت بتثبيت خادم الإدارة وقاعدة البيانات على أجهزة مختلفة، فيجب عليك إتاحة المنافذ الضرورية على الجهاز الموجود به قاعدة البيانات (على سبيل المثال، المنفذ 3306 لخادم MySQL Server أو المنفذ 1433 لخادم Microsoft SQL Server). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

2. يتم تحويل طلبات الاتصال الواردة من خادم الإدارة إلى جميع الأجهزة المدارة غير المحمولة عبر منفذ UDP رقم 15000.

   يرسل عملاء الشبكة طلبات إلى بعضهم البعض ضمن مجال بث واحد. ثم يتم إرسال البيانات إلى خادم الإدارة وتُستخدم لتحديد حدود مجال البث وللتعيين التلقائي لنقاط التوزيع (إذا تم تمكين هذا الخيار).

   إذا لم يكن لدى خادم الإدارة وصول مباشر إلى الأجهزة المدارة، لن يتم إرسال طلبات الاتصال من خادم الإدارة إلى هذه الأجهزة مباشرة.

3. يتم نقل المعلومات عن إيقاف تشغيل الأجهزة المدارة من عميل الشبكة إلى خادم الإدارة عبر منفذ UDP رقم 13000.

4. يستقبل خادم الإدارة الاتصال من عملاء الشبكة ومن خوادم الإدارة الثانوية عبر منفذ TLS رقم 13000.

   إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر المنفذ رقم 14000 غير مستند إلى TLS. ويدعم Kaspersky Security Center أيضًا اتصال عملاء الشبكة عبر المنفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ TLS رقم 13000.

> كان يُطلق على نقطة التوزيع اسم "وكيل التحديث" في الإصدارات السابقة من Kaspersky Security Center.

5. الأجهزة المدارة (باستثناء الأجهزة المحمولة) تتطلب التفعيل عبر منفذ TCP رقم 17000. لكن هذا غير ضروري إذا كان الجهاز يملك صلاحية الوصول إلى الإنترنت الخاصة به، وفي هذه الحالة يرسل الجهاز البيانات إلى خوادم Kaspersky عبر الإنترنت مباشرةً.

6. يتم نقل البيانات من وحدة تحكم الإدارة المستندة إلى MMC إلى خادم الإدارة عبر المنفذ 13291. (يمكن تثبيت وحدة تحكم الإدارة على نفس الجهاز أو على جهاز مختلف.)

7. تتبادل التطبيقات الموجودة على جهاز واحد حركة البيانات المحليَّة (إما على خادم الإدارة أو على جهاز مدار). ولا يتعين فتح أي موانئ خارجية.

8. يتم نقل البيانات من خادم الإدارة إلى خوادم Kaspersky (مثل: بيانات شبكة KSN أو معلومات عن التراخيص)، والبيانات من خوادم Kaspersky إلى خادم الإدارة (مثل: تحديثات التطبيقات وتحديثات قاعدة بيانات مكافحة الفيروسات) عبر بروتوكول HTTPS.

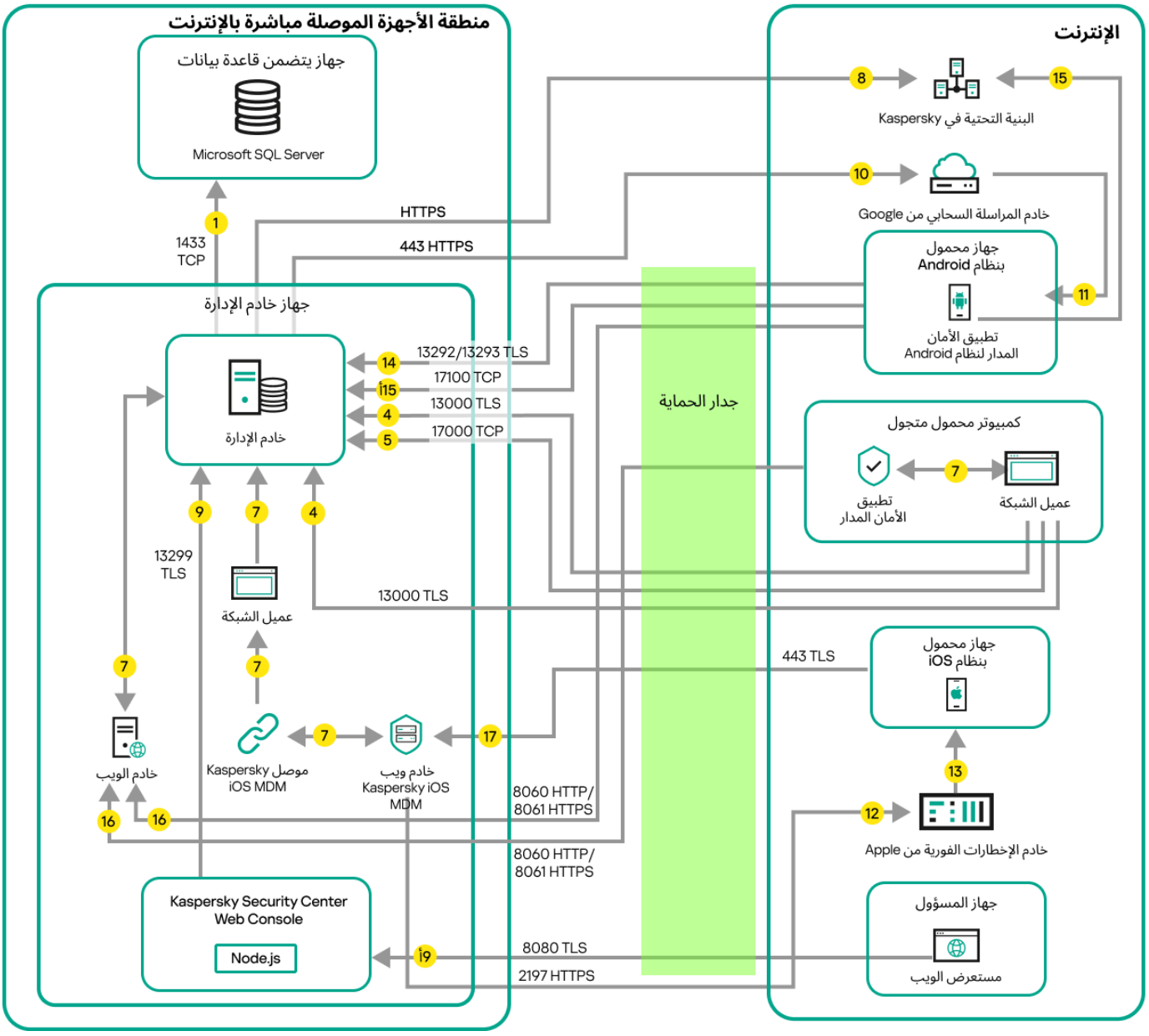
   إذا كنت لا تريد أن يكون لخادم الإدارة الخاص بك اتصالًا بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو على جهاز آخر، عبر منفذ TLS رقم 13299.

   9أ. يتم نقل البيانات من المستعرض، المُثبت على جهاز منفصل للمسؤول، إلى Kaspersky Security Center Web Console Server عبر منفذ TLS رقم 8080. يمكن تثبيت Kaspersky Security Center Web Console Server على خادم الإدارة أو على جهاز آخر.

خادم الإدارة في شبكة الاتصال المحلية (LAN)، الأجهزة المدارة على الإنترنت، الخادم الوكيل العكسي قيد الاستخدام

يوضح الشكل التالي حالة نقل البيانات إذا كان خادم الإدارة موجودًا في شبكة الاتصال المحلية (LAN) وكانت الأجهزة المدارة (بما في ذلك الأجهزة المحمولة) متصلة بالإنترنت. في هذا الشكل، يتم استخدام خادم وكيل عكسي من اختيارك. وارجع إلى وثائق التطبيق للحصول على التفاصيل.



خادم الإدارة الرئيسي في شبكة الاتصال المحلية؛ الأجهزة المدارة تتصل بخادم الإدارة عبر خادم وكيل عكسي

يُوصى بمخطط النشر هذا إذا كنت لا ترغب في أن تتصل الأجهزة المحمولة بخادم الإدارة مباشرةً ولا ترغب في تخصيص بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ).

تشير الأسهم إلى بدء نقل البيانات: يشير كل سهم من جهاز يبدأ الاتصال إلى الجهاز الذي "يرد" على المكالمة. يتم عرض رقم المنفذ واسم البروتوكول المستخدم لنقل البيانات. لكل سهم تسمية رقمية، وتفاصيل عملية نقل البيانات المقابلة كما يلي:

1. خادم الإدارة يُرسل البيانات إلى قاعدة البيانات. إذا قمت بتثبيت خادم الإدارة وقاعدة البيانات على أجهزة مختلفة، فيجب عليك إتاحة المنافذ الضرورية على الجهاز الموجود به قاعدة البيانات (على سبيل المثال، المنفذ 3306 لخادم MySQL Server أو المنفذ 1433 لخادم Microsoft SQL Server). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

2. يتم تحويل طلبات الاتصال الواردة من خادم الإدارة إلى جميع الأجهزة المدارة غير المحمولة عبر منفذ UDP رقم 15000.

   يرسل عملاء الشبكة طلبات إلى بعضهم البعض ضمن مجال بث واحد. ثم يتم إرسال البيانات إلى خادم الإدارة وتُستخدم لتحديد حدود مجال البث وللتعيين التلقائي لنقاط التوزيع (إذا تم تمكين هذا الخيار).

   إذا لم يكن لدى خادم الإدارة وصول مباشر إلى الأجهزة المدارة، لن يتم إرسال طلبات الاتصال من خادم الإدارة إلى هذه الأجهزة مباشرة.

3. يتم نقل المعلومات عن إيقاف تشغيل الأجهزة المدارة من عميل الشبكة إلى خادم الإدارة عبر منفذ UDP رقم 13000.

4. يستقبل خادم الإدارة الاتصال من عملاء الشبكة ومن خوادم الإدارة الثانوية عبر منفذ TLS رقم 13000.

   إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر المنفذ رقم 14000 غير مستند إلى TLS. ويدعم Kaspersky Security Center أيضًا اتصال عملاء الشبكة عبر المنفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ TLS رقم 13000.

كان يُطلق على نقطة التوزيع اسم "وكيل التحديث" في الإصدارات السابقة من Kaspersky Security Center.

5. الأجهزة المدارة (باستثناء الأجهزة المحمولة) تتطلب التفعيل عبر منفذ TCP رقم 17000. لكن هذا غير ضروري إذا كان الجهاز يملك صلاحية الوصول إلى الإنترنت الخاصة به، وفي هذه الحالة يرسل الجهاز البيانات إلى خوادم Kaspersky عبر الإنترنت مباشرةً.

6. يتم نقل البيانات من وحدة تحكم الإدارة المستندة إلى MMC إلى خادم الإدارة عبر المنفذ 13291. (يمكن تثبيت وحدة تحكم الإدارة على نفس الجهاز أو على جهاز مختلف.)

7. تتبادل التطبيقات الموجودة على جهاز واحد حركة البيانات المحليَّة (إما على خادم الإدارة أو على جهاز مدار). ولا يتعين فتح أي موانئ خارجية.

8. يتم نقل البيانات من خادم الإدارة إلى خوادم Kaspersky (مثل: بيانات شبكة KSN أو معلومات عن التراخيص)، والبيانات من خوادم Kaspersky إلى خادم الإدارة (مثل: تحديثات التطبيقات وتحديثات قاعدة بيانات مكافحة الفيروسات) عبر بروتوكول HTTPS.

   إذا كنت لا تريد أن يكون لخادم الإدارة الخاص بك اتصالًا بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو على جهاز آخر، عبر منفذ TLS رقم 13299.

   9أ. يتم نقل البيانات من المستعرض، المُثبت على جهاز منفصل للمسؤول، إلى Kaspersky Security Center Web Console Server عبر منفذ TLS رقم 8080. يمكن تثبيت Kaspersky Security Center Web Console Server على خادم الإدارة أو على جهاز آخر.

10. بالنسبة إلى أجهزة Android المحمولة فقط: يتم نقل البيانات من خادم الإدارة إلى خوادم Google. يُستخدم الاتصال لإبلاغ أجهزة Android المحمولة أنه يجب عليها الاتصال بخادم الإدارة. ثم تُرسل الإشعارات الفورية إلى الأجهزة المحمولة.

11. بالنسبة إلى أجهزة Android المحمولة فقط: تُرسل الإشعارات الفورية من خوادم Google إلى الجهاز المحمول. يُستخدم الاتصال لإبلاغ الأجهزة المحمولة أنه يجب عليها الاتصال بخادم الإدارة.

12. بالنسبة لأجهزة iOS المحمولة فقط: يتم نقل البيانات من خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM إلى خوادم Apple Push Notification. ثم تُرسل الإشعارات الفورية إلى الأجهزة المحمولة.

13. بالنسبة لأجهزة iOS المحمولة فقط: يتم إرسال الإشعارات الفورية من خوادم Apple إلى الجهاز المحمول. يُستخدم الاتصال لإبلاغ الأجهزة المحمولة أنه iOS يجب عليها الاتصال بخادم الإدارة.

14. للأجهزة المحمولة فقط: يتم نقل البيانات من التطبيق المدار إلى خادم الإدارة (أو إلى بوابة الاتصال) عبر منفذ TLS رقم 13293 / 13292— مباشرة أو عبر خادم وكيل عكسي.

15. بالنسبة إلى الأجهزة المحمولة فقط: يتم نقل البيانات من الجهاز المحمول إلى بنية Kaspersky التحتية.

إذا كان الجهاز المحمول لا يملك صلاحية الوصول إلى الإنترنت، تُرسَل البيانات إلى خادم الإدارة عبر منفذ 17100 ثم يُرسلها خادم الإدارة إلى بنية Kaspersky التحتية، ولكن لا يُستخدم هذا السيناريو إلا فيما ندر.

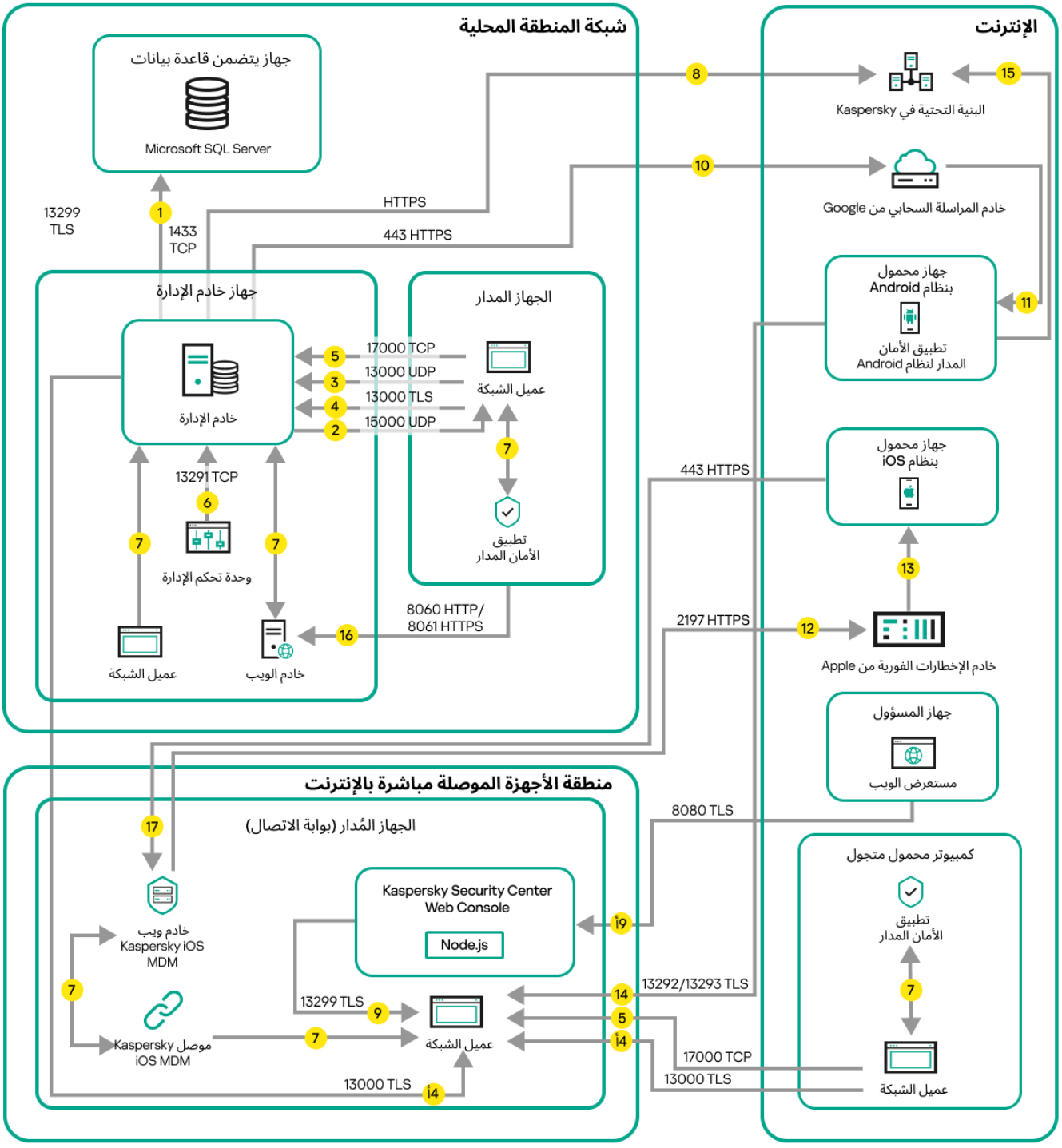
16. يتم نقل طلبات الحزَم من الأجهزة المدارة، وتشمل الأجهزة المحمولة، إلى خادم الويب الموجود على الجهاز نفسه الذي به خادم الإدارة.

17. بالنسبة لأجهزة iOS المحمولة فقط: يتم نقل البيانات من الجهاز المحمول عبر منفذ TLS رقم 443 إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، المثبَّت على الجهاز نفسه المثبَّت عليه خادم الإدارة أو على بوابة الاتصال.

خادم الإدارة في شبكة الاتصال المحلية (LAN)، الأجهزة المدارة متصلة بالإنترنت، بوابة الاتصال قيد الاستخدام

يوضح الشكل التالي حالة نقل البيانات إذا كان خادم الإدارة موجودًا في شبكة الاتصال المحلية (LAN) وكانت الأجهزة المدارة (بما في ذلك الأجهزة المحمولة) متصلة بالإنترنت. بوابة الاتصال قيد الاستخدام.

يوصى باستخدام نظام النشر هذا إذا كنت لا تريد أن تتصل الأجهزة المحمولة بخادم الإدارة مباشرة ولا تريد استخدام خادم وكيل عكسي أو جدار حماية خاص بالشركة.



تتصل الأجهزة المحمولة المدارة بخادم الإدارة عبر بوابة اتصال

في هذا الشكل، تتصل الأجهزة المدارة بخادم الإدارة عبر بوابة اتصال موجودة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ). لا يوجد خادم وكيل عكسي أو جدار حماية خاص بالشركة قيد الاستخدام.

تشير الأسهم إلى بدء نقل البيانات: يشير كل سهم من جهاز يبدأ الاتصال إلى الجهاز الذي "يرد" على المكالمة. يتم عرض رقم المنفذ واسم البروتوكول المستخدم لنقل البيانات. لكل سهم تسمية رقمية، وتفاصيل عملية نقل البيانات المقابلة كما يلي:

1. خادم الإدارة يُرسل البيانات إلى قاعدة البيانات. إذا قمت بتثبيت خادم الإدارة وقاعدة البيانات على أجهزة مختلفة، فيجب عليك إتاحة المنافذ الضرورية على الجهاز الموجود به قاعدة البيانات (على سبيل المثال، المنفذ 3306 لخادم MySQL Server أو المنفذ 1433 لخادم Microsoft SQL Server). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

2. يتم تحويل طلبات الاتصال الواردة من خادم الإدارة إلى جميع الأجهزة المدارة غير المحمولة عبر منفذ UDP رقم 15000.

   يرسل عملاء الشبكة طلبات إلى بعضهم البعض ضمن مجال بث واحد. ثم يتم إرسال البيانات إلى خادم الإدارة وتُستخدم لتحديد حدود مجال البث وللتعيين التلقائي لنقاط التوزيع (إذا تم تمكين هذا الخيار).

   إذا لم يكن لدى خادم الإدارة وصول مباشر إلى الأجهزة المدارة، لن يتم إرسال طلبات الاتصال من خادم الإدارة إلى هذه الأجهزة مباشرة.

3. يتم نقل المعلومات عن إيقاف تشغيل الأجهزة المدارة من عميل الشبكة إلى خادم الإدارة عبر منفذ UDP رقم 13000.

4. يستقبل خادم الإدارة الاتصال من عملاء الشبكة ومن خوادم الإدارة الثانوية عبر منفذ TLS رقم 13000.

   إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر المنفذ رقم 14000 غير مستند إلى TLS. ويدعم Kaspersky Security Center أيضًا اتصال عملاء الشبكة عبر المنفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ TLS رقم 13000.

كان يُطلق على نقطة التوزيع اسم "وكيل التحديث" في الإصدارات السابقة من Kaspersky Security Center.

4أ. تستقبل بوابة الاتصال الموجودة في منطقة الأجهزة الموصلة مباشرة بالإنترنت اتصالًا من خادم الإدارة عبر منفذ TLS رقم 13000. نظرًا لأن بوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت لا يمكنها الوصول إلى منافذ خادم الإدارة، ينشئ خادم الإدارة اتصال إشارة دائمًا مع بوابة اتصال ويحافظ عليه. لا يتم استخدام اتصال الإشارة لنقل البيانات؛ يتم استخدامه فقط لإرسال دعوة إلى تفاعل الشبكة. عندما تحتاج بوابة الاتصال إلى الاتصال بالخادم، فإنها تقوم بإعلام الخادم من خلال اتصال الإشارة هذا، ثم يقوم الخادم بإنشاء الاتصال المطلوب لنقل البيانات.

   تتصل الأجهزة خارج المكتب ببوابة الاتصال عبر منفذ TLS رقم 13000 أيضًا.

5. الأجهزة المدارة (باستثناء الأجهزة المحمولة) تتطلب التفعيل عبر منفذ TCP رقم 17000. لكن هذا غير ضروري إذا كان الجهاز يملك صلاحية الوصول إلى الإنترنت الخاصة به، وفي هذه الحالة يرسل الجهاز البيانات إلى خوادم Kaspersky عبر الإنترنت مباشرةً.

6. يتم نقل البيانات من وحدة تحكم الإدارة المستندة إلى MMC إلى خادم الإدارة عبر المنفذ 13291. (يمكن تثبيت وحدة تحكم الإدارة على نفس الجهاز أو على جهاز مختلف.)

7. تتبادل التطبيقات الموجودة على جهاز واحد حركة البيانات المحليَّة (إما على خادم الإدارة أو على جهاز مدار). ولا يتعين فتح أي موانئ خارجية.

8. يتم نقل البيانات من خادم الإدارة إلى خوادم Kaspersky (مثل: بيانات شبكة KSN أو معلومات عن التراخيص)، والبيانات من خوادم Kaspersky إلى خادم الإدارة (مثل: تحديثات التطبيقات وتحديثات قاعدة بيانات مكافحة الفيروسات) عبر بروتوكول HTTPS.

   إذا كنت لا تريد أن يكون لخادم الإدارة الخاص بك اتصالًا بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو على جهاز آخر، عبر منفذ TLS رقم 13299.

   9أ. يتم نقل البيانات من المستعرض، المُثبت على جهاز منفصل للمسؤول، إلى Kaspersky Security Center Web Console Server عبر منفذ TLS رقم 8080. يمكن تثبيت Kaspersky Security Center Web Console Server على خادم الإدارة أو على جهاز آخر.

10. بالنسبة إلى أجهزة Android المحمولة فقط: يتم نقل البيانات من خادم الإدارة إلى خوادم Google. يُستخدم الاتصال لإبلاغ أجهزة Android المحمولة أنه يجب عليها الاتصال بخادم الإدارة. ثم تُرسل الإشعارات الفورية إلى الأجهزة المحمولة.

11. بالنسبة إلى أجهزة Android المحمولة فقط: تُرسل الإشعارات الفورية من خوادم Google إلى الجهاز المحمول. يُستخدم الاتصال لإبلاغ الأجهزة المحمولة أنه يجب عليها الاتصال بخادم الإدارة.

12. بالنسبة لأجهزة iOS المحمولة فقط: يتم نقل البيانات من خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM إلى خوادم Apple Push Notification. ثم تُرسل الإشعارات الفورية إلى الأجهزة المحمولة.

13. بالنسبة لأجهزة iOS المحمولة فقط: يتم إرسال الإشعارات الفورية من خوادم Apple إلى الجهاز المحمول. يُستخدم الاتصال لإبلاغ الأجهزة المحمولة أنه iOS يجب عليها الاتصال بخادم الإدارة.

14. للأجهزة المحمولة فقط: يتم نقل البيانات من التطبيق المدار إلى خادم الإدارة (أو إلى بوابة الاتصال) عبر منفذ TLS رقم 13293 / 13292— مباشرة أو عبر خادم وكيل عكسي.

15. بالنسبة إلى الأجهزة المحمولة فقط: يتم نقل البيانات من الجهاز المحمول إلى بنية Kaspersky التحتية.

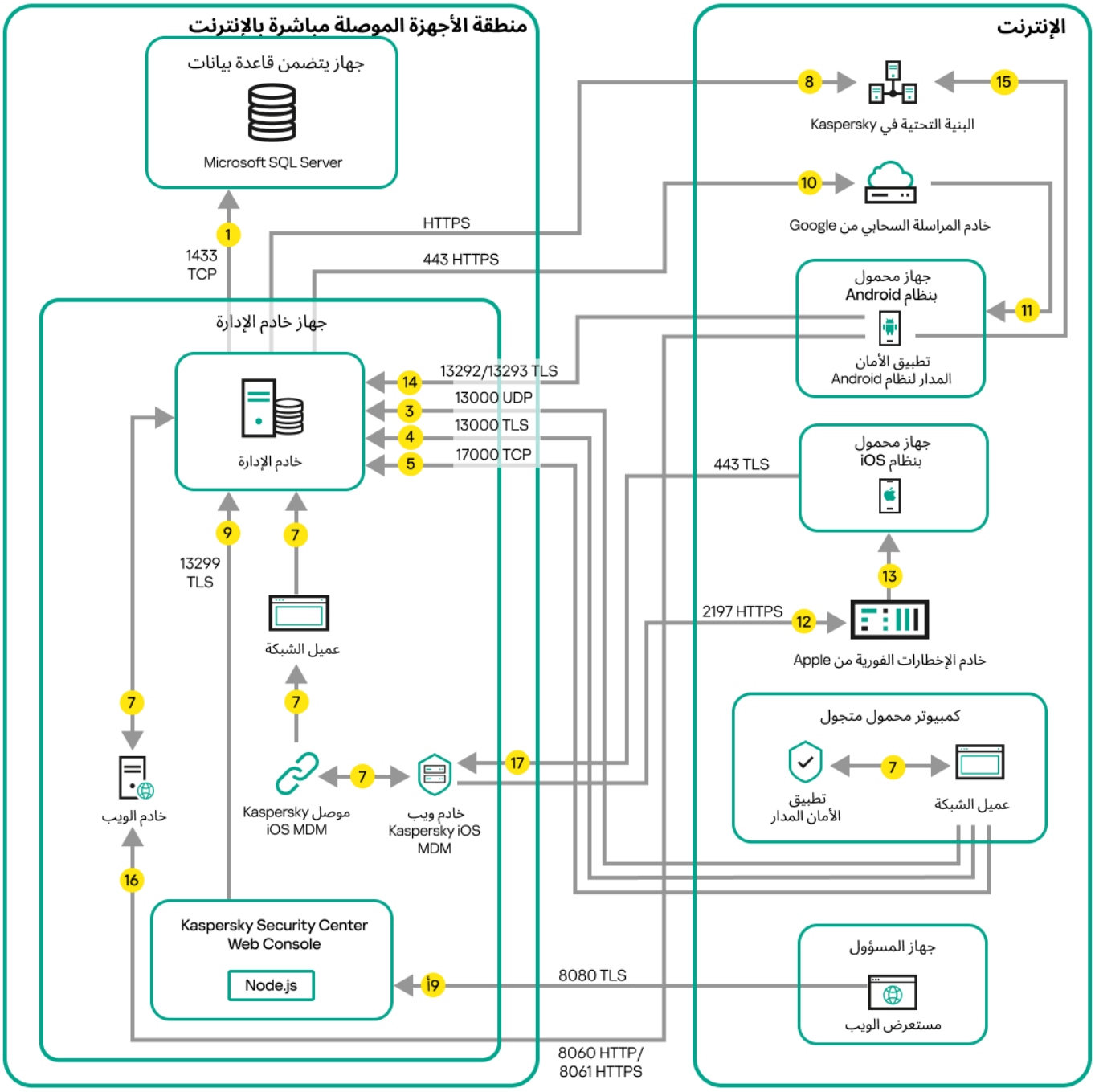
إذا كان الجهاز المحمول لا يملك صلاحية الوصول إلى الإنترنت، تُرسَل البيانات إلى خادم الإدارة عبر منفذ 17100 ثم يُرسلها خادم الإدارة إلى بنية Kaspersky التحتية، ولكن لا يُستخدم هذا السيناريو إلا فيما ندر.

16. يتم نقل طلبات الحزَم من الأجهزة المدارة، وتشمل الأجهزة المحمولة، إلى خادم الويب الموجود على الجهاز نفسه الذي به خادم الإدارة.

17. بالنسبة لأجهزة iOS المحمولة فقط: يتم نقل البيانات من الجهاز المحمول عبر منفذ TLS رقم 443 إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، المثبَّت على الجهاز نفسه المثبَّت عليه خادم الإدارة أو على بوابة الاتصال.

خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، الأجهزة المدارة متصلة بالإنترنت

يوضح الشكل التالي حالة نقل البيانات إذا كان خادم الإدارة موجودًا في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ) وكانت الأجهزة المدارة بما في ذلك الأجهزة المحمولة متصلة بالإنترنت.



خادم الإدارة في منطقة عازلة، أجهزة محمولة مدارة متصلة بالإنترنت

في هذا الشكل، لا توجد بوابة اتصال قيد الاستخدام: تتصل الأجهزة المحمولة بخادم الإدارة مباشرةً.

تشير الأسهم إلى بدء نقل البيانات: يشير كل سهم من جهاز يبدأ الاتصال إلى الجهاز الذي "يرد" على المكالمة. يتم عرض رقم المنفذ واسم البروتوكول المستخدم لنقل البيانات. لكل سهم تسمية رقمية، وتفاصيل عملية نقل البيانات المقابلة كما يلي:

1. خادم الإدارة يُرسل البيانات إلى قاعدة البيانات. إذا قمت بتثبيت خادم الإدارة وقاعدة البيانات على أجهزة مختلفة، فيجب عليك إتاحة المنافذ الضرورية على الجهاز الموجود به قاعدة البيانات (على سبيل المثال، المنفذ 3306 لخادم MySQL Server أو المنفذ 1433 لخادم Microsoft SQL Server). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

2. يتم تحويل طلبات الاتصال الواردة من خادم الإدارة إلى جميع الأجهزة المدارة غير المحمولة عبر منفذ UDP رقم 15000.

   يرسل عملاء الشبكة طلبات إلى بعضهم البعض ضمن مجال بث واحد. ثم يتم إرسال البيانات إلى خادم الإدارة وتُستخدم لتحديد حدود مجال البث وللتعيين التلقائي لنقاط التوزيع (إذا تم تمكين هذا الخيار).

   إذا لم يكن لدى خادم الإدارة وصول مباشر إلى الأجهزة المدارة، لن يتم إرسال طلبات الاتصال من خادم الإدارة إلى هذه الأجهزة مباشرة.

3. يتم نقل المعلومات عن إيقاف تشغيل الأجهزة المدارة من عميل الشبكة إلى خادم الإدارة عبر منفذ UDP رقم 13000.

4. يستقبل خادم الإدارة الاتصال من عملاء الشبكة ومن خوادم الإدارة الثانوية عبر منفذ TLS رقم 13000.

   إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر المنفذ رقم 14000 غير مستند إلى TLS. ويدعم Kaspersky Security Center أيضًا اتصال عملاء الشبكة عبر المنفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ TLS رقم 13000.

كان يُطلق على نقطة التوزيع اسم "وكيل التحديث" في الإصدارات السابقة من Kaspersky Security Center.

5. الأجهزة المدارة (باستثناء الأجهزة المحمولة) تتطلب التفعيل عبر منفذ TCP رقم 17000. لكن هذا غير ضروري إذا كان الجهاز يملك صلاحية الوصول إلى الإنترنت الخاصة به، وفي هذه الحالة يرسل الجهاز البيانات إلى خوادم Kaspersky عبر الإنترنت مباشرةً.

6. يتم نقل البيانات من وحدة تحكم الإدارة المستندة إلى MMC إلى خادم الإدارة عبر المنفذ 13291. (يمكن تثبيت وحدة تحكم الإدارة على نفس الجهاز أو على جهاز مختلف.)

7. تتبادل التطبيقات الموجودة على جهاز واحد حركة البيانات المحليَّة (إما على خادم الإدارة أو على جهاز مدار). ولا يتعين فتح أي موانئ خارجية.

8. يتم نقل البيانات من خادم الإدارة إلى خوادم Kaspersky (مثل: بيانات شبكة KSN أو معلومات عن التراخيص)، والبيانات من خوادم Kaspersky إلى خادم الإدارة (مثل: تحديثات التطبيقات وتحديثات قاعدة بيانات مكافحة الفيروسات) عبر بروتوكول HTTPS.

   إذا كنت لا تريد أن يكون لخادم الإدارة الخاص بك اتصالًا بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو على جهاز آخر، عبر منفذ TLS رقم 13299.

   9أ. يتم نقل البيانات من المستعرض، المُثبت على جهاز منفصل للمسؤول، إلى Kaspersky Security Center Web Console Server عبر منفذ TLS رقم 8080. يمكن تثبيت Kaspersky Security Center Web Console Server على خادم الإدارة أو على جهاز آخر.

10. بالنسبة إلى أجهزة Android المحمولة فقط: يتم نقل البيانات من خادم الإدارة إلى خوادم Google. يُستخدم الاتصال لإبلاغ أجهزة Android المحمولة أنه يجب عليها الاتصال بخادم الإدارة. ثم تُرسل الإشعارات الفورية إلى الأجهزة المحمولة.

11. بالنسبة إلى أجهزة Android المحمولة فقط: تُرسل الإشعارات الفورية من خوادم Google إلى الجهاز المحمول. يُستخدم الاتصال لإبلاغ الأجهزة المحمولة أنه يجب عليها الاتصال بخادم الإدارة.

12. بالنسبة لأجهزة iOS المحمولة فقط: يتم نقل البيانات من خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM إلى خوادم Apple Push Notification. ثم تُرسل الإشعارات الفورية إلى الأجهزة المحمولة.

13. بالنسبة لأجهزة iOS المحمولة فقط: يتم إرسال الإشعارات الفورية من خوادم Apple إلى الجهاز المحمول. يُستخدم الاتصال لإبلاغ الأجهزة المحمولة أنه iOS يجب عليها الاتصال بخادم الإدارة.

14. للأجهزة المحمولة فقط: يتم نقل البيانات من التطبيق المدار إلى خادم الإدارة (أو إلى بوابة الاتصال) عبر منفذ TLS رقم 13293 / 13292— مباشرة أو عبر خادم وكيل عكسي.

15. بالنسبة إلى الأجهزة المحمولة فقط: يتم نقل البيانات من الجهاز المحمول إلى بنية Kaspersky التحتية.

إذا كان الجهاز المحمول لا يملك صلاحية الوصول إلى الإنترنت، تُرسَل البيانات إلى خادم الإدارة عبر منفذ 17100 ثم يُرسلها خادم الإدارة إلى بنية Kaspersky التحتية، ولكن لا يُستخدم هذا السيناريو إلا فيما ندر.

16. يتم نقل طلبات الحزَم من الأجهزة المدارة، وتشمل الأجهزة المحمولة، إلى خادم الويب الموجود على الجهاز نفسه الذي به خادم الإدارة.

17. بالنسبة لأجهزة iOS المحمولة فقط: يتم نقل البيانات من الجهاز المحمول عبر منفذ TLS رقم 443 إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، المثبَّت على الجهاز نفسه المثبَّت عليه خادم الإدارة أو على بوابة الاتصال.

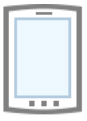
التفاعل مع مكونات Kaspersky Security Center وتطبيقات الأمان: مزيد من المعلومات

يوفر هذا القسم مخططات التفاعل مع مكونات Kaspersky Security Center وتطبيقات الأمان المُدارة. توفر المخططات عدد المنافذ التي يجب توفرها وأسماء العمليات التي تفتح هذه المنافذ.

الاصطلاحات المستخدمة في مخططات التفاعل

يوفر الجدول التالي المصطلحات المستخدمة عبر المخططات.

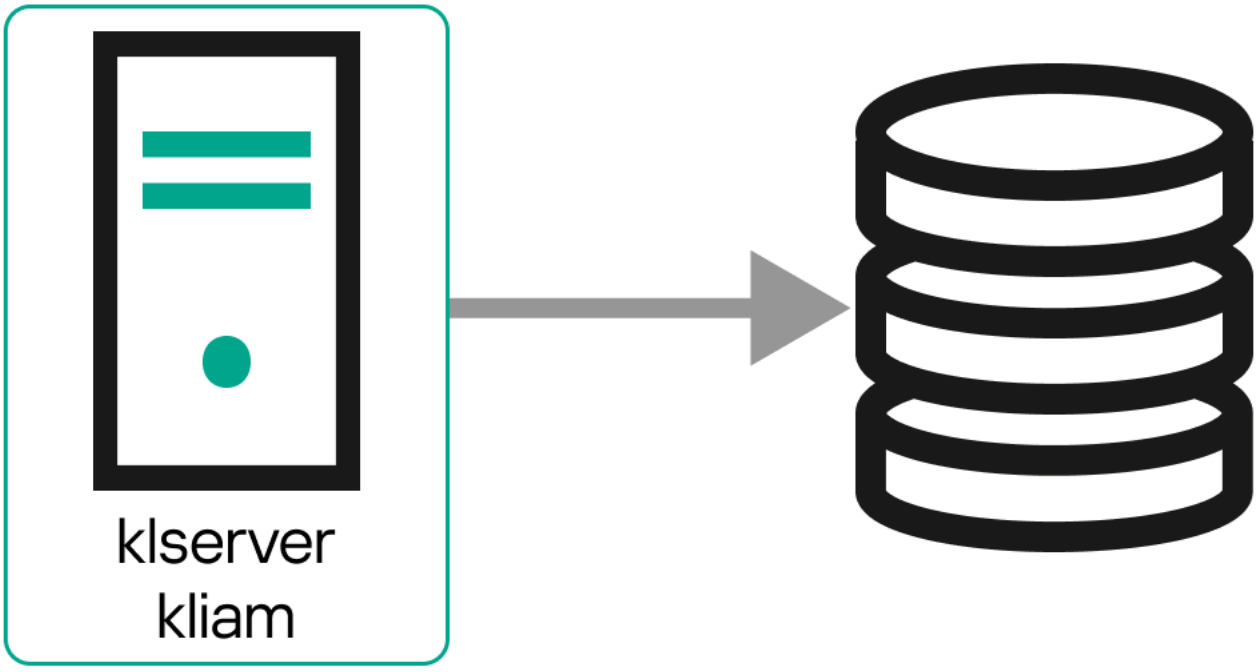
مصطلحات المستندات

الرمز	المعنى
	خادم الإدارة
	خادم الإدارة الثانوي
	نظام إدارة قاعدة البيانات
	جهاز عميل (يحتوي على عميل الشبكة وتطبيق مثبّت من عائلة Kaspersky Endpoint Security أو يحتوي على تطبيق أمان مختلف يمكن لـ Kaspersky Security Center إدارته)
	بوابة الاتصال
	نقطة توزيع
	جهاز عميل محمول عليه Kaspersky Security for Mobile

	المستعرض على جهاز المستخدم
klnagent	عملية تعمل على الجهاز وتفتح منفذًا
13000 TLS	المنفذ ورقمه
	حركة مرور TCP (اتجاه السهم الذي يوضح اتجاه تدفق حركة المرور)
	حركة مرور UDP (اتجاه السهم الذي يوضح اتجاه تدفق حركة المرور)
	استدعاء COM
	نقل نظام إدارة قواعد البيانات
	حد منطقة الأجهزة الموصلة مباشرة بالإنترنت

خادم الإدارة ونظام إدارة قواعد البيانات

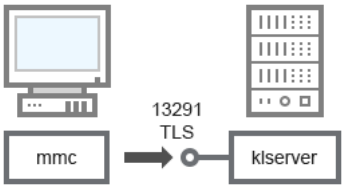
البيانات من خادم الإدارة تدخل قاعدة بيانات SQL Server أو MySQL أو MariaDB.



خادم الإدارة ونظام إدارة قواعد البيانات

إذا قمت بتثبيت خادم الإدارة وقاعدة البيانات على أجهزة مختلفة، فيجب عليك إتاحة المنافذ الضرورية على الجهاز الموجود به قاعدة البيانات (على سبيل المثال، المنفذ 3306 لخادم MySQL Server أو المنفذ 1433 لخادم Microsoft SQL Server). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

خادم الإدارة ووحدة تحكم الإدارة



خادم الإدارة ووحدة تحكم الإدارة

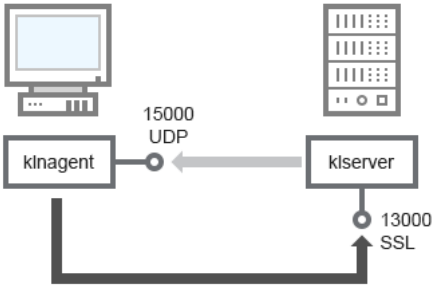
للحصول على توضيحات للمخطط، راجع الجدول أدناه.

خادم الإدارة ووحدة تحكم الإدارة (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
خادم الإدارة	13291	klserver	TCP	نعم	تلقي اتصالات من وحدة تحكم الإدارة

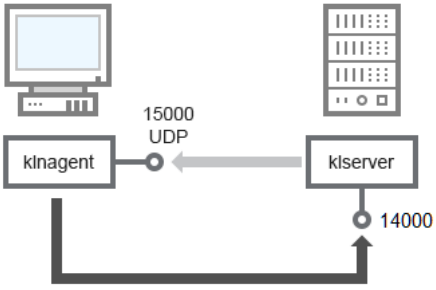
خادم الإدارة والجهاز العميل: إدارة تطبيق الأمان

يتلقى خادم الإدارة الاتصال من عملاء الشبكة عبر منفذ 13000 SSL (راجع الشكل الموضح أدناه).



خادم الإدارة والجهاز العميل: إدارة تطبيق الأمان، الاتصال عبر المنفذ 13000 (مستحسن)

إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر منفذ 14000 غير مستند إلى SSL (راجع الشكل الموضح أدناه). يدعم Kaspersky Security Center 15.1 أيضًا اتصال عملاء الشبكة عبر المنفذ 14000، على الرغم من أنه من المستحسن استخدام منفذ SSL رقم 13000.



خادم الإدارة والجهاز العميل: إدارة تطبيق الأمان والاتصال عبر منفذ 14000 (أمان أقل)

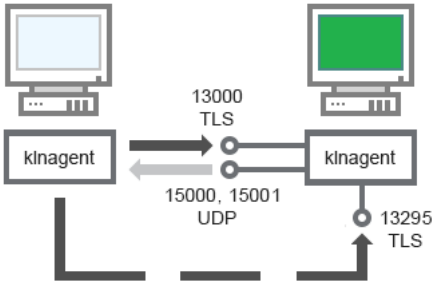
لتوضيح المخططات، راجع الجدول الموضح أدناه.

خادم الإدارة والجهاز العميل: إدارة تطبيق الأمان (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS (لمنافذ TCP فقط)	غرض المنفذ
عميل الشبكة	15000	klnagent	UDP	خالٍ	الإرسال المتعدد لعملاء الشبكة
خادم الإدارة	13000	klserver	TCP	نعم	تلقي اتصالات من عملاء الشبكة
خادم الإدارة	14000	klserver	TCP	لا	تلقي اتصالات من عملاء الشبكة

ترقية البرنامج على جهاز عميل خلال نقطة توزيع

يتصل الجهاز العميل بنقطة التوزيع عبر المنفذ 13000، وإذا كنت تستخدم أيضًا نقطة التوزيع كخادم إرسال عبر المنفذ 13295؛ نقطة التوزيع المتعددة لعملاء الشبكة عبر المنفذ 15000 (انظر الشكل أدناه). يتم استلام حزم التحديثات والتثبيت من نقطة توزيع عبر المنفذ 15001.



ترقية البرنامج على جهاز عميل خلال نقطة توزيع

للحصول على توضيحات للمخطط، راجع الجدول أدناه.

ترقية برنامج من خلال نقطة توزيع (حركة المرور)

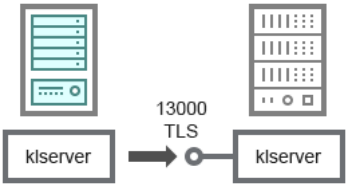
الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS (لمنافذ TCP فقط)	غرض المنفذ
عميل الشبكة	15000	klnagent	UDP	خالٍ	الإرسال المتعدد لعملاء الشبكة
عميل الشبكة	15001	klnagent	UDP	خالٍ	استلام التحديثات وحزم التثبيت من نقطة التوزيع
نقطة توزيع	13000	klnagent	TCP	نعم	تلقي اتصالات من عملاء الشبكة
نقطة توزيع	13295	klnagent	TCP	نعم	استقبال الاتصالات من أجهزة العميل (عن طريق خادم الإرسال)

التسلسل الهرمي لخوادم الإدارة: خادم الإدارة الرئيسي وخادم الإدارة الثانوي

يعرض المخطط (راجع الشكل الموضح أدناه) كيفية استخدام المنفذ 13000 لضمان التفاعل بين خوادم الإدارة المجتمعة في تسلسل هرمي.

عند الجمع بين خادمي إدارة في تسلسل هرمي، تأكد من أنه يمكن الوصول إلى المنفذ 13291 على خادمي الإدارة كليهما. تتصل وحدة تحكم الإدارة بخادم الإدارة عبر المنفذ 13291.

وبالتالي، عند الجمع بين خوادم الإدارة في تسلسل هرمي، ستكون قادرًا على إدارة كلاً منهما باستخدام وحدة تحكم إدارة متصلة بخادم الإدارة الرئيسي. لذلك، فإن إمكانية الوصول إلى المنفذ 13291 الخاص بالخادم الرئيسي هو المتطلب الأساسي الوحيد.



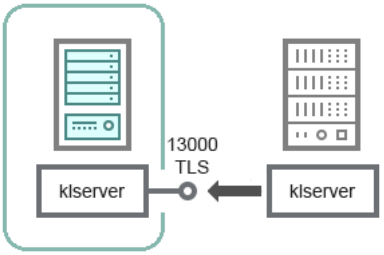
التسلسل الهرمي لخوادم الإدارة: خادم الإدارة الرئيسي وخادم الإدارة الثانوي

للحصول على توضيحات للمخطط، راجع الجدول أدناه.

التسلسل الهرمي لخوادم الإدارة (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
خادم الإدارة الرئيسي	13000	klserver	TCP	نعم	تلقي اتصالات من خوادم إدارة ثانوية

التسلسل الهرمي لخوادم الإدارة مع خادم إدارة تابع في منطقة الأجهزة الموصلة مباشرة بالإنترنت



التسلسل الهرمي لخوادم الإدارة مع خادم إدارة تابع في DMZ

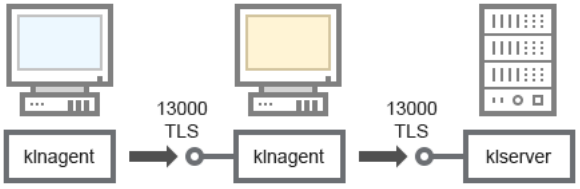
يعرض المخطط تسلسل رقمي لخوادم الإدارة والذي يقوم فيه خادم الإدارة الثانوي الموجودة في منطقة الأجهزة الموصلة مباشرة بالإنترنت بتلقي اتصال من خادم الإدارة الرئيسي (راجع الجدول أدناه لمطالعة توضيحات المخطط). عند الجمع بين خادمي إدارة في تسلسل هرمي، تأكد من أنه يمكن الوصول إلى المنفذ 13291 على خادمي الإدارة كليهما. تتصل وحدة تحكم الإدارة بخادم الإدارة عبر المنفذ 13291.

وبالتالي، عند الجمع بين خوادم الإدارة في تسلسل هرمي، ستكون قادرًا على إدارة كلاً منهما باستخدام وحدة تحكم إدارة متصلة بخادم الإدارة الرئيسي. لذلك، فإن إمكانية الوصول إلى المنفذ 13291 الخاص بالخادم الرئيسي هو المتطلب الأساسي الوحيد.

التسلسل الهرمي لخوادم الإدارة مع خادم إدارة تابع في منطقة الأجهزة الموصلة مباشرة بالإنترنت (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
خادم الإدارة الثانوي	13000	klserver	TCP	نعم	تلقي اتصالات من خادم الإدارة الرئيسي

خادم الإدارة وبوابة اتصال في قطاع شبكة وجهاز عميل



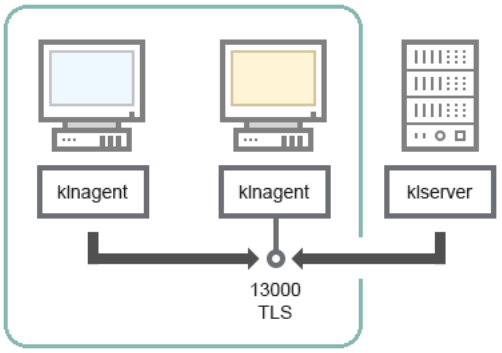
خادم الإدارة وبوابة اتصال في قطاع شبكة وجهاز عميل

للحصول على توضيحات للمخطط، راجع الجدول أدناه.

خادم الإدارة وبوابة اتصال في قطاع شبكة وجهاز عميل(حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
خادم الإدارة	13000	klserver	TCP	نعم	تلقي اتصالات من عملاء الشبكة
عميل الشبكة	13000	klnagent	TCP	نعم	تلقي اتصالات من عملاء الشبكة

خادم الإدارة وجهازان في منطقة الأجهزة الموصلة مباشرة بالإنترنت: بوابة الاتصال وجهاز عميل



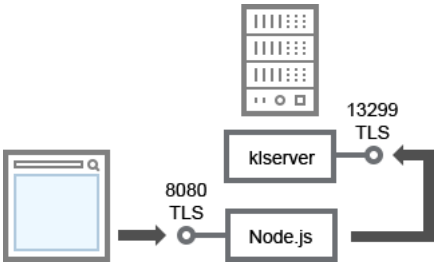
خادم إدارة مع بوابة اتصال وجهاز عميل في DMZ

للحصول على توضيحات للمخطط، راجع الجدول أدناه.

خادم الإدارة مع بوابة اتصال في قطاع شبكة وجهاز عميل (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
عميل الشبكة	13000	klnagent	TCP	نعم	تلقي اتصالات من عملاء الشبكة

خادم الإدارة وKaspersky Security Center Web Console



خادم الإدارة وKaspersky Security Center Web Console

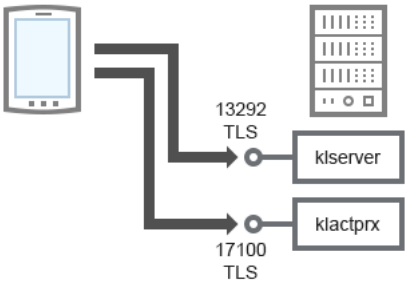
للحصول على توضيحات للمخطط، راجع الجدول أدناه.

خادم الإدارة وKaspersky Security Center Web Console (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
خادم الإدارة	13299	klserver	TCP	نعم	تلقي اتصالات من Kaspersky Security Center Web Console إلى خادم الإدارة عبر OpenAPI
Kaspersky Security Center Web Console أو خادم الإدارة	8080	Node.js: جافا سكريبت من جانب الخادم	TCP	نعم	تلقي اتصالات من Kaspersky Security Center Web Console

يمكن تثبيت Kaspersky Security Center Web Console على خادم الإدارة أو على جهاز أخر.

تفعيل وإدارة تطبيق الأمان على جهاز محمول



تفعيل وإدارة تطبيق الأمان على جهاز محمول

للحصول على توضيحات للمخطط، راجع الجدول أدناه.

تنشيط وإدارة تطبيق الأمان على جهاز محمول (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
خادم الإدارة	13292	klserver	TCP	نعم	تلقي اتصالات من وحدة تحكم الإدارة إلى خادم الإدارة
خادم الإدارة	17100	klactprx	TCP	نعم	تلقي اتصالات لتفعيل التطبيق من الأجهزة المحمولة

أفضل ممارسات النشر

يُعتبر Kaspersky Security Center تطبيقًا موزَّعًا. يشمل Kaspersky Security Center التطبيقات التالية:

- خادم الإدارة—وهو المكوّن الرئيسي، تم تصميمه لإدارة أجهزة إحدى المؤسسات وتخزين البيانات في نظام إدارة قواعد البيانات.
- وحدة تحكم الإدارة—الأداة الأساسية للمسؤول. يتم شحن وحدة تحكم الإدارة مع خادم الإدارة، ولكن يمكن تثبيتها بشكل فردي على جهاز واحد أو أجهزة متعددة يشغّلها المسؤول.
- عميل الشبكة —تم تصميمه لإدارة تطبيق الأمان المُثبّت على أحد الأجهزة، بالإضافة إلى الحصول على معلومات حول هذا الجهاز ونقل هذه المعلومات إلى خادم الإدارة. يتم تثبيت عملاء الشبكة على أجهزة مؤسسة ما.

يتم القيام بنشر Kaspersky Security Center على شبكة المؤسسة كما يلي:

- تثبيت خادم الإدارة
- تثبيت وحدة تحكم الإدارة على جهاز المسؤول
- تثبيت عميل الشبكة وتطبيق الأمان على أجهزة المؤسسة

دليل التقوية

تم تصميم Kaspersky Security Center للتنفيذ المركزي لمهام الإدارة والصيانة الأساسية في شبكة المؤسسة. يوفر التطبيق وصول المسؤول إلى معلومات مفصلة حول مستوى أمان شبكة المؤسسة. يتيح لك Kaspersky Security Center تكوين جميع مكونات الحماية التي تم إنشاؤها باستخدام تطبيقات Kaspersky.

يتمتع خادم إدارة Kaspersky Security Center بالوصول الكامل إلى إدارة حماية الأجهزة العميلة وهو أهم مكون في نظام أمان المؤسسة. لذلك، تكون أساليب الحماية المتزايدة مطلوبة لخادم الإدارة.

قبل التكوين، أنشئ نسخة احتياطية من Kaspersky Security Center Administration Server باستخدام مهمة النسخ الاحتياطي لبيانات خادم الإدارة أو أداة klbackup واحفظها في مكان آمن.

يصف دليل التقوية التوصيات والميزات الخاصة بتكوين Kaspersky Security Center ومكوناته، التي تهدف إلى تقليل مخاطر الاختراق.

يحتوي دليل التقوية على المعلومات التالية:

- تحديد بنية خادم الإدارة
- تكوين اتصال آمن بخادم الإدارة
- تكوين الحسابات للوصول إلى خادم الإدارة
- إدارة حماية خادم الإدارة
- إدارة حماية الأجهزة العميلة
- تكوين الحماية للتطبيقات المدارة
- صيانة خادم الإدارة
- نقل المعلومات إلى تطبيقات الطرف الخارجي
- توصيات الأمان لأنظمة معلومات الجهات الخارجية

نشر خادم الإدارة

بنية خادم الإدارة

بشكل عام، يعتمد اختيار بنية إدارة مركزية على موقع الأجهزة المحمية، والوصول من الشبكات المجاورة، وأنظمة تسليم تحديثات قاعدة البيانات، وما إلى ذلك.

في المرحلة الأولى من تطوير البنية، نوصي بالتعرف على مكونات Kaspersky Security Center وتفاعلها مع بعضها البعض، بالإضافة إلى المخططات الخاصة بحركة البيانات واستخدام المنفذ .

بناءً على هذه المعلومات، يمكنك تكوين بنية تحدد:

- موقع خادم الإدارة واتصالات الشبكة
- تنظيم مساحات عمل المسؤول وطرق الاتصال بخادم الإدارة
- طرق نشر عميل الشبكة وبرامج الحماية
- استخدام نقاط التوزيع
- استخدام خوادم الإدارة الافتراضية
- استخدام تسلسل هرمي لخوادم الإدارة:

- مخطط تحديث قاعدة بيانات مكافحة الفيروسات
- تدفقات المعلومات الأخرى

تحديد جهاز لتثبيت خادم الإدارة

نوصي بتثبيت خادم الإدارة على خادم مخصص في البنية التحتية للمؤسسة. إذا لم يكن هناك برنامج جهة خارجية مثبتًا على الخادم، يمكنك تكوين إعدادات الأمان بناءً على متطلبات Kaspersky Security Center، دون الاعتماد على متطلبات برامج الجهة الخارجية.

ويمكنك نشر خادم الإدارة على خادم فعلي أو على خادم افتراضي. ويرجى التأكد أن الجهاز المحدد يلبي متطلبات الأجهزة والبرامج.

موقع خادم الإدارة

يمكن تحديد موقع الأجهزة التي يديرها خادم الإدارة على النحو التالي:

- على شبكة منطقة محلية (LAN)
- على الإنترنت
- في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)

في الوقت نفسه، يمكن أيضًا وضع خادم الإدارة في قطاعات مختلفة: القطاعات الصناعية والشركات ومنطقة الأجهزة الموصلة مباشرة بالإنترنت.

إذا كنت تستخدم Kaspersky Security Center لإدارة حماية قطاع شبكة معزول، فنحن نوصي بنشر خادم الإدارة في جزء من منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ). يتيح لك ذلك تنظيم تقسيم مناسب للشبكة وتقليل تدفق حركة المرور إلى الجزء المحمي، مع الحفاظ على إمكانات الإدارة الكاملة وتسليم التحديث.

تقييد نشر خادم الإدارة على وحدة تحكم مجال أو خادم طرفي أو جهاز مستخدم

لا نوصي بشدة بتثبيت خادم الإدارة على وحدة تحكم مجال أو خادم طرفي أو جهاز مستخدم.

نوصي بتوفير فصل وظيفي لعقد مفاتيح الشبكة. يتيح لك هذا الأسلوب الحفاظ على قابلية تشغيل الأنظمة المختلفة عند فشل العقدة أو تعرضها للاختراق. في الوقت نفسه، يمكنك إنشاء سياسات أمان مختلفة لكل عقدة.

على سبيل المثال، من الممكن أن تقلل قيود الأمان المطبقة عادة على وحدة تحكم المجال بشكل كبير من أداء خادم الإدارة وتجعل من المستحيل استخدام بعض ميزات خادم الإدارة. وإذا حصل متطفل على امتياز الوصول إلى وحدة تحكم المجال، يمكن تعديل قاعدة بيانات خدمات مجال Active Directory (AD DS) أو إتلافها أو تدميرها. أيضًا، يمكن اختراق جميع الأنظمة والحسابات التي يديرها Active Directory.

حسابات تثبيت خادم الإدارة وتشغيله

نوصي بتشغيل تثبيت خادم الإدارة تحت حساب مسؤول محلي لتجنب استخدام حسابات المجال للوصول إلى قاعدة بيانات خادم الإدارة. تعتمد مجموعة الحسابات المطلوبة وحقوقها على نوع نظام قاعدة البيانات المحدد وموقع نظام قاعدة البيانات وطريقة إنشاء قاعدة بيانات خادم الإدارة.

يتم إنشاء المجموعات KLAdmins وKLOperators تلقائيًا أثناء تثبيت Kaspersky Security Center. وتُمنح إلى هاتين المجموعتين أذونات الاتصال بخادم الإدارة ومعالجة كائناته.

واعتمادًا على نوع الحساب المستخدم لتثبيت Kaspersky Security Center، يتم إنشاء المجموعتين KLAdmins وKLOperators كما يلي:

- إذا تم تثبيت التطبيق بواسطة حساب مستخدم مضمن في مجال، يتم إنشاء المجموعات على جهاز خادم الإدارة وفي المجال الذي يتضمن خادم الإدارة.
- إذا تم تثبيت التطبيق بواسطة حساب النظام، يتم إنشاء المجموعتين على جهاز خادم الإدارة فقط.

لتجنب إنشاء مجموعات KLAdmins وKLOperators في المجال، ونتيجة لذلك، **توفير امتيازات لإدارة خادم الإدارة لحساب خارج جهاز خادم الإدارة**، نوصي بتثبيت Kaspersky Security Center تحت حساب محلي.

أثناء تثبيت خادم الإدارة، حدد الحساب الذي سيتم استخدامه لبدء خادم الإدارة كخدمة. بشكل افتراضي، يُنشئ التطبيق حسابًا محليًا باسم KL-AK-*، حيث سيتم تشغيل خدمة خادم الإدارة (خدمة klserver).

وإذا لزم الأمر، يمكن تشغيل خدمة خادم الإدارة تحت الحساب المحدد. يجب منح هذا الحساب الحقوق المطلوبة للوصول إلى نظام إدارة قواعد البيانات. ولأسباب تتعلق بالأمان، استخدم حسابًا بدون امتياز لتشغيل خدمة خادم الإدارة.

ولتجنب استخدام إعدادات الحساب غير الصحيحة، نوصي بإنشاء الحساب تلقائيًا.

استثناء خادم الإدارة من مجال

إذا كنت تستخدم خادم الإدارة لحماية مجموعات الأجهزة التي تتضمن أنظمة ذات أهمية عالية، فلا نوصي بتضمين جهاز خادم الإدارة في المجال. ويتيح لك هذا التمييز بين حقوق إدارة Kaspersky Security Center ومنع الوصول إلى خادم الإدارة في حالة تعرض حساب المجال للخطر.

ضع في الاعتبار أنه إذا قمت بتثبيت خادم الإدارة على جهاز مضمّن في مجموعة العمل، فلن تتوفر السيناريوهات التالية للعمل مع خادم الإدارة:

- استخدام مجموعة تجاوز الفشل من Kaspersky Security Center
- استخدام نظام مجموعة تجاوز الفشل في Windows Server
- استخدام SQL Server for Windows على جهاز منفصل

  يمكنك استخدام SQL Server for Windows على جهاز منفصل فقط في حالة تضمين خادم الإدارة وSQL Server في المجال نفسه أو المجالات الموثوقة. إذا كان خادم الإدارة وSQL Server ومشاركة UNC للنسخ الاحتياطية في مجموعة عمل، فلا يمكنك إعداد حقوق الوصول والقراءة والكتابة بين SQL Server والمشاركة.
- التثبيت عن بُعد باستخدام أدوات خادم الإدارة عبر سياسات مجموعة Active Directory

إذا كنت بحاجة إلى قطع اتصال خادم الإدارة بمجال Active Directory، فاتبع الخطوات الموضحة في الموضوع: كيفية تغيير اسم Kaspersky Security Center.

إذا كان من الضروري تثبيت خادم الإدارة على جهاز مضمّن في مجموعة العمل، فيمكنك أيضًا استخدام Kaspersky Security Center Linux بدلاً من Kaspersky Security Center Windows.

سلامة الاتصال

استخدام بروتوكول TLS

نوصي بحظر الاتصالات غير الآمنة بخادم الإدارة. على سبيل المثال، يمكنك حظر الاتصالات التي تستخدم بروتوكول HTTP في إعدادات خادم الإدارة.

ويرجى ملاحظة أنه بشكل افتراضي، يتم إغلاق العديد من منافذ HTTP لخادم الإدارة. ويتم استخدام المنفذ المتبقي لخادم ويب خادم الإدارة (8060). ويمكن تقييد هذا المنفذ من خلال إعدادات جدار الحماية لجهاز خادم الإدارة.

إعدادات TLS الصارمة

نوصي باستخدام بروتوكول TLS الإصدار 1.2 وأحدث، وتقييد أو حظر خوارزميات التشفير غير الآمن.

يمكنك تكوين بروتوكولات التشفير (TLS) التي يستخدمها خادم الإدارة. ويرجى ملاحظة أنه في وقت إصدار إصدار خادم الإدارة، تم تكوين إعدادات بروتوكول التشفير افتراضيًا لضمان النقل الآمن للبيانات.

حظر المصادقة عن بُعد باستخدام حسابات Windows

يمكنك استخدام العلامة LP_RestrictRemoteOsAuth لمنع اتصالات SSPI من العناوين البعيدة. وتسمح لك هذه العلامة بمنع المصادقة عن بُعد على خادم الإدارة باستخدام حسابات Windows المحلية أو المجال.

لتبديل العلامة LP_RestrictRemoteOsAuth إلى وضع حظر الاتصالات من العناوين البعيدة:

1. قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky\Kaspersky Security Center\Lab.
2. نفذ الأمر التالي في سطر الأوامر لتحديد قيمة علامة LP_RestrictRemoteOsAuth:

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
```

3. قم بإعادة تشغيل خدمة خادم الإدارة.

لا تعمل العلامة LP_RestrictRemoteOsAuth إذا تم إجراء المصادقة عن بُعد من خلال Kaspersky Security Center Web Console أو وحدة تحكم الإدارة المثبتة على جهاز خادم الإدارة.

تقييد الوصول إلى قاعدة بيانات خادم الإدارة

نوصي بتقييد الوصول إلى قاعدة بيانات خادم الإدارة. على سبيل المثال، امنح الوصول فقط من جهاز خادم الإدارة. ويقلل هذا من احتمالية اختراق قاعدة بيانات خادم الإدارة بسبب ثغرات أمنية معروفة.

ويمكنك تكوين المعلمات وفقًا لتعليمات التشغيل الخاصة بقاعدة البيانات المستخدمة، بالإضافة إلى توفير منافذ مغلقة على جدران الحماية.

مصادقة Microsoft SQL Server

إذا كان Kaspersky Security Center يستخدم Microsoft SQL Server كنظام لإدارة قاعدة البيانات، من الضروري حماية بيانات Kaspersky Security Center المنقولة إلى قاعدة البيانات والبيانات المخزنة في قاعدة البيانات أو منها من الوصول غير المصرح به. ولفعل ذلك، يجب عليك توفير اتصال آمن بين Kaspersky Security Center وSQL Server. الطريقة الأكثر موثوقية لتوفير اتصال آمن هي تثبيت Kaspersky Security Center و SQL Server على نفس الجهاز واستخدام آلية الذاكرة المشتركة لكلا التطبيقين. وفي جميع الحالات الأخرى، نوصي باستخدام شهادة / SSL TLS لمصادقة مثيل SQL Server.

بشكل عام، يستطيع خادم الإدارة معالجة SQL Server من خلال موفري الخدمة التاليين:

- SQLOLEDB باستخدام TCP/IP أو قنوات مسماة

  يتم تثبيت موفر الخدمة هذا في نظام التشغيل Windows ويتم استخدامه بشكل افتراضي.

- MSOLEDBSQL باستخدام TCP/IP أو القنوات المسماة أو الذاكرة المشتركة

  إذا كنت تريد استخدام موفر الخدمة هذا، فيجب عليك تثبيته على الجهاز المزود بخادم الإدارة، ثم تعيين القيمة 1 إلى متغير البيئة العام `KLDBADO_UseMSOLEDBSQL`.

- MSOLEDBSQL19 باستخدام TCP/IP أو القنوات المسماة أو الذاكرة المشتركة

  إذا كنت تريد استخدام موفر الخدمة هذا، فيجب عليك تثبيته على الجهاز المزود بخادم الإدارة، ثم تعيين القيمة 1 إلى متغير البيئة العام `KLDBADO_UseMSOLEDBSQL`، والقيمة `MSOLEDBSQL19` إلى متغير البيئة العام `KLDBADO_ProviderName`.

أيضًا، قبل استخدام TCP/IP أو القنوات المسماة أو الذاكرة المشتركة، تأكد من تمكين البروتوكول المطلوب.

التفاعل الأمني مع نظام إدارة قواعد البيانات الخارجي

في حالة تثبيت نظام إدارة قواعد البيانات على جهاز منفصل أثناء تثبيت خادم الإدارة (نظام إدارة قواعد البيانات الخارجي)، فنحن نوصي بتكوين المعلمات للتفاعل الآمن والمصادقة مع نظام إدارة قواعد البيانات هذا. وللمزيد من المعلومات عن تكوين مصادقة SSL، راجع مصادقة خادم PostgreSQL والسيناريو: مصادقة خادم MySQL.

تكوين قائمة السماح بعناوين IP للاتصال بخادم الإدارة

بشكل افتراضي، يمكن لمستخدمي Kaspersky Security Center تسجيل الدخول إلى Kaspersky Security Center من أي جهاز تم تثبيت وحدة تحكم الإدارة المستندة إلى MMC أو Kaspersky Security Center Web Console أو تطبيقات OpenAPI عليه. ويمكنك تكوين خادم الإدارة بحيث يمكن للمستخدمين الاتصال به فقط من الأجهزة ذات عناوين IP المسموح بها. على سبيل المثال، إذا حاول أحد المتطفلين الاتصال بتطبيق Kaspersky Security Center عبر Kaspersky Security Center Web Console Server المثبت على جهاز غير مدرج في القائمة المسموح بها، فلن يتمكن من تسجيل الدخول إلى Kaspersky Security Center.

تكوين قائمة السماح لعناوين IP للاتصال مع Kaspersky Security Center Web Console

بشكل افتراضي، يمكن لمستخدمي Kaspersky Security Center الاتصال بتطبيق Kaspersky Security Center Web Console من أي جهاز. وعلى جهاز تم تثبيت Kaspersky Security Center Web Console عليه، يجب عليك تكوين جدار الحماية (المدمج في نظام التشغيل أو نظام خاص بجهة خارجية) حتى يتمكن المستخدمون من الاتصال بتطبيق Kaspersky Security Center Web Console فقط من عناوين IP المسموح بها.

أمان الاتصال بوحدة التحكم بالمجال أثناء الاستقصاء

يتصل خادم الإدارة أو نقطة توزيع Linux بوحدة التحكم بالمجال عبر LDAPS لاستقصاء المجال. وبشكل افتراضي، لا يلزم التحقق من الشهادة عند الاتصال. ولفرض التحقق من الشهادة، اضبط علامة KLNAG_LDAP_TLS_REQCERT على 1. أيضًا، يمكنك تحديد مسار مخصص إلى هيئة الشهادات (CA) للوصول إلى سلسلة الشهادات باستخدام علامة KLNAG_LDAP_SSL_CACERT.

الحسابات والمصادقة

قبل التكوين، أنشئ نسخة احتياطية من Kaspersky Security Center Administration Server باستخدام مهمة النسخ الاحتياطي لبيانات خادم الإدارة أو أداة klbackup واحفظها في مكان آمن.

استخدام التحقق الثنائي مع خادم الإدارة

يوفر Kaspersky Security Center التحقق الثنائي لمستخدمي Kaspersky Security Center Web Console ووحدة تحكم الإدارة، استنادًا إلى معيار RFC 6238 (TOTP: خوارزمية كلمة المرور لمرة واحدة المستندة إلى الوقت).

عند تمكين التحقق الثنائي لحسابك الخاص، في كل مرة تسجل الدخول فيها إلى Kaspersky Security Center Web Console أو وحدة تحكم الإدارة، تقوم بإدخال اسم المستخدم وكلمة المرور ورمز أمان إضافي للاستخدام مرة واحدة. إذا كنت تستخدم مصادقة المجال لحسابك، ما عليك سوى إدخال رمز أمان إضافي يستخدم مرة واحدة. لتلقي رمز أمان للاستخدام مرة واحدة، يجب أن تقوم بتثبيت تطبيق مصادقة على جهاز الكمبيوتر لديك أو على جهازك المحمول.

توجد تطبيقات مصادقة للبرامج والأجهزة (الرموز المميزة) تدعم معيار RFC 6238. على سبيل المثال، تتضمن تطبيقات مصادقة البرامج Google Authenticator وMicrosoft Authenticator وFreeOTP.

لا نوصي بشدة بتثبيت تطبيق المصادقة على الجهاز نفسه الذي تم من خلاله إنشاء الاتصال بخادم الإدارة. يمكنك تثبيت تطبيق مصادقة على جهازك المحمول.

تقييد المستخدمين الجدد من إعداد التحقق بخطوتين لأنفسهم.

لزيادة تحسين أمان الوصول إلى Kaspersky Security Center Web Console، يمكنك منع المستخدمين الجدد من إعداد التحقق بخطوتين لأنفسهم.

وفي حالة تمكين هذا الخيار، لن يتمكن المستخدم الذي عطل التحقق بخطوتين، مثل مسؤول مجال جديد، من تكوين التحقق بخطوتين لنفسه. لذلك، لا يمكن المصادقة على هذا المستخدم على خادم الإدارة ولا يمكنه تسجيل الدخول إلى Kaspersky Security Center Web Console دون الحصول على موافقة من مسؤول Kaspersky Security Center آخر تم تمكين التحقق بخطوتين بالفعل لأجله.

استخدام المصادقة ثنائية العوامل لنظام تشغيل

نوصي باستخدام المصادقة متعددة العوامل (MFA) للمصادقة على جهاز خادم الإدارة باستخدام رمز مميز أو بطاقة ذكية أو طريقة أخرى (إن أمكن).

تقييد حفظ كلمة مرور المسؤول

إذا كنت تستخدم وحدة تحكم الإدارة، فلا نوصي بحفظ كلمة مرور المسؤول في خانة حوار اتصال خادم الإدارة.

إذا كنت تستخدم Kaspersky Security Center Web Console، لا نوصي بحفظ كلمة مرور المسؤول في المستعرض المثبت على جهاز المستخدم.

مصادقة حساب مستخدم داخلي

بشكل افتراضي، يجب أن تتوافق كلمة مرور حساب المستخدم الداخلي لخادم الإدارة مع القواعد التالية:

- يجب أن يتراوح طول كلمة المرور من 8 إلى 256 حرفًا.
- يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
  - الأحرف الكبيرة (A-Z)
  - الأحرف الصغيرة (a-z)
  - الأعداد (0-9)
  - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

افتراضيًا، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد محاولات إدخال كلمة المرور المسموح بها.

يمكن لمستخدم Kaspersky Security Center إدخال كلمة مرور غير صالحة لعدد محدود من المرات. بعد الوصول إلى الحد الأقصى، يتم حظر حساب المستخدم لمدة ساعة واحدة.

تكوين خيارات تغيير كلمة المرور لحساب مستخدم داخلي

نوصي بتكوين الخيارات التالية لتغيير كلمة المرور لحساب مستخدم داخلي:

- مدة تغيير كلمة المرور
- وقت التحذير الأولي بضرورة تغيير كلمة المرور
- قيمة خيار **User must change password at first sign-in**

حماية الحساب من التعديل غير المصرح به

نوصي بتمكين خيار إضافي لحماية حساب المستخدم الداخلي لخادم الإدارة من التعديل غير المصرح به. ويجب تكوين هذه الحماية بشكل منفصل لكل مستخدم داخلي.

مجموعة الإدارة المخصصة لخادم الإدارة

نوصي بإنشاء مجموعة إدارة مخصصة لخادم الإدارة. امنح هذه المجموعة حقوق وصول خاصة وأنشئ سياسة أمان خاصة بها.

لتجنب خفض مستوى أمان خادم الإدارة عن عمد، نوصي بتقييد قائمة الحسابات التي يمكنها إدارة مجموعة الإدارة المخصصة.

مجموعتا KLAdmins وKLOperators

يتم إنشاء مجموعتا KLAdmins وKLOperators تلقائيًا أثناء تثبيت Kaspersky Security Center. يتم منح مجموعة KLAdmins جميع حقوق الوصول. يتم منح مجموعة KLOperators حقوق القراءة والتنفيذ فقط. ويتم **قفل** الحقوق الممنوحة إلى مجموعة KLAdmins.

يمكنك عرض مجموعتي KLAdmins وKLOperators، وإجراء تغييرات على هذه المجموعات، باستخدام الأدوات الإدارية القياسية لنظام التشغيل.

عند وضع لوائح للعمل مع خادم الإدارة، من الضروري تحديد ما إذا كان أخصائي أمان المعلومات يحتاج إلى الوصول الكامل (والتضمين في مجموعة KLAdmins) لأداء المهام القياسية.

ويمكن توزيع معظم مهام الإدارة الأساسية بين أقسام الشركة (أو مختلف الموظفين في القسم نفسه) وبالتالي بين الحسابات المختلفة. ويمكنك أيضًا إعداد تمييز وصول مجموعات الإدارة في Kaspersky Security Center. نتيجة لذلك، من الممكن تنفيذ سيناريو يكون فيه الإذن بموجب الحسابات من مجموعة KLAdmins أمرًا شاذًا ويمكن اعتباره حادثًا.

وفي حالة تثبيت Kaspersky Security Center تحت حساب نظام، فلن يتم إنشاء المجموعات إلا على جهاز خادم الإدارة. وفي هذه الحالة، نوصي بالتأكد من تضمين المجموعة فقط الإدخالات التي تم إنشاؤها أثناء تثبيت Kaspersky Security Center. لا نوصي بإضافة أي مجموعات إلى مجموعة KLAdmins (المحلية و/أو المجال) التي يتم إنشاؤها تلقائيًا أثناء تثبيت Kaspersky Security Center. ويجب عليك أيضًا تقييد حقوق تغيير هذه المجموعة. يجب أن تتضمن مجموعة KLAdmins حسابات فردية غير مميزة فقط.

في حالة إجراء التثبيت تحت حساب مستخدم المجال، يتم إنشاء مجموعتي KLAdmins وKLOperators على خادم الإدارة وفي المجال الذي يتضمن خادم الإدارة. يوصى باتباع نهج مماثل مثل تثبيت الحساب المحلي.

تقييد عضوية دور المسؤول الرئيسي

نوصي بتقييد عضوية دور المسؤول الرئيسي.

بشكل افتراضي، بعد تثبيت خادم الإدارة، يتم تعيين دور المسؤول الرئيسي لمجموعة المسؤولين المحليين ومجموعة KLAdmins التي تم إنشاؤها. وهذا مفيد للإدارة، لكنه مهم من وجهة نظر الأمان، لأن دور المسؤول الرئيسي يتضمن مجموعة واسعة من الامتيازات، ويجب تنظيم تعيين هذا الدور للمستخدمين بشكل صارم.

ويمكن استبعاد المسؤولين المحليين من قائمة المستخدمين الذين يتمتعون بامتيازات المسؤول في Kaspersky Security Center. ولا يمكن إزالة دور المسؤول الرئيسي من مجموعة KLAdmins. يمكنك تضمين الحسابات التي سيتم استخدامها لإدارة خادم الإدارة في مجموعة KLAdmins.

وإذا كنت تستخدم مصادقة المجال، نوصي بتقييد امتيازات حسابات مسؤول المجال في Kaspersky Security Center. وبشكل افتراضي، تتمتع هذه الحسابات بدور المسؤول الرئيسي. أيضًا، يستطيع مسؤول المجال تضمين حسابه في مجموعة KLAdmins للحصول على دور المسؤول الرئيسي. ولتجنب ذلك، في إعدادات أمان Kaspersky Security Center، يمكنك إضافة مجموعة Domain Admins، ثم تحديد قواعد الحظر الخاصة بها. ويجب أن يكون لهذه القواعد الأسبقية على القواعد المسموح بها.

يمكنك أيضًا استخدام أدوار المستخدم المحددة مسبقًا مع مجموعة من الحقوق المكونة بالفعل.

تكوين حقوق الوصول إلى ميزات التطبيق

نوصي باستخدام التكوين المرن لحقوق الوصول إلى ميزات Kaspersky Security Center لكل مستخدم أو مجموعة من المستخدمين.

يسمح التحكم في الوصول المستند إلى الدور بإنشاء أدوار مستخدم قياسية مع مجموعة محددة مسبقًا من الحقوق وتعيين هذه الأدوار للمستخدمين اعتمادًا على نطاق واجباتهم.

المزايا الرئيسية لنموذج التحكم في الوصول المستند إلى الدور:

- سهولة الإدارة
- التسلسل الهرمي للدور
- نهج الامتياز الأقل
- الفصل بين الواجبات

يمكنك تعيين أدوار مضمنة لبعض الموظفين بناءً على مناصبهم، أو إنشاء أدوار جديدة تمامًا.

وأثناء تكوين الأدوار، انتبه إلى الامتيازات المرتبطة بتغيير حالة الحماية لجهاز خادم الإدارة والتثبيت عن بُعد لبرامج الجهة الخارجية:

- إدارة مجموعات الإدارة.
- العمليات مع خادم الإدارة.
- التثبيت عن بُعد.
- تغيير المعلمات لتخزين الأحداث وإرسال الإخطارات.
  يسمح لك هذا الامتياز بتعيين الإخطارات التي تقوم بتشغيل برنامج نصي أو وحدة نمطية قابلة للتنفيذ على جهاز خادم الإدارة عند وقوع حدث ما.

الحساب المنفصل للتثبيت عن بُعد للتطبيقات

بالإضافة إلى التمييز الأساسي لحقوق الوصول، نوصي بتقييد التثبيت عن بُعد للتطبيقات لجميع الحسابات (باستثناء حساب المسؤول الرئيسي أو حساب متخصص آخر).

نوصي باستخدام حساب منفصل للتثبيت عن بُعد للتطبيقات. يمكنك تعيين دور أو أذونات للحساب المنفصل.

تأمين الوصول المتميز على نظام التشغيل Windows

ونوصي بمراعاة توصيات Microsoft لتوفير أمان الوصول المتميز. ولعرض هذه التوصيات، انتقل إلى مقالة تأمين الوصول المتميز.

تتمثل إحدى النقاط الرئيسية للتوصيات في تنفيذ محطات العمل ذات الوصول المتميز (PAW).

استخدام حساب خدمة مُدار (MSA) أو مجموعة حسابات خدمة مُدارة (gMSA) لتشغيل خدمة خادم الإدارة

يحتوي Active Directory على نوع خاص من الحسابات للخدمات التي يتم تشغيلها بأمان، تسمى حساب الخدمة المُدارة للمجموعة (MSA/gMSA). ويدعم Kaspersky Security Center حسابات الخدمة المُدارة (MSA) وحسابات الخدمة المُدارة للمجموعة (gMSA). في حالة استخدام أنواع الحسابات هذه في مجالك، فيمكنك تحديد واحد منها كحساب لخدمة خادم الإدارة.

تدقيق منتظم لجميع المستخدمين وإجراءات المستخدمين.

نوصي بإجراء تدقيق منتظم لجميع المستخدمين على جهاز خادم الإدارة. يتيح لك ذلك الرد على أنواع معينة من تهديدات الأمان المرتبطة بالاختراق المحتمل للجهاز.

يمكنك أيضًا تتبع إجراءات المستخدمين، مثل الاتصال بخادم الإدارة وقطع الاتصال به، والاتصال بخادم الإدارة مع وجود خطأ، وتعديل الكائنات (للكائنات التي تدعم إدارة المراجعة).

إدارة حماية خادم الإدارة

تحديد برنامج حماية خادم الإدارة

بناءً على نوع نشر خادم الإدارة واستراتيجية الحماية العامة، حدد التطبيق لحماية جهاز خادم الإدارة.

إذا قمت بنشر خادم الإدارة على جهاز مخصص، نوصي بتحديد تطبيق Kaspersky Endpoint Security لحماية جهاز خادم الإدارة. ويتيح ذلك تطبيق جميع التقنيات المتاحة لحماية جهاز خادم الإدارة، بما في ذلك وحدات تحليل السلوك.

وفي حالة تثبيت خادم الإدارة على جهاز موجود في البنية التحتية وتم استخدامه مسبقًا في مهام أخرى، نوصي بالنظر في برامج الحماية التالية:

- الأمن الإلكتروني الصناعي من Kaspersky للعقد: ونوصي بتثبيت هذا التطبيق على الأجهزة المضمنة في شبكة صناعية. Kaspersky Industrial CyberSecurity for Nodes هو تطبيق يمتلك شهادات توافق مع مختلف الشركات المصنعة للبرامج الصناعية.
- حلول الأمان الموصى بها. في حالة تثبيت خادم الإدارة على جهاز عليه برنامج آخر، نوصي بمراعاة التوصيات المقدمة من بائع البرنامج هذا بشأن توافق حلول الأمان (قد تكون هناك بالفعل توصيات لتحديد حل الأمان، وقد تحتاج إلى تكوين المنطقة الموثوقة).

إنشاء سياسة أمان منفصلة لتطبيق الحماية

نوصي بأن تنشئ سياسة أمان منفصلة للتطبيق الذي يحمي جهاز خادم الإدارة. يجب أن تكون هذه السياسة مختلفة عن سياسة الأمان للأجهزة العميلة. ويسمح هذا بتحديد إعدادات الأمان الأكثر ملاءمة لخادم الإدارة، دون التأثير على مستوى الحماية للأجهزة الأخرى.

ونوصي بتقسيم الأجهزة إلى مجموعات، ثم وضع جهاز خادم الإدارة في مجموعة منفصلة يمكنك إنشاء سياسة أمان خاصة لها.

وحدات الحماية

إذا لم تكن هناك توصيات خاصة من بائع برنامج الجهة الخارجية المثبت على الجهاز نفسه مثل خادم الإدارة، نوصي بتفعيل وتكوين جميع وحدات الحماية المتاحة (بعد التحقق من تشغيل وحدات الحماية هذه لفترة معينة).

تكوين جدار الحماية لجهاز خادم الإدارة

على جهاز خادم الإدارة، نوصي بتكوين جدار الحماية لتقييد عدد الأجهزة التي يستطيع المسؤولون من خلالها الاتصال بخادم الإدارة من خلال وحدة تحكم الإدارة أو Kaspersky Security Center Web Console.

وبشكل افتراضي، يستخدم خادم الإدارة المنفذ 13291 لتلقي الاتصالات من وحدة تحكم الإدارة والمنفذ 13299 لتلقي الاتصالات من Kaspersky Security Center Web Console. نوصي بتقييد عدد الأجهزة التي يمكن من خلالها إدارة خادم الإدارة باستخدام هذه المنافذ.

إدارة حماية الأجهزة العميلة

تقييد إضافة مفاتيح الترخيص لحزم التثبيت

يتم تخزين حزم التثبيت في المجلد المشترك لخادم الإدارة، في المجلد الفرعي "Packages". وإذا أضفت مفتاح ترخيص إلى حزمة التثبيت، فقد يتم اختراق مفتاح الترخيص لأن حقوق الوصول للقراءة المشتركة يتم تمكينها لمخزن حزم التثبيت.

لتجنب المساس بمفتاح الترخيص، لا نوصي بإضافة مفاتيح الترخيص إلى حزم التثبيت.

نوصي باستخدام التوزيع التلقائي لمفاتيح الترخيص للأجهزة المُدارة، والنشر من خلال مهمة إضافة مفتاح الترخيص لتطبيق مُدار، وإضافة رمز تفعيل أو ملف مفتاح يدويًا إلى الأجهزة.

القواعد التلقائية لنقل الأجهزة بين مجموعات الإدارة

نوصي بتقييد استخدام القواعد التلقائية لنقل الأجهزة بين مجموعات الإدارة.

وإذا كنت تستخدم قواعد تلقائية لنقل الأجهزة، فقد يؤدي ذلك إلى نشر السياسات التي توفر المزيد من الامتيازات للجهاز المنقول أكثر مما يتمتع به الجهاز قبل النقل.

أيضًا، قد يؤدي نقل جهاز عميل إلى مجموعة إدارة أخرى إلى نشر إعدادات السياسة. وقد تكون إعدادات السياسة هذه غير مرغوب في توزيعها على أجهزة الضيف والأجهزة غير الموثوق بها.

ولا تنطبق هذه التوصية على التخصيص الأولي لمرة واحدة للأجهزة لمجموعات الإدارة.

متطلبات الأمان لنقاط التوزيع وبوابات الاتصال

من الممكن أن تعمل الأجهزة التي تم تثبيت عميل الشبكة عليها كنقطة توزيع وتؤدي الوظائف التالية:

- توزيع حزم التحديثات والتثبيت المستلمة من خادم الإدارة على الأجهزة العميلة داخل المجموعة.
- تنفيذ التثبيت عن بُعد لبرامج الجهات الخارجية وتطبيقات Kaspersky على الأجهزة العميلة.
- قم باستقصاء الشبكة لاكتشاف الأجهزة الجديدة وتحديث المعلومات حول الأجهزة الموجودة بالفعل. من الممكن أن تستخدم نقطة التوزيع طرق اكتشاف الجهاز نفسها التي يستخدمها خادم الإدارة.

وضع نقاط التوزيع على شبكة المؤسسة المستخدمة لأجل:

- تخفيف الحمل على خادم الإدارة
- تحسين حركة المرور
- تزويد خادم الإدارة بإمكانية الوصول إلى الأجهزة الموجودة في الأجزاء التي يصعب الوصول إليها من الشبكة

مع الأخذ في الاعتبار الإمكانات المتاحة، نوصي بحماية الأجهزة التي تعمل كنقاط توزيع من أي نوع من الوصول غير المصرح به (بما في ذلك الوصول المادي).

تقييد التخصيص التلقائي لنقاط التوزيع

لتبسيط الإدارة والحفاظ على قابلية تشغيل الشبكة، نوصي باستخدام التعيين التلقائي لنقاط التوزيع. ومع ذلك، بالنسبة للشبكات الصناعية والشبكات الصغيرة، نوصيك بتجنب تعيين نقاط التوزيع تلقائيًا، حيث يمكن، على سبيل المثال، نقل المعلومات الخاصة للحسابات المستخدمة لدفع مهام التثبيت عن بُعد إلى نقاط التوزيع عن طريق نظام التشغيل.

بالنسبة للشبكات الصناعية والشبكات الصغيرة، يمكنك تعيين الأجهزة يدويًا للعمل كنقاط توزيع.

ويمكنك أيضًا عرض التقرير الخاص بنشاط نقاط التوزيع.

متطلبات الأمان لأجهزة مستخدمي Kaspersky Security Center

يجب تطبيق متطلبات أمان خاصة على أجهزة مستخدمي Kaspersky Security Center. ونوصي بحماية هذه الأجهزة ضد أي نوع من الوصول غير المصرح به (بما في ذلك الوصول الفعلي):

تتضمن أجهزة مستخدم Kaspersky Security Center ما يلي:

- الأجهزة التي يتصل منها المستخدمون بتطبيق Kaspersky Security Center Web Console باستخدام مستعرض.
- الأجهزة التي يتصل منها المستخدمون بتطبيق Kaspersky Security Center باستخدام وحدة تحكم الإدارة المستندة إلى MMC.
- الأجهزة التي تتصل منها التطبيقات التي تتفاعل مع خادم الإدارة عبر OpenAPI بتطبيق Kaspersky Security Center.

متطلبات الأمان للأجهزة المثبت عليها Kaspersky Security Center Web Console

يتم استخدام الأجهزة التي تم تثبيت Kaspersky Security Center Web Console عليها لإدارة Kaspersky Security Center، لذا يجب تطبيق متطلبات خاصة على أمان هذه الأجهزة. ونوصي بحماية هذه الأجهزة ضد أي نوع من الوصول غير المصرح به (بما في ذلك الوصول الفعلي).

تكوين الحماية للتطبيقات المدارة

سياسات التطبيقات المُدارة

نوصي بإنشاء سياسة لكل نوع من أنواع التطبيقات والمكونات المستخدمة في Kaspersky Security Center (عميل الشبكة وKaspersky Endpoint Security for Windows وKaspersky Endpoint Agent وغيرها). يجب تطبيق هذه السياسة على جميع الأجهزة المُدارة (مجموعة إدارة الجذر) أو على مجموعة منفصلة يتم نقل الأجهزة المُدارة الجديدة إليها تلقائيًا وفقًا لقواعد الحركة المكونة.

تحديد كلمة المرور لتعطيل الحماية وإلغاء تثبيت التطبيق

لمنع المتطفلين من تعطيل تطبيقات الأمان من Kaspersky، نوصي بشدة بتمكين الحماية بكلمة مرور لتعطيل الحماية وإلغاء تثبيت تطبيقات الأمان من Kaspersky. ويمكنك تعيين كلمة المرور، على سبيل المثال، لتطبيق Kaspersky Endpoint Security for Windows وKaspersky Security for Windows Servers وعميل الشبكة وتطبيقات Kaspersky الأخرى. وبعد تمكين الحماية بكلمة مرور، نوصي بقفل هذه الإعدادات عن طريق إغلاق "القفل".

تحديد كلمة المرور للاتصال اليدوي لجهاز عميل بخادم الإدارة (الأداة المساعدة klmover)

تسمح لك الأداة المساعدة klmover بتوصيل جهاز عميل يدويًا بخادم الإدارة. عندما يتم تثبيت عميل الشبكة على جهاز عميل، يتم نسخ الأداة المساعدة تلقائيًا إلى مجلد تثبيت عميل الشبكة.

لمنع الدخلاء من نقل الأجهزة بعيدًا عن سيطرة خادم الإدارة، نوصي بشدة بتمكين الحماية بكلمة مرور لتشغيل الأداة المساعدة klmover. لتمكين الحماية بكلمة مرور ، حدد الخيار **Use uninstallation password** في إعدادات سياسة عميل الشبكة.

تتطلب الأداة المساعدة klmover حقوق المسؤول المحلي. ويمكن حذف الحماية بكلمة مرور لتشغيل الأداة المساعدة klmover للأجهزة التي تعمل بدون حقوق المسؤول المحلي.

يؤدي تمكين الخيار **Use uninstallation password** أيضًا إلى تمكين الحماية بكلمة مرور لأداة التنظيف (cleaner.exe).

استخدام Kaspersky Security Network

في جميع سياسات التطبيقات المُدارة وفي خصائص خادم الإدارة، نوصي بتمكين استخدام Kaspersky Security Network (KSN) وقبول بيان KSN. عند تحديث خادم الإدارة أو ترقيته، يمكنك قبول بيان KSN المحدث. في بعض الحالات، عندما يكون استخدام الخدمات السحابية محظورًا بموجب القانون أو اللوائح الأخرى، فيمكنك تعطيل KSN.

الفحص المنتظم للأجهزة المدارة

بالنسبة لجميع مجموعات الأجهزة، نوصي بإنشاء مهمة تقوم بشكل دوري بإجراء فحص كامل للأجهزة.

اكتشاف الأجهزة الجديدة

نوصي بتكوين إعدادات اكتشاف الاجهزة بشكل صحيح: قم بإعداد التكامل مع Active Directory، وحدد نطاقات عناوين IP لاكتشاف الأجهزة الجديدة.

لأغراض الأمان، يمكنك استخدام مجموعة الإدارة الافتراضية التي تتضمن جميع الأجهزة الجديدة والسياسات الافتراضية التي تؤثر على هذه المجموعة.

تحديد مجلد مشترك

ونشرت خادم الإدارة على الجهاز الذي يعمل بنظام Windows مع تحديد مجلد مشترك موجود (يتم استخدامه، على سبيل المثال، لوضع حزم التثبيت وتخزين قواعد البيانات المحدثة)، نوصي بضمان منح حقوق القراءة لمجموعة Everyone، ويتم منح حقوق الكتابة لمجموعة KLAdmins.

صيانة خادم الإدارة

النسخ الاحتياطي لبيانات خادم الإدارة

ويسمح لك النسخ الاحتياطي للبيانات باستعادة بيانات خادم الإدارة دون فقد البيانات.

بشكل افتراضي، يتم إنشاء مهمة النسخ الاحتياطي للبيانات تلقائيًا بعد تثبيت خادم الإدارة ويتم تنفيذها بشكل دوري، مع حفظ النسخ الاحتياطية في الدليل المناسب. ويمكن تغيير إعدادات مهمة النسخ الاحتياطي للبيانات على النحو التالي:

- يزيد تكرار النسخ الاحتياطي
- يتم تحديد دليل خاص لحفظ النسخ
- يتم تغيير كلمات المرور للنسخ الاحتياطية

إذا خزنت النسخ الاحتياطية في دليل خاص، يختلف عن الدليل الافتراضي، نوصي بتحديد قائمة التحكم بالوصول (ACL) لهذا الدليل. ويجب أن يكون لحسابات خادم الإدارة والحسابات في قاعدة بيانات خادم الإدارة حق الوصول للكتابة لهذا الدليل.

صيانة خادم الإدارة

تتيح لك صيانة خادم الإدارة خفض حجم قاعدة البيانات، وتحسين أداء التطبيق ومصداقيته التشغيلية. نوصيك بصيانة خادم الإدارة كل أسبوع على الأقل.

يتم إجراء صيانة خادم الإدارة باستخدام المهمة المخصصة. يجري التطبيق الإجراءات التالية عند صيانة خادم الإدارة:

- فحص قاعدة البيانات بحثًا عن أخطاء
- إعادة تنظيم فهارس قاعدة البيانات
- تحديث إحصائيات قاعدة البيانات
- تقليص قاعدة البيانات (إذا لزم الأمر)

تثبيت تحديثات نظام التشغيل وتحديثات برامج الجهات الخارجية

نوصي بشدة بتثبيت تحديثات البرامج لنظام التشغيل وبرامج الجهة الخارجية بانتظام على جهاز خادم الإدارة.

ولا تتطلب الأجهزة العميلة اتصالاً مستمراً بخادم الإدارة، لذلك من الآمن إعادة تشغيل جهاز خادم الإدارة بعد تثبيت التحديثات. ويتم إرسال جميع الأحداث المسجلة على الأجهزة العميلة أثناء تعطل خادم الإدارة إليها بعد استعادة الاتصال.

نقل الحدث إلى أنظمة الطرف الثالث

المراقبة وإعداد التقارير

للاستجابة في الوقت المناسب لمشاكل الأمان، نوصي بتكوين ميزات المراقبة وإعداد التقارير.

تصدير الأحداث إلى أنظمة SIEM

للاكتشاف السريع لمشاكل الأمان قبل حدوث ضرر كبير، نوصي باستخدام تصدير الحدث في نظام SIEM.

إشعارات البريد الإلكتروني لأحداث المراجعة

يتيح لك Kaspersky Security Center تلقي معلومات عن الأحداث التي تقع أثناء تشغيل خادم الإدارة وتطبيقات Kaspersky المثبتة على الأجهزة المُدارة. وللاستجابة لحالات الطوارئ في الوقت المناسب، نوصي بتكوين خادم الإدارة لإرسال إخطارات حول أحداث التدقيق، والأحداث الحرجة، وأحداث الفشل، والتحذيرات التي ينشرها.

ونظرًا لأن هذه الأحداث هي أحداث داخل النظام، يمكن توقع عدد صغير منها، وهو أمر قابل للتطبيق تمامًا للبريد.

إحصائيات وظيفة خادم الإدارة

للاستجابة السريعة لمشاكل الأمان، نوصي بتكوين إرسال إحصائيات وظيفة خادم الإدارة إلى تطبيقات الطرف الثالث، باستخدام بروتوكول إدارة الشبكة البسيط (SNMP).

توصيات الأمان لأنظمة معلومات الجهات الخارجية

توصيات أمنية من معايير CIS

عند استخدام إصدارات أنظمة التشغيل أو منصات المحاكاة الافتراضية أو خوادم قواعد البيانات التي يدعمها خادم الإدارة وعميل الشبكة، نوصي بتطبيق أفضل ممارسات أمان المعلومات من مركز أمان الإنترنت (CIS)، إن وجدت، لضبط أنظمة المعلومات هذه.

مركز أمان الإنترنت (CIS) منظمة غير ربحية مخصصة لتحسين الأمان في مجال تكنولوجيا المعلومات. على وجه الخصوص، يطور CIS ويوزع معايير السلامة مثل ضوابط CIS ومعايير CIS. وتعتبر هذه المعايير بمثابة مجموعة من التوصيات والممارسات لضمان أمان أنظمة المعلومات.

يحتوي CIS على توصيات للإصدارات التالية من أنظمة المعلومات التي يدعمها خادم الإدارة وعميل الشبكة:

- أنظمة التشغيل للعائلات التالية:
  - Windows لأجهزة سطح المكتب
  - Windows للخوادم
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- منصات المحاكاة الافتراضية VMware
- خوادم قواعد البيانات:
  - خادم Microsoft SQL
  - MySQL
  - MariaDB
  - PostgreSQL

توصيات الأمان لنظام التشغيل Astra Linux

عند استخدام نظام التشغيل Astra Linux، يجب عليك اتباع توصيات الأمان الموضحة في الكتاب الأحمر للإصدار المقابل من Astra Linux.

توصيات الأمان لنظام التشغيل RED OS

عند استخدام نظام التشغيل RED OS، يجب عليك استخدام توصيات الأمان من دليل المسؤول الموضحة في وثائق RED OS الرسمية.

توصيات لاستخدام تطبيقات الأمان من Kaspersky

استخدام كلمة مرور KLAdmin في Kaspersky Endpoint Security for Windows

يمكن لمستخدمين متعددين بمستويات مختلفة من معرفة الكمبيوتر مشاركة جهاز مُثبت عليه Kaspersky Endpoint Security for Windows. وإذا كان لدى المستخدمين وصول غير مقيد إلى Kaspersky Endpoint Security for Windows وإعداداته، فقد ينخفض المستوى الإجمالي لحماية الجهاز. وتتيح لك حماية كلمة المرور تقييد وصول المستخدمين إلى Kaspersky Endpoint Security for Windows، وفقًا للأذونات الممنوحة لهم (على سبيل المثال، الإذن بالخروج من التطبيق).

إحدى الطرق لتقييد الوصول إلى Kaspersky Endpoint Security for Windows ومعامِلاته هي استخدام حساب KLAdmin. حساب KLAdmin هو حساب مسؤول يتمتع بإمكانية الوصول غير المقيد إلى Kaspersky Endpoint Security for Windows. يحق لحساب KLAdmin تنفيذ أي إجراء محمي بكلمة مرور في Kaspersky Endpoint Security for Windows. لا يمكن إلغاء الأذونات الخاصة بحساب KLAdmin. يمكنك تعيين كلمة المرور لحساب KLAdmin في خصائص سياسة Kaspersky Endpoint Security for Windows. يتحمل مسؤول Kaspersky Endpoint Security for Windows المسؤولية الكاملة عن الاستخدام الآمن لكلمة المرور لحساب KLAdmin. وإذا كانت مؤسستك لديها سياسة كلمة مرور خاصة بها، فاتبع تعليمات تلك السياسة.

توصياتنا لحماية المؤسسة من سرقة كلمة مرور KLAdmin هي كما يلي:

- **المتطلبات العامة**

  لا تستخدم اسم الحساب أو جزء من الاسم ككلمة مرور.

- **متطلبات الحد الأدنى لطول كلمة المرور**

  أنشئ كلمة مرور يبلغ طولها 10 أحرف على الأقل.

- **متطلبات استخدام أنواع أحرف متعددة**

  قم بتعيين كلمة مرور معقدة تحتوي على أحرف من فئات مختلفة: أحرف صغيرة وكبيرة وأرقام وأحرف خاصة.

- **متطلبات انتهاء صلاحية كلمة المرور**

  قم بتعيين تاريخ انتهاء صلاحية كلمة المرور على الأقل لمدة 90 يومًا. ويجب ألا تتطابق كلمة المرور الجديدة مع أي من كلمات المرور الأربع والعشرين الأخيرة.

التحضير للنشر

يصف هذا القسم الخطوات الواجب عليك اتخاذها قبل نشر Kaspersky Security Center.

التخطيط لنشر Kaspersky Security Center

يوفر هذا القسم معلومات حول الاختيارات الأكثر ملائمة لنشر مكونات Kaspersky Security Center على شبكة المؤسسة استنادًا إلى المعايير التالية:

- إجمالي عدد الأجهزة
- الوحدات (المكاتب المحلية، الفروع) المنفصلة مؤسسيًا أو جغرافيًا
- الشبكات المنفصلة المتصلة بواسطة قنوات ضيقة
- الحاجة إلى الوصول عبر الإنترنت إلى خادم الإدارة

الأنظمة التقليدية لنشر نظام الحماية

يوضح هذا القسم الأنظمة القياسية لنشر الحماية ضد الفيروسات في شبكة مؤسسة باستخدام Kaspersky Security Center.

يجب حماية النظام ضد أي نوع من أنواع الوصول غير المصرح به. نوصي بتثبيت جميع تحديثات الأمان المتوفرة لنظام التشغيل لديك قبل تثبيت التطبيق على جهازك وحماية خادم الإدارة (خوادم الإدارة) ونقطة التوزيع (نقاط التوزيع) بشكل فعلي.

يمكنك استخدام Kaspersky Security Center لنشر نظام حماية على شبكة شركة عن طريق أنظمة النشر التالية:

- نشر نظام حماية من خلال Kaspersky Security Center، باستخدام إحدى الطرق التالية:
  - من خلال وحدة تحكم الإدارة
  - من خلال Kaspersky Security Center Web Console

  يتم تثبيت تطبيقات Kaspersky تلقائيًا على أجهزة العملاء، التي بدورها تتصل تلقائيًا بخادم الإدارة عن طريق استخدام Kaspersky Security Center.

  ويُعد نظام التوزيع الأساسي هو توزيع نظام الحماية من خلال وحدة تحكم الإدارة. يتيح لك استخدام Kaspersky Security Center Web Console بدء تثبيت تطبيقات Kaspersky من مستعرض.

- نشر نظام حماية يدويًا باستخدام حزم تثبيت مستقلة تم إنشاؤها بواسطة Kaspersky Security Center.

  يتم تثبيت تطبيقات Kaspersky على أجهزة العملاء ومحطة عمل المسؤول يدويًا؛ حيث يتم تحديد إعدادات اتصال أجهزة العملاء بخادم الإدارة عند تثبيت عميل الشبكة.

  ننصح بطريقة النشر هذه، في الحالات التي يتعذر فيها التثبيت عن بُعد.

يتيح Kaspersky Security Center لك أيضًا نشر نظام الحماية الخاص بك باستخدام سياسات مجموعة Microsoft Active Directory®.

حول تخطيط نشر Kaspersky Security Center على شبكة مؤسسة

يمكن لخادم إدارة واحد دعم 100 000 جهاز بحد أقصى. إذا كان إجمالي عدد الأجهزة في شبكة مؤسسة ما يتخطى 100 000 جهاز، فيجب نشر خوادم إدارة متعددة في هذه الشبكة وجمعها في تسلسل هرمي للحصول على إدارة مركزية ملائمة.

إذا كانت مؤسسة ما تضم مكاتب فرعية بعيدة واسعة النطاق (فروع) لكلٍ منها مسؤولون، فمن المفيد القيام بنشر خوادم إدارة في هذه المكاتب. وإلا، يجب أن يتم عرض هذه المكاتب كشبكات منفصلة متصلة بواسطة قنوات بمعدل نقل منخفض؛ راجع القسم "التكوين القياسي: عدد قليل من المكاتب واسعة النطاق تُدار بواسطة مسؤوليها".

عند استخدام شبكات منفصلة متصلة بقنوات ضيقة، يمكن حفظ حركة المرور عن طريق تعيين عميل شبكة واحد أو أكثر للعمل كنقطة توزيع (راجع جدول لحساب عدد نقاط التوزيع). في هذه الحالة، تقوم كل الأجهزة الموجودة على شبكة منفصلة باسترداد التحديثات من مراكز التحديث المحلية هذه. يمكن لنقاط التوزيع الفعلية تنزيل التحديثات من خادم الإدارة (السيناريو الافتراضي)، ومن خوادم Kaspersky على الإنترنت (انظر القسم التكوين القياسي: مكاتب صغيرة متعددة بعيدة).

يقدّم القسم "التكوينات القياسية لـ Kaspersky Security Center" وصف تفصيلي للتكوينات القياسية لـ Kaspersky Security Center. عند التخطيط لعملية النشر، حدد التكوين القياسي الأكثر ملاءمة بناءً على هيكل المؤسسة.

في مرحلة التخطيط للنشر، يجب وضع تعيين شهادة X.509 الخاصة لخادم الإدارة في الاعتبار. قد يكون تعيين شهادة X.509 لخادم الإدارة مفيدًا في الحالات التالية (قائمة جزئية):

- فحص حركة مرور طبقة مآخذ التوصيل الآمنة (SSL) بواسطة وكيل إنهاء SSL أو لاستخدام وكيل عكسي
- التكامل مع البنية الأساسية للمفاتيح العامة (PKI) لمؤسسة ما
- تحديد القيم المطلوبة في حقول الشهادة
- تقديم قوة التشفير المطلوبة لشهادة ما

تحديد بنية لحماية مؤسسة ما

يتم تحديد بنية حماية مؤسسة عن طريق العوامل التالية:

- مخطط شبكة مؤسسة.
- البنية المؤسسية.
- عدد الموظفين المسؤولين عن حماية الشبكة وتوزيع المسؤوليات عليهم.
- موارد الأجهزة التي يمكن تخصيصها لمكونات إدارة الحماية.
- معدل نقل قنوات الاتصال والتي يمكن تخصيصها لصيانة مكونات الحماية على شبكة المؤسسة.
- القيود الزمنية لتنفيذ العمليات الإدارية الحرجة على شبكة المؤسسة. تشمل العمليات الإدارية الحرجة، على سبيل المثال، توزيع قواعد بيانات مكافحة الفيروسات وتعديل السياسات للأجهزة العميلة.

عند تحديد بنية حماية، يُوصى أولاً بتقدير مصادر الشبكة والأجهزة المتوفرة والتي يمكن استخدامها لتشغيل نظام حماية مركزي.

لتحليل البنية التحتية للشبة والبرامج، ننصح بإتباع العملية أدناه:

1. تحديد الإعدادات التالية للشبكة التي سيتم نشر الحماية عليها:
   - عدد أجزاء الشبكة.
   - سرعة قنوات الاتصال بين أجزاء الشبكة الفردية.
   - عدد الأجهزة المُدارة في كل جزء من أجزاء الشبكة.
   - معدل نقل كل قناة اتصال يمكن توزيعها للاحتفاظ بتشغيل الحماية.
2. تحديد الحد الأقصى للوقت المسموح به لتنفيذ العمليات الإدارية الأساسية لجميع الأجهزة المُدارة

3. تحليل البيانات من الخطوة 1 والخطوة 2، بالإضافة إلى البيانات من اختبار تحميل نظام الإدارة. بناءً على التحليل، قم بالإجابة عن الأسئلة التالية:

- هل من الممكن خدمة جميع العملاء في خادم إدارة واحد، أم أن هناك حاجة إلى تسلسل هرمي لخوادم الإدارة؟
- ما التكوين المطلوب لأجهزة لخوادم الإدارة للتعامل مع جميع العملاء ضمن القيود الزمنية المحددة في الخطوة 2؟
- هل من المطلوب استخدام نقاط التوزيع لتقليل الحمل على قنوات الاتصال؟

بمجرد الحصول على إجابات على الأسئلة الواردة في الخطوة 3 أعلاه، يمكنك إعداد مجموعة الهياكل المسموح بها لحماية المؤسسة.

على شبكة المؤسسة، يمكنك استخدام إحدى بنى الحماية القياسية التالية:

- خادم إدارة واحد. يتم اتصال جميع الأجهزة العميلة بخادم إدارة واحد. يعمل خادم الإدارة كنقطة توزيع.
- خادم إدارة واحد مع نقاط التوزيع. يتم اتصال جميع الأجهزة العميلة بخادم إدارة واحد. تعمل بعض الأجهزة العميلة المتصلة بالشبكة كنقاط توزيع.
- التسلسل الهرمي لخوادم الإدارة. لكل جزء من أجزاء الشبكة، يتم تخصيص خادم إدارة فردي، ويصبح جزء من التسلسل الهرمي العام لخوادم الإدارة. يعمل خادم الإدارة الرئيسي كنقطة توزيع.
- التسلسل الهرمي لخوادم الإدارة مع نقاط التوزيع. لكل جزء من أجزاء الشبكة، يتم تخصيص خادم إدارة فردي، ويصبح جزء من التسلسل الهرمي العام لخوادم الإدارة. تعمل بعض الأجهزة العميلة المتصلة بالشبكة كنقاط توزيع.

التكوينات القياسية لـ Kaspersky Security Center

يوضح هذا القسم التكوينات القياسية التالية المستخدمة لنشر مكونات Kaspersky Security Center على شبكة مؤسسة ما:

- مكتب واحد
- عدد قليل من المكاتب واسعة النطاق، منفصلة جغرافيًا تُدار بواسطة مسؤوليها
- مكاتب صغيرة متعددة، منفصلة جغرافيًا

التكوين القياسي: مكتب واحد

يمكن نشر خادم إدارة واحد أو خوادم إدارة متعددة على شبكة المؤسسة. يمكن تحديد عدد خوادم الإدارة بناءً على الجهاز المتوفر، أو بناءً على عدد الإجمالي للأجهزة المدارة.

يمكن لخادم إدارة واحد دعم ما يصل إلى 100 000 جهاز. يجب عليك وضع احتمالية زيادة عدد الأجهزة المدارة في المستقبل القريب في الاعتبار: قد يكون من المفيد توصيل عدد أقل قليلاً من الأجهزة بخادم إدارة واحد.

يمكن نشر خوادم الإدارة إما على الشبكة الداخلية أو على DMZ، بناءً على ما إذا كان الوصول إلى خادم الإدارة عبر الإنترنت مطلوبًا أم لا.

في حالة استخدام خوادم متعددة، فمن المستحسن الجمع بينها في ترتيب هرمي. يتيح لك استخدام الترتيب الهرمي لخوادم الإدارة تجنب السياسات والمهام المسمّاة والتعامل مع مجموعة الأجهزة المُدارة بالكامل كما لو أنها تتم إدارتها بواسطة خادم إدارة واحد (أي البحث عن أجهزة وبناء تحديدات الأجهزة وإنشاء التقارير).

التكوين القياسي: عدد قليل من المكاتب واسعة النطاق تُدار بواسطة مسؤوليها

إذا كان لدى إحدى المؤسسات عدد قليل من المكاتب واسعة النطاق المنفصلة جغرافيًا، فيجب أن تفكر في خيار نشر خوادم الإدارة في كل مكتب من المكاتب. يمكن نشر واحد أو أكثر من خوادم الإدارة لكل مكتب، وهذا يتوقف على عدد الأجهزة العميلة وتوفر الأجهزة. في هذه الحالة، يمكن عرض كل مكتب من المكاتب كـ "التكوين القياسي: مكتب واحد". لسهولة الإدارة، يوصى بدمج كافة خوادم الإدارة في تسلسل هرمي (ربما متعدد المستويات).

إذا كان بعض الموظفين يتنقلون بين المكاتب بأجهزتهم (أجهزة الكمبيوتر المحمولة)، أنشئ ملفات تعريف اتصال عميل الشبكة في سياسة عميل الشبكة. يتم دعم ملفات تعريف اتصال عميل الشبكة فقط لمضيفي Windows وأجهزة macOS.

التكوين القياسي: مكاتب صغيرة متعددة بعيدة

يتوفر هذا التكوين القياسي لمكتب المقر الرئيسي والعديد من المكاتب الصغيرة البعيدة التي ربما تكون متصلة بمكتب المقر الرئيسي عبر الإنترنت. قد يكون كل مكتب من هذه المكاتب البعيدة موجودًا وراء ترجمة عناوين الشبكة (NAT) بمعنى أنه لا يمكن إنشاء اتصال بين مكتبين بعيدين طالما أنهما معزولان.

يجب نشر خادم إدارة في مكتب المقر الرئيسي، ويجب تعيين نقطة توزيع واحدة أو نقاط توزيع متعددة إلى كل المكاتب الأخرى. إذا كانت المكاتب مرتبطة عبر الإنترنت، فقد يكون من المفيد إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع لنقاط التوزيع، بحيث يتم تنزيل التحديثات مباشرة من خوادم Kaspersky، أو مجلد محلي أو مجلد الشبكة، وليس من خادم الإدارة.

إذا كان لا يتوفر لبعض الأجهزة في مكتب بعيد إمكانية الوصول المباشر إلى خادم الإدارة (على سبيل المثال، يتوفر الوصول إلى خادم الإدارة عبر الإنترنت ولكن بعض الأجهزة ليس لديها وصولاً إلى الإنترنت)، فعندها يجب تحويل نقاط التوزيع إلى وضع بوابة الاتصال. في هذه الحالة، سيكون عملاء الشبكة الموجودون على الأجهزة في المكتب البعيد متصلين بخادم الإدارة – للحصول على مزيد من المزامنة – ولكن عبر البوابة وليس مباشرةً.

ولأن خادم الإدارة على الأرجح لن يتمكن من استقصاء شبكة المكتب البعيد، فقد يكون من المفيد تحويل هذه الوظيفة إلى نقطة التوزيع.

سيتعذر على خادم الإدارة إرسال إخطارات إلى المنفذ 15000 UDP الموجود على الأجهزة المدارة الموجودة وراء NAT في المكتب البعيد. لحل هذه المشكلة، يمكنك تمكين وضع الاتصال المستمر بخادم الإدارة من خصائص الأجهزة التي تعمل كنقاط توزيع (خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة**). يتوفر هذا الوضع إذا كان عدد نقاط التوزيع الإجمالي لا يتعدى 300. استخدم خوادم الإرسال للتأكد من وجود اتصال مستمر بين جهاز مُدار وخادم الإدارة. راجع الموضوع التالي للحصول على التفاصيل: استخدام نقطة توزيع كخادم إرسال.

تحديد نظام إدارة قواعد البيانات (DBMS) لخادم الإدارة

عند اختيار نظام إدارة قواعد البيانات (DBMS) الذي سيستخدمه خادم الإدارة، يجب عليك الأخذ في الاعتبار عدد الأجهزة التي يغطيها خادم الإدارة.

يسرد الجدول التالي خيارات نظام إدارة قاعدة البيانات الصالحة، بالإضافة إلى توصيات وقيود استخدامها.

التوصيات والقيود حول نظام إدارة قواعد البيانات

نظام إدارة قاعدة البيانات	التوصيات والقيود
إصدار SQL Server Express Edition 2016 أو الإصدار الأحدث.	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 10000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يمكنك تحديد الحد الأقصى لعدد الأحداث في مخزن الأحداث لمنع تجاوز قاعدة البيانات. يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات. يُحظر تمامًا الاستخدام المتزامن لنظام إدارة قواعد البيانات الخاص بـ SQL Server Express Edition DBMS بواسطة خادم الإدارة وتطبيق آخر. لا يتم دعم قاعدة بيانات Microsoft SQL Express لمهمة **إجراء مزامنة Windows Update**.
إصدار 2016 أو الإصدارات الأحدث من خادم SQL Server المحلي، غير الإصدار Express.	بلا قيود.
إصدار 2016 من SQL Server البعيد، غير الإصدار Express، أو الإصدار الأحدث.	صالح فقط في حالة وجود الجهازين في مجال Windows® نفسه؛ وفي حالة اختلاف المجالات، يجب إنشاء علاقة ثقة ثنائية بينهم.
إصدارات MySQL 5.5 أو 5.6 أو 5.7 المحلية أو البعيدة (لم تعد إصدارات MySQL 5.5.1 و5.5.2 و5.5.3 و5.5.4 و5.5.5 مدعومة)	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 10000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.
MySQL 8.0.20 محلي أو عن بُعد أو إصدار أحدث	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 50000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.

نظام إدارة قاعدة البيانات	التوصيات والقيود
MariaDB محلي أو بعيد (انظر الإصدارات المدعومة)	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 20000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.
PostgreSQL، Postgres Pro (انظر الإصدارات المدعومة)	استخدم أحد نظم إدارة قواعد البيانات هذه إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 50000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.

إذا حددت MSSQL 2019، فيجب عليك استخدام التصحيح التراكمي CU12 أو إصدار أحدث. ويتيح لك ذلك تجنب الأخطاء والعبء الزائد على النظام الذي قد يحدث.

تطبيق التصحيح التراكمي CU12 عند استخدام SQL Server 2019 كنظام لإدارة قاعدة البيانات

إذا كنت تستخدم SQL Server 2019 كنظام لإدارة قاعدة البيانات (DBMS) ولم يكن لديك التحديث التراكمي CU12 أو أي إصدار أحدث لتجنب الأخطاء، مثل "ذاكرة النظام غير كافية في مجمع الموارد 'internal' لتشغيل هذا الاستعلام".

بعد تثبيت Kaspersky Security Center، نفذ الخطوات التالية:

1. اتصل بـ SQL Server باستخدام SQL Management Studio.
2. قم بتشغيل الأوامر التالية (إذا اخترت اسمًا مختلفًا لقاعدة البيانات، فاستخدم هذا الاسم بدلاً من KAV):

```
USE KAV
GO
OFF = ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING
GO
```

3. أعد تشغيل خدمة SQL Server 2019.

تكوين خادم MariaDB x64 للعمل مع Kaspersky Security Center 15.1

لتكوين خادم MariaDB x64 بنجاح للعمل مع Kaspersky Security Center، يجب عليك استخدام معلمات الخادم الافتراضية باستثناء معلمات الخادم المحددة في هذه المقالة.

يدعم Kaspersky Security Center 15.1 نظام MariaDB DBMS. لمزيد من المعلومات حول الإصدارات المدعومة من MariaDB، راجع القسم متطلبات الأجهزة والبرامج.

إذا كنت تستخدم نظام إدارة قواعد البيانات MariaDB مع Kaspersky Security Center، مكّن دعم تخزين InnoDB و MEMORY، وكذلك ترميزي UTF-8 و UCS-2.

الإعدادات الموصى بها لملف my.ini

لتكوين ملف my.ini:

1. افتح ملف my.ini في أي محرر نصوص.

2. أضف الأسطر التالية إلى قسم [mysqld] من ملف my.ini:

```
10M=sort_buffer_size
100M=join_buffer_size
300M=join_buffer_space_limit
8=join_cache_level
512M=tmp_table_size
512M=max_heap_table_size
200M=key_buffer_size
>=innodb_buffer_pool_size يجب ألا تقل القيمة الحقيقية عن 80% من حجم قاعدة بيانات KAV المتوقع <
20=innodb_thread_concurrency
0=innodb_flush_log_at_trx_commit
300=innodb_lock_wait_timeout
32M=max_allowed_packet
151=max_connections
12800=max_prepared_stmt_count
60000=table_open_cache
4=table_open_cache_instances
60000=table_definition_cache
"NO_ENGINE_SUBSTITUTION,NO_AUTO_CREATE_USER,STRICT_TRANS_TABLES"=sql_mode
```

قيمة innodb_buffer_pool_size يجب أن تكون أعلى من 80 بالمائة من الحجم المتوقع لقاعدة البيانات KAV. ولاحظ أنه يتم تخصيص الذاكرة المحددة عند بدء تشغيل الخادم. وإذا كان حجم قاعدة البيانات أصغر من حجم المخزن المؤقت المحدد، سيتم تخصيص الذاكرة المطلوبة فقط. وإذا كنت تستخدم MariaDB 10.4.3 أو أقدم، فإن الحجم الفعلي للذاكرة المخصصة يكون أكبر بنسبة 10 بالمائة تقريبًا من حجم المخزن المؤقت المحدد.

ننصح باستخدام قيمة المعلمة 0=innodb_flush_log_at_trx_commit لأن القيم "1" أو "2" تؤثر بالسلب على سرعة تشغيل MariaDB. تأكد من تعيين المعلمة innodb_file_per_table على 1.

بالنسبة إلى MariaDB 10.1، أدخل الأسطر التالية في قسم [mysqld]:

```
'Barracuda'=innodb_file_format
dynamic=innodb_default_row_format
1=innodb_large_prefix
```

بالنسبة إلى MariaDB 10.6، أدخل الأسطر التالية في قسم [mysqld]:

```
0=optimizer_prune_level
8=optimizer_search_depth
```

بشكل افتراضي، يتم تمكين إضافات المحسن join_cache_incremental و join_cache_hashed و join_cache_bka . في حال عدم تفعيل هذه الإضافات، يجب أن تقوم بتفعيلهم.

للتحقق مما إذا كانت إضافات المحسن مفعلة أم لا:

1. في وحدة تحكم عميل MariaDB، نفذ الأمر التالي:

```
SELECT @@optimizer_switch;
```

2. تحقق من أن خارجه يحتوي على السطور التالية:

```
on=join_cache_incremental
on=join_cache_hashed
on=join_cache_bka
```

إذا كانت هذه السطور موجودة وكانت قيمتها on، هذا يعني أن إضافات المحسن مفعلة.

إذا لم تكن هذه السطور موجودة أو قيمتها `off`، فعليك عمل التالي:

1. افتح ملف my.ini في أي محرر نصوص.

2. أضف الأسطر التالية إلى قسم `[mysqld]` من ملف my.ini:

```
'on=join_cache_incremental'=optimizer_switch
'on=join_cache_hashed'=optimizer_switch
'on=join_cache_bka'=optimizer_switch
```

تم تمكين الإضافات `join_cache_incremental` و`join_cache_hash` و`join_cache_bka`.

تكوين خادم MySQL x64 للعمل مع Kaspersky Security Center 15.1

لتكوين خادم MySQL x64 بنجاح للعمل مع Kaspersky Security Center، يجب عليك استخدام معلمات الخادم الافتراضية باستثناء معلمات الخادم المحددة في هذه المقالة.

إذا كنت تستخدم نظام إدارة قواعد البيانات MySQL مع Kaspersky Security Center، قم بتمكين دعم تخزين InnoDB وMEMORY، وكذلك ترميزي UTF-8 وUCS-2.

الإعدادات الموصى بها لملف my.ini

لتكوين ملف my.ini:

1. افتح ملف my.ini في أي محرر نصوص.

2. أضف الأسطر التالية إلى قسم `[mysqld]` من ملف my.ini:

```
10M=sort_buffer_size
20M=join_buffer_size
600M=tmp_table_size
600M=max_heap_table_size
200M=key_buffer_size
>=innodb_buffer_pool_size يجب ألا تقل القيمة الحقيقية عن 80% من حجم قاعدة بيانات KAV المتوقع <
20=innodb_thread_concurrency
0=innodb_flush_log_at_trx_commit (في معظم الحالات ، يستخدم الخادم معاملات صغيرة)
300=innodb_lock_wait_timeout
32M=max_allowed_packet
151=max_connections
12800=max_prepared_stmt_count
60000=table_open_cache
4=table_open_cache_instances
60000=table_definition_cache
```

لاحظ أنه يتم تخصيص الذاكرة المحددة في قيمة `innodb_buffer_pool_size` عند بدء تشغيل الخادم. وإذا كان حجم قاعدة البيانات أصغر من حجم المخزن المؤقت المحدد، سيتم تخصيص الذاكرة المطلوبة فقط. ويكون الحجم الفعلي للذاكرة المخصصة أكبر بنسبة 10 بالمائة تقريبًا من حجم المخزن المؤقت المحدد. يرجى الرجوع إلى وثائق MySQL للحصول على التفاصيل.

ينصح باستخدام قيمة المعلمة `innodb_flush_log_at_trx_commit = 0` = 0 لأن القيم "1" أو "2" تؤثر بالسلب على سرعة تشغيل MySQL. تأكد من تعيين المعلمة `innodb_file_per_table` على 1.

تكوين خادم PostgreSQL أو Postgres Pro للعمل مع Kaspersky Security Center 15.1

لتكوين خادم PostgreSQL أو Postgres Pro بنجاح للعمل مع Kaspersky Security Center، يجب عليك استخدام معلمات الخادم الافتراضية باستثناء معلمات الخادم المحددة في هذه المقالة.

يدعم مركز الأمن Kaspersky 15.1 PostgreSQL و Postgres Pro DBMSs. إذا كنت تستخدم أحد نظم إدارة قاعدة البيانات هذه، ففكر في تكوين معلمات خادم DBMS لتحسين عمل DBMS مع Kaspersky Security Center.

المسار الافتراضي لملف التكوين هو: `postgresql.conf\data\< VERSION >\PostgreSQL\Program Files\:C`

المعلمات الموصى بها لـ PostgreSQL و Postgres Pro:

- `151 = max_connections`
- `N = shared_buffers`

  N = 25 25 في المائة من قيمة ذاكرة الوصول العشوائي للجهاز حيث تم تثبيت نظام إدارة قاعدة البيانات. إذا كانت ذاكرة الوصول العشوائي أقل من 1 جيجابايت، فاترك القيمة الافتراضية.
- `24MB = temp_buffers`
- `16MB = work_mem`
- `128MB = maintenance_work_mem`
- `2MB = max_stack_depth`
- `0 = max_parallel_workers_per_gather`
- `on = standard_conforming_strings`

إذا كنت تستخدم Postgres Pro 15.7 أو Postgres Pro 15.7.1، فقم بتعطيل المعلمة `enable_compound_index_stats`:

`off = enable_compound_index_stats`

أعد تحميل التكوين أو أعد تشغيل خادم نظام إدارة قاعدة البيانات (DBMS) بعد تحديث ملف التكوين.

للحصول على معلومات مفصلة عن معلمات خادم PostgreSQL و Postgres Pro وعن كيفية تحديدها، راجع وثائق نظام إدارة قاعدة البيانات المقابلة.

راجع الموضوع التالي للحصول على تفاصيل حول كيفية إنشاء وتكوين حسابات لأجل PostgreSQL و Postgres Pro: تكوين الحسابات للعمل مع PostgreSQL و Postgres Pro.

دعم المجموعة المتاحة بدرجة كبيرة

يتم دعم مجموعات PostgreSQL المتوفرة بدرجة كبيرة بالإعدادات التالية:

- نوع التكرار: متزامن
- الحد الأدنى لعدد العقد: 3
- الحد الأقصى لعدد العقد: 15

لاستخدام الوظيفة، قم بتشغيل الأمر التالي لتمكين KLCS_FF_SUPPORT_POSTGRES_FAIILOVER flag:

```
s klcsff -n- "core/.independent." sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv
KLCS_FF_SUPPORT_POSTGRES_FAIILOVER -t d -v 1
```

يحتاج دور Postgres الذي يستخدمه الخادم للوصول إلى نظام إدارة قواعد البيانات (DBMS) إلى الحصول على امتيازات لقراءة طرق العرض التالية (يتم تمكينها بشكل افتراضي):

- pg_stat_replication
- pg_stat_wal_receiver

إدارة الأجهزة المحمولة باستخدام Kaspersky Endpoint Security for Android

تتم إدارة الأجهزة المحمولة المثبّت عليها Kaspersky Endpoint Security for Android™ (يُشار إليها فيما بعد باسم أجهزة KES) بواسطة خادم الإدارة. يدعم Kaspersky Security Center الميزات التالية لإدارة أجهزة KES:

- التعامل مع الأجهزة المحمولة كأجهزة عميلة:
  - عضوية في مجموعات الإدارة
  - المراقبة، مثل عرض الحالات والأحداث والتقارير
  - تعديل الإعدادات المحلية وتعيين السياسات لـ Kaspersky Endpoint Security for Android
- إرسال الأوامر في الوضع المركزي
- تثبيت حزم تطبيقات الأجهزة المحمولة عن بُعد.

خادم الإدارة يدير أجهزة KES من خلال TLS، منفذ TCP 13292.

توفير الوصول عبر الإنترنت إلى خادم الإدارة

تتطلب الحالات التالية وصولاً عبر الإنترنت إلى خادم الإدارة:

- حول تحديث قواعد بيانات Kaspersky ووحدات البرامج والتطبيقات
- تحديث برامج الطرف الثالث

بشكل افتراضي، لا يلزم اتصال خادم الإدارة بالإنترنت لتثبيت تحديثات برامج Microsoft على الأجهزة المدارة. على سبيل المثال، يمكن للأجهزة المدارة تنزيل تحديثات برامج Microsoft مباشرة من خوادم تحديث Microsoft أو من خادم Windows وخدمات تحديث خادم Microsoft Windowsالمنتشرة في شبكة مؤسستك. يجب أن يكون خادم الإدارة متصلاً بالإنترنت في الحالات التالية:

- عنج استخدام خادم الإدارة كخادم WSUS
- لتثبيت تحديثات برامج الطرف الثالث بخلاف برامج Microsoft

- إصلاح الثغرات الأمنية ببرامج الجهات الخارجية

يلزم اتصال خادم الإدارة بالإنترنت للقيام بالمهام التالية:

- لعمل قائمة بالإصلاحات الموصى بها بشأن الثغرات الأمنية في برنامج Microsoft. يقوم المتخصصون من Kaspersky بإنشاء القائمة وتحديثها بانتظام.
- لإصلاح الثغرات الأمنية في برامج طرف خارجي بدلاً من برامج Microsoft.

- إدارة الأجهزة (أجهزة الكمبيوتر المحمولة) الخاصة بالمستخدمين خارج المكتب
- إدارة الأجهزة الموجودة في المكاتب البعيدة
- التفاعل مع الخوادم الرئيسية أو التابعة الموجودة في المكاتب البعيدة
- إدارة الأجهزة المحمولة

يوضح هذا القسم الطرق النمطية لتوفير الوصول إلى خادم الإدارة عبر الإنترنت. قد تتطلب كل حالة من الحالات التي تركز على توفير وصول إلى خادم الإدارة عبر الإنترنت شهادة مخصصة لخادم الإدارة.

الوصول إلى الإنترنت: خادم الإدارة في شبكة محلية

في حالة وجود خادم الإدارة في الشبكة الداخلية لمؤسسة ما، فقد ترغب إتاحة الوصول إلى منفذ TCP رقم 13000 الخاص بخادم الإدارة من الخارج عن طريق إعادة توجيه المنفذ. إذا كانت إدارة الأجهزة المحمولة مطلوبة، فقد ترغب في جعل المنفذ رقم TCP 13292 متاحًا.

الوصول إلى الإنترنت: خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت

إذا كان خادم الإدارة موجودًا في منطقة الأجهزة الموصلة مباشرة بالإنترنت الخاصة بشبكة المؤسسة فلن يتمكن من الوصول إلى الشبكة الداخلية للمؤسسة. لذا، يتم تطبيق القيود التالية:

- يتعذر على خادم الإدارة اكتشاف أجهزة جديدة.
- يتعذر على خادم الإدارة القيام بالنشر الأولي لعميل الشبكة عبر التثبيت الإجباري على الأجهزة الموجودة في الشبكة الداخلية للمؤسسة.

ينطبق هذا على التثبيت الأولي فقط لعميل الشبكة. يمكن القيام بأي ترقيات إضافية لعميل الشبكة أو تثبيت تطبيق الأمان، من ناحية أخرى، بواسطة خادم الإدارة. في الوقت نفسه، يمكن القيام بنشر وكلاء الشبكة بطرق أخرى، على سبيل المثال، من خلال سياسات المجموعة الخاصة بـ ®Microsoft® Active Directory.

- يتعذر على خادم الإدارة إرسال إخطارات إلى الأجهزة المُدارة عبر منفذ UDP 15000، الأمر الذي لا يعد حدثًا حرجًا يؤثر على عمل Kaspersky Security Center.
- يتعذر على خادم الإدارة استقصاء Active Directory. ومن ناحية أخرى، فإن نتائج استقصاء Active Directory غير مطلوبة في معظم السيناريوهات.

في حالة اعتبار القيود الموجودة أعلاه قيودًا حرجة، يمكن إزالتها باستخدام نقاط التوزيع الموجودة في شبكة المؤسسة:

- للقيام بنشر أولي على الأجهزة التي لا تحتوي على عميل الشبكة، عليك القيام أولاً بتثبيت عميل الشبكة على أحد الأجهزة ثم تعيين حالة نقطة التوزيع له. وكنتيجة لذلك، سيتم القيام بتثبيت أولي لعميل الشبكة على الأجهزة الأخرى بواسطة خادم الإدارة عبر نقطة التوزيع.
- لاكتشاف أجهزة جديدة في الشبكة الداخلية للمؤسسة وإجراء استقصاء Active Directory، يجب عليك تمكين وسائل اكتشاف الأجهزة ذات الصلة على أحد نقاط التوزيع.

لضمان إرسال الإخطارات بنجاح إلى منفذ UDP 15000 على الأجهزة المُدارة الموجودة في الشبكة الداخلية للمؤسسة، يجب عليك تغطية الشبكة بالكامل باستخدام نقاط التوزيع. في خصائص نقاط التوزيع التي تم تعيينها، حدد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة**. ونتيجة لذلك، سيقوم خادم الإدارة بإنشاء اتصال مستمر بنقاط التوزيع بينما سيكونون قادرين على إرسال إعلامات إلى المنفذ UDP 15000 على الأجهزة الموجودة على الشبكة الداخلية للمؤسسة.(يمكن أن تكون شبكة IPv4 أو IPv6).

الوصول إلى الإنترنت: عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت

يمكن أن يتواجد خادم الإدارة في الشبكة الداخلية للمؤسسة، كما يمكن أن يتواجد في منطقة الأجهزة الموصلة مباشرة بالإنترنت الخاصة بهذه الشبكة جهاز مثبت عليه عميل الشبكة يعمل كبوابة اتصال باستخدام الاتصال العكسي (يقوم خادم الإدارة بإنشاء اتصال بعميل الشبكة). في هذه الحالة، يجب تحقيق الشروط التالية لضمان الوصول إلى الإنترنت:

- يجب تثبيت عميل الشبكة على الجهاز الموجود في منطقة الأجهزة الموصلة مباشرة بالإنترنت. عند تثبيت عميل الشبكة في نافذة **بوابة الاتصال** الخاصة بمعالج الإعداد، حدد **استخدام عميل الشبكة كبوابة اتصال في DMZ**.

- يجب إضافة الجهاز المزود ببوابة الاتصال المثبتة كنقطة توزيع . عند إضافة بوابة الاتصال في نافذة **إضافة نقطة توزيع** حدد الخيار **تحديد** ← **إضافة بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت حسب العنوان**.

- لاستخدام اتصال الإنترنت في توصيل الأجهزة المكتبية الخارجية بخادم الإدارة، يجب تصحيح حزمة تثبيت عميل الشبكة. في خصائص حزمة التثبيت التي تم إنشاؤها، حدد خيار **متقدم** ← **الاتصال بخادم الإدارة باستخدام بوابة الاتصال**، ثم حدد بوابة الاتصال المنشأة حديثًا.

بالنسبة لبوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت، يقوم خادم الإدارة بإنشاء شهادة موقعة بجانب شهادة خادم الإدارة. إذا قرر المسؤول تعيين شهادة مخصصة لخادم الإدارة، فيجب القيام بذلك قبل إنشاء بوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

في حالة استخدام بعض الموظفين لأجهزة كمبيوتر محمولة يمكنها الاتصال بخادم الإدارة إما عن طريق الشبكة المحلية أو عبر الإنترنت، فقد يكون من المفيد إنشاء قاعدة تبديل لعميل الشبكة في سياسة عميل الشبكة.

حول نقاط التوزيع

يمكن استخدام جهاز مثبت عليه عميل الشبكة كنقطة توزيع. في هذا الوضع، يمكن أن يؤدي عميل الشبكة الوظائف التالية:

- توزيع التحديثات (والتي يمكن استردادها إما من خادم الإدارة أو من خوادم Kaspersky). في الحالة الأخيرة، يجب إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع للجهاز الذي يعمل كنقطة توزيع:

  - تثبيت البرنامج (بما في ذلك عملية النشر الأولي لعملاء الشبكة) على أجهزة أخرى.

  - قم باستقصاء الشبكة لاكتشاف الأجهزة الجديدة وتحديث المعلومات حول الأجهزة الموجودة بالفعل. يمكن لنقطة التوزيع تطبيق نفس وسائل اكتشاف الأجهزة كخادم الإدارة.

تحقق عملية نشر نقاط التوزيع على شبكة مؤسسة ما الأهداف التالية:

- تخفيف الحمل على خادم الإدارة.

- تحسين حركة المرور.

- توفير وصول خادم الإدارة إلى الأجهزة الموجودة في أماكن يصعب الوصول إليها من شبكة المؤسسة. يتيح توفر نقطة توزيع على الشبكة خارج نطاق تقنية NAT (فيما يتعلق بخادم الإدارة) لخادم الإدارة القيام بالإجراءات التالية:

  - أرسل إشعارات إلى الأجهزة عبر UDP على شبكة IPv4 أو IPv6

  - استطلع رأي شبكة IPv4 أو IPv6

  - إجراء نشر أولي

  - العمل ك خادم إرسال

يتم تعيين نقطة توزيع لمجموعة إدارة. في هذه الحالة، يشمل نطاق نقطة التوزيع جميع الأجهزة الموجودة ضمن مجموعة الإدارة وجميع المجموعات الفرعية التابعة لها. ومع ذلك، قد لا يتم إدراج الجهاز، الذي يعمل كنقطة التوزيع، في مجموعة الإدارة التي تم تعيينه إليها.

يمكنك تعيين وظيفة نقطة توزيع كبوابة اتصال. وفي هذه الحالة، ستكون الأجهزة الموجودة في نطاق نقطة التوزيع متصلة بخادم الإدارة عبر البوابة وليس مباشرةً. يمكن أن يكون هذا الوضع مفيدًا في السيناريوهات التي لا تسمح بتأسيس اتصال مباشر بين خادم الإدارة والأجهزة المُدارة.

إذا كنت تستخدم جهازًا يعمل بنظام التشغيل Linux كنقطة توزيع، فنحن نوصي بشدة بزيادة حد واصفات الملفات لخدمة klnagent، لأنه إذا كان نطاق نقطة التوزيع يتضمن العديد من الأجهزة، فقد يكون العدد الأقصى الافتراضي للملفات التي يمكن فتحها غير كافٍ.

زيادة حد واصفات الملفات لخدمة klnagent

إذا كان نطاق نقطة التوزيع المستندة إلى Linux يتضمن العديد من الأجهزة، فقد لا يكون الحد الافتراضي للملفات التي يمكن فتحها (واصفات الملفات) كافيًا. لتجنب ذلك، يمكنك زيادة حد واصفات الملفات لخدمة klnagent.

لزيادة حد واصفات الملفات لخدمة klnagent:

1. على الجهاز الذي يعمل بنظام التشغيل Linux الذي يعمل كنقطة توزيع، نفذ الأمر التالي:

```
systemctl edit klnagent64.service
```

2. حدد القيود الصارمة والمرنة لواصفات الملفات في `LimitNOFILE` معلمة في قسم `[Service]`:

```
<hard resource limit>:<soft resource limit>=LimitNOFILE
```

على سبيل المثال، `131072:32768=LimitNOFILE`. لاحظ أن الحد غير الواضح لواصفات الملف يجب أن يكون أقل من الحد الثابت أو مساويًا له.

3. قم بتشغيل الأمر التالي للتأكد من تحديد المعلمات بشكل صحيح:

```
systemd-analyze verify klnagent64.service
```

إذا تم تحديد المعلمات بشكل غير صحيح، فمن الممكن أن يُخرج هذا الأمر أحد الأخطاء التالية:

- `:ignoring ,Failed to parse resource value :11:lib/systemd/system/klnagent64.service/ 13107:32768`

  في حالة حدوث هذا الخطأ، فقد تم تحديد الرموز الموجودة في السطر `LimitNOFILE` بشكل غير صحيح. ويجب عليك التحقق من السطر الذي تم إدخاله وتصحيحه.

- `Soft resource limit chosen higher than :11:lib/systemd/system/klnagent64.service/ 13107:32768 :ignoring ,hard limit`

  في حالة حدوث هذا الخطأ، يكون الحد غير الواضح لواصفات الملف التي أدخلتها أكبر من الحد الثابت. يجب عليك التحقق من السطر الذي تم إدخاله والتأكد من أن الحد غير الواضح لواصفات الملف أقل من الحد الثابت أو مساويًا له.

4. قم بتشغيل الأمر التالي لإعادة تحميل عملية systemd:

```
systemctl daemon-reload
```

5. قم بتشغيل الأمر التالي لإعادة تشغيل خدمة عميل الشبكة:

```
systemctl restart klnagent
```

6. قم بتشغيل الأمر التالي للتأكد من تطبيق المعلمات المحددة بشكل صحيح:

```
limits/<nagent process id>/less /proc
```

حيث معلمة `<nagent process id>` هي معرف عملية عميل الشبكة. ويمكنك تشغيل الأمر التالي للحصول على المعرف:

```
grep klnagent | ps -ax
```

بالنسبة لنقطة التوزيع المعتمدة على Linux، يتم زيادة حد الملفات التي يمكن فتحها.

حساب عدد نقاط التوزيع وتكوينهم

كلما زاد عدد الأجهزة العميلة التي تحتوي عليها الشبكة، زاد عدد نقاط التوزيع المطلوبة بالنسبة لها. لا نوصي بتعطيل التعيين التلقائي لنقاط التوزيع. عند تمكين التعيين التلقائي لنقاط التوزيع، يقوم خادم الإدارة بتعيين نقاط التوزيع إذا كان عدد الأجهزة العميلة كبيرًا إلى حد ما ويقوم بتحديد تكوينهم.

استخدام نقاط التوزيع المعينة بشكل حصري

إذا كنت تخطط لاستخدام أجهزة محددة كنقاط توزيع (أي الخوادم المخصصة حصريًا)، فيمكنك إلغاء الاشتراك من استخدام التعيين التلقائي لنقاط التوزيع. وفي هذه الحالة، تأكد من أن الأجهزة التي تنوي تعيينها كنقاط توزيع تحتوي على حجم كافٍ من مساحة القرص الفارغة ولا يتم إيقاف تشغيلها بانتظام وتم تعطيل وضع السكون بها.

عدد نقاط التوزيع التي تم تعيينها حصريًا في شبكة تحتوي على مقطع شبكة واحد بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العميلة في مقطع الشبكة	عدد نقاط التوزيع
أقل من 300	0 (لا تقم بتعيين نقاط توزيع)
أكثر من 300	مقبول: (1 N/10 + 000)، موصى به: (2 N/5 + 000)، حيث N هو عدد الأجهزة المتصلة بالشبكة

عدد نقاط التوزيع التي تم تعيينها حصريًا في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العملية لكل مقطع شبكة	عدد نقاط التوزيع
أقل من 10	0 (لا تقم بتعيين نقاط توزيع)
10–100	1
أكثر من 100	مقبول: (1 N/10 + 000)، موصى به: (2 N/5 + 000)، حيث N هو عدد الأجهزة المتصلة بالشبكة

استخدام الأجهزة العميلة القياسية (محطات العمل) كنقاط توزيع

إذا كنت تخطط لاستخدام أجهزة عميلة قياسية (أي محطات العمل) كنقاط توزيع، فنوصيك بتعيين نقاط التوزيع كما هو موضح في الجداول أدناه لتجنب التحميل الزائد على قنوات الاتصال وخادم الإدارة:

عدد محطات العمل التي تعمل كنقاط توزيع في شبكة تحتوي على مقطع شبكة واحد بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العميلة في مقطع الشبكة	عدد نقاط التوزيع
أقل من 300	0 (لا تقم بتعيين نقاط توزيع)
أكثر من 300	(1 + N/300)، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل

عدد محطات العمل التي تعمل كنقاط توزيع في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العملية لكل مقطع شبكة	عدد نقاط التوزيع
أقل من 10	0 (لا تقم بتعيين نقاط توزيع)
10–30	1
31–300	2
أكثر من 300	(1 + N/300)، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل

في حالة إيقاف تشغيل نقطة توزيع (أو عدم توفرها لسبب آخر)، يمكن للأجهزة المُدارة الموجودة في نطاقها الوصول إلى خادم الإدارة للحصول على تحديثات.

التسلسل الهرمي لخوادم الإدارة

قد تقوم مؤسسة MSP ما بتشغيل العديد من خوادم الإدارة. ويمكن أن يكون من الشاق إدارة العديد من خوادم الإدارة المنفصلة، وبذلك يمكن استخدام ترتيب هرمي. يمكن للتكوين الرئيسي/التابع لاثنين من خوادم الإدارة توفير الخيارات التالية:

- يرث خادم الإدارة الثانوي السياسات والمهام من خادم الإدارة الرئيسي، وهذا يمنع تكرار الإعدادات.
- يمكن أن يشمل تحديد أجهزة على خادم الإدارة الرئيسي أجهزة من خوادم الإدارة الثانوية.
- يمكن أن تحتوي التقارير الموجودة على خادم الإدارة الرئيسي على بيانات (تشمل معلومات تفصيلية) من خوادم الإدارة الثانوية.

يتلقى خادم الإدارة الأساسي البيانات فقط من خوادم الإدارة الثانوية غير الافتراضية ضمن نطاق الخيارات المذكورة أعلاه. لا ينطبق هذا القيد على خوادم الإدارة الافتراضية، التي تشارك قاعدة البيانات مع خادم الإدارة الأساسي الخاص بها.

خوادم الإدارة الافتراضية

بالاستناد إلى خادم الإدارة الفعلي، يمكن إنشاء خوادم إدارة افتراضية متعددة، والتي ستكون مشابهة لخوادم الإدارة الثانوية. بالمقارنة بطراز الوصول الاختياري، الذي يستند إلى قوائم التحكم في الوصول (ACL)، يُعتبر طراز خادم الإدارة الافتراضي أكثر وظيفية ويوفر درجة أكبر من العزل. بالإضافة إلى الهيكل المحدد لمجموعات الإدارة للأجهزة المخصصة ذات السياسات والمهام، يتميز كل خادم إدارة افتراضي بمجموعته الخاصة من الأجهزة غير المخصصة، ومجموعات التقارير الخاصة، والأجهزة والأحداث المحددة، وحزم التثبيت، وقواعد النقل، وما إلى ذلك. يمكن استخدام النطاق الوظيفي لخوادم الإدارة الافتراضية من قبل موفري الخدمة (xSP) وذلك لزيادة عزل العملاء إلى أقصى حد، ومن قبل المؤسسات الكبرى التي تمتلك تدفقات العمل المعقدة والعديد من المديرين.

خوادم الإدارة الافتراضية تشبه إلى حدٍ كبير خوادم الإدارة الثانوية، ولكن مع الفروق التالية:

- يفتقد خادم الإدارة الافتراضي لأغلب الإعدادات العمومية ومنافذ TCP الخاصة به.
- لا يحتوي خادم الإدارة الافتراضي على خوادم إدارة ثانوية.
- لا يحتوي خادم الإدارة الافتراضي على خوادم إدارة افتراضية أخرى.
- يمكن لخادم الإدارة الفعلي عرض الأجهزة والمجموعات والأحداث والكائنات الموجودة على الأجهزة المدارة (العناصر الموجودة في العزل وسجل التطبيقات وما إلى ذلك) الخاصة بكل خوادم الإدارة الافتراضية الخاصة به.
- لا يمكن لخادم الإدارة الافتراضي فحص الشبكة إلا مع اتصال نقاط التوزيع.

معلومات حول قيود Kaspersky Security Center

يعرض الجدول التالي قيود الإصدار الحالي لـ Kaspersky Security Center .

قيود Kaspersky Security Center

نوع القيد	القيمة
العدد الأقصى للأجهزة المدارة لكل خادم إدارة	100,000
تم تحديد الحد الأقصى لعدد الأجهزة مع تحديد خيار **عدم قطع الاتصال عن خادم الإدارة**	300
الحد الأقصى لعدد مجموعات الإدارة	10,000
الحد الأقصى لعدد الأحداث التي سيتم تخزينها	45,000,000
الحد الأقصى لعدد السياسات	2000
الحد الأقصى لعدد المهام	2000
الحد الأقصى للعدد الإجمالي لعناصر الوحدات التنظيمية Active Directory، وحسابات المستخدمين، والأجهزة، ومجموعات الأمان)	1,000,000

نوع القيد	القيمة
الحد الأقصى لعدد ملفات التعريف في سياسة ما	100
الحد الأقصى لعدد خوادم الإدارة الثانوية على خادم إدارة أساسي واحد	500
الحد الأقصى لعدد خوادم الإدارة الافتراضية	500
الحد الأقصى لعدد الأجهزة التي يمكن أن تغطيها نقطة توزيع واحدة (تستطيع نقاط التوزيع تغطية الأجهزة غير المحمولة فقط)	000,10
الحد الأقصى لعدد الأجهزة التي قد تستخدم بوابة اتصال واحدة	10 000، بما في ذلك الأجهزة المحمولة
العدد الأقصى للأجهزة المحمولة لكل خادم إدارة	100 000 ناقص عدد الأجهزة المدارة الثابتة

تحميل الشبكة

يحتوي هذا القسم على معلومات حول حجم حركة مرور الشبكة التي تتبادلها الأجهزة العميلة وخادم الإدارة أثناء سيناريوهات الإدارة الأساسية.

ويرجع السبب في وجود التحميل الرئيسي على الشبكة إلى سيناريوهات الإدارة التالية قيد التقدم:

- النشر الأولي للحماية ضد الفيروسات
- التحديث المبدئي لقواعد بيانات مكافحة الفيروسات
- مزامنة جهاز عميل مع خادم الإدارة
- التحديث المنتظم لقواعد بيانات مكافحة الفيروسات
- معالجة الأحداث على الأجهزة العميلة بواسطة خادم الإدارة

النشر الأولي للحماية ضد الفيروسات

يوفر هذا القسم معلومات عن قيم حجم حركة المرور بعد تثبيت عميل الشبكة وKaspersky Endpoint Security for Windows على الجهاز العميل (راجع الجدول أدناه).

يتم تثبيت عميل الشبكة باستخدام التثبيت الإجباري، عندما يتم نسخ الملفات المطلوبة للتثبيت بواسطة خادم الإدارة إلى مجلد مشترك على الجهاز العميل. بعد التثبيت، يسترد عميل الشبكة حزمة توزيع Kaspersky Endpoint Security for Windows باستخدام الاتصال بخادم الإدارة.

حركة المرور

سيناريو	تثبيت عميل شبكة لجهاز عميل واحد	تثبيت Kaspersky Endpoint Security for Windows على جهاز عميل واحد (مع تحديث قواعد البيانات)	التثبيت المتزامن لعميل الشبكة وKaspersky Endpoint Security for Windows
حركة المرور من الجهاز العميل إلى خادم الإدارة، بالكيلو بايت	1638.4	7843.84	9707.52
حركة المرور من خادم الإدارة إلى الكمبيوتر العميل، بالكيلو بايت	990.4,69	317.76,259	318.4,329
إجمالي حركة المرور (جهاز عميل فردي)، بالكيلو بايت	628.8,71	161.6,267	025.92,339

بعد تثبيت عملاء الشبكة على الأجهزة العميلة، يمكن تعيين أحد الأجهزة في مجموعة الإدارة للعمل كنقطة توزيع. وسيتم استخدامه لتوزيع حزم التثبيت. في هذه الحالة، سيختلف حجم حركة المرور الذي تم تحويله أثناء التوزيع المبدئي لتطبيق الحماية ضد الفيروسات بشكل كبير اعتمادًا على استخدام IP متعدد الإرسال.

إذا تم استخدام IP متعدد الإرسال، فسيتم إرسال حزم التثبيت مرة واحدة لكل الأجهزة قيد التشغيل في مجموعة الإدارة. لذا، فإن إجمالي حركة المرور سيصبح N مرات أقل، حيث إن N ترمز إلى إجمالي عدد الأجهزة قيد التشغيل في مجموعة الإدارة. في حالة عدم استخدام IP متعدد الإرسال، فإن إجمالي حركة المرور سيكون مطابقًا لحركة المرور التي تم حسابها عندما يتم تنزيل حزم التوزيع من خادم الإدارة. ومع هذا، سيكون مصدر الحزمة هو نقطة التوزيع وليس خادم الإدارة.

التحديث المبدئي لقواعد بيانات مكافحة الفيروسات

معدلات حركة البيانات أثناء التحديث الأولي لقواعد بيانات مكافحة الفيروسات (عند بدء مهمة تحديث قاعدة البيانات لأول مرة على جهاز العميل)، هي كما يلي:

- حركة البيانات من جهاز العميل إلى خادم الإدارة: 1,8 ميجا بايت
- حركة البيانات من خادم الإدارة إلى جهاز العميل: 113 ميجا بايت
- إجمالي حركة البيانات (جهاز عميل فردي): 114ميجا بايت

قد تختلف البيانات الموجودة قليلاً اعتمادًا على إصدار قاعدة بيانات مكافحة الفيروسات الحالي.

مزامنة عميل مع خادم الإدارة

يوضح هذا السيناريو حالة نظام الإدارة عند وقوع مزامنة مكثفة للبيانات بين الجهاز العميل وخادم الإدارة. تقوم أجهزة الكمبيوتر العميلة بالاتصال بخادم الإدارة خلال الفترة التي يحددها المسؤول. يقارن خادم الإدارة حالة البيانات على جهاز عميل بتلك الموجودة على الخادم، ويسجل المعلومات في قاعدة بيانات حول أخر اتصال للجهاز العميل، ويقوم بمزامنة البيانات.

يحتوي هذا القسم على معلومات حول قيم حركة المرور لسيناريوهات الإدارة الأساسية عند اتصال عميل بخادم الإدارة (انظر الجدول أدناه). قد تختلف البيانات الموجودة في الجدول قليلاً اعتمادًا على إصدار قاعدة بيانات مكافحة الفيروسات الحالي.

حركة المرور

سيناريو	حركة المرور من الأجهزة العميلة إلى خادم الإدارة، بالكيلو بايت	حركة المرور من خادم الإدارة إلى الأجهزة العميلة، بالكيلو بايت	إجمالي حركة المرور (جهاز عميل فردي)، بالكيلو بايت
المزامنة الأولية قبل تحديث قواعد البيانات على جهاز عميل	699.44	568.42	1267.86
المزامنة الأولية بعد تحديث قواعد البيانات على جهاز عميل	735.8	4474.88	5210.68
مزامنة مع عدم وجود تغيرات في الجهاز العميل وخادم الإدارة	11.99	6.73	18.72
المزامنة بعد تغيير قيمة إعداد في سياسة مجموعة	9.79	11.39	21.18
المزامنة بعد تغيير قيمة إعداد في مهمة جماعية	11.27	11.72	22.99
مزامنة إجبارية مع عدم وجود تغيرات في الجهاز العميل	77.59	99.45	177.04

يختلف حجم حركة المرور الكلي بشكل كبير اعتمادًا على ما إذا كان قد تم استخدام البث المتعدد لـ IP ضمن مجموعات الإدارة. إذا تم استخدامIP متعدد الإرسال، فسيزيد حجم حركة المرور الكلي تقريبًا بنسبة N مرات للمجموعة، حيث أن N ترمز إلى العدد الكلي للأجهزة المضمنة في مجموعة الإدارة.

يتم تحديد حجم حركة المرور في المزامنة الأولية قبل وبعد تحديث العناوين للحالات التالية:

- تثبيت عميل الشبكة وتطبيق الأمان على جهاز عميل
- نقل جهاز عميل إلى مجموعة إدارة
- تطبيق السياسة والمهمات التي تم إنشاؤها للمجموعة بشكل افتراضي، على جهاز عميل

يحدد الجدول معدلات حركة المرور في حال طرأت تغييرات على إحدى إعدادات الحماية المضمنة في إعدادات سياسة Kaspersky Endpoint Security. قد تختلف بيانات إعدادات سياسة أخرى عن تلك المعروضة في الجدول.

التحديث الإضافي لقواعد بيانات مكافحة الفيروسات

معدلات حركة البيانات في حال التحديث المتزايد لقواعد بيانات مكافحة الفيروسات بعد 20 ساعة من التحديث السابق هي كما يلي:

- حركة البيانات من جهاز العميل إلى خادم الإدارة: 169 كيلو بايت
- حركة البيانات من خادم الإدارة إلى جهاز العميل: 16 ميجا بايت
- إجمالي حركة البيانات (جهاز عميل فردي): 16.3ميجا بايت

قد تختلف البيانات الموجودة في الجدول قليلاً اعتمادًا على إصدار قاعدة بيانات مكافحة الفيروسات الحالي.

يختلف حجم حركة المرور بشكل كبير اعتمادًا على ما إذا كان قد تم استخدام IP متعدد الإرسال ضمن مجموعات الإدارة أم لا. إذا تم استخدامIP متعدد الإرسال، فسيزيد حجم حركة المرور الكلي تقريبًا بنسبة N مرات للمجموعة، حيث أن N ترمز إلى العدد الكلي للأجهزة المضمنة في مجموعة الإدارة.

معالجة الأحداث الخاصة بالعملاء بواسطة خادم الإدارة

يقدم هذا القسم معلومات حول حجم حركة المرور عند مواجهة جهاز عميل حدث "اكتشاف فيروس"، الذي سيتم إرساله بعد ذلك إلى خادم الإدارة وتسجيله في قاعدة البيانات (راجع الجدول الموجود أدناه).

حركة المرور

سيناريو	نقل البيانات إلى خادم الإدارة عند وقوع حدث "اكتشاف الفيروس"	نقل البيانات إلى خادم الإدارة عند وقوع 9 أحداث "اكتشاف الفيروس"
حركة المرور من الجهاز العميل إلى خادم الإدارة، بالكيلو بايت	49.66	64.05
حركة المرور من خادم الإدارة إلى الكمبيوتر العميل، بالكيلو بايت	28.64	31.97
إجمالي حركة المرور (جهاز عميل فردي)، بالكيلو بايت	78.3	96.02

قد تختلف البيانات المضمنة في الجدول قليلاً اعتمادًا على إصدار تطبيق مكافحة الفيروسات الحالي والأحداث المحددة في سياسته للتسجيل في قاعدة بيانات خادم الإدارة.

حركة المرور كل 24 ساعة

يحتوي هذا القسم على معلومات حول معدلات حركة المرور لمدة 24 ساعة من نشاط نظام الإدارة في حالة "هادئة"، عندما لا يتم إجراء تغيرات في البيانات بواسطة الأجهزة العميلة أو بواسطة خادم الإدارة (انظر الجدول أدناه).

توضح البيانات في الجدول حالة الشبكة بعد التثبيت القياسي لـ Kaspersky Security Center واكتمال معالج البدء السريع. بلغ تردد مزامنة الجهاز العميل مع خادم الإدارة 20 دقيقة، وتم تنزيل التحديثات إلى مستودع خادم الإدارة مرة كل ساعة.

معدلات حركة المرور لكل 24 ساعة في حالة الخمول

تدفق حركة المرور	القيمة
حركة المرور من الجهاز العميل إلى خادم الإدارة، بالكيلو بايت	3235.84
حركة المرور من خادم الإدارة إلى الكمبيوتر العميل، بالكيلو بايت	378.88,64
إجمالي حركة المرور (جهاز عميل فردي)، بالكيلو بايت	614.72,67

التحضير لإدارة الجهاز المحمول

هذا القسم يوفر المعلومات التالية:

- حول خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM المخصص لإدارة أجهزة iOS عن طريق تثبيت ملفات تعريف iOS MDM مخصصة عليها
- حول إدارة الأجهزة المحمولة المثبّت عليها Kaspersky Endpoint Security for Android

خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يتيح لك خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM إدارة أجهزة iOS عن طريق تثبيت ملفات تعريف iOS MDM مخصصة عليها. يتم دعم المزايا التالية:

- قفل الجهاز
- إعادة تعيين كلمة المرور
- مسح البيانات

- تثبيت التطبيقات أو إزالتها

- استخدام ملف تعريف iOS MDM يحتوي على إعدادات متقدمة (مثل إعدادات VPN، وإعدادات البريد الإلكتروني، وإعدادات Wi-Fi، وإعدادات الكاميرا، والشهادات، وما إلى ذلك).

خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM هو خدمة ويب تتلقى الاتصالات الواردة من الأجهزة المحمولة عبر منفذ TLS الخاص بها (المنفذ 443 بشكل افتراضي)، الذي يُدار بواسطة Kaspersky Security Center باستخدام عميل الشبكة. يتم تثبيت عميل الشبكة محليًا على جهاز تم نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عليه.

عند نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، يجب على المسؤول القيام بالإجراءات التالية:

- تزويد عميل الشبكة بإمكانية الوصول إلى خادم الإدارة

- تزويد الأجهزة المحمولة بإمكانية الوصول إلى منفذ TCP الخاص بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يعالج هذا القسم تكوينين قياسيين لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

التكوين القياسي: Kaspersky Device Management for iOS في منطقة الأجهزة الموصلة مباشرة بالإنترنت

يوجد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في DMZ الخاصة بالشبكة المحلية لمؤسسة ما مع وصول للإنترنت. الميزة الخاصة بهذا النهج هو غياب أي مشكلات عند الوصول إلى خدمة iOS MDM على الويب من أجهزة عبر الإنترنت.

ولأن إدارة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM تتطلب تثبيت عميل شبكة محليًا، يجب عليك التأكد من تفاعل عميل الشبكة مع خادم الإدارة. يمكنك التأكد من ذلك باستخدام إحدى الطرق التالية:

- عن طريق نقل خادم الإدارة إلى DMZ.

- عن طريق استخدام بوابة اتصال:

a. على الجهاز الذي تم نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عليه، قم بتوصيل عميل الشبكة بخادم الإدارة عبر بوابة الاتصال.

b. على الجهاز الذي تم نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عليه، قم بتعيين عميل الشبكة ليعمل كبوابة اتصال.

التكوين القياسي: خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الشبكة المحلية لمؤسسة ما

يوجد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على الشبكة الداخلية للمؤسسة. ويجب تمكين المنفذ 443 (المنفذ الافتراضي) للوصول الخارجي، على سبيل المثال، عن طريق نشر خدمة ويب iOS MDM على الخادم الوكيل العكسي الذي يدعم تفويض Kerberos المقيد.

يتطلب أي تكوين قياسي وصولاً إلى خدمات Apple على الويب الخاصة بخادم iOS MDM (النطاق 17.0.0.0/8) عبر منذ TCP رقم 2197. يُستخدم هذا المنفذ لإخطار الأجهزة بالأوامر الجديدة عن طريق خدمة مخصصة تُسمى APN.

إدارة الأجهزة المحمولة باستخدام Kaspersky Endpoint Security for Android

تتم إدارة الأجهزة المحمولة المثبّت عليها Kaspersky Endpoint Security for Android™ (يُشار إليها فيما بعد باسم أجهزة KES) بواسطة خادم الإدارة. يدعم Kaspersky Security Center الميزات التالية لإدارة أجهزة KES:

- التعامل مع الأجهزة المحمولة كأجهزة عميلة:

  - عضوية في مجموعات الإدارة

  - المراقبة، مثل عرض الحالات والأحداث والتقارير

  - تعديل الإعدادات المحلية وتعيين السياسات لـ Kaspersky Endpoint Security for Android

- إرسال الأوامر في الوضع المركزي
- تثبيت حزم تطبيقات الأجهزة المحمولة عن بُعد.

خادم الإدارة يدير أجهزة KES من خلال TLS، منفذ TCP 13292.

معلومات حول أداء خادم الإدارة

يعرض هذا القسم نتائج اختبار أداء خادم الإدارة لتكوينات الأجهزة المختلفة، وكذلك القيود على اتصال الأجهزة المدارة بخادم الإدارة.

قيود على الاتصال بخادم إدارة

يقدم خادم الإدارة الدعم لما يصل إلى 100 000 جهاز دون حدوث تقصير في الأداء.

القيود على الاتصال بخادم الإدارة دون حدوث تقصير في الأداء:

- يمكن لخادم إدارة واحد دعم ما يصل إلى 500 خادم إدارة افتراضي.
- لا يدعم خادم الإدارة الرئيسي أكثر من 1000 جلسة في آن واحد.
- لا تدعم خوادم الإدارة الافتراضية أكثر من 1000 جلسة في آن واحد.

نتائج اختبار أداء خادم الإدارة

تسمح نتائج اختبار أداء خادم الإدارة بتحديد الحد الأقصى لعدد الأجهزة العميلة التي يمكن مزامنتها مع خادم الإدارة خلال فواصل زمنية محددة. يمكنك استخدام هذه المعلومات لتحديد المخطط الأمثل لنشر الحماية لمكافحة الفيروسات على شبكات الكمبيوتر.

تم استخدام الأجهزة التي تحتوي على تكوينات الجهاز التالية (راجع الجدول الموجود أدناه) للاختبار:

تكوين جهاز خادم الإدارة

المعلمة	القيمة
وحدة المعالجة المركزية	Intel Xeon وحدة المعالجة المركزية E5630، سرعة الساعة 2.53 جيجاهرتز، 2 مأخذ، 8 مراكز معالجة، 16 معالجًا منطقيًا
الذاكرة العشوائية	26 جيجابايت
محرك القرص الثابت	جهاز قرص IBM ServeRAID M5014 SCSI، 487 جيجابايت
نظام التشغيل	Microsoft Windows Server 2019 القياسي، إصدار 10.0.17763 وإصدار 17763
الشبكة	QLogic BCM5709C جيجابت إيثرنت (عميل NDIS VBD)

تكوين جهاز لجهاز خادم SQL Server.

المعلمة	القيمة
وحدة المعالجة المركزية	وحدة معالجة مركزية Intel Xeon طراز X5570، سرعة الساعة 2.93 جيجاهرتز، مقبسان، 8 نوى، 16 معالجًا منطقيًا
الذاكرة العشوائية	32 جيجابايت
محرك القرص الثابت	جهاز قرص Adaptec Array SCSI بسعة 2047 جيجابايت
نظام التشغيل	Microsoft Windows Server 2019 القياسي، إصدار 10.0.17763 وإصدار 17763
الشبكة	Intel 82576 جيجابت

يدعم خادم الإدارة إنشاء 500 خادم إدارة افتراضي.

كان الفاصل الزمني للمزامنة هو 15 دقيقة لكل 10 000 جهاز مُدار (انظر الجدول أدناه).

ملخص نتائج اختبار تحميل خادم الإدارة

الفاصل الزمني للمزامنة (بالدقائق)	عدد الأجهزة المدارة
15	000,10
30	000,20
45	000,30
60	000,40
75	000,50
90	000,60
105	000,70
120	000,80
135	000,90
150	000,100

إذا قمت بتوصيل خادم الإدارة بخادم قاعدة بيانات MySQL أو SQL Express أو MariaDB، فلا يُوصى باستخدام التطبيق لإدارة أكثر من 10 000 جهاز. بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20 000 جهاز.

نتائج اختبار أداء خادم وكيل KSN

إذا كانت شبكة المؤسسة الخاصة بك تتضمن عددًا كبيرًا من الأجهزة العميلة وتستخدم خادم الإدارة كخادم وكيل KSN، فيجب أن تفي أجهزة خادم الإدارة بمتطلبات معينة لتتمكن من معالجة الطلبات من الأجهزة العميلة. يمكنك استخدام نتائج الاختبار أدناه لتقييم تحميل خادم الإدارة في شبكتك وتخطيط موارد الأجهزة لتوفير الأداء العادي لخدمة وكيل KSN.

توضح الجداول أدناه تكوين الجهاز لخادم الإدارة وخادم SQL. تم استخدام هذا التكوين للاختبار.

تكوين جهاز خادم الإدارة

المعلمة	القيمة
وحدة المعالجة المركزية	وحدة معالجة مركزية Intel Xeon E5450، سرعة الساعة 3.00 جيجاهرتز، مقبسان، 8 نوى، 16 معالجًا منطقيًا
الذاكرة العشوائية	32 جيجابايت
نظام التشغيل	نظام تشغيل Microsoft Windows Server 2016 قياسي

تكوين جهاز خادم SQL

المعلمة	القيمة
وحدة المعالجة المركزية	وحدة معالجة مركزية Intel Xeon E5450، سرعة الساعة 3.00 جيجاهرتز، مقبسان، 8 نوى، 16 معالجًا منطقيًا
الذاكرة العشوائية	32 جيجابايت
نظام التشغيل	نظام تشغيل Microsoft Windows Server 2019 قياسي

يعرض الجدول أدناه نتائج الاختبار.

نتائج ملخصة لاختبار أداء خادم وكيل KSN

المعلمة	القيمة
الحد الأقصى لعدد الطلبات التي تتم معالجتها في الثانية	4914
الحد الأقصى لاستخدام CPU	%36

إعدادات الشبكة للتفاعل مع الخدمات الخارجية

يستخدم Kaspersky Security Center إعدادات الشبكة التالية للتفاعل مع الخدمات الخارجية.

إعدادات الشبكة

إعدادات الشبكة	العنوان	الوصف
Port: 443 Protocol: HTTPS	activation-v2.kaspersky.com	تفعيل التطبيق.
Port: 443 Protocol: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات.
Port: 443 Protocol: HTTPS	https://downloads.upd.kaspersky.com	• تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. • التحقق من إمكانية الوصول إلى خوادم Kaspersky. قبل تنزيل قواعد بيانات Kaspersky ووحدات البرامج النمطية، يتحقق Kaspersky Security Center من إمكانية الوصول إلى خوادم Kaspersky. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة.

إعدادات الشبكة	العنوان	الوصف
Port: 80 Protocol: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات.
Port: 443 Protocol: HTTPS	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	استخدام Kaspersky Security Network.
Port: 443, 1443 Protocol: HTTPS	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	استخدام Kaspersky Security Network.

إعدادات الشبكة	العنوان	الوصف
Port: 443 Protocol: HTTPS	click.kaspersky.com redirect.kaspersky.com	Following links from the interface.
Port: 80 Protocol: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	تعد هذه الخوادم جزءًا من البنية التحتية للمفتاح العام (PKI) وهي ضرورية للتحقق من حالة صلاحية شهادات التوقيع الرقمي من Kaspersky. قائمة الشهادات الباطلة (CRL) هي قائمة بالشهادات التي تم إبطالها. ويتيح لك بروتوكول حالة الشهادة عبر الإنترنت (OCSP) طلب حالة شهادة معينة في الوقت الحقيقي. وتساعد هذه الخوادم على ضمان أمان التفاعل مع الشهادات الرقمية والحماية من الهجمات المحتملة.
Port: 443 Protocol: HTTPS	https://ipm-klca.kaspersky.com	الأخبار التسويقية.

للتفاعل الصحيح لحل Kaspersky Security Center مع الخدمات الخارجية، ضع في اعتبارك التوصيات التالية:
- يجب السماح بحركة مرور شبكة الاتصال غير المشفرة على المنفذين 1443 443 على معدات الشبكة والخادم الوكيل لمؤسستك.
- عندما يتفاعل خادم الإدارة مع خوادم تحديث Kaspersky وخوادم Kaspersky Security Network، فمن الضروري تجنب قرصنة حركة مرور الشبكة من خلال استبدال الشهادة (هجمات الوسيط).

لتنزيل التحديثات من خلال بروتوكول HTTP أو HTTPS باستخدام الأداة المساعدة klscflag:

1. قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Security Center\Lab.

2. إذا كنت ترغب في تنزيل التحديثات من خلال بروتوكول HTTP، فقم بتشغيل أحد الأوامر التالية:

- على الجهاز المُثبت عليه خادم الإدارة:

```
klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
```

- على نقطة توزيع:

```
klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
```

إذا كنت ترغب في تنزيل التحديثات من خلال بروتوكول HTTPS، فقم بتشغيل أحد الأوامر التالية:

- على الجهاز المُثبت عليه خادم الإدارة:

```
klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
```

- على نقطة توزيع:

```
klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
```

نشر عميل الشبكة وتطبيق الأمان

لإدارة أجهزة في مؤسسة ما، يجب عليك تثبيت عميل الشبكة على كلٍ منها. تبدأ عملية نشر Kaspersky Security Center الموزّع على أجهزة المؤسسة عادةً بتثبيت عميل الشبكة عليها.

في Microsoft Windows XP، قد لا يُجري عميل الشبكة العمليات التالية بشكل صحيح: تنزيل التحديثات مباشرة من خوادم Kaspersky (كنقطة توزيع) والعمل كخادم وكيل لشبكة KSN (كنقطة توزيع) واكتشاف الثغرات الأمنية لجهة خارجية (في حالة استخدام إدارة الثغرات الأمنية والتصحيحات).

النشر الأولي

لإدارة أجهزة في مؤسسة ما، يجب عليك تثبيت عميل الشبكة على كل جهاز.

ويمكن تثبيت عميل الشبكة على الجهاز المُدار الذي يعمل بنظام Windows بالطرق التالية:

- باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد.
- عن طريق استنساخ صورة لمحرك القرص الثابت الخاص بالمسؤول والمثبت عليه نظام التشغيل وعميل الشبكة، أو باستخدام الأدوات المقدمة من Kaspersky Security Center للتعامل مع صور القرص، أو باستخدام أدوات الجهة الخارجية.
- عن طريق سياسات مجموعة Windows باستخدام أدوات الإدارة القياسية من Windows لسياسات المجموعة، أو في الوضع التلقائي، عبر الخيار المخصص المقابل في مهمة التثبيت عن بُعد لبرنامج Kaspersky Security Center.
- في الوضع القسري، باستخدام موارد نظام التشغيل من خلال مهمة التثبيت عن بُعد لبرنامج Kaspersky Security Center.
- عن طريق إرسال روابط الحزم المستقلة التي يتم إنشاؤها بواسطة Kaspersky Security Center إلى مستخدمي الجهاز. الحزم المستقلة هي وحدات نمطية تنفيذية تحتوي على حزم التوزيع الخاصة بالتطبيقات المحددة مع تحديد إعداداتها.
- يدويًا، عن طريق تشغيل مثبّتات التطبيق على الأجهزة.

يمكن إجراء التثبيت الأولي لعميل الشبكة على الجهاز المُدار الذي يعمل بنظام Linux بالطرق التالية:

- عن طريق الاتصال بالجهاز المُدار عبر SSH وتشغيل مهمة التثبيت عن بعد.
- عن طريق تشغيل تثبيت الحزمة على الجهاز المُدار.

يمكن إجراء التثبيت الأولي لعميل الشبكة على الجهاز المُدار الذي يعمل بنظام macOS بالطرق التالية:

- من خلال تشغيل مهمة التثبيت عن بعد من خلال نقطة توزيع لنظام macOS.
- عن طريق إرسال روابط الحزم المستقلة التي يتم إنشاؤها بواسطة Kaspersky Security Center إلى مستخدمي الجهاز. الحزم المستقلة هي وحدات نمطية تنفيذية تحتوي على حزم التوزيع الخاصة بالتطبيقات المحددة، مع إعدادات محددة مسبقًا.

بعد تثبيت عميل الشبكة على جهاز، يمكنك إجراء التثبيت عن بعد لتطبيقات Kaspersky على هذا الجهاز من خلال عميل الشبكة هذا. يتم نقل حزمة التوزيع الخاصة بتطبيق ما المراد تثبيتها عبر قنوات الاتصال بين عملاء الشبكة وخادم الإدارة، بالإضافة إلى إعدادات التثبيت المحددة بواسطة المسؤول. لنقل حزمة التوزيع ، يمكنك استخدام عقد توزيع الترحيل، أي نقاط التوزيع، وتسليم البث المتعدد، وما إلى ذلك.

عند تحديد طريقة وإستراتيجية لنشر التطبيقات في شبكة مُدارة، يجب عليك وضع عدد من العوامل في الاعتبار (قائمة جزئية):

- تكوين شبكة المؤسسة
- إجمالي عدد الأجهزة.
- وجود أجهزة في شبكة المؤسسة ليست أعضاءً في مجال Active Directory؛ ووجود حسابات موحدة تتمتع بحقوق المسؤول على هذه الأجهزة.
- سعة القناة بين خادم الإدارة والأجهزة.
- نوع الاتصال بين خادم الإدارة والشبكات الفرعية البعيدة وسعة قنوات الشبكة في هذه الشبكات الفرعية.
- إعدادات الأمان المطبقة على الأجهزة البعيدة في بداية النشر. تسمح هذه المعلمات بإنشاء اتصال عن بُعد بالجهاز المُدار وبدء التثبيت.

تكوين أدوات التثبيت

قبل البدء في نشر تطبيقات Kaspersky على شبكة ما، يجب عليك تحديد إعدادات التثبيت، أي هذه التي يتم تحديدها أثناء تثبيت التطبيق. عند تثبيت عميل الشبكة، يجب عليك تحديد عنوان، واحد على الأقل، للاتصال بخادم الإدارة؛ كما يمكن أن تكون بعض الإعدادات المتقدمة مطلوبة. بناءً على طريقة التثبيت التي حددتها، يمكنك تحديد الإعدادات بطرق مختلفة. في الحالات الأكثر بساطة (تثبيت تفاعلي يدوي على جهاز محدد)، يمكن تحديد كل الإعدادات ذات الصلة من خلال واجهة المستخدم الخاصة بالمثبّت.

طريقة تحديد الإعدادات هذه غير مناسبة للتثبيت الصامت للتطبيقات على مجموعات من الأجهزة. بشكل عام، يجب على المسؤول تحديد قيم للإعدادات في الوضع المركزي؛ ويمكن استخدام هذه القيم لاحقًا للتثبيت الصامت على الأجهزة المتصلة بالشبكة التي يتم تحديدها.

حزم التثبيت

الطريقة الأولى والرئيسية لتحديد إعدادات التثبيت الخاصة بالتطبيقات تتميز بأنها متعددة الأغراض وبذلك فهي مناسبة لكل طرق التثبيت، باستخدام كلاً من أدوات Kaspersky Security Center وأغلب أدوات الجهة الخارجية. تتكون هذه الطريقة من إنشاء حزم تثبيت للتطبيقات في Kaspersky Security Center.

يتم إنشاء حزم التثبيت باستخدام الطرق التالية:

- تلقائيًا: من حزم توزيع محددة، على أساس أدوات الوصف المضمنة (ملفات بامتداد kud. والتي تحتوي على قواعد للتثبيت وتحليل النتائج ومعلومات أخرى)
- من الملفات القابلة للتنفيذ للمُثبتات أو من المُثبتات بالتنسيق الأصلي (.msi و.deb و.rpm) ، للتطبيقات القياسية أو المدعومة

حزم التثبيت التي تم إنشاؤها مرتبة ترتيبًا هرميًا كمجلدات بها مجلدات فرعية وملفات. بالإضافة إلى حزمة التوزيع الأصلية، تحتوي حزمة التثبيت على إعدادات قابلة للتحرير (تتضمن إعدادات المثبت وقواعد معالجة حالات مثل ضرورة إعادة تشغيل نظام التشغيل لإكمال التثبيت) بالإضافة إلى الوحدات النمطية الإضافية الثانوية.

قيم إعدادات التثبيت التي قد تكون خاصة بتطبيق واحد مدعوم يمكن تحديدها في واجهة المستخدم الخاصة بوحدة تحكم الإدارة عند إنشاء حزمة التثبيت. عند إجراء تثبيت التطبيقات عن بُعد باستخدام أدوات Kaspersky Security Center tools، يتم تسليم حزم التثبيت إلى الأجهزة وبذلك يمكن أن يؤدي تشغيل مثبّت تطبيق ما إلى جعل كل الإعدادات المحددة للمسؤول متوفرة لهذا التطبيق. عند استخدام أدوات جهة خارجية لتثبيت تطبيقات Kaspersky، يجب عليك التأكد من توفر حزمة التثبيت بالكامل على الجهاز، أي توفر حزمة التوزيع وإعداداتها. يتم إنشاء حزم التثبيت وتخزينها بواسطة Kaspersky Security Center في مجلد فرعي مخصص في المجلد المشترك.

> لا تقم بتحديد أي من التفاصيل للحسابات المميزة في معلمات حزم التثبيت.

للحصول على إرشادات حول استخدام طريقة التكوين هذه لتطبيقات Kaspersky قبل نشرها باستخدام أدوات جهة خارجية، انظر القسم "النشر باستخدام سياسات المجموعة الخاصة بـ Microsoft Windows".

مباشرةً بعد تثبيت Kaspersky Security Center، يتم إنشاء عدد قليل من حزم التثبيت تلقائيًا؛ والتي تكون جاهزة للتثبيت وتشمل حزم عميل الشبكة وحزم تطبيقات الأمان الخاصة بـ Microsoft Windows.

> على الرغم من إمكانية تعيين مفتاح الترخيص لتطبيق ما في خصائص حزمة التثبيت، يُنصح بتجنب طريقة توزيع الترخيص هذه لأن فيها يكون من السهل الحصول على وصول قراءة لحزم التثبيت. ينبغي عليك استخدام مفاتيح الترخيص الموزعة تلقائيًا أو مهام تثبيت لمفاتيح الترخيص.

خصائص MSI وملفات التحويل

طريقة أخرى لتكوين تثبيت على النظام الأساسي Windows هي تحديد خصائص MSI وملفات التحويل. يمكن تطبيق هذه الطريقة في الحالات التالية:

- عند إجراء التثبيت من خلال سياسات المجموعة الخاصة بـ Windows أو عن طريق استخدام أدوات Microsoft العادية أو أدوات الجهة الخارجية الأخرى للتعامل مع سياسات المجموعة الخاصة بـ Windows
- عند تثبيت تطبيقات باستخدام أدوات الجهة الخارجية المخصصة للتعامل مع تنسيق المثبتات في Microsoft.

النشر باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد.

عند توفر أي أدوات لتثبيت التطبيقات عن بُعد في مؤسسة ما (مثل Microsoft System Center)، فمن الملائم إجراء نشر أولي باستخدام هذه الأدوات.

يجب القيام بالإجراءات التالية:

- تحديد طريقة تكوين التثبيت الأنسب لأداة النشر المستخدمة.
- تحديد آلية المزامنة بين تعديل إعدادات حزم التثبيت (عبر واجهة وحدة تحكم الإدارة) وعمل أدوات الجهة الخارجية المحددة المستخدمة في نشر التطبيقات من بيانات حزمة التثبيت.
- عند إجراء التثبيت من مجلد مشترك، يجب عليك التأكد من أن مورد هذا الملف يحتوي على سعة كافية.

معلومات حول مهام التثبيت عن بُعد في Kaspersky Security Center

يقدم Kaspersky Security Center آليات مختلفة لتثبيت التطبيقات عن بُعد، والتي يتم تطبيقها كمهام تثبيت عن بُعد (التثبيت الإجباري، التثبيت عن طريق نسخ صورة القرص الثابت، التثبيت من خلال سياسات مجموعة Microsoft Windows). يمكنك إنشاء مهمة تثبيت عن بُعد لمجموعة إدارة محددة ولأجهزة محددة أو مجموعة من الأجهزة (يتم عرض تلك المهام في وحدة تحكم الإدارة، في المجلد **المهام**). عند إنشاء مهمة، يمكنك تحديد حزم التثبيت (الخاصة بعميل الشبكة و/ أو تطبيق آخر) التي سيتم تثبيتها في هذه المهمة، بالإضافة إلى تحديد إعدادات خاصة تحدد طريقة التثبيت عن بُعد. بالإضافة إلى ذلك، يمكنك استخدام معالج التثبيت عن بُعد، الذي يستند إلى إنشاء مهمة تثبيت عن بُعد ومراقبة النتائج.

تؤثر مهام مجموعات الإدارة على كلٍ من الأجهزة المضمنة في مجموعة محددة وكل الأجهزة الموجودة في كل المجموعات الفرعية داخل مجموعة الإدارة هذه. تغطي المهمة أجهزة خوادم الإدارة المضمنة في مجموعة ما أو أي من مجموعاتها الفرعية في حالة تمكين الإعداد المقابل في المهمة.

تحدّث المهام الأجهزة المحددة قائمة الأجهزة العميلة عند كل تشغيل وفقًا لمحتويات التحديد عند بدء تشغيل المهمة. إذا احتوي تحديد ما على أجهزة تم توصيلها بخوادم الإدارة الثانوية، ستعمل المهمة على هذه الأجهزة أيضًا. للحصول على تفاصيل حول هذه الإعدادات وطرق التثبيت، راجع ما يلي في هذا القسم.

لضمان نجاح تشغيل مهمة تثبيت عن بُعد على أجهزة متصلة بخوادم الإدارة الثانوية، يجب عليك استخدام مهمة الترحيل لترحيل حزم التثبيت التي استخدمتها المهمة الخاصة بك إلى خوادم الإدارة الثانوية المقابلة مقدمًا.

النشر عن طريق التقاط صورة جهاز ونسخها

إذا أردت تثبيت عميل الشبكة على أجهزة يجب تثبيت نظام تشغيل وبرنامج آخر عليها (أو إعادة تثبيتها)، يمكنك استخدام آلية التقاط صورة هذا الجهاز ونسخها.

لإجراء النشر عن طريق التقاط صورة محرك أقراص ثابت ونسخها:

1. أنشئ جهاز مرجعي مثبّت عليه نظام تشغيل وبرنامج ذي صلة، بما في ذلك عميل الشبكة وتطبيق أمان.

2. التقاط الصورة المرجعية على الجهاز وتوزيع هذه الصورة على أجهزة جديدة عبر مهمة Kaspersky Security Center المخصصة.

لالتقاط صور القرص وتثبيتها، يمكنك استخدام إما أدوات الجهة الخارجية المتوفرة في المؤسسة، أو الميزة المتوفرة (بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات) بواسطة Kaspersky Security Center.

إذا استخدمت أي أدوات جهة خارجية لمعالجة صور القرص، يجب عليك حذف المعلومات التي يستخدمها Kaspersky Security Center لتحديد الجهاز المدار، عند إجراء نشر على جهاز من صورة مرجعية. وإلا، فلن يتمكن خادم الإدارة بشكل صحيح من تمييز الأجهزة التي تم إنشاؤها عن طريق نسخ الصورة نفسها.

عند التقاط صورة قرص باستخدام أدوات Kaspersky Security Center، يتم حل هذه المشكلة تلقائيًا.

نسخ صورة قرص باستخدام أدوات الجهة الخارجية

عند استخدام أدوات الجهة الخارجية لالتقاط صورة جهاز مثّبت عليه عميل شبكة، استخدم طريقة من الطرق التالية:

- الطريقة الموصى بها. عند تثبيت عميل شبكة على جهاز مرجعي والتقاط صورة للجهاز قبل تشغيل خدمة عميل الشبكة (لأن المعلومات الفريدة التي تحدد الجهاز يتم إنشاؤها عند أول اتصال لعميل الشبكة بخادم الإدارة). بعد ذلك، من المستحسن أن تتجنب تشغيل خدمة عميل الشبكة حتى اكتمال عملية التقاط الصورة.

- على الجهاز المرجعي، قم بإيقاف خدمة عميل الشبكة وقم بتشغيل الأداة المساعدة klmover باستخدام مفتاح -dupfix. الأداة المساعدة klmover مضمنة في حزمة تثبيت عميل الشبكة. تجنب أي عمليات تشغيل لاحقة لخدمة عميل الشبكة حتى تكتمل عملية التقاط الصورة.

- من الضروري تشغيل الأداة المساعدة klmover باستخدام مفتاح -dupfix قبل أول تشغيل لخدمة عميل الشبكة على الأجهزة المستهدفة، عند بدء تشغيل نظام التشغيل لأول مرة بعد نشر الصورة. الأداة المساعدة klmover مضمنة في حزمة تثبيت عميل الشبكة.

- استخدم وضع استنساخ قرص عميل الشبكة.

إذا تم نسخ صورة محرك الأقراص الثابتة بشكل غير صحيح، يمكنك حل هذه المشكلة.

يمكنك أيضًا التقاط صورة لجهاز دون تثبيت عميل الشبكة. ولفعل ذلك، نفذ نشر الصورة على الأجهزة المستهدفة ثم انشر عميل الشبكة. وفي حالة استخدام هذه الطريقة، وفر الوصول إلى مجلد الشبكة باستخدام حزم التثبيت المستقلة من أحد الأجهزة.

النسخ غير الصحيح لصورة القرص الثابت

في حالة تم نسخ صورة قرص ثابت مثبّت عليها عميل شبكة بدون تطبيق قواعد النشر التالية، فقد يتم عرض بعض الأجهزة معًا كرمز واحد باسم يتغير باستمرار في وحدة تحكم الإدارة.

يمكنك حل هذه المشكلة باستخدام إحدى الطرق التالية:

- إزالة عميل الشبكة

هذه هي الطريقة الأكثر موثوقية. يجب عليك إزالة عميل الشبكة الموجود على الجهاز والذي تم نسخه بشكل غير صحيح من الصورة، باستخدام أدوات الجهة الخارجية، ثم أعد تثبيته مرة أخرى. لا يمكن إزالة عميل الشبكة باستخدام أدوات Kaspersky Security Center، لأن خادم الإدارة لا يمكنه التمييز بين الأجهزة الخاطئة (التي تتشارك جميعًا الرمز نفسه في وحدة تحكم الإدارة).

- تشغيل الأداة المساعدة klmover باستخدام مفتاح "-dupfix"

استخدم أدوات الجهة الخارجية لتشغيل الأداة المساعدة klmover، الموجودة في مجلد تثبيت عميل الشبكة، باستخدام مفتاح "-dupfix" (klmover -dupfix) مرة واحدة على الأجهزة الخاطئة (تلك التي تم نسخها بطريقة غير صحيحة من الصورة). لا يمكنك تشغيل الأداة باستخدام أدوات Kaspersky Security Center، لأن خادم الإدارة لا يمكنه التمييز بين الأجهزة الخاطئة (التي تتشارك جميعًا الرمز نفسه في وحدة تحكم الإدارة).

ثم قم بحذف الرمز المعروض عليه الأجهزة الخاطئة قبل قيامك بتشغيل الأداة المساعدة.

- قم بتشديد القواعد الخاصة باكتشاف الأجهزة المنسوخة بشكل غير صحيح.

هذه الطريقة قابلة للتطبيق فقط في حالة تثبيت خادم الإدارة ووكلاء الشبكة من الإصدار 10 Service Pack 1 أو الإصدارات الأحدث.

يجب تشديد القواعد الخاصة باكتشاف عملاء الشبكة المنسوخة بشكل غير صحيح وبذلك يمكن أن يؤدي تغيير اسم NetBIOS الخاص بالجهاز إلى "الإصلاح" التلقائي لعملاء الشبكة هؤلاء (بافتراض أن كل الأجهزة المنسوخة لها أسماء NetBIOS فريدة).

على الجهاز المثبت عليه خادم الإدارة، يجب عليك استيراد ملف السجل المعروض أدناه إلى السجل ثم إعادة تشغيل خدمة خادم الإدارة.

- في حالة تثبيت نظام تشغيل 32 بت على الجهاز المثبّت عليه خادم الإدارة:

```
REGEDIT4
[ServerFlags\1.0.0.0\1093\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE]
00000003:dword="KLSRV_HST_VM_REVERT_DETECTION"
```

- في حالة تثبيت نظام تشغيل 64 بت على الجهاز المثبّت عليه خادم الإدارة:

```
REGEDIT4
[ServerFlags\1.0.0.0\1093\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE]
00000003:dword="KLSRV_HST_VM_REVERT_DETECTION"
```

النشر باستخدام سياسات المجموعة الخاصة بـ Microsoft Windows

من المستحسن إجراء النشر الأولي لعملاء الشبكة عبر سياسات مجموعة Microsoft Windows في حالة الوفاء بالشروط التالية:

- أن يكون هذا الجهاز عضوًا في مجال Active Directory
- يتيح لك نظام النشر الانتظار لإعادة التشغيل الروتيني التالي للأجهزة الهدف قبل بدء نشر عملاء الشبكة عليها (أو يمكنك إجبار تطبيق سياسة مجموعة Windows على هذه الأجهزة.)

يتكون نظام النشر هذا مما يلي:

- توجد حزمة توزيع التطبيق بتنسيق مثبّت Microsoft (حزمة MSI) في مجلد مشترك (هو المجلد الذي تحتوي فيه حسابات LocalSystem الخاصة بالأجهزة الهدف على أذونات قراءة).
- في سياسة مجموعة Active Directory، يتم إنشاء كائن تثبيت لحزمة التوزيع.
- يتم تعيين نطاق التثبيت عن طريق تحديد الوحدة التنظيمية (OU) و/أو مجموعة الأمان التي تحتوي على الأجهزة الهدف.
- في المرة القادمة التي يتم فيها تسجيل دخول جهاز هدف إلى المجال (قبل دخول مستخدمي الجهاز إلى النظام)، يتم التحقق من كل التطبيقات المثبتة بحثًا عن التطبيق المطلوب. في حالة عدم العثور على التطبيق، يتم تنزيل حزمة التوزيع من المورد المحدد في السياسة ثم يتم تثبيتها.

يتميز نظام النشر هذا بأن التطبيقات المعيّنة يتم تثبيتها على الأجهزة الهدف أثناء تحميل نظام التشغيل، أي حتى قبل دخول المستخدم إلى النظام. حتى وإن قام شخص يملك الحقوق الكافية بإزالة التطبيق، فسيتم إعادة تثبيته عند بدء التشغيل التالي لنظام التشغيل. نقطة ضعف نظام النشر هذا هي أن التغييرات التي يقوم بها المسؤول على سياسة المجموعة لن تسري حتى تتم إعادة تشغيل الأجهزة (في حالة عدم تضمين أدوات إضافية).

يمكنك استخدام سياسات المجموعة لتثبيت كلاً من عميل الشبكة والتطبيقات الأخرى إذا كانت المثبتات الخاصة بها بتنسيق مثبّت Windows.

عند تحديد نظام النشر هذا، يجب عليك أيضًا تقييم الحمل على مورد الملف الذي سيتم نسخ الملفات منه إلى الأجهزة بعد تطبيق سياسة مجموعة Windows.

التعامل مع سياسات Microsoft Windows عبر مهمة التثبيت عن بُعد الخاصة بـ Kaspersky Security Center

الطريقة الأسهل لتثبيت التطبيقات من خلال سياسات المجموعة الخاصة بـ Microsoft Windows هي تحديد خيار **تعيين تثبيت الحزمة في سياسات مجموعة Active Directory** في خصائص مهمة التثبيت عن بُعد الخاصة بـ Kaspersky Security Center. في هذه الحالة، يقوم خادم الإدارة تلقائيًا بالإجراءات التالية عند تشغيل المهمة:

- إنشاء الكائنات المطلوبة في سياسة المجموعة الخاصة بـ Microsoft Windows.
- إنشاء security groups مخصصة، تشمل الأجهزة الهدف الموجود في هذه المجموعات، وتقوم بتعيين تثبيت التطبيقات المحددة لها. سيتم تحديث security groups عند كل تشغيل لمهمة، وفقًا لمجموعة الأجهزة في وقت التشغيل.

لجعل هذه الميزة قابلة للتشغيل، من خصائص المهمة، حدد حسابًا يحتوي على أذونات كتابة في سياسات مجموعة Active Directory.

إذا أردت تثبيت عميل الشبكة وتطبيق آخر خلال المهمة ذاتها، فسيتسبب تحديد خيار**تعيين تثبيت الحزمة في سياسات مجموعة Active Directory** في قيام التطبيق بإنشاء كائن تثبيت في سياسة Active Directory لعميل الشبكة فقط. سيتم تثبيت التطبيق الثاني المحدد في المهمة باستخدام أدوات عميل الشبكة بمجرد تثبيت عميل الشبكة على الجهاز. إذا أردت تثبيت تطبيق غير عميل الشبكة من خلال سياسات مجموعة Windows، فيجب عليك إنشاء مهمة تثبيت لحزمة التثبيت هذه فقط (بدون حزمة عميل الشبكة). لا يمكن تثبيت كل تطبيق باستخدام سياسات المجموعة من Microsoft Windows. لاكتشاف هذه الإمكانية، يمكنك الرجوع إلى المعلومات حول الطرق الممكنة لتثبيت التطبيق.

إذا كانت الكائنات المطلوبة يتم إنشاؤها في سياسة مجموعة باستخدام أدوات Kaspersky Security Center، فسيتم استخدام المجلد المشترك لـ Kaspersky Security Center كمصدر لحزمة التثبيت. عند التخطيط للنشر، يجب عليك ربط سرعة القراءة لهذا المجلد بعدد الأجهزة وحجم حزمة التوزيع التي سيتم تثبيتها. من المفيد تحديد موقع المجلد المشترك لـ Kaspersky Security Center في مستودعات ملفات مخصصةعالية الأداء.

بالإضافة إلى سهولة الاستخدام، يتميز الإنشاء التلقائي لسياسات مجموعة Windows عبر Kaspersky Security Center بهذه الميزة: عند التخطيط لتثبيت عميل الشبكة، يمكنك بسهولة تحديد مجموعة إدارة Kaspersky Security Center التي سيتم نقل الأجهزة تلقائيًا إليها بعد اكتمال التثبيت. يمكنك تحديد هذه المجموعة في معالج المهمة الجديدة أو في نافذة الإعدادات الخاصة بمهمة التثبيت عن بُعد.

عند التعامل مع سياسات مجموعة Windows عبر Kaspersky Security Center، يمكنك تحديد أجهزة لكائن سياسة المجموعة عن طريق إنشاء مجموعة أمان. يقوم Kaspersky Security Center بمزامنة محتويات مجموعة الأمان مع مجموعة الأجهزة الحالية في المهمة. عند استخدام أدوات أخرى لسياسات المجموعة، يمكنك ربط كائنات سياسات المجموعة بالوحدات التنظيمية الخاصة بـ Active Directory مباشرةً.

تثبيت التطبيقات بدون مساعدة عبر سياسات Microsoft Windows

يمكن للمسؤول إنشاء كائنات مطلوبة للتثبيت في سياسة مجموعة Windows بشكل مستقل. في هذه الحالة، يمكن للمسؤول توفير روابط للحزم المخزنة في المجلد المشترك الخاص بـ Kaspersky Security Center، أو تحميل هذه الحزم إلى خادم الملفات المخصص ثم توفير روابط للوصول إليها.

سيناريوهات التثبيت التالية ممكنة:

- يقوم المسؤول بإنشاء حزمة تثبيت وإعداد خصائصها في وحدة تحكم الإدارة. يوفر كائن سياسة المجموعة رابط إلى ملف MSI الخاص بهذه الحزمة المخزنة في المجلد المشترك الخاص بـ Kaspersky Security Center.
- يقوم المسؤول بإنشاء حزمة تثبيت وإعداد خصائصها في وحدة تحكم الإدارة. وبعدها يقوم المسؤول بنسخ المجلد الفرعي EXEC بكامله الخاص بهذه الحزمة من المجلد المشترك الخاص بـ Kaspersky Security Center إلى مجلد موجود على مورد ملفات محدد خاص بالمؤسسة. يوفر كائن سياسة المجموعة رابط إلى ملف MSI الخاص بهذه الحزمة المخزنة في مجلد فرعي على مورد ملفات مخصص خاص بالمؤسسة.
- يقوم المسؤول بتنزيل حزمة توزيع التطبيق (بما في ذلك الخاصة بعميل الشبكة) من الإنترنت وتحميلها إلى مورد الملفات المخصص الخاص بالمؤسسة. يوفر كائن سياسة المجموعة رابط إلى ملف MSI الخاص بهذه الحزمة المخزنة في مجلد فرعي على مورد ملفات مخصص خاص بالمؤسسة. يتم تحديد إعدادات التثبيت عن طريق تكوين خصائص MSI أو عن طريق تكوين ملفات تحويل MST.

النشر الإجباري عبر مهمة تثبيت عن بُعد من Kaspersky Security Center

لإجراء النشر الأولي لعميل الشبكة أو التطبيقات الأخرى، يمكنك فرض تثبيت حزم التثبيت المحددة باستخدام مهمة التثبيت عن بُعد في Kaspersky Security Center - شريطة أن يكون لكل جهاز حساب (حسابات) مستخدم يتمتع بحقوق المسؤول المحلي.

يمكن تطبيق التثبيت الإجباري أيضًا إذا تعذر الوصول المباشر إلى الأجهزة بواسطة خادم الإدارة: على سبيل المثال، تتواجد الأجهزة في شبكات معزولة أو في شبكة محلية بينما يوجد عنصر خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

في حالة النشر الأولي، لن يتم تثبيت عميل الشبكة. لذلك، في إعدادات مهمة التثبيت عن بعد، لا يمكنك تحديد توزيع الملفات المطلوبة لتثبيت التطبيق باستخدام عميل الشبكة. ويمكنك فقط اختيار توزيع الملفات باستخدام موارد نظام التشغيل عبر خادم الإدارة أو نقاط التوزيع.

يجب تشغيل خدمة خادم الإدارة تحت حساب يتمتع بامتيازات إدارية على الأجهزة المستهدفة. وبدلاً من ذلك، يمكنك تحديد حساب لديه حق الوصول إلى مشاركة admin$ في إعدادات مهمة التثبيت عن بُعد.

بشكل افتراضي، يتم تطبيق مهمة التثبيت عن بعد على الأجهزة باستخدام بيانات اعتماد الحساب الذي يعمل تحته خادم الإدارة. ومن المهم توضيح أن هذا هو الحساب المستخدم للوصول إلى مشاركة admin$، وليس الحساب الذي يتم تشغيل مهمة التثبيت عن بُعد تحته. ويتم إجراء التثبيت تحت حساب LocalSystem.

يمكنك تحديد أجهزة مستهدفة إما بشكل صريح (باستخدام قائمة) أو عن طريق تحديد مجموعة الإدارة الخاصة بـ Kaspersky Security Center التي ينتمون لها، أو عن طريق إنشاء مجموعة من الأجهزة بالاستناد إلى معيار محدد. يتم تحديد وقت بدء التثبيت بواسطة جدول المهمة. في حالة تمكين إعداد **Run missed tasks** في خصائص المهمة، فيمكن تشغيل المهمة إما فورًا أو بعد تشغيل الأجهزة المستهدفة أو عند نقلها إلى مجموعة الإدارة المستهدفة.

يتألف التثبيت الإجباري من تسليم حزم التثبيت إلى الأجهزة المستهدفة، والنسخ التالي للملفات إلى مورد admin$ على كل جهاز من الأجهزة المستهدفة، والتسجيل عن بُعد لخدمات الدعم على تلك الأجهزة. يتم تنفيذ تسليم حزم التثبيت إلى الأجهزة المستهدفة من خلال ميزة Kaspersky Security Center التي تضمن تفاعل الشبكة. يجب الوفاء بالشروط التالية في هذه الحالة:

- يمكن الوصول إلى الأجهزة المستهدفة من جانب خادم الإدارة أو من جانب نقطة التوزيع.
- يعمل تحليل الاسم للأجهزة الهدف بشكل صحيح على الشبكة.
- تظل المشاركات الإدارية (admin $) ممكّنة على الأجهزة الهدف.
- يتم تشغيل خدمات النظام التالية على الأجهزة المستهدفة:
  - الخادم (LanmanServer)

    بشكل افتراضي، يتم تشغيل هذه الخدمة.
  - مشغل عملية خادم DCOM (DcomLaunch)
  - مُعيّن نقطة نهاية RPC (RpcEptMapper)
  - استدعاء الإجراء عن بعد (RpcSs)
- تم فتح منفذ TCP 445 على الأجهزة المستهدفة لتمكين الوصول عن بعد من خلال Windows Management Instrumentation.

  يتم أيضًا فحص منفذ TCP 445 لتحديد نوع نظام التشغيل للجهاز المستهدف قبل إجراء التثبيت عن بُعد (في حالة عدم توفر منفذ UDP 137).

يتم استخدام منافذ TCP 139 وUDP 137 وUDP 138 بواسطة البروتوكولات القديمة ولم تعد ضرورية للتطبيقات الحالية.

يجب السماح بمنافذ الوصول الخارجي الديناميكية على جدار الحماية للاتصالات من خادم الإدارة ونقاط التوزيع إلى الأجهزة المستهدفة.

- يُسمح لإعدادات أمان سياسة مجال Active Directory بتوفير تشغيل بروتوكول NTLM أثناء نشر عميل الشبكة.
- يتم تعطيل وضع مشاركة الملفات البسيطة على الأجهزة المستهدفة التي تعمل بنظام التشغيل Microsoft Windows XP.
- على الأجهزة المستهدفة، يتم تعيين نموذج مشاركة الوصول والأمان على كلاسيكي - يتحقق المستخدمون المحليون من هوياتهم بأنفسهم. ولا يمكن بأي حال من الأحوال أن يكون مخصصًا للضيوف فقط - يتم التحقق من صحة المستخدمين المحليين كضيوف.
- يجب أن تكون الأجهزة الهدف أعضاءً في المجال، أو يجب إنشاء حسابات موحدة باستخدام حقوق المسؤول على الأجهزة الهدف مقدمًا.

لنشر عميل الشبكة أو التطبيقات الأخرى بنجاح على جهاز غير منضم إلى Windows Server 2003 أو مجال Active Directory أحدث، يجب عليك تعطيل التحكم في حساب المستخدم (UAC) عن بُعد على هذا الجهاز. ويعد التحكم في حساب المستخدم (UAC) عن بُعد أحد الأسباب التي تمنع الحسابات الإدارية المحلية من الوصول إلى admin$، وهو أمر ضروري للنشر الإجباري لعميل الشبكة أو التطبيقات الأخرى. ولا يؤثر تعطيل التحكم في حساب المستخدم عن بُعد على التحكم في حساب المستخدم المحلي.

أثناء التثبيت على أجهزة جديدة لم يتم تخصيصها بعد إلى أي من مجموعات إدارة Kaspersky Security Center، يمكنك فتح خصائص مهمة التثبيت عن بُعد وتحديد مجموعات الإدارة التي تريد نقل الأجهزة إليها بعد تثبيت عميل الشبكة.

عند إنشاء مهمة جماعية، ضع في اعتبارك أن كل مهمة جماعية تؤثر على كل الأجهزة الموجودة في كل المجموعات المتداخلة ضمن مجموعة محددة. لذلك، يجب عليك تجنب تكرار مهام التثبيت في المجموعات الفرعية.

يعد التثبيت التلقائي طريقة مبسطة لإنشاء مهام التثبيت الإجباري للتطبيقات. ولفعل ذلك، يجب عليك فتح خصائص مجموعة الإدارة، وفتح قائمة حزم التثبيت، ثم تحديد تلك التي يجب تثبيتها على الأجهزة في هذه المجموعة. وكنتيجة لذلك، سيتم تثبيت حزم التثبيت المحددة تلقائيًا على كل الأجهزة في هذه المجموعة وكل مجموعاتها الفرعية. الفاصل الزمني الذي سيتم تثبيت الحزم عبره يعتمد على معدل نقل الشبكة وإجمالي عدد الأجهزة المتصلة بالشبكة.

لتقليل الحمل على خادم الإدارة أثناء تسليم حزم التثبيت إلى الأجهزة المستهدفة، يمكنك تحديد التثبيت عبر نقاط التوزيع في مهمة التثبيت. لاحظ أن طريقة التثبيت هذه تضع حملاً كبيرًا على الأجهزة التي تعمل كنقاط توزيع. ولذلك، يوصى بتحديد الأجهزة التي تلبي متطلبات نقاط التوزيع. وإذا كنت تستخدم نقاط التوزيع، فيجب عليك التأكد من وجودها في كل من الشبكات الفرعية المعزولة التي تستضيف الأجهزة المستهدفة.

قد يكون استخدام نقاط التوزيع كمراكز تثبيت محلية مفيدًا عند القيام بالتثبيت على أجهزة في الشبكات الفرعية التي تتصل بخادم الإدارة عبر قناة منخفضة السعة في حين تتاح قناة أوسع بين الأجهزة في نفس الشبكة الفرعية.

علاوة على ذلك، يجب أن تتجاوز مساحة القرص الخالية في القسم الذي يحتوي على المجلد %ALLUSERSPROFILE%\Application adminkit\KasperskyLab\Data، بعدة مرات، الحجم الإجمالي لحزم توزيع التطبيقات المثبتة.

تشغيل الحزم المستقلة التي أنشأها Kaspersky Security Center

لا يمكن تطبيق الطرق الموضحة أعلاه للنشر الأولي لعميل الشبكة والتطبيقات الأخرى دائمًا بسبب تعذر تحقق كل الشروط القابلة للتطبيق. في مثل هذه الحالات، يمكنك إنشاء ملف تنفيذي مشترك يُسمى حزمة تثبيت مستقلة من خلال Kaspersky Security Center، باستخدام حزمة التثبيت ذات إعدادات التثبيت ذات الصلة التي تم إعدادها بواسطة المسؤول. يتم تخزين حزمة التثبيت المستقلة في المجلد المشترك لـ Kaspersky Security Center.

يمكنك استخدام Kaspersky Security Center لإرسال رسالة بريد إلكتروني إلى المستخدمين المحددين تحتوي على رابط هذا الملف في المجلد المشترك، مطالبًا إياهم بتشغيل الملف (إما في الوضع التفاعلي أو باستخدام المفتاح "-s" للتثبيت الصامت). يمكنك إرفاق حزمة تثبيت مستقلة برسالة بريد إلكتروني ثم إرسالها إلى مستخدمي الأجهزة التي لا يتوفر لها وصول إلى المجلد المشترك الخاص بـ Kaspersky Security Center. كما يمكن للمسؤول نسخ الحزمة المستقلة إلى محرك أقراص قابل للإزالة، وتسليمه إلى جهاز ذي صلة ثم تشغيله لاحقًا.

يمكنك إنشاء حزمة مستقلة من حزمة عميل شبكة أو حزمة تطبيق آخر (على سبيل المثال، تطبيق الأمان) أو كليهما. إذا تم إنشاء حزمة مستقلة من عميل شبكة وتطبيق آخر، يبدأ التثبيت بعميل الشبكة.

عند إنشاء حزمة مستقلة باستخدام عميل الشبكة، يمكنك تحديد مجموعة الإدارة التي سيتم نقل الأجهزة الجديدة إليها (الأجهزة التي لم يتم تخصيصها لأي مجموعات إدارة) عند اكتمال تثبيت عميل الشبكة عليها.

يمكن تشغيل الحزم المستقلة في الوضع التفاعلي (بشكل افتراضي)، وعرض نتائج تثبيت التطبيقات التي تحتوي عليها أو يمكن تشغيلها في الوضع الصامت (عند التشغيل باستخدام المفتاح "-s"). يمكن استخدام الوضع الصامت للتثبيت من البرامج النصية، على سبيل المثال، من البرامج النصية التي تم تكوينها للتشغيل بعد نشر صورة نظام التشغيل. يتم تحديد نتيجة التثبيت في الوضع الصامت عن طريق رمز الإرجاع الخاص بالعملية.

يحتوي عميل الشبكة المستقل لنظام Linux على اعتماد اختياري من أداة nmap. وإذا كانت أداة nmap مفقودة أو أقدم من الإصدار 6.0، فلن يتم دعم وظيفة Broadcast DHCP Discover.

خيارات التثبيت اليدوي للتطبيقات

يمكن للمسؤولين أو المستخدمين ذوي الخبرة تثبيت التطبيقات يدويًا في الوضع التفاعلي. يمكنهم استخدام إما حزم التوزيع الأصلية أو حزم التثبيت التي تم إنشاؤها منها وتخزينها في المجلد المشترك الخاص بـ Kaspersky Security Center. بشكل افتراضي، يتم تشغيل أدوات التثبيت في الوضع التفاعلي وتطالب المستخدمين بكل القيم المطلوبة. ولكن عند تشغيل العملية setup.exe من جذر حزمة تثبيت باستخدام المفتاح "-s"، سيعمل المثبت في الوضع الصامت وبالإعدادات التي تم تحديدها عند تكوين حزمة التثبيت.

عند تشغيل setup.exe من جذر حزمة تثبيت مخزنة في المجلد المشترك الخاص بـ Kaspersky Security Center، سيتم نسخ الحزمة أولاً إلى مجلد محلي مؤقت، ثم سيتم تشغيل مثبّت التطبيق من المجلد المحلي.

إنشاء ملف MST

لتحويل محتوى حزمة MSI وتطبيق الإعدادات المخصصة على ملف MSI موجود، يجب عليك إنشاء ملف تحويل بتنسيق MST. ولفعل ذلك، استخدم محرر Orca.exe المضمن في Windows SDK.

لإنشاء ملف MST:

1. قم بتشغيل محرر Orca.exe.
2. انتقل إلى علامة التبويب **ملف**، وفي القائمة انقر فوق **فتح**.
3. حدد ملف Kaspersky Network Agent.msi.
4. انتقل إلى علامة التبويب **التحويل**، وفي القائمة حدد **تحويل جديد**.
5. في عمود **الجداول**، حدد **الخاصية** واكتب القيم التالية:
   - 1=EULA
   - <Administration Server address>=SERVERADDRESS

   انقر على زر **حفظ**.
6. انتقل إلى علامة التبويب **التحويل**، وفي القائمة حدد **إنشاء تحويل**.
7. في النافذة التي تفتح، حدد اسمًا لملف التحويل الذي تقوم بإنشائه، ثم انقر فوق الزر **حفظ**.

   يتم حفظ ملف MST.

تثبيت التطبيقات عن بُعد على الأجهزة المثبت عليها عميل الشبكة.

في حالة إن كان عميل شبكة قابل للتشغيل ومتصل بخادم الإدارة الرئيسي (أو متصل بأي من الخوادم التابعة له) مثبتًا على جهاز ما، فيمكنك ترقية عميل الشبكة على هذا الجهاز، بالإضافة إلى تثبيت أي تطبيقات مدعومة أو ترقيتها أو إزالتها من خلال عميل الشبكة.

يمكنك تمكين خيار **استخدام عميل الشبكة** في خصائص مهمة التثبيت عن بُعد.

في حالة تحديد هذا الخيار، سيتم نقل حزم التثبيت التي تم تحديد إعدادات التثبيت بها من قِبل المسؤول إلى الأجهزة الهدف عبر قنوات الاتصال بين عميل الشبكة وخادم الإدارة.

لتحسين التحميل على خادم الإدارة وتقليل حركة المرور بين خادم الإدارة والأجهزة، من المفيد تعيين نقاط توزيع في كل شبكة عن بُعد أو في كل مجال بث (انظر القسم "حول نقاط التوزيع" و"إنشاء هيكل مجموعات الإدارة وتعيين نقاط التوزيع"). في هذه الحالة، يتم توزيع حزم التثبيت وإعدادات المثبت من خادم الإدارة إلى الأجهزة الهدف عبر نقاط التوزيع.

علاوةً على ذلك، يمكنك استخدام نقاط التوزيع لبث تسليم (متعدد الإرسال) لحزم التثبيت، مما يسمح بتقليل حركة مرور الشبكة بشكل كبير عند نشر التطبيقات.

عند نقل حزم التثبيت إلى الأجهزة الهدف عبر قنوات اتصال بين عملاء الشبكة وخادم الإدارة، كل حزم التثبيت التي تم تحضيرها للنقل سيتم تخزينها مؤقتًا في المجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\working.\FTServer. عند استخدام حزم تثبيت كبيرة متعددة من أنواع مختلفة وتضمين عدد كبير من نقاط التوزيع، قد يزداد حجم هذا المجلد بشكل كبير.

لا يمكن حذف الملفات من مجلد FTServer يدويًا. عند حذف حزم التثبيت الأصلية، سيتم حذف البيانات المقابلة لها تلقائيًا من المجلد FTServer.

يتم حفظ البيانات التي تستلمها نقاط التوزيع في المجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\FTClTmp$.

لا يمكن حذف الملفات من المجلد FTClTmp$ يدويًا. عند اكتمال المهام التي تستخدم بيانات من هذا المجلد، سيتم حذف محتويات هذا المجلد تلقائيًا.

ولأن حزم التثبيت يتم توزيعها عبر قنوات اتصال بين خادم الإدارة وعملاء الشبكة من مستودع وسيط بتنسيق محسّن لعمليات النقل عبر الشبكة، فلا يتم السماح بإحداث تغييرات في حزم التثبيت المخزنة في المجلد الأصلي لكل حزمة تثبيت. لن يتم تسجيل هذه التغييرات تلقائيًا بواسطة خادم الإدارة. إذا احتجت لتعديل ملفات حزم التثبيت يدويًا (على الرغم من أنه من المستحسن تجنب هذا السيناريو)، يجب عليك تحرير أيٍ من إعدادات حزمة التثبيت في وحدة تحكم الإدارة. يؤدي تحرير إعدادات حزمة تثبيت في وحدة تحكم الإدارة إلى قيام خادم الإدارة بتحديث صورة الحزمة في ذاكرة التخزين المؤقتة التي تم تحضيرها للنقل إلى الأجهزة الهدف.

إدارة عمليات إعادة تشغيل الجهاز في مهمة التثبيت عن بُعد

غالبًا ما تحتاج الأجهزة لإعادة التشغيل لإكمال تثبيت التطبيقات عن بُعد (بخاصةً في Windows).

في حالة استخدام مهمة التثبيت عن بُعد من Kaspersky Security Center، في معالج المهمة الجديدة أو في نافذة خصائص المهمة التي تم إنشاؤها (قسم **إعادة تشغيل نظام التشغيل**)، يمكنك تحديد الإجراء الذي سيتم اتخاذه عندما يتطلب جهاز Windows إعادة تشغيله:

- **عدم إعادة تشغيل الجهاز**. في هذه الحالة، لن يتم إجراء إعادة تشغيل تلقائي. لإكمال التثبيت، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). سيتم حفظ المعلومات حول إعادة التشغيل المطلوبة في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب لتثبيت المهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل مهمًا.

- **إعادة تشغيل الجهاز**. في هذه الحالة، تتم إعادة تشغيل الجهاز تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال التثبيت. هذا الخيار مفيد لمهام التثبيت على أجهزة تعمل على عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **مطالبة المستخدم باتخاذ إجراء**. في هذه الحالة، سيتم عرض تذكير إعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد الخيار **مطالبة المستخدم باتخاذ إجراء** هو الخيار الأكثر ملاءمةً لمحطات العمل حيث يحتاج المستخدمون لإمكانية تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

ملاءمة تحديث قواعد البيانات في حزمة تثبيت ما خاصة بتطبيق أمان

قبل بدء نشر الحماية، يجب عليك أن تضع في اعتبارك إمكانية تحديث قواعد بيانات مكافحة الفيروسات (بما في ذلك الوحدات النمطية للتصحيحات التلقائية) التي يتم شحنها مع حزمة التوزيع الخاصة بتطبيق الأمان. من المفيد تحديث قواعد البيانات الموجودة في حزمة تثبيت التطبيق قبل البدء في النشر (على سبيل المثال، باستخدام الأمر المقابل من قائمة السياق الخاصة بحزم التثبيت المحددة). سيقلل هذا من عدد عمليات إعادة التشغيل المطلوبة لإكمال نشر الحماية على الأجهزة الهدف.

استخدام الأدوات لتثبيت التطبيقات عن بُعد في Kaspersky Security Center لتشغيل الملفات التنفيذية ذات الصلة على الأجهزة المدارة

باستخدام معالج الحزمة الجديدة، يمكنك تحديد أي ملف تنفيذي وتحديد إعدادات سطر الأوامر الخاص به. للقيام بذلك، يمكنك إضافة إما الملف المحدد نفسه أو المجلد بالكامل المخزّن فيه هذا الملف لحزمة التثبيت. بعد ذلك، يجب عليك إنشاء مهمة التثبيت عن بُعد وتحديد حزمة التثبيت التي تم إنشاؤها.

عندما تكون المهمة قيد التشغيل، سيتم تشغيل الملف التنفيذي المحدد مع الإعدادات المحددة لموجه الأوامر على الأجهزة الهدف.

إذا كنت تستخدم مثبتات بتنسيق Microsoft Windows Installer (MSI)، يقوم Kaspersky Security Center بتحليل نتائج التثبيت بواسطة الأدوات القياسية.

في حالة توفر ترخيص إدارة الثغرات الأمنية والتصحيحات، يستخدم Kaspersky Security Center (عند إنشاء حزمة تثبيت لأي تطبيق مدعوم في بيئة الشركة) أيضًا قواعد التثبيت وتحليل نتائج التثبيت التي توجد في قاعدة البيانات القابلة للتحديث الخاص به.

وإلا، ستنتظر المهمة الافتراضية للملفات التنفيذية اكتمال العملية قيد التشغيل وكل عملياتها الفرعية. بعد اكتمال كل العمليات قيد التشغيل، ستكتمل المهمة بنجاح بعض النظر عن رمز الإرجاع الخاص بالعملية الأولية. لتغيير مثل هذا السلوك في هذه المهمة، قبل إنشاء المهمة، عليك تعديل الملفات ذات التنسيق .kpd يدويًا والتي أنشأها Kaspersky Security Center في مجلد حزمة التثبيت المنشأة حديثًا ومجلداتها الفرعية.

تستخدم ملفات .kpd ترميز ASCII. وتستخدم ملفات .kud ترميز Unicode.

لجعل المهمة لا تنتظر اكتمال العملية قيد التشغيل، قم بتعيين قيم إعداد الانتظار إلى 0 في القسم [SetupProcessResult]:

```
[SetupProcessResult]
0=Wait
```

لجعل المهمة تنتظر اكتمال العملية قيد التشغيل فقط على Windows، وليس اكتمال كل العمليات الفرعية، قم بتعيين قيمة إعداد WaitJob إلى 0 في القسم [SetupProcessResult]، على سبيل المثال:

```
[SetupProcessResult]
0=WaitJob
```

لكي تكتمل المهمة بنجاح أو ترجع خطأً بناءً على رمز الإرجاع لعملية التشغيل، أنشئ الملف التنفيذي .bat الذي يحفظ رمز الخطأ في ملف، على سبيل المثال:

```
setup.log < [ResponseResult] echo
setup.log << 2=echo ResultCode
exit 0
```

ثم قم بتعديل ملفات .kud التي تم إنشاؤها بواسطة Kaspersky Security Center في مجلد حزمة التثبيت التي تم إنشاؤه حديثًا:

```
[SetupMainResult]
setup.log=File
ResponseResult=Section
ResultCode=Value
[SetupMainResult_SuccessCodes]
.Installation completed successfully=0
[SetupMainResult_ErrorCodes]
Installation script error=1
Custom error=2
```

في هذه الحالة، أي رمز غير تلك المدرجة سيؤدي إلى إرجاع خطأ.

لعرض سلسلة تحتوي على تعليق عند اكتمال المهمة بنجاح أو عند حدوث خطأ في نتائج المهمة، قم بإدخال أوصاف مختصرة للأخطاء المقابلة لرموز الإرجاع الخاصة بالعملية في الأقسام [SetupProcessResult_SuccessCodes] و[SetupProcessResult_ErrorCodes] على سبيل المثال:

```
[SetupProcessResult_SuccessCodes]
Installation completed successfully =0
A restart is required to complete the installation=3010
[SetupProcessResult_ErrorCodes]
Installation canceled by the user=1602
Fatal error during installation=1603
```

لاستخدام أدوات Kaspersky Security Center لإدارة إعادة تشغيل الجهاز (إذا كانت إعادة التشغيل مطلوبة لإكمال عملية ما)، قم بإدراج رموز الإرجاع الخاصة بالعملية التي تشير إلى أنه يجب القيام بإعادة التشغيل، في القسم [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
=3010
```

مراقبة النشر

لمراقبة نشر Kaspersky Security Center وللتأكد من أن تطبيق الأمان وعميل الشبكة تم تثبيتهما على الأجهزة المدارة، يجب عليك التحقق من إشارة حركة المرور في القسم **النشر**. توجد إشارة المرور هذه في مساحة عمل عقدة خادم الإدارة في النافذة الرئيسية لوحدة تحكم الإدارة. تعكس إشارة حركة المرور حالة النشر الحالية. يتم عرض عدد الأجهزة المثبّت عليها عميل الشبكة وتطبيقات الأمان بجوار إشارة حركة المرور. عندما تكون أي مهام تثبيت قيد التشغيل، يمكنك مراقبة تقدمها هنا. في حالة حدوث أخطاء في التثبيت، يتم عرض عدد الأخطاء هنا. يمكنك عرض تفاصيل أي خطأ عن طريق النقر فوق الرابط.

يمكنك أيضًا استخدام مخطط النشر في مساحة العمل الخاصة بالمجلد **الأجهزة المُدارة** من علامة التبويب **المجموعات**. يعكس المخطط عملية النشر، ويوضح عدد الأجهزة التي لا تحتوي على عميل شبكة أو تحتوي على عميل شبكة أو تحتوي على عميل شبكة وتطبيق أمان.

للحصول على مزيد من المعلومات حول تقدم النشر (أو عمل مهمة تثبيت محددة) افتح نافذة النتائج الخاصة بمهمة التثبيت عن بُعد ذات الصلة: انقر بزر الماوس الأيمن فوق المهمة وحدد **النتائج** في قائمة السياق. تعرض النافذة قائمتين: العليا تحتوي على حالات المهمة على الأجهزة، بينما تحتوي السفلى على أحداث المهمة على الجهاز المحدد حاليًا في القائمة العليا.

تتم إضافة معلومات حول أخطاء النشر إلى سجل أحداث Kaspersky على خادم الإدارة. تتوفر معلومات حول الأخطاء أيضًا من خلال تحديد الحدث المقابل في عقدة خادم الإدارة على علامة التبويب **الأحداث**.

تكوين أدوات التثبيت

يقدم هذا القسم معلومات حول ملفات أدوات تثبيت Kaspersky Security Center وإعدادات التثبيت، بالإضافة إلى توصيات حول كيفية تثبيت خادم الإدارة وعميل الشبكة في الوضع الصامت.

معلومات عامة

أدوات تثبيت مكونات Kaspersky Security Center 15.1 (خادم الإدارة، وعميل الشبكة، ووحدة تحكم الإدارة) مضمنة في تقنية مثبّت Windows Installer. حزمة MSI هي أساس أداة التثبيت. يتيح تنسيق الحزمة استخدام كل الميزات التي يقدمها Windows Installer: وهي قابلية التوسع وتوفر نظام التصحيح ونظام التحويل والتثبيت المركزي من خلال حلول الجهة الخارجية والتسجيل الشفاف باستخدام نظام التشغيل.

التثبيت في الوضع الصامت (مع ملف الاستجابة)

تحتوي أدوات تثبيت خادم الإدارة وعميل الشبكة على ميزة العمل باستخدام ملف الاستجابة (ss_install.xml)، عندما تكون معلمات التثبيت في الوضع الصامت دون تضمين مشاركة المستخدم. يوجد الملف ss_install.xml في المجلد نفسه الذي توجد فيه الحزمة MSI، ويُستخدم تلقائيًا أثناء التثبيت في الوضع الصامت. يمكنك تمكين وضع التثبيت الصامت باستخدام مفتاح سطر الأوامر "/s".

نظرة عامة على تشغيل مثال كما يلي:

```
setup.exe /s
```

قبل بدء المُثبت في الوضع الصامت، اقرأ اتفاقية ترخيص المستخدم النهائي (EULA). إذا لم تتضمن مجموعة توزيع Kaspersky Security Center ملف TXT يحتوي على نصل اتفاقية ترخيص المستخدم النهائي، يمكنك تنزيل الملف من موقع ويب Kaspersky.

الملف ss_install.xml هو مثيل للتنسيق الداخلي لمعلمات مثبّت Kaspersky Security Center. تحتوي حزمة التوزيع على الملف ss_install.xml مع المعلمات الافتراضية.

يرجى عدم تعديل ملف ss_install.xml يدويًا. يمكن تعديل هذا الملف عبر أدوات Kaspersky Security Center عند تحرير معلمات حزم التثبيت في وحدة تحكم الإدارة.

لتعديل ملف الاستجابة لتثبيت خادم الإدارة:

1. افتح حزمة توزيع Kaspersky Security Center. إذا كنت تستخدم ملف EXE حزمة كاملة، قم بفك ضغطه.
2. من مجلد الخادم، افتح سطر الأوامر، ثم قم بتشغيل الأمر التالي:

   ```
   setup.exe /r ss_install.xml
   ```

   يبدأ مُثبِّت Kaspersky Security Center.
3. اتبع خطوات المعالج لتكوين تثبيت Kaspersky Security Center.

عند إكمال المعالج، يتم تعديل ملف الاستجابة تلقائيًا وفقًا للإعدادات الجديدة التي حددتها.

تثبيت عميل الشبكة في الوضع الصامت (دون ملف استجابة)

يمكنك تثبيت عميل الشبكة باستخدام حزمة msi واحدة، مع تحديد قيم خصائص MSI بالطريقة القياسية. يتيح هذا السيناريو تثبيت عميل الشبكة باستخدام سياسات المجموعة.

لا تقم بإعادة تسمية حزمة التثبيت Kaspersky Network Agent.msi. وقد يؤدي إعادة تسمية هذه الحزمة إلى حدوث أخطاء في التثبيت أثناء التحديثات المستقبلية لعميل الشبكة.

لتجنب التعارض بين المعلمات المحددة عبر خصائص MSI والمعلمات المحددة في ملف الاستجابة، يمكنك تعطيل ملف الاستجابة عن طريق تعيين الخاصية 1=DONT_USE_ANSWER_FILE. يقع ملف .MSI في حزمة توزيع Kaspersky Security Center، في المجلد exec\NetAgent\Packages. مثال على تشغيل مثبّت عميل الشبكة باستخدام حزمة msi يتم كما يلي.

يتطلب تثبيت عميل الشبكة في الوضع الصامت قبول بنود اتفاقية ترخيص المستخدم النهائي. استخدم معلمة 1=EULA، إذا قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها.

مثال:
```
1=kscserver.mycompany.com EULA=1 SERVERADDRESS=qn DONT_USE_ANSWER_FILE/ "Kaspersky Network Agent.msi" msiexec /i
```

يمكنك أيضًا تحديد معلمات التثبيت الخاصة بحزمة .msi عن طريق إعداد ملف الاستجابة مقدمًا (الملف ذي الامتداد .mst). يظهر هذا الأمر كما يلي:

مثال:
```
test2.mst;test.mst=qn TRANSFORMS/ "Kaspersky Network Agent.msi" msiexec /i
```

يمكنك تحديد ملفات استجابة متعددة في أمر واحد.

إذا كنت تريد ترقية عميل الشبكة باستخدام Windows Installer، فقم بتشغيل الأمر التالي:

```
nag_inst.log\temp\windows\:vx c*qn /l/ "Kaspersky Network Agent.msi" msiexec /i
vomus /norestart=ALL REINSTALLMODE=REINSTALL
```

تكوين التثبيت الجزئي عبر setup.exe

عند تشغيل تثبيت التطبيقات عبر setup.exe، يمكنك إضافة القيم الخاصة بأي خصائص لـ MSI إلى حزمة MSI.

يظهر هذا الأمر كما يلي:

مثال:
```
"PROPERTYVALUE2=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTY_NAME1"v/
```

معلمات تثبيت خادم الإدارة

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت خادم الإدارة. جميع المعلمات اختيارية، ماعدا الخاصة باتفاقية ترخيص المستخدم النهائي (EULA) وPRIVACYPOLICY (سياسة الخصوصية).

خاصية MSI	الوصف	القيم المتوفرة
EULA	الموافقة على شروط اتفاقية الترخيص (مطلوب)	• 1—لقد قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها. • قيمة أخرى أو بلا قيمة—لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت).
PRIVACYPOLICY	الموافقة على شروط سياسة الخصوصية (مطلوب)	• 1— أنني أدرك وأوافق على التعامل مع بياناتي ونقلها (بما في ذلك، نقلها إلى البلدان الثالثة) كما هو موضح في سياسة الخصوصية. أؤكد على أني قد قرأت سياسة الخصوصية وفهمتها بالكامل. • قيمة أخرى أو بلا قيمة— لا أوافق على بنود سياسة الخصوصية (لا يتم إجراء التثبيت).
INSTALLATIONMODETYPE	نوع تثبيت خادم الإدارة	• قياسي. • مخصص.
INSTALLDIR	مجلد تثبيت التطبيق	قيمة السلسلة.
ADDLOCAL	قائمة بالمكونات التي سيتم تثبيتها (مفصولة بفاصلة)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. قائمة الحد الأدنى من المكونات الكافية للتثبيت الصحيح لخادم الإدارة: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	حجم الشبكة	• NRT_1_100—من 1 إلى 100 جهاز. • NRT_100_1000—من 101 إلى 1000 جهاز. • NRT_GREATER_1000—أكثر من 1000 جهاز.
SRV_ACCOUNT_TYPE	طريقة تحديد المستخدم لتشغيل خدمة خادم الإدارة	• SrvAccountDefault—سيتم إنشاء حساب المستخدم تلقائيًا. • SrvAccountUser—يتم تحديد حساب المستخدم يدويًا.
SERVERACCOUNTNAME	اسم المستخدم للخدمة	قيمة السلسلة.
SERVERACCOUNTPWD	كلمة مرور المستخدم للخدمة	قيمة السلسلة.
DBTYPE	نوع قاعدة البيانات	• MySQL — سيتم استخدام قاعدة بيانات MySQL أو MariaDB • MSSQL— سيتم استخدام قاعدة بيانات Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	الاسم الكامل لخادم MySQL أو MariaDB	قيمة السلسلة.
MYSQLSERVERPORT	رقم منفذ الاتصال بخادم MySQL أو MariaDB	قيمة رقمية.
MYSQLDBNAME	اسم قاعدة بيانات خادم MySQL أو MariaDB	قيمة السلسلة.
MYSQLACCOUNTNAME	اسم المستخدم للاتصال بقاعدة بيانات خادم MySQL أو MariaDB	قيمة السلسلة.
MYSQLACCOUNTPWD	كلمة مرور المستخدم للاتصال بقاعدة بيانات خادم MySQL أو MariaDB	قيمة السلسلة.
MSSQLCONNECTIONTYPE	نوع استخدام قاعدة بيانات MSSQL	• InstallMSSEE — التثبيت من حزمة. • ChooseExisting — استخدام الخادم المثبّت.
MSSQLSERVERNAME	الاسم الكامل لمثيل خادم SQL Server	قيمة السلسلة.
MSSQLDBNAME	اسم قاعدة بيانات خادم SQL Server	قيمة السلسلة.
MSSQLAUTHTYPE	طريقة مصادقة الاتصال بخادم SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	اسم المستخدم للاتصال بخادم SQL Server في وضع SQLServer	قيمة السلسلة.
MSSQLACCOUNTPWD	كلمة مرور المستخدم للاتصال بخادم SQL Server في وضع SQLServer	قيمة السلسلة.
CREATE_SHARE_TYPE	طريقة تحديد مجلد مشترك	• إنشاء—إنشاء مجلد مشترك جديد. في هذه الحالة، يجب تحديد الخصائص التالية: • SHARELOCALPATH — المسار إلى مجلد محلي. • SHAREFOLDERNAME — اسم الشبكة لمجلد ما • Null — يجب تحديد خاصية EXISTSHAREFOLDERNAME.
EXISTSHAREFOLDERNAME	المسار الكامل لمجلد مشترك موجود	قيمة السلسلة.
SERVERPORT	رقم المنفذ الخاص بالاتصال بخادم الإدارة	قيمة رقمية.
SERVERSSLPORT	رقم منفذ إنشاء اتصال SSL بخادم الإدارة	قيمة رقمية.

خاصية MSI	الوصف	القيم المتوفرة
SERVERADDRESS	عنوان خادم الإدارة	قيمة السلسلة.
SERVERCERT2048BITS	حجم المفتاح لشهادة خادم الإدارة (بوحدات البت)	• 1—حجم المفتاح لشهادة خادم الإدارة هو 2048 بت. • 0—حجم المفتاح لشهادة خادم الإدارة هو 1024 بت. • إذا لم يتم تحديد قيمة، فيكون حجم المفتاح لشهادة خادم الإدارة هو 2048 بت.
MOBILESERVERADDRESS	عنوان خادم الإدارة للاتصال بالأجهزة المحمولة، يتم تجاهله إن لم يتم تحديد مكوّن MobileSupport	قيمة السلسلة.

معلمات تثبيت عميل الشبكة

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت عميل الشبكة. وجميع المعلمات اختيارية باستثناء اتفاقية ترخيص المستخدم النهائي (EULA) وSERVERADDRESS.

معلمات تثبيت عميل الشبكة في الوضع الصامت

خاصية MSI	الوصف	القيم المتوفرة
EULA	الموافقة على شروط اتفاقية الترخيص	• 1—أؤكد على أنني قرأت الشروط والأحكام الواردة في اتفاقية ترخيص المستخدم النهائي هذه بالكامل واستوعبتها وقبلتها1—أؤكد أنني قرأت شروط وأحكام اتفاقية ترخيص المستخدم النهائي وفهمتها وأوافق عليها بالكامل. • 0—لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت). • بلا قيمة—لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت).
DONT_USE_ANSWER_FILE	إعدادات تثبيت القراءة لملف الاستجابة	• 1—عدم الاستخدام. • قيمة أخرى أو دون قيمة — عدم القراءة.
INSTALLDIR	مسار لمجلد تثبيت عميل الشبكة	قيمة السلسلة.
SERVERADDRESS	عنوان خادم الإدارة (مطلوب)	قيمة السلسلة.
SERVERPORT	رقم منفذ الاتصال بخادم الإدارة	قيمة رقمية.
SERVERSSLPORT	عدد المنافذ لاتصال مشفر لخادم الإدارة باستخدام بروتوكول SSL	قيمة رقمية.
USESSL	سواء يتم استخدام اتصال SSL أم لا	• 1 — الاستخدام • قيمة أخرى أو دون قيمة — عدم الاستخدام.
OPENUDPPORT	سواء يتم فتح منفذ UDP أم لا	• 1 — فتح. • قيمة أخرى أو دون قيمة — عدم الفتح.
UDPPORT	رقم منفذ UDP	قيمة رقمية.
USEPROXY	سواء يتم استخدام خادم وكيل أم لا. لأغراض التوافق، لا يوصى بتحديد إعدادات اتصال الخادم الوكيل في إعدادات حزمة تثبيت عميل الشبكة.	• 1 — الاستخدام • قيمة أخرى أو دون قيمة — عدم الاستخدام.
موقع الوكيل (عنوان الوكيل:منفذ الوكيل)	عنوان الوكيل ورقم المنفذ للاتصال بالخادم الوكيل	قيمة السلسلة.
PROXYLOGIN	حساب للاتصال بخادم وكيل	قيمة السلسلة.
PROXYPASSWORD	كلمة مرور الحساب للاتصال بالخادم الوكيل (لا تحدد أي تفاصيل عن الحسابات المميزة في معلمات حزم التثبيت.)	قيمة السلسلة.
GATEWAYMODE	وضع استخدام عبّارة الاتصال	• 0 — عدم استخدام بوابة الاتصال. • 1 — استخدم عميل الشبكة هذا كبوابة اتصال • 2 — الاتصال بخادم الإدارة باستخدام بوابة الاتصال.
GATEWAYADDRESS	عنوان بوابة الاتصال	قيمة السلسلة.
CERTSELECTION	طريقة تلقي شهادة	• GetOnFirstConnection — تلقي شهادة من خادم الإدارة. • GetExistent — تحديد شهادة موجودة إذا كان هذا الخيار محددًا، فيجب تحديد الخاصية CERTFILE.

خاصية MSI	الوصف	القيم المتوفرة
CERTFILE	مسار إلى ملف الشهادة	قيمة السلسلة.
VMVDI	تمكين الوضع الديناميكي للبنية الأساسية لسطح المكتب الافتراضي (VDI).	• 1 — التمكين. • 0 — عدم التمكين. • بلا قيمة — لا تمكّن.
VMOPTIMIZE	ما إذا كانت إعدادات عميل الشبكة هي الأمثل لبرنامج Hypervisor	• 1 — التمكين. • 0 — عدم التمكين. • بلا قيمة — لا تمكّن.
LAUNCHPROGRAM	سواء لبدء خدمة عميل الشبكة بعد اكتمال التثبيت أم لا. يتم تجاهل المعلمة إذا كانت VMVDI=1	• 1 — البدء. • قيمة أخرى أو دون قيمة — عدم البدء.
NAGENTTAGS	علامة عميل الشبكة (لها الأولوية على العلامة الواردة في ملف الاستجابة)	قيمة السلسلة.

البنية التحتية الافتراضية

يدعم Kaspersky Security Center استخدام الأجهزة الظاهرية. يمكنك تثبيت عميل الشبكة وتطبيق الأمان على كل جهاز ظاهري، كما يمكنك حماية الأجهزة الظاهرية على مستوى مراقب الأجهزة الظاهرية. في الحالة الأولى، يمكنك استخدام إما تطبيق أمان قياسي أو Kaspersky Security for Virtualization Light Agent لحماية الأجهزة الظاهرية الخاصة بك. في الحالة الثانية، يمكنك استخدام Kaspersky Security for Virtualization Agentless .

Kaspersky Security Center يدعم عمليات عودة الأجهزة الافتراضية إلى حالتها السابقة.

نصائح لتقليل الحمل على الأجهزة الظاهرية

عند تثبيت عميل شبكة على جهاز ظاهري، ننصحك بالتفكير في تعطيل بعض مزايا Kaspersky Security Center التي يبدو أنها ذات فائدة بسيطة للأجهزة الظاهرية.

عند تثبيت عميل شبكة على جهاز ظاهري أو على قالب مخصص لإنشاء أجهزة ظاهرية، نحن ننصح بالإجراءات التالية:

- إذا كنت تجري تثبيتًا عن بُعد، ففي نافذة الخصائص الخاصة بحزمة تثبيت عميل الشبكة، في قسم **خيارات متقدمة)** حدد خيار **تحسين إعدادات البنية الأساسية لسطح المكتب الافتراضي (VDI)**.
- إذا كنت تُجري تثبيتًا تفاعليًا من خلال معالج، فمن نافذة المعالج، حدد خيار **تحسين إعدادات عميل الشبكة للبنية الأساسية الظاهرية**.

تحديد هذه الخيارات سيبدّل إعدادات عميل الشبكة وبذلك تظل المزايا التالية معطلة بشكل افتراضي (قبل تطبيق سياسة):

- استرجاع معلومات حول البرامج المثبتة
- استرجاع معلومات حول الأجهزة
- استرجاع معلومات حول الثغرات الأمنية المكتشفة
- استرجاع معلومات حول التحديثات المطلوبة

غالبًا ما تكون هذه المزايا غير ضرورية على الأجهزة الظاهرية لأنها تستخدم برنامج موحد وجهاز ظاهري.

يمكن التراجع عن تعطيل المزايا. إذا كانت أي من المزايا المعطلة مطلوبة، يمكنك تمكينها عبر سياسة عميل الشبكة أو عبر الإعدادات المحلية لعميل الشبكة. تتوفر الإعدادات المحلية لعميل الشبكة عبر قائمة السياق الخاصة بالجهاز ذي الصلة في وحدة تحكم الإدارة.

دعم الأجهزة الظاهرية الديناميكية

يدعم Kaspersky Security Center الأجهزة الافتراضية الديناميكية. إذا تم نشر بنية أساسية ظاهرية على شبكة المؤسسة، فيمكن استخدام أجهزة ظاهرية ديناميكية (مؤقتة) في حالات محددة. يتم إنشاء الأجهزة الظاهرية الديناميكية بأسماء فريدة بناءً على القالب الذي تم تحضيره بواسطة المسؤول. يعمل المستخدم على جهاز ظاهري لفترة، ثم بعد أن يتم إيقافه، ستتم إزالة هذا الجهاز الظاهري من البنية الأساسية. إذا تم نشر Kaspersky Security Center على شبكة مؤسسة، فستتم إضافة جهاز ظاهري مثبّت عليه عميل الشبكة إلى قاعدة بيانات خادم الإدارة. بعد إيقاف جهاز ظاهري، يجب حذف الإدخال المقابل أيضًا من قاعدة بيانات خادم الإدارة.

لتفعيل ميزة الحذف التلقائي للإدخالات على الأجهزة الظاهرية، عند تثبيت عميل الشبكة على قالب لأجهزة ظاهرية ديناميكية، حدد خيار **تمكين الوضع الديناميكي لـ VDI**:

- بالنسبة للتثبيت عن بُعد، في نافذة خصائص حزمة تثبيت عميل الشبكة (القسم **خيارات متقدمة**)
- للتثبيت التفاعلي - في معالج تثبيت عميل الشبكة

تجنب تحديد خيار **تمكين الوضع الديناميكي لـ VDI** عند تثبيت عميل الشبكة على الأجهزة الفعلية.

إذا أردت تخزين الأحداث من الأجهزة الظاهرية الديناميكية على خادم الإدارة لبعض الوقت بعد إزالة هذه الأجهزة الظاهرية، ففي نافذة خصائص خادم الإدارة وفي القسم **مستودع الأحداث** حدد خيار **تخزين الأحداث بعد حذف الأجهزة** وحدد الحد الأقصى لمدّة تخزين الأحداث (بالأيام).

لا نوصي بتمكين تشفير محرك الأقراص على الأجهزة الافتراضية الديناميكية.

دعم نسخ الأجهزة الظاهرية

عملية نسخ جهاز ظاهري باستخدام عميل شبكة مثبّت أو إنشاء واحد من قالب باستخدام عميل شبكة مثبّت هي عملية مشابهة لنشر عملاء الشبكة عن طريق التقاط صورة قرص ثابت ونسخها. لذلك، بشكل عام، عند نسخ الأجهزة الافتراضية، تحتاج إلى تنفيذ نفس الإجراءات كما هو الحال عند نشر عميل الشبكة عن طريق نسخ صورة قرص.

ولكن، الحالتان الموضحتان أدناه تعرضان عميل الشبكة، الذي يكتشف النسخ تلقائيًا. بسبب الأسباب الموضحة أعلاه، ليس عليك إجراء العمليات المعقدة الموضحة ضمن "النشر عن طريق التقاط صورة القرص الثابت لجهاز ما ونسخها":

- تم تحديد خيار **تمكين الوضع الديناميكي لـ VDI** عندما تم تثبيت عميل الشبكة—بعد كل إعادة تشغيل لنظام التشغيل، سيتم التعرف على الجهاز الظاهري كجهاز جديد، بغض النظر عما إذا كان تم نسخه أم لا.
- أن يكون واحد من مراقبي الأجهزة الظاهرية التالية قيد الاستخدام VMware™ أو Hyper V® أو Xen®: اكتشف عميل الشبكة عملية نسخ للجهاز الظاهري عن طريق معرّفات الأجهزة الظاهرية التي تم تغييرها.

تحليل التغييرات في الأجهزة الظاهرية ليست موثوق بها تمامًا. قبل تطبيق هذه الطريقة بشكل واسع، يجب عليك اختبارها على مجموعة صغيرة من الأجهزة الظاهرية الخاصة بإصدار مراقب الأجهزة الظاهرية المستخدم حاليًا في مؤسستك.

دعم عودة نظام الملفات الخاص بالأجهزة المثبّت عليها عميل الشبكة إلى حالته السابقة

يُعتبر Kaspersky Security Center تطبيقًا موزَّعًا. ستؤدي عودة نظام الملفات إلى الحالة السابقة على جهاز مثبّت عليه عميل الشبكة إلى عدم مزامنة البيانات وعمل Kaspersky Security Center بشكل غير صحيح.

يمكن إرجاع نظام الملفات (أو جزء منه) في الحالات التالية:

- عند نسخ صورة من القرص الثابت.
- عند استعادة حالة الجهاز الظاهري بواسطة البنية الأساسية الظاهرية.
- عند استعادة بيانات من نسخة احتياطية أو نقطة استرداد.

السيناريوهات التي يؤثر فيها برنامج جهة خارجية على الأجهزة المثبّت عليها عميل شبكة على المجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ هي فقط السيناريوهات الحرجة لـ Kaspersky Security Center. لذلك، يجب عليك دائمًا استثناء هذا المجلد من إجراء الاسترجاع، إن أمكن.

ولأن قواعد مكان العمل الخاصة ببعض المؤسسات تعمل على عودة نظام الملفات على الأجهزة إلى حالته السابقة، فقد تمت إضافة دعم عودة نظام الملفات على الأجهزة المثبّت عليها عميل شبكة إلى حالته السابقة إلى Kaspersky Security Center، بدءًا من الإصدار 10 من Maintenance Release 1 (يجب أن يكون خادم الإدارة وعملاء الشبكة من الإصدار 10 من Maintenance Release 1 أو الإصدارات الأحدث). عند اكتشاف ذلك، يتم إعادة توصيل هذه الأجهزة تلقائيًا إلى خادم الإدارة مع تطهير كامل للبيانات وإجراء مزامنة كاملة.

بشكل افتراضي، يتم تمكين دعم اكتشاف عودة نظام الملفات إلى حالته السابقة في Kaspersky Security Center 15.1.

على قدر الإمكان، تجنب إعادة مجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ إلى حالته السابقة على جهاز مثبّت عليه عميل شبكة، لأن إعادة المزامنة الكاملة للبيانات تتطلب كمية كبيرة من المصادر.

عودة حالة النظام إلى حالتها السابقة غير مسموح بها إطلاقًا على جهاز مثبّت عليه خادم الإدارة. كما لا تُستخدم عودة قاعدة البيانات إلى حالتها السابقة بواسطة خادم الإدارة.

يمكنك استعادة حالة خادم الإدارة من النسخ الاحتياطي عن طريق أداة klbackup المساعدة القياسية فقط.

التثبيت المحلي للتطبيقات

يوفر هذا القسم إجراء التثبيت الخاص بالتطبيقات التي يمكن تثبيتها على أجهزة محلية فقط.

لتنفيذ التثبيت المحلي للتطبيقات على جهاز عميل محدد، يجب أن تمتلك حقوق المسؤول على هذا الجهاز.

لتثبيت التطبيقات محليًا على جهاز عميل محدد:

1. قم بتثبيت عميل الشبكة على الجهاز العميل وتكوين الاتصال بين الجهاز العميل وخادم الإدارة.
2. قم بتثبيت التطبيقات الضرورية على الجهاز كما تم الوصف في الأدلة الخاصة بهذه التطبيقات.
3. قم بتثبيت مكون الإدارة الإضافي لكل تطبيق مثبت على محطة عمل المسؤول.

يدعم Kaspersky Security Center أيضًا خيار التثبيت المحلي للتطبيقات باستخدام حزمة تثبيت مستقلة. لا يدعم Kaspersky Security Center تثبيت جميع تطبيقات Kaspersky.

التثبيت المحلي لعميل الشبكة

لتثبيت عميل الشبكة على الجهاز محليًا:

1. على الجهاز، قم بتشغيل الملف setup.exe من حزمة التوزيع التي تم تنزيلها من الإنترنت. يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: الحصول على حزمة تثبيت عميل الشبكة من مجموعة توزيع Kaspersky Security Center.

   يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها.

2. في نافذة تحديد التطبيق، انقر فوق الرابط **تثبيت عميل شبكة Kaspersky Security Center** لبدء تشغيل معالج إعداد عميل الشبكة. اتبع إرشادات المعالج.

   a. **Administration Server**

   المنفذ

   يحدد المنفذ غير منفذ SSL الذي يستخدمه خادم الإدارة لتلقي الاتصالات من عملاء الشبكة.

   وبشكل افتراضي، يتم تعيين هذا الخيار على 14000.

   منفذ SSL

   يحدد منفذ SSL الذي يستخدمه خادم الإدارة لتلقي الاتصالات من عملاء الشبكة.

   وبشكل افتراضي، يتم تعيين هذا الخيار على 13000.

   استخدام SSL للاتصال بخادم الإدارة

   في حال تمكين هذا الخيار، يتم إجراء الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL.

   يتم تمكين هذا الخيار افتراضيًا.

   السماح لعميل الشبكة بفتح منفذ UDP

   في حالة تمكين هذا الخيار، يفتح المُثبت تلقائيًا المنفذ الذي يستخدمه خادم الإدارة لإدارة جهاز العميل وتلقي معلومات عنه.

   يتم تمكين هذا الخيار افتراضيًا.

   منفذ UDP

   يسمح لك بتكوين المنفذ الذي يستخدمه خادم الإدارة لإدارة الجهاز العميل وتلقي معلومات عنه.

   وبشكل افتراضي، يتم تعيين هذا الخيار على 15000.

   b. **تكوين الخادم الوكيل**

   استخدام الخادم الوكيل

   إذا تم تمكين هذا الخيار، يمكنك تحديد بيانات الاعتماد لمصادقة الخادم الوكيل.

   ونوصي بتحديد بيانات اعتماد حساب لديه الحد الأدنى من الامتيازات المطلوبة فقط لمصادقة الخادم الوكيل.

   يتم تعطيل هذا الخيار افتراضيًا.

   العنوان

المنفذ

الحساب

اسم حساب المستخدم الذي تم من خلاله إنشاء الاتصال بالخادم الوكيل.

ونوصي بتحديد بيانات اعتماد حساب لديه الحد الأدنى من الامتيازات المطلوبة فقط لمصادقة الخادم الوكيل.

كلمة المرور

كلمة مرور الحساب الذي من خلاله تم إنشاء الاتصال بالخادم الوكيل.

ونوصي بتحديد بيانات اعتماد حساب لديه الحد الأدنى من الامتيازات المطلوبة فقط لمصادقة الخادم الوكيل.

c. **بوابة الاتصال**

عدم استخدام بوابة الاتصال

استخدام عميل الشبكة كبوابة اتصال في DMZ

حدد هذا الخيار لاستخدام عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ) للاتصال بخادم الإدارة والتواصل معه والحفاظ على البيانات الموجودة على عميل الشبكة آمنة أثناء نقل البيانات.

الاتصال بخادم الإدارة باستخدام بوابة الاتصال

حدد هذا الخيار ثم حدد الجهاز الذي سيعمل كبوابة الاتصال.

d. **شهادة خادم الإدارة**

e. **علامات الوكيل**

f. **إعدادات متقدمة**

قم بالتثبيت التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة

ونوصي بإبقاء هذا الخيار في وضع التمكين. ويمكنك مسح هذا الخيار لتعطيل التحديث التلقائي والتصحيح لمكونات Kaspersky Security Center. يستطيع المسؤول إعادة تمكين التحديث والتصحيح التلقائي في وقت لاحق باستخدام سياسة.

يتم تعطيل هذا الخيار افتراضيًا.

قم بتمكين حماية خدمة عميل الشبكة

عند تمكين هذا الخيار، بعد تثبيت عميل الشبكة على جهاز مُدار، يتعذر إزالة المكون أو إعادة تكوينه دون الامتيازات المطلوبة. يتعذر إيقاف خدمة عميل الشبكة. هذا الخيار ليس له أي تأثير على وحدات التحكم في المجال.

قم بتمكين هذا الخيار لحماية عميل الشبكة في محطات العمل التي تعمل بحقوق المسؤول المحلي.

يتم تعطيل هذا الخيار افتراضيًا.

تمكين الوضع الديناميكي لـ VDI

إذا تم تمكين هذا الخيار، فسيتم تمكين الوضع الديناميكي للبنية الأساسية لسطح المكتب الافتراضي (VDI) بالنسبة إلى عميل الشبكة المثبت على الجهاز الافتراضي.

يتم تعطيل هذا الخيار افتراضيًا.

تحسين إعدادات عميل شبكة Kaspersky Security Center للبنية التحتية لسطح المكتب الافتراضي (VDI). تعطيل فحص الثغرات الأمنية وجرد التطبيقات والأجهزة. يمكنك تحرير الإعدادات الحالية من خلال سياسات عميل الشبكة.

إذا تم تمكين هذا الخيار، فسيتم تعطيل الميزات التالية في إعدادات عميل الشبكة:

- استرجاع معلومات حول البرامج المثبتة
- استرجاع معلومات حول الأجهزة
- استرجاع معلومات حول الثغرات الأمنية المكتشفة
- استرجاع معلومات حول التحديثات المطلوبة

يتم تعطيل هذا الخيار افتراضيًا.

g. **بدء التطبيق**

عند انتهاء معالج الإعداد، سيتم تثبيت عميل الشبكة على الجهاز.

يمكنك عرض خصائص خدمة عميل شبكة Kaspersky Security Center، ويمكنك كذلك بدء نشاط عميل الشبكة وإيقافه ومراقبته عن طريق استخدام أدوات Microsoft Windows القياسية: إدارة/خدمات الكمبيوتر.

تثبيت عميل الشبكة في الوضع الصامت

يمكن تثبيت عميل الشبكة في الوضع الصامت، أي، دون إدخال تفاعلي لمعلمات التثبيت. يستخدم التثبيت الصامت حزمة Windows Installer (MSI) لعميل الشبكة. يقع ملف .MSI في حزمة توزيع Kaspersky Security Center، في المجلد exec\NetAgent\Packages.

لا تقم بإعادة تسمية حزمة التثبيت Kaspersky Network Agent.msi. وقد يؤدي إعادة تسمية هذه الحزمة إلى حدوث أخطاء في التثبيت أثناء التحديثات المستقبلية لعميل الشبكة.

لا يمكن تثبيت عميل الشبكة من حزمة MSI إلا في الوضع الصامت، ولا يتم دعم التثبيت التفاعلي من حزمة MSI.

لتثبيت عميل الشبكة على جهاز محلي في الوضع الصامت:

1. أقرأ اتفاقية ترخيص المستخدم النهائي. استخدم الأمر أدناه فقط إذا فهمت ووافقت على شروط اتفاقية ترخيص المستخدم النهائي.
2. قم بتشغيل الأمر

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

حيث إن `setup_parameters` هي قائمة معلمات وقيمها الخاصة المفصولة بمسافة (`PROP1=PROP2VAL PROP2=PROP2VAL`).

وفي قائمة المعلمات، يجب عليك تضمين اتفاقية `EULA=1`. وإلا، فلن يتم تثبيت عميل الشبكة.

إذا كنت تستخدم إعدادات الاتصال القياسية لتطبيق Kaspersky Security Center وعميل الشبكة على الأجهزة البعيدة، فقم بتشغيل الأمر:

```
msiexec /i "Kaspersky Network Agent.msi" /qn* /lvx:C:\temp\windows\nag_inst.log
ks1=kscserver.mycompany.com EULA=SERVERADDRESS
```

`/lvx*` هو مفتاح سجلات الكتابات. يتم إنشاء السجل أثناء تثبيت عميل الشبكة وحفظه في C:\temp\windows\nag_inst.log.

بالإضافة إلى nag_inst.log، يقوم التطبيق بإنشاء ملف klssinstlib.log $ الذي يحتوي على سجل التثبيت. يتم تخزين هذا الملف في المجلد %windir\temp أو %temp%. لأغراض استكشاف الأخطاء وإصلاحها، قد تحتاج أنت أو أخصائي الدعم الفني في Kaspersky إلى كلا ملفي السجل — nag_inst.log و klssinstlib.log $.

وبالإضافة إلى ذلك، إذا كنت بحاجة إلى تحديد منفذ الاتصال بخادم الإدارة، فقم بتشغيل الأمر:

```
nag_inst.log\temp\windows\:vx c*qn /l/ "Kaspersky Network Agent.msi" msiexec /i
14000=1 SERVERPORT=kscserver.mycompany.com EULA=SERVERADDRESS
```

تتوافق معلمة SERVERPORT مع عدد منافذ الاتصال بخادم الإدارة.

يتم إدراج الأسماء والقيم المحتملة للمعلمات التي يمكن استخدامها عند تثبيت عميل الشبكة في الوضع الصامت في القسم معلمات تثبيت عميل الشبكة.

إذا كنت تريد ترقية عميل الشبكة باستخدام Windows Installer، فقم بتشغيل الأمر التالي:

```
nag_inst.log\temp\windows\:vx c*qn /l/ "Kaspersky Network Agent.msi" msiexec /i
vomus /norestart=ALL REINSTALLMODE=REINSTALL
```

تثبيت عميل الشبكة لنظام Linux في الوضع الصامت (مع ملف إجابات)

يمكنك تثبيت عميل الشبكة على أجهزة Linux باستخدام ملف إجابات - ملف نصي يحتوي على مجموعة مخصصة من معلمات التثبيت: المتغيرات والقيم الخاصة بها. يسمح لك استخدام ملف الإجابات هذا بتشغيل التثبيت في الوضع الصامت، أي دون مشاركة المستخدم.

لإجراء تثبيت عميل الشبكة لنظام Linux في الوضع الصامت:

1. قم بإعداد جهاز Linux ذي الصلة للتثبيت عن بُعد. قم بتنزيل حزمة التثبيت عن بُعد وإنشائها باستخدام حزمة .deb أو .rpm الخاصة بعميل الشبكة عن طريق أي نظام إدارة حزم مناسب.

2. إذا كنت ترغب في تثبيت وكيل الشبكة على الأجهزة التي تعمل بنظام التشغيل SUSE Linux Enterprise Server 15، فثبت أول حزمة insserv-Compatible لتكوين وكيل الشبكة.

   إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تستخدم نظام التشغيل RED OS 7.3.4 أو أحدث أو MSVSPHERE 9.2 أو أحدث، فقم بتثبيت حزمة libxcrypt-compat لكي يعمل عميل الشبكة بشكل صحيح.

3. أقرأ اتفاقية ترخيص المستخدم النهائي. لا تتبع الخطوات أدناه إلا إذا فهمت شروط اتفاقية ترخيص المستخدم النهائي ووافقت عليها.

4. أنشئ ملف الإجابات (بتنسيق TXT). أضف إلى ملف الإجابات قائمة من المتغيرات بتنسيق variable_value=VARIABLE_NAME، وكل متغير في سطر منفصل.

   للاستخدام الصحيح لملف الإجابات، يجب أن يتضمن فيه الحد الأدنى من المتغيرين المطلوبين:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   يمكنك أيضًا إضافة أي متغيرات اختيارية لاستخدام معلمات أكثر تحديدًا للتثبيت عن بُعد. يسرد الجدول التالي جميع المتغيرات التي يمكن تضمينها في ملف الإجابات:

متغيرات ملف الإجابات المستخدمة كمعلمات عميل الشبكة لتثبيت Linux في الوضع الصامت

متغيرات ملف الإجابات المستخدمة كمعلمات عميل الشبكة لتثبيت Linux في الوضع الصامت

اسم المتغير	مطلوب	الوصف	القيم الممكنة
KLNAGENT_SERVER	نعم	يحتوي على اسم خادم الإدارة المقدم كاسم مجال مؤهل بالكامل (FQDN) أو عنوان IP.	اسم DNS أو عنوان IP.
KLNAGENT_AUTOINSTALL	نعم	يحدد ما إذا كان وضع التثبيت الصامت تم تمكينه.	1 —تم تمكين الوضع الصامت؛ لا تتم مطالبة المستخدم بأي إجراءات أثناء التثبيت. أخرى —تم تعطيل الوضع الصامت؛ قد تتم مطالبة المستخدم بالإجراءات أثناء التثبيت.

EULA_ACCEPTED	نعم	يحدد ما إذا كان المستخدم يقبل اتفاقية ترخيص المستخدم النهائي (EULA) لعميل الشبكة ؛ عند فقدانه، يمكن تفسيره على أنه عدم قبول لاتفاقية ترخيص المستخدم النهائي.	1—أؤكد أنني قرأت شروط وأحكام اتفاقية ترخيص المستخدم النهائي وفهمتها وأوافق عليها بالكامل. أخرى أو غير محددة—لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت).
KLNAGENT_PROXY_USE	لا	يحدد ما إذا كان الاتصال بخادم الإدارة سيستخدم إعدادات الوكيل. القيمة الافتراضية هي 0.	1 —يتم استخدام إعدادات الوكيل. أخرى —لا يتم استخدام إعدادات الوكيل.
KLNAGENT_PROXY_ADDR	لا	يحدد عنوان الخادم الوكيل المستخدم للاتصال بخادم الإدارة.	اسم DNS أو عنوان IP.
KLNAGENT_PROXY_LOGIN	لا	يحدد اسم المستخدم المُستَخدم لتسجيل الدخول إلى خادم الوكيل.	أي اسم مستخدم موجود.
KLNAGENT_PROXY_PASSWORD	لا	يحدد كلمة مرور المستخدم المُستَخدمة لتسجيل الدخول إلى الخادم الوكيل.	أي مجموعة من الأحرف الأبجدية الرقمية التي يسمح بها تنسيق كلمة المرور في نظام التشغيل.
KLNAGENT_VM_VDI	لا	يحدد ما إذا كان عميل الشبكة مثبتًا على صورة لإنشاء أجهزة افتراضية ديناميكية.	1 —يتم تثبيت عميل الشبكة على صورة، والتي يتم استخدامها فيما بعد لإنشاء أجهزة افتراضية ديناميكية. أخرى —لا يتم استخدام أي صورة أثناء التثبيت.
KLNAGENT_VM_OPTIMIZE	لا	يحدد ما إذا كانت إعدادات عميل الشبكة هي الأمثل لبرنامج Hypervisor.	1 —يتم تعديل الإعدادات المحلية الافتراضية لـعميل الشبكة بحيث تسمح بالاستخدام الأمثل لبرنامج Hypervisor.
KLNAGENT_TAGS	لا	يسرد العلامات المعينة لمثيل عميل الشبكة.	واحد أو أكثر من أسماء العلامات مفصولة بفاصلة منقوطة.
KLNAGENT_UDP_PORT	لا	يحدد منفذ UDP الذي يستخدمه عميل الشبكة. القيمة الافتراضية هي 15000.	أي رقم منفذ موجود.
KLNAGENT_PORT	لا	يحدد المنفذ غير TLS الذي يستخدمه عميل الشبكة. القيمة الافتراضية هي 14000.	أي رقم منفذ موجود.
KLNAGENT_SSLPORT	لا	يحدد منفذ TLS الذي يستخدمه عميل الشبكة. القيمة الافتراضية هي 13000.	أي رقم منفذ موجود.
KLNAGENT_USESSL	لا	يحدد ما إذا كان أمان طبقة النقل (TLS) يستخدم للاتصال.	1 (افتراضي)— يتم استخدام TLS. أخرى—لا يتم استخدام TLS.
KLNAGENT_GW_MODE	لا	يحدد ما إذا كان سيتم استخدام بوابة الاتصال.	1 (افتراضي)— لم يتم تعديل الإعدادات الحالية (في المكالمة الأولى، ولم يتم تحديد بوابة اتصال). 2—لا يتم استخدام بوابة اتصال. 3—يتم استخدام بوابة الاتصال. KLNAGENT_GW_ADDRESS مطلوبة. 4— يتم استخدام مثيل عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ). شهادة الخادم مطلوبة.
KLNAGENT_GW_ADDRESS	لا	يحدد عنوان بوابة الاتصال. لا تنطبق القيمة إلا إذا كان KLNAGENT_GW_MODE=3.	اسم DNS أو عنوان IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	لا	للسماح بتشغيل تسجيل المستخدم كأداة مساعدة لمالك الجهاز بعد تثبيت عميل الشبكة. وفي حالة إيقاف التشغيل، فلن يكون التسجيل كمالك جهاز متاحًا للمستخدم.	1— سيتم تشغيل تسجيل المستخدم كأداة مساعدة لمالك الجهاز بعد تثبيت عميل الشبكة. غير ذلك - معطل.

5. قم بتشغيل تثبيت عميل الشبكة. يتم تمرير متغير البيئة KLAUTOANSWERS، الذي يحدد المسار إلى ملف الإجابات، إلى أمر التثبيت. قم بتشغيل أحد الأوامر التالية:

- لتثبيت عميل الشبكة من حزمة RPM إلى نظام تشغيل 32 بت، نفذ الأمر التالي:
  `sudo KLAUTOANSWERS=<المسار إلى ملف الإجابات> yum install ./klnagent -y <رقم الإصدار>.i386.rpm`
- لتثبيت عميل الشبكة من حزمة RPM إلى نظام تشغيل 64 بت، نفذ الأمر التالي:
  `sudo KLAUTOANSWERS=<المسار إلى ملف الإجابات> yum install ./klnagent64 -y <رقم الإصدار>.x86_64.rpm`
- لتثبيت عميل الشبكة من حزمة RPM على نظام تشغيل 64 بت لهندسة ARM، نفذ الأمر التالي:
  `sudo KLAUTOANSWERS=<المسار إلى ملف الإجابات> yum install ./klnagent64 -y <رقم الإصدار>.aarch64.rpm`
- لتثبيت عميل الشبكة من حزمة DEB إلى نظام تشغيل 32 بت ، نفذ الأمر التالي:
  `sudo KLAUTOANSWERS=<المسار إلى ملف الإجابات> apt install ./klnagent_<رقم الإصدار>.i386.deb`
- لتثبيت عميل الشبكة من حزمة DEB إلى نظام تشغيل 64 بت ، نفذ الأمر التالي:
  `sudo KLAUTOANSWERS=<المسار إلى ملف الإجابات> apt install ./klnagent64_<رقم الإصدار>.amd64.deb`
- لتثبيت عميل الشبكة من حزمة DEB على نظام تشغيل 64 بت لهندسة ARM، نفذ الأمر التالي:
  `sudo KLAUTOANSWERS=<المسار إلى ملف الإجابات> apt install ./klnagent64_<رقم الإصدار>.arm64.deb`

بناءً على تكوين نظام التشغيل، يمكنك أيضًا استخدام مديري حزم rpm أو dpkg أو dnf لتثبيت عميل الشبكة.

يبدأ تثبيت عميل الشبكة لنظام التشغيل Linux في الوضع الصامت؛ ولا تتم مطالبة المستخدم بأي إجراءات أثناء العملية.

تجهيز جهاز يعمل بنظام التشغيل Astra Linux في وضع بيئة البرامج المغلقة لتثبيت عميل الشبكة

قبل تثبيت عميل الشبكة على جهاز يعمل بنظام التشغيل Astra Linux في وضع بيئة البرنامج المغلق، يجب عليك تنفيذ إجرائين للتحضير - الإجراء الوارد في التعليمات أدناه وخطوات الإعداد العامة لأي جهاز Linux.

قم بتشغيل المتوفرة في هذه التعليمات من حساب يتمتع بامتيازات التعامل مع الجذر.

لتجهيز جهاز يعمل بنظام التشغيل Astra Linux في وضع بيئة البرامج المغلقة لتثبيت عميل الشبكة:

1. افتح الملف /etc/digsig/digsig_initramfs.conf، ثم حدد الإعداد التالي:
   `1=DIGSIG_ELF_MODE`
2. في سطر الأوامر، قم بتشغيل الأمر التالي لتثبيت حزمة التوافق:
   `apt install astra-digsig-oldkeys`
3. أنشئ دليلاً لمفتاح التطبيق:
   `/mkdir -p /etc/digsig/keys/legacy/kaspersky`
4. ضع مفتاح التطبيق /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg في الدليل الذي تم إنشاؤه في الخطوة السابقة:
   `/cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky`

إذا لم تتضمن مجموعة أدوات توزيع Kaspersky Security Center مفتاح التطبيق kaspersky_astra_pub_key.gpg، يمكنك تنزيله بالنقر فوق الرابط: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. قم بتحديث أقراص RAM:

```
update-initramfs -u -k all
```

أعد تشغيل النظام.

جهاز Linux جاهز لتثبيت عميل الشبكة. يمكنك تثبيت عميل الشبكة عن بُعد، في الوضع التفاعلي، أو في الوضع الصامت.

تثبيت عميل الشبكة لنظام التشغيل Linux في الوضع التفاعلي

توضح هذه المقالة كيفية تثبيت عميل الشبكة على أجهزة Linux في الوضع التفاعلي، عن طريق تحديد معلمات التثبيت خطوة بخطوة. وبدلاً من ذلك، يمكنك استخدام ملف إجابات — وهو ملف نصي يحتوي على مجموعة مخصصة من معلمات التثبيت: المتغيرات والقيم الخاصة بها. يسمح لك استخدام ملف الإجابات هذا بتشغيل التثبيت في الوضع الصامت، أي دون مشاركة المستخدم.

إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تستخدم نظام التشغيل RED OS 7.3.4 أو أحدث أو MSVSPHERE 9.2 أو أحدث، فقم بتثبيت حزمة libxcrypt-compat لكي يعمل عميل الشبكة بشكل صحيح.

لتثبيت عميل الشبكة في الوضع التفاعلي:

1. قم بتشغيل تثبيت عميل الشبكة. أدخل أحد الأوامر التالية، ويعتمد ذلك على توزيعة Linux لديك:

- لتثبيت عميل الشبكة من حزمة RPM إلى نظام تشغيل 32 بت:

```
# klnagent -i -yum <رقم الإصدار>.rpm.i386
```

- لتثبيت عميل الشبكة من حزمة RPM إلى نظام تشغيل 64 بت:

```
# klnagent64 -i -yum <رقم الإصدار>.rpm.x86_64
```

- لتثبيت عميل الشبكة من حزمة RPM على نظام تشغيل 64 بت لبنية Arm:

```
# klnagent64 -i -yum <رقم الإصدار>.rpm.aarch64
```

- لتثبيت عميل الشبكة من حزمة DEB إلى نظام تشغيل 32 بت:

```
# klnagent ./ install -apt <رقم الإصدار>_.deb_i386
```

- لتثبيت عميل الشبكة من حزمة DEB إلى نظام تشغيل 64 بت:

```
# klnagent64 ./ install -apt <رقم الإصدار>_.deb_amd64
```

- لتثبيت عميل الشبكة من حزمة DEB على نظام تشغيل 64 بت لبنية Arm:

```
# klnagent64 ./ install -apt <رقم الإصدار>_.deb_arm64
```

2. قم بتشغيل تكوين عميل الشبكة:

```
# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
```

3. أقرأ اتفاقية ترخيص المستخدم النهائي (EULA). يتم عرض النص في نافذة سطر الأوامر. اضغط على شريط المسافة لعرض جزء النص التالي. ثم عند المطالبة، أدخل واحدة من القيم التالية:

- اكتب y إذا كنت قد قرأت شروط اتفاقية ترخيص المستخدم النهائي (EULA).
- اكتب n إذا كنت لا تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA). لاستخدام عميل الشبكة، يجب أن تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA).
- أدخل r لإظهار اتفاقية ترخيص المستخدم النهائي مرة أخرى.

4. أدخل اسم DNS أو عنوان IP لخادم الإدارة.

5. أدخل رقم منفذ خادم الإدارة. يتم استخدام المنفذ 14000 بشكل افتراضي.

6. أدخل رقم منفذ SSL لخادم الإدارة. يتم استخدام المنفذ 13000 بشكل افتراضي.

7. أدخل y إذا كنت تريد استخدام تشفير SSL لحركة المرور بين عميل الشبكة وخادم الإدارة. وبخلاف ذلك، أدخل n.

8. حدد أحد الخيارات التالية لتكوين عميل الشبكة:

- [1] — عدم تكوين بوابة اتصال.
  لن يعمل جهازك كبوابة اتصال ولن يتصل بخادم الإدارة من خلال بوابة اتصال.
- [2] — عدم استخدام بوابة اتصال.
  لن يتصل جهازك بخادم الإدارة من خلال بوابة اتصال.
- [3] —الاتصال بخادم الإدارة باستخدام بوابة اتصال.
  سيتصل جهازك بخادم الإدارة من خلال بوابة اتصال.
- [4] — الاستخدام كبوابة اتصال.
  سيعمل جهازك كبوابة اتصال.

يتم تثبيت عميل الشبكة على جهاز Linux.

التثبيت المحلي لمكون الإدارة الإضافي للتطبيق

لتثبيت مكون الإدارة الإضافي للتطبيق:

على جهاز مثبت عليه وحدة تحكم الإدارة، قم بتشغيل الملف klcfginst.exe، المضمن في حزمة توزيع التطبيق.

يتم تضمين الملف klcfginst.exe في جميع التطبيقات التي يمكن إدارتها بواسطة Kaspersky Security Center. يتم تسهيل عملية التثبيت من خلال استخدام المعالج ولا تتطلب وجود أي تدخل يدوي لتكوين الإعدادات.

تثبيت التطبيقات في الوضع الصامت

لتثبيت تطبيق في الوضع الصامت:

1. قم بفتح نافذة التطبيق الرئيسية لـ Kaspersky Security Center.

2. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، في المجلد الفرعي **حزم التثبيت**، حدد حزمة التثبيت الخاصة بالتطبيق ذي الصلة أو قم بإنشاء حزمة تثبيت جديدة لهذا التطبيق.

سيتم تخزين حزمة التثبيت على خادم الإدارة في مجلد خدمة الحزم الموجود في المجلد المشترك. يوجد مجلد فرعي منفصل مقابل لكل حزمة تثبيت.

3. افتح المجلد الذي تم فيه تخزين حزمة التثبيت المطلوبة بأي من الطرق التالية:

- عن طريق نسخ المجلد المقابل لحزمة التثبيت ذات الصلة من خادم الإدارة إلى الجهاز العميل. ثم قم بفتح المجلد المنسوخ على الجهاز العميل.
- عن طريق فتح الجهاز العميل الموجود داخل المجلد المشترك المقابل لحزمة التثبيت الضرورية الموجودة على خادم الإدارة.

في حالة وجود المجلد المشترك على جهاز مثبت عليه Microsoft Windows Vista، يجب عليك تعيين القيمة **معطل** للإعداد **التحكم في حساب المستخدم: تشغيل جميع المسؤولين في وضع موافقة المسؤول** إعداد(**بدء** > **لوحة التحكم** > **الإدارة** > **سياسة الأمان المحلية** > **إعدادات الأمان**).

4. بناءً على التطبيق المحدد، قم بإجراء ما يلي:

- في حالة Kaspersky Anti-Virus for Windows Workstations وKaspersky Anti-Virus for Windows Servers وKaspersky Security Center، انتقل إلى المجلد الفرعي exec وقم بتشغيل الملف القابل للتنفيذ (ملف بامتداد exe.) الذي يتضمن المفتاح /s.
- في حالة تطبيقات Kaspersky الأخرى، قم بتشغيل الملف التنفيذي (ملف له الامتداد .exe) الذي يتضمن المفتاح /s في المجلد المفتوح.

تشغيل الملف التنفيذي باستخدام مفتاحي EULA=1 و PRIVACYPOLICY=1 يعني أنك قد قرأت بالكامل وتفهم وتقبل شروط اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية، على التوالي. كما أنك تدرك أنه يتم التعامل جميع بياناتك ونقلها (بما في ذلك، نقلها إلى البلدان الثالثة) كما هو موضح في سياسة الخصوصية. نص اتفاقية الترخيص وسياسة الخصوصية مُضمن في مجموعة توزيع Kaspersky Security Center. تُعد الموافقة على شروط اتفاقية الترخيص وسياسة الخصوصية أمرًا ضروريًا لتثبيت التطبيق أو ترقية إصدار سابق من التطبيق.

تثبيت التطبيقات باستخدام الحزم المستقلة

يتيح لك Kaspersky Security Center إنشاء حزم تثبيت مستقلة للتطبيقات. حزمة التثبيت المستقلة هي عبارة عن ملف تنفيذي يمكن إيجاده على خادم الويب، أو إرساله بواسطة البريد الإلكتروني، أو نقله إلى جهاز عميل بطريقة أخرى. يمكن تشغيل الملف الذي تم استلامه محليًا على الجهاز العميل لتثبيت تطبيق بدون استخدام Kaspersky Security Center.

يحتوي عميل الشبكة المستقل لنظام Linux على اعتماد اختياري من أداة nmap. وإذا كانت أداة nmap مفقودة أو أقدم من الإصدار 6.0، فلن يتم دعم وظيفة Broadcast DHCP Discover.

لتثبيت تطبيق باستخدام حزمة تثبيت مستقلة:

1. قم بالاتصال بخادم الإدارة المطلوب.

2. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.

3. في مساحة العمل، حدد حزمة التثبيت الخاصة بالتطبيق المطلوب.

4. يمكنك بدء عملية إنشاء حزمة التثبيت المستقلة بإحدى الطرق التالية:

- من خلال تحديد **إنشاء حزمة تثبيت مستقلة** في قائمة السياق الخاصة بحزمة التثبيت.
- من خلال النقر فوق الرابط **إنشاء حزمة تثبيت مستقلة** في مساحة عمل حزمة التثبيت.

يبدأ معالج إنشاء حزمة التثبيت المستقلة. اتبع إرشادات المعالج.
في الخطوة الأخيرة من المعالج، حدد طريقة لنقل حزمة التثبيت المستقلة إلى الجهاز العميل.

5. قم بنقل حزمة التثبيت المستقلة إلى الجهاز العميل.

6. قم بتشغيل حزمة التثبيت المستقلة على الجهاز العميل.

التطبيق المثبت حاليًا على الجهاز العميل بموجب الإعدادات المحددة في حزمة التثبيت المستقلة.

عند إنشاء حزمة تثبيت مستقلة، يتم نشرها تلقائيًا على خادم الويب. يتم عرض رابط تنزيل الحزمة المستقلة في قائمة حزم التثبيت المستقلة التي تم إنشاؤها. عند الضرورة، يمكنك إلغاء نشر الحزمة المستقلة المحددة وإعادة نشرها على خادم الويب. يتم استخدام المنفذ 8060 بشكل افتراضي لتنزيل حزم التثبيت المستقلة.

إعدادات حزمة تثبيت عميل الشبكة

لتكوين حزمة تثبيت عميل الشبكة:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.
إن المجلد **التثبيت عن بُعد** هو مجلد فرعي من المجلد **خيارات متقدمة** بشكل افتراضي.

2. في قائمة سياق حزمة تثبيت عميل الشبكة، حدد **خصائص**.

يتم فتح نافذة خصائص حزمة تثبيت عميل الشبكة.

عام

يعرض القسم **عام** معلومات عامة عن حزمة التثبيت:

- اسم حزمة التثبيت
- اسم وإصدار التطبيق الذي تم إنشاء حزمة التثبيت له
- حجم حزمة التثبيت
- تاريخ إنشاء حزمة التثبيت
- المسار إلى مجلد حزمة التثبيت

الإعدادات

يقدم هذا القسم الإعدادات اللازمة لضمان التشغيل السليم لعميل الشبكة بعد تثبيته مباشرةً. تكون الإعدادات الموجودة في هذا القسم متوفرة فقط على الأجهزة التي تعمل بنظام التشغيل Windows.

في مجموعة الإعدادات **المجلد الوجهة**، يمكنك تحديد مجلد الجهاز العميل الذي سيتم تثبيت عميل الشبكة فيه.

- **التثبيت في المجلد الافتراضي**

إذا تم تحديد هذا الخيار، فسيتم تثبيت عامل الشبكة في المجلد <محرك الأقراص>:\Program Files\Kaspersky Lab\NetworkAgent. إذا لم يكن هذا المجلد موجودًا، فسيتم إنشاؤه تلقائيًا.

يتم تحديد هذا الخيار افتراضيًا.

- **التثبيت في المجلد المحدد**

إذا تم تحديد هذا الخيار، فسيتم تثبيت عامل الشبكة في المجلد المحدد في حقل الإدخال.

في مجموعة الإعدادات التالية، يمكنك إعداد كلمة مرور لمهمة إلغاء تثبيت عميل الشبكة عن بُعد.

- **استخدام كلمة مرور إلغاء التثبيت**

إذا تم تمكين هذا الخيار، بالنقر فوق زر **تعديل**، فيمكنك إدخال كلمة مرور إزالة التثبيت (متاحة فقط لعميل الشبكة على الأجهزة التي تعمل بأنظمة التشغيل Windows).

يتم تعطيل هذا الخيار افتراضيًا.

- **الحالة**

حالة كلمة المرور: **تم تعيين كلمة المرور** أو **لم يتم تعيين كلمة مرور**.

بشكل افتراضي، تكون كلمة المرور غير مثبتة.

- **Protect the Network Agent service against unauthorized removal or termination, and prevent changes to the settings**

عند تمكين هذا الخيار، بعد تثبيت عميل الشبكة على جهاز مُدار، يتعذر إزالة المكون أو إعادة تكوينه دون الامتيازات المطلوبة. يتعذر إيقاف خدمة عميل الشبكة. هذا الخيار ليس له أي تأثير على وحدات التحكم في المجال.

قم بتمكين هذا الخيار لحماية عميل الشبكة في محطات العمل التي تعمل بحقوق المسؤول المحلي.

يتم تعطيل هذا الخيار افتراضيًا.

- **التثبيت التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة**

إذا تم تمكين هذا الخيار، فسيتم تلقائيًا تثبيت جميع التحديثات والتصحيحات التي تم تنزيلها لخادم الإدارة، وعميل الشبكة، ووحدة التحكم في الإدارة، وخادم iOS MDM.

إذا تم تعطيل هذا الخيار، فلن يتم تثبيت التحديثات والتصحيحات التي تم تنزيلها إلا بعد تغيير حالتها إلى تمت الموافقة. لن يتم تثبيت التحديثات والتصحيحات ذات الحالة غير محددة.

يتم تمكين هذا الخيار افتراضيًا.

الاتصال

في هذا القسم يمكنك تكوين اتصال عميل الشبكة بخادم الإدارة. لإنشاء اتصال، يمكنك استخدام بروتوكول SSL أو UDP. لتكوين الاتصال، حدد الإعدادات التالية:

- **خادم الإدارة**

عنوان الجهاز المثبت عليه خادم الإدارة.

- **المنفذ**

رقم المنفذ المستخدم في الاتصال.

- **منفذ SSL**

رقم المنفذ المستخدم في الاتصال عبر بروتوكول SSL.

- **استخدام شهادة الخادم**

إذا تم تمكين هذا الخيار، فستستخدم مصادقة وصول عميل الشبكة إلى خادم الإدارة ملف الشهادة الذي يمكنك تحديده بالنقر فوق زر **تصفح**.
إذا تم تعطيل هذا الخيار، فسيتم استلام ملف الشهادة من خادم الإدارة عند أول اتصال لعميل الشبكة بالعنوان المحدد في حقل **عنوان الخادم**.
نوصيك بعدم تعطيل هذا الخيار لأن الاستلام التلقائي لشهادة خادم الإدارة بواسطة عميل الشبكة عند الاتصال بخادم الإدارة يُعد غير آمن.
تكون خانة الاختيار هذه محددة بشكل افتراضي.

- **استخدام SSL**

في حال تمكين هذا الخيار، يتم إجراء الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL.
يتم تعطيل هذا الخيار افتراضيًا. نوصي بعدم تعطيل هذا الخيار حتى يظل اتصالك آمنًا.

- **استخدام منفذ UDP**

في حال تمكين هذا الخيار، يتم إجراء الاتصال بين عميل الشبكة وخادم الإدارة من خلال منفذ UDP. هذا يسمح بإدارة أجهزة العميل وتلقي معلومات عنها.
الجدول أدناه يوضح المنفذ الذي يجب فتحه على الأجهزة المدارة المثبت عليها عميل الشبكة. لذلك، نوصي بعدم تعطيل هذا الخيار.
يتم تمكين هذا الخيار افتراضيًا.

- **رقم منفذ UDP**

في هذا الحقل يمكنك تحديد المنفذ المطلوب لتوصيل خادم الإدارة بعميل الشبكة باستخدام بروتوكول UDP.
منفذ UDP الافتراضي هو 15000.

- **فتح منافذ عميل الشبكة في جدار حماية Microsoft Windows**

في حالة تمكين هذا الخيار، تتم إضافة المنافذ المستخدمة بواسطة عميل الشبكة إلى قائمة استثناءات جدار الحماية على نظام Microsoft Windows.
يتم تمكين هذا الخيار افتراضيًا.

- **Use proxy server**

في حالة تمكين هذا الخيار، حدد معلمات الخادم الوكيل:

- **Proxy server address**
- **Proxy server port**

إذا كان الخادم الوكيل يتطلب المصادقة، فقم بتمكين الخيار **Proxy server authentication** وحدد **User name** و**Password** للحساب الذي تم إنشاء اتصال بالخادم الوكيل باستخدامه. ونوصي بتحديد بيانات اعتماد حساب لديه الحد الأدنى من الامتيازات المطلوبة فقط لمصادقة الخادم الوكيل.

لأغراض التوافق، لا يوصى بتحديد إعدادات اتصال الخادم الوكيل في إعدادات حزمة تثبيت عميل الشبكة.

متقدم

في قسم **الإعدادات المتقدمة**، يمكنك تكوين كيفية استخدام بوابة الاتصال. لهذا الغرض، يمكنك إجراء ما يلي:

- استخدم عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت للاتصال بخادم الإدارة والتواصل معه و الحفاظ على البيانات الموجودة على عميل الشبكة آمنة أثناء نقل البيانات.

- اتصل بخادم الإدارة باستخدام بوابة اتصال لتقليل عدد الاتصالات بخادم الإدارة. في هذه الحالة، أدخل عنوان الجهاز الذي سيعمل كبوابة الاتصال في حقل **عنوان بوابة الاتصال**.

- قم بتكوين الاتصال للبنية التحتية الافتراضية لسطح المكتب (VDI) إذا كانت شبكتك تتضمن أجهزة افتراضية. في هذه الحالة، نفذ ما يلي:

- **تمكين الوضع الديناميكي لـ VDI**

إذا تم تمكين هذا الخيار، فسيتم تمكين الوضع الديناميكي للبنية الأساسية لسطح المكتب الافتراضي (VDI) بالنسبة إلى عميل الشبكة المثبت على الجهاز الافتراضي.

يتم تعطيل هذا الخيار افتراضيًا.

- **تحسين إعدادات البنية الأساسية لسطح المكتب الافتراضي (VDI)**

إذا تم تمكين هذا الخيار، فسيتم تعطيل الميزات التالية في إعدادات عميل الشبكة:

- استرجاع معلومات حول البرامج المثبتة
- استرجاع معلومات حول الأجهزة
- استرجاع معلومات حول الثغرات الأمنية المكتشفة
- استرجاع معلومات حول التحديثات المطلوبة

يتم تعطيل هذا الخيار افتراضيًا.

- **Allow running the user registration utility after Network Agent installation**

إذا تم تمكين هذا الخيار ، فسيتم تشغيل تسجيل المستخدم كأداة مساعدة لمالك الجهاز بعد تثبيت عميل الشبكة. يتم تعطيل هذا الخيار افتراضيًا.

المكونات الإضافية

في هذا القسم، يمكنك تحديد مكونات إضافية للتثبيت المتزامن مع عميل الشبكة.

العلامات

يعرض القسم **العلامات** قائمة بالكلمات الرئيسية (العلامات) التي بإمكان أجهزة العميل إضافتها عقب تثبيت عميل الشبكة. يمكنك إضافة أو إزالة علامات من القائمة، وكذلك إعادة تسميتها.

إذا تم تحديد خانة الاختيار هذه بجوار العلامة، فستتم إضافة هذه العلامة تلقائيًا إلى الأجهزة المدارة أثناء تثبيت عميل الشبكة.

إذا تم إلغاء تحديد خانة الاختيار الموجودة بجوار العلامة، فلن تتم إضافة هذه العلامة تلقائيًا إلى الأجهزة المُدارة أثناء تثبيت عميل الشبكة. يمكنك إضافة هذه العلامة تلقائيًا إلى الأجهزة.

عند إزالة علامة من القائمة، فسيتم إزالة العلامة تلقائيًا من جميع الأجهزة التي تمت إضافتها إليها.

محفوظات المراجعة

في هذا القسم، يمكنك عرض محفوظات المراجعات الخاصة بحزمة التثبيت. يمكنك مقارنة المراجعات وعرضها وحفظها على ملف وإضافة أوصاف مراجعات وتحريرها.

تكون إعدادات حزمة تثبيت عميل الشبكة متاحة مع أنظمة تشغيل محددة والموضحة في الجدول أدناه.

إعدادات حزمة تثبيت عميل الشبكة

قسم الخاصية	Windows	Mac	Linux
عام	✓	✓	✓
إعدادات	✓	—	—
الاتصال	✓	✓ (باستثناء **فتح منافذ عميل الشبكة في جدار حماية Microsoft Windows** وخيارات **استخدام الاكتشاف التلقائي فقط لخادم الوكيل**)	✓ (باستثناء **فتح منافذ عميل الشبكة في جدار حماية Microsoft Windows** وخيارات **استخدام الاكتشاف التلقائي فقط لخادم الوكيل**)

قسم الخاصية	Windows	Mac	Linux
خيارات متقدمة	✓	✓	✓
مكونات إضافية	✓	✓	✓
العلامات	✓	✓ (باستثناء قواعد وضع العلامات التلقائي)	✓ (باستثناء قواعد وضع العلامات التلقائي)
سجل المراجعة	✓	✓	✓

عرض سياسة الخصوصية

سياسة الخصوصية متاحة عبر الإنترنت على https://www.kaspersky.com/products-and-services-privacy-policy ؛ كما أنها متاحة في وضع عدم الاتصال أيضًا. يمكنك قراءة سياسة الخصوصية، على سبيل المثال، قبل تثبيت عميل الشبكة.

لقراءة سياسة الخصوصية في وضع عدم الاتصال:

1. بدء مثبّت Kaspersky Security Center.
2. في نافذة المثبت، انتقل إلى رابط **استخراج حزم التثبيت**.
3. في القائمة التي تفتح، حدد عميل شبكة Kaspersky Security Center ، ثم انقر على **التالي**.

يظهر ملف privacy_policy.txt على جهازك، في المجلد الذي حددته في المجلد الفرعي NetAgent.

نشر نظم إدارة الأجهزة المحمولة

يشرح هذا القسم نشر أنظمة إدارة جهاز المحمول باستخدام بروتوكولات iOS MDM و Kaspersky Endpoint Security.

نشر نظام للإدارة باستخدام بروتوكول iOS MDM

يسمح لك Kaspersky Security Center بإدارة الأجهزة المحمولة التي تعمل بنظام iOS. وأجهزة iOS MDM هي الأجهزة المحمولة بنظام iOS المتصلة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM والمُدارة بواسطة خادم الإدارة.

يتم توصيل الأجهزة المحمولة بخادم iOS MDM من خلال الخطوات التالية:

1. يقوم المسؤول بتثبيت خادم iOS MDM.
2. يحصل المسؤول على شهادة أسماء نقاط الوصول (APNs) (استلام شهادة أسماء نقاط الوصول (APNs)، https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   تتيح شهادة أسماء نقاط الوصول (APNs) لخادم الإدارة الاتصال بخادم APNs لإرسال إخطارات الرسائل إلى أجهزة iOS MDM.
3. يقوم المسؤول بتثبيت شهادة APN على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.
4. ينشئ المسؤول ملف تعريف iOS MDM لمستخدم الجهاز المحمول iOS.

   يحتوي ملف تعريف iOS MDM على مجموعة من الإعدادات لاتصال الأجهزة المحمولة التي تعمل بنظام iOS بخادم الإدارة.

بعد تثبيت ملف تعريف iOS MDM ومزامنة جهاز iOS MDM مع خادم الإدارة، يتم عرض الجهاز في المجلد **Mobile devices** وهو المجلد الفرعي للمجلد **Mobile Device Management** في شجرة وحدة التحكم.

تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

لتثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على جهاز محلي:

1. قم بتشغيل الملف التنفيذي setup.exe.

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها.

في نافذة تحديد التطبيقات، انقر فوق الرابط **تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM** لتشغيل معالج إعداد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

2. حدد المجلد الوجهة.

مجلد الوجهة الافتراضي هو <Disk>:\Mobile Device Management for iOS\Kaspersky Lab\Program Files\. في حالة عدم وجود هذا المجلد، يتم إنشاؤه بشكل تلقائي أثناء التثبيت. يمكنك تغيير المجلد الوجهة باستخدام الزر **استعراض**.

3. في نافذة المعالج **حدد إعدادات الاتصال بخادم الأجهزة المحمولة التي تعمل بنظام iOS**، في الحقل **منفذ خارجي للاتصال بخدمة iOS MDM** حدد منفذ خارجي لاتصال الأجهزة المحمولة بخدمة iOS MDM.

يتم استخدام المنفذ الخارجي 5223 بواسطة الأجهزة المحمولة للاتصال بخادم APNs. تأكد من المنفذ 5223 مفتوح في جدار الحماية للاتصال بنطاق العنوان 17.0.0.0/8.

يُستخدم المنفذ 443 للاتصال بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بشكل افتراضي. إذا كان المنفذ 443 قيد الاستخدام بالفعل بواسطة خدمة أخرى أو تطبيق أخر، فيمكن استبداله، على سبيل المثال، بالمنفذ 9443.

يستخدم خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM المنفذ الخارجي 2197 لإرسال إخطارات إلى خادم APNs.

يتم تشغيل خوادم APNs في وضع موازنة التحميل. لا تتصل الأجهزة المحمولة دائمًا بنفس عناوين IP لاستلام الإخطارات. نطاق العنوان 17.0.0.0/8 محجوز لـ Apple، ولذلك ننصح بتحديد هذا النطاق بالكامل كنطاق مسموح به في إعدادات جدار الحماية.

4. إذا كنت ترغب في تكوين منافذ التفاعل لمكونات التطبيق يدويًا، فحدد خيار **إعداد المنافذ المحلية يدويًا** ثم قم بتحديد قيم للإعدادات التالية:

- **منفذ للاتصال بعميل الشبكة**. في هذا الحقل، حدد منفذًا لاتصال خدمة iOS MDM بعميل الشبكة. رقم المنفذ الافتراضي هو 9799.
- **المنفذ المحلي للاتصال بخدمة iOS MDM**. في هذا الحقل يمكنك تحديد منفذًا محليًا لاتصال عميل الشبكة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. رقم المنفذ الافتراضي هو 9899.

يوصى باستخدام القيم الافتراضية.

5. في نافذة المعالج **العنوان الخارجي لخادم الجهاز المحمول**، في حقل **عنوان الويب للاتصال البعيد بخادم الجهاز المحمول**، حدد عنوان الجهاز العميل الذي سيتم تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عليه.

سيتم استخدام هذا العنوان لاتصال الأجهزة المحمولة المُدارة بخدمة iOS MDM. يجب أن يتوفر الجهاز العميل لاتصال أجهزة iOS MDM.

يمكنك تحديد عنوان كمبيوتر عميل بأيّ من التنسيقات التالية:

- رقم FQDN (مثل mdm.example.com)
- اسم NetBIOS للجهاز

يُرجى تجنب إضافة نظام URI ورقم المنفذ في سلسلة العنوان: ستتم إضافة هذه القيم تلقائيًا.

عند انتهاء المعالج، يتم تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على الجهاز المحلي. يتم عرض خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في المجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم.

تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الوضع الصامت

يتيح لك Kaspersky Security Center تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على جهاز محلي في الوضع الصامت، أي بدون الإدخالات التفاعلية لإعدادات التثبيت.

لتثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على جهاز محلي في الوضع الصامت:

1. أقرأ اتفاقية ترخيص المستخدم النهائي. استخدم الأمر أدناه فقط إذا فهمت ووافقت على شروط اتفاقية ترخيص المستخدم النهائي.

2. قم بتشغيل الأمر التالي:

```
"< setup_parameters > 1=1 EULA=DONT_USE_ANSWER_FILE"setup.exe /s /v\exec\.
```

حيث إن `setup_parameters` هو قائمة إعدادات وقيمها الخاصة المفصولة بمسافات (`PROP2VAL=PROP1VAL PROP2=PROP1`). يوجد الملف setup.exe في مجلد الخادم، والذي يُعد جزءً من مجموعة توزيع Kaspersky Security Center.

يتم إدراج الأسماء والقيم المحتملة للمعلمات التي يمكن استخدامها عند تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الوضع الصامت في الجدول أدناه. يمكن تحديد المعلمات في أي ترتيب مناسب.

معلمات تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الوضع الصامت

اسم المعلمة	وصف المعلمة	القيم المتوفرة
EULA	الموافقة على شروط اتفاقية ترخيص المستخدم النهائي لبرنامج. هذه المعلمة إلزامية.	• 1—لقد قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها. • قيمة أخرى أو بلا قيمة—لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت).
DONT_USE_ANSWER_FILE	ما إذا كان سيتم استخدام ملف XML مع إعدادات تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. يتم إدراج ملف XML في حزمة التثبيت أو يتم تخزينه على خادم الإدارة. لا يلزم تحديد مسار إضافي إلى الملف. هذه المعلمة إلزامية.	• 1—لا تستخدم ملف XML مع المعلمات. • قيمة أخرى أو بلا قيمة—استخدم ملف XML مع المعلمات.
INSTALLDIR	مجلد تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. هذه المعلمة اختيارية.	قيمة السلسلة، على سبيل المثال، `"\install\:C"\=INSTALLDIR`
CONNECTORPORT	المنفذ المحلي لاتصال خدمة iOS MDM بعميل الشبكة. رقم المنفذ الافتراضي هو 9799. هذه المعلمة اختيارية.	قيمة رقمية.
LOCALSERVERPORT	المنفذ المحلي لاتصال عميل الشبكة بخدمة iOS MDM. رقم المنفذ الافتراضي هو 9899. هذه المعلمة اختيارية.	قيمة رقمية.
EXTERNALSERVERPORT	منفذ لاتصال جهاز بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. رقم المنفذ الافتراضي هو 443. هذه المعلمة اختيارية.	قيمة رقمية.
EXTERNAL_SERVER_URL	العنوان الخارجي للجهاز العميل الذي سيتم تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عليه. سيتم استخدام هذا العنوان لاتصال الأجهزة المحمولة المُدارة بخدمة iOS MDM. يجب أن يكون الجهاز العميل متاحًا للاتصال عبر iOS MDM. يجب ألا يتضمن العنوان نظام عنوان URL أو رقم المنفذ، لأنه سيتم إضافة هذه القيم تلقائيًا. هذه المعلمة اختيارية.	• رقم FQDN (مثل mdm.example.com) • اسم NetBIOS للجهاز • عنوان IP الخاص بالجهاز

اسم المعلمة	وصف المعلمة	القيم المتوفرة
WORKFOLDER	مجلد عمل خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. إذا لم يتم تحديد مجلد عمل، فسيتم كتابة البيانات في المجلد الافتراضي. هذه المعلمة اختيارية.	قيمة السلسلة، على سبيل المثال، `"\work\:C"\=WORKFOLDER`
MTNCY	استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من الخوادم الافتراضية. هذه المعلمة اختيارية.	• 1—سيتم استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من خوادم الإدارة الافتراضية. • قيمة أخرى أو بلا قيمة—لن يتم استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من خوادم الإدارة الافتراضية.

مثال:

```
www.test-"\=9443 EXTERNAL_SERVER_URL=1 EXTERNALSERVERPORT=1 DONT_USE_ANSWER_FILE=EULA"setup.exe /s /v\exec\
""\mdm.com
```

يتم توفير تفاصيل معلمات تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في القسم "تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM".

سيناريوهات نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يمكن تحديد عدد نسخ خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM التي سيتم تثبيتها بناءً على الجهاز المتوفر أو العدد الإجمالي للأجهزة المحمولة المغطاة.

ولكن ضع في اعتبارك أن الحد الأقصى المستحسن لعدد الأجهزة المحمولة للتثبيت الواحد لـ Kaspersky Device Management for iOS هو 50 000 على الأكثر. لتقليل الحمل، يمكن توزيع مجموعة الأجهزة بالكامل بين خوادم متعددة مثبّت عليها خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

يتم إجراء مصادقة أجهزة iOS MDM عبر شهادة المستخدم (أي ملف تعريف مثبّت على جهاز يحتوي على شهادة مالك الجهاز). ولذا، يتوفر نظامي نشر لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM:

- النظام المبسط
- نظام النشر الذي يتضمن تفويض Kerberos مقيّد (KCD)

نظام النشر المبسّط

عند نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بموجب النظام المبسّط، تتصل الأجهزة المحمولة بخدمة iOS MDM على الويب مباشرةً. في هذه الحالة، يمكن استخدام شهادات المستخدم التي أصدرها خادم الإدارة فقط لمصادقة الأجهزة. التكامل مع البنية الأساسية للمفتاح العام (PKI) غير ممكن لشهادات المستخدم.

نظام النشر الذي يتضمن تفويض Kerberos مقيّد (KCD)

لاستخدام مخطط النشر مع تفويض Kerberos المقيد (KCD)، يجب تلبية المتطلبات التالية:

- يوجد خادم الإدارة وخادم iOS MDM على الشبكة الداخلية للمؤسسة.
- يتم استخدام الخادم الوكيل العكسي مع دعم KCD.

يعمل نظام النشر هذا على ما يلي:

- التكامل مع الخادم الوكيل العكسي الذي يدعم KCD
- استخدام KCD لمصادقة الأجهزة المحمولة
- التكامل مع PKI لتطبيق شهادات المستخدم

عند استخدام نظام النشر هذا، يجب عليك القيام بما يلي:

- في وحدة تحكم الإدارة، في إعدادات خدمة iOS MDM على الويب، حدد خانة الاختيار **ضمان التوافق مع تفويض Kerberos المقيد**.
- بالنسبة لشهادة خدمة iOS MDM على الويب، حدد الشهادة المخصصة التي تم تحديدها عندما تم نشر خدمة iOS MDM على الويب على الخادم الوكيل العكسي.
- يجب إصدار شهادات المستخدم لأجهزة iOS بواسطة هيئة إصدار الشهادات (CA) الخاصة بالمجال. إذا كان المجال يحتوي على هيئات إصدار شهادات جذر متعددة، يجب إصدار الشهادة بواسطة هيئة إصدار الشهادات التي تم تحديدها عندما تم نشر خدمة iOS MDM على الويب على الخادم الوكيل العكسي.

  يمكنك التأكد أن شهادة المستخدم متوافقة مع متطلب إصدار هيئة إصدار الشهادات عن طريق استخدام طريقة من الطرق التالية:

  - حدد شهادة المستخدم في معالج ملف تعريف iOS MDM الجديد وفي معالج تثبيت الشهادة.
  - دمج خادم الإدارة مع البنية الأساسية للمفتاح العام (PKI) وتحديد الإعداد المقابل في قواعد إصدار الشهادات:

    1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد المجلد الفرعي **الشهادات**.
    2. في مساحة عمل المجلد **الشهادات**، انقر فوق الزر **تكوين قواعد إصدار الشهادات** لفتح النافذة **قواعد إصدار الشهادات**.
    3. في القسم **التكامل مع PKI**، قم بتكوين التكامل مع البنية الأساسية للمفتاح العام (PKI).
    4. في القسم **إصدار شهادات المحمول**، حدد مصدر الشهادات.

يوجد أدناه مثال لإعداد تفويض Kerberos المقيّد (KCD) مع الافتراضيات التالية:

- خدمة iOS MDM على الويب قيد التشغيل على المنفذ 443
- اسم الجهاز المزود بالخادم الوكيل العكسي هو firewall.mydom.local.
- اسم الجهاز الذي يحتوي على خدمة iOS MDM على الويب هو iosmdm.mydom.local.
- اسم النشر الخارجي لخدمة iOS MDM على الويب هو iosmdm.mydom.global.

الاسم الأساسي للخدمة لـ http/iosmdm.mydom.local

في المجال، يجب عليك تسجيل الاسم الأساسي للخدمة (SPN) للجهاز الذي يحتوي على خدمة iOS MDM على الويب (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

تكوين خصائص المجال للجهاز باستخدام الخادم الوكيل العكسي (firewall.mydom.local)

لتفويض حركة المرور، قم باعتماد الجهاز الذي يحتوي على الخادم الوكيل العكسي (firewall.mydom.local) إلى الخدمة المحددة بواسطة SPN (http/iosmdm.mydom.local).

لاعتماد الخدمة التي تحتوي على الخادم الوكيل العكسي إلى الخدمة المحددة بواسطة SPN (http/iosmdm.mydom.local)، يجب أن ينفذ المسؤول الإجراءات التالية:

1. في أداة الإضافة في Microsoft Management Console التي تحمل الاسم "مستخدمو وأجهزة كمبيوتر Active Directory"، حدد الجهاز المثبّت عليه الخادم الوكيل العكسي (firewall.mydom.local).
2. في خصائص الجهاز، من علامة التبويب **التفويض**، قم بتعيين مؤشر التبديل **اعتماد هذا الكمبيوتر للتفويض إلى الخدمة المحددة فقط** إلى **استخدام أي بروتوكول مصادقة**.
3. أضف SPN (http/iosmdm.mydom.local) إلى قائمة **الخدمات التي يمكن لهذا الجهاز تقديم بيانات الاعتماد المفوضة لها**.

شهادة خاصة (مخصصة) لخدمة الويب المنشورة (iosmdm.mydom.global)

يجب عليك إصدار شهادة خاصة (مخصصة) لخدمة iOS MDM على الويب على FQDN iosmdm.mydom.global وحدد أنها تستبدل الشهادة الافتراضية في الإعدادات الخاصة بخدمة iOS MDM على الويب في وحدة تحكم الإدارة.

الرجاء ملاحظة أن حاوية الشهادة (ملف امتداده p12 أو pfx) يجب أن يحتوي أيضًا على سلسلة الشهادات الجذر (المفاتيح العامة).

نشر خدمة iOS MDM على الويب على الخادم الوكيل العكسي

على الخادم الوكيل العكسي، لحركة المرور التي تنتقل من جهاز محمول إلى المنفذ 443 الخاص بـ iosmdm.mydom.global، يجب عليك تكوين KCD على SPN (http/iosmdm.mydom.local)، باستخدام الشهادة التي تم إصدارها لـ FQDN (iosmdm.mydom.global). الرجاء ملاحظة أن عملية النشر هذه وخدمة الويب التي تم نشرها يجب أن يتشاركا في شهادة الخادم نفسها.

تلقي شهادة أسماء نقاط الوصول (APNs)

إذا كان لديك بالفعل شهادة APNs، فيرجى مراعاة تجديدها بدلاً من إنشاء واحدة جديدة. عندما تستبدل شهادة APN الحالية بشهادة تم إنشاؤها حديثًا، يفقد خادم الإدارة القدرة على إدارة أجهزة iOS المحمولة المتصلة حاليًا.

عند إنشاء طلب توقيع الشهادة (CSR) في الخطوة الأولى لمعالج شهادة أسماء نقاط الوصول (APNs)، يتم تخزين مفتاحه الخاص في ذاكرة الوصول العشوائي (RAM) بالجهاز الخاص بك. ولذلك، يجب اكتمال جميع خطوات المعالج في جلسة واحدة للتطبيق.

لتلقي شهادة أسماء نقاط الوصول (APNs):

1. في مجلد **إدارة الجهاز المحمول** في شبكة وحدة التحكم، حدد المجلد الفرعي **خوادم الأجهزة المحمولة**.
2. في مساحة عمل المجلد **خوادم الأجهزة المحمولة**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.
3. في قائمة السياق لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد **خصائص**.
   يؤدي هذا إلى فتح نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.
4. في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM حدد القسم **الشهادات**.
5. في القسم **الشهادات** في مجموعة إعدادات **شهادة إخطار الرسائل من Apple**، انقر فوق الزر **طلب جديد**.
   يبدأ معالج تلقي شهادة خدمة APN، وتفتح النافذة **طلب جديد**.
6. قم بإنشاء طلب توقيع الشهادة (المشار إليه فيما بعد بطلب CSR). للقيام بذلك، قم بالإجراءات التالية:
   a. انقر فوق الزر **إنشاء CSR**.
   b. في النافذة **إنشاء CSR** التي يتم فتحها، حدد اسم طلبك واسم الشركة والقسم ومدينتك ومنطقتك وبلدك.
   c. انقر فوق الزر **حفظ** وحدد اسمًا للملف الذي سيتم حفظ CSR عليه.

   يتم حفظ المفتاح الخاص للشهادة في ذاكرة الجهاز.
7. استخدم CompanyAccount لإرسال الملف مع طلب توقيع الشهادة (CSR) الذي أنشأته إلى Kaspersky ليتم توقيعه.

لن يتوافر التوقيع على طلب CSR الخاص بك إلا بعد تحميل مفتاح إلى مدخل CompanyAccount يتيح استخدام إدارة جهاز المحمول.

بعد معالجة طلبك على الإنترنت، ستتلقى ملف CSR موقعًا من Kaspersky.

8. قم بإرسال ملف طلب CSR الموقع إلى موقع ويب Apple Inc. باستخدام مُعرف Apple ID عشوائي.

> نوصي بتجنب استخدام مُعرف Apple شخصي. قم بإنشاء مُعرف Apple مخصص لاستخدامه كمعرف شركة خاص بك. بعد إنشاء مُعرف Apple، قم بربطه بصندوق بريد المؤسسة، وليس صندوق بريد موظف.

بعد معالجة طلب CSR الخاص بك في Apple Inc.، ستتلقى المفتاح العام لشهادة أسماء نقاط الوصول (APNs). احفظ الملف على قرص.

9. قم بتصدير شهادة أسماء نقاط الوصول (APNs) مع المفتاح الخاص الذي تم إنشاؤه عند إنشاء CSR، بتنسيق ملف PFX. لفعل هذا:

a. في **طلب شهادة أسماء نقاط الوصول (APNs) جديدة** ، انقر فوق زر **إكمال CSR**.

b. من النافذة **افتح** اختر ملفًا مزودًا بالمفتاح العام للشهادة، والذي تم تلقيه من شركة Apple Inc، كنتيجة لمعالجة CSR، وانقر فوق الزر **فتح**.
سيتم بدء عملية تصدير الشهادة.

c. في النافذة التالية، أدخل كلمة مرور المفتاح الخاص وانقر فوق **موافق**.
سيتم استخدام كلمة المرور هذه لتثبيت شهادة أسماء نقاط الوصول (APNs) على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

d. في النافذة **حفظ شهادة أسماء نقاط الوصول (APNs)**، حدد اسم ملف لشهادة خدمة APN واختر مجلدًا، وانقر فوق **حفظ**.

يتم تجميع المفاتيح الخاصة والعامة للشهادة، ويتم حفظ شهادة أسماء نقاط الوصول (APNs) بتنسيق PFX. بعد ذلك، يمكنك تثبيت شهادة أسماء نقاط الوصول (APNs) على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

تجديد شهادة أسماء نقاط الوصول (APNs)

لتجديد شهادة APN:

1. في مجلد **إدارة الجهاز المحمول** في شبكة وحدة التحكم، حدد المجلد الفرعي **خوادم الأجهزة المحمولة**.

2. في مساحة عمل المجلد **خوادم الأجهزة المحمولة**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

3. في قائمة السياق لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد **خصائص**.
يؤدي هذا إلى فتح نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

4. في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM حدد القسم **الشهادات**.

5. في القسم **الشهادات**، في مجموعة الإعدادات **شهادة إخطار الرسائل من Apple** انقر فوق الزر **تجديد**.
يبدأ معالج تجديد شهادة أسماء نقاط الوصول (APNs)، وتفتح النافذة **تجديد شهادة أسماء نقاط الوصول (APNs)**.

6. قم بإنشاء طلب توقيع الشهادة (المشار إليه فيما بعد بطلب CSR). للقيام بذلك، قم بالإجراءات التالية:

a. انقر فوق الزر **إنشاء CSR**.

b. في النافذة **إنشاء CSR** التي يتم فتحها، حدد اسم طلبك واسم الشركة والقسم ومدينتك ومنطقتك وبلدك.

c. انقر فوق الزر **حفظ** وحدد اسمًا للملف الذي سيتم حفظ CSR عليه.

يتم حفظ المفتاح الخاص للشهادة في ذاكرة الجهاز.

7. استخدم CompanyAccount لإرسال الملف مع طلب توقيع الشهادة (CSR) الذي أنشأته إلى Kaspersky ليتم توقيعه.

لن يتوافر التوقيع على طلب CSR الخاص بك إلا بعد تحميل مفتاح إلى مدخل CompanyAccount يتيح استخدام إدارة جهاز المحمول.

بعد معالجة طلبك على الإنترنت، ستتلقى ملف CSR موقعًا من Kaspersky.

8. قم بإرسال ملف طلب CSR الموقع إلى موقع ويب Apple Inc. باستخدام مُعرف Apple ID عشوائي.

نوصي بتجنب استخدام مُعرف Apple شخصي. قم بإنشاء مُعرف Apple مخصص لاستخدامه كمعرف شركة خاص بك. بعد إنشاء مُعرف Apple، قم بربطه بصندوق بريد المؤسسة، وليس صندوق بريد موظف.

بعد معالجة طلب CSR الخاص بك في Apple Inc.، ستتلقى المفتاح العام لشهادة أسماء نقاط الوصول (APNs). احفظ الملف على قرص.

9. اطلب المفتاح العام للشهادة. للقيام بذلك، قم بالإجراءات التالية:

a. تابع إلى بوابة شهادات Apple Push . لتسجيل الدخول إلى البوابة، استخدام معرّف Apple الذي استلمته عند الطلب الأولي للشهادة.

b. في قائمة الشهادات، حدد الشهادة التي يطابق اسم APSP الخاص بها (بتنسيق "APSP: <number>") اسم APSP الخاص بالشهادة المستخدمة بواسطة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM وانقر فوق الزر **تجديد**.

تم تجديد شهادة أسماء نقاط الوصول (APNs).

c. احفظ الشهادة التي تم إنشاؤها على البوابة.

10. قم بتصدير شهادة أسماء نقاط الوصول (APNs) مع المفتاح الخاص الذي تم إنشاؤه عند إنشاء CSR، بتنسيق ملف PFX. للقيام بذلك، قم بالإجراءات التالية:

a. في **تجديد شهادة أسماء نقاط الوصول (APNs)**، انقر على زر **إكمال CSR** .

b. من النافذة **فتح** اختر ملفًا مزودًا بالمفتاح العام للشهادة، والذي تم تلقيه من Apple Inc، كنتيجة لمعالجة CSR، وانقر فوق الزر على **فتح**.

سيتم بدء عملية تصدير الشهادة.

c. في النافذة التالية، أدخل كلمة مرور المفتاح الخاص وانقر فوق **موافق**.

سيتم استخدام كلمة المرور هذه لتثبيت شهادة أسماء نقاط الوصول (APNs) على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

d. في النافذة **تجديد شهادة أسماء نقاط الوصول (APNs)** التي تفتح، حدد اسم ملف لشهادة أسماء نقاط الوصول (APNs) واختر مجلدًا، وانقر فوق **حفظ**.

يتم تجميع المفاتيح الخاصة والعامة للشهادة، ويتم حفظ شهادة أسماء نقاط الوصول (APNs) بتنسيق PFX.

تكوين شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM احتياطية

وظيفة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM تمكنك من إصدار شهادة احتياطية. هذه الشهادة مخصصة للاستخدام في ملفات تعريف iOS MDM لضمان تحول سلس لأجهزة iOS المُدارة بعد انتهاء شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

إذا كان خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لديك يستخدم شهادة افتراضية من إصدار Kaspersky، يمكنك إصدار شهادة احتياطية (أو تحديد شهادتك المخصصة الخاصة كاحتياطية) قبل أن تنتهي شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. بشكل افتراضي، تصدر الشهادة الاحتياطية تلقائيًا كل 60 يومًا قبل انتهاء شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM الاحتياطية تصبح الشهادة الأساسية فورًا بعد انتهاء شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. يتم توزيع المفتاح العام على جميع الأجهزة المُدارة من خلال ملفات تعريف التكوين حتى لا تضطر إلى نقلها يدويًا.

لإصدار شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM احتياطية أو تحديد شهادة احتياطية مخصصة:

1. من شجرة وحدة التحكم، في مجلد **إدارة الجهاز المحمول** حدد مجلد الفرعي **خوادم الأجهزة المحمولة**.

2. في قائمة خوادم الأجهزة المحمولة، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM ذي الصلة، وفي الجزء الأيمن انقر على زر **تكوين خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM**.

3. في نافذة إعدادات خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM التي تفتح، حدد قسم **الشهادات**.

4. قم بأحد الإجراءات التالية في كتلة الإعدادات **الشهادة الاحتياطية**.

- إذا كنت تخطط للاستمرار في استخدام شهادة ذاتية التوقيع (أي الشهادة الصادرة من Kaspersky):

a. انقر فوق الزر **المشكلة**.

b. في نافذة **تاريخ التفعيل** التي تفتح، حدد أحد خياري التاريخ الذي يجب فيه تطبيق الشهادة:

- إذا كنت ترغب في تطبيق الشهادة الاحتياطية في وقت انتهاء الشهادة الحالية، حدد خيار **عند انتهاء صلاحية الشهادة الحالية**.
- إذا كنت ترغب في تطبيق الشهادة الاحتياطية قبل وقت انتهاء الشهادة الحالية، حدد خيار **بعد فترة (أيام) محددة**. في الحقل الافتتاحي بجوار هذا الخيار، حدد مدة الفترة التي يجب بعدها أن تقوم الشهادة الاحتياطية باستبدال الشهادة الحالية.

فترة صلاحية الشهادة الاحتياطية التي تحددها لا يمكن أن تتخطى فترة صلاية شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM الحالية.

c. انقر على زر **موافق**.

يتم إصدار شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM الاحتياطية.

- إذا كنت تخطط لاستخدام شهادة مخصصة من إصدار هيئة إصدار شهادات خاصة بك:

a. انقر على الزر **إضافة**.

b. في نافذة مستكشف الملفات التي تفتح، حدد ملف شهادة بتنسيق PEM أو PFX أو P12 مخزن على جهازك ثم انقر على زر **فتح**.

يتم تحديد شهادتك المخصصة كشهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM الاحتياطية.

أنت تملك شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM احتياطية محددة. يتم عرض تفاصيل الشهادة الاحتياطية في كتلة إعدادات **الشهادة الاحتياطية** (اسم الشهادة واسم المصدر وتاريخ الانتهاء وتاريخ وجوب تطبيق الشهادة الاحتياطية في حال وجودهم).

تثبيت شهادة APN على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

بعد تلقي شهادة أسماء نقاط الوصول (APNs)، يجب تثبيتها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

لتثبيت شهادة أسماء نقاط الوصول (APNs) على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM:

1. في مجلد **إدارة الجهاز المحمول** في شبكة وحدة التحكم، حدد المجلد الفرعي **خوادم الأجهزة المحمولة**.

2. في مساحة عمل المجلد **خوادم الأجهزة المحمولة**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

3. في قائمة السياق لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد **خصائص**.

يؤدي هذا إلى فتح نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

4. في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM حدد القسم **الشهادات**.

5. في القسم **الشهادات** في مجموعة إعدادات **شهادة إخطار الرسائل من Apple** انقر فوق الزر **تثبيت**.

6. حدد ملف PFX الذي يحتوي على شهادة أسماء نقاط الوصول (APNs).

7. أدخل كلمة مرور المفتاح الخاص المحدد عند تصدير شهادة أسماء نقاط الوصول (APNs).

سيتم تثبيت شهادة أسماء نقاط الوصول (APNs) على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. سيتم عرض تفاصيل الشهادة في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في القسم **الشهادات**.

تكوين الوصول إلى خدمة Apple Push Notification

لضمان عمل خدمة iOS MDM على الويب بشكل صحيح والاستجابة الفورية من الأجهزة المحمولة لأوامر المسؤول، فأنت في حاجة لتحديد شهادة خدمة Apple Push Notification (يُشار إليها فيما بعد باسم شهادة أسماء نقاط الوصول (APNs)) في إعدادات خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

التفاعل مع Apple Push Notification (يُشار إليها فيما بعد باسم APNs)، تتصل خدمة الويب iOS MDM بالعنوان الخارجي api.push.apple.com من خلال منفذ 2197 (الصادر). لذلك، تتطلب خدمة iOS MDM على الويب الوصول إلى المنفذ TCP 2197 لنطاق العناوين 17.0.0.0/8. من جهة جهاز خدمة iOS يكون الوصول إلى المنفذ TCP 5223 لنطاق العناوين 17.0.0.0/8.

إذا كنت تقصد الوصول إلى خدمة APNs من جهة خدمة iOS MDM على الويب من خلال خادم وكيل، يجب عليك القيام بالإجراءات التالية على الأجهزة المثبّت عليها خدمة iOS MDM على الويب:

1. قم بإضافة السلاسل التالية إلى السجل:

- لأنظمة التشغيل 32 بت:

```
Conset\1.0.0.0\KLIOSMDM\Connectors\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE
"<Proxy Host Name>"="ApnProxyHost"
"<Proxy Port>"="ApnProxyPort"
"<Proxy Login>"="ApnProxyLogin"
"<Proxy Password>"="ApnProxyPwd"
```

- لأنظمة التشغيل 64 بت:

```
Conset\1.0.0.0\KLIOSMDM\Connectors\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE
"<Proxy Host Name>"="ApnProxyHost"
"<Proxy Port>"="ApnProxyPort"
"<Proxy Login>"="ApnProxyLogin"
"<Proxy Password>"="ApnProxyPwd"
```

2. أعد تشغيل خدمة iOS MDM على الويب.

إصدار وتثبيت شهادة مشتركة على جهاز محمول

لإصدار شهادة مشتركة إلى مستخدم:

1. في شجرة وحدة التحكم، في مجلد **حسابات المستخدمين**، حدد حساب مستخدم.

2. في قائمة سياق حساب المستخدم، حدد **استيراد شهادة**.

   يبدأ معالج تثبيت الشهادة. اتبع إرشادات المعالج.

عند انتهاء المعالج، سيتم إنشاء شهادة وإضافتها إلى قائمة شهادات المستخدم.

سيتم تنزيل الشهادة التي تم إصدارها بواسطة المستخدم، بجانب حزمة التثبيت التي تحتوي على ملف التعريف iOS MDM.

بعد اتصال الجهاز المحمول بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، سيتم تطبيق إعدادات ملف تعريف iOS MDM على جهاز المستخدم. سيتمكن المسؤول من إدارة الجهاز بعد الاتصال.

يتم عرض الجهاز المحمول الخاص بالمستخدم والمتصل بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في المجلد الفرعي **الأجهزة المحمولة** الموجود في المجلد **إدارة جهاز المحمول** في شجرة وحدة التحكم.

إضافة جهاز KES إلى قائمة الأجهزة المدارة

لإضافة جهاز KES خاص بمستخدم إلى قائمة الأجهزة المدارة باستخدام رابط Google Play™:

1. من شجرة وحدة التحكم، حدد المجلد **حسابات المستخدمين**.

   بشكل افتراضي، يكون المجلد **حسابات المستخدمين** مجلد فرعي للمجلد **خيارات متقدمة**.

2. حدد حساب المستخدم الذي تريد إضافة الجهاز المحمول الخاص به إلى قائمة الأجهزة المدارة.

3. في قائمة سياق حساب المستخدم، حدد **إضافة جهاز محمول** .

   يبدأ تشغيل معالج اتصال الجهاز المحمول الجديد. في نافذة **مصدر الشهادة** في المعالج، يجب عليك تحديد طريقة إنشاء الشهادة المشتركة التي سوف يستخدمها خادم الإدارة لتحديد الجهاز المحمول. يمكنك تحديد شهادة مشتركة باستخدام إحدى الطرق التالية:

   - إنشاء شهادة مشتركة تلقائيًا، بواسطة أدوات خادم الإدارة، ثم تسليم الشهادة إلى الجهاز.
   - تحديد ملف شهادة مشتركة.

4. في نافذة **نوع الجهاز** الخاصة بالمعالج، حدد **الارتباط بـ Google Play**.

5. في نافذة **طريقة إعلام المستخدم** من المعالج، حدد إعدادات إعلام مستخدم الجهاز المحمول بشأن إنشاء شهادة (عبر رسالة SMS أو عبر البريد الإلكتروني أو عبر عرض المعلومات عند اكتمال المعالج).

6. في نافذة معلومات الشهادة للمعالج، انقر فوق زر **إنهاء** لإغلاق المعالج.

بعد انتهاء أنشطة المعالج، سيتم إرسال رابط ورمز QR إلى الجهاز المحمول الخاص بالمستخدم، مما يتيح للمستخدم تنزيل Kaspersky Endpoint Security من Google Play. يمكن للمستخدم المتابعة إلى Google Play باستخدام الرابط أو عبر مسح رمز QR. بعد ذلك، يطالب نظام تشغيل الجهاز المستخدم بقبول تثبيت Kaspersky Endpoint Security for Android. بعد تنزيل Kaspersky Endpoint Security for Android وتثبيته، يتصل الجهاز المحمول بخادم الإدارة ويقوم بتنزيل الشهادة المشتركة. بعد تثبيت الشهادة على الجهاز المحمول، يتم عرض الجهاز في مجلد **الأجهزة المحمولة**، وهو المجلد الفرعي لمجلد **إدارة الجهاز المحمول** الموجود بشجرة وحدة التحكم.

إذا كان Kaspersky Endpoint Security for Android مثبتًا بالفعل على الجهاز، فيجب على المستخدم تلقي إعدادات اتصال خادم الإدارة من المسؤول ثم إدخالها بشكل مستقل. بعد تحديد إعدادات الاتصال، يتصل الجهاز المحمول بخادم الإدارة. يقوم المسؤول بإصدار شهادة مشتركة للجهاز ويرسل رسالة بريد إلكتروني ورسائل SMS إلى المستخدم تحتوي على بيانات تسجيل الدخول وكلمة المرور لتنزيل الشهادة. يقوم المستخدم بتنزيل الشهادة المشتركة وتثبيتها. بعد تثبيت الشهادة على الجهاز المحمول، يتم عرض الجهاز في مجلد **الأجهزة المحمولة**، وهو المجلد الفرعي لمجلد **إدارة الجهاز المحمول** الموجود بشجرة وحدة التحكم. في هذه الحالة، لن يتم تنزيل Kaspersky Endpoint Security for Android وتثبيته مرة أخرى.

توصيل أجهزة KES بخادم الإدارة

بالاعتماد على الطريقة المستخدمة لاتصال الأجهزة بخادم الإدارة، يتوفر نظاما نشر لـ Kaspersky Device Management for iOS لأجهزة KES:

- نظام نشر باستخدام الاتصال المباشر للأجهزة بخادم الإدارة
- مخطط النشر الذي يتضمن الخادم الوكيل العكسي الذي يدعم تفويض Kerberos المقيد

الاتصال المباشر للأجهزة بخادم الإدارة

يمكن لأجهزة KES الاتصال مباشرةً بمنفذ 13292 الخاص بخادم الإدارة.

بناءً على الطريقة المستخدمة للمصادقة، يتوفر خياران لاتصال أجهزة KES بخادم الإدارة:

- توصيل الأجهزة باستخدام شهادة مستخدم
- توصيل الأجهزة بدون استخدام شهادة مستخدم

توصيل جهاز باستخدام شهادة مستخدم

عند توصيل جهاز باستخدام شهادة مستخدم، يقترن الجهاز بحساب المستخدم الذي تم إسناد الشهادة المقابلة له عبر أدوات خادم الإدارة.

في هذه الحالة، سيتم استخدام مصادقة SSL ثنائية الاتجاه (مصادقة تبادلية). ستتم مصادقة كلاً من خادم الإدارة والجهاز باستخدام الشهادات.

توصيل جهاز بدون استخدام شهادة مستخدم

عند توصيل جهاز بدون شهادة مستخدم، لن يقترن هذا الجهاز بأي من حسابات المستخدم على خادم الإدارة. ولكن، عندما يتلقى الجهاز أي شهادة، سيقترن الجهاز بالمستخدم الذي تم إسناد الشهادة المقابلة له عبر أدوات خادم الإدارة.

عند توصل ذلك الجهاز بخادم الإدارة، سيتم تطبيق مصادقة SSL أحادية الاتجاه، وهذا يعني مصادقة خادم الإدارة فقط باستخدام الشهادة. بعد استرداد الجهاز شهادة المستخدم، سيتغير نوع المصادقة إلى مصادقة SSL ثنائية الاتجاه (مصادقة SSL ثنائية الاتجاه، مصادقة تبادلية).

نظام توصيل أجهزة KES بالخادم الذي يتضمن تفويض Kerberos المقيّد (KCD)

يعمل نظام توصيل أجهزة KES بخادم الإدارة الذي يتضمن تفويض Kerberos المقيّد (KCD) على ما يلي:

- التكامل مع خادم وكيل عكسي يدعم KCD.
- استخدام تفويض Kerberos المقيّد (يُشار إليه فيما بعد باسم KCD) لمصادقة الأجهزة المحمولة.
- التكامل مع البنية الأساسية للمفتاح العام (يُشار إليها فيما بعد باسم PKI) لتطبيق شهادات المستخدم.

عند استخدام نظام الاتصال هذا، الرجاء ملاحظة ما يلي:

- يجب أن يكون نوع اتصال أجهزة KES بالخادم الوكيل العكسي "مصادقة SSL ثنائية الاتجاه"، أي أن الجهاز يجب أن يتصل بالخادم الوكيل العكسي عبر شهادة المستخدم الشخصية الخاصة به. للقيام بذلك، أنت في حاجة لدمج شهادة المستخدم في حزمة تثبيت Kaspersky Endpoint Security for Android، التي تم تثبيتها على الجهاز. يجب إنشاء حزمة KES هذه بواسطة خادم الإدارة خصيصًا لهذا الجهاز (المستخدم).
- يجب عليك تحديد الشهادة الخاصة (المخصصة) بدلاً من شهادة الخادم الافتراضية لبروتوكول الجهاز المحمول:
  1. في نافذة خصائص خادم الإدارة، في قسم **الإعدادات**، حدد خانة الاختيار **فتح منفذ للأجهزة المحمولة** ثم حدد **إضافة شهادة** من القائمة المنسدلة.
  2. في النافذة التي تفتح، حدد الشهادة ذاتها التي تم تعيينها على الخادم الوكيل العكسي عند نشر نقطة الوصول إلى بروتوكول الجهاز المحمول على خادم الإدارة.
- يجب إصدار شهادات المستخدم لأجهزة KES بواسطة هيئة إصدار الشهادات (CA) الخاصة بالمجال. ضع في اعتبارك في حالة احتواء المجال على هيئات إصدار شهادات جذر متعددة، يجب إصدار شهادات المستخدم بواسطة هيئة إصدار الشهادات (CA)، التي تم تعيينها في النشر على الخادم الوكيل العكسي.

  يمكنك التأكد أن شهادة المستخدم متوافقة مع المتطلب الموضح أعلاه عن طريق استخدام طريقة من الطرق التالية:
  - حدد شهادة المستخدم الخاصة في معالج الحزمة الجديدة وفي معالج تثبيت الشهادة.
  - دمج خادم الإدارة مع البنية الأساسية للمفتاح العام (PKI) وتحديد الإعداد المقابل في قواعد إصدار الشهادات:
    1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد المجلد الفرعي **الشهادات**.
    2. في مساحة عمل المجلد **الشهادات**، انقر فوق الزر **تكوين قواعد إصدار الشهادات** لفتح النافذة **قواعد إصدار الشهادات**.
    3. في القسم **التكامل مع PKI**، قم بتكوين التكامل مع البنية الأساسية للمفتاح العام (PKI).
    4. في القسم **إصدار شهادات المحمول**، حدد مصدر الشهادات.

يوجد أدناه مثال لإعداد تفويض Kerberos المقيّد (KCD) مع الافتراضيات التالية:

- يتم تعيين نقطة الوصول إلى بروتوكول الجهاز المحمول على خادم الإدارة إلى المنفذ 13292.
- اسم الجهاز المزود بالخادم الوكيل العكسي هو firewall.mydom.local.
- اسم الجهاز المثبّت عليه خادم الإدارة هو ksc.mydom.local.
- اسم النشر الخارجي لنقطة الوصول إلى بروتوكول الجهاز المحمول هو kes4mob.mydom.global.

حساب المجال لخادم الإدارة

يجب عليك إنشاء حساب مجال (على سبيل المثال KSCMobileSrvcUsr) الذي ستعمل خدمة خادم الإدارة بموجبه. يمكنك تحديد حساب لخادم الإدارة عند تثبيت خادم الإدارة أو عبر الأداة المساعدة klsrvswch. توجد الأداة المساعدة klsrvswch في مجلد التثبيت الخاص بخادم الإدارة. مسار التثبيت الافتراضي: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

يجب تحديد حساب مجال للأسباب التالية:

- الميزة إدارة أجهزة KES هي جزء متكامل من خادم الإدارة.
- لضمان العمل الصحيح لتفويض Kerberos المقيّد (KCD)، يجب أن تعمل جهة الاستلام (أي خادم الإدارة) أسفل حساب مجال.

الاسم الأساسي للخدمة لـ http/kes4mob.mydom.local

في المجال، أسفل حساب KSCMobileSrvcUsr، قم بإضافة SPN لنشر خدمة بروتوكول الجهاز المحمول على المنفذ 13292 الخاص بالجهاز المثبّت عليه خادم الإدارة. بالنسبة لجهاز kes4mob.mydom.local المثبّت عليه خادم الإدارة، سيظهر الاسم كمل يلي:

```
KSCMobileSrvcUsr\13292 mydom:setspn -a http/kes4mob.mydom.local
```

تكوين خصائص المجال للجهاز باستخدام الخادم الوكيل العكسي (firewall.mydom.local)

لتفويض حركة المرور، يجب عليك اعتماد الجهاز الذي يحتوي على الخادم الوكيل العكسي (firewall.mydom.local) إلى الخدمة المحددة بواسطة SPN (13292:http/kes4mob.mydom.local).

لاعتماد الخدمة التي تحتوي على الخادم الوكيل العكسي إلى الخدمة المحددة بواسطة SPN (13292:http/kes4mob.mydom.local)، يجب أن ينفذ المسؤول الإجراءات التالية:

1. في أداة الإضافة في Microsoft Management Console التي تحمل الاسم "مستخدمو وأجهزة كمبيوتر Active Directory"، حدد الجهاز المثبّت عليه الخادم الوكيل العكسي (firewall.mydom.local).

2. في خصائص الجهاز، من علامة التبويب **التفويض**، قم بتعيين مؤشر التبديل **اعتماد هذا الكمبيوتر للتفويض إلى الخدمة المحددة فقط** إلى **استخدام أي بروتوكول مصادقة**.

3. في قائمة **الخدمات التي يمكن لهذا الجهاز تقديم بيانات الاعتماد المفوضة لها**، قم بإضافة 13292:SPN http/kes4mob.mydom.local.

شهادة خاصة (مخصصة) لعملية النشر (kes4mob.mydom.global)

لنشر بروتوكول الجهاز المحمول الخاص بخدام الإدارة، يجب عليك إصدار شهادة خاصة (مخصصة) لـ FQDN kes4mob.mydom.global وحدد شهادة الخادم الافتراضية في إعدادات بروتوكول الجهاز المحمول الخاص بخادم الإدارة في وحدة تحكم الإدارة. للقيام بذلك، في نافذة الخصائص الخاصة بخادم الإدارة، في قسم **الإعدادات**، حدد خانة الاختيار **فتح منفذ للأجهزة المحمولة** ثم حدد **إضافة شهادة** من القائمة المنسدلة.

الرجاء ملاحظة أن حاوية شهادة الخادم (ملف امتداده p12 أو pfx) يجب أن يحتوي أيضًا على سلسلة الشهادات الجذر (المفاتيح العامة).

تكوين النشر على الخادم الوكيل العكسي

على الخادم الوكيل العكسي، بالنسبة لحركة المرور التي تنتقل من جهة الجهاز المحمول إلى المنفذ 13292 الخاص بـ kes4mob.mydom.global، يجب عليك تكوين KCD على SPN (13292:http/kes4mob.mydom.local)، باستخدام شهادة الخادم التي تم إصدارها لـ FQND kes4mob.mydom.global. الرجاء ملاحظة أن النشر ونقطة الوصول المنشورة (المنفذ 13292 الخاص بخادم الإدارة) يجب أن تتشارك شهادة الخادم نفسها.

استخدام مراسلة Firebase Cloud

لضمان تسليم الأوامر إلى أجهزة KES التي تتم إدارتها بواسطة نظام تشغيل Android في الوقت المناسب، يستخدم Kaspersky Security Center آلية إرسال الإخطارات. يتم تبادل الإخطارات الفورية بين أجهزة KES وخادم الإدارة من خلال Firebase Cloud Messaging (المشار إليه فيما يلي باسم FCM). في وحدة تحكم إدارة Kaspersky Security Center، يمكنك تحديد إعدادات Firebase Cloud Messaging لتوصيل أجهزة KES بالخدمة.

لاستعادة إعدادات مراسلة Google Firebase Cloud، يجب أن تمتلك حساب.

لتمكين استخدام مراسلة FCM:

1. في وحدة تحكم الإدارة، حدد العقدة **إدارة الجهاز المحمول**، والمجلد **الأجهزة المحمولة**.

2. من قائمة سياق المجلد **الأجهزة المحمولة**، حدد **خصائص**.

3. في خصائص المجلد، حدد القسم **إعدادات Firebase Cloud Messaging**.

4. في الحقل **رقم مشروع Firebase**، حدد معرف مرسل FCM.

5. في الحقل **ملف المفتاح الخاص (بتنسيق JSON)**، حدد ملف المفتاح الخاص.

في المزامنة التالية مع خادم الإدارة، ستتصل أجهزة KES التي تمت إدارتها بواسطة أنظمة التشغيل Android بمراسلة Firebase Cloud.

يمكنك تحرير إعدادات Firebase Cloud Messaging من خلال النقر فوق الزر **إعادة تعيين الإعدادات**.

عند التبديل إلى مشروع Firebase مختلف، فإنك تحتاج إلى الانتظار لمدة 10 دقائق لاستئناف FCM.

تعمل خدمة FCM في نطاق العناوين التالي:

- من جهة جهاز KES، مطلوب الوصول إلى المنافذ: 443 (HTTPS) و5228 (HTTPS) و5229 (HTTPS) و5230 (HTTPS) الخاصة بالعناوين التالية:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - كل عناوين IP المُدرجة في ASN الخاص بـ Google لـ 15169
- من جهة خادم الإدارة، مطلوب الوصول إلى المنفذ 443 (HTTPS) الخاص بالعناوين التالية:
  - fcm.googleapis.com
  - كل عناوين IP المُدرجة في ASN الخاص بـ Google لـ 15169

إذا تم تحديد إعدادات الخادم الوكيل (**متقدم / تكوين الاتصال بالإنترنت**) في خصائص خادم الإدارة في وحدة تحكم الإدارة، فسيتم استخدامها للتفاعل مع FCM.

تكوين FCM: الحصول على معرف المرسل وملف المفتاح الخاص

لتكوين FCM:

1. التسجيل على بوابة Google.

2. انتقل إلى وحدة تحكم Firebase.

3. قم بأحد الإجراءات التالية:
   - لإنشاء مشروع جديد، انقر فوق **إنشاء مشروع** واتبع التعليمات التي تظهر على الشاشة.
   - افتح مشروعًا موجودًا.

4. انقر على أيقونة الترس واختر **إعدادات المشروع**.
   تفتح النافذة **إعدادات المشروع**.

5. حدد علامة التبويب **المراسلة السحابية**.

6. استرجع معرف المرسل ذي الصلة من الحقل **معرف المرسل** في القسم **Firebase Cloud Messaging API (V1)**.

7. حدد علامة التبويب **حسابات الخدمة** وانقر فوق **إنشاء مفتاح خاص جديد**.

8. في النافذة التي تفتح، انقر فوق **إنشاء مفتاح** لإنشاء ملف مفتاح خاص وتنزيله.

تم تكوين Firebase Cloud Messaging الآن.

التكامل مع البنية الأساسية للمفاتيح العامة

التكامل مع البنية الأساسية للمفتاح العام (يُشار إليه فيما بعد باسم PKI) يُقصد به بشكل أساسي تسهيل إصدار شهادات المستخدم الخاصة بالمجال بواسطة خادم الإدارة.

يمكن للمسؤول تعيين شهادة مجال لمستخدم ما في وحدة تحكم الإدارة. يمكن القيام بهذا باستخدام واحدة من الطرق التالية:

- قم بتعيين شهادة خاصة (مخصصة) للمستخدم من ملف في معالج تثبيت الشهادة.
- القيام بالتكامل مع PKI وتعيين PKI للعمل كمصدر للشهادات لنوع محدد من الشهادات أو لكل أنواع الشهادات.

تتوفر إعدادات التكامل مع PKI في مساحة عمل المجلد **إدارة الجهاز المحمول / الشهادات** من خلال النقر فوق الرابط **التكامل مع البنية الأساسية للمفتاح العام**.

المبدأ العام للتكامل مع PKI لإصدار شهادات المستخدم الخاصة بالمجال

في وحدة تحكم الإدارة، انقر فوق الرابط **التكامل مع البنية الأساسية للمفتاح العام** في مساحة عمل المجلد **إدارة الجهاز المحمول / الشهادات** لتحديد حساب المجال الذي سيُستخدم بواسطة خادم الإدارة لإصدار شهادات عميل المجال عبر هيئة إصدار الشهادات الخاصة بالمجال (يُشار إليه فيما بعد باسم الحساب الذي يتم أسفله إجراء التكامل مع PKI).

الرجاء ملاحظة ما يلي:

- تقدم لك إعدادات التكامل مع PKI إمكانية تحديد القالب الافتراضي لكل أنواع الشهادات. لاحظ أن قواعد إصدار الشهادات (المتوفرة في مساحة عمل المجلد **إدارة الجهاز المحمول / الشهادات** عن طريق النقر فوق الزر **تكوين قواعد إصدار الشهادات**) تتيح لك تحديد قالب فردي لكل نوع من أنواع الشهادات.
- يجب تثبيت شهادة وكيل تسجيل (EA) خاصة على الجهاز المثبت عليه خادم الإدارة، في مستودع الشهادات الخاص بالحساب الذي سيتم التكامل مع PKI أسفله. يتم إصدار شهادة عميل التسجيل (EA) بواسطة مسؤول CA (هيئة إصدار الشهادات) الخاصة بالمجال.

يجب أن يفي الحساب الذي سيتم التكامل مع PKI أسفله بالمعايير التالية:

- أن يكون مستخدم مجال.
- أن يكون مسؤول محلي للجهاز المثبّت عليه خادم الإدارة الذي يتم بدء التكامل مع PKI منه.
- أن يملك حق تسجيل الدخول كخدمة.
- يجب أن يعمل الجهاز المثبّت عليه خادم الإدارة مرة واحدة على الأقل أسفل هذا الحساب لإنشاء ملف تعريف مستخدم دائم.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (يُشار إليه فيما بعد بخادم الويب) هو مكوّن من مكونات Kaspersky Security Center. تم تصميم خادم الويب لنشر حزم التثبيت المستقلة وحزم التثبيت المستقلة للأجهزة المحمولة وملفات تعريف iOS MDM وملفات من المجلد المشترك.

ملفات تعريف iOS MDM وحزم التثبيت التي تم إنشاؤها يتم نشرها على خادم الويب تلقائيًا ثم تتم إزالتها بعد التنزيل الأول. ويمكن للمسؤول إرسال الرابط الجديد إلى المستخدم بأي طريقة مناسبة: على سبيل المثال عبر البريد الإلكتروني.

عن طريق النقر على الرابط، يمكن للمستخدم تنزيل المعلومات المطلوبة على الجهاز المحمول.

إعدادات خادم الويب

إذا كان ضبط خادم الويب مطلوبًا، توفر خصائص خادم الويب الخاص بوحدة تحكم الإدارة إمكانية تغيير المنافذ لـ HTTP (8060) وHTTPS (8061). بالإضافة إلى تغيير المنافذ، يمكنك استبدال شهادة الخادم لـ HTTPS وتغير FQDN الخاص بخادم الويب الخاص بـ HTTP.

تثبيت Kaspersky Security Center

يوضح هذا القسم تثبيت مكونات Kaspersky Security Center. إذا كنت ترغب في تثبيت التطبيق محليًا على جهاز واحد فقط، فيتوفر خياران للتثبيت:

- **قياسي**. من المستحسن استخدام هذا الخيار إذا كنت ترغب في تجربة Kaspersky Security Center، على سبيل المثال، عن طريق اختبار تشغيله في منطقة صغيرة ضمن شبكتك. أثناء التثبيت القياسي، تقوم فقط بتكوين قاعدة البيانات. ويمكنك أيضًا تثبيت مجموعة المكونات الإضافية الافتراضية فقط الخاصة بإدارة تطبيقات Kaspersky. كما يمكنك أيضًا استخدام عملية التثبيت القياسي إذا كانت لديك خبرة في استخدام Kaspersky Security Center ويمكنك تحديد كل الإعدادات ذات الصلة بعد إجراء عملية التثبيت القياسي.

- **مخصص**. من المستحسن استخدام هذا الخيار إذا كنت تخطط لتعديل إعدادات Kaspersky Security Center، مثل المسار إلى المجلد المشترك والحسابات ومنافذ الاتصال بخادم الإدارة وإعدادات قاعدة البيانات. يمكّنك التثبيت المخصص من تحديد مكونات الإدارة الإضافية لـ Kaspersky المراد تثبيتها. إذا لزم الأمر، يمكنك بدء تثبيت مخطط في الوضع الصامت.

إذا تم تثبيت خادم إدارة واحد على الأقل على الشبكة، فيمكن تثبيت الخوادم على أجهزة أخرى عن بُعد من خلال مهمة التثبيت عن بُعد باستخدام التثبيت الإجباري. عند إنشاء مهمة التثبيت عن بُعد ، يجب استخدام حزمة تثبيت خادم الإدارة: localization> _full_ <build number> .<version_number> _ksc .exe. <language

استخدم هذه الحزمة إذا كنت ترغب في تثبيت جميع المكونات المطلوبة لعمل الوظائف الكاملة لـ Kaspersky Security Center أو لترقية الإصدارات الحالية لتلك المكونات.

إذا كنت تريد نشر مجموعة تجاوز الفشل من Kaspersky Security Center، فأنت بحاجة إلى تثبيت Kaspersky Security Center على جميع عقد المجموعة.

الإعداد للتثبيت

نفذ الإجراءات التالية قبل بدء التثبيت.

- **تحقق من متطلبات الأجهزة والبرامج**

تأكد من توافق الأجهزة والبرامج على الجهاز مع متطلبات خادم الإدارة ووحدة تحكم الإدارة.

- **حدد وقم بتثبيت نظام إدارة قاعدة البيانات (DBMS)**

يخزن Kaspersky Security Center معلوماته في قاعدة بيانات يديرها نظام إدارة قاعدة البيانات. قم بتثبيت نظام إدارة قاعدة البيانات على الشبكة قبل Kaspersky Security Center (اعرف المزيد عن كيفية تحديد نظام إدارة قاعدة البيانات). إذا قررت تثبيت PostgreSQL أو Postgres Pro DBMS، حدد كلمة مرور للمستخدم المتميز. إذا لم يتم تحديد كلمة المرور، فقد يتعذر على خادم الإدارة الاتصال بقاعدة البيانات.

يوصى بأن تقوم بتثبيت خادم الإدارة على خادم مخصص بدلاً من وحدة تحكم في المجال. ومع ذلك، إذا قمت بتثبيت Kaspersky Security Center على خادم يعمل كوحدة تحكم بالمجال للقراءة فقط (RODC)، فلا يجب حينها تثبيت Microsoft SQL Server (SQL Express) محليًا (على نفس الجهاز). في هذه الحالة، نوصي بتثبيت Microsoft SQL Server (SQL Express) عن بُعد (على جهاز آخر)، أو استخدام MySQL أو MariaDB، إذا كنت بحاجة إلى تثبيت DBMS محليًا.

- **جهز المجلدات لخادم الإدارة وعميل الشبكة ووحدة تحكم الإدارة**

يلزم تثبيت خادم الإدارة وعميل الشبكة ووحدة تحكم الإدارة في مجلدات لا يتم تشغيل ميزة حساسية حالة الأحرف فيها. بالإضافة إلى ذلك، يجب تعطيل حساسية حالة الأحرف للمجلد المشترك لخادم الإدارة والمجلد المخفي لتطبيق Kaspersky Security Center (adminkit\KasperskyLab\%ALLUSERSPROFILE%).

- **إزالة عميل الشبكة القديم**

يتم تثبيت إصدار خادم عميل الشبكة على الجهاز مع خادم الإدارة. يتعذر تثبيت خادم الإدارة مع الإصدار العادي من عميل الشبكة. إذا كان إصدار خادم عميل الشبكة مثبتًا بالفعل على جهازك، فقم بإزالته وابدأ تثبيت خادم الإدارة مرة أخرى. للحصول على تفاصيل عن إصدار الخادم من عميل الشبكة، ارجع إلى التغييرات في النظام بعد تثبيت Kaspersky Security Center.

- **التحقق من الحسابات**

يتطلب تثبيت Kaspersky Security Center حقوق المسؤول على الجهاز الذي سيتم تنفيذ التثبيت عليه.

يدعم Kaspersky Security Center حسابات الخدمة المُدارة وحسابات الخدمة المُدارة الجماعية. إذا تم استخدام هذه الأنواع من الحسابات في مجالك، وتريد تحديد أحدها كحساب لخدمة خادم الإدارة، فقم أولاً بتثبيت الحساب على نفس الجهاز الذي تريد تثبيت خادم الإدارة عليه. للحصول على تفاصيل حول تثبيت حسابات الخدمة المُدارة على جهاز محلي، راجع وثائق Microsoft الرسمية.

حسابات للعمل باستخدام نظام إدارة قواعد البيانات (DBMS)

لتثبيت خادم الإدارة والعمل معه، فأنت بحاجة إلى حساب Windows ستقوم بموجبه بتشغيل مثبت خادم الإدارة (المشار إليه فيما يلي أيضًا باسم المثبت)، وحساب Windows الذي ستبدأ بموجبه خدمة خادم الإدارة، ونظام إدارة قواعد البيانات الداخلي حساب للوصول إلى نظام إدارة قواعد البيانات. يمكنك إنشاء حسابات جديدة أو استخدام الحسابات الموجودة سابقًا. كل هذه الحسابات تتطلب حقوقًا محددة. تعتمد مجموعة الحسابات المطلوبة وحقوقها على المعايير التالية:

- نوع نظام إدارة قاعدة البيانات:
  - خادم Microsoft SQL (مع مصادقة Windows أو مصادقة خادم SQL)
  - MySQL أو MariaDB
  - PostgreSQL أو Postgres Pro
- موقع نظام إدارة قواعد بيانات نظام إدارة قاعدة البيانات:
  - **نظام إدارة قواعد البيانات المحلية**. نظام إدارة قواعد البيانات (DBMS) المحلي هو نظام إدارة قواعد بيانات مثبّت على الجهاز الذي يعمل كخادم إدارة.
  - **نظام إدارة قاعدة البيانات عن بُعد**. نظام إدارة قواعد البيانات (DBMS) عن بُعد هو نظام إدارة قواعد بيانات مثبّت على جهاز مختلف.
- طريقة إنشاء قاعدة بيانات خادم الإدارة:
  - **تلقائيًا**. أثناء تثبيت خادم الإدارة، يمكنك إنشاء قاعدة بيانات خادم الإدارة تلقائيًا (يشار إليها فيما يلي أيضًا باسم قاعدة بيانات الخادم) باستخدام المُثبت.
  - **يدويًا**. يمكنك استخدام تطبيق جهة خارجية (على سبيل المثال، SQL Server Management Studio) أو برنامج نصي لإنشاء قاعدة بيانات فارغة. بعد ذلك، يمكنك تحديد قاعدة البيانات هذه كقاعدة بيانات الخادم أثناء تثبيت خادم الإدارة.

اتبع مبدأ إعطاء أقل امتياز عند منح الحقوق والأذونات للحسابات. هذا يعني أن الحقوق الممنوحة يجب أن تكون كافية فقط لأداء الإجراءات المطلوبة.

تحتوي الجداول أدناه على معلومات حول حقوق النظام وحقوق نظام إدارة قاعدة البيانات التي يجب أن تمنحها للحسابات قبل تثبيت خادم الإدارة وبدء تشغيله.

Microsoft SQL Server مع مصادقة Windows

إذا اخترت SQL Server باعتباره نظام إدارة قاعدة البيانات، فيمكنك استخدام مصادقة Windows للوصول إلى SQL Server. قم بتكوين حقوق النظام لحساب Windows المستخدَم لتشغيل المثبت وحساب Windows المستخدم لبدء خدمة خادم الإدارة. في SQL Server، قم بإنشاء تسجيلات دخول لكل من حسابات Windows هذه. بناءً على طريقة إنشاء قاعدة بيانات الخادم، امنح حقوق SQL Server المطلوبة لهذه الحسابات كما هو موضح في الجدول أدناه. لمزيد من المعلومات حول كيفية تكوين حقوق الحسابات، يُرجى الرجوع إلى تكوين الحسابات للعمل مع SQL Server (مصادقة Windows).

نظام إدارة قواعد البيانات: خادم SQL Server (يشمل Express Edition) مع مصادقة Windows

	إنشاء قاعدة بيانات تلقائيًا (بواسطة المثبت)	إنشاء قاعدة بيانات يدويًا (بواسطة المسؤول)
الحساب الذي يعمل بموجبه المثبّت	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه. • نظام إدارة قواعد البيانات المحلي: حساب مسؤول محلي أو حساب مجال.	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه. • نظام إدارة قواعد البيانات المحلي: حساب مسؤول محلي أو حساب مجال.

حقوق الحساب الذي يعمل بموجبه المثبّت	• حقوق النظام: حقوق المسؤول المحلي.
	• حقوق SQL Server:
	  • الدور على مستوى الخادم: مسؤول النظام.
		• حقوق النظام: حقوق المسؤول المحلي.
		• حقوق SQL Server:
		  • دور على مستوى الخادم: العامة.
		  • عضوية دور قاعدة البيانات لقاعدة بيانات الخادم: db_owner، عام.
		  • المخطط الافتراضي لقاعدة بيانات الخادم: dbo.

حساب خدمة خادم إدارة	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه.
	• نظام إدارة قاعدة البيانات المحلي:
	  • يتم اختيار حساب Windows بواسطة المسؤول.
	  • حساب بتنسيق KL-AK- * يقوم المثبت تلقائيًا بإنشائه.
		• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه.
		• نظام إدارة قاعدة البيانات المحلي:
		  • يتم اختيار حساب Windows بواسطة المسؤول.
		  • حساب بتنسيق KL-AK- * يقوم المثبت تلقائيًا بإنشائه (في هذه الحالة، لا نوصيك بإنشاء حساب KL-AK-*).

حقوق حساب خدمة خادم الإدارة	• حقوق النظام: الحقوق المطلوبة المعيّنة بواسطة المثبّت.
	• حقوق SQL Server: الحقوق المطلوبة المعيّنة بواسطة المثبّت.
		• حقوق النظام: الحقوق المطلوبة المعيّنة بواسطة المثبّت.
		• حقوق SQL Server:
		  • دور على مستوى الخادم: العامة.
		  • عضوية دور قاعدة البيانات لقاعدة بيانات الخادم: db_owner، عام.
		  • المخطط الافتراضي لقاعدة بيانات الخادم: dbo.

Microsoft SQL Server مع مصادقة SQL Server

إذا اخترت SQL Server باعتباره نظام إدارة قاعدة البيانات، فيمكنك استخدام مصادقة SQL Serverللوصول إلى SQL Server. قم بتكوين حقوق النظام لحساب Windows المستخدَم لتشغيل المثبت ولحساب Windows المستخدم لبدء خدمة خادم الإدارة. في SQL Server، أنشئ تسجيل دخول بكلمة مرور لاستخدامها في المصادقة. ثم امنح حساب SQL Server هذه الحقوق المطلوبة المدرجة في الجدول أدناه. لمزيد من المعلومات حول كيفية تكوين حقوق الحسابات، يُرجى الرجوع إلى تكوين الحسابات للعمل مع SQL Server (مصادقة SQL Server).

نظام إدارة قواعد بيانات:Microsoft SQL Server (يشمل Express Edition) مع مصادقة SQL Server

	إنشاء قاعدة بيانات تلقائيًا (بواسطة المثبت)	إنشاء قاعدة بيانات يدويًا (بواسطة المسؤول)
الحساب الذي يعمل بموجبه المثبّت	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه. • نظام إدارة قواعد البيانات المحلي: حساب مسؤول محلي أو حساب مجال.	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه. • نظام إدارة قواعد البيانات المحلي: حساب مسؤول محلي أو حساب مجال.

	إنشاء قاعدة بيانات تلقائيًا (بواسطة المثبت)	إنشاء قاعدة بيانات يدويًا (بواسطة المسؤول)
حقوق الحساب الذي يعمل بموجبه المثبّت	حقوق النظام: حقوق المسؤول المحلي.	حقوق النظام: حقوق المسؤول المحلي.
حساب خدمة خادم إدارة	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه. • نظام إدارة قاعدة البيانات المحلي: • يتم اختيار حساب Windows بواسطة المسؤول. • حساب بتنسيق KL-AK- * يقوم المثبت تلقائيًا بإنشائه.	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد الذي تم تثبيت نظام إدارة قاعدة البيانات عليه. • نظام إدارة قاعدة البيانات المحلي: • يتم اختيار حساب مستخدم Windows بواسطة المسؤول. • حساب بتنسيق KL-AK- * يقوم المثبت تلقائيًا بإنشائه.
حقوق حساب خدمة خادم الإدارة	حقوق النظام: الحقوق المطلوبة المعيّنة بواسطة المثبّت.	حقوق النظام: الحقوق المطلوبة المعيّنة بواسطة المثبّت.
حقوق تسجيل الدخول المستخدمة لمصادقة SQL Server	مطلوب حقوق SQL Server لإنشاء قاعدة بيانات وتثبيت خادم الإدارة: • دور على مستوى الخادم: العامة. • عضوية دور قاعدة البيانات لقاعدة البيانات الرئيسية: db_owner. • المخطط الافتراضي لقاعدة البيانات الرئيسية: dbo. • الأذونات: • CONNECT ANY DATABASE • اتصال SQL • CREATE ANY DATABASE • VIEW ANY DATABASE • عرض حالة الخادم (إذا تم تمكين خيار **التشغيل الدائم**) حقوق SQL Server المطلوبة للعمل مع خادم الإدارة: • دور على مستوى الخادم: العامة. • عضوية دور قاعدة البيانات لقاعدة بيانات الخادم: db_owner. • المخطط الافتراضي لقاعدة بيانات الخادم: dbo. • الأذونات: • اتصال SQL • VIEW ANY DATABASE • عرض حالة الخادم (إذا تم تمكين خيار **التشغيل الدائم**) • VIEW ANY DEFINITION	حقوق SQL Server: • دور على مستوى الخادم: العامة. • عضوية دور قاعدة البيانات لقاعدة بيانات الخادم: db_owner. • المخطط الافتراضي لقاعدة بيانات الخادم: dbo. • الأذونات: • اتصال SQL • VIEW ANY DATABASE • VIEW ANY DEFINITION

تكوين حقوق SQL Server لاستعادة بيانات خادم الإدارة

لاستعادة بيانات خادم الإدارة من النسخة الاحتياطية، شغّل الأداة المساعدة klbackup ضمن حساب Windows المستخدم لتثبيت خادم الإدارة. قبل بدء تشغيل الأداة المساعدة klbackup، على SQL Server، امنح حقوق تسجيل الدخول إلى SQL Server المرتبط بحساب Windows هذا. تختلف حقوق SQL Server بناءً على إصدار خادم الإدارة. بالنسبة إلى خادم الإدارة الإصدار 14.2 أو أحدث، يمكنك منح مسؤول النظام دور مستوى الخادم أو دور dbcreator على مستوى الخادم.

حقوق SQL Server لاسترداد قاعدة بيانات خادم الإدارة

خادم الإدارة الإصدار 14.2 أو أحدث	إصدارات خادم الإدارة الأخرى
• حقوق SQL Server: • الدور على مستوى الخادم: dbcreator. • الأذونات: • VIEW ANY DEFINITION قبل بدء تشغيل الأداة المساعدة klbackup، حدد علامة خادم KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. بعد ذلك، نفذ الأمر التالي في سطر الأوامر: `klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL و MariaDB

إذا اخترت MySQL أو MariaDB باعتباره DBMS، فأنشئ حساب DBMS داخليًا ومنح هذا الحساب الحقوق المطلوبة المدرجة في الجدول أدناه. يستخدم المثبت وخدمة خادم الإدارة حساب نظام إدارة قاعدة البيانات الداخلي هذا للوصول إلى نظام إدارة قاعدة البيانات. لاحظ أن طريقة إنشاء قاعدة البيانات لا تؤثر على مجموعة الحقوق المطلوبة. لمزيد من المعلومات حول كيفية تكوين حقوق الحساب، يُرجى الرجوع إلى تكوين الحسابات للعمل مع MySQL و MariaDB.

نظام إدارة قاعدة البيانات: MySQL و MariaDB

	إنشاء قاعدة بيانات تلقائية أو يدوية
الحساب الذي يعمل بموجبه المثبّت	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد مع نظام إدارة قاعدة البيانات المثبتة. • نظام إدارة قواعد البيانات المحلي: حساب مسؤول محلي أو حساب مجال.
حقوق الحساب الذي يعمل بموجبه المثبّت	حقوق النظام: حقوق المسؤول المحلي.

حساب خدمة خادم إدارة	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد مع نظام إدارة قاعدة البيانات المثبتة.
	• نظام إدارة قاعدة البيانات المحلي:
	  • يتم اختيار حساب Windows بواسطة المسؤول.
	  • حساب بتنسيق KL-AK- * يقوم المثبّت بإنشائه تلقائيًا.

حقوق حساب خدمة خادم الإدارة	حقوق النظام: الحقوق المطلوبة المعيّنة بواسطة المثبّت.
حقوق حساب نظام إدارة قاعدة البيانات الداخلي	امتيازات المخطط: • قاعدة بيانات خادم الإدارة: ALL (باستثناء GRANT OPTION) • مخططات النظام (mysql و sys): تحديد، إظهار العرض. • الإجراء المخزن sys.table_exists: EXECUTE (إذا كنت تستخدم MariaDB 10.5 أو ما قبله ك DBMS، فلن تحتاج إلى منح امتياز EXECUTE). امتيازات عالمية لجميع المخططات: إجراء، SUPER.

للحصول على تفاصيل عن كيفية نقل البيانات من مساحة جدول مشتركة إلى مساحة جدول ملف لكل جدول، راجع نقل البيانات من مساحة جدول مشتركة إلى مساحة الجدول لكل ملف في MySQL و MariaDB DBMS.

تكوين الامتيازات لاستعادة بيانات خادم الإدارة

الحقوق التي منحتها لحساب نظام إدارة قاعدة البيانات الداخلي كافية لاستعادة بيانات خادم الإدارة من النسخة الاحتياطية. لبدء الاستعادة، قم بتشغيل الأداة المساعدة klbackup ضمن حساب Windows المستخدم لتثبيت خادم الإدارة.

PostgreSQL أو Postgres Pro

إذا اخترت PostgreSQL أو Postgres Pro باعتباره نظام إدارة قاعدة البيانات، فيمكنك استخدام مستخدم Postgres (دور Postgres الافتراضي) أو إنشاء دور Postgres جديدًا (يشار إليه فيما يلي أيضًا بالدور) للوصول إلى نظام إدارة قواعد البيانات. بناءً على طريقة إنشاء قاعدة بيانات الخادم، امنح الحقوق المطلوبة للدور كما هو موضح في الجدول أدناه. للمزيد من المعلومات حول كيفية تكوين حقوق الدور ، يُرجى الرجوع إلى تكوين الحسابات للعمل مع PostgreSQL أو Postgres Pro.

نظام إدارة قاعدة البيانات: PostgreSQL أو Postgres Pro

	إنشاء قاعدة بيانات تلقائيًا	إنشاء قاعدة بيانات يدويًا
الحساب الذي يعمل بموجبه المثبّت	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد مع نظام إدارة قاعدة البيانات المثبتة. • نظام إدارة قواعد البيانات المحلي: حساب مسؤول محلي أو حساب مجال.	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد مع نظام إدارة قاعدة البيانات المثبتة. • نظام إدارة قواعد البيانات المحلي: حساب مسؤول محلي أو حساب مجال.

حقوق الحساب الذي يعمل بموجبه المثبّت	حقوق النظام: حقوق المسؤول المحلي.		حقوق النظام: حقوق المسؤول المحلي.
حساب خدمة خادم إدارة	• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد مع نظام إدارة قاعدة البيانات المثبتة. • نظام إدارة قاعدة البيانات المحلي: • يتم اختيار حساب Windows بواسطة المسؤول. • حساب بتنسيق KL-AK- * يقوم المثبّت بإنشائه تلقائيًا.		• نظام إدارة قاعدة البيانات عن بُعد: فقط حساب مجال للجهاز البعيد مع نظام إدارة قاعدة البيانات المثبتة. • نظام إدارة قاعدة البيانات المحلي: • يتم اختيار حساب Windows بواسطة المسؤول. • حساب بتنسيق KL-AK- * يقوم المثبّت بإنشائه تلقائيًا.
حقوق حساب خدمة خادم الإدارة	حقوق النظام: الحقوق المطلوبة المعيّنة بواسطة المثبّت.		حقوق النظام: الحقوق المطلوبة المعيّنة بواسطة المثبّت.
حقوق دور Postgres	لا يتطلب مستخدم Postgres حقوقًا إضافية.	امتيازات دور جديد: CREATEDB.	لدور جديد: • الامتيازات في قاعدة بيانات خادم الإدارة: ALL. • الامتيازات في جميع الجداول في المخطط العام: ALL. • الامتيازات في جميع التسلسلات في المخطط العام: ALL.

تكوين الامتيازات لاستعادة بيانات خادم الإدارة

لاستعادة بيانات خادم الإدارة من النسخة الاحتياطية، شغّل الأداة المساعدة klbackup ضمن حساب Windows المستخدم لتثبيت خادم الإدارة. لاحظ أن دور Postgres المستخدم للوصول إلى نظام إدارة قاعدة البيانات يجب أن يتمتع بحقوق المالك في قاعدة بيانات خادم الإدارة.

تكوين الحسابات للعمل مع SQL Server (مصادقة Windows)

المتطلبات الأساسية

قبل تعيين الحقوق للحسابات، قم بتنفيذ الإجراءات التالية:

1. تأكد من تسجيل الدخول إلى النظام تحت حساب المسؤول المحلي.
2. قم بتثبيت بيئة للعمل مع SQL Server.
3. تأكد من أن لديك حساب Windows ستقوم بتثبيت خادم الإدارة ضمنه.
4. تأكد من أن لديك حساب Windows ستبدأ بموجبه خدمة خادم الإدارة.
5. في SQL Server، قم بإنشاء تسجيل دخول لحساب Windows المستخدَم لتشغيل مثبت خادم الإدارة (يشار إليه فيما يلي أيضًا باسم المثبت). قم بتكوين حقوق النظام لحساب Windows المستخدَم لتشغيل المثبت وحساب Windows المستخدم لبدء خدمة خادم الإدارة.

إذا كنت تستخدم SQL Server Management Studio، في صفحة **عام** في نافذة خصائص تسجيل الدخول، حدد خيار **مصادقة Windows**.

إذا كنت ترغب في تثبيت خادم الإدارة وSQL Server على الأجهزة الموجودة في مجالات Windows منفصلة، لاحظ أن هذه المجالات يجب أن تتضمن علاقات ثقة ثنائية الاتجاه لضمان التشغيل الصحيح لخادم الإدارة، بما في ذلك المهام قيد التشغيل وتطبيق السياسات. للحصول على معلومات عن الحسابات المطلوبة للعمل مع مختلف نظم إدارة قواعد البيانات وحقوق الحسابات، راجع الحسابات للعمل مع نظام إدارة قواعد البيانات.

تكوين الحسابات لتثبيت خادم الإدارة (الإنشاء التلقائي لقاعدة بيانات خادم الإدارة)

لتكوين حسابات تثبيت خادم الإدارة:

1. في SQL Server، قم بتعيين دور مسؤول النظام على مستوى الخادم لتسجيل الدخول إلى حساب Windows المستخدم لتشغيل المثبت.

2. قم بتسجيل الدخول إلى النظام تحت حساب Windows المستخدم لتشغيل برنامج التثبيت.

3. قم بتشغيل مثبت خادم الإدارة.

   يبدأ معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

4. حدد الخيار تثبيت مخصص لخادم الإدارة.

5. حدد ملف Microsoft SQL Server باعتباره نظام إدارة قاعدة البيانات الذي يخزن قاعدة بيانات خادم الإدارة.

6. حدد وضع مصادقة Microsoft Windows لإنشاء اتصال بين خادم الإدارة و SQL Server من خلال حساب Windows.

7. حدد حساب Windows المستخدم لبدء خدمة خادم الإدارة.

   يمكنك تحديد حساب مستخدم Windows الذي قمت بإنشاء تسجيل دخول إلى SQL Server له مسبقًا. بدلاً من ذلك، يمكنك إنشاء حساب Windows جديد تلقائيًا بتنسيق KL-AK- * باستخدام برنامج التثبيت. في هذه الحالة، يقوم المثبت تلقائيًا بإنشاء تسجيل دخول إلى SQL Server لهذا الحساب. بغض النظر عن اختيار الحساب، يقوم المثبت بتعيين حقوق النظام وحقوق SQL Server المطلوبة لحساب خدمة خادم الإدارة.

بعد انتهاء التثبيت، يتم إنشاء قاعدة بيانات الخادم وتعيين جميع حقوق النظام وحقوق SQL Server المطلوبة إلى حساب خدمة خادم الإدارة. خادم الإدارة جاهز للاستخدام.

تكوين الحسابات لتثبيت خادم الإدارة (إنشاء قاعدة بيانات خادم الإدارة يدويًا)

لتكوين حسابات تثبيت خادم الإدارة:

1. في SQL Server، قم بإنشاء قاعدة بيانات فارغة. سيتم استخدام قاعدة البيانات هذه كقاعدة بيانات خادم الإدارة (يشار إليها فيما يلي أيضًا باسم قاعدة بيانات الخادم).

2. بالنسبة إلى كل من عمليات تسجيل الدخول إلى SQL Server التي تم إنشاؤها لحسابات Windows، حدد الدور العام على مستوى الخادم ثم كون التعيين إلى قاعدة البيانات التي تم إنشاؤها:

   - دور على مستوى الخادم: العامة
   - عضوية دور قاعدة البيانات: db_owner، عام
   - المخطط الافتراضي: dbo

3. قم بتسجيل الدخول إلى النظام تحت حساب Windows المستخدم لتشغيل برنامج التثبيت.

4. قم بتشغيل مثبت خادم الإدارة.

   يبدأ معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

5. حدد الخيار تثبيت مخصص لخادم الإدارة.

6. حدد ملف Microsoft SQL Server باعتباره نظام إدارة قاعدة البيانات الذي يخزن قاعدة بيانات خادم الإدارة.

7. حدد اسم قاعدة البيانات التي تم إنشاؤها كملف اسم قاعدة بيانات خادم الإدارة.

8. حدد وضع مصادقة Microsoft Windows لإنشاء اتصال بين خادم الإدارة و SQL Server من خلال حساب Windows.

9. حدد حساب Windows المستخدم لبدء خدمة خادم الإدارة.

يمكنك تحديد حساب مستخدم Windows الذي قمت بإنشاء تسجيل دخول إلى SQL Server له وتكوين حقوق تسجيل الدخول مسبقًا.

لا نوصي بإنشاء حساب Windows جديد تلقائيًا بتنسيق KL-AK- *. في هذه الحالة، يقوم المثبت بإنشاء حساب Windows جديد لم تقم بإنشاء حساب SQL Server وتكوينه. لا يمكن لخادم الإدارة استخدام هذا الحساب لبدء خدمة خادم الإدارة. إذا كان من الضروري إنشاء حساب KL-AK- * Windows ، فلا تبدأ تشغيل وحدة تحكم الإدارة بعد التثبيت. نفذ ما يلي بدلاً من ذلك:

1. أوقف خدمة kladminserver.

2. في SQL Server، قم بإنشاء تسجيل دخول إلى SQL Server لحساب KL-AK- * Windows الذي تم إنشاؤه.

3. امنح حقوق تسجيل الدخول إلى SQL Server هذا وقم بتكوين التعيين إلى قاعدة البيانات التي تم إنشاؤها:

- دور على مستوى الخادم: العامة
- عضوية دور قاعدة البيانات: db_owner، عام
- المخطط الافتراضي: dbo

4. أعد تشغيل خدمة kladminserver، ثم قم بتشغيل وحدة التحكم الإدارة.

بعد انتهاء التثبيت، سيستخدم خادم الإدارة قاعدة البيانات التي تم إنشاؤها لتخزين بيانات الخادم. خادم الإدارة جاهز للاستخدام.

تكوين الحسابات للعمل مع SQL Server (مصادقة SQL Server)

المتطلبات الأساسية

قبل تعيين الحقوق للحسابات، قم بتنفيذ الإجراءات التالية:

1. تأكد من تسجيل الدخول إلى النظام تحت حساب المسؤول المحلي.

2. قم بتثبيت بيئة للعمل مع SQL Server.

3. تأكد من أن لديك حساب Windows ستقوم بتثبيت خادم الإدارة ضمنه.

4. تأكد من أن لديك حساب Windows ستبدأ بموجبه خدمة خادم الإدارة.

5. في SQL Server، قم بتمكين وضع مصادقة SQL Server.

إذا كنت تستخدم SQL Server Management Studio، في نافذة خصائص SQL Server، في صفحة **الحماية**، حدد خيار **وضع مصادقة SQL Server و Windows**.

6. في SQL Server، قم بإنشاء تسجيل دخول بكلمة مرور. سيستخدم مثبت خادم الإدارة (المشار إليه فيما يلي أيضًا باسم المثبت) وخدمة خادم الإدارة حساب SQL Server هذا للوصول إلى SQL Server.

إذا كنت تستخدم SQL Server Management Studio، في صفحة **عام** من نافذة خصائص تسجيل الدخول، حدد الخيار **مصادقة خادم SQL**.

إذا كنت ترغب في تثبيت خادم الإدارة وSQL Server على الأجهزة الموجودة في مجالات Windows منفصلة، لاحظ أن هذه المجالات يجب أن تتضمن علاقات ثقة ثنائية الاتجاه لضمان التشغيل الصحيح لخادم الإدارة، بما في ذلك المهام قيد التشغيل وتطبيق السياسات. للحصول على معلومات عن الحسابات المطلوبة للعمل مع مختلف نظم إدارة قواعد البيانات وحقوق الحسابات، راجع الحسابات للعمل مع نظام إدارة قواعد البيانات.

تكوين الحسابات لتثبيت خادم الإدارة (الإنشاء التلقائي لقاعدة بيانات خادم الإدارة)

لتكوين حسابات تثبيت خادم الإدارة:

1. في SQL Server، قم بتعيين حساب SQL Server إلى الإعداد الافتراضي رئيسي - سيد قاعدة البيانات. قاعدة البيانات الرئيسية هي نموذج لقاعدة بيانات خادم الإدارة (يشار إليها فيما يلي أيضًا باسم قاعدة بيانات الخادم). يتم استخدام قاعدة البيانات الرئيسية للتعيين حتى يقوم المثبت بإنشاء قاعدة بيانات الخادم. امنح الحقوق والأذونات التالية لحساب SQL Server:
   - دور على مستوى الخادم: العامة
   - عضوية دور قاعدة البيانات لقاعدة البيانات الرئيسية: db_owner
   - المخطط الافتراضي لقاعدة البيانات الرئيسية: dbo
   - الأذونات:
     - CONNECT ANY DATABASE
     - اتصال SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. قم بتسجيل الدخول إلى النظام تحت حساب Windows المستخدم لتشغيل برنامج التثبيت.
3. قم بتشغيل المثبّت.

   يبدأ معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.
4. حدد الخيار تثبيت مخصص لخادم الإدارة.
5. حدد ملف Microsoft SQL Server باعتباره نظام إدارة قاعدة البيانات الذي يخزن قاعدة بيانات خادم الإدارة.
6. حدد اسم قاعدة بيانات خادم الإدارة.
7. حدد وضع مصادقة خادم SQL لإنشاء اتصال بين خادم الإدارة و SQL Server من خلال حساب SQL Server الذي تم إنشاؤه. ثم حدد بيانات اعتماد حساب SQL Server.
8. حدد حساب Windows المستخدم لبدء خدمة خادم الإدارة.

   يمكنك تحديد حساب مستخدم Windows موجود أو إنشاء حساب Windows جديد بتنسيق KL-AK-* باستخدام المُثبت. بغض النظر عن اختيار الحساب، يقوم المثبت بتعيين حقوق النظام المطلوبة لحساب خدمة خادم الإدارة.

بعد انتهاء التثبيت، يتم إنشاء قاعدة بيانات الخادم وتعيين جميع حقوق النظام المطلوبة إلى حساب خدمة خادم الإدارة. خادم الإدارة جاهز للاستخدام.

يمكنك إلغاء التعيين إلى قاعدة البيانات الرئيسية، لأن المثبّت قد أنشأ قاعدة بيانات خادم وضبط التعيين إلى قاعدة البيانات هذه أثناء تثبيت خادم الإدارة.

نظرًا لأن إنشاء قاعدة البيانات تلقائيًا يتطلب أذونات أكثر من العمل العادي مع خادم الإدارة، يمكنك إبطال بعض الأذونات. في SQL Server، حدد حساب SQL Server ثم امنح الحقوق التالية للعمل مع خادم الإدارة:

- دور على مستوى الخادم: العامة
- عضوية دور قاعدة البيانات لقاعدة بيانات الخادم: db_owner
- المخطط الافتراضي لقاعدة بيانات الخادم: dbo
- الأذونات:
  - اتصال SQL
  - VIEW ANY DATABASE

تكوين الحسابات لتثبيت خادم الإدارة (إنشاء قاعدة بيانات خادم الإدارة يدويًا)

لتكوين حسابات تثبيت خادم الإدارة:

1. في SQL Server، قم بإنشاء قاعدة بيانات فارغة. سيتم استخدام قاعدة البيانات هذه كقاعدة بيانات خادم الإدارة.
2. في SQL Server، امنح الحقوق والأذونات التالية لحساب SQL Server:
   - دور على مستوى الخادم: العامة.
   - عضوية دور قاعدة البيانات لقاعدة البيانات التي تم إنشاؤها: db_owner.
   - المخطط الافتراضي لقاعدة البيانات التي تم إنشاؤها: dbo.
   - الأذونات:
     - اتصال SQL
     - VIEW ANY DATABASE
3. قم بتسجيل الدخول إلى النظام تحت حساب Windows المستخدم لتشغيل برنامج التثبيت.
4. قم بتشغيل المثبّت.
   يبدأ معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.
5. حدد الخيار تثبيت مخصص لخادم الإدارة.
6. حدد ملف Microsoft SQL Server باعتباره نظام إدارة قاعدة البيانات الذي يخزن قاعدة بيانات خادم الإدارة.
7. حدد اسم قاعدة البيانات التي تم إنشاؤها كملف اسم قاعدة بيانات خادم الإدارة.
8. حدد وضع مصادقة خادم SQL لإنشاء اتصال بين خادم الإدارة و SQL Server من خلال حساب SQL Server الذي تم إنشاؤه. ثم حدد بيانات اعتماد حساب SQL Server.

9. حدد حساب Windows المستخدم لبدء خدمة خادم الإدارة.

يمكنك تحديد حساب مستخدم Windows موجود أو إنشاء حساب Windows جديد بتنسيق KL-AK-* باستخدام المُثبت. بغض النظر عن اختيار الحساب، يقوم المثبت بتعيين حقوق النظام المطلوبة لحساب خدمة خادم الإدارة.

بعد انتهاء التثبيت، سيستخدم خادم الإدارة قاعدة البيانات التي تم إنشاؤها لتخزين بيانات خادم الإدارة. يتم تعيين جميع حقوق النظام المطلوبة لحساب خدمة خادم الإدارة. خادم الإدارة جاهز للاستخدام.

تكوين الحسابات للعمل مع MySQL وMariaDB

المتطلبات الأساسية

قبل تعيين الحقوق للحسابات، قم بتنفيذ الإجراءات التالية:

1. تأكد من تسجيل الدخول إلى النظام تحت حساب المسؤول المحلي.
2. قم بتثبيت بيئة للعمل مع MySQL أو MariaDB.
3. تأكد من أن لديك حساب Windows ستقوم بتثبيت خادم الإدارة ضمنه.
4. تأكد من أن لديك حساب Windows ستبدأ بموجبه خدمة خادم الإدارة.

تكوين الحسابات لتثبيت خادم الإدارة

لتكوين حسابات تثبيت خادم الإدارة:

1. قم بتشغيل بيئة للعمل مع MySQL أو MariaDB ضمن حساب الجذر الذي قمت بإنشائه عند تثبيت DBMS.
2. قم بإنشاء حساب DBMS داخلي بكلمة مرور. ستستخدم أداة تثبيت خادم الإدارة (المشار إليها فيما يلي أيضًا باسم المثبت) وخدمة خادم الإدارة حساب DBMS الداخلي هذا للوصول إلى نظام إدارة قواعد البيانات. امنح الامتيازات التالية لهذا الحساب:
   - امتيازات المخطط:
     - قاعدة بيانات خادم الإدارة: ALL (باستثناء `GRANT OPTION`)
     - مخططات النظام (mysql و sys): `SELECT`، `SHOW VIEW`
     - الإجراء المخزن sys.table_exists: `EXECUTE`
   - الامتيازات العالمية لجميع المخططات: `PROCESS`، `SUPER`

لإنشاء حساب نظام إدارة قواعد البيانات (DBMS) الداخلي ومنح الامتيازات المطلوبة لهذا الحساب، قم بتشغيل البرنامج النصي أدناه (في هذا البرنامج النصي، يكون اسم تسجيل الدخول إلى DBMS هو KCSAdmin، واسم قاعدة بيانات خادم الإدارة هو kav):

```
/* Create a user named KSCAdmin */
'KSCAdmin' CREATE USER
/* Specify a password for KSCAdmin */
;'<password>' IDENTIFIED BY
```

إذا كنت تستخدم MySQL 8.0 أو إصدارًا أقدم باعتباره DBMS، فلاحظ أنه بالنسبة لهذه الإصدارات، لا يتم دعم مصادقة "Caching SHA2 password". غيّر المصادقة الافتراضية من "التخزين المؤقت لكلمة مرور SHA2" إلى "كلمة المرور الأصلية لـ MySQL:"

- لإنشاء حساب DBMS يستخدم مصادقة "كلمة مرور MySQL الأصلية"، قم بتنفيذ الأمر التالي:

```
;'<password>' IDENTIFIED WITH mysql_native_password BY '%'@'KSCAdmin' CREATE USER
```

- لتغيير المصادقة لحساب DBMS موجود، قم بتنفيذ الأمر التالي:

```
;'<password>' IDENTIFIED WITH mysql_native_password BY '%'@'KSCAdmin' ALTER USER
```

```
/* Grant privileges to KSCAdmin */
;'KSCAdmin' TO *.* GRANT USAGE ON
;'KSCAdmin' TO *.GRANT ALL ON kav
;'KSCAdmin' TO *.SHOW VIEW ON mysql ,GRANT SELECT
;'KSCAdmin' TO *.SHOW VIEW ON sys ,GRANT SELECT
;'KSCAdmin' GRANT EXECUTE ON PROCEDURE sys.table_exists TO
;'KSCAdmin' TO *.* GRANT PROCESS ON
;'KSCAdmin' TO *.* GRANT SUPER ON
```

إذا كنت تستخدم MariaDB 10.5 أو إصدارًا أقدم باعتباره DBMS، فلن تحتاج إلى منح امتياز EXECUTE. في هذه الحالة، استبعد الأمر التالي من البرنامج النصي: `'KSCAdmin' GRANT EXECUTE ON PROCEDURE sys.table_exists TO`.

3. لعرض قائمة الامتيازات الممنوحة لحساب نظام إدارة قاعدة البيانات، قم بتشغيل البرنامج النصي التالي:

```
;'KSCAdmin' SHOW grants for
```

4. لإنشاء قاعدة بيانات خادم الإدارة يدويًا، قم بتشغيل البرنامج النصي التالي (في هذا البرنامج النصي، يكون اسم قاعدة بيانات خادم الإدارة هو kav):

```
CREATE DATABASE kav
DEFAULT CHARACTER SET ascii
;DEFAULT COLLATE ascii_general_ci
```

استخدم نفس اسم قاعدة البيانات الذي تحدده في البرنامج النصي الذي ينشئ حساب نظام إدارة قاعدة البيانات.

5. قم بتسجيل الدخول إلى النظام تحت حساب Windows المستخدم لتشغيل برنامج التثبيت.

6. قم بتشغيل المثبّت.

يبدأ معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

7. حدد الخيار تثبيت مخصص لخادم الإدارة.

8. حدد ملف MySQL أو MariaDB باعتباره نظام إدارة قاعدة البيانات الذي يخزن قاعدة بيانات خادم الإدارة.

9. حدد اسم قاعدة بيانات خادم الإدارة. استخدم نفس اسم قاعدة البيانات الذي تحدده في البرنامج النصي.

10. حدد ال بيانات اعتماد حساب نظام إدارة قاعدة البيانات الذي قمت بإنشائه بواسطة البرنامج النصي.

11. حدد حساب Windows المستخدم لبدء خدمة خادم الإدارة.

يمكنك تحديد حساب مستخدم Windows موجود أو إنشاء حساب Windows جديد تلقائيًا بتنسيق KL-AK- * باستخدام برنامج التثبيت. بغض النظر عن اختيار الحساب، يقوم المثبت بتعيين حقوق النظام المطلوبة لحساب خدمة خادم الإدارة.

بعد انتهاء التثبيت، يتم إنشاء قاعدة بيانات خادم الإدارة ويكون خادم الإدارة جاهزًا للاستخدام.

نقل البيانات من مساحة جدول مشتركة إلى مساحة جدول لكل ملف في MySQL وMariaDB DBMS

بالنسبة إلى MySQL وMariaDB DBMS، يمكنك تخزين البيانات بالطرق التالية:

- كمساحة جدول مشتركة، عندما يتم تخزين بيانات جميع قواعد بيانات المستخدم في ملف واحد (عادةً ، في ملف `ibdata1`).
- كملف لكل جدول، عندما يتم إنشاء مساحة بيانات منفصلة لكل جدول كملف منفصل.

ويؤدي استخدام مساحة جدول مشتركة إلى زيادة مخاطر تجزئة مساحة الجدول. ونظرًا لأنه من غير الممكن تنفيذ عملية `SHRINK`، فقد يشغل ملف في مساحة جدول مشتركة حوالي 90% من مساحة القرص. يؤثر هذا سلبًا على أداء النظام الفرعي للقرص. بالتالي، من المفيد اختيار مساحة جدول ملف لكل جدول.

توضح هذه المقالة كيفية نقل البيانات من مساحة جدول مشتركة إلى مساحة جدول ملف لكل جدول. في حالة استخدام MySQL أو MariaDB DBMS أيضًا بواسطة تطبيقات أخرى، فيجب عليك نقل قواعد بيانات هذه التطبيقات إلى مساحة الجدول لكل ملف.

نوصي بتنفيذ هذا الإجراء فقط إذا كنت تستخدم MySQL أو MariaDB DBMS لخادم الإدارة.
قد يؤدي نقل البيانات من مساحة جدول مشترك إلى مساحة جدول ملف لكل جدول إلى زيادة الحمل على النظام الفرعي للقرص.

المتطلبات الأساسية

قبل البدء، تأكد مما يلي:

- أنك أنشأت نسخة احتياطية من بيانات خادم الإدارة عن طريق تشغيل مهمة نسخ احتياطي للبيانات أو الأداة المساعدة klbackup.
- أنك أنشأت نسخة احتياطية من التطبيقات الأخرى التي تدار قواعد بياناتها بواسطة MySQL أو MariaDB DBMS (إن وجدت).
- على الجهاز الذي تم تثبيت نظام إدارة قواعد البيانات (DBMS) عليه، توجد مساحة خالية على القرص في القسم الذي يحتوي على قاعدة البيانات.

تبلغ مساحة القرص المطلوبة 150% من إجمالي حجم قواعد البيانات الحالي (الحجم الحالي لملف `ibdata1`).

المعالجة

ولنقل البيانات من مساحة جدول مشتركة إلى مساحة جدول ملف لكل جدول:

1. أوقف خدمة خادم إدارة Kaspersky Security Center والتطبيقات الأخرى باستخدام مثيل نظام إدارة قواعد البيانات (DBMS) الذي تريد تنفيذ هذا الإجراء من أجله.
2. حسب إصدار نظام إدارة قواعد البيانات (DBMS)، سجل الدخول إلى نظام إدارة قواعد البيانات (DBMS) الخاص بك كمستخدم متميز، ثم في أي تطبيق مناسب، قم بتشغيل البرنامج النصي `fix_tablespace.sql`.

   يمكنك عرض البرامج النصية `fix_tablespace.sql` بالنقر فوق هذه الروابط:

   عرض البرنامج النصي لقاعدة البيانات MySQL 5.7 وMariaDB 10.1+

```
;DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb
// DELIMITER
() `upgd_alter_all_tables_for_all_databases_to_innodb` CREATE PROCEDURE
BEGIN
;DECLARE __st_FETCH_STATUS INT
;(192)VARCHAR `schemaName` DECLARE
```

```
;(192)VARCHAR `tableName` DECLARE
CURSOR FOR `curIX` DECLARE
`TABLE_NAME` , `TABLE_SCHEMA` SELECT
FROM information_schema.TABLES
;'BASE TABLE' = AND TABLE_TYPE ('sys' ,'performance_schema' ,'mysql') NOT IN `TABLE_SCHEMA` WHERE
;1 = SET __st_FETCH_STATUS '02000' DECLARE CONTINUE HANDLER FOR SQLSTATE
;`curIX` OPEN
;`tableName` ,`schemaName` INTO `curIX` FETCH ;0 = `st_FETCH_STATUS__` SET
DO ( 0 = 0 AND __st_FETCH_STATUS = 0) WHILE : while1
;( ';''InnoDB''=ENGINE `' ,`tableName`,'`.`' ,`schemaName` , '` ALTER TABLE' )CONCAT = `strSQL`@ SET
;`strSQL`@ PREPARE stmt1 FROM
;EXECUTE stmt1
;DEALLOCATE PREPARE stmt1
;`tableName` ,`schemaName` INTO `curIX` FETCH ;0 = `st_FETCH_STATUS__` SET
;END WHILE
;`curIX` CLOSE
END
//
; DELIMITER
;1 = SET GLOBAL innodb_file_per_table
;()CALL upgd_alter_all_tables_for_all_databases_to_innodb
;DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb
```

اعرض البرنامج النصي لقاعدة بيانات MySQL 8.0+

```
;DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb
// DELIMITER
() `upgd_alter_all_tables_for_all_databases_to_innodb` CREATE PROCEDURE
BEGIN
;DECLARE __st_FETCH_STATUS INT
;(192)VARCHAR `schemaName` DECLARE
;(192)VARCHAR `tableName` DECLARE
CURSOR FOR `curIX` DECLARE
`TABLE_NAME` , `TABLE_SCHEMA` SELECT
FROM information_schema.TABLES
;'BASE TABLE' = AND TABLE_TYPE ('sys' ,'performance_schema' ,'mysql') NOT IN `TABLE_SCHEMA` WHERE
;1 = SET __st_FETCH_STATUS '02000' DECLARE CONTINUE HANDLER FOR SQLSTATE
;`curIX` OPEN
;`tableName` ,`schemaName` INTO `curIX` FETCH ;0 = `st_FETCH_STATUS__` SET
DO ( 0 = 0 AND __st_FETCH_STATUS = 0) WHILE : while1
;( ';''InnoDB''=ENGINE `' ,`tableName`,'`.`' ,`schemaName` , '` ALTER TABLE' )CONCAT = `strSQL`@ SET
;`strSQL`@ PREPARE stmt1 FROM
;EXECUTE stmt1
;DEALLOCATE PREPARE stmt1
= TABLESPACE `' ,`tableName`,'`.`' ,`schemaName` , '` ALTER TABLE' )CONCAT = `strSQL`@ SET
;( ';innodb_file_per_table
;`strSQL`@ PREPARE stmt2 FROM
;EXECUTE stmt2
;DEALLOCATE PREPARE stmt2
;`tableName` ,`schemaName` INTO `curIX` FETCH ;0 = `st_FETCH_STATUS__` SET
;END WHILE
;`curIX` CLOSE
END
//
; DELIMITER
;1 = SET GLOBAL innodb_file_per_table
;()CALL upgd_alter_all_tables_for_all_databases_to_innodb
;DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb
```

يجب ألا توقف تنفيذ البرنامج النصي.
إذا لم تحدث أخطاء في نظام إدارة قواعد البيانات (DBMS)، لكنك أنهيت تنفيذ البرنامج النصي، فقم إما بتشغيل البرنامج النصي مرة أخرى أو توقف عن تنفيذ خطوات هذا الإجراء، وأعد تشغيل خدمة نظام إدارة قواعد البيانات (DBMS)، واستعد بيانات خادم الإدارة من النسخة الاحتياطية.

3. في القسم `[mysqld]` من ملف my.cnf، اضبط المعلمة `innodb_file_per_table` على 1.

4. أعد تشغيل خدمة MySQL أو MariaDB.

5. ابدأ تشغيل خدمة خادم إدارة Kaspersky Security Center.

يتم نقل البيانات من مساحة جدول مشتركة إلى مساحة ملف لكل جدول.

تكوين الحسابات للعمل مع PostgreSQL و Postgres Pro

المتطلبات الأساسية

قبل تعيين الحقوق للحسابات، قم بتنفيذ الإجراءات التالية:

1. تأكد من تسجيل الدخول إلى النظام تحت حساب المسؤول المحلي.
2. قم بتثبيت بيئة للعمل مع PostgreSQL و Postgres Pro.
3. تكوين خادم PostgreSQL أو Postgres Pro للعمل مع Kaspersky Security Center 15.1.
4. تأكد من أن لديك حساب Windows ستقوم بتثبيت خادم الإدارة ضمنه.
5. تأكد من أن لديك حساب Windows ستبدأ بموجبه خدمة خادم الإدارة.

تكوين الحسابات لتثبيت خادم الإدارة (الإنشاء التلقائي لقاعدة بيانات خادم الإدارة)

لتكوين حسابات تثبيت خادم الإدارة:

1. شغّل بيئة للعمل مع PostgreSQL و Postgres Pro.
2. اختر دور Postgres للوصول إلى نظم إدارة قواعد البيانات. يمكنك تحديد أي من الأدوار التالية:
   - مستخدِم Postgres (دور Postgres الافتراضي).

     إذا كنت تستخدم مستخدم Postgres، فإنك لا تحتاج إلى منح حقوق إضافية له.
   - دور Postgres جديد.

     إذا كنت تريد استخدام دور Postgres جديد، فأنشئ هذا الدور وامنحه امتياز CREATEDB. ولفعل ذلك، قم بتشغيل البرنامج النصي التالي (في هذا البرنامج النصي، يكون الدور هو KCSAdmin):

```
;CREATEDB '<password>' WITH PASSWORD "KSCAdmin" CREATE USER
```

   سيتم استخدام الدور الذي تم إنشاؤه كمالك لقاعدة بيانات خادم الإدارة (يشار إليها فيما يلي أيضًا باسم قاعدة بيانات الخادم).
3. قم بتسجيل الدخول إلى النظام تحت حساب Windows المستخدم لتشغيل مثبت خادم الإدارة (يشار إليه فيما يلي أيضًا باسم المثبت).
4. قم بتشغيل المثبّت.

   يبدأ معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.
5. حدد الخيار تثبيت مخصص لخادم الإدارة.
6. حدد ملف PostgreSQL أو Postgres Pro كنظام إدارة قاعدة البيانات الذي يخزن قاعدة بيانات خادم الإدارة.
7. حدد اسم قاعدة بيانات الخادم. سيقوم المثبت تلقائيًا بإنشاء قاعدة بيانات الخادم.

8. حدد بيانات اعتماد دور Postgres.

9. حدد حساب Windows المستخدم لبدء خدمة خادم الإدارة.

يمكنك تحديد حساب مستخدم Windows موجود أو إنشاء حساب Windows جديد تلقائيًا بتنسيق KL-AK- * باستخدام برنامج التثبيت. بغض النظر عن اختيار الحساب، يقوم المثبت بتعيين حقوق النظام المطلوبة لحساب خدمة خادم الإدارة.

بعد انتهاء التثبيت، يتم إنشاء قاعدة بيانات الخادم تلقائيًا ويكون خادم الإدارة جاهزًا للاستخدام.

تكوين الحسابات لتثبيت خادم الإدارة (إنشاء قاعدة بيانات خادم الإدارة يدويًا)

لتكوين حسابات تثبيت خادم الإدارة:

1. شغّل بيئة للعمل مع Postgres.

2. تسجيل الدخول تحت اسم مستخدم Postgres في قاعدة بيانات Postgres.

3. أنشئ دور Postgres جديد (في هذا المثال، الدور هو KSCAdmin):

```
;'<password>' WITH PASSWORD "KSCAdmin" CREATE USER
```

4. أنشئ قاعدة بيانات لخادم الإدارة (في هذا المثال، اسم قاعدة بيانات خادم الإدارة هو KAV):

```
;"KSCAdmin" OWNER 'UTF8' ENCODING "KAV" CREATE DATABASE
```

في حال حدوث خطأ "الترميز الجديد (UTF8) غير متوافق مع ترميز قاعدة بيانات القالب"، أنشئ قاعدة بيانات باستخدام الأمر:

```
;TEMPLATE template0 "KSCAdmin" OWNER 'UTF8' ENCODING "KAV" CREATE DATABASE
```

بدلاً من:

```
;"KSCAdmin" OWNER 'UTF8' ENCODING "KAV" CREATE DATABASE
```

5. منح جميع الامتيازات للدور في قاعدة بيانات خادم الإدارة:

```
;"KSCAdmin" TO "KAV" GRANT ALL PRIVILEGES ON DATABASE
```

وتأكد أن الدور يمتلك امتيازات CONNECT وTEMPORARY الافتراضية في قاعدة بيانات خادم الإدارة.

6. منح الامتيازات التالية لدور Postgres الذي تم إنشاؤه:

- الامتيازات في جميع الجداول في المخطط العام: ALL
- الامتيازات في جميع التسلسلات في المخطط العام: ALL

لفعل ذلك، سجل الدخول تحت مستخدم Postgres في قاعدة بيانات الخادم وشغّل البرنامج النصي التالي (في هذا البرنامج النصي، يكون الدور هو KSCAdmin):

```
;"KSCAdmin" TO "public" GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA
;"KSCAdmin" TO "public" GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA
```

7. قم بتسجيل الدخول إلى النظام تحت حساب Windows المستخدم لتشغيل برنامج التثبيت.

8. قم بتشغيل مثبت خادم الإدارة.

يبدأ معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

9. حدد الخيار تثبيت مخصص لخادم الإدارة.

10. حدد ملف PostgreSQL أو Postgres Pro كنظام إدارة قاعدة البيانات الذي يخزن قاعدة بيانات خادم الإدارة.

11. حدد اسم قاعدة بيانات الخادم. استخدم نفس اسم قاعدة البيانات الذي تحدده في البرنامج النصي. لاحظ أن اسم قاعدة البيانات حساس لحالة الأحرف.

12. حدد بيانات اعتماد دور Postgres.

13. حدد حساب Windows المستخدم لبدء خدمة خادم الإدارة.

يمكنك تحديد حساب مستخدم Windows موجود أو إنشاء حساب Windows جديد تلقائيًا بتنسيق KL-AK- * باستخدام برنامج التثبيت. بغض النظر عن اختيار الحساب، يقوم المثبت بتعيين حقوق النظام المطلوبة لحساب خدمة خادم الإدارة.

بعد انتهاء التثبيت، سيستخدم خادم الإدارة قاعدة البيانات التي تم إنشاؤها لتخزين بيانات خادم الإدارة. خادم الإدارة جاهز للاستخدام.

السيناريو: مصادقة خادم Microsoft SQL

تنطبق المعلومات الواردة في هذا القسم فقط على التكوينات التي يُستخدم فيها Microsoft SQL Server كنظام Kaspersky Security Center لإدارة قواعد البيانات.

لحماية بيانات Kaspersky Security Center المنقولة إلى قاعدة البيانات والبيانات المخزنة في قاعدة البيانات أو المنقولة منها من الوصول غير المصرح به، يجب عليك تأمين الاتصال بين Kaspersky Security Center و SQL Server. الطريقة الأكثر موثوقية لتوفير اتصال آمن هي تثبيت Kaspersky Security Center و SQL Server على نفس الجهاز واستخدام آلية الذاكرة المشتركة لكلا التطبيقين. في جميع الحالات الأخرى، نوصي باستخدام شهادة SSL أو TLS لمصادقة مثيل SQL Server. يمكنك استخدام شهادة من مرجع معتمد موثوق (CA) أو شهادة موقعة ذاتيًا. نوصي باستخدام شهادة من مرجع مصدق موثوق به لأن الشهادة الموقعة ذاتيًا توفر حماية محدودة فقط.

تستمر مصادقة خادم SQL Server على مراحل:

1. **إنشاء شهادة SSL أو TLS موقعة ذاتيًا لخادم SQL Server وفقًا لمتطلبات الشهادة**

إذا كان لديك بالفعل شهادة لخادم SQL Server، فتخط هذه الخطوة.

شهادة SSL قابلة للتطبيق فقط على إصدارات SQL Server الأقدم من 2016 (13.x). في SQL Server 2016 (13.x) والإصدارات الأحدث، استخدم شهادة TLS.

على سبيل المثال، لإنشاء شهادة TLS، أدخل الأمر التالي في PowerShell:

```
LocalMachine\:New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert
-KeySpec KeyExchange
```

بخصوص الأمر، بدلاً من SQL_HOST_NAME، يجب كتابة اسم مضيف SQL Server إذا كان المضيف مضمنًا في المجال أو اكتب اسم المجال المؤهل بالكامل (FQDN) للمضيف إذا لم يكن المضيف مدرجًا في المجال. يجب تحديد نفس الاسم - اسم المضيف أو FQDN - كاسم مثيل خادم SQL Server في معالج إعداد خادم الإدارة.

2. **إضافة الشهادة لمثيل SQL Server**

تعتمد التعليمات الخاصة بهذه المرحلة على النظام الأساسي الذي يعمل عليه SQL Server. راجع الوثائق الرسمية للاطلاع على التفاصيل:

- Windows
- Linux
- Amazon Relational Database Service

لاستخدام الشهادة على نظام مجموعة تجاوز الفشل، يجب عليك تثبيت الشهادة على كل عقدة في نظام مجموعة تجاوز الفشل. للحصول على التفاصيل، راجع وثائق Microsoft .

3 **تعيين أذونات حساب الخدمة**

تأكد من أن حساب الخدمة الذي يتم تشغيل خدمة خادم SQL Server عليه لديه إذن التحكم الكامل للوصول إلى المفاتيح الخاصة. للحصول على التفاصيل، راجع وثائق Microsoft .

4 **إضافة الشهادة إلى قائمة الشهادات الموثوقة لـ Kaspersky Security Center**

على جهاز خادم الإدارة، أضف الشهادة إلى قائمة الشهادات الموثوقة. للحصول على التفاصيل، راجع وثائق Microsoft .

5 **تمكين الاتصالات المشفرة بين مثيل SQL Server و Kaspersky Security Center**

على جهاز خادم الإدارة، اضبط القيمة 1 على متغير البيئة `KLDBADO_UseEncryption`. على سبيل المثال، في Windows Server 2012 R2، يمكنك تغيير متغيرات البيئة بالنقر على **متغيرات البيئة** في علامة التبويب **المتقدمة** لنافذة **خصائص النظام** . أضف متغيرًا جديدًا، وقم بتسميته `KLDBADO_UseEncryption`، ثم قم بتعيين القيمة 1.

6 **تكوين إضافي لاستخدام بروتوكول TLS 1.2**

إذا كنت تستخدم بروتوكول TLS 1.2، فقم بما يلي أيضًا:

- تأكد من أن الإصدار المثبت من خادم SQL Server هو تطبيق 64 بت.
- قم بتثبيت برنامج تشغيل Microsoft OLE DB على جهاز خادم الإدارة. للحصول على التفاصيل، راجع وثائق Microsoft .
- على جهاز خادم الإدارة، اضبط القيمة 1 على متغير البيئة `KLDBADO_UseMSOLEDBSQL`. على سبيل المثال، في Windows Server 2012 R2، يمكنك تغيير متغيرات البيئة بالنقر على **متغيرات البيئة** في علامة التبويب **المتقدمة** لنافذة **خصائص النظام** . أضف متغيرًا جديدًا، وقم بتسميته `KLDBADO_UseMSOLEDBSQL`، ثم قم بتعيين القيمة 1.

  إذا كان إصدار برنامج تشغيل OLE DB هو 19 أو أحدث ، فقم أيضًا بتعيين القيمة `MSOLEDBSQL19` إلى متغير البيئة `KLDBADO_ProviderName` .

7 **تمكين استخدام بروتوكول TCP/IP على مثيل مسمى لخادم SQL Server**

إذا كنت تستخدم مثيلًا مسمًا لخادم SQL Server، فقم أيضًا بتمكين استخدام بروتوكول TCP/IP وتعيين رقم منفذ TCP/IP لمشغل قاعدة بيانات SQL Server. عند تكوين اتصال خادم SQL Server في معالج إعداد خادم الإدارة، حدد اسم مضيف خادم SQL Server ورقم المنفذ في الحقل **اسم مثيل SQL Server**.

السيناريو: مصادقة MySQL Server

نوصي باستخدام شهادة TLS للمصادقة على خادم MySQL. يمكنك استخدام شهادة من مرجع معتمد موثوق (CA) أو شهادة موقعة ذاتيًا.

يدعم خادم الإدارة كلاً من مصادقة SSL أحادية الاتجاه وثنائية الاتجاه لبرنامج MySQL.

تمكين مصادقة SSL أحادية الاتجاه

اتبع هذه الخطوات لتكوين مصادقة SSL أحادية الاتجاه لبرنامج MySQL:

1 أنشئ شهادة TLS موقعة ذاتيًا لخادم MySQL

في PowerShell، قم بتغيير الدليل إلى المجلد الذي تريد تخزين الشهادات فيه. ونفذ الأوامر التالية:

```
` New-SelfSignedCertificate = CertCA$
` "CertCA=CN" Subject-
` "My\CurrentUser\:Cert" CertStoreLocation-
` "SHA256" HashAlgorithm-
(365)AddDays.(Get-Date) NotAfter-

,CertCA.RawData$)ToBase64String::[System.Convert] = CertCABase64$
(InsertLineBreaks::[System.Base64FormattingOptions]

` New-SelfSignedCertificate = CertLeaf$
` "CertLeaf=CN" Subject-
` CertCA$ Signer-
` "My\CurrentUser\:Cert" CertStoreLocation-
` "SHA256" HashAlgorithm-
` KeyExportPolicy Exportable-
(365)AddDays.(Get-Date) NotAfter-

,CertLeaf.RawData$)ToBase64String::[System.Convert] = CertLeafBase64$
(InsertLineBreaks::[System.Base64FormattingOptions]

= CertLeafRSACng$
(CertLeaf$)GetRSAPrivateKey::[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]
= CertLeafKeyBytes$
(Pkcs8PrivateBlob::[System.Security.Cryptography.CngKeyBlobFormat])CertLeafRSACng.Key.Export$
,CertLeafKeyBytes$)ToBase64String::[System.Convert] = CertLeafKeyBase64$
(InsertLineBreaks::[System.Base64FormattingOptions]

"@ = CertCAPemCert$
-----BEGIN CERTIFICATE-----
CertCABase64$
-----END CERTIFICATE-----
@"

"@ = CertLeafPemKey$
-----BEGIN PRIVATE KEY-----
CertLeafKeyBase64$
-----END PRIVATE KEY-----
@"

"@ = CertLeafPemCert$
-----BEGIN CERTIFICATE-----
CertLeafBase64$
-----END CERTIFICATE-----
@"

Output to file #

Out-File -FilePath ca-cert.pem -Encoding Ascii | CertCAPemCert$

Out-File -FilePath server-key.pem -Encoding Ascii | CertLeafPemKey$
Out-File -FilePath server-cert.pem -Encoding Ascii | CertLeafPemCert$
```

تنشئ هذه الأوامر شهادات للمستخدم الحالي وتقوم بتصدير الشهادات إلى تنسيق PEM. وتحتاج فقط إلى ملفات PEM التي تم تصديرها لمصادقة الخادم. ولإزالة الشهادات التي تم إنشاؤها من Windows، نفذ الأمر التالي في PowerShell:

```
certmgr.msc
```

حدد موقع الشهادات التي تم إنشاؤها في مجلد **Personal** ← **Certificates** واحذفها.

2 إنشاء ملف علامة خادم

قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky\Kaspersky Security Center\Lab.

استخدم الأداة المساعدة klscflag لإنشاء علامة خادم KLSRV_MYSQL_OPT_SSL_CA وتحديد المسار إلى الشهادة كقيمتها.

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <المسار إلى ca-cert.pem>
```

3 **تكوين قاعدة البيانات**

حدد الشهادات في ملف my.cnf. افتح ملف my.cnf في محرر نصوص وأضف الأسطر التالية إلى قسم [mysqld]:

```
[mysqld]
ssl-ca="ca-cert.pem\mysqlcerts\..."
ssl-cert="server-cert.pem\mysqlcerts\..."
ssl-key="server-key.pem\mysqlcerts\..."
```

تمكين مصادقة SSL ثنائية الاتجاه

اتبع هذه الخطوات لتكوين مصادقة SSL ثنائية الاتجاه لبرنامج MySQL:

1 **إنشاء ملفات علامة الخادم**

قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky\Kaspersky Security Center\Lab.

استخدم الأداة المساعدة klscflag لإنشاء علامات الخادم وتحديد المسار إلى ملفات الشهادات كقيم لها:

```
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <المسار إلى ca-cert.pem>
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <المسار إلى server-cert.pem>
klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <المسار إلى server-key.pem>
```

2 **حدد عبارة المرور (اختياري)**

إذا كان server-key.pem يتطلب عبارة مرور، فقم بإنشاء علامة KLSRV_MARIADB_OPT_TLS_PASPHRASE وحدد عبارة المرور كقيمة لها:

```
klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <عبارة المرور>
```

3 **تكوين قاعدة البيانات**

حدد الشهادات في ملف my.cnf. افتح ملف my.cnf في محرر نصوص وأضف الأسطر التالية إلى قسم [mysqld]:

```
[mysqld]
ssl-ca="ca-cert.pem\..."
ssl-cert="server-cert.pem\..."
ssl-key="server-key.pem\..."
```

السيناريو: مصادقة خادم PostgreSQL

نوصي باستخدام شهادة TLS للمصادقة على خادم PostgreSQL. يمكنك استخدام شهادة من مرجع معتمد موثوق (CA) أو شهادة موقعة ذاتيًا. استخدم شهادة من مرجع مصدق موثوق به لأن الشهادة الموقعة ذاتيًا توفر حماية محدودة فقط.

يدعم خادم الإدارة كلاً من مصادقة SSL أحادية الاتجاه وثنائية الاتجاه لبرنامج PostgreSQL.

تتم عملية مصادقة خادم PostgreSQL على مراحل:

1. **إنشاء شهادة لخادم PostgreSQL**

   من أداة مساعدة عبر النظام الأساسي مستندة إلى OpenSSL، قم بتنفيذ الأوامر التالية:

   ```
   /" openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj
   "psql=CN
   ```

   ```
   chmod og-rwx psql.key
   ```

2. **إنشاء شهادة لخادم الإدارة**

   قم بتشغيل الأوامر التالية. ويجب أن تتطابق قيمة CN مع اسم المستخدم الذي يتصل ببرنامج PostgreSQL نيابة عن خادم الإدارة. ويتم تعيين اسم المستخدم على postgres بشكل افتراضي.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -
   "postgres=CN/" subj
   ```

   ```
   chmod og-rwx postgres.key
   ```

3. **تكوين مصادقة شهادة العميل**

   Modify pg_hba.conf على النحو التالي:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   تأكد أن pg_hba.conf لا يتضمن سجلًا يبدأ باستخدام `host`.

4. **تحديد شهادة PostgreSQL**

   مصادقة SSL أحادية الاتجاه

   تعديل postgresql.conf كما يلي (حدد المسار الصحيح لملفات .crt و.key):

   ```
   'server-ip ,localhost'= listen_addresses
   on = ssl
   '<psql.crt>' = ssl_cert_file
   '<psql.key>' = ssl_key_file
   ```

   مصادقة SSL ثنائية الاتجاه

   قم بتعديل postgresql.conf كما يلي (حدد المسار الصحيح لملفات .crt و.key):

   ```
   'server-ip ,localhost'= listen_addresses
   on = ssl
   '<postgres.crt>' = ssl_ca_file
   '<psql.crt>' = ssl_cert_file
   '<psql.key>' = ssl_key_file
   ```

5 **إعادة تشغيل مكون PostgreSQL**

قم بتشغيل الأمر التالي:

```
systemctl restart postgresql-14.service
```

6 **تحديد علامة الخادم لخادم الإدارة**

مصادقة SSL أحادية الاتجاه

استخدم الأداة المساعدة klscflag لإنشاء علامة خادم KLSRV_POSTGRES_OPT_SSL_CA وتحديد المسار إلى الشهادة كقيمة لها.

قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو Program Files\:<Disk>\(x86)\Kaspersky Lab\Kaspersky Security Center.

قم بتشغيل الأمر التالي:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v < المسار إلى psql.crt>
```

مصادقة SSL ثنائية الاتجاه

استخدم الأداة المساعدة klscflag لإنشاء علامات الخادم وتحديد المسار إلى ملفات الشهادات كقيم لها.

قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو Program Files\:<Disk>\(x86)\Kaspersky Lab\Kaspersky Security Center.

قم بتشغيل الأوامر التالية:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v < المسار إلى psql.crt>
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v < المسار إلى postgres.crt>
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v < المسار إلى postgres.key>
```

إذا كان postgres.key يتطلب عبارة مرور، فأنشئ علامة KLSRV_POSTGRES_OPT_TLS_PASPHRASE وحدد عبارة المرور كقيمة لها:

```
klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v < عبارة المرور>
```

7 **إعادة تشغيل خدمة خادم الإدارة**

توصيات حول تثبيت خادم الإدارة

يحتوي هذا القسم على توصيات حول كيفية تثبيت خادم الإدارة. يقدّم هذا القسم أيضًا سيناريوهات استخدام مجلد مشترك موجود على جهاز خادم الإدارة لنشر عميل الشبكة على أجهزة عميلة.

إنشاء حسابات لخدمات خادم الإدارة على مجموعة تجاوز الفشل.

بشكل افتراضي، يقوم المثبّت تلقائيًا بإنشاء حسابات غير مميزة لخدمات خادم الإدارة. هذا السلوك هو الأكثر ملاءمةً لتثبيت خادم الإدارة على جهاز عادي.

على الرغم من ذلك، يتطلب تثبيت خادم الإدارة على مجموعة تجاوز الفشل سيناريو مختلفًا:

1. قم بإنشاء حسابات مجال غير مميزة لخدمات خادم الإدارة وأعطها العضوية في مجموعة أمان المجال العمومي المسمّى KLAdmins

2. في مثبّت خادم الإدارة، حدد حسابات المجال التي تم إنشاؤها للخدمات.

تحديد مجلد مشترك

عند تثبيت خادم الإدارة، يمكنك تحديد موقع المجلد المشترك. كما يمكنك أيضًا تحديد موقع المجلد المشترك بعد التثبيت، في خصائص خادم الإدارة. بشكل افتراضي، سيتم إنشاء المجلد المشترك على الجهاز الذي يحتوي على خادم الإدارة (مع منح حقوق القراءة للمجموعة الفرعية **الجميع**). ولكن في بعض الحالات (مثل: التحميل العالي أو الحاجة إلى الوصول من شبكة معزولة)، من المفيد تحديد موقع المجلد المشترك على مورد ملف مخصص.

يُستخدم المجلد المشترك أحيانًا في نشر عميل الشبكة.

يلزم تعطيل حساسية حالة الأحرف للمجلد المشترك.

التثبيت عن بُعد باستخدام أدوات خادم الإدارة عبر سياسات مجموعة Active Directory

في حالة وجود الأجهزة المستهدفة ضمن مجال Windows (وليس مجموعات العمل)، يجب إجراء النشر الأولي (تثبيت عميل الشبكة وتطبيق الأمان على الأجهزة التي لم تتم إدارتها بعد) من خلال سياسات مجموعة Active Directory. يتم القيام بالنشر باستخدام المهمة القياسية للتثبيت عن بُعد من Kaspersky Security Center. إذا كانت الشبكة واسعة النطاق، فمن المفيد تحديد موقع المجلد المشترك على مورد ملف مخصص لتقليل الحمل على النظام الفرعي للقرص الخاص بجهاز خادم الإدارة.

التثبيت عن بُعد من خلال تسليم مسار UNC إلى حزمة مستقلة

إذا كان مستخدمو الأجهزة المتصلة بالشبكة في المؤسسة لديهم حقوق المسؤول المحلي، فإن الطريقة الأخرى للنشر الأولي هي إنشاء حزمة عميل شبكة مستقلة (أو حتى حزمة عميل شبكة "مقترنة" بالإضافة إلى تطبيق الأمان). بعد قيامك بإنشاء حزمة مستقلة، أرسل إلى المستخدمين رابط هذه الحزمة المخزنة في المجلد المشترك. يبدأ التثبيت عندما ينقر المستخدمون فوق الرابط.

التحديث من المجلد المشترك لخادم الإدارة

في مهمة تحديث مكافحة الفيروسات، يمكنك تكوين التحديث من المجلد المشترك الخاص بخادم الإدارة. في حالة تعيين المهمة إلى عدد كبير من الأجهزة، فمن المفيد تحديد موقع المجلد المشترك على مورد ملف مخصص.

تثبيت صور أنظمة التشغيل

يتم تثبيت صور أنظمة التشغيل دائمًا من خلال المجلد المشترك: تقرأ الأجهزة صور أنظمة التشغيل من هذا المجلد. في حالة التخطيط لنشر الصور على عدد كبير من أجهزة الشركة، فمن المفيد تحديد موقع المجلد المشترك على مورد ملف مخصص.

تحديد عنوان خادم الإدارة

عند تثبيت خادم الإدارة، يمكنك تحديد عنوان خادم الإدارة. سيتم استخدام هذا العنوان كعنوان افتراضي عند إنشاء حزمة التثبيت الخاصة بعميل الشبكة.

بصفتك عنوان خادم الإدارة، يمكنك تحديد ما يلي:

- اسم NetBIOS لخادم الإدارة المحدد افتراضيًا
- اسم المجال المؤهل بالكامل (FQDN) لخادم الإدارة إذا تم تكوين نظام اسم المجال (DNS) على شبكة المؤسسة ويعمل بشكل صحيح
- العنوان الخارجي إذا تم تثبيت خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ).

وبعد ذلك، سيكون بإمكانك تغيير عنوان خادم الإدارة باستخدام أدوات وحدة تحكم الإدارة، ولن يتغير العنوان تلقائيًا في حزم تثبيت عميل الشبكة التي تم إنشاؤها بالفعل.

التثبيت القياسي

التثبيت القياسي هو تثبيت خادم الإدارة الذي يستخدم المسارات الافتراضية لملفات التطبيق والذي يعمل على تثبيت مجموعة المكونات الإضافية الافتراضية ولا يقوم بتمكين إدارة جهاز المحمول.

لتثبيت خادم إدارة Kaspersky Security Center على جهاز محلي:

تشغيل الملف التنفيذي ksc_<رقم الإصدار>_full_<لغة الترجمة>.exe.

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط **تثبيت خادم إدارة Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

الخطوة 1. مراجعة اتفاقية الترخيص وسياسة الخصوصية

عند هذه المرحلة من معالج الإعداد، يجب قراءة اتفاقية الترخيص المبرمة بينك وبين Kaspersky، بالإضافة إلى سياسة الخصوصية.

قد تتم مطالبتك أيضًا بعرض اتفاقيات الترخيص وسياسات الخصوصية لمكونات إدارة التطبيق الإضافية المتوفرة في حزمة توزيع Kaspersky Security Center.

يُرجى قراءة اتفاقية الترخيص وسياسة الخصوصية بعناية. إذا كنت توافق على جميع شروط اتفاقية الترخيص وسياسة الخصوصية، أكد ذلك عن طريق تحديد خانات الاختيار المناسبة.

سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من خانتي الاختيار.

في حالة عدم قبولك لاتفاقية الترخيص أو سياسة الخصوصية، قم بإلغاء عملية التثبيت عن طريق النقر فوق الزر **إلغاء**.

الخطوة 2. تحديد طريقة التثبيت

في نافذة تحديد نوع التثبيت، حدد **قياسي**.

من المستحسن إجراء التثبيت القياسي إذا كنت ترغب في تجربة Kaspersky Security Center، على سبيل المثال، عن طريق اختبار تشغيله في منطقة صغيرة ضمن شبكة مؤسستك. أثناء التثبيت القياسي، تقوم فقط بتكوين قاعدة البيانات. لا تقوم بتحديد أي من إعدادات خادم الإدارة: يتم استخدام القيم الافتراضية الخاصة بها بدلاً منها. لا يسمح لك التثبيت القياسي بتحديد مكونات الإدارة الإضافية للتثبيت؛ ويتم تثبيت مجموعة المكونات الإضافية الافتراضية فقط. أثناء التثبيت القياسي، لا يتم إنشاء حزم تثبيت للأجهزة المحمولة. ولكن، يمكنك إنشائها بعد ذلك في وحدة تحكم الإدارة.

الخطوة 3. تثبيت Kaspersky Security Center Web Console

يتم عرض هذه الخطوة فقط إذا كنت تستخدم نظام تشغيل 64 بت. وخلافًا لذلك، لا يتم عرض هذه الخطوة، لأن Kaspersky Security Center Web Console لا يعمل مع أنظمة تشغيل 32 بت.

بشكل افتراضي، سيتم تثبيت كل من both Kaspersky Security Center Web ووحدة تحكم الإدارة المستندة إلى MMC.

إذا كنت ترغب في تثبيت Kaspersky Security Center Web Console فقط:

1. حدد **تثبيت وحدة التحكم هذه فقط**.
2. اختر **وحدة تحكم مستندة إلى الويب** من القائمة المنسدلة.

تثبيت Kaspersky Security Center Web Console يبدأ آليًا بعد إكمال تثبيت خادم الإدارة.

إذا كنت ترغب في تثبيت وحدة تحكم الإدارة المستندة إلى MMC فقط:

1. حدد **تثبيت وحدة التحكم هذه فقط**.
2. اختر **وحدة تحكم مستندة إلى MMC** من القائمة المنسدلة.

الخطوة 4. اختيار حجم الشبكة

حدد حجم الشبكة التي سيتم تثبيت Kaspersky Security Center عليها. بناءً على عدد الأجهزة الموجودة على الشبكة، يقوم المعالج بتكوين التثبيت ومظهر واجهة التطبيق بحيث يتطابقوا.

يسرد الجدول التالي إعدادات تثبيت التطبيق وإعدادات مظهر الواجهة التي تم ضبطها بناءً على أحجام الشبكة المختلفة.

اعتمادًا على إعدادات التثبيت الموجودة على مقياس الشبكة المحدد

الإعدادات	1—100 جهاز مُدار	101—1000 جهاز مُدار	1001—5000 جهاز مُدار	أكثر من 5000 جهاز مُدار
عرض مع عقدة خوادم الإدارة الثانوية والظاهرية وجميع الإعدادات المتعلقة بخوادم الإدارة الثانوية والظاهرية في شجرة وحدة التحكم (متاح فقط في وحدة تحكم الإدارة المستندة إلى MMC)	غير متاح	غير متاح	متاح	متاح
عرض مع أقسام **الأمان** في نوافذ خصائص خادم الإدارة ومجموعات الإدارة (متاح فقط في وحدة تحكم الإدارة المستندة إلى MMC)	غير متاح	غير متاح	متاح	متاح
التوزيع العشوائي لوقت بدء التشغيل لمهمة التحديث على الأجهزة العميلة	غير متاح	على مدى فاصل مدته 5 دقائق	على مدى فاصل مدته 10 دقائق	على مدى فاصل مدته 10 دقائق

إذا قمت بتوصيل خادم الإدارة بخادم قاعدة بيانات MySQL 5.7 أو SQL Express، فلا يوصى باستخدام التطبيق لإدارة أكثر من 10 000 جهاز. بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20 000 جهاز.

الخطوة 5. تحديد قاعدة البيانات

في هذه الخطوة من المعالج، حدد أحد أنظمة إدارة قواعد البيانات (DBMS) التالية التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة:

- **خادم Microsoft SQL أو SQL Server Express**
- **MySQL أو MariaDB**
- **PostgreSQL أو Postgres Pro**

يوصى بتثبيت خادم الإدارة على خادم مخصص بدلاً من وحدة التحكم بالمجال. ومع ذلك، إذا قمت بتثبيت Kaspersky Security Center على خادم يعمل كوحدة تحكم بالمجال للقراءة فقط (RODC)، فلا يجب حينها تثبيت Microsoft SQL Server (SQL Express) محليًا (على نفس الجهاز). في هذه الحالة، نوصي بتثبيت Microsoft SQL Server (SQL Express) عن بُعد (على جهاز آخر)، أو استخدام MySQL أو MariaDB، إذا كنت بحاجة إلى تثبيت DBMS محليًا.

يتم توفير بنية قاعدة بيانات خادم الإدارة في الملف klakdb.chm، الموجود في مجلد تثبيت Kaspersky Security Center. يتوفر هذا الملف أيضًا في أرشيف يوجد على بوابة Kaspersky: klakdb.zip.

الخطوة 6. تكوين خادم SQL Server

في هذه الخطوة من المعالج، حدد إعدادات الاتصال التالية، اعتمادًا على نظام إدارة قاعدة البيانات (DBMS) الذي حددته:

- إذا اخترت **خادم Microsoft SQL أو SQL Server Express** في الخطوة السابقة:

- في الحقل **اسم مثيل خادم SQL Server**، حدد اسم خادم SQL Server على الشبكة. لعرض قائمة بجميع خوادم SQL Server الموجودة على الشبكة، انقر فوق الزر **استعراض**. هذا الحقل فارغ بصورة افتراضية.

  إذا قمت بالاتصال بخادم SQL Server عبر منفذ مخصص، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصولاً بفاصلة، على سبيل المثال:

  ```
  1433,SQL_Server_host_name
  ```

  إذا قمت بتأمين الاتصال بين خادم الإدارة و SQL Server عن طريق شهادة، فحدد في حقل **اسم مثيل خادم SQL Server** نفس اسم المضيف الذي تم استخدامه في إنشاء الشهادة. إذا كنت تستخدم مثيلًا مسمًا من SQL Server، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصولاً بفاصلة، على سبيل المثال:

  ```
  1433,SQL_Server_name
  ```

  إذا كنت تستخدم العديد من مثيلات خادم SQL Server على نفس المضيف، فحدد أيضًا اسم المثيل مفصولاً بشرطة مائلة للخلف، على سبيل المثال:

  ```
  1433,SQL_Server_instance_name\SQL_Server_name
  ```

  إذا تم تمكين ميزة "التشغيل الدائم" في خادم SQL على شبكة المؤسسة، فحدد اسم مستمع مجموعة الإتاحة في حقل **اسم مثيل خادم SQL Server**. يرجى العلم أن خادم الإدارة يدعم فقط وضع توفر الالتزام المتزامن عند تمكين ميزة "التشغيل الدائم".

- في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

في هذه المرحلة، إذا كنت ترغب في تثبيت خادم SQL Server على الجهاز الذي تقوم بتشغيل تثبيت Kaspersky Security Center من خلاله، فيجب عليك إيقاف التثبيت وإعادة تشغيله بعد تثبيت خادم SQL Server. تم إدراج إصدارات خادم SQL المدعومة في متطلبات النظام.

إذا كنت ترغب في تثبيت خادم SQL Server على جهاز بعيد، فلا توجد حاجة لمقاطعة معالج إعداد Kaspersky Security Center. قم بتثبيت خادم SQL Server واستئناف تثبيت Kaspersky Security Center.

- إذا حددت **MySQL** أو **MariaDB** في الخطوة السابقة:

- في الحقل **اسم مثيل خادم SQL Server**، حدد اسم مثيل نظام إدارة قاعدة البيانات. بشكل افتراضي، يكون الاسم هو عنوان IP الخاص بالجهاز الذي سيتم تثبيت Kaspersky Security Center عليه.

- في الحقل **المنفذ**، حدد المنفذ الخاص باتصال خادم الإدارة بنظام إدارة قاعدة البيانات. رقم المنفذ الافتراضي هو 3306.

- في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

- إذا حددت **PostgreSQL** أو **Postgres Pro** في الخطوة السابقة:

- في الحقل **خادم PostgreSQL** أو **Postgres Pro**، حدد اسم مثيل نظام إدارة قاعدة البيانات. بشكل افتراضي، يكون الاسم هو عنوان IP الخاص بالجهاز الذي سيتم تثبيت Kaspersky Security Center عليه.

- في الحقل **المنفذ**، حدد المنفذ الخاص باتصال خادم الإدارة بنظام إدارة قاعدة البيانات. رقم المنفذ الافتراضي هو 5432.

- في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

الخطوة 7. تحديد وضع مصادقة

حدد وضع المصادقة الذي سيتم استخدامه عند اتصال خادم الإدارة بنظام إدارة قواعد البيانات (DBMS).

بناءً على نظام إدارة قاعدة البيانات المحدد، يمكنك الاختيار من بين أوضاع المصادقة التالية:

- لـ SQL Express أو خادم Microsoft SQL Server، حدد أي من الخيارات التالية:

- **وضع مصادقة Microsoft Windows**. التحقق من حقوق استخدام الحساب المستخدم لبدء تشغيل خادم الإدارة.

- **وضع مصادقة خادم SQL**. في حالة تحديد هذا الخيار، سيتم استخدام الحساب المحدد في النافذة للتحقق من حقوق الوصول. املأ حقلي **الحساب** و**كلمة المرور**.

  لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار**.

بالنسبة لوضعي المصادقة، يتحقق التطبيق مما إذا كانت قاعدة البيانات متوفرة. إذا لم تكن قاعدة البيانات متوفرة، تظهر رسالة خطأ ويتوجب عليك إدخال بيانات اعتماد صحيحة.

إذا كانت قاعدة بيانات خادم الإدارة مخزنة على جهاز آخر وحساب خادم الإدارة لا يملك الوصول إلى خادم قاعدة البيانات، فعليك استخدام وضع مصادقة خادم SQL عند تثبيت أو ترقية خادم الإدارة. قد يحدث هذا عندما يكون الجهاز الذي يقوم بتخزين قاعدة البيانات خارج المجال أو عندما يتم تثبيت خادم الإدارة بموجب حساب النظام المحلي.

- بالنسبة إلى MySQL أو MariaDB أو PostgreSQL أو Postgres Pro، حدد الحساب وكلمة المرور.

الخطوة 8. فك وتثبيت الملفات على القرص الثابت

بعد تكوين تثبيت مكونات Kaspersky Security Center، يمكنك بدء تثبيت الملفات على محرك الأقراص الثابتة.

إذا كان التثبيت يتطلب وجود برامج إضافية، فسيقوم معالج الإعداد بإخطارك، في صفحة **متطلبات التثبيت الأساسية**، قبل بدء تثبيت Kaspersky Security Center. سيتم تثبيت البرامج المطلوبة تلقائيًا بعد النقر فوق الزر **التالي**.

في الصفحة الأخيرة، يمكنك تحديد وحدة تحكم لبدء العمل مع Kaspersky Security Center:

- **بدء وحدة تحكم الإدارة القائمة على MMC**
- **تثبيت Kaspersky Security Center Web Console**

يكون هذا الخيار متاحًا فقط في حالة اختيارك لتثبيت Kaspersky Security Center Web Console في إحدى الخطوات السابقة.

يمكنك أيضًا النقر فوق **إنهاء** لإغلاق المعالج دون بدء العمل مع Kaspersky Security Center. يمكنك بدء العمل لاحقًا في أي وقت.

عند بدء التشغيل الأول لوحدة تحكم الإدارة أو Kaspersky Security Center Web Console، يمكنك القيام بـ الإعداد الأولي للتطبيق.

عند انتهاء معالج الإعداد، يتم تثبيت مكونات التطبيق التالية على القرص الثابت الذي تم تثبيت نظام التشغيل عليه:

- خادم الإدارة (مع إصدار خادم عميل الشبكة)
- وحدة تحكم الإدارة التي تعمل على Microsoft Management Console
- Kaspersky Security Center Web Console (في حال اخترت تثبيته)
- تتوفر مكونات الإدارة الإضافية للتطبيق في مجموعة التوزيع

إضافة إلى ذلك، سيتم تثبيت Microsoft Windows Installer 4.5 ما لم يتم تثبيته سابقًا.

التثبيت المخصص

التثبيت المخصص هو تثبيت لخادم الإدارة تتم مطالبتك من خلاله بتحديد المكونات المراد تثبيتها وتحديد المجلد الذي يجب تثبيت التطبيق فيه.

باستخدام هذا النوع من التثبيت، يمكنك تكوين قاعدة البيانات وخادم الإدارة، بالإضافة إلى تثبيت مكونات غير مُضمنة في التثبيت القياسي أو مكونات الإدارة الإضافية لتطبيقات الأمان المختلفة من Kaspersky. يمكنك أيضًا تمكين إدارة جهاز المحمول.

لتثبيت خادم إدارة Kaspersky Security Center على جهاز محلي:

تشغيل الملف التنفيذي ksc_<رقم الإصدار>_full_<لغة الترجمة>.exe.

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط **تثبيت خادم إدارة Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

الخطوة 1. مراجعة اتفاقية الترخيص وسياسة الخصوصية

عند هذه المرحلة من معالج الإعداد، يجب قراءة اتفاقية الترخيص المبرمة بينك وبين Kaspersky، بالإضافة إلى سياسة الخصوصية.

قد تتم مطالبتك أيضًا بعرض اتفاقيات الترخيص وسياسات الخصوصية لمكونات إدارة التطبيق الإضافية المتوفرة في حزمة توزيع Kaspersky Security Center.

يُرجى قراءة اتفاقية الترخيص وسياسة الخصوصية بعناية. إذا كنت توافق على جميع شروط اتفاقية الترخيص وسياسة الخصوصية، أكد ذلك عن طريق تحديد خانات الاختيار المناسبة.

سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من خانتي الاختيار.

في حالة عدم قبولك لاتفاقية الترخيص أو سياسة الخصوصية، قم بإلغاء عملية التثبيت عن طريق النقر فوق الزر **إلغاء**.

الخطوة 2. تحديد طريقة التثبيت

في نافذة تحديد نوع التثبيت، حدد **مخصص**.

يتيح لك التثبيت المخصص تعديل إعدادات Kaspersky Security Center، مثل المسار إلى المجلد المشترك والحسابات ومنافذ الاتصال بخادم الإدارة وإعدادات قاعدة البيانات. يمكّنك التثبيت المخصص من تحديد مكونات الإدارة الإضافية لـ Kaspersky المُراد تثبيتها. أثناء التثبيت المخصص، يمكنك إنشاء حزم تثبيت للأجهزة المحمولة عن طريق تمكين الخيار المطابق.

الخطوة 3. تحديد المكونات المراد تثبيتها

حدد مكونات خادم إدارة Kaspersky Security Center التي ترغب في تثبيتها:

- **إدارة جهاز المحمول** حدد خانة الاختيار هذه إذا كان يجب عليك إنشاء حزم تثبيت للأجهزة المحمولة عندما يتم تشغيل معالج إعداد Kaspersky Security Center. يمكنك أيضًا إنشاء حزم تثبيت للأجهزة المحمولة يدويًا، بعد تثبيت خادم الإدارة، باستخدام أدوات وحدة تحكم الإدارة.
- **وكيل SNMP**. يتلقى هذا المكون معلومات إحصائية لخادم الإدارة عبر بروتوكول SNMP. يتوفر المكون في حالة تثبيت التطبيق على جهاز مثبت عليه SNMP.

> بعد تثبيت Kaspersky Security Center، سيتم وضع ملفات .mib المطلوبة لتلقي البيانات الإحصائية في المجلد الفرعي SNMP من مجلد تثبيت التطبيق.

لن يتم عرض عميل الشبكة ووحدة تحكم الإدارة في قائمة المكونات. يتم تثبيت هذه المكونات تلقائيًا، ولا يمكنك إلغاء تثبيتهما.

عند هذه الخطوة، يجب أن تحدد مجلدًا لتثبيت مكونات خادم الإدارة. بشكل افتراضي، يتم تثبيت المكونات على <Disk>:\Program Files\Kaspersky\Lab\Kaspersky Security Center. في حالة عدم وجود مثل هذا المجلد، يتم إنشاء هذا المجلد تلقائيًا أثناء التثبيت. يمكنك تغيير المجلد الوجهة باستخدام الزر **استعراض**.

الخطوة 4. تثبيت Kaspersky Security Center Web Console

> يتم عرض هذه الخطوة فقط إذا كنت تستخدم نظام تشغيل 64 بت. وخلافًا لذلك، لا يتم عرض هذه الخطوة، لأن Kaspersky Security Center Web Console لا يعمل مع أنظمة تشغيل 32 بت.

بشكل افتراضي، سيتم تثبيت كل من both Kaspersky Security Center Web ووحدة تحكم الإدارة المستندة إلى MMC.

إذا كنت ترغب في تثبيت Kaspersky Security Center Web Console فقط:

1. حدد **تثبيت وحدة التحكم هذه فقط**.
2. اختر **وحدة تحكم مستندة إلى الويب** من القائمة المنسدلة.

> تثبيت Kaspersky Security Center Web Console يبدأ آليًا بعد إكمال تثبيت خادم الإدارة.

إذا كنت ترغب في تثبيت وحدة تحكم الإدارة المستندة إلى MMC فقط:

1. حدد **تثبيت وحدة التحكم هذه فقط**.

2. اختر **وحدة تحكم مستندة إلى MMC** من القائمة المنسدلة.

الخطوة 5. اختيار حجم الشبكة

حدد حجم الشبكة التي سيتم تثبيت Kaspersky Security Center عليها. بناءً على عدد الأجهزة الموجودة على الشبكة، يقوم المعالج بتكوين التثبيت ومظهر واجهة التطبيق بحيث يتطابقوا.

يسرد الجدول التالي إعدادات تثبيت التطبيق وإعدادات مظهر الواجهة التي تم ضبطها بناءً على أحجام الشبكة المختلفة.

اعتمادًا على إعدادات التثبيت الموجودة على مقياس الشبكة المحدد

الإعدادات	1—100 جهاز مُدار	101—1000 جهاز مُدار	1001—5000 جهاز مُدار	أكثر من 5000 جهاز مُدار
عرض مع عقدة خوادم الإدارة الثانوية والظاهرية وجميع الإعدادات المتعلقة بخوادم الإدارة الثانوية والظاهرية في شجرة وحدة التحكم (متاح فقط في وحدة تحكم الإدارة المستندة إلى MMC)	غير متاح	غير متاح	متاح	متاح
عرض مع أقسام **الأمان** في نوافذ خصائص خادم الإدارة ومجموعات الإدارة (متاح فقط في وحدة تحكم الإدارة المستندة إلى MMC)	غير متاح	غير متاح	متاح	متاح
التوزيع العشوائي لوقت بدء التشغيل لمهمة التحديث على الأجهزة العميلة	غير متاح	على مدى فاصل مدته 5 دقائق	على مدى فاصل مدته 10 دقائق	على مدى فاصل مدته 10 دقائق

إذا قمت بتوصيل خادم الإدارة بخادم قاعدة بيانات MySQL 5.7 أوSQL Express، فلا يوصى باستخدام التطبيق لإدارة أكثر من 10 000 جهاز.
بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20 000 جهاز.

الخطوة 6. تحديد قاعدة البيانات

في هذه الخطوة من المعالج، حدد أحد أنظمة إدارة قواعد البيانات (DBMS) التالية التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة:

- **خادم Microsoft SQL أو SQL Server Express**
- **MySQL أو MariaDB**
- **PostgreSQL أو Postgres Pro**

يوصى بتثبيت خادم الإدارة على خادم مخصص بدلاً من وحدة التحكم بالمجال. ومع ذلك، إذا قمت بتثبيت Kaspersky Security Center على خادم يعمل كوحدة تحكم بالمجال للقراءة فقط (RODC)، فلا يجب حينها تثبيت Microsoft SQL Server (SQL Express) محليًا (على نفس الجهاز). في هذه الحالة، نوصي بتثبيت Microsoft SQL Server (SQL Express) عن بُعد (على جهاز آخر)، أو استخدام MySQL أو MariaDB، إذا كنت بحاجة إلى تثبيت DBMS محليًا.

يتم توفير بنية قاعدة بيانات خادم الإدارة في الملف klakdb.chm، الموجود في مجلد تثبيت Kaspersky Security Center. يتوفر هذا الملف أيضًا في أرشيف يوجد على بوابة Kaspersky: klakdb.zip.

الخطوة 7. تكوين خادم SQL Server

في هذه الخطوة من المعالج، حدد إعدادات الاتصال التالية، اعتمادًا على نظام إدارة قاعدة البيانات (DBMS) الذي حددته:

- إذا اخترت **خادم Microsoft SQL** أو **SQL Server Express** في الخطوة السابقة:

  - في الحقل **اسم مثيل خادم SQL Server**، حدد اسم خادم SQL Server على الشبكة. لعرض قائمة بجميع خوادم SQL Server الموجودة على الشبكة، انقر فوق الزر **استعراض**. هذا الحقل فارغ بصورة افتراضية.

    إذا قمت بالاتصال بخادم SQL Server عبر منفذ مخصص، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصولاً بفاصلة، على سبيل المثال:

    `1433,SQL_Server_host_name`

    إذا قمت بتأمين الاتصال بين خادم الإدارة و SQL Server عن طريق شهادة، فحدد في حقل **اسم مثيل خادم SQL Server** نفس اسم المضيف الذي تم استخدامه في إنشاء الشهادة. إذا كنت تستخدم مثيلًا مسمًا من SQL Server، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصولاً بفاصلة، على سبيل المثال:

    `1433,SQL_Server_name`

    إذا كنت تستخدم العديد من مثيلات خادم SQL Server على نفس المضيف، فحدد أيضًا اسم المثيل مفصولاً بشرطة مائلة للخلف، على سبيل المثال:

    `1433,SQL_Server_instance_name\SQL_Server_name`

    إذا تم تمكين ميزة "التشغيل الدائم" في خادم SQL على شبكة المؤسسة، فحدد اسم مستمع مجموعة الإتاحة في حقل **اسم مثيل خادم SQL Server**. يرجى العلم أن خادم الإدارة يدعم فقط وضع توفر الالتزام المتزامن عند تمكين ميزة "التشغيل الدائم".

  - في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

  في هذه المرحلة، إذا كنت ترغب في تثبيت خادم SQL Server على الجهاز الذي تقوم بتشغيل تثبيت Kaspersky Security Center من خلاله، فيجب عليك إيقاف التثبيت وإعادة تشغيله بعد تثبيت خادم SQL Server. تم إدراج إصدارات خادم SQL المدعومة في متطلبات النظام.

  إذا كنت ترغب في تثبيت خادم SQL Server على جهاز بعيد، فلا توجد حاجة لمقاطعة معالج إعداد Kaspersky Security Center. قم بتثبيت خادم SQL Server واستئناف تثبيت Kaspersky Security Center.

- إذا حددت **MySQL** أو **MariaDB** في الخطوة السابقة:

  - في الحقل **اسم مثيل خادم SQL Server**، حدد اسم مثيل نظام إدارة قاعدة البيانات. بشكل افتراضي، يكون الاسم هو عنوان IP الخاص بالجهاز الذي سيتم تثبيت Kaspersky Security Center عليه.

  - في الحقل **المنفذ**، حدد المنفذ الخاص باتصال خادم الإدارة بنظام إدارة قاعدة البيانات. رقم المنفذ الافتراضي هو 3306.

  - في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

- إذا حددت **PostgreSQL** أو **Postgres Pro** في الخطوة السابقة:

  - في الحقل **خادم PostgreSQL** أو **Postgres Pro**، حدد اسم مثيل نظام إدارة قاعدة البيانات. بشكل افتراضي، يكون الاسم هو عنوان IP الخاص بالجهاز الذي سيتم تثبيت Kaspersky Security Center عليه.

  - في الحقل **المنفذ**، حدد المنفذ الخاص باتصال خادم الإدارة بنظام إدارة قاعدة البيانات. رقم المنفذ الافتراضي هو 5432.

  - في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

الخطوة 8. تحديد وضع مصادقة

حدد وضع المصادقة الذي سيتم استخدامه عند اتصال خادم الإدارة بنظام إدارة قواعد البيانات (DBMS).

بناءً على نظام إدارة قاعدة البيانات المحدد، يمكنك الاختيار من بين أوضاع المصادقة التالية:

- لـ SQL Express أو خادم Microsoft SQL Server، حدد أي من الخيارات التالية:
  - **وضع مصادقة Microsoft Windows**. التحقق من حقوق استخدام الحساب المستخدم لبدء تشغيل خادم الإدارة.
  - **وضع مصادقة خادم SQL**. في حالة تحديد هذا الخيار، سيتم استخدام الحساب المحدد في النافذة للتحقق من حقوق الوصول. املأ حقلي **الحساب** و**كلمة المرور**.

    لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار**.

بالنسبة لوضعي المصادقة، يتحقق التطبيق مما إذا كانت قاعدة البيانات متوفرة. إذا لم تكن قاعدة البيانات متوفرة، تظهر رسالة خطأ ويتوجب عليك إدخال بيانات اعتماد صحيحة.

إذا كانت قاعدة بيانات خادم الإدارة مخزنة على جهاز آخر وحساب خادم الإدارة لا يملك الوصول إلى خادم قاعدة البيانات، فعليك استخدام وضع مصادقة خادم SQL عند تثبيت أو ترقية خادم الإدارة. قد يحدث هذا عندما يكون الجهاز الذي يقوم بتخزين قاعدة البيانات خارج المجال أو عندما يتم تثبيت خادم الإدارة بموجب حساب النظام المحلي.

- بالنسبة إلى MySQL أو MariaDB أو PostgreSQL أو Postgres Pro، حدد الحساب وكلمة المرور.

الخطوة 9. تحديد الحساب لتشغيل خادم الإدارة

حدد الحساب الذي سيتم استخدامه لبدء خادم الإدارة كخدمة.

- **إنشاء الحساب تلقائيًا**. ينشئ التطبيق حسابًا باسم KL-AK-*، الذي سيتم من خلاله تشغيل خدمة kladminserver.

  يمكنك تحديد هذا الخيار إن كانت خطتك هي تحديد موقع المجلد المشترك ونظام إدارة قواعد البيانات على الجهاز نفسه مثل خادم الإدارة.

- **تحديد حساب**. ستعمل خدمة خادم الإدارة (kladminserver) بموجب الحساب الذي حددته.

  سيتعين عليك تحديد حساب مجال، على سبيل المثال إن كنت تخطط لاستخدام مثيل خادم SQL Server من أي إصدار كـ DBMS، بما في ذلك SQL Express الموجود على جهاز آخر و/أو كنت تخطط لتحديد موقع المجلد المشترك على جهاز آخر.

  يدعم Kaspersky Security Center حسابات الخدمة (MSA) المُدارة وحسابات الخدمة المُدارة الجماعية (gMSA). في حالة استخدام أنواع الحسابات هذه في مجالك، فيمكنك تحديد واحد منها كحساب لخدمة خادم الإدارة.

  قبل تحديد MSA أو gMSA، يجب تثبيت الحساب على نفس الجهاز الذي تريد تثبيت خادم الإدارة عليه. إذا لم يتم تثبيت الحساب بعد، فقم بإلغاء تثبيت خادم الإدارة وتثبيت الحساب، ثم أعد تشغيل تثبيت خادم الإدارة. للحصول على تفاصيل حول تثبيت حسابات الخدمة المُدارة على جهاز محلي، راجع وثائق Microsoft الرسمية.

  لتحديد MSA أو gMSA:

  1. انقر فوق الزر **استعراض**.
  2. في النافذة التي تظهر، انقر فوق الزر **أنواع الكائنات**.
  3. حدد النوع **حساب للخدمات** وانقر فوق **موافق**.
  4. حدد الحساب ذي الصلة وانقر فوق **موافق**.

  يجب أن يحتوي الحساب الذي حددته على أذونات مختلفة، بناءً على نظام إدارة قواعد البيانات الذي تخطط لاستخدامه.

لأسباب أمنية، يُرجى عدم تعيين الحالة المميزة لحساب يعمل خادم الإدارة بموجبه.

لا يمكن تغيير حساب خادم الإدارة لاحقًا. يتعين عليك إعادة تثبيت مجموعة تجاوز الفشل لاستخدام حساب خادم إدارة آخر.

الخطوة 10. تحديد الحساب لتشغيل خدمات Kaspersky Security Center

حدد الحساب الذي سيتم تشغيل خدمات Kaspersky Security Center فيه على هذا الجهاز.

- **إنشاء الحساب تلقائيًا**. يقوم Kaspersky Security Center بإنشاء حساب محلي يُسمى KlScSvc على هذا الجهاز الموجود في مجموعة kladmins. سيتم تشغيل خدمات Kaspersky Security Center تحت الحساب الذي تم إنشاؤه.
- **تحديد حساب**. ستعمل خدمات Kaspersky Security Center بموجب الحساب الذي حددته.

سيتعين عليك تحديد حساب المجال إذا، على سبيل المثال، كنت تنوي حفظ التقارير في مجلد موجود على جهاز مختلف أو إذا كان الأمر مطلوبًا من قِبل سياسة أمان المؤسسة الخاصة بك. كما قد يتعين عليك تحديد حساب مجال عند تثبيت خادم الإدارة على مجموعة تجاوز الفشل.

لأسباب أمنية، لا تمنح حالة مميزة للحساب الذي يتم تشغيل الخدمات بموجبه.

سيتم تشغيل خدمة الوكيل لـ KSN (ksnproxy) وخدمة الوكيل لتنشيط Kaspersky (klactprx) وخدمة بوابة مصادقة Kaspersky (klwebsrv) ضمن الحساب المحدد.

الخطوة 11. تحديد مجلد مشترك

حدد موقع واسم المجلد المشترك الذي سيتم استخدامه لتنفيذ ما يلي:

- تخزين الملفات الضرورية لتثبيت التطبيقات عن بُعد (يتم نسخ الملفات إلى خادم الإدارة أثناء إنشاء حزم التثبيت).
- تخزين التحديثات التي تم تزيلها من مصدر محدث إلى خادم الإدارة.

سيتم تمكين مشاركة الملفات (للقراءة فقط) لجميع المستخدمين.

يمكنك تحديد أي من الخيارين التاليين:

- **إنشاء مجلد مشترك**. قم بإنشاء مجلد جديد. في مربع النص، حدد المسار إلى المجلد.
- **تحديد مجلد مشترك موجود**. حدد مجلد مشترك موجود بالفعل.

يمكن أن يكون المجلد المشترك إما مجلدًا محليًا موجودًا على الجهاز المستخدم للتثبيت أو دليلاً بعيدًا موجودًا على أي من الأجهزة العميلة الموجودة على شبكة الشركة. يمكنك النقر فوق الزر **استعراض** لتحديد المجلد المشترك أو تحديده يدويًا عن طريق إدخال مسار UNC الخاص به (على سبيل المثال، \\server\Share) في الحقل المقابل.

بشكل افتراضي، يقوم المثبت بإنشاء مجلد فرعي KLSHARE محلي في مجلد التطبيق يحتوي على مكونات Kaspersky Security Center.

يمكنك تحديد مجلد مشترك لاحقًا إذا لزم الأمر.

الخطوة 12. تكوين الاتصال بخادم الإدارة

قم بتكوين الاتصال بخادم الإدارة.

- **المنفذ**

رقم المنفذ المستخدم للاتصال بخادم الإدارة.

رقم المنفذ الافتراضي هو 14000.

- **منفذ SSL**

رقم منفذ طبقة مآخذ التوصيل الآمنة (SSL) المستخدم للاتصال الآمن بخادم الإدارة عبر SSL.

رقم المنفذ الافتراضي هو 13000.

- **طول مفتاح التشفير**

حدد طول مفتاح التشفير: 1024 بت أو 2048 بت.

يضع مفتاح التشفير 1024-بت حمل أقل على وحدة المعالجة المركزية (CPU)، ولكنه يعتبر قديمًا لأنه لا يمكنه تقديم عملية تشفير موثوق بها نتيجة لمواصفاته الفنية. قد يتبين أيضًا أن الجهاز الحالي غير متوافق مع شهادات SSL التي تقدم مفاتيح 1024-بت.

يتوافق مفتاح التشفير 2048-بت مع أحدث معايير التشفير. ومع ذلك، قد يؤدي استخدام مفتاح التشفير 2048-بت إلى إضافة حمل على وحدة المعالجة المركزية (CPU).

بشكل افتراضي، يتم تحديد **2048 بت (أفضل أمان)**.

يمكنك أيضًا تغيير معلمات الاتصال بخادم الإدارة لاحقًا على النحو التالي:

- يمكنك تغيير المنفذ وأرقام منفذ SSL في القسم **Connection ports** في خصائص خادم الإدارة. وللمزيد من المعلومات عن منافذ اتصال خادم الإدارة، يرجى الرجوع إلى المنافذ المستخدمة بواسطة Kaspersky Security Center.

- يمكنك تغيير طول مفتاح التشفير عند استبدال شهادة خادم الإدارة بالأداة المساعدة klsetsrvcert باستخدام المعلمة `-RsaKeyLen o:<طول المفتاح>`.

الخطوة 13. تعريف عنوان خادم الإدارة

حدد عنوان خادم الإدارة بإحدى الطرق التالية:

- **اسم مجال DNS**. يمكنك استخدام هذه الطريقة إذا كانت الشبكة تتضمن خادم DNS ويمكن لأجهزة العميل استخدامها لتلقي عنوان خادم الإدارة.

- **اسم NetBIOS**. تستخدم هذه الطريقة إذا كانت أجهزة العميل تتلقى عنوان خادم الإدارة باستخدام بروتوكول NetBIOS أو إذا كان خادم WINS متوفرًا على الشبكة.

- **عنوان IP**. يتم استخدام هذا الخيار إذا كان خادم الإدارة لديه عنوان IP ثابت لن يتم تغييره لاحقًا.

إذا قمت بتثبيت Kaspersky Security Center على العقدة المفعلة لمجموعة تجاوز الفشل من Kaspersky Security Center وقمت بإنشاء محول شبكة ثانوي عند إعداد عقد المجموعة، فحدد عنوان IP لهذا المحول. خلاف ذلك، أدخل عنوان IP الخاص بموازنة تحميل الجهة الخارجية التي تستخدمها.

الخطوة 14. عنوان خادم الإدارة للاتصال بالأجهزة المحمولة

تتوفر هذه الخطوة من معالج الإعداد إذا قمت بتحديد إدارة جهاز المحمول للتثبيت.

في نافذة **عنوان الاتصال الأجهزة المحمولة** حدد العنوان الخارجي لخادم الإدارة للاتصال بالأجهزة المحمولة الموجودة خارج الشبكة المحلية. يمكنك تحديد عنوان IP أو نظام اسم النطاق (DNS) لخادم الإدارة.

الخطوة 15. تحديد مكونات الإدارة الإضافية للتطبيق

حدد الأدوات الإضافية الخاصة بإدارة التطبيق التي تحتاج إلى تثبيتها مع Kaspersky Security Center.

لسهولة البحث، تنقسم المكونات الإضافية إلى مجموعات بناءً على نوع الكائنات المؤمنة.

الخطوة 16. فك وتثبيت الملفات على القرص الثابت

بعد تكوين تثبيت مكونات Kaspersky Security Center، يمكنك بدء تثبيت الملفات على محرك الأقراص الثابتة.

إذا كان التثبيت يتطلب وجود برامج إضافية، فسيقوم معالج الإعداد بإخطارك، في صفحة **متطلبات التثبيت الأساسية**، قبل بدء تثبيت Kaspersky Security Center. سيتم تثبيت البرامج المطلوبة تلقائيًا بعد النقر فوق الزر **التالي**.

في الصفحة الأخيرة، يمكنك تحديد وحدة تحكم لبدء العمل مع Kaspersky Security Center:

- **بدء وحدة تحكم الإدارة القائمة على MMC**
- **تثبيت Kaspersky Security Center Web Console**

  يكون هذا الخيار متاحًا فقط في حالة اختيارك لتثبيت Kaspersky Security Center Web Console في إحدى الخطوات السابقة.

يمكنك أيضًا النقر فوق **إنهاء** لإغلاق المعالج دون بدء العمل مع Kaspersky Security Center. يمكنك بدء العمل لاحقًا في أي وقت.

عند بدء التشغيل الأول لوحدة تحكم الإدارة أو Kaspersky Security Center Web Console، يمكنك القيام بـ الإعداد الأولي للتطبيق.

نشر مجموعة تجاوز الفشل في Kaspersky Security Center

يحتوي هذا القسم على معلومات عامة حول مجموعة تجاوز الفشل من Kaspersky Security Center وإرشادات حول إعداد ونشر مجموعة تجاوز الفشل من Kaspersky Security Center في شبكتك.

السيناريو: نشر مجموعة تجاوز الفشل في Kaspersky Security Center

توفر مجموعة تجاوز الفشل من Kaspersky Security Center إتاحةً عالية لحل Kaspersky Security Center وتقلل من وقت تعطل خادم الإدارة في حالة حدوث فشل. تستند مجموعة تجاوز الفشل إلى مثيلين متطابقين من Kaspersky Security Center مثبتين على جهازي كمبيوتر. تعمل إحدى المثيلات كعقدة نشطة والأخرى هي عقدة خاملة. تدير العقدة المفعلة حماية أجهزة العميل، بينما تكون العقدة الخاملة جاهزة لأخذ جميع وظائف العقدة المفعلة في حالة فشل العقدة المفعلة. عند حدوث فشل، تصبح العقدة الخاملة نشطة وتصبح العقدة المفعلة خاملة.

المتطلبات الأساسية

لديك جهاز يلبي المتطلبات لمجموعة تجاوز الفشل.

المراحل

يتقدم نشر تطبيقات Kaspersky في مراحل:

1. **إنشاء حساب لخدمات Kaspersky Security Center**

قم بإنشاء مجموعة مجال جديدة (في هذا السيناريو ، يتم استخدام اسم 'KLAdmins' لهذه المجموعة)، ثم منح أذونات المسؤول المحلي للمجموعة على كل من العقد وعلى خادم الملفات. أنشئ حسابين جديدين لمستخدمي المجال (في هذا السيناريو، يتم استخدام الأسماء 'ksc' و 'rightless' لهذه الحسابات)، وأضف الحسابات إلى مجموعة مجال KLAdmins.

أضف حساب المستخدم، الذي سيتم بموجبه تثبيت Kaspersky Security Center، إلى مجموعة مجال KLAdmins التي تم إنشائها مسبقًا.

2. **إعداد خادم الملفات**

قم بإعداد خادم الملفات للعمل كأحد مكونات مجموعة تجاوز الفشل من Kaspersky Security Center. تأكد من أن خادم الملفات يلبي متطلبات الأجهزة والبرامج، وأنشئ مجلدين مشتركين لبيانات Kaspersky Security Center، وقم بتكوين الأذونات للوصول إلى المجلدات المشتركة.

إرشادات الطريقة: إعداد خادم ملفات لمجموعة تجاوز الفشل من Kaspersky Security Center

3. **إعداد العقد المفعلة والخاملة**

قم بإعداد جهازين بمكونات أجهزة وبرامج متطابقة للعمل كعقدة نشطة وخاملة.

إرشادات الطريقة: تحضير عقد لمجموعة تجاوز الفشل من Kaspersky Security Center

4. **تثبيت نظام إدارة قواعد البيانات (DBMS)**

حدد أيًا من نظام إدارة قاعدة البيانات (DBMS) المدعوم، ثم قم بتثبيت نظام إدارة قاعدة البيانات على جهاز مخصص. للمزيد من المعلومات عن كيفية تثبيت نظام إدارة قاعدة البيانات، يُرجى الرجوع إلى وثائقه.

5. **تثبيت Kaspersky Security Center**

قم بتثبيت Kaspersky Security Center في وضع مجموعة تجاوز الفشل على كلا العقدتين. يجب عليك أولاً تثبيت Kaspersky Security Center على الجهاز الذي تريده أن يكون المضيف النشط، ثم تثبيته على الجهاز الخامل.

يجب عليك تثبيت Kaspersky Security Center Web Console على جهاز منفصل ليس عقدة نظام مجموعة.

إرشادات الطريقة: تثبيت Kaspersky Security Center على عقد مجموعة تجاوز الفشل من Kaspersky Security Center

6. **اختبار مجموعة تجاوز الفشل**

تحقق من تكوين نظام مجموعة تجاوز الفشل بنجاح وأنه يعمل بشكل صحيح. على سبيل المثال، يمكنك إيقاف إحدى خدمات Kaspersky Security Center على العقدة المفعلة: kladminserver أو klnagent أو ksnproxy أو klactprx أو klwebsrv. بعد إيقاف الخدمة، يجب تحويل إدارة الحماية تلقائيًا إلى العقدة الخاملة.

النتائج

تم نشر مجموعة تجاوز الفشل من Kaspersky Security Center. يرجى التعرف على الأحداث التي تؤدي إلى التبديل بين العقد المفعلة والعقد الخاملة.

حول مجموعة تجاوز الفشل من Kaspersky Security Center

توفر مجموعة تجاوز الفشل من Kaspersky Security Center إتاحةً عالية لحل Kaspersky Security Center وتقلل من وقت تعطل خادم الإدارة في حالة حدوث فشل. تستند مجموعة تجاوز الفشل إلى مثيلين متطابقين من Kaspersky Security Center مثبتين على جهازي كمبيوتر. تعمل إحدى المثيلات كعقدة نشطة والأخرى هي عقدة خاملة. تدير العقدة المفعلة حماية أجهزة العميل، بينما تكون العقدة الخاملة جاهزة لأخذ جميع وظائف العقدة المفعلة في حالة فشل العقدة المفعلة. عند حدوث فشل، تصبح العقدة الخاملة نشطة وتصبح العقدة المفعلة خاملة.

لا يؤثر استخدام مجموعة تجاوز الفشل على العمليات الحسابية بناءً على دليل تغيير الحجم.

استخدم ميزة Kaspersky Event Log لاستكشاف المشكلات وإصلاحها.

لا يتم دعم مجموعة تجاوز الفشل الموزعة جغرافيًا في Kaspersky Security Center. لا يمكن نشر مجموعة تجاوز الفشل في Kaspersky Security Center إلا داخل موقع جغرافي واحد.

تبديل الشروط:

تبدل مجموعة تجاوز الفشل إدارة الحماية لأجهزة العميل من العقدة المفعلة إلى العقدة الخاملة في حالة حدوث أي من الأحداث التالية على العقدة المفعلة:

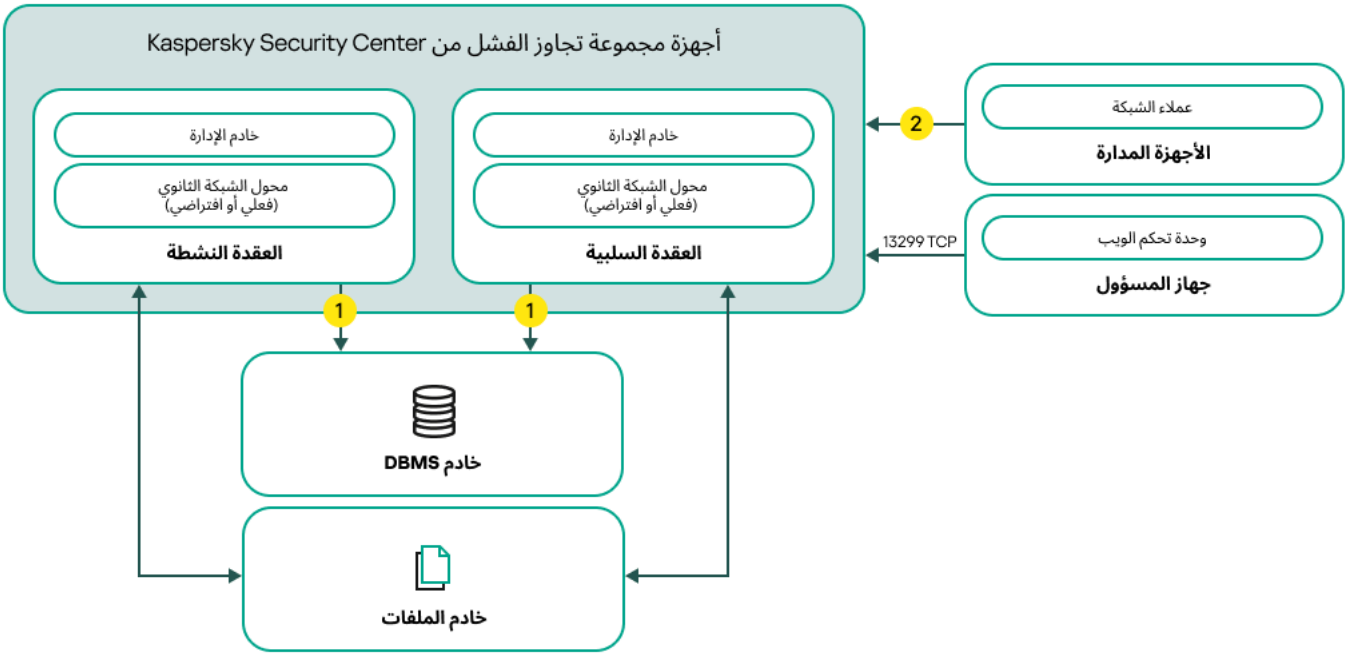
- العقدة المفعلة معطلة بسبب عطل في البرامج أو الأجهزة.
- تم إيقاف العقدة المفعلة مؤقتًا لأنشطة الصيانة.
- فشلت واحدة على الأقل من خدمات (أو عمليات) Kaspersky Security Center أو تم إنهاؤها عمدًا من قِبل المستخدم. خدمات Kaspersky Security Center هي التالية: kladminserver وklnagent وklactprx وklwebsrv.
- تم قطع اتصال الشبكة بين العقدة المفعلة والتخزين على خادم الملفات أو إنهاؤه.

تدير مجموعة تجاوز من الفشل Kaspersky Security Center جميع خدمات Kaspersky Security Center تلقائيًا. ولا تقم بإعادة تشغيل الخدمات يدويًا.

مخططات النشر

يمكنك اختيار أحد المخططات التالية لنشر مجموعة تجاوز الفشل من Kaspersky Security Center :

- مخطط يستخدم محول شبكة ثانوي.
- مخطط يستخدم موازن تحميل من جهة خارجية.

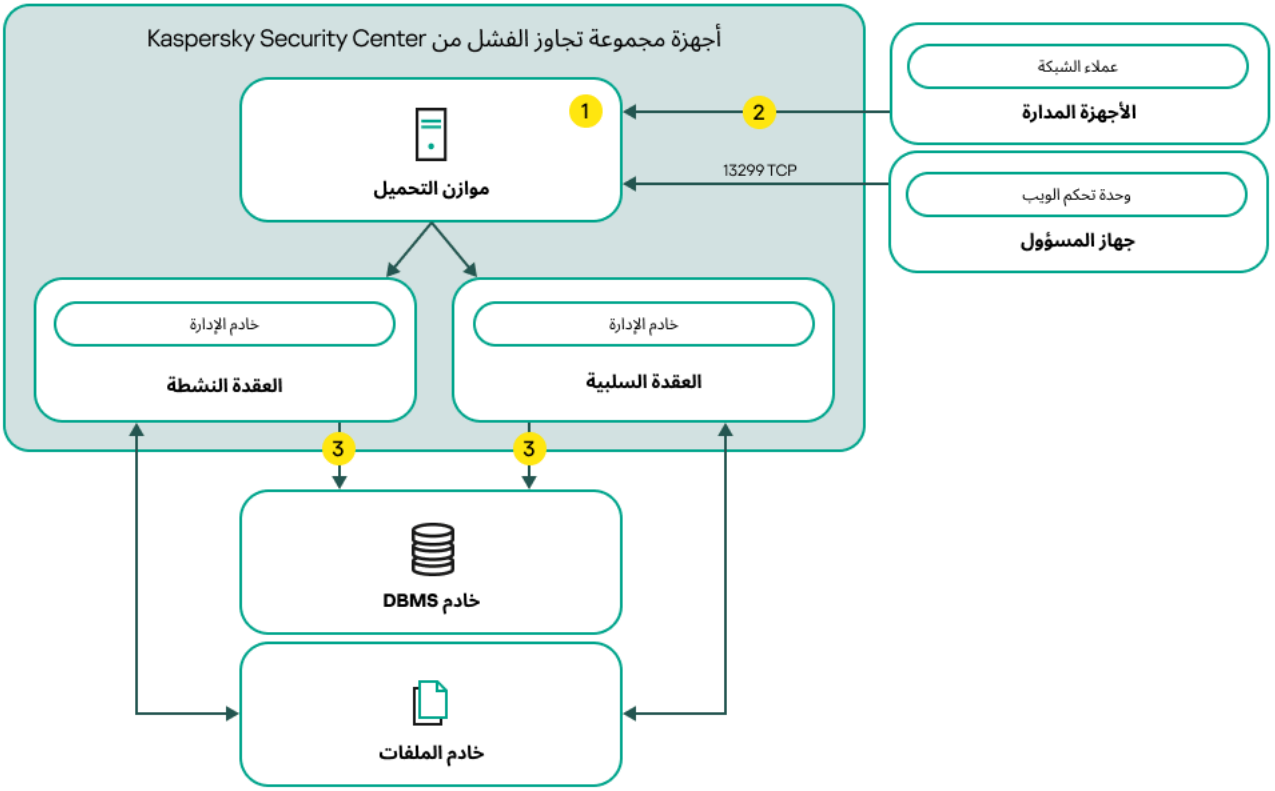


مخطط يستخدم محول شبكة ثانوي

مفتاح المخطط:

1 يُرسل خادم الإدارة البيانات إلى قاعدة البيانات. افتح المنافذ الضرورية على الجهاز حيث توجد قاعدة البيانات، على سبيل المثال، المنفذ 3306 لنظام MySQL Server، أو المنفذ 1433 لنظام Microsoft SQL Server. يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

2 على الأجهزة المدارة، افتح المنافذ التالية: TCP 13000 وUDP 13000 وTCP 17000.



مخطط يستخدم موازن تحميل من جهة خارجية

مفتاح المخطط:

1 على جهاز موازن التحميل، افتح جميع منافذ خادم الإدارة: TCP 13000 وUDP13000 وTCP 13299 وTCP 17000.

إذا كنت تريد استخدام أداة klakaut للأتمتة، فيجب عليك أيضًا فتح منفذ TCP 13291.

2 على الأجهزة المدارة، افتح المنافذ التالية: TCP 13000 وUDP 13000 وTCP 17000.

3 يُرسل خادم الإدارة البيانات إلى قاعدة البيانات. افتح المنافذ الضرورية على الجهاز حيث توجد قاعدة البيانات، على سبيل المثال، المنفذ 3306 لنظام MySQL Server، أو المنفذ 1433 لنظام Microsoft SQL Server. يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

تحضير خادم ملف لمجموعة تجاوز الفشل في Kaspersky Security Center

يعمل خادم الملفات كمكون مطلوب من مجموعة تجاوز الفشل من Kaspersky Security Center.

لتحضير خادم ملفات:

1. تأكد من أن خادم الملفات يلبي متطلبات الأجهزة والبرامج.

2. تأكد من أن خادم الملف وكلا العقدتين (المفعلة والخاملة) مضمنة في نفس المجال أو أن خادم الملفات هو وحدة تحكم المجال.

3. على خادم الملفات، أنشئ مجلدين مشتركين. يتم استخدام أحدها للاحتفاظ بالمعلومات حول حالة مجموعة تجاوز الفشل. يتم استخدام الآخر لتخزين بيانات وإعدادات Kaspersky Security Center. ستحدد مسارات المجلدات المشتركة أثناء تكوين تثبيت Kaspersky Security Center.

4. امنح أذونات الوصول الكامل (أذونات المشاركة وأذونات NTFS) للمجلدات المشتركة التي تم إنشاؤها لحسابات المستخدمين والمجموعات التالية:

- مجموعة مجال KLAdmins.
- حسابات المستخدمين $ <node1> و $ <node2>. هنا، <node1> و<node2> هما أسماء الأجهزة الخاصة بالعقد النشطة والخاملة.

تم إعداد خادم الملفات. لنشر مجموعة تجاوز الفشل Kaspersky Security Center، اتبع الإرشادات الإضافية في هذا السيناريو.

تحضير العقد لنظام مجموعة تجاوز الفشل من Kaspersky Security Center

قم بإعداد جهازين للعمل كعقد نشطة وخاملة لمجموعة تجاوز الفشل من Kaspersky Security Center.

لتحضير عقد لمجموعة تجاوز الفشل من Kaspersky Security Center:

1. تأكد أن الجهازين يلبيان متطلبات الأجهزة والبرامج. وستعمل هذه الأجهزة هذه كعقد نشطة وخاملة لمجموعة تجاوز الفشل.

2. تأكد من أن خادم الملفات وكلا العقدتين (المفعلة والخاملة) مضمنة في نفس المجال أو أن خادم الملفات هو وحدة تحكم المجال.

3. قم بأحد الإجراءات التالية:

- في كل عقدة من العقد، كوّن محول شبكة ثانوي.

ويمكن أن يكون محول الشبكة الثانوي فعليًا أو افتراضيًا. وإذا كنت تريد استخدام محول شبكة فعلي، قم بتوصيله وتكوينه باستخدام أدوات نظام التشغيل القياسية. وإذا كنت تريد استخدام محول شبكة افتراضي، فقم بإنشائه باستخدام برنامج تابع لجهة خارجية.

يرجى التأكد من استيفاء الشروط التالية:

- تم تعطيل محولات الشبكة الثانوية.

يمكنك إنشاء محولات الشبكة الثانوية في حالة التعطيل أو تعطيلها بعد الإنشاء.

- تمتلك محولات الشبكة الثانوية على كلا العقدتين عنوان IP نفسه.

- استخدم موازن تحميل تابع لجهة خارجية. على سبيل المثال، يمكنك استخدام خادم nginx. في هذه الحالة، نفذ ما يلي:

a. قم بتوفير جهاز يعمل بنظام Linux مع تثبيت nginx عليه.

b. قم بتكوين موازن التحميل. قم بتعيين العقدة المفعلة كخادم رئيسي والعقدة الخاملة كخادم النسخ الاحتياطي.

c. على خادم nginx، افتح جميع منافذ خادم الإدارة: TCP 13000 وUDP13000 وTCP 13299 وTCP 17000.

> إذا كنت تريد استخدام أداة klakaut للأتمتة، فيجب عليك أيضًا فتح منفذ TCP 13291.

4. أعد تشغيل كلا العقدتين وخادم الملفات.

5. قم بتعيين المجلدين المشتركين، اللذين قمت بإنشائهما أثناء خطوة إعداد خادم الملفات، لكل عقدة. يجب عليك تعيين المجلدات المشتركة كمحركات أقراص الشبكة. عند تعيين المجلدات، يمكنك تحديد أي أحرف محركات أقراص شاغرة. للوصول إلى المجلدات المشتركة، استخدم بيانات اعتماد حساب المستخدم الذي قمت بإنشائه أثناء الخطوة 1 من السيناريو.

العقد جاهزة. لنشر مجموعة تجاوز الفشل Kaspersky Security Center، اتبع الإرشادات الإضافية الواردة في السيناريو.

تثبيت Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky Security Center

تم تثبيت Kaspersky Security Center على كلا العقدتين في مجموعة تجاوز الفشل من Kaspersky Security Center بشكل منفصل. أولاً، تقوم بتثبيت التطبيق على العقدة المفعلة، ثم على العقدة الخاملة. عند التثبيت، أنت تختار العقدة التي ستكون نشطة والعقدة ستكون خاملة.

يمكن فقط لمستخدم من مجموعة مجالات KLAdmins تثبيت Kaspersky Security Center على كل عقدة.

لتثبيت Kaspersky Security Center على العقدة المفعلة لمجموعة تجاوز الفشل من Kaspersky Security Center:

1. تشغيل الملف التنفيذي exe.<language>_full_<build number>_ksc_15.1

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط **تثبيت خادم إدارة Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

2. يُرجى قراءة اتفاقية الترخيص وسياسة الخصوصية بعناية. في حالة الموافقة على شروط اتفاقية الترخيص وسياسة الخصوصية، حدد خانة الاختيار التالية في قسم **أؤكد على أنني قد قرأت ما يلي واستوعبته جيدًا وأوافق عليه**:

- **شروط وبنود اتفاقية ترخيص المستخدم النهائي (EULA) هذه**
- **تصف سياسة الخصوصية طريقة التعامل مع البيانات**

سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من خانتي الاختيار.

في حالة عدم قبولك لاتفاقية الترخيص أو سياسة الخصوصية، قم بإلغاء عملية التثبيت عن طريق النقر فوق الزر **إلغاء**.

3. حدد **العقدة الأساسية لمجموعة تجاوز الفشل من Kaspersky Security Center** لتثبيت التطبيق على العقدة المفعلة.

4. في نافذة **المجلد المشترك**، نفذ ما يلي:

- في حقل **مشاركة الحالة** وحقل **مشاركة البيانات**، حدد المسارات إلى المجلدات المشتركة التي قمت بإنشائها على خادم الملفات أثناء الإعداد.
- في حقل **محرك أقراص مشاركة الحالة** وحقل **محرك أقراص مشاركة البيانات**، حدد محركات أقراص الشبكة التي قمت بتعيين المجلدات المشتركة إليها أثناء إعداد العقد.
- حدد وضع اتصال المجموعة: عبر محول شبكة ثانوي أو موازن تحميل تابع لجهة خارجية.

5. قم بإجراء خطوات أخرى للتثبيت المخصص، بدءًا من الخطوة 3.

في الخطوة 13، حدد عنوان IP لمحول شبكة ثانوي إذا كنت قد أنشأت محولًا أثناء تحضير عُقد المجموعة. خلاف ذلك، أدخل عنوان IP الخاص بموازنة تحميل الجهة الخارجية التي تستخدمها.

تم تثبيت Kaspersky Security Center على العقدة المفعلة.

لتثبيت Kaspersky Security Center على العقدة الخاملة لمجموعة تجاوز الفشل من Kaspersky Security Center:

1. تشغيل الملف التنفيذي exe.<language>_full_<build number>_ksc_15.1

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط **تثبيت خادم إدارة Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

2. يُرجى قراءة اتفاقية الترخيص وسياسة الخصوصية بعناية. في حالة الموافقة على شروط اتفاقية الترخيص وسياسة الخصوصية، حدد خانة الاختيار التالية في قسم **أؤكد على أنني قد قرأت ما يلي واستوعبته جيدًا وأوافق عليه**:

- **شروط وبنود اتفاقية ترخيص المستخدم النهائي (EULA) هذه**
- **تصف سياسة الخصوصية طريقة التعامل مع البيانات**

سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من خانتي الاختيار.

في حالة عدم قبولك لاتفاقية الترخيص أو سياسة الخصوصية، قم بإلغاء عملية التثبيت عن طريق النقر فوق الزر **إلغاء**.

3. حدد **العقدة الثانوية لمجموعة تجاوز الفشل من Kaspersky Security Center** لتثبيت التطبيق على العقدة الخاملة.

4. في نافذة **المجلد المشترك** ونافذة **مشاركة الحالة**، حدد مسارًا للمجلد المشترك بمعلومات حول حالة الكتلة التي قمت بإنشائها على خادم الملفات أثناء الإعداد.

5. انقر على زر**تثبيت** . عندما ينتهي التثبيت، انقر فوق الزر **Finish**.

تم تثبيت Kaspersky Security Center على العقدة الخاملة. يمكنك الآن اختبار مجموعة تجاوز الفشل من Kaspersky Security Center للتأكد من أنك قمت بتكوينها بشكل صحيح وأن الكتلة تعمل بشكل صحيح.

بدء تشغيل مهمة وإيقافها يدويًا

قد تحتاج إلى إيقاف مجموعة تجاوز الفشل من Kaspersky Security Center بالكامل أو فصل إحدى عقد المجموعة مؤقتًا للصيانة. إذا كانت هذه هي الحالة، فاتبع الإرشادات في هذا القسم. لا تحاول بدء أو إيقاف الخدمات أو العمليات المتعلقة بمجموعة تجاوز الفشل باستخدام أي وسيلة أخرى. قد يتسبب هذا في فقد البيانات.

بدء وإيقاف مجموعة تجاوز الفشل بأكملها للصيانة

لبدء أو إيقاف مجموعة تجاوز الفشل بالكامل:

1. في العقدة المفعلة، انتقل إلى<Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. افتح سطر الأوامر، ثم قم بتشغيل أحد الأوامر التالية:

- لإيقاف المجموعة، قم بتشغيل: `klfoc -stopcluster --stp klfoc`
- لبدء المجموعة، قم بتشغيل: `klfoc -startcluster --stp klfoc`

يتم بدء تشغيل نظام مجموعة تجاوز الفشل أو إيقافه، بناءً على الأمر الذي تقوم بتشغيله.

المحافظة على إحدى العقد

للحفاظ على إحدى العقد:

1. على العقدة المفعلة، قم بإيقاف مجموعة تجاوز الفشل باستخدام الأمر `klfoc -stopcluster --stp klfoc`.

2. في العقدة التي تريد الحفاظ عليها، انتقل إلى <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

3. افتح سطر الأوامر، ثم افصل العقدة عن المجموعة عن طريق تشغيل الأمر `detach_node.cmd`.

4. على العقدة المفعلة ، ابدأ تشغيل نظام مجموعة تجاوز الفشل باستخدام الأمر `klfoc -startcluster --stp klfoc`.

5. أداء أنشطة الصيانة.

6. على العقدة المفعلة، قم بإيقاف مجموعة تجاوز الفشل باستخدام الأمر `klfoc -stopcluster --stp klfoc`.

7. في العقدة التي تم الحفاظ عليها، انتقل إلى <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

8. افتح سطر الأوامر ، ثم قم بإرفاق العقدة بالكتلة عن طريق تشغيل الأمر `attach_node.cmd`.

9. على العقدة المفعلة ، ابدأ تشغيل نظام مجموعة تجاوز الفشل باستخدام الأمر `klfoc -startcluster --stp klfoc`.

يتم الاحتفاظ بالعقدة وإرفاقها بمجموعة تجاوز الفشل.

تثبيت خادم الإدارة على مجموعة تجاوز الفشل في Windows Server

تختلف عملية تثبيت خادم الإدارة على مجموعة تجاوز الفشل عن التثبيت القياسي والمخصص على جهاز مستقل.

لا يتم دعم نظام مجموعات تجاوز الفشل الموزعة جغرافيًا في نظام التشغيل Windows. لا يمكن نشر نظام مجموعة تجاوز الفشل في Windows Server إلا في موقع جغرافي واحد يوفر توفرًا عاليًا للشبكة ووقت استجابة سريعًا بين عقد المجموعة.

قم بتنفيذ الإجراء الموضح في هذا القسم على العقدة التي تحتوي على تخزين بيانات مشترك لنظام المجموعة.

لتثبيت خادم إدارة Kaspersky Security Center على نظام المجموعة:

تشغيل الملف التنفيذي ksc_<رقم الإصدار>_full_<لغة الترجمة>.exe.

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط **تثبيت خادم إدارة Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.

الخطوة 1. مراجعة اتفاقية الترخيص وسياسة الخصوصية

عند هذه المرحلة من معالج الإعداد، يجب قراءة اتفاقية الترخيص المبرمة بينك وبين Kaspersky، بالإضافة إلى سياسة الخصوصية.

قد تتم مطالبتك أيضًا بعرض اتفاقيات الترخيص وسياسات الخصوصية لمكونات إدارة التطبيق الإضافية المتوفرة في حزمة توزيع Kaspersky Security Center.

يُرجى قراءة اتفاقية الترخيص وسياسة الخصوصية بعناية. إذا كنت توافق على جميع شروط اتفاقية الترخيص وسياسة الخصوصية، أكد ذلك عن طريق تحديد خانات الاختيار المناسبة.

سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من خانتي الاختيار.

في حالة عدم قبولك لاتفاقية الترخيص أو سياسة الخصوصية، قم بإلغاء عملية التثبيت عن طريق النقر فوق الزر **إلغاء**.

الخطوة 2. تحديد نوع التثبيت على نظام المجموعة

حدد نوع التثبيت على نظام المجموعة:

- **نظام المجموعة (يتم التثبيت على جميع عقد نظام المجموعة)**

هذا هو الخيار الموصى به. إذا حددت هذا الخيار، فسيتم تثبيت خادم الإدارة على جميع عقد نظام المجموعة في وقت واحد.

في خطوة تحديد وحدة تحكم الإدارة للتثبيت، ستحتاج إلى تحديد وحدة التحكم التي سيتم تثبيتها على عقدة المجموعة الحالية. إذا قمت بتثبيت وحدة تحكم على عقدة نظام المجموعة فقط، ففي حالة فشل العقدة، ستفقد الوصول إلى خادم الإدارة. نوصي أثناء هذه الخطوة بأن تحدد وحدة تحكم الإدارة المستندة إلى MMC للتثبيت على كل عقد المجموعة. بعد تثبيت خادم الإدارة ، قم بتثبيت Kaspersky Security Center Web Console على جهاز منفصل ليس عقدة نظام مجموعة. ويتيح لك ذلك إدارة خادم الإدارة باستخدام Kaspersky Security Center Web Console إذا فشلت عقدة المجموعة.

- **محليًا (يكون التثبيت على هذا الجهاز فقط)**

إذا حددت هذا الخيار، فسيتم تثبيت خادم الإدارة فقط على العقدة الحالية، كما لو كان مثبتا على خادم مستقل، ولن يعمل خادم الإدارة كتطبيق نظام المجموعات. على سبيل المثال، قد ترغب في تحديد هذا الخيار لحفظ مساحة التخزين المشتركة، إذا لم يتطلب خادم الإدارة التسامح مع الخطأ. في حالة فشل العقدة الحالية، سيتعين عليك تثبيت خادم الإدارة على عقدة أخرى واستعادة حالة خادم الإدارة من نسخة احتياطية.

تكون الخطوات الإضافية متشابهة عند استخدام طريقة التثبيت القياسية أو المخصصة، بدءًا من خطوة تحديد طريقة التثبيت.

الخطوة 3. تحديد اسم خادم الإدارة الافتراضي

حدد اسم الشبكة الخاص بخادم الإدارة الافتراضي الجديد. ستتمكن من استخدام هذا الاسم لتوصيل وحدة تحكم الإدارة أو Kaspersky Security Center Web Console بخادم الإدارة.

يجب أن يختلف الاسم الذي تحدده عن اسم نظام المجموعة.

الخطوة 4. تحديد تفاصيل الشبكة الخاصة بخادم الإدارة الافتراضي

لتحديد تفاصيل الشبكة الخاصة بمثيل خادم الإدارة الافتراضي الجديد:

1. في **الشبكة المستخدمة**، حدد شبكة المجال التي تتصل بها عقدة نظام المجموعة الحالية.

2. قم بأحد الإجراءات التالية:

- إذا تم استخدام DHCP في الشبكة المحددة لتعيين عناوين IP، فحدد خيار **استخدام DHCP**.

- إذا لم يتم استخدام DHCP في الشبكة المحددة، فحدد عنوان IP المطلوب.

  يجب أن يختلف عنوان IP الذي تحدده عن عنوان IP لنظام المجموعة.

3. انقر فوق **إضافة** لتطبيق الإعدادات المحددة.

ستتمكن من استخدام عنوان IP المعين تلقائيًا أو عنوان IP المحدد لتوصيل وحدة تحكم الإدارة أو Kaspersky Security Center Web Console بخادم الإدارة.

الخطوة 5. تحديد مجموعة الكتلة

تعد مجموعة نظام المجموعة من أدوار مجموعة تجاوز الفشل الخاصة التي تحتوي على موارد مشتركة في جميع العقد. لديك خياران:

- إنشاء مجموعة جديدة في نظام المجموعات.

  يوصى بهذا الخيار في معظم الحالات. ستحتوي المجموعة الجديدة في نظام المجموعة على كافة الموارد العامة المتعلقة بمثيل خادم الإدارة.

- اختيار مجموعة موجودة بنظام المجموعات.

  حدد هذا الخيار إذا كنت تريد استخدام مورد مشترك ومرتبط بالفعل بمجموعة موجودة بنظام المجموعات. على سبيل المثال، قد ترغب في استخدام هذا الخيار إذا كنت تريد استخدام مخزن مرتبط بمجموعة موجودة بنظام المجموعات، وإذا لم يتوفر تخزين آخر لمجموعة جديدة في نظام المجموعة.

الخطوة 6. تحديد تخزين بيانات نظام المجموعة:

لتحديد تخزين بيانات نظام المجموعة:

1. في **المستودعات المتاحة**، حدد تخزين البيانات الذي سيتم تثبيت الموارد المشتركة الخاصة بمثيل خادم الإدارة الافتراضي عليها.
2. إذا كانت وحدة تخزين البيانات المحددة تحتوي على عدة وحدات للتخزين، ضمن **الأقسام المتوفرة على محرك الأقراص**، فحدد وحدة التخزين المطلوبة.
3. في **مسار التثبيت**، أدخل المسار في وحدة تخزين البيانات المشتركة الذي سيتم تثبيت موارد مثيل خادم الإدارة الافتراضي عليه.

   يتم تحديد وحدة تخزين البيانات.

الخطوة 7. تحديد حساب للتثبيت عن بُعد

حدد اسم المستخدم وكلمة المرور اللذين سيتم استخدامهما لتثبيت مثيل خادم الإدارة الافتراضي عن بُعد على عقدة سلبية في نظام المجموعة.

يتطلب منك منح الحساب الذي تحدده امتيازات إدارية على جميع عقد نظام المجموعة.

الخطوة 8. تحديد المكونات المراد تثبيتها

حدد مكونات خادم إدارة Kaspersky Security Center التي ترغب في تثبيتها:

- **إدارة جهاز المحمول** حدد خانة الاختيار هذه إذا كان يجب عليك إنشاء حزم تثبيت للأجهزة المحمولة عندما يتم تشغيل معالج إعداد Kaspersky Security Center. يمكنك أيضًا إنشاء حزم تثبيت للأجهزة المحمولة يدويًا، بعد تثبيت خادم الإدارة، باستخدام أدوات وحدة تحكم الإدارة.
- **وكيل SNMP**. يتلقى هذا المكون معلومات إحصائية لخادم الإدارة عبر بروتوكول SNMP. يتوفر المكون في حالة تثبيت التطبيق على جهاز مثبت عليه SNMP.

> بعد تثبيت Kaspersky Security Center، سيتم وضع ملفات .mib المطلوبة لتلقي البيانات الإحصائية في المجلد الفرعي SNMP من مجلد تثبيت التطبيق.

لن يتم عرض عميل الشبكة ووحدة تحكم الإدارة في قائمة المكونات. يتم تثبيت هذه المكونات تلقائيًا، ولا يمكنك إلغاء تثبيتهما.

عند هذه الخطوة، يجب أن تحدد مجلدًا لتثبيت مكونات خادم الإدارة. بشكل افتراضي، يتم تثبيت المكونات على <Disk>:\Program Files\Kaspersky\Kaspersky Security Center\Lab. في حالة عدم وجود مثل هذا المجلد، يتم إنشاء هذا المجلد تلقائيًا أثناء التثبيت. يمكنك تغيير المجلد الوجهة باستخدام الزر **استعراض**.

الخطوة 9. اختيار حجم الشبكة

حدد حجم الشبكة التي سيتم تثبيت Kaspersky Security Center عليها. بناءً على عدد الأجهزة الموجودة على الشبكة، يقوم المعالج بتكوين التثبيت ومظهر واجهة التطبيق بحيث يتطابقوا.

يسرد الجدول التالي إعدادات تثبيت التطبيق وإعدادات مظهر الواجهة التي تم ضبطها بناءً على أحجام الشبكة المختلفة.

اعتمادًا على إعدادات التثبيت الموجودة على مقياس الشبكة المحدد

الإعدادات	1—100 جهاز مُدار	101—1000 جهاز مُدار	1001—5000 جهاز مُدار	أكثر من 5000 جهاز مُدار
عرض مع عقدة خوادم الإدارة الثانوية والظاهرية وجميع الإعدادات المتعلقة بخوادم الإدارة الثانوية والظاهرية في شجرة وحدة التحكم (متاح فقط في وحدة تحكم الإدارة المستندة إلى MMC)	غير متاح	غير متاح	متاح	متاح
عرض مع أقسام **الأمان** في نوافذ خصائص خادم الإدارة ومجموعات الإدارة (متاح فقط في وحدة تحكم الإدارة المستندة إلى MMC)	غير متاح	غير متاح	متاح	متاح
التوزيع العشوائي لوقت بدء التشغيل لمهمة التحديث على الأجهزة العميلة	غير متاح	على مدى فاصل مدته 5 دقائق	على مدى فاصل مدته 10 دقائق	على مدى فاصل مدته 10 دقائق

إذا قمت بتوصيل خادم الإدارة بخادم قاعدة بيانات MySQL 5.7 أوSQL Express، فلا يوصى باستخدام التطبيق لإدارة أكثر من 10 000 جهاز. بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20 000 جهاز.

الخطوة 10. تحديد قاعدة البيانات

في هذه الخطوة من المعالج، حدد أحد أنظمة إدارة قواعد البيانات (DBMS) التالية التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة:

- **خادم Microsoft SQL أو SQL Server Express**
- **MySQL أو MariaDB**
- **PostgreSQL أو Postgres Pro**

يوصى بتثبيت خادم الإدارة على خادم مخصص بدلاً من وحدة التحكم بالمجال. ومع ذلك، إذا قمت بتثبيت Kaspersky Security Center على خادم يعمل كوحدة تحكم بالمجال للقراءة فقط (RODC)، فلا يجب حينها تثبيت Microsoft SQL Server (SQL Express) محليًا (على نفس الجهاز). في هذه الحالة، نوصي بتثبيت Microsoft SQL Server (SQL Express) عن بُعد (على جهاز آخر)، أو استخدام MySQL أو MariaDB، إذا كنت بحاجة إلى تثبيت DBMS محليًا.

يتم توفير بنية قاعدة بيانات خادم الإدارة في الملف klakdb.chm، الموجود في مجلد تثبيت Kaspersky Security Center. يتوفر هذا الملف أيضًا في أرشيف يوجد على بوابة Kaspersky: klakdb.zip.

الخطوة 11. تكوين خادم SQL Server

في هذه الخطوة من المعالج، حدد إعدادات الاتصال التالية، اعتمادًا على نظام إدارة قاعدة البيانات (DBMS) الذي حددته:

- إذا اخترت **خادم Microsoft SQL** أو **SQL Server Express** في الخطوة السابقة:

- في الحقل **اسم مثيل خادم SQL Server**، حدد اسم خادم SQL Server على الشبكة. لعرض قائمة بجميع خوادم SQL Server الموجودة على الشبكة، انقر فوق الزر **استعراض**. هذا الحقل فارغ بصورة افتراضية.

إذا قمت بالاتصال بخادم SQL Server عبر منفذ مخصص، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصولاً بفاصلة، على سبيل المثال:

```
1433,SQL_Server_host_name
```

إذا قمت بتأمين الاتصال بين خادم الإدارة و SQL Server عن طريق شهادة، فحدد في حقل **اسم مثيل خادم SQL Server** نفس اسم المضيف الذي تم استخدامه في إنشاء الشهادة. إذا كنت تستخدم مثيلًا مسمًا من SQL Server، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصولاً بفاصلة، على سبيل المثال:

```
1433,SQL_Server_name
```

إذا كنت تستخدم العديد من مثيلات خادم SQL Server على نفس المضيف، فحدد أيضًا اسم المثيل مفصولاً بشرطة مائلة للخلف، على سبيل المثال:

```
1433,SQL_Server_instance_name\SQL_Server_name
```

إذا تم تمكين ميزة "التشغيل الدائم" في خادم SQL على شبكة المؤسسة، فحدد اسم مستمع مجموعة الإتاحة في حقل **اسم مثيل خادم SQL Server**. يرجى العلم أن خادم الإدارة يدعم فقط وضع توفر الالتزام المتزامن عند تمكين ميزة "التشغيل الدائم".

- في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

في هذه المرحلة، إذا كنت ترغب في تثبيت خادم SQL Server على الجهاز الذي تقوم بتشغيل تثبيت Kaspersky Security Center من خلاله، فيجب عليك إيقاف التثبيت وإعادة تشغيله بعد تثبيت خادم SQL Server. تم إدراج إصدارات خادم SQL المدعومة في متطلبات النظام.

إذا كنت ترغب في تثبيت خادم SQL Server على جهاز بعيد، فلا توجد حاجة لمقاطعة معالج إعداد Kaspersky Security Center. قم بتثبيت خادم SQL Server واستئناف تثبيت Kaspersky Security Center.

- إذا حددت **MySQL** أو **MariaDB** في الخطوة السابقة:

- في الحقل **اسم مثيل خادم SQL Server**، حدد اسم مثيل نظام إدارة قاعدة البيانات. بشكل افتراضي، يكون الاسم هو عنوان IP الخاص بالجهاز الذي سيتم تثبيت Kaspersky Security Center عليه.

- في الحقل **المنفذ**، حدد المنفذ الخاص باتصال خادم الإدارة بنظام إدارة قاعدة البيانات. رقم المنفذ الافتراضي هو 3306.

- في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

- إذا حددت **PostgreSQL** أو **Postgres Pro** في الخطوة السابقة:

- في الحقل **خادم PostgreSQL** أو **Postgres Pro**، حدد اسم مثيل نظام إدارة قاعدة البيانات. بشكل افتراضي، يكون الاسم هو عنوان IP الخاص بالجهاز الذي سيتم تثبيت Kaspersky Security Center عليه.

- في الحقل **المنفذ**، حدد المنفذ الخاص باتصال خادم الإدارة بنظام إدارة قاعدة البيانات. رقم المنفذ الافتراضي هو 5432.

في الحقل اسم **اسم قاعدة البيانات**، حدد اسم نظام إدارة قاعدة البيانات الذي تم إنشاؤه لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

الخطوة 12. تحديد وضع مصادقة

حدد وضع المصادقة الذي سيتم استخدامه عند اتصال خادم الإدارة بنظام إدارة قواعد البيانات (DBMS).

بناءً على نظام إدارة قاعدة البيانات المحدد، يمكنك الاختيار من بين أوضاع المصادقة التالية:

- لـ SQL Express أو خادم Microsoft SQL Server، حدد أي من الخيارات التالية:
  - **وضع مصادقة Microsoft Windows**. التحقق من حقوق استخدام الحساب المستخدم لبدء تشغيل خادم الإدارة.
  - **وضع مصادقة خادم SQL**. في حالة تحديد هذا الخيار، سيتم استخدام الحساب المحدد في النافذة للتحقق من حقوق الوصول. املأ حقلي **الحساب** و**كلمة المرور**.

    لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار**.

بالنسبة لوضعي المصادقة، يتحقق التطبيق مما إذا كانت قاعدة البيانات متوفرة. إذا لم تكن قاعدة البيانات متوفرة، تظهر رسالة خطأ ويتوجب عليك إدخال بيانات اعتماد صحيحة.

إذا كانت قاعدة بيانات خادم الإدارة مخزنة على جهاز آخر وحساب خادم الإدارة لا يملك الوصول إلى خادم قاعدة البيانات، فعليك استخدام وضع مصادقة خادم SQL عند تثبيت أو ترقية خادم الإدارة. قد يحدث هذا عندما يكون الجهاز الذي يقوم بتخزين قاعدة البيانات خارج المجال أو عندما يتم تثبيت خادم الإدارة بموجب حساب النظام المحلي.

بالنسبة إلى MySQL أو MariaDB أو PostgreSQL أو Postgres Pro، حدد الحساب وكلمة المرور.

الخطوة 13. تحديد الحساب لتشغيل خادم الإدارة

حدد الحساب الذي سيتم استخدامه لبدء خادم الإدارة كخدمة.

- **إنشاء الحساب تلقائيًا**. ينشئ التطبيق حسابًا باسم KL-AK-*، الذي سيتم من خلاله تشغيل خدمة kladminserver.

  يمكنك تحديد هذا الخيار إن كانت خطتك هي تحديد موقع المجلد المشترك ونظام إدارة قواعد البيانات على الجهاز نفسه مثل خادم الإدارة.

- **تحديد حساب**. ستعمل خدمة خادم الإدارة (kladminserver) بموجب الحساب الذي حددته.

  سيتعين عليك تحديد حساب مجال، على سبيل المثال إن كنت تخطط لاستخدام مثيل خادم SQL Server من أي إصدار كـ DBMS، بما في ذلك SQL Express الموجود على جهاز آخر و/أو كنت تخطط لتحديد موقع المجلد المشترك على جهاز آخر.

  يدعم Kaspersky Security Center حسابات الخدمة (MSA) المُدارة وحسابات الخدمة المُدارة الجماعية (gMSA). في حالة استخدام أنواع الحسابات هذه في مجالك، فيمكنك تحديد واحد منها كحساب لخدمة خادم الإدارة.

  قبل تحديد MSA أو gMSA، يجب تثبيت الحساب على نفس الجهاز الذي تريد تثبيت خادم الإدارة عليه. إذا لم يتم تثبيت الحساب بعد، فقم بإلغاء تثبيت خادم الإدارة وتثبيت الحساب، ثم أعد تشغيل تثبيت خادم الإدارة. للحصول على تفاصيل حول تثبيت حسابات الخدمة المُدارة على جهاز محلي، راجع وثائق Microsoft الرسمية.

  لتحديد MSA أو gMSA:

  1. انقر فوق الزر **استعراض**.
  2. في النافذة التي تظهر، انقر فوق الزر **أنواع الكائنات**.
  3. حدد النوع **حساب للخدمات** وانقر فوق **موافق**.
  4. حدد الحساب ذي الصلة وانقر فوق **موافق**.

  يجب أن يحتوي الحساب الذي حددته على أذونات مختلفة، بناءً على نظام إدارة قواعد البيانات الذي تخطط لاستخدامه.

لأسباب أمنية، يُرجى عدم تعيين الحالة المميزة لحساب يعمل خادم الإدارة بموجبه.

لا يمكن تغيير حساب خادم الإدارة لاحقًا. يتعين عليك إعادة تثبيت مجموعة تجاوز الفشل لاستخدام حساب خادم إدارة آخر.

الخطوة 14. تحديد الحساب لتشغيل خدمات Kaspersky Security Center

حدد الحساب الذي سيتم تشغيل خدمات Kaspersky Security Center فيه على هذا الجهاز.

- **إنشاء الحساب تلقائيًا**. يقوم Kaspersky Security Center بإنشاء حساب محلي يُسمى KlScSvc على هذا الجهاز الموجود في مجموعة kladmins. سيتم تشغيل خدمات Kaspersky Security Center تحت الحساب الذي تم إنشاؤه.
- **تحديد حساب**. ستعمل خدمات Kaspersky Security Center بموجب الحساب الذي حددته.

سيتعين عليك تحديد حساب المجال إذا، على سبيل المثال، كنت تنوي حفظ التقارير في مجلد موجود على جهاز مختلف أو إذا كان الأمر مطلوبًا من قِبل سياسة أمان المؤسسة الخاصة بك. كما قد يتعين عليك تحديد حساب مجال عند تثبيت خادم الإدارة على مجموعة تجاوز الفشل.

لأسباب أمنية، لا تمنح حالة مميزة للحساب الذي يتم تشغيل الخدمات بموجبه.

سيتم تشغيل خدمة الوكيل لـ KSN (ksnproxy) وخدمة الوكيل لتنشيط Kaspersky (klactprx) وخدمة بوابة مصادقة Kaspersky (klwebsrv) ضمن الحساب المحدد.

الخطوة 15. تحديد مجلد مشترك

حدد موقع واسم المجلد المشترك الذي سيتم استخدامه لتنفيذ ما يلي:

- تخزين الملفات الضرورية لتثبيت التطبيقات عن بُعد (يتم نسخ الملفات إلى خادم الإدارة أثناء إنشاء حزم التثبيت).
- تخزين التحديثات التي تم تنزيلها من مصدر محدث إلى خادم الإدارة.

سيتم تمكين مشاركة الملفات (للقراءة فقط) لجميع المستخدمين.

يمكنك تحديد أي من الخيارين التاليين:

- **إنشاء مجلد مشترك**. قم بإنشاء مجلد جديد. في مربع النص، حدد المسار إلى المجلد.
- **تحديد مجلد مشترك موجود**. حدد مجلد مشترك موجود بالفعل.

يمكن أن يكون المجلد المشترك إما مجلدًا محليًا موجودًا على الجهاز المستخدم للتثبيت أو دليلاً بعيدًا موجودًا على أي من الأجهزة العميلة الموجودة على شبكة الشركة. يمكنك النقر فوق الزر **استعراض** لتحديد المجلد المشترك أو تحديده يدويًا عن طريق إدخال مسار UNC الخاص به (على سبيل المثال، \\Share\server) في الحقل المقابل.

بشكل افتراضي، يقوم المثبت بإنشاء مجلد فرعي KLSHARE محلي في مجلد التطبيق يحتوي على مكونات Kaspersky Security Center.

يمكنك تحديد مجلد مشترك لاحقًا إذا لزم الأمر.

الخطوة 16. تكوين الاتصال بخادم الإدارة

قم بتكوين الاتصال بخادم الإدارة.

- **المنفذ**

رقم المنفذ المستخدم للاتصال بخادم الإدارة.

رقم المنفذ الافتراضي هو 14000.

- **منفذ SSL**

رقم منفذ طبقة مآخذ التوصيل الآمنة (SSL) المستخدم للاتصال الآمن بخادم الإدارة عبر SSL.

رقم المنفذ الافتراضي هو 13000.

- **طول مفتاح التشفير**

حدد طول مفتاح التشفير: 1024 بت أو 2048 بت.

يضع مفتاح التشفير 1024-بت حمل أقل على وحدة المعالجة المركزية (CPU)، ولكنه يعتبر قديمًا لأنه لا يمكنه تقديم عملية تشفير موثوق بها نتيجة لمواصفاته الفنية. قد يتبين أيضًا أن الجهاز الحالي غير متوافق مع شهادات SSL التي تقدم مفاتيح 1024-بت.

يتوافق مفتاح التشفير 2048-بت مع أحدث معايير التشفير. ومع ذلك، قد يؤدي استخدام مفتاح التشفير 2048-بت إلى إضافة حمل على وحدة المعالجة المركزية (CPU).

بشكل افتراضي، يتم تحديد **2048 بت (أفضل أمان)**.

يمكنك أيضًا تغيير معلمات الاتصال بخادم الإدارة لاحقًا على النحو التالي:

- يمكنك تغيير المنفذ وأرقام منفذ SSL في القسم **Connection ports** في خصائص خادم الإدارة. وللمزيد من المعلومات عن منافذ اتصال خادم الإدارة، يرجى الرجوع إلى المنافذ المستخدمة بواسطة Kaspersky Security Center.

- يمكنك تغيير طول مفتاح التشفير عند استبدال شهادة خادم الإدارة بالأداة المساعدة klsetsrvcert باستخدام المعلمة `-RsaKeyLen o:<` طول المفتاح >.

الخطوة 17. تعريف عنوان خادم الإدارة

تحديد نافذة عنوان خادم الإدارة يمكنك تحديد أي من الخيارات التالية:

- **اسم مجال DNS**. يمكنك استخدام هذه الطريقة إذا كانت الشبكة تتضمن خادم DNS ويمكن لأجهزة العميل استخدامها لتلقي عنوان خادم الإدارة.

- **اسم NetBIOS**. تستخدم هذه الطريقة إذا كانت أجهزة العميل تتلقى عنوان خادم الإدارة باستخدام بروتوكول NetBIOS أو إذا كان خادم WINS متوفرًا على الشبكة.

- **عنوان IP**. يتم استخدام هذا الخيار إذا كان خادم الإدارة لديه عنوان IP ثابت لن يتم تغييره لاحقًا.

الخطوة 18. عنوان خادم الإدارة للاتصال بالأجهزة المحمولة

تتوفر هذه الخطوة من معالج الإعداد إذا قمت بتحديد إدارة جهاز المحمول للتثبيت.

في نافذة **عنوان الاتصال الأجهزة المحمولة** حدد العنوان الخارجي لخادم الإدارة للاتصال بالأجهزة المحمولة الموجودة خارج الشبكة المحلية. يمكنك تحديد عنوان IP أو نظام اسم النطاق (DNS) لخادم الإدارة.

الخطوة 19. فك وتثبيت الملفات على القرص الثابت

بعد تكوين تثبيت مكونات Kaspersky Security Center، يمكنك بدء تثبيت الملفات على محرك الأقراص الثابتة.

إذا كان التثبيت يتطلب وجود برامج إضافية، فسيقوم معالج الإعداد بإخطارك، في صفحة **متطلبات التثبيت الأساسية**، قبل بدء تثبيت Kaspersky Security Center. سيتم تثبيت البرامج المطلوبة تلقائيًا بعد النقر فوق الزر **التالي**.

في الصفحة الأخيرة، يمكنك تحديد وحدة تحكم لبدء العمل مع Kaspersky Security Center:

- **بدء وحدة تحكم الإدارة القائمة على MMC**
- **تثبيت Kaspersky Security Center Web Console**

يكون هذا الخيار متاحًا فقط في حالة اختيارك لتثبيت Kaspersky Security Center Web Console في إحدى الخطوات السابقة.

يمكنك أيضًا النقر فوق **إنهاء** لإغلاق المعالج دون بدء العمل مع Kaspersky Security Center. يمكنك بدء العمل لاحقًا في أي وقت.

عند بدء التشغيل الأول لوحدة تحكم الإدارة أو Kaspersky Security Center Web Console، يمكنك القيام بـ الإعداد الأولي للتطبيق.

تثبيت خادم الإدارة في الوضع الصامت

يمكن تثبيت خادم الإدارة في الوضع الصامت، أي، بدون إدخال تفاعلي لإعدادات التثبيت.

لتثبيت خادم الإدارة على جهاز محلي في الوضع الصامت:

1. أقرأ اتفاقية ترخيص المستخدم النهائي. استخدم الأمر أدناه فقط إذا فهمت ووافقت على شروط اتفاقية ترخيص المستخدم النهائي.
2. اقرأ سياسة الخصوصية. استخدم الأمر أدناه فقط إذا كنت تستوعب وتوافق على أنه سيتم التعامل مع بياناتك ونقلها (بما في ذلك، نقلها إلى البلدان الثالثة) كما هو موضح في سياسة الخصوصية.
3. قم بتشغيل الأمر

```
"<setup_parameters> 1=1 PRIVACYPOLICY=1 EULA=DONT_USE_ANSWER_FILE"setup.exe /s /v
```

حيث إن `setup_parameters` هو قائمة معلمات وقيمها الخاصة المفصولة بمسافات (`PARAM2VAL=PARAM1VAL PARAM2=PARAM1`). يوجد الملف setup.exe في مجلد الخادم، والذي يُعد جزءً من مجموعة توزيع Kaspersky Security Center.

يتم إدراج الأسماء والقيم المحتملة للمعلمات التي يمكن استخدامها عند تثبيت خادم الإدارة في الوضع الصامت في الجدول أدناه.

معلمات تثبيت خادم الإدارة في الوضع الصامت

اسم المعلمة	وصف المعلمة	القيم المتوفرة
EULA	الموافقة على شروط اتفاقية الترخيص.	• 1—لقد قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها. • قيمة أخرى أو بلا قيمة—لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت).
PRIVACYPOLICY	الموافقة على شروط سياسة الخصوصية.	• 1— أدرك أنه سيتم التعامل مع بياناتي ونقلها (بما يشمل نقل البيانات إلى دول ثالثة) وفقًا لما ورد في سياسة الخصوصية وأوافق على ذلك. أؤكد على أني قد قرأت سياسة الخصوصية وفهمتها بالكامل. • قيمة أخرى أو بلا قيمة– لا أوافق على بنود سياسة الخصوصية (لا يتم إجراء التثبيت).
INSTALLATIONMODETYPE	نوع تثبيت خادم الإدارة.	• قياسي—تثبيت قياسي. • مخصص—تثبيت مخصص.
INSTALLDIR	مسار إلى مجلد تثبيت خادم الإدارة.	قيمة السلسلة.

اسم المعلمة	وصف المعلمة	القيم المتوفرة
ADDLOCAL	قائمة بمكونات خادم الإدارة (مفصولة بفاصلة) المُراد تثبيتها.	NSAC, CSAdminKitConsole, NAgent, CSAdminKitServer, GdiPlusRedist, SNMPAgent, KSNProxy, MobileSupport, Microsoft_VC100_CRT_x86, Microsoft_VC90_CRT_x86. قائمة الحد الأدنى من المكونات الكافية للتثبيت الصحيح لخادم الإدارة: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.
NETRANGETYPE	حجم الشبكة (عدد الأجهزة الموجودة على الشبكة).	• NRT_1_100—من 1 إلى 100 جهاز. • NRT_100_1000—من 101 إلى 1000 جهاز. • NRT_GREATER_1000—أكثر من 1000 جهاز.
SRV_ACCOUNT_TYPE	وضع تحديد حساب الذي سيتم تشغيل خادم الإدارة كخدمة من خلاله.	• SrvAccountDefault—تم إنشاء الحساب تلقائيًا. • SrvAccountUser—تم تحديد الحساب يدويًا. وفي هذه الحالة، يجب عليك تحديد قيم للمعلمتين `SERVERACCOUNTNAME` و `SERVERACCOUNTPWD`.
SERVERACCOUNTNAME	اسم الحساب الذي سيتم تشغيل خادم الإدارة تحته كخدمة. يجب عليك تحديد قيمة للمعلمة في حالة SrvAccountUser=SRV_ACCOUNT_TYPE.	قيمة السلسلة.
SERVERACCOUNTPWD	كلمة مرور الحساب الذي سيتم استخدامه لبدء خادم الإدارة كخدمة. يجب عليك تحديد قيمة للمعلمة في حالة SrvAccountUser=SRV_ACCOUNT_TYPE.	قيمة السلسلة.
SERVERCER	حجم المفتاح لشهادة خادم الإدارة (بوحدات البت).	• 1- حجم المفتاح لشهادة خادم الإدارة هو 2048 بت. • بدون قيمة - حجم المفتاح لشهادة خادم الإدارة هو 1024 بت.
DBTYPE	نوع قاعدة البيانات التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة. هذه المعلمة مطلوبة.	• MySQL — سيتم استخدام قاعدة بيانات MySQL أو MariaDB في هذه الحالة، يجب عليك تحديد قيم للمعلمات `MYSQLSERVERNAME` و `MYSQLSERVERPORT` و `MYSQLDBNAME` و `MYSQLACCOUNTNAME` و `MYSQLACCOUNTPWD`. • MSSQL— سيتم استخدام قاعدة بيانات Microsoft SQL Server (SQL Express). في هذه الحالة، يجب عليك تحديد قيم لمعلمات `MSSQLSERVERNAME` و `MSSQLDBNAME` و `MSSQLAUTHTYPE`. • POSTGRES - سيتم استخدام قاعدة بيانات PostgreSQL أو Postgres Pro. في هذه الحالة، يجب عليك تحديد قيم للمعلمات `POSTGRESSERVERNAME` و `POSTGRESSERVERPORT` و `POSTGRESDBNAME` و `POSTGRESACCOUNTNAME` و `POSTGRESACCOUNTPWD`.
MYSQLSERVERNAME	الاسم الكامل لخادم SQL Server. يجب عليك تحديد قيمة للمعلمة في حالة MySQL=DBTYPE.	قيمة السلسلة.
MYSQLSERVERPORT	عدد المنافذ للاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة في حالة MySQL=DBTYPE.	قيمة رقمية.
MYSQLDBNAME	نوع قاعدة البيانات التي سيتم إنشاؤها لتخزين بيانات خادم الإدارة. يجب عليك تحديد قيمة للمعلمة في حالة MySQL=DBTYPE.	قيمة السلسلة.
MYSQLACCOUNTNAME	اسم الحساب الخاص بالاتصال بقاعدة البيانات. يجب عليك تحديد قيمة للمعلمة في حالة MySQL=DBTYPE.	قيمة السلسلة.
MYSQLACCOUNTPWD	كلمة مرور الحساب للاتصال بقاعدة البيانات. يجب عليك تحديد قيمة للمعلمة في حالة MySQL=DBTYPE.	قيمة السلسلة.
MSSQLSERVERNAME	الاسم الكامل لخادم SQL Server. يجب عليك تحديد قيمة للمعلمة إذا كانت MySQL=DBTYPE.	قيمة السلسلة.
MSSQLDBNAME	اسم قاعدة البيانات. يجب عليك تحديد قيمة للمعلمة إذا كانت MySQL=DBTYPE.	قيمة السلسلة.
MSSQLAUTHTYPE	نوع التخويل عند الاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة إذا كانت MySQL=DBTYPE.	• Windows—وضع مصادقة Microsoft Windows. • SQL Server —وضع مصادقة خادم SQL Server. في هذه الحالة، يجب عليك تحديد قيم للمعلمتين `MSSQLACCOUNTNAME` و `MSSQLACCOUNTPWD`.
MSSQLACCOUNTNAME	اسم الحساب للاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة إذا كانت SQLServer=MSSQLAUTHTYPE.	قيمة السلسلة.

اسم المعلمة	وصف المعلمة	القيم المتوفرة
MSSQLACCOUNTPWD	كلمة مرور الحساب للاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة إذا كانت SQLServer=MSSQLAUTHTYPE.	قيمة السلسلة.
CREATE_SHARE_TYPE	طريقة تحديد المجلد المشترك.	• إنشاء—إنشاء مجلد مشترك جديد. في هذه الحالة، يجب عليك تحديد قيم للمعلمتين SHARELOCALPATH و SHAREFOLDERNAME. • ChooseExisting—حدد مجلد موجود. في هذه الحالة، يجب عليك تحديد قيم للمعلمة EXISTSHAREFOLDERNAME.
SHARELOCALPATH	المسار الكامل إلى مجلد محلي. يجب عليك تحديد قيمة للمعلمة في حالة Create=CREATE_SHARE_TYPE	قيمة السلسلة.
SHAREFOLDERNAME	اسم الشبكة لمجلد مشترك. يجب عليك تحديد قيمة للمعلمة إذا كانت Create=CREATE_SHARE_TYPE.	قيمة السلسلة.
EXISTSHAREFOLDERNAME	المسار الكامل لمجلد مشترك موجود. يجب عليك تحديد قيمة للمعلمة في حالة ChooseExisting=CREATE_SHARE_TYPE.	قيمة السلسلة.
SERVERPORT	رقم المنفذ الخاص بالاتصال بخادم الإدارة.	قيمة رقمية.
SERVERSSLPORT	عدد المنافذ لاتصال مشفر لخادم الإدارة باستخدام بروتوكول SSL.	قيمة رقمية.
SERVERADDRESS	عنوان خادم الإدارة.	قيمة السلسلة.
MOBILESERVERADDRESS	عنوان خادم الإدارة الخاص بالاتصال بالأجهزة المحمولة.	قيمة السلسلة.

للحصول على وصف مفصل لمعلمات إعداد خادم الإدارة، يُرجى الرجوع إلى القسم التثبيت المخصص.

تثبيت وحدة تحكم الإدارة على محطة عمل المسؤول

يمكنك تثبيت وحدة تحكم الإدارة على محطة عمل المسؤول بشكل منفصل وإدارة خادم الإدارة من خلال شبكة باستخدام وحدة التحكم هذه.

لتثبيت وحدة تحكم الإدارة على محطة عمل المسؤول:

1. قم بتشغيل الملف التنفيذي setup.exe.

   يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها.

2. في نافذة تحديد التطبيق، انقر فوق الرابط **تثبيت وحدة تحكم إدارة Kaspersky Security Center** لتشغيل معالج إعداد وحدة تحكم الإدارة. اتبع إرشادات المعالج.

3. حدد المجلد الوجهة. بشكل افتراضي، سيكون هذا المجلد هو <Drive>:\Program Files\Kaspersky Lab\Kaspersky Security Center\Console. في حالة عدم وجود هذا المجلد، يتم إنشاؤه بشكل تلقائي أثناء التثبيت. يمكنك تغيير المجلد الوجهة باستخدام الزر **استعراض**.

4. في الصفحة الأخيرة من معالج الإعداد، انقر فوق الزر **ابدأ** لبدء تثبيت وحدة تحكم الإدارة.

   عند اكتمال المعالج، سيتم تثبيت وحدة تحكم الإدارة على محطة عمل المسؤول.

لتثبيت وحدة تحكم الإدارة على محطة عمل المسؤول في الوضع الصامت:

1. أقرأ اتفاقية ترخيص المستخدم النهائي. استخدم الأمر أدناه فقط إذا فهمت ووافقت على شروط اتفاقية ترخيص المستخدم النهائي.

2. في المجلد Console\Distrib لمجموعة توزيع Kaspersky Security Center، قم بتشغيل ملف setup.exe باستخدام الأمر التالي:

```
"1=EULA"setup.exe /s /v
```

إذا كنت ترغب في تثبيت كافة مكونات الإدارة الإضافية من مجلد Plugins\Console\Distrib مع وحدة تحكم الإدارة، فقم بتشغيل الأمر التالي:

```
pALL/ "1=EULA"setup.exe /s /v
```

إذا كنت تريد تحديد مكونات الإدارة الإضافية التي تريد تثبيتها من مجلد `Plugins\Console\Distrib` مع وحدة تحكم الإدارة، فحدد المكونات الإضافية بعد المفتاح "/p" وافصل بينها بفاصلة منقوطة:

```
P3;P2;pP1/ "1=EULA"setup.exe /s /v
```

حيث إن `P1`و`P2`و `P3` هي أسماء المكونات الإضافية التي تتوافق مع أسماء مجلد المكونات الإضافية في مجلد `Plugins\Console\Distrib`. فمثلاً:

```
MDM4IOS;KESS;pKES4Mac/ "1=EULA"setup.exe /s /v
```

سيتم تثبيت وحدة تحكم الإدارة ومكونات الإدارة الإضافية (إن وجدت) على محطة عمل المسؤول.

بعد تثبيت وحدة تحكم الإدارة، يجب أن تؤسس اتصالاً بخادم الإدارة. للقيام بذلك، قم بتشغيل وحدة تحكم الإدارة، وفي النافذة التي تفتح، حدد الاسم أو عنوان IP للجهاز المثبت عليه خادم الإدارة، بالإضافة إلى إعدادات الحساب المستخدم للاتصال به. بعد تأسيس الاتصال بخادم الإدارة، يمكنك إدارة نظام الحماية ضد الفيروسات باستخدام وحدة التحكم في الإدارة هذه.

يمكنك إزالة وحدة تحكم الإدارة باستخدام أدوات الإضافة/الإزالة القياسية من Microsoft Windows.

التغييرات في النظام بعد تثبيت Kaspersky Security Center

رمز وحدة تحكم الإدارة

بعد أن يتم تثبيت وحدة تحكم الإدارة على الجهاز الخاص بك، سيظهر الرمز الخاص بها، الذي يسمح لك ببدء تشغيل وحدة تحكم الإدارة. ابحث عن وحدة تحكم الإدارة في قائمة **بدء** ← **البرامج** ← **Kaspersky Security Center**.

خدمات خادم الإدارة وعميل الشبكة

يتم تثبيت خادم الإدارة وعميل الشبكة على الجهاز كخدمات تتضمن الخصائص المسردة أدناه. يحتوي الجدول أيضًا على سمات الخدمات الأخرى التي تنطبق على الجهاز بعد تثبيت خادم الإدارة.

خصائص خدمات Kaspersky Security Center

المكون	اسم الخدمة	اسم الخدمة المعروض	الحساب
خادم الإدارة	kladminserver	خادم إدارة Kaspersky Security Center	يتم إنشاء حساب محدد من قبل المستخدم أو مخصص غير مميز بتنسيق KL-AK-* أثناء التثبيت
عميل الشبكة	klnagent	عميل شبكة Kaspersky Security Center	النظام المحلي
خادم الويب للوصول إلى Kaspersky Security Center Web Console وإدارة الإنترنت في المؤسسة	klwebsrv	خادم ويب Kaspersky	حساب KlScSvc مخصص وغير مميز
خادم وكيل التنشيط	klactprx	خادم وكيل تنشيط Kaspersky	حساب KlScSvc مخصص وغير مميز
خادم وكيل KSN	ksnproxy	خادم وكيل Kaspersky Security Network	حساب KlScSvc مخصص وغير مميز

إذا قمت بتثبيت Kaspersky Security Center على عقد مجموعة تجاوز الفشل من Kaspersky Security Center، فستصبح خدمة klfocsvc_klfoc متاحة. تعمل خدمتا klnagent_klfoc وklfocsvc_klfoc تحت حساب النظام المحلي. ويجب تشغيل خدمة kladminserver_klfoc تحت حساب "ksc"، كما يجب تشغيل الخدمات الأخرى تحت حساب 'rightless'. ويجب إضافة حسابي 'ksc' و'rightless' في مجموعة KLAdmins مع أذونات المسؤول المحلي. ولكي يعمل Kaspersky Security Center بشكل صحيح، يجب عليك استخدام حسابي 'ksc' و"rightless" فقط لتشغيل الخدمات. ولا نوصي باستخدام حسابات أخرى تمتلك الحقوق ذاتها. ويحتوي الجدول أدناه على خصائص الخدمات التي يتم تطبيقها على الجهاز بعد تثبيت خادم الإدارة على مجموعة تجاوز الفشل من Kaspersky Security Center.

تثبيت خصائص خدمات Kaspersky Security Center في مجموعة تجاوز الفشل من Kaspersky Security Center

المكون	اسم الخدمة	اسم الخدمة المعروض	الحساب
خادم الإدارة	kladminserver_klfoc	خادم إدارة Kaspersky Security Center	ksc
عميل الشبكة	klnagent_klfoc	عميل شبكة Kaspersky Security Center	النظام المحلي
خادم الويب للوصول إلى Kaspersky Security Center Web Console وإدارة الإنترنت في المؤسسة	klwebsrv_klfoc	خادم ويب Kaspersky	rightless
خادم وكيل التنشيط	klactprx_klfoc	خادم وكيل تنشيط Kaspersky	rightless
خادم وكيل KSN	ksnproxy_klfoc	خادم وكيل Kaspersky Security Network	rightless
مجموعة تجاوز الفشل من Kaspersky Security Center	klfocsvc_klfoc	مجموعة تجاوز الفشل من Kaspersky Security Center	النظام المحلي

خدمات Kaspersky Security Center Web Console

إذا قمت بتثبيت Kaspersky Security Center Web Console على الجهاز، سيتم نشر الخدمات التالية (انظر الجدول أدناه):

خدمات Kaspersky Security Center Web Console

اسم الخدمة المعروض	الحساب
Kaspersky Security Center Service Web Console	خدمة NT / KSCSvcWebConsole
Kaspersky Security Center Web Console	خدمة الشبكة
Kaspersky Security Center خادم المكونات الإضافية.	خدمة NT/KSCWebConsolePlugin
خدمة Kaspersky Security Center Web Console	النظام المحلي
قائمة انتظار رسائل Kaspersky Security Center Web Console	خدمة NT / KSCWebConsoleMessageQueue

إصدار خادم عميل الشبكة

سيتم تثبيت إصدار خادم عميل الشبكة على الجهاز مع خادم الإدارة. يعتبر إصدار خادم عميل الشبكة جزء من خادم الإدارة، ويتم تثبيته وإزالته مع خادم الإدارة، ويمكن أن يتفاعل فقط مع خادم الإدارة المثبت محليًا. ليس عليك تكوين اتصال عميل الشبكة بخادم الإدارة: حيث يتم تنفيذ التكوين من خلال برنامج نظرًا لتثبيت المكونات على نفس الجهاز. يتم تثبيت إصدار خادم عميل الشبكة مع نفس الخصائص الخاصة بعميل الشبكة القياسي مع تنفيذ نفس وظائف إدارة التطبيق. سيُدار هذا الإصدار بواسطة سياسة مجموعة الإدارة التي ينتمي إليها الجهاز العميل لخادم الإدارة. بالنسبة لإصدار خادم عميل الشبكة، سيتم إنشاء جميع المهام من النطاق المتوفر من قبل خادم الإدارة، باستثناء مهمة تغيير الخادم.

يتعذر تثبيت عميل شبكة بشكل منفصل على جهاز مثبّت عليه خادم إدارة بالفعل.

يمكنك عرض خصائص كل خدمة لخادم الإدارة وعميل الشبكة، بالإضافة إلى مراقبة تشغيلهما باستخدام أدوات إدارة Windows Microsoft القياسية: إدارة الكمبيوتر/الخدمات. يتم تخزين معلومات حول نشاط خدمة خادم إدارة Kaspersky في سجل نظام Microsoft Windows في فرع سجل أحداث Kaspersky منفصل موجود على الجهاز المثبت عليه خادم الإدارة.

نوصي بتجنب بدء تشغيل الخدمات وإيقافها يدويًا مع ترك حسابات الخدمة في إعدادات الخدمة بدون تغيير. إذا لزم الأم، يمكنك تعديل حساب خدمة خادم الإدارة باستخدام الأداة المساعدة klsrvswch. لاحظ أنه يجب عليك تشغيل الأداة المساعدة klsrvswch على جهاز خادم الإدارة تحت الحساب الذي يتمتع بحقوق المسؤول التي تم استخدامه لتثبيت خادم الإدارة.

حسابات المستخدمين ومجموعات الأمان

يقوم مثبّت خادم الإدارة بإنشاء الحسابات التالية بشكل افتراضي:

- KL-AK-*: حساب خدمة خادم إدارة
- KlScSvc: حساب للخدمات الأخرى من مجموعة خادم الإدارة
- KlPxeUser: حساب لنشر أنظمة التشغيل

إذا حددت حسابات أخرى لخدمة خادم الإدارة والخدمات الأخرى أثناء تشغيل المثبِّت، فيتم استخدام الحسابات المحددة.

سيتم أيضًا إنشاء مجموعات أمان محلية مزودة بمجموعة من الحقوق لكل منهم بشكل تلقائي على الجهاز المثبّت عليه خادم الإدارة.

لا يوصى بتثبيت خادم الإدارة على وحدة التحكم بالمجال، ومع ذلك، إذا قمت بتثبيت خادم الإدارة على وحدة التحكم بالمجال، فيجب أن تبدأ بحقوق مسؤول المجال على المُثبّت. في هذه الحالة، يقوم المُثبّت تلقائيًا بإنشاء مجموعات أمان المجال باسم KLAdmins و KLOperators. إذا قمت بتثبيت خادم الإدارة على جهاز لا يمثل وحدة تحكم المجال، فيجب أن تبدأ بحقوق المسؤول المحلي على أداة التثبيت بدلاً من ذلك. في هذه الحالة، يقوم المثبت تلقائيًا بإنشاء مجموعات أمان محلية باسم KLAdmins و KLOperators.

عند تكوين إخطارات البريد الإلكتروني، قد يلزم عليك إنشاء حساب على خادم البريد لمصادقة ESMTP.

إزالة التطبيق

يمكنك إزالة Kaspersky Security Center باستخدام أدوات الإضافة / الإزالة القياسية لـ Microsoft Windows. تتطلب إزالة التطبيق بدء المعالج الذي يعمل على إزالة جميع مكونات التطبيق من الجهاز (بما في ذلك المكونات الإضافية). يجعل المعالج متصفحك الافتراضي يفتح صفحة ويب بها استقصاء حيث يمكنك إخبارنا بسبب اختيارك التوقف عن استخدام Kaspersky Security Center. إذا لم تقم بتحديد الإزالة من المجلد المشترك (KLSHARE) أثناء تشغيل المعالج، فيمكنك حذفه يدويًا بعد إكمال جميع المهام ذات الصلة.

بعد إزالة التطبيق، قد تظل بعض ملفاته في المجلد المؤقت للنظام.

سيقترح معالج إنشاء مهمة إزالة التطبيق أن تخزن نسخة احتياطية من خادم الإدارة.

عند إزالة التطبيق من Microsoft Windows 7 و Microsoft Windows 2008، قد يحدث الإنهاء المبكر لمعالج إنشاء مهمة إزالة التطبيق. ويمكن تجنب هذا الأمر عن طريق تعطيل التحكم في حساب المستخدم (UAC) في نظام التشغيل وإعادة تشغيل إزالة التطبيق.

حول ترقية Kaspersky Security Center

يحتوي هذا القسم على معلومات حول كيفية ترقية Kaspersky Security Center من إصدار سابق. يمكنك ترقية Kaspersky Security Center بطرق مختلفة، اعتمادًا على ما إذا كان Kaspersky Security Center مثبتًا محليًا أو على عُقد مجموعة تجاوز الفشل من Kaspersky Security Center.

أثناء الترقية، يُحظر تمامًا الاستخدام المتزامن لنظام إدارة قواعد البيانات بواسطة خادم الإدارة وتطبيق آخر.

لاحظ أنه إذا قمت بترقية خادم الإدارة إلى الإصدار 15.1، فلن تتمكن من إنشاء حزم تثبيت جديدة لإصدار Network Agent 15 أو أقدم. ومع ذلك، ستكون حزم التثبيت التي تم إنشاؤها مسبقًا متاحة.

عند ترقية Kaspersky Security Center من إصدار سابق، يتم الاحتفاظ بجميع المكونات الإضافية المثبتة لتطبيقات Kaspersky المدعومة. تتم ترقية المكون الإضافي لخادم الإدارة والمكون الإضافي عميل الشبكة تلقائيًا (بالنسبة لكلٍ من وحدة تحكم الإدارة وبرنامج Kaspersky Security Center Web Console).

ترقية Kaspersky Security Center من إصدار سابق

يصف الموضوع التالي خطوات التحضير الموصى بها للترقية: ترقية Kaspersky Security Center وتطبيقات الأمان المُدارة.

يمكنك تثبيت الإصدار 15.1 من خادم الإدارة على جهاز مثبت عليه إصدار أقدم من خادم الإدارة (بدءًا من الإصدار 11 (11.0.0.1131b)). عند الترقية إلى الإصدار 15.1، يتم حفظ جميع البيانات والإعدادات من الإصدار السابق لخادم الإدارة.

في حالة حدوث مشكلة أثناء تثبيت خادم الإدارة، يمكنك استعادة الإصدار السابق من خادم الإدارة باستخدام النسخة الاحتياطية لبيانات خادم الإدارة التي تم إنشاؤها قبل الترقية.

إذا تم تثبيت خادم إدارة واحد على الأقل من الإصدار الجديد على الشبكة، فيمكنك ترقية خوادم الإدارة الأخرى على الشبكة باستخدام مهمة التثبيت عن بُعد التي تستخدم حزمة تثبيت خادم الإدارة.

إذا قمت بنشر مجموعة تجاوز الفشل من Kaspersky Security Center، يمكنك أيضًا ترقية Kaspersky Security Center على العقد الخاصة به.

لترقية إصدار قديم من خادم الإدارة إلى الإصدار 15.1:

1. قم بتشغيل ملف التثبيت exe.<language>_full_<build number>_ksc_15.1 للإصدار 15.1 (يمكنك تنزيل هذا الملف من موقع ويب Kaspersky).
2. في النافذة التي تفتح، انقر فوق الرابط **تثبيت Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع إرشادات المعالج.
3. قم بقراءة اتفاقية الترخيص وسياسة الخصوصية. في حالة الموافقة على شروط اتفاقية الترخيص وسياسة الخصوصية، حدد خانة الاختيار التالية في قسم **أؤكد على أنني قد قرأت ما يلي واستوعبته جيدًا وأوافق عليه**:
   - **شروط وبنود اتفاقية ترخيص المستخدم النهائي (EULA) هذه**
   - **تصف سياسة الخصوصية طريقة التعامل مع البيانات**

   سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من خانتي الاختيار. يُطالبك معالج الإعداد بإنشاء نسخة احتياطية لبيانات خادم الإدارة للإصدار الأقدم.

   يدعم Kaspersky Security Center استعادة البيانات من نسخة احتياطية تم إنشاؤها باستخدام إصدار أقدم من خادم الإدارة.

4. إذا كنت تريد إنشاء نسخة احتياطية من بيانات خادم الإدارة، فحدد ذلك في نافذة **النسخ الاحتياطي لبيانات خادم الإدارة** لخادم الإدارة التي يتم فتحها.

يتم إنشاء نسخة احتياطية عن طريق الأداة المساعدة klbackup. يتم تضمين هذه الأداة المساعدة في مجموعة التوزيع، الموجودة في جذر مجلد تثبيت Kaspersky Security Center.

5. قم بتثبيت إصدار خادم الإدارة 15.1 من خلال اتباع معالج الإعداد.

إذا ظهرت رسالة تفيد بأن خدمة Kaspersky Security Center Web Console مشغولة، انقر على الزر **Ignore** في نافذة المعالج.

ننصحك بتجنب إنهاء معالج الإعداد. إذا قمت بإلغاء الترقية عند خطوة تثبيت خادم الإدارة إلى فشل إصدار Kaspersky Security Center الذي تم ترقيته.

6. للأجهزة المثبت عليها إصدار عميل شبكة قديم، قم بإنشاء وتشغيل مهمة التثبيت عن بُعد للإصدار الجديد من عميل الشبكة.

نوصي بترقية عميل الشبكة لنظام Linux إلى إصدار Kaspersky Security Center نفسه.

بعد إتمام مهمة التثبيت عن بُعد، سيتم ترقية إصدار عميل الشبكة.

قم بتشغيل الأوامر التالية على الأصول المستندة إلى Linux لإزالة التبعيات التي لم تعد ضرورية:

- بالنسبة للأصول المستندة إلى Debian، قم بتشغيل أي من الأمرين التاليين:
  - `apt-get -y autoremove`
  - `apt -y autoremove`
- بالنسبة للأصول المستندة إلى RPM، قم بتشغيل أي من الأمرين التاليين:
  - `dnf autoremove`
  - `yum autoremove`

ترقية Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky Security Center

يمكنك تثبيت الإصدار 15.1 من خادم الإدارة على كل عقدة نظام مجموعة تجاوز الفشل في Kaspersky Security Center مثبت عليها إصدار سابق من خادم الإدارة (بدءًا من الإصدار 13.2). عند الترقية إلى الإصدار 15.1، يتم حفظ جميع البيانات والإعدادات من الإصدار السابق لخادم الإدارة.

إذا قمت مسبقًا بتثبيت Kaspersky Security Center على الأجهزة محليًا ، يمكنك أيضًا ترقية Kaspersky Security Center على هذه الأجهزة.

لترقية Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky Security Center:

1. قم بتنفيذ الإجراءات التالية على العقدة النشطة للمجموعة:

a. تشغيل الملف التنفيذي exe.<language>_full_<build number>_ksc_15.1

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي ستتم ترقيتها. انقر على الرابط **تثبيت خادم إدارة Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع تعليمات المعالج.

b. قم بقراءة اتفاقية الترخيص وسياسة الخصوصية. في حالة الموافقة على شروط اتفاقية الترخيص وسياسة الخصوصية، حدد خانة الاختيار التالية في قسم **أؤكد على أنني قد قرأت ما يلي واستوعبته جيدًا وأوافق عليه**:

- **شروط وبنود اتفاقية ترخيص المستخدم النهائي (EULA) هذه**
- **تصف سياسة الخصوصية طريقة التعامل مع البيانات**

حدد خانتي الاختيار لمتابعة التثبيت.

إذا كنت لا تقبل اتفاقية الترخيص أو سياسة الخصوصية، فانقر فوق الزر **إلغاء** لإلغاء الترقية.

2. نفذ الإجراءات نفسها على العقدة الخاملة لمجموعة تجاوز الفشل من Kaspersky Security Center كما على العقدة النشطة.

3. ابدأ المجموعة .

نتيجة لذلك، قمت بتثبيت أحدث إصدار من خادم الإدارة على عُقد مجموعة تجاوز الفشل من Kaspersky Security Center.

ترقية Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Microsoft

يمكنك ترقية الإصدار 15.1 من خادم الإدارة على كل عقدة نظام مجموعة تجاوز الفشل من Microsoft مثبت عليها إصدار سابق من خادم الإدارة (بدءًا من الإصدار 13.2). عند الترقية إلى الإصدار 15.1، يتم حفظ جميع البيانات والإعدادات من الإصدار السابق لخادم الإدارة.

لترقية Kaspersky Security Center على عقد مجموعة تجاوز الفشل من Microsoft، نفذ الإجراءات التالية على أي عقدة من عقد المجموعة:

1. تشغيل الملف التنفيذي exe.<language>_full_<build number>_ksc_15.1

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي ستتم ترقيتها. انقر على الرابط **تثبيت خادم إدارة Kaspersky Security Center** لبدء معالج إعداد خادم الإدارة. اتبع تعليمات المعالج.

2. قم بقراءة اتفاقية الترخيص وسياسة الخصوصية. في حالة الموافقة على شروط اتفاقية الترخيص وسياسة الخصوصية، حدد خانة الاختيار التالية في قسم **أؤكد على أنني قد قرأت ما يلي واستوعبته جيدًا وأوافق عليه**:

- **شروط وبنود اتفاقية ترخيص المستخدم النهائي (EULA) هذه**
- **تصف سياسة الخصوصية طريقة التعامل مع البيانات**

حدد خانتي الاختيار لمتابعة التثبيت.

إذا كنت لا تقبل اتفاقية الترخيص أو سياسة الخصوصية، فانقر فوق الزر **إلغاء** لإلغاء الترقية.

3. في النافذة **نوع التثبيت على نظام المجموعة**، حدد **المجموعة (تثبيت على كل عقد المجموعة)**.

بعد ذلك، يقوم المثبت بتكوين خادم الإدارة والانتهاء من ترقيته على جميع عقد المجموعة. أثناء الترقية، يتعذر تغيير إعدادات خادم الإدارة.

نتيجة لذلك، قمت بتثبيت أحدث إصدار من خادم الإدارة على عُقد مجموعة تجاوز الفشل من Microsoft.

الإعداد الأولي لـ Kaspersky Security Center

يرد في هذا القسم الخطوات التي يجب عليك اتخاذها بعد تثبيت Kaspersky Security Center.

دليل التقوية

صُمم دليل التقوية للمحترفين الذين يقومون بتثبيت Kaspersky Security Center وإدارته، بالإضافة إلى هؤلاء الذين يقدمون الدعم الفني للمؤسسات التي تستخدم Kaspersky Security Center.

يصف دليل التقوية التوصيات والميزات الخاصة بتكوين Kaspersky Security Center ومكوناته، التي تهدف إلى تقليل مخاطر الاختراق.

قبل التكوين، أنشئ نسخة احتياطية من Kaspersky Security Center Administration Server باستخدام مهمة النسخ الاحتياطي لبيانات خادم الإدارة أو أداة klbackup واحفظها في مكان آمن.

يتضمن دليل التقوية المعلومات التالية:

- تحديد بنية خادم الإدارة
- تكوين اتصال آمن بخادم الإدارة
- تكوين الحسابات للوصول إلى خادم الإدارة
- إدارة حماية خادم الإدارة والأجهزة العميلة
- تكوين الحماية للتطبيقات المدارة
- صيانة خادم الإدارة
- نقل المعلومات إلى تطبيقات الطرف الخارجي

قبل أن تبدأ في العمل مع خادم الإدارة، يطالبك Kaspersky Security Center بقراءة الإصدار المختصر من دليل التقوية.

ولاحظ أنه لا يمكنك استخدام خادم الإدارة حتى تؤكد أنك قرأت دليل التقوية.

لقراءة دليل التقوية:

1. افتح وحدة تحكم الإدارة أو Kaspersky Security Center Web Console وسجل الدخول إلى وحدة التحكم. تتحقق وحدة التحكم مما إذا كنت قد أكدت قراءة الإصدار الحالي من دليل التقوية.

   وإذا لم تكن قد قرأت دليل التقوية بعد، ستفتح نافذة وتعرض نسخة مختصرة منه.

2. قم بأحد الإجراءات التالية:

   - إذا كنت تريد عرض الإصدار المختصر من دليل التقوية كمستند نصي، انقر فوق الرابط **Open in new window**.
   - إذا كنت تريد عرض الإصدار الكامل من دليل التقوية، فانقر فوق الرابط **Open the Hardening guide in Online Help**.

3. بعد قراءة دليل التقوية، حدد خانة الاختيار **I confirm that I have fully read and understand the Hardening guide**، ثم انقر فوق الزر **Accept**.

   الآن، يمكنك العمل مع خادم الإدارة.

عندما يظهر إصدار جديد من دليل التقوية، سيطالبك Kaspersky Security Center بقراءته.

معالج البدء السريع لخادم الإدارة

يقدم هذا القسم معلومات حول معالج البدء السريع لخادم الإدارة.

حول معالج البدء السريع

يقدم هذا القسم معلومات حول معالج البدء السريع لخادم الإدارة.

يسمح لك معالج البدء السريع لخادم الإدارة بإنشاء الحد الأدنى من المهام والسياسات الضرورية، وضبط الحد الأدنى من الإعدادات، وتنزيل وتثبيت المكونات الإضافية لتطبيقات Kaspersky المُدارة، وإنشاء حزم تثبيت لتطبيقات Kaspersky المُدارة. عند تشغيل المعالج، يمكن إجراء التغييرات التالية على التطبيق:

- قم بتنزيل المكونات الإضافية وتثبيتها للتطبيقات التي تتم إدارتها. بعد الانتهاء من "معالج البدء السريع"، يتم عرض قائمة مكونات الإدارة الإضافية المثبتة في القسم **المتقدم** ← **تفاصيل المكونات الإضافية المثبتة لإدارة التطبيق** من نافذة خصائص خادم الإدارة.

- قم بإنشاء حزمة تثبيت تطبيقات Kaspersky المُدارة. بعد الانتهاء من معالج البدء السريع، يتم عرض حزم تثبيت عميل الشبكة الخاص بنظام التشغيل Windows وتطبيقات Kaspersky المُدارة في **خادم الإدارة** ← **الإعدادات المتقدمة** ← **التثبيت عن بُعد** ← فائمة **حزم التثبيت** .

- أضف ملفات مفاتيح أو أدخل رموز تنشيط يمكن نشرها تلقائيًا على الأجهزة الموجودة ضمن مجموعات الإدارة. بعد الانتهاء من معالج البدء السريع، يتم عرض معلومات حول مفاتيح الترخيص في **خادم الإدارة** ← **قائمة تراخيص Kaspersky** وفي قسم**المفاتيح** الخاص بنافذة خصائص خادم الإدارة.

- قم بتكوين التفاعل مع Kaspersky Security Network (KSN).

- إعداد تسليم البريد الإلكتروني للإخطارات بالأحداث التي تحدث أثناء تشغيل خادم الإدارة والتطبيقات المُدارة (يتطلب تسليم الإخطار بنجاح تشغيل خدمة Messenger على خادم الإدارة وجميع الأجهزة المستلمة). بعد الانتهاء من "معالج البدء السريع"، يتم عرض إعدادات إشعارات البريد الإلكتروني في قسم **الإخطار** الخاص بنافذة خصائص خادم الإدارة.

- ضبط إعدادات التحديث وإعدادات إصلاح الثغرات الأمنية للتطبيقات المثبتة على الأجهزة.

- إنشاء سياسة حماية لمحطات العمل والخوادم ومهام فحص البرامج الضارة ومهام تنزيل التحديثات ومهام النسخ الاحتياطي للبيانات لأعلى مستوى بالتسلسل الهرمي للأجهزة المدارة. بعد الانتهاء من "معالج البدء السريع"، يتم عرض المهام التي تم إنشاؤها في قائمة **خادم الإدارة** ← **مهام**، ويتم عرض السياسات المقابلة للمكونات الإضافية للتطبيقات التي تتم إدارتها في **خادم الإدارة** ← قائمة **السياسات**.

ينشئ معالج البدء السريع للتطبيقات التي تتم إدارتها، مثل Kaspersky Endpoint Security for Windows، ما لم يتم بالفعل إنشاء هذه السياسات لمجموعة **الأجهزة التي تتم إدارتها**. يعمل معالج البدء السريع على إنشاء المهام إذا كانت المهام التي تحمل الأسماء نفسها غير موجودة لمجموعة **الأجهزة التي تتم إدارتها**.

في وحدة تحكم الإدارة، يطالبك Kaspersky Security Center تلقائيًا بتشغيل معالج البدء السريع بعد بدء تشغيله لأول مرة. يمكنك أيضًا بدء تشغيل معالج البدء السريع في أي وقت.

بدء معالج البدء السريع لخادم الإدارة

يطالبك التطبيق تلقائيًا بتشغيل معالج البدء السريع بعد تثبيت خادم الإدارة عند أو اتصال به. يمكنك أيضًا بدء تشغيل معالج البدء السريع في أي وقت.

لبدء تشغيل معالج البدء السريع يدويًا:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

2. في قائمة السياق الخاصة بالعقدة، حدد **جميع المهام** ← **معالج البدء السريع لخادم الإدارة**.

سيطالبك المعالج بإجراء التكوين الأولي لخادم الإدارة. اتبع إرشادات المعالج.

إذا بدأت تشغيل معالج البدء السريع مرة أخرى، فلا يمكن إنشاء المهام والسياسات التي تم إنشاؤها في التشغيل السابق للمعالج مرة أخرى.

الخطوة 1. تكوين خادم وكيل

حدد إعدادات الوصول إلى الإنترنت لخادم الإدارة. يجب تكوين الوصول إلى الإنترنت لاستخدام Kaspersky Security Network ولتنزيل تحديثات لقواعد بيانات مكافحة الفيروسات لـ Kaspersky Security Center وتطبيقات Kaspersky المُدارة.

حدد خيار **استخدام الخادم الوكيل** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. إذا تم تحديد هذا الخيار، ستتوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

- **العنوان**

  عنوان الخادم الوكيل المستخدم لاتصال Kaspersky Security Center بالإنترنت.

- **رقم المنفذ**

  رقم المنفذ الذي سيتم من خلاله إنشاء اتصال وكيل Kaspersky Security Center.

- **تجاوز الخادم الوكيل للعناوين المحلية**

  لن يتم استخدام خادم وكيل للاتصال بالأجهزة في الشبكة المحلية.

- **مصادقة الخادم الوكيل**

  إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

  يتوفر حقل الإدخال هذا إذا تم تحديد خانة الاختيار **استخدام الخادم الوكيل**.

- **اسم المستخدم**

  حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

- **كلمة المرور**

  تم تعيين كلمة مرور بواسطة المستخدم الذي تم إنشاء اتصال الخادم الوكيل من خلال حسابه (هذا الحقل متاح في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

  لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار** حتى تظهر لك كلمة المرور.

يمكنك تكوين الوصول إلى الإنترنت لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 2. تحديد طريقة تفعيل التطبيق

حدد أحد خيارات تفعيل Kaspersky Security Center التالية:

- **عن طريق إدخال رمز التنشيط الخاص بك**

  رمز التنشيط هو تسلسل فريد مكون من 20 حرفًا أبجديًا رقميًا. حيث تقوم بإدخال رمز تنشيط لإضافة مفتاح الذي يقوم بدوره بتنشيط Kaspersky Security Center. تتلقى رمز التنشيط عبر عنوان البريد الإلكتروني الذي حددته بعد شراء Kaspersky Security Center.

  لتفعيل التطبيق باستخدام رمز التفعيل، ستحتاج إلى الوصول إلى الإنترنت لإنشاء اتصال مع خوادم تفعيل Kaspersky.

  إذا قمت بتحديد خيار التفعيل هذا، فيمكنك تمكين خيار **Automatically distribute license key to managed devices**.

  إذا تم تمكين هذا الخيار، فسيتم نشر مفتاح الترخيص تلقائيًا على الأجهزة المُدارة.

  إذا تم تعطيل هذا الخيار، فيمكنك نشر مفتاح الترخيص للأجهزة المُدارة فيما بعد، في جزء **تراخيص Kaspersky** لشجرة وحدة تحكم الإدارة.

إذا لم ينجح التفعيل عن طريق إدخال رمز التفعيل الخاص بك لأي سبب من الأسباب، فيمكنك تفعيل التطبيق عن طريق تحديد ملف مفتاح.

- **عن طريق تحديد ملف مفتاح**

ملف المفتاح هو ملف بامتداد .key مقدم لك من Kaspersky. الهدف من ملف المفتاح هو إضافة مفتاح لتنشيط التطبيق.

يتم وصف طرق الحصول على ملف المفتاح في القسم التالي: حول ملف المفتاح.

لتنشيط التطبيق باستخدام ملف المفتاح، لا تحتاج إلى الاتصال بخوادم تنشيط Kaspersky.

إذا قمت بتحديد خيار التفعيل هذا، فيمكنك تمكين خيار **Automatically distribute license key to managed devices**.

إذا تم تمكين هذا الخيار، فسيتم نشر مفتاح الترخيص تلقائيًا على الأجهزة المُدارة.

إذا تم تعطيل هذا الخيار، فيمكنك نشر مفتاح الترخيص للأجهزة المُدارة فيما بعد، في جزء **تراخيص Kaspersky** لشجرة وحدة تحكم الإدارة.

- **عن طريق تأجيل تفعيل التطبيق**

سيعمل التطبيق باستخدام الوظائف الأساسية، دون إدارة الجهاز المحمول ودون إدارة الثغرات الأمنية والتصحيحات.

إذا اخترت تأجيل تنشيط التطبيق، فيمكنك إضافة مفتاح ترخيص لاحقًا في أي وقت.

الخطوة 3. تحديد مناطق الحماية وأنظمة التشغيل

حدد مناطق الحماية وأنظمة التشغيل المستخدمة على شبكتك. عند تحديد هذه الخيارات، فإنك تحدد عوامل تصفية مكونات الإدارة الإضافية للتطبيق وحزم التوزيع على خوادم Kaspersky التي يمكنك تنزيلها للتثبيت على أجهزة العملاء في الشبكة لديك. حدد الخيارات:

- **المناطق**

يمكنك تحديد مناطق الحماية التالية:

- **محطات العمل**. حدد هذا الخيار إذا كنت تريد حماية محطات العمل في شبكتك. حسب الإعدادات الافتراضية، يتم تحديد خيار مساحة العمل افتراضيًا.
- **خوادم الملفات والتخزين**. حدد هذا الخيار إذا كنت تريد حماية خوادم الملفات في شبكتك.
- **الأجهزة المحمولة**. حدد هذا الخيار إذا أردت حماية الأجهزة المحمولة التي تمتلكها الشركة أو موظفو الشركة. إذا قمت بتحديد هذا الخيار ولكنك لم تقدم ترخيصًا مع ميزة إدارة الأجهزة المحمولة، فسيتم عرض رسالة تخبرك بضرورة توفير ترخيص مع ميزة إدارة الأجهزة المحمولة. إذا لم تقدم ترخيصًا، فلا يمكنك استخدام ميزة الجهاز المحمول.
- **Virtualization**. حدد هذا الخيار إذا كنت تريد حماية الأجهزة الافتراضية في شبكتك.
- **مكافحة البريد غير المرغوب فيه من Kaspersky**. حدد هذا الخيار إذا أردت حماية خوادم البريد الإلكتروني في مؤسستك من البريد غير المرغوب فيه والاحتيال وتسليم البرامج الضارة.

- **Operating systems**

يمكنك تحديد المنصات التالية:

- Microsoft Windows
- Linux
- macOS
- Android
- أخرى

للحصول على معلومات عن أنظمة التشغيل المدعومة، يرجع الرجوع إلى متطلبات الأجهزة والبرامج.

يمكنك تحديد حزم تطبيق Kaspersky من قائمة الحزم المتوفرة لاحقًا، بشكل منفصل عن معالج البدء السريع. لتبسيط البحث عن الحزم المطلوبة، يمكنك ذلك تصفية قائمة الحزم المتاحة بالمعايير التالية:

- منطقة الحماية
- نوع البرنامج الذي تم تنزيله (حزمة توزيع أو أداة مساعدة أو مكون إضافي أو مكون ويب إضافي)
- نسخة من تطبيق Kaspersky
- لغة ترجمة تطبيق Kaspersky

الخطوة 4. تحديد المكونات الإضافية للتطبيقات المُدارة

حدد المكونات الإضافية للتطبيقات المُدارة لتثبيتها. تُعرَض قائمة كاملة بالمكونات الإضافية الموجودة على خوادم Kaspersky. يتم تصفية القائمة وفقًا للخيارات المحددة في الخطوة السابقة من المعالج. حسب الإعدادات الافتراضية، تشمل القائمة الكاملة المكونات الإضافية لجميع اللغات. لعرض المكون الإضافي الخاص بلغة معينة فقط، حدد اللغة من القائمة المنسدلة **إظهار لغة ترجمة وحدة تحكم الإدارة أو**. تتضمن قائمة المكونات الإضافية الأعمدة التالية:

- **اسم التطبيق**

  تم تحديد المكونات الإضافية حسب مناطق الحماية والأنظمة الأساسية التي حددتها في الخطوة السابقة.

- **إصدار التطبيق**

  تتضمن القائمة مكونات إضافية لجميع الإصدارات الموجودة على خوادم Kaspersky. حسب الإعدادات الافتراضية، يتم تحديد المكونات الإضافية لأحدث الإصدارات.

- **لغة التعريب**

  حسب الإعدادات الافتراضية، تُعرَّف لغة الترجمة الخاصة بالمكون الإضافي بواسطة لغة Kaspersky Security Center التي حددتها عند التثبيت. يمكنك تحديد لغات أخرى في قائمة **إظهار لغة ترجمة وحدة تحكم الإدارة أو** المنسدلة.

بعد تحديد المكونات الإضافية، يبدأ تثبيتها تلقائيًا في نافذة منفصلة. لتثبيت بعض المكونات الإضافية، يجب عليك قبول شروط اتفاقية ترخيص المستخدم النهائي. قراءة نص اتفاقية ترخيص المستخدم النهائي ثم حدد خيار **أوافق على بنود اتفاقية الترخيص** وانقر على زر **تثبيت**. إذا لم تقبل شروط اتفاقية ترخيص المستخدم النهائي، فلن يتم تثبيت المكون الإضافي.

بعد اكتمال التثبيت، أغلق نافذة التثبيت.

يمكنك أيضًا حدد المكونات الإضافية للإدارة لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 5. تنزيل حزم التوزيع وإنشاء حزم التثبيت

يتضمن Kaspersky Endpoint Security for Windows أداة تشفير للمعلومات المخزنة على أجهزة العملاء. لتنزيل حزمة توزيع Kaspersky Endpoint Security for Windows صالحة لاحتياجات مؤسستك، راجع تشريعات البلد التي توجد بها أجهزة العملاء الخاصة بمؤسستك.

في النافذة **نوع التشفير**، حدد أحد أنواع التشفير التالية:

- تشفير قوي (AES256). يستخدم هذا النوع من التشفير طول مفتاح 256 بت.
- تشفير ضعيف (AES56). يستخدم هذا النوع من التشفير طول مفتاح 56 بت.

يتم عرض نافذة **نوع التشفير** فقط إذا قمت بتحديد **محطات العمل** كنطاق حماية و**Microsoft Windows** كمنصة.

بعد تحديد نوع التشفير، يتم عرض القائمة الكاملة بحزم توزيع نوعي التشفير على حد سواء. يتم تحديد حزمة التوزيع في القائمة مع نوع التشفير الذي حددته. تتوافق لغة حزمة التوزيع مع لغة Kaspersky Security Center. في حالة عدم وجود حزمة توزيع من Kaspersky Endpoint Security for Windows للغة Kaspersky Security Center، يتم تحديد حزمة توزيع اللغة الإنجليزية.

في القائمة، يمكنك تحديد لغات حزمة التوزيع عن طريق **إظهار لغة ترجمة وحدة تحكم الإدارة أو** .

التوزيعات التطبيقات المُدارة قد يتطلب تثبيت إصدار أدنى محدد من Kaspersky Security Center.

في القائمة، يمكنك تحديد حزم توزيع من أي نوع تشفير مختلف عن تلك التي حددتها في النافذة **نوع التشفير**. بعد تحديد حزمة توزيع لـ Kaspersky Endpoint Security for Windows، يبدأ تنزيل جميع حزم التوزيع، المقابلة للمكونات والمنصات. يمكنك مراقبة تقدم التنزيل في العمود **حالة التنزيل**. بعد الانتهاء من معالج البدء السريع، يتم عرض حزم تثبيت عميل الشبكة الخاص بنظام التشغيل Windows وتطبيقات Kaspersky المُدارة في **خادم الإدارة** ← **الإعدادات المتقدمة** ← **التثبيت عن بُعد** ← قائمة **حزم التثبيت** .

لإنهاء تنزيل بعض حزم التوزيع، يجب عليك قبول EULA. عند النقر على زر **أوافق** ، يُعرَض نص اتفاقية ترخيص المستخدم النهائي. للمضي قدمًا إلى الخطوة التالية، يجب عليك قبول شروط وأحكام اتفاقية ترخيص المستخدم النهائي وأحكامها وشروط سياسة الخصوصية الخاصة بـ Kaspersky وأحكامها. حدد الخيارات المتعلقة باتفاقية ترخيص المستخدم النهائي وسياسة خصوصية Kaspersky، ثم انقر على زر **قبول الكل**. في حالة عدم قبول الشروط والأحكام، فسيتم إلغاء تنزيل الحزمة.

بعد قبولك لشروط اتفاقية ترخيص المستخدم النهائي وأحكامها وشروط سياسة خصوصية Kaspersky وأحكامها، يستمر تنزيل حزم التوزيع. عند الانتهاء من التنزيل، تُعرَض الحالة **تم إنشاء حزمة التثبيت**. ستستخدم فيما بعد حزم التثبيت لنشر تطبيقات Kaspersky على أجهزة العملاء.

يمكنك إنشاء حزم التثبيت يدويًا، بشكل منفصل عن معالج البدء السريع. انتقل إلى **Administration Server** ← **خيارات متقدمة** ← **التثبيت عن بُعد** ← **حزم التثبيت** في شجرة وحدة تحكم الإدارة.

الخطوة 6. تكوين استخدام Kaspersky Security Network

يمكنك الوصول إلى قواعد بيانات السمعة الخاصة بشبكة Kaspersky Security Networkلضمان استجابات أسرع من قبل تطبيقات Kaspersky للتهديدات، وتحسين فعالية بعض مكونات الحماية، وتقليل مخاطر الإيجابيات الكاذبة.

اقرأ بيان KSN المعروض في النافذة. تحديد الإعدادات لترحيل المعلومات حول عمليات Kaspersky Security Center إلى قاعدة معارف Kaspersky Security Network. حدد أحد الخيارات التالية:

- **أوافق على استخدام Kaspersky Security Network**

  سيقوم Kaspersky Security Center والتطبيقات المدارة المثبتة على الأجهزة العميلة بنقل تفاصيل عملياته تلقائيًا إلى Kaspersky Security Network. تضمن المشاركة في Kaspersky Security Network التحديثات السريعة لقواعد البيانات التي تشتمل على معلومات حول الفيروسات وغيرها من التهديدات، مما يضمن الاستجابة السريعة للتهديدات الأمنية الطارئة.

- **لا أوافق على استخدام Kaspersky Security Network**

  لن يوفر Kaspersky Security Center والتطبيقات المدارة أية معلومات إلى Kaspersky Security Network.

  إذا قمت بتحديد هذا الخيار، فسيتم تعطيل استخدام Kaspersky Security Network.

إذا قمت بتنزيل المكون الإضافي لتطبيق Kaspersky Endpoint Security for Windows، فسيتم عرض عباراتي KSN على حد سواء—عبارة KSN لتطبيق Kaspersky Security Center وعبارة KSN لتطبيق Kaspersky Endpoint Security for Windows. يتم عرض عبارات KSN لتطبيقات Kaspersky الأخرى المُدارة، التي تم تنزيل مكوناتها الإضافية، في نوافذ منفصلة ويتعين عليك قبول (أو عدم قبول) كل عبارة على حدة.

يمكنك أيضا إعداد وصول خادم الإدارة إلى Kaspersky Security Network (KSN) لاحقًا في نافذة خصائص خادم الإدارة لوحدة تحكم الإدارة.

الخطوة 7. تكوين إشعارات البريد الإلكتروني

كوّن إرسال الإشعارات حول الأحداث المسجلة أثناء تشغيل تطبيقات Kaspersky على الأجهزة المُدارة. وسيتم استخدام هذه الإعدادات كإعدادات افتراضية لخادم الإدارة.

لتكوين تسليم الإخطارات المتعلقة بالأحداث التي تجري في تطبيقات Kaspersky، استخدم الإعدادات التالية:

- **المستلمون (عناوين البريد الإلكتروني)**

عناوين البريد الإلكتروني للمستخدمين التي ستقوم التطبيقات بإرسال الإخطارات إليها. يمكنك إدخال عنوان واحد أو أكثر، وفي حالة إدخال أكثر من عنوان، فافصل بينها باستخدام فواصل منقوطة.

- **خوادم SMTP**

عنوان أو عناوين خوادم البريد الخاصة بمؤسستك.

في حالة إدخال أكثر من عنوان واحد، افصل بينها باستخدام فواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

- **منفذ خادم SMTP**

رقم منفذ الاتصال الخاص بخادم SMTP. إذا كنت تستخدم عدة خوادم SMTP، فسيتم إنشاء الاتصال بها من خلال منفذ الاتصال المحدد. رقم المنفذ الافتراضي هو 25.

- **استخدام مصادقة ESMTP**

تمكين دعم مصادقة ESMTP. عند تحديد خانة الاختيار الموجودة في الحقول **اسم المستخدم** و**كلمة المرور**، يمكنك تحديد إعدادات مصادقة ESMTP. تكون خانة الاختيار غير محددة بشكل افتراضي.

- **الإعدادات**

حدد الإعدادات التالية:

- **الموضوع** (اسم موضوع رسالة بريد إلكتروني)
- **عنوان البريد الإلكتروني للمرسل**
- **إعدادات TLS لخادم SMTP**

يمكنك تحديد إعدادات TLS لخادم SMTP:

يمكنك تعطيل استخدام TLS، استخدام TLS إذا كان خادم SMTP يدعم هذا البروتوكول أو يمكنك فرض استخدام TLS فقط. إذا اخترت استخدام TLS فقط، حدد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال عبر أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. إذا اخترت أيضًا استخدام TLS فقط، فيمكنك تحديد شهادة لمصادقة العميل على خادم SMTP.

  - تصفح للوصول إلى ملف شهادة خادم SMTP:

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

  - تصفح للوصول إلى ملف شهادة العميل:

يمكنك استخدام شهادة استلمتها من أي مصدر، على سبيل المثال، من أي جهة إصدار موثوقة. يجب تحديد الشهادة ومفتاحها الخاص باستخدام أحد أنواع الشهادات التالية:

- شهادة X-509:

حدد الملف بالشهادة والملف بالمفتاح الخاص. يمكنك تحميل هذه الملفات بأي ترتيب. عند تحميل كلا الملفين، حدد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- الحاوية pkcs12:

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك بعد ذلك تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

يمكنك اختبار إعدادات إخطار البريد الإلكتروني الجديدة بالنقر فوق الزر **إرسال رسالة اختبار**.

يمكنك أيضًا تكوين إخطارات الحدث لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 8. تكوين إعدادات التحديث

تكوين إعدادات إدارة تحديثات التطبيقات المثبتة على الأجهزة العميلة.

لا يمكنك تكوين هذه الإعدادات إلا إذا كنت قد قدمت مفتاح ترخيص مع خيار إدارة التصحيحات والثغرات الأمنية.

في مجموعة الإعدادات **البحث عن التحديثات وتثبيتها**، يمكنك تحديد وضع البحث عن تحديث Kaspersky Security Center وتثبيته:

- **البحث عن تحديثات مطلوبة**

  يتم إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا، إذا لم يكن لديك واحدة.

  ويتم تحديد هذا الخيار بصورة افتراضية.

- **بحث عن التحديثات المطلوبة وتثبيتها**

  يتم إنشاء مهام بحث عن الثغرات الأمنية والتحديثات المطلوبة وتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية تلقائيًا، إذا لم يكن لديك واحدة.

في مجموعة الإعدادات **Windows Server Update Services**، يمكنك تحديد مصدر مزامنة التحديث:

- **استخدام مصادر التحديث المحددة في سياسة المجال**

ستقوم أجهزة العملاء بتنزيل تحديثات Windows Update وفقًا لإعدادات سياسة المجال الخاصة بك. يتم إنشاء سياسة عميل الشبكة تلقائيًا، إذا لم يكن لديك واحدة.

- **استخدام خادم الإدارة كخادم WSUS**

تقوم أجهزة العملاء بتنزيل تحديثات Windows Update من خادم الإدارة. يتم إنشاء مهمة إجراء مزامنة Windows Update وسياسة عميل الشبكة تلقائيًا، إذا لم يكن لديك واحدة.

يمكنك إنشاء مهمتي البحث عن الثغرات الأمنية والتحديثات المطلوبة وتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية بشكل منفصل عن معالج البدء السريع. لاستخدام خادم الإدارة كخادم WSUS، أنشئ مهمة إجراء مزامنة Windows Update، ثم حدد الخيار **استخدام خادم الإدارة كخادم WSUS** في سياسة عميل الشبكة.

الخطوة 9. إنشاء تكوين حماية أولية

ستعرض النافذة **تكوين الحماية الأولية** قائمة بالسياسات والمهام التي تم إنشاؤها تلقائيًا. يتم إنشاء السياسات والمهام التالية:

- سياسة عميل شبكة Kaspersky Security Center
- سياسات لتطبيقات Kaspersky المُدارة التي تم تثبيت المكونات الإضافية للإدارة مسبقًا
- مهمة صيانة خادم الإدارة
- مهمة النسخ الاحتياطي لبيانات خادم الإدارة
- تنزيل التحديثات إلى مستودع خادم الإدارة
- بحث عن الثغرات الأمنية والتحديثات المطلوبة
- مهمة تثبيت تحديث

انتظار حتى اكتمال إنشاء السياسات والمهام قبل المتابعة إلى الخطوة التالية للمعالج.

إذا قمت بتنزيل المكون الإضافي للحزمة الأولى من Kaspersky Endpoint Security for Windows 10 Service Pack 1 والإصدارات الأحدث حتى الإصدار 11.0.1، أثناء إنشاء السياسات والمهام، فسيتم فتح نافذة لإجراء تكوين أولي للمنطقة الموثوقة الخاصة بـ Kaspersky Endpoint Security for Windows. سيطالبك التطبيق بإضافة الموردين الذين تم التحقق منهم بواسطة Kaspersky في المنطقة الموثوقة لأغراض استثناء تطبيقاتهم من عمليات الفحص لمنع حجبها عن طريق الخطأ. يمكنك الآن إنشاء الاستثناءات المُوصى بها أو إنشاء قائمة استثناءات لاحقًا عن طريق تحديد ما يلي في شجرة وحدة التحكم: **السياسات** ← قائمة خصائص Kaspersky Endpoint Security ← **الحماية من التهديدات المتقدمة** ← **المنطقة الموثوق بها** ← **الإعدادات** ← **إضافة**. تتوفر قائمة الاستثناءات من الفحص للتحرير في أي وقت باستخدام التطبيق.

> يتم إجراء العمليات في المنطقة الموثوق بها باستخدام أدوات مدمجة في Kaspersky Endpoint Security for Windows. للحصول على إرشادات مفصلة حول كيفية تنفيذ العمليات وتوضيح لمزايا التشفير، يرجى الرجوع إلى التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows.

لإنهاء التكوين الأولي للمنطقة الموثوقة والعودة إلى المعالج، انقر على **موافق**.

انقر فوق **التالي**. يتوفر هذا الزر بعد إنشاء جميع السياسات والمهام الضرورية.

يمكنك أيضًا إنشاء المهام و السياسات الطلوبة لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 10. توصيل الأجهزة المحمولة

إذا حددت مسبقًا تمكين نطاق حماية **الأجهزة المحمولة** في إعدادات المعالج، فحدد الإعدادات لتوصيل أجهزة المؤسسة المحمولة التابعة للمؤسسة المُدارة. في حالة عدم تمكين نطاق حماية **الأجهزة المحمولة**، فسيتم تخطي هذه الخطوة.

في هذه الخطوة من المعالج، عليك بالقيام بما يلي:

- تكوين منافذ اتصال الأجهزة المحمولة.
- تكوين مصادقة خادم الإدارة.
- إنشاء الشهادات أو إدارتها.

- إعداد إصدار الشهادات من النوع العام وتحديثها تلقائيًا وتشفيرها.
- إنشاء قاعدة نقل الأجهزة المحمولة

لإعداد منافذ اتصال الأجهزة المحمولة:

1. انقر على الزر **تكوين** الموجود على يمين الحقل **اتصال الجهاز المحمول**.
2. في القائمة المنسدلة، حدد **تكوين منافذ**.
   يتم فتح نافذة خصائص خادم الإدارة التي تعرض القسم **منافذ إضافية**.
3. في القسم **منافذ إضافية**، يمكنك تحديد إعدادات اتصال الجهاز المحمول:
   - **منفذ SSL لخادم وكيل التفعيل**

     رقم منفذ SSL لاتصال Kaspersky Endpoint Security for Windows بخوادم تفعيل Kaspersky.
     رقم المنفذ الافتراضي هو 17000.
   - **فتح منفذ للأجهزة المحمولة**

     يفتح منفذ لاتصال الأجهزة المحمولة بخادم الترخيص. يمكنك تحديد رقم المنفذ والإعدادات الأخرى في الحقول الموضحة أدناه.
     يتم تمكين هذا الخيار افتراضيًا.
   - **منفذ لمزامنة الأجهزة المحمولة**

     رقم المنفذ الذي ستتصل من خلاله الأجهزة المحمولة بخادم الإدارة وستتبادل معه البيانات. رقم المنفذ الافتراضي هو 13292.
     يمكنك تخصيص منفذ مختلف إذا تم استخدام المنفذ 13292 لأغراض أخرى.
   - **المنفذ الخاص بتفعيل جهاز المحمول**

     منفذ اتصال Kaspersky Endpoint Security for Android بخوادم تنشيط Kaspersky.
     رقم المنفذ الافتراضي هو 17100.
   - **فتح منفذ لأجهزة حماية جهاز UEFI وأجهزة KasperskyOS**

     يمكن لأجهزة حماية UEFI الاتصال بخادم الإدارة.
   - **منفذ لأجهزة حماية UEFI وأجهزة KasperskyOS**

     يمكنك تغيير رقم المنفذ إذا تم تمكين الخيار **فتح منفذ لأجهزة حماية جهاز UEFI وأجهزة KasperskyOS**. رقم المنفذ الافتراضي هو 13294.
   - **فتح منفذ بروميثيوس**

     منفذ طلبات سحب نظام Prometheus. رقم المنفذ الافتراضي هو 13296.
4. انقر فوق **موافق** لحفظ التغييرات والعودة إلى معالج البدء السريع.

سيتعين عليك تكوين مصادقة خادم الإدارة بواسطة الأجهزة المحمولة ومصادقة الأجهزة المحمولة بواسطة خادم الإدارة. وإذا كنت ترغب في ذلك، يمكنك تكوين المصادقة لاحقًا، بشكل منفصل من خلال معالج البدء السريع.

لتكوين مصادقة خادم الإدارة بواسطة الأجهزة المحمولة:

1. انقر على الزر **تكوين** الموجود على يمين الحقل **اتصال الجهاز المحمول**.
2. في القائمة المنسدلة، حدد **تكوين مصادقة**.
   يتم فتح نافذة خصائص خادم الإدارة التي تعرض قسم **الشهادات**.

3. حدد خيار المصادقة للأجهزة المحمولة في مجموعة الإعدادات **مصادقة خادم الإدارة من خلال الأجهزة المحمولة**، وحدد خيار المصادقة لأجهزة حماية UEFI في مجموعة الإعدادات **مصادقة خادم الإدارة من خلال أجهزة حماية جهاز UEFI**.

عندما يتبادل خادم الإدارة البيانات مع الأجهزة العميلة، تتم مصادقته عن طريق استخدام شهادة.

يستخدم خادم الإدارة الشهادة التي تم إنشائها أثناء تثبيت خادم الإدارة بشكل افتراضي. إذا كنت ترغب، يمكنك إضافة شهادة جديدة.

لإضافة شهادة جديدة (اختياري):

1. حدد **شهادة أخرى**.

سيظهر الزر **استعراض**.

2. انقر فوق زر **استعراض**.

3. في النافذة التي تفتح، حدد إعدادات الشهادة:

- **نوع الشهادة**

في القائمة المنسدلة يمكنك تحديد نوع الشهادة.

- **الشهادة X.509**. إذا تم تحديد هذا الخيار، فيجب عليك تحديد المفتاح الخاص بشهادة وشهادة مفتوحة:
  - **المفتاح الخاص (.prk, .pem)**. في هذا الحقل، انقر فوق زر **استعراض** لتحديد المفتاح الخاص بشهادة بتنسيق PKCS #8 (*.prk).
  - **المفتاح العام (.cer)**. في هذا الحقل، انقر فوق زر **استعراض** لتحديد مفتاح عام بتنسيق PEM (*.cer).
- **الحاوية PKCS#12**. إذا حددت هذا الخيار، فيمكنك تحديد ملف شهادة بتنسيق P12 أو PFX بالنقر فوق زر **استعراض** وملء حقل **ملف الشهادة**.

- وقت التفعيل:

- **فورًا**

سيتم استبدال الشهادة الحالية فورًا بالشهادة الجديد بعد النقر فوق **موافق**.

سيتعذر على الأجهزة المحمولة المتصلة فيما سبق الاتصال بخادم الإدارة.

- **بعد انتهاء هذه الفترة، أيام**

بعد تحديد هذا الخيار، سيتم إنشاء شهادة احتياطية. سيتم استبدال الشهادة الحالية بالشهادة الجديدة خلال عدد الأيام المحدد. يتم عرض تاريخ سريان الشهادة الاحتياطية في القسم **الشهادات**.

يُوصى بتخطيط إعادة الإصدار مسبقًا. يجب تنزيل شهادة احتياطية على الأجهزة المحمولة قبل انتهاء الفترة المحددة. بعد استبدال الشهادة الحالية بشهادة جديدة، سيتعذر على الأجهزة المحمولة المتصلة مسبقًا الاتصال بخادم الإدارة.

4. انقر فوق الزر **خصائص** لعرض إعدادات شهادة خادم الإدارة التي تم تحديدها.

لإعادة إصدار الشهادة الصادرة من خلال خادم الإدارة:

1. حدد **تم إصدار الشهادة من خلال خادم الإدارة**.

2. انقر فوق زر **جارٍ إعادة الإصدار**.

3. في النافذة التي تفتح، حدد الإعدادات التالية:

- عنوان الاتصال:

- **استخدام عنوان اتصال قديم**

عنوان خادم الإدارة الذي تتصل به الأجهزة المحمولة لم تطرأ عليه تغييرات بعد.

ويتم تحديد هذا الخيار بصورة افتراضية.

- **تغيير عنوان الاتصال إلى**

إذا كنت ترغب في اتصال الأجهزة المحمولة بعنوان آخر، فحدد العنوان ذي الصلة في هذا الحقل.

إذا حدث تغيير في عنوان اتصال الجهاز المحمول، فيجب إصدار شهادة جديدة. ستصبح الشهادة القديمة غير صالحة على جميع الأجهزة المحمولة المتصلة. سيتعذر على الأجهزة المتصلة فيما سبق الاتصال بخادم الإدارة ولذلك لن تتم إدارتها.

- وقت التفعيل:

- **فورًا**

سيتم استبدال الشهادة الحالية فورًا بالشهادة الجديد بعد النقر فوق **موافق**.

سيتعذر على الأجهزة المحمولة المتصلة فيما سبق الاتصال بخادم الإدارة.

- **بعد انتهاء هذه الفترة، أيام**

بعد تحديد هذا الخيار، سيتم إنشاء شهادة احتياطية. سيتم استبدال الشهادة الحالية بالشهادة الجديدة خلال عدد الأيام المحدد. يتم عرض تاريخ سريان الشهادة الاحتياطية في القسم **الشهادات**.

يُوصى بتخطيط إعادة الإصدار مسبقًا. يجب تنزيل شهادة احتياطية على الأجهزة المحمولة قبل انتهاء الفترة المحددة. بعد استبدال الشهادة الحالية بشهادة جديدة، سيتعذر على الأجهزة المحمولة المتصلة مسبقًا الاتصال بخادم الإدارة.

4. انقر فوق **موافق** لحفظ التغييرات والعودة إلى النافذة **الشهادات**.

5. انقر فوق **موافق** لحفظ التغييرات والعودة إلى معالج البدء السريع.

لإعداد إصدار شهادات من النوع العام وتحديثها تلقائيًا وتشفيرها لتحديد الأجهزة المحمولة بواسطة خادم الإدارة:

1. انقر فوق الزر **تكوين** الموجود على يمين الحقل **مصادقة جهاز المحمول**.

يتم فتح النافذة **قواعد إصدار الشهادات**، وعرض القسم **إصدار شهادات المحمول**.

2. إذا لزم الأمر، قم بتحديد الإعدادات التالية في القسم **إعدادات الإصدار**:

- **مدة بقاء الشهادة، الأيام**

مدة بقاء الشهادة بالأيام. مدة البقاء الافتراضية للشهادة هي 365 يومًا. عند انتهاء صلاحية هذه الشهادة، سيتعذر على الجهاز المحمول الاتصال بخادم الإدارة.

- **مصدر الشهادة**

حدد مصدر الشهادات من النوع العام للأجهزة المحمولة: يتم إصدار الشهادات من قبل خادم الإدارة أو يتم تحديدها يدويًا.

يمكنك تعديل قوالب الشهادات إذا تم تكوين التكامل مع البنية الأساسية للمفاتيح العامة (PKI) في القسم **التكامل مع PKI**. في هذه الحالة، تتوفر حقول التحديد التالية في القالب:

- **القالب الافتراضي**

استخدام شهادة صادرة بواسطة مصدر شهادة خارجي – مركز الشهادات – باستخدام القالب الافتراضي.

يتم تحديد هذا الخيار افتراضيًا.

- **قالب آخر**

حدد قالبًا مستخدم في إصدار الشهادات. يمكنك تحديد قوالب شهادة في المجال. يؤدي النقر فوق الزر **تحديث القائمة** إلى تحديث قائمة قوالب الشهادة.

3. إذا لزم الأمر، حدد الإعدادات التالية لإصدار الشهادات تلقائيًا في القسم **إعدادات التحديثات التلقائية**:

- **التجديد عند انتهاء صلاحية الشهادة خلال (أيام)**

عدد الأيام المتبقية على انتهاء صلاحية الشهادة حيث ينبغي خلالها إصدار شهادة جديدة من قبل خادم الإدارة. على سبيل المثال، إذا كانت قيمة الحقل هي 4، فيصدر خادم الإدارة شهادة جديدة قبل أربعة أيام من انتهاء صلاحية الشهادة الحالية. القيمة الافتراضية هي 7.

- **إعادة إصدار الشهادة تلقائيًا إن أمكن**

حدد هذا الخيار لإعادة إصدار شهادة تلقائيًا لعدد الأيام المحدد في حقل **التجديد عند انتهاء صلاحية الشهادة خلال (أيام)**. إذا تم تعريف الشهادة يدويًا، فلا يمكن تجديدها تلقائيًا، ولن يعمل الخيار المُمكّن.

يتم تعطيل هذا الخيار افتراضيًا.

يتم إعادة إصدار الشهادات تلقائيًا من قبل هيئة إصدار الشهادات.

4. عند اللزوم، في قسم الإعدادات **حماية بكلمة مرور**، قم بتحديد الإعدادات لفك تشفير الشهادات أثناء التثبيت.

حدد خيار **المطالبة بكلمة مرور أثناء تثبيت الشهادة** لمطالبة المستخدم بكلمة المرور عند تثبيت الشهادة على جهاز محمول. يتم استخدام كلمة المرور مرة واحدة فقط—وذلك أثناء تثبيت الشهادة على الجهاز المحمول.

سيتم إنشاء كلمة المرور تلقائيًا بواسطة خادم الإدارة وتُرسل إلى البريد الذي حددته. يمكنك تحديد عنوان البريد الإلكتروني للمستخدم أو عنوان البريد الإلكتروني الخاص بك إذا كنت ترغب في استخدام طريقة أخرى لإعادة توجيه كلمة المرور إلى المستخدم.

يمكنك استخدام الشريحة لتحديد عدد الأحرف المضمنة في كلمة مرور فك تشفير الشهادة.

خيار المطالبة بكلمة المرور مطلوب، على سبيل المثال، لحماية شهادة مشتركة في حزمة تثبيت مستقلة لـ Kaspersky Endpoint Security for Android. ستمنع الحماية بكلمة مرور المتسللين من الوصول إلى الشهادة المشتركة عن طريق سرقة حزمة التثبيت المستقلة من Kaspersky Security Center Web Server.

إذا تم تعطيل هذا الخيار، سيتم فك تشفير الشهادة تلقائيًا أثناء التثبيت ولن تتم مطالبة المستخدم بكلمة المرور. يتم تعطيل هذا الخيار افتراضيًا.

5. انقر فوق **موافق** لحفظ التغييرات والعودة إلى نافذة معالج البدء السريع.

انقر فوق الزر **إلغاء** للعودة إلى معالج البدء السريع دون حفظ أي من التغييرات التي أُجريت.

لتمكين وظيفة نقل الأجهزة المحمولة إلى مجموعة الإدارة التي حددتها،

في حقل **النقل التلقائي للأجهزة المحمولة**، حدد خيار **إنشاء قاعدة نقل للأجهزة المحمولة**.

في حالة تحديد خيار **إنشاء قاعدة نقل للأجهزة المحمولة**، سيقوم التطبيق تلقائيًا بإنشاء قاعدة نقل لنقل الأجهزة التي تعمل بنظم التشغيل Android وiOS إلى المجموعة **الأجهزة المُدارة**:

- باستخدام أنظمة تشغيل Android المثبّت عليها Kaspersky Endpoint Security for Android وشهادة الجهاز المحمول
- باستخدام أنظمة تشغيل iOS المثبت عليها ملف تعريف iOS MDM ذي الشهادة المشتركة

إذا كانت هذه القاعدة موجودة بالفعل، فلن يقوم التطبيق بإنشائها مرة أخري.

يتم تعطيل هذا الخيار افتراضيًا.

لم يعد Kaspersky يدعم Kaspersky Safe Browser بعد الآن.

الخطوة 11. تنزيل التحديثات

يتم تلقائيًا تنزيل تحديثات قواعد بيانات مكافحة الفيروسات الخاصة بـ Kaspersky Security Center وتطبيقات Kaspersky المُدارة. يتم تنزيل التحديثات من خوادم Kaspersky.

لتنزيل التحديثات بشكل منفصل عن معالج البدء السريع، قم بإنشاء وتكوين تحديثاتالتنزيل إلى مهمة مستودع خادم الإدارة.

الخطوة 12. اكتشاف الأجهزة

ستعرض النافذة **استقصاء الشبكة** معلومات حول حالة استقصاء الشبكة الذي تم إجراؤه بواسطة خادم الإدارة.

يمكنك عرض أجهزة الشبكة التي اكتشفها خادم الإدارة والحصول على تعليمات حول التعامل مع النافذة **اكتشاف الأجهزة** عن طريق النقر فوق الروابط الموجودة في الجانب السفلي من النافذة.

يمكنك التحقق من إرسال البيانات على شبكتك لاحقًا، بشكل منفصل عن معالج البدء السريع. واستخدم وحدة التحكم الإدارة لتكوين التحقق من إرسال البيانات في مجالات Windows وActive Directory ونطاقات IP وشبكات IPv6.

الخطوة 13. إغلاق معالج البدء السريع

في نافذة إكمال معالج البدء السريع، حدد خيار **تشغيل معالج التثبيت عن بُعد** إذا كنت ترغب في بدء التثبيت التلقائي لتطبيقات مكافحة الفيروسات و/أو عميل الشبكة على الأجهزة الموجودة في شبكتك.

لإكمال المعالج، انقر على زر **إنهاء**.

تكوين اتصال وحدة تحكم الإدارة بخادم الإدارة

وحدة تحكم الإدارة متصلة بخادم الإدارة عبر منفذ SSL TCP 13291. يمكن استخدام نفس المنفذ بواسطة عناصر أتمتة klakaut.

يمكن استخدام منفذ TCP 14000 للاتصال بوحدة تحكم الإدارة ونقاط التوزيع وخوادم الإدارة الثانوية وكائنات التشغيل التلقائي لـ klakaut بالإضافة إلى تلقي البيانات من الأجهزة العميلة.

عادةً، لا يمكن استخدام منفذ SSL TCP 13000 إلا بواسطة عميل الشبكة وخادم الإدارة الثانوي وخادم الإدارة الرئيسي في منطقة الأجهزة الموصلة مباشرة بالإنترنت. وفي بعض الحالات، قد يلزم اتصال وحدة تحكم الإدارة عبر منفذ SSL 13000:

- إذا كان من المحتمل استخدام منفذ SSL واحد لوحدة تحكم الإدارة ولأنشطة أخرى (تلقي بيانات من الأجهزة العميلة والاتصال بنقاط التوزيع والاتصال بخوادم الإدارة الثانوية).
- إذا كان كائن التشغيل التلقائي لـ klakaut غير متصل بخادم الإدارة مباشرة لكنه متصل عبر نقطة توزيع في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

للسماح باتصال وحدة تحكم الإدارة عبر منفذ 13000:

1. افتح سجل النظام الخاص بالجهاز المثبت عليه خادم الإدارة (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** ← **تشغيل**).
2. انتقل إلى الخلية التالية:
   - لأنظمة 32 بت:

     KLLIM\independent.\core.\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE
   - لأنظمة 64 بت:

     ndependent.\core.\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE

3. بالنسبة لمفتاح LP_ConsoleMustUsePort13291 (DWORD)، قم بتحديد رقم 00000000 باعتباره القيمة.

1 هو القيمة الافتراضية المحددة لهذا المفتاح.

4. قم بإعادة تشغيل خدمة خادم الإدارة.

سيمكنك الآن توصيل وحدة تحكم الإدارة بخادم الإدارة عبر منفذ 13000.

تكوين إعدادات الوصول إلى الإنترنت لخادم الإدارة

يجب تكوين الوصول إلى الإنترنت لاستخدام Kaspersky Security Network، ولتنزيل تحديثات لقواعد بيانات مكافحة الفيروسات لتطبيق Kaspersky Security Center وتطبيقات Kaspersky المُدارة.

لتحديد إعدادات الوصول إلى الإنترنت لخادم الإدارة:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة، انتقل إلى **خيارات متقدمة** ← **تكوين وصول الإنترنت**.

4. حدد خيار **استخدام الخادم الوكيل** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. إذا تم تحديد هذا الخيار، ستتوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

- **العنوان**

  عنوان الخادم الوكيل المستخدم لاتصال Kaspersky Security Center بالإنترنت.

- **رقم المنفذ**

  رقم المنفذ الذي سيتم من خلاله إنشاء اتصال وكيل Kaspersky Security Center.

- **تجاوز الخادم الوكيل للعناوين المحلية**

  لن يتم استخدام خادم وكيل للاتصال بالأجهزة في الشبكة المحلية.

- **مصادقة الخادم الوكيل**

  إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

  يتوفر حقل الإدخال هذا إذا تم تحديد خانة الاختيار **استخدام الخادم الوكيل**.

- **اسم المستخدم**

  حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

- **كلمة المرور**

  تم تعيين كلمة مرور بواسطة المستخدم الذي تم إنشاء اتصال الخادم الوكيل من خلال حسابه (هذا الحقل متاح في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

  لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار** حتى تظهر لك كلمة المرور.

يمكنك أيضًا تكوين الوصول إلى الإنترنت باستخدام معالج البدء السريع.

توصيل الأجهزة خارج المكتب

يصف هذا السيناريو كيفية توصيل الأجهزة الموجودة خارج المكتب (المدارة والموجودة خارج نطاق الشبكة الرئيسية) بخادم الإدارة.

السيناريو: توصيل الأجهزة الموجودة خارج المكتب عن طريق بوابة الاتصال

يوضح هذا السيناريو كيفية توصيل الأجهزة المدارة والموجودة خارج الشبكة الرئيسية بخادم الإدارة.

المتطلبات الأساسية

السيناريو له متطلبات أساسية كالآتي:

- يتم تنظيم منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ) في شبكة مؤسستك.
- يتم نشر خادم إدارة Kaspersky Security Center على شبكة الشركة.

المراحل

يستمر هذا السيناريو على مراحل:

1. **تحديد جهاز عميل في منطقة الأجهزة الموصلة مباشرة بالإنترنت**

   سيتم استخدام هذا الجهاز كبوابة اتصال. يجب أن يستوفي الجهاز الذي تحدده متطلبات بوابات الاتصال.

2. **تثبيت دور عميل الشبكة في بوابة الاتصال**

   نوصي باستخدام التثبيت المحلي لتثبيت عميل الشبكة على الجهاز المحدد.

   بشكلٍ افتراضي، يوجد ملف التثبيت في:\\<server name>\KLSHARE\PkgInst\<version number>_NetAgent

   في النافذة **بوابة الاتصال** في معالج إعداد عميل الشبكة، حدد **استخدام عميل الشبكة كبوابة اتصال في DMZ**. ينشط هذا الوضع دور بوابة الاتصال بشكل متزامن، ويطلب من عميل الشبكة انتظار الاتصالات من خادم الإدارة بدلاً من إنشاء الاتصالات بخادم الإدارة.

   بدلاً من ذلك، يمكنك تثبيت عميل الشبكة على جهاز Linux وتكوين عميل الشبكة للعمل كبوابة اتصال، ولكن انتبه إلى قائمة قيود عميل الشبكة الذي يعمل على أجهزة Linux.

3. **السماح بالاتصالات بجدران الحماية على بوابة الاتصال**

   للتأكد من أن خادم الإدارة يمكنه الاتصال فعليًا ببوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت، اسمح بالاتصالات بمنفذ TCP رقم 13000 في جميع جدران الحماية بين خادم الإدارة وبوابة الاتصال.

   إذا لم يكن لبوابة الاتصال عنوان IP حقيقي على الإنترنت ولكنها تقع خلف ترجمة عنوان الشبكة (NAT)، فقم بتكوين قاعدة لإعادة توجيه الاتصالات من خلال ترجمة عنوان الشبكة.

4. **قم بإنشاء مجموعة إدارة للأجهزة الخارجية**

   أنشئ مجموعة جديدة تحت مجموعة **الأجهزة المُدارة**. المجموعة الجديدة ستحتوي على الأجهزة المُدارة الخارجية.

5. **توصيل بوابة الاتصال بخادم الإدارة**

تنتظر بوابة الاتصال التي قمت بتكوينها اتصالاً من خادم الإدارة. ومع ذلك، لا يقوم خادم الإدارة بإدراج الجهاز وبوابة الاتصال بين الأجهزة المدارة. وذلك لأن بوابة الاتصال لم تحاول إنشاء اتصال بخادم الإدارة. لذلك، تحتاج إلى القيام بإجراء خاص للتأكد من أن خادم الإدارة ينشأ اتصالاً ببوابة الاتصال.

قم بما يلي:

1. أضف بوابة الاتصال كنقطة توزيع.
2. انقل بوابة الاتصال من مجموعة **الأجهزة غير المعينة** إلى المجموعة التي قمت بإنشائها للأجهزة الخارجية.

تم توصيل بوابة الاتصال وتكوينها.

6 **توصيل الأجهزة المكتبية الخارجية بخادم الإدارة**

في العادة، لا يتم نقل الأجهزة المكتبية الخارجية داخل المحيط. لذلك أنت بحاجة إلى تكوينها للاتصال بخادم الإدارة من خلال البوابة عند تثبيت عميل الشبكة.

7 **إعداد تحديثات الأجهزة المكتبية الخارجية**

إذا تم تكوين تحديثات تطبيقات الأمان بحيث يتم تنزيلها من خادم الإدارة، فستقوم الأجهزة الخارجية بتنزيل التحديثات من خلال بوابة الاتصال. هذا الأمر له عيبان:

- هذه حركة مرور غير ضرورية، تستهلك عرض النطاق الترددي لقناة الاتصال عبر الإنترنت الخاصة بالشركة.
- هذه ليست بالضرورة أسرع طريقة للحصول على التحديثات. من المحتمل جدًا أنه سيكون من الأرخص والأسرع أن تتلقى الأجهزة الخارجية التحديثات من خوادم Kaspersky.

قم بما يلي:

1. انقل جميع الأجهزة الخارجية إلى مجموعة الإدارة المنفصلة التي سبق لك إنشاؤها.
2. استبعد المجموعة ذات الأجهزة الخارجية من مهمة التحديث.
3. قم بإنشاء مهمة تحديث منفصلة للمجموعة ذات الأجهزة الخارجية.

8 **توصيل أجهزة الكمبيوتر المحمولة المتنقلة بخادم الإدارة**

تقع أجهزة الكمبيوتر المحمولة المتنقلة في نطاق الشبكة في بعض الأحيان وخارجها في أوقات أخرى. للإدارة الفعالة، أنت بحاجة للاتصال بخادم الإدارة بشكل مختلف حسب موقعها. للاستخدام الفعال لحركة المرور، يتطلب أيضًا تلقي تحديثات من مصادر مختلفة حسب موقعها.

أنت بحاجة إلى تكوين القواعد للمستخدمين خارج المكتب : ملفات تعريف الاتصال وأوصاف موقع الشبكة. تحدد كل قاعدة خادم الإدارة الذي يلزم اتصاله بأجهزة الكمبيوتر المحمولة المتنقلة بناءً على موقعها وخادم الإدارة الذي يتطلب تلقي التحديثات منه.

السيناريو: توصيل الأجهزة خارج المكتب من خلال خادم إدارة ثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)

إذا كنت تريد توصيل الأجهزة المدارة الموجودة خارج الشبكة الرئيسية بخادم الإدارة، يمكنك فعل ذلك باستخدام خادم إدارة ثانوي موجود في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ).

المتطلبات الأساسية

قبل البدء، تأكد من إجرائك لما يلي:

- يتم تنظيم منطقة أجهزة موصلة مباشرة بالإنترنت (DMZ) في شبكة مؤسستك.
- يتم نشر خادم إدارة Kaspersky Security Center على الشبكة الداخلية للمؤسسة.

المراحل

يستمر هذا السيناريو على مراحل:

1. **تحديد جهاز عميل في منطقة الأجهزة الموصلة مباشرة بالإنترنت**

   في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، حدد جهاز العميل الذي سيتم استخدامه كخادم إدارة ثانوي.

2. **تثبيت خادم إدارة Kaspersky Security Center**

   قم بتثبيت خادم إدارة Kaspersky Security Center على جهاز العميل هذا:

3. **إنشاء تسلسل هرمي لخوادم الإدارة**

   إذا وضعت خادم إدارة ثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، فيجب أن يتلقى خادم الإدارة الثانوي اتصالاً من خادم الإدارة الأساسي. ولكي تفعل هذا، أضف خادم إدارة جديد كخادم تابع وبذلك يمكن لخادم الإدارة الرئيسي الاتصال بخادم الإدارة الثانوي عبر المنفذ 13000. عند الجمع بين خادمي إدارة في تسلسل هرمي، تأكد من أنه يمكن الوصول إلى المنفذ 13291 على خادمي الإدارة كليهما. تتصل وحدة تحكم الإدارة بخادم إدارة عبر المنفذ 13291.

4. **توصيل الأجهزة المُدارة خارج المكتب بخادم الإدارة الثانوي**

   يمكنك توصيل الأجهزة خارج المكتب بخادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ) بالطريقة نفسها التي يتم استخدامها لإنشاء الاتصال بين خادم الإدارة والأجهزة المدارة الموجودة في الشبكة الرئيسية. تبدأ الأجهزة المدارة خارج المكتب الاتصال عبر المنفذ 13000.

حول توصيل الأجهزة خارج المكتب

دائمًا ما تقع بعض الأجهزة المُدارة خارج نطاق الشبكة الرئيسية (على سبيل المثال، الأجهزة في الفروع الإقليمية للشركة؛ الأكشاك وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ الأجهزة في المكاتب المنزلية للموظفين). تنتقل بعض الأجهزة خارج المحيط من وقت لآخر (على سبيل المثال، أجهزة الكمبيوتر المحمولة بالمستخدمين الذين يزورون الفروع الإقليمية أو مكاتب العملاء).

ما زلت بحاجة إلى مراقبة حماية الأجهزة خارج المكتب وإدارتها – تلقي معلومات فعلية حول حالة الحماية الخاصة بهم والحفاظ على تطبيقات الأمان الموجودة عليها في حالة محدثة. هذا الأمر ضروري لأنه، على سبيل المثال، إذا تم اختراق مثل هذا الجهاز أثناء وجوده بعيدًا عن الشبكة الرئيسية، فقد يصبح منصة لنشر التهديدات بمجرد اتصاله بالشبكة الرئيسية. لتوصيل الأجهزة خارج المكتب بخادم الإدارة، يمكنك استخدام طريقتين:

- بوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)

  اطلع على نظام حركة مرور البيانات: خادم الإدارة الموجود في الشبكة المحلية، والأجهزة المدارة على الإنترنت، وبوابة الاتصال المستخدمة بالفعل

- خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت

  اطلع على نظام حركة مرور البيانات: خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت والأجهزة المدارة على الإنترنت

بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت

الطريقة الموصى بها لتوصيل الأجهزة الموجودة خارج المكتب بخادم الإدارة هي تنظيم منطقة الأجهزة الموصلة مباشرة بالإنترنت في شبكة المؤسسة وتثبيت بوابة اتصال فيها. ستتصل الأجهزة الخارجية ببوابة الاتصال، وسيبدأ خادم الإدارة الموجود بداخل الشبكة الاتصال بالأجهزة عبر بوابة الاتصال.

بالمقارنة مع الطريقة الأخرى، تعد هذه الطريقة أكثر أمانًا:

- فهي لا تحتاج إلى فتح الوصول إلى خادم الإدارة من خارج الشبكة.
- لا تشكل بوابة الاتصال المخترقة خطراً كبيراً على سلامة الأجهزة المتصلة بالشبكة. لا تدير بوابة الاتصال أي شيء فعليًا ولا تنشئ أي اتصالات.

ولا تتطلب بوابة الاتصال أيضًا توفر العديد من موارد الأجهزة.

ومع ذلك، فإن هذه الطريقة بها عملية تكوين أكثر تعقيدًا:

- لجعل جهاز يعمل كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت، يتطلب منك تثبيت عميل الشبكة وتوصيله بخادم الإدارة بطريقة محددة.
- لن تتمكن من استخدام نفس العنوان للاتصال بخادم الإدارة في جميع الحالات. في حالة الخروج عن المحيط، لن تحتاج فقط إلى استخدام عنوان مختلف (عنوان بوابة الاتصال)، ولكن سيتطلب منك أيضًا استخدام وضع اتصال مختلف: من خلال بوابة الاتصال.
- كما يتطلب منك تحديد إعدادات اتصال مختلفة لأجهزة الكمبيوتر المحمولة في مواقع مختلفة.

لإضافة بوابة اتصال إلى شبكة تم تكوينها مسبقًا:

1. قم بتثبيت عميل الشبكة في وضع بوابة الاتصال.
2. أعد تثبيت عميل الشبكة على الأجهزة التي تريد توصيلها ببوابة الاتصال المضافة حديثًا.

خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت

هناك طريقة أخرى وهي تثبيت خادم إدارة واحد في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

هذا التكوين أقل أمانًا من الطريقة الأخرى. لإدارة أجهزة الكمبيوتر المحمولة الخارجية في هذه الحالة، يجب أن يقبل خادم الإدارة الاتصالات من أي عنوان على الإنترنت. سيستمر في إدارة جميع الأجهزة ضمن الشبكة الداخلية، لكن من منطقة الأجهزة الموصلة مباشرة بالإنترنت. لذا، قد يتسبب الخادم الذي تم اختراقه في إحداث قدر هائل من الضرر، على الرغم من انخفاض احتمالية وقوع مثل هذا الحدث.

ينخفض الخطر بشكل ملحوظ إذا كان خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت لا يدير الأجهزة ضمن الشبكة الداخلية. يمكن لمزود الخدمة استخدام هذا التكوين، على سبيل المثال، لإدارة أجهزة العملاء.

قد ترغب في استخدام هذه الطريقة في الحالات التالية:

- إذا كنت معتادًا على تثبيت خادم الإدارة وتكوينه ولا ترغب في القيام بإجراء آخر لتثبيت بوابة الاتصال وتكوينها.
- إذا كنت بحاجة إلى إدارة المزيد من الأجهزة. تبلغ السعة القصوى لخادم الإدارة 100 000 جهاز، بينما يمكن لبوابة الاتصال أن تدعم ما يصل إلى 10 000 جهاز.

لهذا الحل أيضًا صعوبات محتملة:

- يتطلب خادم الإدارة توفر المزيد من موارد الأجهزة وقواعد بيانات أخرى.
- سيتم تخزين المعلومات بشأن الأجهزة في قاعدتي بيانات غير مرتبطين بها (بخادم الإدارة الموجود داخل الشبكة وآخر في منطقة الأجهزة الموصلة مباشرة بالإنترنت)، مما يعقد المراقبة.
- لإدارة جميع الأجهزة، يجب ضم خادم الإدارة في شكل تسلسل هرمي، مما يعقد المراقبة وكذلك الإدارة. يفرض مثيل خادم الإدارة الثانوي قيودًا على الهياكل المحتملة لمجموعات الإدارة. عليك أن تقرر طريقة وماهية المهام والسياسات لتوزيعها على مثيل خادم الإدارة الثانوي.
- يعد تكوين الأجهزة الخارجية لاستخدام خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت من الخارج واستخدام خادم الإدارة الرئيسي من الداخل معقدًا أكثر من مجرد تكوينها لاستخدام اتصال مشروط من خلال بوابة.
- مخاطر أمنية عالية. يُعرّض مثيل خادم الإدارة المخترق أجهزة الكمبيوتر المحمولة المدارة للاختراق بسهولة. في حالة حدوث ذلك، يحتاج المخترقون فقط إلى انتظار عودة أحد أجهزة الكمبيوتر المحمولة إلى الاتصال بشبكة المؤسسة حتى يتمكنوا من مواصلة هجومهم على شبكة المنطقة المحلية.

توصيل الأجهزة المكتبية الخارجية بخادم الإدارة

لا يمكن توصيل الأجهزة المكتبية التي دائمًا ما تكون خارج الشبكة الرئيسية (على سبيل المثال، الأجهزة في الفروع الإقليمية للشركة؛ الأكشاك وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ الأجهزة في المكاتب المنزلية للموظفين) بخادم الإدارة مباشرةً. يجب أن تكون متصلة بخادم الإدارة عبر بوابة اتصال مثبتة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ). ويتم إجراء هذا التكوين عند تثبيت عميل الشبكة على تلك الأجهزة.

لتوصيل الأجهزة المكتبية الخارجية بخادم الإدارة:

1. قم بإنشاء حزمة تثبيت جديدة لعميل الشبكة.

2. افتح خصائص حزمة التثبيت التي تم إنشاؤها، وانتقل إلى قسم **الخيارات المتقدمة**، ثم حدد خيار **الاتصال بخادم الإدارة باستخدام بوابة الاتصال**.

إعداد **الاتصال بخادم الإدارة باستخدام بوابة الاتصال** غير متوافق مع إعداد **استخدام عميل الشبكة كبوابة اتصال في DMZ**. لا يمكنك تمكين هذين الإعدادين في نفس الوقت.

3. في **عنوان بوابة الاتصال**، حدد العنوان العام لبوابة الاتصال.

إذا كانت بوابة الاتصال موجودة خلف ترجمة عنوان الشبكة (NAT) وليس لها عنوان عام خاص بها، فقم بتكوين قاعدة بوابة NAT لإعادة توجيه الاتصالات من العنوان العام إلى العنوان الداخلي لبوابة الاتصال.

4. قم بإنشاء حزمة تثبيت مستقلة بناءً على حزمة التثبيت التي تم إنشاؤها.

5. قم بتسليم حزمة التثبيت المستقلة للأجهزة المستهدفة إما إلكترونيًا أو على محرك أقراص قابل للإزالة.

6. قم بتثبيت عميل الشبكة من الحزمة المستقلة.

الأجهزة المكتبية الخارجية متصلة بخادم الإدارة.

حول ملفات التعريف الخاصة باتصال المستخدمين المتواجدين خارج المكتب

قد يحتاج مستخدمو الكمبيوتر المحمول خارج المكتب (يُشار إليهم فيما بعد باسم "الأجهزة") إلى تغيير طريقة الاتصال بخادم الإدارة أو التبديل بين خوادم الإدارة بناءً على الموقع الحالي للجهاز على شبكة المؤسسة.

إن ملفات تعريف الاتصال مدعومة فقط للأجهزة التي تعمل بنظام Windows و macOS.

استخدام عناوين مختلفة لخادم إدارة واحد

الأجهزة المثبت عليها عميل الشبكة يمكنها الاتصال بخادم الإدارة إما من إنترانت المؤسسة أو من الإنترنت. قد يتطلب هذا الموقف من عميل الشبكة استخدام عناوين مختلفة للاتصال بخادم الإدارة: عنوان خادم الإدارة الخارجي للاتصال بالإنترنت وعنوان خادم الإدارة الداخلي للاتصال بالشبكة الداخلية.

للقيام بذلك، يجب عليك إضافة ملف تعريف (للاتصال بخادم الإدارة من الإنترنت) إلى سياسة عميل الشبكة. أضف ملف التعريف في خصائص السياسة (قسم **الاتصال**، القسم الفرعي **ملفات تعريف الاتصال**). في نافذة إنشاء ملف التعريف، يجب عليك تعطيل خيار **الاستخدام لاستلام التحديثات فقط**، وتحديد خيار **مزامنة إعدادات الاتصال مع إعدادات خادم الإدارة المحددة في ملف التعريف هذا**. إذا كنت تستخدم بوابة اتصال للوصول إلى خادم الإدارة (على سبيل المثال تكوين Kaspersky Security Center كما هو موضح في الوصول إلى الإنترنت: عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت)، فيجب عيك تحديد عنوان بوابة الاتصال في الحقل المقابل لملف تعريف الاتصال.

التبديل بين خوادم الإدارة بناءً على الشبكة الحالية

إذا كان للمؤسسة مكاتب متعددة بها خوادم إدارة مختلفة وتنتقل بعض الأجهزة المثبّت عليها عميل الشبكة فيما بينها، فأنت تحتاج لتوصيل عميل الشبكة بخادم الإدارة الخاص بالشبكة المحلية في المكتب الذي يوجد به الجهاز حاليًا.

في هذه الحالة، يجب إنشاء ملف تعريف للاتصال بخادم الإدارة في خصائص سياسة عميل الشبكة لكل مكتب من المكاتب، ماعدا المكتب الرئيسي الذي يوجد به خادم الإدارة الرئيسي. يجب عليك تحديد عناوين خوادم الإدارة في ملفات تعريف الاتصال وتمكين أو تعطيل خيار **الاستخدام لاستلام التحديثات فقط**:

- حدد الخيار إذا كنت تريد مزامنة عميل الشبكة باستخدام خادم الإدارة الرئيسي، بينما تستخدم الخادم المحلي لتنزيل التحديثات فقط.
- قم تعطيل هذا الخيار إذا كان يلزم إدارة عميل الشبكة بالكامل بواسطة خادم الإدارة المحلي.

بعد ذلك، يجب عليك إعداد شروط التحويل إلى ملفات التعريف التي تم إنشاؤها حديثًا: على الأقل شرط واحد لكل مكتب من المكاتب، ما عدا المكتب الرئيسي. يتكون غرض كل شرط من الشروط من الكشف عن العناصر الخاصة لبيئة شبكة مكتب ما. إذا تحقق شرط ما، يتم تنشيط ملف التعريف المقابل له. إن لم يتحقق شرط من الشروط، يتم تبديل عميل الشبكة إلى خادم الإدارة الرئيسي.

إنشاء ملف تعريف خاص باتصال المستخدمين المتواجدين خارج المكتب

يتوفر ملف تعريف اتصال خادم الإدارة فقط على الأجهزة التي تعمل بنظام Windows و macOS.

لإنشاء ملف تعريف لاتصال عميل الشبكة بخادم الإدارة للمستخدمين خارج المكتب:

1. في شجرة وحدة التحكم، حدد مجموعة إدارة التي تحتوي على الأجهزة العميلة التي تريد لأجلها إنشاء ملف تعريف لاتصال عميل الشبكة بخادم الإدارة.
2. قم بأحد الإجراءات التالية:
   - إذا أردت إنشاء ملف تعريف اتصال لجميع الأجهزة في المجموعة، حدد سياسة عميل الشبكة في مساحة عمل المجموعة، في علامة التبويب **السياسات**. افتح نافذة الخصائص التابعة للسياسة المحددة.
   - إذا أردت إنشاء ملف تعريف اتصال لجهاز في مجموعة، فحدد هذا الجهاز في مساحة عمل المجموعة، على علامة التبويب **الأجهزة**، وقم بتنفيذ الإجراءات التالية:
     a. افتح نافذة الخصائص التابعة للجهاز المحدد.
     b. في القسم **التطبيقات** الخاص بنافذة خصائص الجهاز، حدد عميل الشبكة.
     c. افتح نافذة خصائص عميل الشبكة.
3. في نافذة الخصائص، في قسم **الاتصال**، حدد القسم الفرعي **ملفات تعريف الاتصال**.
4. من مجموعة الإعدادات **ملفات تعريف اتصال خادم الإدارة**، انقر فوق الزر **إضافة**.

بشكل افتراضي، قائمة ملفات تعريف الاتصال تحتوي على ملفات تعريف <وضع غير متصل> و<خادم الإدارة الرئيسي>. لا يمكن تعديل ملفات التعريف أو إزالتها.

لا يحدد <Offline mode> أي خادم للاتصال. لذلك، لا يحاول عميل الشبكة، عند الانتقال إلى ملف التعريف ذاك، الاتصال بأي خادم إدارة بينما تعمل التطبيقات المثبتة على الأجهزة العميلة بموجب سياسات العمل المتعلقة بحالات خارج المكتب. يمكن استخدام ملف تعريف <وضع غير متصل> في حالة فصل الأجهزة عن الشبكة.

يحدد ملف التعريف <Home Administration Server> الاتصال بخادم الإدارة الذي تم تحديده أثناء تثبيت عميل الشبكة. يتم تطبيق ملف تعريف <خادم الإدارة الرئيسي > عند إعادة اتصال الجهاز بخادم الإدارة الرئيسي بعد تشغيله في شبكة خارجية لبعض الوقت.

5. من النافذة **ملف تعريف جديد** التي ستفتح، قم بتكوين ملف تعريف الاتصال:

- **اسم ملف التعريف**

يمكنك من خلال حقل الإدخال عرض اسم ملف تعريف الاتصال وتغييره.

- **خادم الإدارة**

عنوان خادم الإدارة الذي يجب توصيل الجهاز العميل به أثناء تفعيل ملف التعريف.

- **المنفذ**

رقم المنفذ المستخدم في الاتصال.

- **منفذ SSL**

رقم المنفذ الخاص بالاتصال في حالة استخدام بروتوكول SSL.

- **استخدام SSL**

في حال تمكين هذا الخيار، يتم تأسيس الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL.

يتم تمكين هذا الخيار افتراضيًا. نوصي بعدم تعطيل هذا الخيار حتى يظل اتصالك آمنًا.

- انقر فوق الرابط **تكوين الاتصال عبر الخادم الوكيل** لتكوين الاتصال من خلال خادم وكيل: حدد خيار **استخدام الخادم الوكيل** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. إذا تم تحديد هذا الخيار، ستتوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

- **عنوان الخادم الوكيل**

عنوان الخادم الوكيل المستخدم لاتصال Kaspersky Security Center بالإنترنت.

- **رقم المنفذ**

رقم المنفذ الذي سيتم من خلاله إنشاء اتصال وكيل Kaspersky Security Center.

- **مصادقة الخادم الوكيل**

إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

يتوفر حقل الإدخال هذا إذا تم تحديد خانة الاختيار **استخدام الخادم الوكيل**.

- **اسم المستخدم** (يتوفر هذا الحقل في حالة تحديد خيار مصادقة الخادم الوكيل)

حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

- **كلمة المرور** (يتوفر هذا الحقل في حالة تحديد خيار مصادقة الخادم الوكيل)

تم تعيين كلمة مرور بواسطة المستخدم الذي تم إنشاء اتصال الخادم الوكيل من خلال حسابه (هذا الحقل متاح في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار** حتى تظهر لك كلمة المرور.

- **إعدادات بوابة الاتصال**

عنوان البوابة التي من خلالها يتم اتصال الأجهزة العميلة بخادم الإدارة.

- **تمكين وضع الوجود خارج المكتب**

في حال تمكين هذا الخيار، وفي حال وجود اتصال عبر ملف التعريف ذلك، ستقوم التطبيقات المثبتة على الجهاز العميل باستخدام ملفات تعريف السياسة للأجهزة التي في وضع الوجود خارج المكتب، بالإضافة إلى سياسات الوجود خارج المكتب. في حالة عدم تحديد سياسة الوجود خارج المكتب للتطبيق، سيتم استخدام السياسة المفعلة.

في حال تعطيل هذا الخيار، ستستخدم التطبيقات السياسات المفعلة.

يتم تعطيل هذا الخيار افتراضيًا.

- **الاستخدام لاستلام التحديثات فقط**

في حال تمكين هذا الخيار، سيتم استخدام ملف التعريف فقط لتنزيل التحديثات بواسطة التطبيقات المثبتة على الجهاز العميل. بالنسبة للعمليات الأخرى، سيتم إنشاء اتصال بخادم الإدارة باستخدام إعدادات الاتصال الأولية المحددة أثناء تثبيت عميل الشبكة.

يتم تمكين هذا الخيار افتراضيًا.

- **مزامنة إعدادات الاتصال مع إعدادات خادم الإدارة المحددة في ملف التعريف هذا**

في حال تمكين هذا الخيار، سيتصل عميل الشبكة بخادم الإدارة باستخدام الإعدادات المحددة في خصائص ملف التعريف.

في حال تعطيل هذا الخيار، سيتصل عميل الشبكة بخادم الإدارة باستخدام الإعدادات الأصلية المحددة أثناء التثبيت.

يتوفر هذا الخيار في حال تعطيل خيار **الاستخدام لاستقبال التحديثات فقط**.

يتم تعطيل هذا الخيار افتراضيًا.

6. حدد خيار **تمكين وضع الوجود خارج المكتب عندما يكون خادم الإدارة غير متاح** للسماح للتطبيقات المثبتة على جهاز عميل باستخدام ملفات تعريف السياسة للأجهزة في وضع الوجود خارج المكتب، بالإضافة إلى سياسات خارج المكتب، عند أي محاولة للاتصال عندما لا يكون خادم الإدارة متاحًا. في حالة عدم تحديد سياسة الوجود خارج المكتب للتطبيق، سيتم استخدام السياسة المفعلة.

تم إنشاء ملف تعريف لاتصال عميل الشبكة بخادم الإدارة للمستخدمين خارج المكتب. عندما يتصل عميل الشبكة بخادم الإدارة باستخدام ملف التعريف هذا، فسوف تستخدم التطبيقات المثبتة على الأجهزة العميلة سياسات مخصصة للأجهزة في وضع الوجود خارج المكتب، أو سياسات خارج المكتب.

حول تبديل عميل الشبكة إلى خوادم إدارة أخرى

يتم تحديد الإعدادات الأولية لاتصال عميل الشبكة بالخادم عند تثبيت عميل الشبكة. لتبديل عميل الشبكة إلى خوادم الإدارة الأخرى، يمكنك استخدام قواعد التبديل . هذه الميزة مدعومة فقط لوكلاء الشبكة المثبتين على الأجهزة التي تعمل بنظام Windows أو macOS.

يمكن تشغيل قواعد التبديل عند تغيير معلمات الشبكة التالية:

- عنوان البوابة الافتراضية.
- عنوان IP الخاص بخادم بروتوكول تكوين المضيف الديناميكي (DHCP).
- لاحقة DNS للشبكة الفرعية.
- عنوان IP لخادم DNS للشبكة.
- إمكانية الوصول إلى مجال Windows هذه المعلمة متاحة فقط للأجهزة التي تعمل بنظام التشغيل Windows.
- عنوان الشبكة الفرعية والقناع.
- عنوان IP لخادم WINS للشبكة. هذه المعلمة متاحة فقط للأجهزة التي تعمل بنظام التشغيل Windows.
- اسم DNS أو NetBIOS للجهاز العميل.
- إمكانية الوصول إلى عنوان اتصال SSL.

في حالة إنشاء قواعد لتبديل عميل الشبكة إلى خوادم إدارة أخرى، سيستجيب عميل الشبكة للتغييرات في معاملات الشبكة على النحو التالي:

- إذا كانت إعدادات الشبكة تتوافق مع أي من القواعد التي تم إنشاؤها، فيتم اتصال عميل الشبكة بخادم الإدارة المحدد في هذه القاعدة. تتحول التطبيقات المثبتة على الأجهزة العميلة إلى سياسات خارج المكتب، شريطة أن يتم تمكين هذا السلوك بواسطة قاعدة.
- في حالة عدم تطبيق أي من القواعد، يعود عميل الشبكة إلى الإعدادات الافتراضية للاتصال بخادم الإدارة المحددة أثناء التثبيت. تعود التطبيقات المثبتة على الأجهزة العميلة إلى السياسات المفعلة.
- في حالة تعذر الوصول إلى خادم الإدارة، يستخدم عميل الشبكة سياسات خارج المكتب.

ينتقل Network Agent إلى سياسة الوجود خارج المكتب فقط إذ تم تمكين الخيار **تمكين وضع الوجود خارج المكتب عندما يكون خادم الإدارة غير متاح** في إعدادات سياسة Network Agent.

يتم حفظ إعدادات اتصال عميل الشبكة بخادم الإدارة في ملف تعريف الاتصال. في ملف تعريف الاتصال، يمكنك إنشاء قواعد لتبديل الأجهزة العميلة إلى سياسات خارج المكتب ويمكنك تكوين ملف التعريف كي يستخدم فقط لتنزيل التحديثات.

إنشاء قاعدة تبديل عميل شبكة حسب موقع الشبكة

لا يكون تبديل عميل الشبكة حسب موقع الشبكة متاحًا إلا على الأجهزة التي تعمل بنظام Windows وmacOS.

لإنشاء قاعدة لتبديل عميل الشبكة من خادم إدارة إلى آخر في حالة تغيير إعدادات الشبكة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي تحتوي على الأجهزة التي تريد إنشاء قواعد نقل عميل الشبكة لها حسب وصف موقع الشبكة.
2. قم بأحد الإجراءات التالية:
   - إذا أردت إنشاء قاعدة لجميع الأجهزة في المجموعة، فانتقل إلى مساحة عمل المجموعة وحدد سياسة عميل الشبكة في علامة التبويب **السياسات**. افتح نافذة الخصائص التابعة للسياسة المحددة.
   - إذا أردت إنشاء قاعدة لجهاز محدد من مجموعة، فانتقل إلى مساحة عمل المجموعة، وحدد الجهاز من علامة التبويب **الأجهزة**، وقم بتنفيذ الإجراءات التالية:
     a. افتح نافذة الخصائص التابعة للجهاز المحدد.
     b. في القسم **التطبيقات** الخاص بنافذة خصائص الجهاز، حدد عميل الشبكة.
     c. افتح نافذة خصائص عميل الشبكة.
3. في نافذة **خصائص** التي تفتح، في القسم **الاتصال** حدد القسم الفرعي **ملفات تعريف الاتصال**.
4. في قسم**إعدادات موقع الشبكة** ، انقر على زر **إضافة**.
5. في النافذة **وصف جديد** التي تفتح، قم بتكوين وصف موقع الشبكة وقاعدة التبديل. حدد إعدادات وصف موقع الشبكة التالية:
   - **اسم وصف موقع الشبكة**

     لا يمكن أن يكون اسم وصف موقع الشبكة أطول من 255 حرف أو يحتوي على رموز خاصة، مثل (|:/\?<>*").

- **استخدم ملف تعريف الاتصال**

يمكنك تحديد ملف تعريف الاتصال الذي يستخدمه عميل الشبكة للاتصال بخادم الإدارة من خلال القائمة المنسدلة. سيستخدم ملف التعريف هذا عند استيفاء شروط وصف موقع الشبكة. يحتوي ملف تعريف الاتصال على إعدادات اتصال عميل الشبكة بخادم الإدارة؛ كما يحدد متى يجب أن تتحول الأجهزة العميلة إلى سياسات خارج المكتب. يتم استخدام ملف التعريف لتنزيل التحديثات فقط.

6. في القسم **تبديل الشروط**، انقر فوق الزر **إضافة** لإنشاء قائمة بشروط وصف موقع الشبكة.

يتم تجميع شروط القاعدة باستخدام عامل التشغيل المنطقي AND. لتشغيل قاعدة التبديل حسب وصف موقع الشبكة، يجب استيفاء شروطها.

7. في القائمة المنسدلة، حدد القيمة التي تتوافق مع التغير في خصائص الشبكة التي يتصل بها الجهاز العميل:

- **عنوان بوابة اتصال افتراضي**—تم تغيير عنوان بوابة الشبكة الرئيسية.
- **عنوان خادم DHCP**—تم تغيير عنوان IP الخاص بخادم بروتوكول تكوين المضيف الديناميكي (DHCP) الخاص بالشبكة.
- **مجال DNS**—تم تغيير لاحقة DNS للشبكة الفرعية.
- **عنوان خادم DNS**—تم تغيير عنوان IP الخاص بخادم DNS الخاص بالشبكة.
- **وإمكانية الوصول إلى مجال Windows (Windows فقط)**— تغيير حالة مجال Windows الذي يتصل به الجهاز العميل. استخدم هذا الإعداد فقط للأجهزة التي تعمل بنظام Windows.
- **الشبكة الفرعية**— تغيير عنوان الشبكة الفرعية والقناع.
- **عنوان خادم WINS (Windows فقط)**—تم تغيير عنوان IP الخاص بخادم WINS للشبكة. استخدم هذا الإعداد فقط للأجهزة التي تعمل بنظام Windows.
- **إمكانية تحليل الاسم** - تم تغيير اسم DNS أو NetBIOS للجهاز العميل.
- **إمكانية الوصول إلى عنوان اتصال SSL** —يمكن للجهاز العميل أو لا يمكنه (اعتمادًا على الخيار الذي تحدده) إنشاء اتصال SSL بخادم محدد (الاسم: المنفذ). لكل خادم، يمكنك أيضًا تحديد شهادة SSL. في هذه الحالة، يتحقق وكيل الشبكة من شهادة الخادم بالإضافة إلى التحقق من إمكانية اتصال SSL. إذا لم تتطابق الشهادة، فسيفشل الاتصال. تردد الاتصال هو مرة واحدة في الدقيقة.

8. في القائمة التي ستظهر، حدد شرط تبديل عميل الشبكة إلى خادم إدارة آخر. يعتمد اسم النافذة على القيمة المحددة في الخطوة السابقة. حدد الإعدادات التالية لشرط التبديل:

- **القيمة**

في هذا الحق، يمكنك إضافة قيمة واحدة أو أكثر للشرط الجاري إنشائه.

- **مطابقة قيمة واحدة على الأقل من القيم الموجودة في القائمة**

في حالة تحديد هذا الخيار، ستتم مقابلة الشرط بصرف النظر عن أي قيمة محددة في قائمة **القيمة**.

يتم تحديد هذا الخيار افتراضيًا.

- **عدم مطابقة أي من القيم الموجودة في القائمة**

في حالة تحديد هذا الخيار، سيتم مطابقة الشرط في حالة عدم وجود القيمة الخاصة به في القائمة **القيمة**.

9. في نافذة **وصف جديد** قم بتحديد خيار **تم تمكين الوصف** لتمكين استخدام وصف موقع الشبكة الجديد.

يتم إنشاء قاعدة تبديل جديدة حسب وصف موقع الشبكة، في أي وقت يتم استيفاء شروطها يستخدم عميل الشبكة ملف تعريف الاتصال المحدد في القاعدة للاتصال بخادم الإدارة.

تتم مراجعة أوصاف موقع الشبكة للعثور على مطابقة مع مخطط الشبكة بالترتيب الذي تظهر به الأوصاف في القائمة. في حالة مطابقة الشبكة للعديد من

الأوصاف، سيتم استخدام الوصف الأول. يمكنك تغيير ترتيب القواعد في القائمة باستخدام زر **النقل لأعلى** (⬆) وزر **النقل لأسفل** (⬇).

إخطارات الأحداث

يوضح هذا القسم كيفية تحديد طريقة لتسليم إخطارات المسؤول حول الأحداث المتعلقة بالأجهزة العميلة وكيفية تكوين إعدادات إخطار الحدث.

ويصف أيضًا كيفية اختبار توزيع إخطارات الأحداث باستخدام اختبار الفيروس Eicar.

تكوين إخطار الحدث

يتيح لك Kaspersky Security Center تحديد طريقة لإخطار المسؤول بالأحداث التي تحدث على الأجهزة العميلة وكذلك تكوين الإخطار:

- البريد الإلكتروني. عند وقوع حدث ما، يقوم التطبيق بإرسال إخطار لعناوين البريد الإلكتروني المحددة. يمكنك تحرير نص الإخطار.
- SMS عند وقوع حدث ما، يقوم التطبيق بإرسال إخطار لأرقام الهاتف المحددة. يمكنك تكوين إخطارات SMS ليتم إرسالها عبر بوابة البريد.
- الملف التنفيذي عند وقوع حدث ما على جهاز، يتم بدء الملف التنفيذي على محطة عمل المسؤول. باستخدام الملف التنفيذي، يمكن للمسؤول تلقي معلمات أي حدث وقع.

لتكوين إخطار بالأحداث التي تحدث على أجهزة الكمبيوتر العميلة:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.
3. انقر فوق الرابط **تكوين الإخطارات وتصدير الأحداث** وحدد القيمة **تكوين الإخطارات** في القائمة المنسدلة.

   يؤدي ذلك لفتح النافذة **خصائص: الأحداث**.
4. في القسم **إخطار**، حدد طريقة الإخطار (عبر البريد الإلكتروني، أو عبر SMS أو عبر تشغيل ملف تنفيذي) وحدد إعدادات الإخطار:

- **البريد الإلكتروني**

تتيح لك علامة التبويب **البريد الإلكتروني** تكوين إشعارات الأحداث عبر البريد الإلكتروني.

في حقل **المستلمون (عناوين البريد الإلكتروني)**، حدد عناوين البريد الإلكتروني التي سيرسل التطبيق الإخطارات إليها. يمكنك تحديد عدة عناوين في هذا الحقل بالفصل بينهم بفواصل منقوطة.

في حقل **SMTP خوادم**، حدد عناوين خادم البريد، مع الفصل بينهم بفواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

في حقل **منفذ خادم SMTP**، حدد رقم منفذ اتصال خادم SMTP. رقم المنفذ الافتراضي هو 25.

إذا قمت بتمكين خيار **استخدم بحث DNS MX**، فيمكنك استخدام عدة سجلات من MX لعناوين IP الخاصة بنفس اسم منطقة DNS في خادم SMTP. قد يكون لاسم DNS نفسه عدة سجلات من MX بقيم مختلفة لتلقي رسائل البريد الإلكتروني ذو الأولوية. يحاول خادم الإدارة إرسال إشعارات البريد الإلكتروني إلى خادم SMTP بترتيب تصاعدي لسجلات MX ذات الأولوية. يتم تعطيل هذا الخيار افتراضيًا.

إذا قمت بتمكين خيار **استخدم بحث DNS MX**، ولم تقم بتمكين استخدام إعدادات TLS، فإننا نوصي باستخدام إعدادات DNSSEC على جهاز الخادم الخاص بك كإجراء إضافي للحماية لإرسال إعلامات البريد الإلكتروني.

انقر على رابط **الإعدادات** لتحديد إعدادات الإشعارات الإضافية:انقر على رابط الإعدادات لتحديد إعدادات الإشعارات الإضافية:

- اسم الموضوع (اسم موضوع رسالة البريد الإلكتروني)
- عنوان البريد الإلكتروني للمرسل
- إعدادات مصادقة ESMTP

يجب عليك تحديد حساب للمصادقة على خادم SMTP، إذا تم تمكين خيار مصادقة ESMTP لخادم SMTP.

- إعدادات TLS لخادم SMTP:
  - **لا تستخدم TLS**

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

  - **استخدم TLS إذا كان يدعمه خادم SMTP**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام اتصال TLS مع خادم SMTP. إذا كان خادم SMTP لا يدعم TLS، فإن خادم الإدارة يتصل بخادم SMTP بدون استخدام TLS.

  - **استخدام TLS دومًا، وتحقق من شهادة الخادم للتحقق من الصلاحية**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام إعدادات مصادقة TLS. إذا كان خادم SMTP لا يدعم TLS، فلن يتمكن خادم الإدارة من توصيل خادم SMTP.

نوصي باستخدام هذا الخيار لتوفير حماية أفضل للاتصال بخادم SMTP. إذا قمت بتحديد هذا الخيار، فيمكنك تعيين إعدادات المصادقة لاتصال TLS.

إذا اخترت قيمة **استخدام TLS دومًا والتحقق من شهادة الخادم للتحقق من الصلاحية**، فيمكنك تحديد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال من خلال أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. يمكنك أيضًا تحديد شهادة لمصادقة العميل على خادم SMTP.

يمكنك تحديد إعدادات TLS لخادم SMTP:

- تصفح للوصول إلى ملف شهادة خادم SMTP:

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

- تصفح للوصول إلى ملف شهادة العميل:

يمكنك استخدام شهادة استلمتها من أي مصدر، على سبيل المثال، من أي جهة إصدار موثوقة. يجب تحديد الشهادة ومفتاحها الخاص باستخدام أحد أنواع الشهادات التالية:

- شهادة X-509:

يجب تحديد ملف مع الشهادة وملف مع المفتاح الخاص. كلا الملفين لا يعتمدان على بعضهما البعض وترتيب تحميل الملفات ليس مهمًا. عند تحميل كلا الملفين، يجب تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- الحاوية pkcs12:

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك بعد ذلك تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

يحتوي الحقل **رسالة إخطار** على نص قياسي يحتوي على معلومات حول الحدث الذي يرسله التطبيق عند وقوع حدث. يتضمن هذا النص معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة من خلال إضافة معلمات بديلة أخرى مع تفاصيل ذات صلة أكثر بالحدث. تتوفر قائمة بالمعلمات البديلة عبر النقر فوق الزر على يمين الحقل.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

انقر فوق رابط **تكوين حد الإخطارات الرقمي** لتحديد الحد الأقصى لعدد الإشعارات التي يمكن للتطبيق إرسالها خلال الفترة الزمنية المحددة.

انقر فوق زر **إرسال رسالة اختبار** للتحقق مما إذا كنت قد قمت بتكوين الإشعارات بشكل صحيح. يجب أن يرسل التطبيق إشعار الاختبار إلى عناوين البريد الإلكتروني التي حددتها.

- **رسالة SMS**

تتيح لك علامة التبويب **رسالة SMS** تكوين إرسال إخطارات بمختلف الأحداث عبر رسالة SMS إلى هاتف محمول. يتم إرسال الرسائل النصية القصيرة عبر بوابة بريد.

في الحقل **المستلمين (عناوين البريد الإلكتروني)**، حدد عناوين البريد الإلكتروني التي سيرسل التطبيق الإخطارات إليها. يمكنك تحديد عدة عناوين في هذا الحقل بالفصل بينهم بفواصل منقوطة. سيتم إرسال الإخطارات إلى أرقام الهواتف المرتبطة بعناوين البريد الإلكتروني المحددة.

في الحقل **خوادم SMTP**، حدد عناوين خادم البريد، مع الفصل بينهم بفواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

في الحقل **منفذ خادم SMTP**، حدد رقم منفذ اتصال خادم SMTP. رقم المنفذ الافتراضي هو 25.

انقر على رابط **الإعدادات** لتحديد إعدادات الإشعارات الإضافية:انقر على رابط الإعدادات لتحديد إعدادات الإشعارات الإضافية:

- اسم الموضوع (اسم موضوع رسالة البريد الإلكتروني)
- عنوان البريد الإلكتروني للمرسل
- إعدادات مصادقة ESMTP

إذا لزم الأمر، يمكنك تحديد حساب للمصادقة على خادم SMTP إذا تم تمكين خيار مصادقة ESMTP لخادم SMTP.

- إعدادات TLS لخادم SMTP

يمكنك تعطيل استخدام TLS، استخدام TLS إذا كان خادم SMTP يدعم هذا البروتوكول أو يمكنك فرض استخدام TLS فقط. إذا اخترت استخدام TLS فقط، فيمكنك تحديد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال عبر أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. إذا اخترت أيضًا استخدام TLS فقط، فيمكنك تحديد شهادة لمصادقة العميل على خادم SMTP.

- تصفح للبحث عن ملف شهادة خادم SMTP

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى Kaspersky Security Center. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك بعد ذلك تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم ترميز المفتاح الخاص. يحتوي حقل **رسالة الإشعار** على نص قياسي به معلومات عن الحدث الذي يرسله التطبيق عند وقوع حدث ما. يتضمن هذا النص معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة من خلال إضافة معلمات بديلة أخرى مع تفاصيل ذات صلة أكثر بالحدث. تتوفر قائمة بالمعلمات البديلة عبر النقر فوق الزر على يمين الحقل.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

انقر فوق رابط **تكوين حد الإشعارات الرقمي** لتحديد الحد الأقصى لعدد الإشعارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

انقر فوق زر **إرسال رسالة اختبار** للتحقق مما إذا كنت قد قمت بتكوين الإشعارات بشكل صحيح. يجب أن يرسل التطبيق إشعار اختبار إلى المستلم الذي حددته.

- **الملف التنفيذي المراد تشغيله**

إذا تم تحديد أسلوب الإخطار هذا، ففي حقل الإدخال يمكنك تحديد التطبيق الذي سيتم بدء تشغيله عند وقوع حدث ما.

يتيح لك النقر فوق الرابط **تكوين حد الإخطارات الرقمي** تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

يتيح لك النقر فوق الزر **إرسال رسالة اختبار** التحقق مما إذا قمت بتكوين الإخطارات بطريقة صحيحة: يرسل التطبيق إخطار اختبار إلى عناوين البريد الإلكتروني التي حددتها.

5. في الحقل **رسالة إخطار**، أدخل النص الذي سيرسله التطبيق عند وقوع حدث.

يمكنك استخدام القائمة المنسدلة الموجودة على يسار حقل النص لإضافة إعدادات الاستبدال مع تفاصيل الحدث (على سبيل المثال، وصف الحدث أو قت وقوع الحدث).

> إذا كان نص الإخطار يحتوي على نسبة (%)، فيجب عليك تحديده مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

6. انقر فوق الزر **إرسال رسالة اختبار** للتحقق مما إذا تم تكوين الإخطار بشكل صحيح أم لا.

يرسل التطبيق رسالة اختبار إلى المستخدم المحدد.

7. انقر فوق **موافق** لحفظ التغييرات.

يتم تطبيق إعدادات الإخطارات المعاد ضبطها على كل الأحداث التي تحدث على الأجهزة العميلة.

يمكنك تجاوز إعدادات الإخطار لبعض الأحداث من القسم **تكوين الحدث** لإعدادات خادم الإدارة، أو لإعدادات السياسة، أو إعدادات التطبيق.

إخطارات الاختبار

للتحقق من إرسال إشعارات الحدث أم لا، يستخدم التطبيق إشعار الاختبار لاكتشاف فيروس EICAR في الأجهزة العميلة.

للتحقق من إرسال إخطارات الأحداث:

1. أوقف مهمة حماية نظام الملفات في الوقت الحقيقي على الجهاز العميل وانسخ اختبار "الفيروس" EICAR إلى ذلك الجهاز العميل. الآن قم بإعادة تمكين الحماية في الوقت الحقيقي لملف النظام.

2. قم بتشغيل مهمة الفحص للأجهزة العميلة في إحدى مجموعات الإدارة أو للأجهزة المحددة، بما في ذلك الجهاز الذي يحتوي على "الفيروس" EICAR.

إذا تم تكوين مهمة الفحص بشكل صحيح، فسوف يتم اكتشاف الاختبار "الفيروس". إذا تم تكوين الإخطارات بشكل صحيح، فيتم إخطارك بأنه قد تم اكتشاف أحد الفيروسات.

في مساحة عمل العقدة **خادم الإدارة**، على علامة التبويب **الأحداث**، يعرض التحديد **الأحداث الأخيرة** سجل بحالات اكتشاف "فيروس".

> لا يحتوي اختبار "الفيروس" EICAR على أية رموز قد تضر جهازك. ومع ذلك، تحدد معظم تطبيقات الأمن للشركة المصنعة هذا الملف كفيروس. يمكنك تنزيل ملف اختبار "الفيروس" من موقع ويب EICAR الرسمي.

إخطارات الحدث التي يتم عرضها بواسطة الملف التنفيذي

بإمكان Kaspersky Security Center إخطار المسؤول بشأن الأحداث على الأجهزة العميلة عبر تشغيل الملف التنفيذي. يجب أن يحتوي الملف التنفيذي على ملف تنفيذي آخر مع العناصر النائبة للحدث ليتم ترحيله إلى المسؤول (انظر الجدول أدناه).

عنصر نائب	وصف عنصر نائب
%الخطورة%	خطورة الحدث. القيم الممكنة: • Info • Warning • خطأ • Critical
%الكمبيوتر%	اسم الجهاز الذي وقع عليه الحدث. الحد الأقصى لطول اسم الجهاز هو 256 حرفًا.
%المجال%	اسم المجال للجهاز الذي وقع عليه الحدث.
%الحدث%	اسم نوع الحدث. الحد الأقصى لطول اسم نوع الحدث هو 50 حرفًا.
%DESCR%	وصف الحدث. الحد الأقصى لطول اسم الجهاز هو 1000 حرفًا.
%RISE_TIME%	وقت إنشاء الحدث.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	اسم المهمة. الحد الأقصى لطول اسم المهمة هو 100 حرف.
%KL_PRODUCT%	اسم التطبيق.
%KL_VERSION%	رقم إصدار التطبيق.
%KLCSAK_EVENT_SEVERITY_NUM%	رقم خطورة الحدث. القيم الممكنة: • Info—1 • Warning—2 • Error—3 • Critical—4
%HOST_IP%	عنوان IP للجهاز الذي وقع عليه الحدث.
%HOST_CONN_IP%	عنوان IP للاتصال بالجهاز الذي وقع عليه الحدث.

مثال:
يتم إرسال إشعارات الحدث بواسطة ملف تنفيذي (مثل script1.bat) الذي يوجد بداخله ملف تنفيذي آخر (مثل script2.bat) مع تشغيل العنصر النائب %COMPUTER%. عند وقوع حدث ما، سيتم تشغيل الملف script1.bat على جهاز المسؤول والذي بدوره يشغّل الملف script2.bat مع العنصر النائب %COMPUTER%. يتلقى المسؤول اسم الجهاز حيث وقع الحدث.

تشفير الاتصال باستخدام بروتوكول TLS

لإصلاح الثغرات الأمنية الموجودة في شبكة الشركة الخاصة بمؤسستك، يمكنك تمكين تشفير حركة المرور باستخدام بروتوكول TLS. ويمكنك تمكين بروتوكولات التشفير TLS ومجموعات التشفير المدعومة على خادم الإدارة وخادم iOS MDM. ويدعم Kaspersky Security Center الإصدارات 1.0 و1.1 و1.2 و1.3 لبروتوكول TLS. ويمكنك تحديد بروتوكول التشفير المطلوب ومجموعات التشفير المطلوبة.

يستخدم Kaspersky Security Center شهادات موقعة ذاتيًا. التكوين الإضافي لأجهزة iOS غير مطلوب. يمكنك أيضًا استخدام شهاداتك الخاصة. يوصي أخصائيو Kaspersky باستخدام الشهادات الصادرة عن هيئات إصدار الشهادات الموثوق بها.

خادم الإدارة

قم بما يلي لتكوين بروتوكولات التشفير ومجموعات التشفير المسموح بها على خادم الإدارة:

1. قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Security Center\Lab.

2. استخدم العلامة SrvUseStrictSslSettings لتكوين بروتوكولات التشفير ومجموعات التشفير المسموح بها على خادم الإدارة. أدخل الأمر التالي:

```
s Transport -n SrvUseStrictSslSettings -- "core/.independent." klscflag -fset -pv
t d- < القيمة > v
```

حدد معلمة <value> لعلامة SrvUseStrictSslSettings:

- 4 - يتم تمكين بروتوكولي TLS 1.2 وTLS 1.3 فقط. ويتم أيضًا تمكين مجموعات التشفير مع TLS_RSA_WITH_AES_256_GCM_SHA384 (مجموعات التشفير هذه مطلوبة للتوافق مع الإصدارات السابقة مع الإصدارات السابقة من Kaspersky Security Center). وهذه هي القيمة الافتراضية.

  مجموعات التشفير المدعومة لبروتوكول TLS 1.2:

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - AES256-GCM-SHA384 (مجموعة تشفير مع TLS_RSA_WITH_AES_256_GCM_SHA384)
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

  مجموعات التشفير المدعومة لبروتوكول TLS 1.3:

  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_128_CCM_SHA256

- 5 - يتم تمكين بروتوكولي TLS 1.2 وTLS 1.3 فقط. بالنسبة لبروتوكولي TLS 1.2 وTLS 1.3، يتم دعم مجموعات التشفير المحددة المدرجة أدناه.

  مجموعات التشفير المدعومة لبروتوكول TLS 1.2:

  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-SHA384
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES128-SHA256

مجموعات التشفير المدعومة لبروتوكول TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

لا نوصي باستخدام 0 أو 1 أو 2 أو 3 كقيمة معلمة لعلامة SrvUseStrictSslSettings. وتتوافق قيم المعلمات هذه مع إصدارات بروتوكول TLS غير الآمنة (بروتوكولا TLS 1.0 وTLS 1.1) ومجموعات التشفير غير الآمنة وتستخدم فقط للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

3. أعد تشغيل خدمات Kaspersky Security Center 15.1 التالية:

- خادم الإدارة
- خادم الويب
- وكيل التفعيل

يتم تمكين تشفير حركة البيانات باستخدام بروتوكول TLS.

يمكنك استخدام علامتي KLTR_TLS12_ENABLED وKLTR_TLS13_ENABLED لتمكين دعم بروتوكولي TLS 1.2 وTLS 1.3 على التوالي. يتم تمكين هذه العلامات بشكل افتراضي.

لتمكين أو تعطيل دعم بروتوكولي TLS 1.2 وTLS 1.3:

1. قم بتشغيل الأداة المساعدة klscflag.

قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Security Center\Lab.

2. أدخل أحد الأوامر التالية في موجه أوامر Windows، باستخدام حقوق المسؤول:

- استخدم هذا الأمر لتمكين دعم بروتوكول TLS 1.2 أو تعطيله:

```
s Transport -n KLTR_TLS12_ENABLED -v- "core/.independent." klscflag -fset -pv
t d- < القيمة >
```

- استخدم هذا الأمر لتمكين دعم بروتوكول TLS 1.3 أو تعطيله:

```
s Transport -n KLTR_TLS13_ENABLED -v- "core/.independent." klscflag -fset -pv
t d- < القيمة >
```

حدد المعلمة `< value >` للعلامة:

- `1` - لتمكين دعم بروتوكول TLS.
- `0` - لتعطيل دعم بروتوكول TLS.

خادم الأجهزة المحمولة التي تعمل بنظام iOS

يتم تشفير الاتصال بين أجهزة iOS وخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM افتراضيًا.

قم بما يلي لتكوين بروتوكولات التشفير ومجموعات التشفير المسموح بها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM:

1. افتح سجل النظام الخاص بالجهاز العميل المثبت عليه خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** > **تشغيل**).

2. انتقل إلى الخلية التالية:

- لأنظمة 32 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Settings

- لأنظمة 64 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM

3. قم بإنشاء مفتاح بالاسم `StrictSslSettings`.

4. حدد `DWORD` كنوع المفتاح.

5. قم بتعيين قيمة المفتاح:

- 2 - يتم تمكين بروتوكولات TLS 1.0 وTLS 1.1 وTLS 1.2.

- 3 - يتم تمكين بروتوكول TLS 1.2 فقط (القيمة الافتراضية).

6. أعد تشغيل خدمة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM الخاص بتطبيق Kaspersky Security Center.

تكوين الواجهة

يمكنك تكوين واجهة Kaspersky Security Center:

- إظهار الكائنات وإخفاؤها في شجرة وحدة التحكم، ومساحة العمل، وخصائص نوافذ الكائنات (المجلدات، الأقسام)، اعتمادًا على الميزات المستخدمة.

- إظهار وإخفاء عناصر النافذة الرئيسية (على سبيل المثال، شجرة وحدة التحكم أو القوائم القياسية مثل **إجراءات** و**عرض**).

لتكوين واجهة Kaspersky Security Center وفقًا لمجموعة المزايا المُستخدمة حاليًا:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

2. من شريط القوائم في نافذة التطبيق الرئيسية، حدد **عرض** ← **تكوين الواجهة**.

3. في نافذة **تكوين الواجهة** التي تفتح، قم بتكوين عرض عناصر الواجهة باستخدام خانات الاختيار التالية:

- **عرض إدارة الثغرات الأمنية والتصحيحات**

إذا تم تمكين هذا الخيار، فسيعرض مجلد **التثبيت عن بُعد** المجلد الفرعي **نشر صور الجهاز**، ويعرض مجلد **المستودعات** المجلد الفرعي **العتاد**.

يتم تعطيل هذا الخيار بشكل افتراضي في حال عدم انتهاء معالج البدء السريع. يتم تمكين هذا الخيار افتراضيًا بعد انتهاء معالج البدء السريع.

في حالة تعطيل هذا الخيار، فلن يتوفر عنصرا القائمة **إنشاء جلسة RDP** و**Windows Desktop Sharing** حتى إذا كان لديك ترخيص لإدارة الأنظمة.

- **عرض تشفير البيانات وحمايتها**

في حال تمكين هذا الخيار، تعرض شجرة وحدة التحكم مجلد **تشفير البيانات وحمايتها**.

يتم تمكين هذا الخيار افتراضيًا.

- **إعدادات التحكم في نقطة النهاية**

في حال تمكين هذا الخيار، يتم عرض الأقسام الفرعية التالية في قسم **عناصر التحكم في الأمان** من نافذة الخصائص في سياسة Kaspersky Endpoint Security for Windows:

- **التحكم في التطبيقات**
- **التحكم في الجهاز**
- **التحكم في الويب**
- **التحكم في الخارج عن المألوف التكيفي**

إذا تم تعطيل هذا الخيار، فلن يتم عرض الأقسام الفرعية المحددة أعلاه في قسم **عناصر التحكم في الأمان**.

يتم تمكين هذا الخيار افتراضيًا.

- **عرض إدارة الأجهزة المحمولة**

إذا تم تمكين هذا الخيار، تكون ميزة **إدارة الأجهزة المحمولة** متاحة. بعد إعادة تشغيل التطبيق، تعرض شجرة وحدة التحكم مجلد **الأجهزة المحمولة**.

يتم تمكين هذا الخيار افتراضيًا.

- **عرض خوادم الإدارة الثانوية**

إذا تم تحديد خانة الاختيار، فإن شجرة وحدة التحكم تعرض العُقد الخاصة بخدمات الخوادم الافتراضية التابعة ضمن مجموعات الإدارة. تتوفر الميزات المتصلة بخوادم الإدارة الافتراضية والتابعة – على سبيل المثال، إنشاء مهام للتثبيت عن بُعد للتطبيقات على خوادم الإدارة الثانوية – على هذا الخيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **عرض أقسام إعدادات الأمان**

إذا تم تمكين هذا الخيار، فسيتم عرض قسم **الأمان** في نافذة خصائص خادم الإدارة ومجموعات الإدارة والعناصر الأخرى. يسمح لك هذا الخيار بمنح المستخدمين ومجموعات المستخدمين أذونات مخصصة للعمل مع العناصر.

يتم تعطيل هذا الخيار افتراضيًا.

4. انقر فوق **موافق**.

لتطبيق بعض التغييرات، يجب عليك إغلاق نافذة التطبيق الرئيسية ثم فتحها مرة أخرى.

لتكوين عرض العناصر في نافذة التطبيق الرئيسية:

1. في شريط القوائم في نافذة التطبيق الرئيسية، حدد **عرض** ← **تكوين**.
2. في نافذة **تكوين طريقة العرض** التي تنفتح، قم بتكوين عرض عناصر النافذة الرئيسية باستخدام خانات الاختيار.
3. انقر فوق **موافق**.

اكتشاف الأجهزة المتصلة بالشبكة

يصف هذا القسم الخطوات الواجب عليك اتخاذها بعد تثبيت Kaspersky Security Center.

سيناريو: اكتشاف الأجهزة المتصلة بالشبكة

يجب عليك إجراء عملية اكتشاف الأجهزة قبل تثبيت تطبيقات الأمان. يتلقى خادم الإدارة معلومات عن الأجهزة المكتشفة ويسمح لك بإدارة الأجهزة من خلال السياسات. يلزم إجراء استقصاءات منتظمة للشبكة لتحديث قائمة الأجهزة المتوفرة في الشبكة.

قبل أن تبدأ استقصاء الشبكة، تأكد من تمكين بروتوكول SMB. خلاف ذلك، يتعذر على Kaspersky Security Center اكتشاف الأجهزة في الشبكة التي تم استطلاعها. لتمكين بروتوكول SMB، اتبع الإرشادات الخاصة بنظام التشغيل الخاص بك.

يتم اكتشاف الأجهزة المتصلة بالشبكة في المراحل التالية:

1. **اكتشاف الأجهزة**

   يوجهك معالج البداية السريعة خلال عملية اكتشاف الأجهزة الأولي، ويساعدك على العثور على الأجهزة المتصلة بالشبكة مثل أجهزة الكمبيوتر والأجهزة اللوحية والهواتف المحمولة. ويمكنك أيضًا إجراء اكتشاف الأجهزة يدويًا.

2. **تكوين الاستقصاءات المجدولة**

   حدد نوع (أنواع) الاستقصاء الذي تريد استخدامه بانتظام. وقم بتمكين الأنواع المطلوبة وتكوين جدول الاستقصاء. يمكنك الرجوع إلى التوصيات الخاصة بتكرار استقصاء الشبكة.

3. **إعداد القواعد لإضافة الأجهزة المكتشفة إلى مجموعات الإدارة (اختياري)**

   إذا ظهرت أجهزة جديدة على شبكتك، فسيتم اكتشافها أثناء الاستقصاءات المنتظمة وسيتم تضمينها تلقائيًا في المجموعة **الأجهزة غير المخصصة**. يمكنك إعداد قواعد نقل الجهاز لأتمتة تخصيص الأجهزة لمجموعة **الأجهزة المُدارة**. يمكنك أيضًا تكوين قواعد الاستبقاء.

   إذا تخطيت الخطوة 3، سيتم تخصيص الأجهزة المكتشفة حديثًا لمجموعة **الأجهزة غير المخصصة**. وإذا كنت تريد ذلك، يمكنك نقل هذه الأجهزة إلى المجموعة **الأجهزة المُدارة** يدويًا. أما إذا قمت بنقل الأجهزة إلى المجموعة **الأجهزة المُدارة** يدويًا، فيمكنك تحليل المعلومات حول كل جهاز وتحديد ما إذا كنت تريد نقله إلى مجموعة إدارة وإذا كان الأمر كذلك، فحدد المجموعة الدقيقة المطلوب النقل إليها.

النتائج

ينتج عن إكمال السيناريو ما يلي:

- يكتشف خادم إدارة Kaspersky Security Center الأجهزة الموجودة على الشبكة ويوفر لك معلومات حولها.
- يتم إعداد الاستقصاءات المستقبلية ويتم إجراؤها وفقًا للجدول المحدد.
- يتم ترتيب الأجهزة المكتشفة حديثًا وفقًا للقواعد التي تم تكوينها. (أو، إذا لم يكن هناك أي قواعد مكونة، فستبقى الأجهزة في مجموعة **الأجهزة غير المخصصة**).

الأجهزة غير المخصصة

يقدم هذا القسم معلومات عن طريقة إدارة الأجهزة على شبكة إحدى الشركات إذا لم تكن متضمنة في إحدى مجموعات الإدارة.

اكتشاف الأجهزة

يصف هذا القسم أنواع اكتشاف الأجهزة المتاحة في Kaspersky Security Center ويوفر معلومات حول استخدام كل نوع.

يتلقى خادم الإدارة معلومات حول بنية الشبكة والأجهزة الموجودة على هذه الشبكة من خلال استقصاء منتظم. يتم تسجيل المعلومات في قاعدة بيانات خادم الإدارة. يمكن لخادم الإدارة استخدام الأنواع التالية من الاستقصاء:

- **استقصاء شبكة Windows**. يستطيع خادم الإدارة تنفيذ نوعين من استقصاء شبكة Windows: السريع والكامل. أثناء إجراء استقصاء سريع، يقوم خادم الإدارة باسترداد المعلومات من قائمة أسماء NetBIOS الخاصة بالأجهزة في جميع مجالات الشبكة ومجموعات العمل فقط. خلال الاستقصاء الكامل، يتم طلب المزيد من المعلومات من كل جهاز عميل مثل اسم نظام التشغيل، وعنوان IP، واسم DNS، واسم NetBIOS. يتم تمكين كل من الاستقصاء السريع والاستقصاء الكامل بصورة افتراضية. قد يفشل استقصاء شبكة Windows في اكتشاف الأجهزة، على سبيل المثال إذا كانت المنافذ UDP 137، وUDP 138، وTCP 139 مغلقة على جهاز التوجيه أو بواسطة جدار الحماية.

- **استقصاء Active Directory**. يقوم خادم الإدارة باسترداد المعلومات حول بنية وحدة Active Directory وحول أسماء DNS للأجهزة من مجموعات Active Directory. يتم تمكين هذا النوع من الاستقصاء بشكل افتراضي. نوصي باستخدام استقصاء Active Directory إذا كنت تستخدم Active directory؛ وبخلاف ذلك، لن يكتشف خادم الإدارة أي أجهزة. إذا كنت تستخدم Active directory، إلا إن بعض الأجهزة المتصلة بالشبكة غير مدرجة كأعضاء، فإنه يتعذر على استقصاء Active Directory اكتشاف هذه الأجهزة.

- **استقصاء نطاق IP** يستقصي خادم الإدارة نطاقات IP المحددة باستخدام حزم ICMP أو بروتوكول NBNS ويجمع مجموعة كاملة من البيانات على الأجهزة ضمن نطاقات IP هذه. يتم تعطيل نوع الاستقصاء هذا افتراضيًا. لا يوصى باستخدام هذا النوع من الاستقصاء إذا كنت تستخدم استقصاء شبكة Windows و/أو استقصاء Active Directory.

- **استطلاع شبكة لا تتطلب تكوينًا**. تقوم نقطة توزيع باستقصاء شبكة IPv6 باستخدام شبكات التكوين الصفري (كما يشار إلى Zeroconf). يتم تعطيل نوع الاستقصاء هذا افتراضيًا. يمكنك استخدام استقصاء شبكة لا تتطلب تكوينًا إذا كانت نقطة التوزيع تعمل بنظام Linux.

إذا قمت بإعداد وتمكين قواعد نقل الأجهزة، فسيتم تضمين الأجهزة المكتشفة حديثًا تلقائيًا في المجموعة **الأجهزة المُدارة**. في حالة عدم تمكين أي من قواعد النقل، فسيتم تضمين الأجهزة المكتشفة حديثًا تلقائيًا في المجموعة **الأجهزة غير المخصصة**.

يمكنك تعديل إعدادات اكتشاف الأجهزة لكل نوع. على سبيل المثال، قد ترغب في تعديل جدول الاستقصاء أو تعيين إما استقصاء المجال بالكامل أو فقط مجال محدد.

قبل أن تبدأ استقصاء الشبكة، تأكد من تمكين بروتوكول SMB. خلاف ذلك، يتعذر على Kaspersky Security Center اكتشاف الأجهزة في الشبكة التي تم استطلاعها. لتمكين بروتوكول SMB، اتبع الإرشادات الخاصة بنظام التشغيل الخاص بك.

استقصاء شبكة Windows

حول استقصاء شبكة Windows

أثناء إجراء استقصاء سريع، يقوم خادم الإدارة باسترداد المعلومات من قائمة أسماء NetBIOS الخاصة بالأجهزة في جميع مجالات الشبكة ومجموعات العمل فقط. خلال الاستقصاء الكامل، يتم طلب المعلومات التالية من كل جهاز عميل:

- اسم نظام التشغيل
- عنوان IP
- اسم DNS
- اسم NetBIOS

يتطلب كل من الاستقصاء السريع والكامل ما يلي:

- يجب أن تكون المنافذ UDP 137/138، و139 TCP، و445 UDP، و445 TCP متاحة على الشبكة.
- تم تمكين بروتوكول SMB.
- يجب استخدام خدمة استعراض الكمبيوتر في Microsoft ويجب تمكين كمبيوتر الاستعراض الأساسي على خادم الإدارة.
- يجب استخدام خدمة استعراض الكمبيوتر في Microsoft ويجب تمكين كمبيوتر الاستعراض الأساسي على الأجهزة العميلة:
  - على جهاز واحد على الأقل، إذا كان عدد الأجهزة المتصلة بالشبكة لا يتجاوز 32.
  - على جهاز واحد على الأقل لكل 32 من الأجهزة المتصلة بالشبكة.

لا يمكن تشغيل الاستقصاء الكامل إلا إذا كان قد سبق تشغيل الاستقصاء السريع مرة واحدة على الأقل.

عرض وتعديل إعدادات استقصاء شبكة Windows

لتعديل إعدادات استقصاء شبكة Windows:

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **المجالات**.
   يمكنك المتابعة من المجلد **الأجهزة غير المخصصة** إلى المجلد **اكتشاف الأجهزة** من خلال النقر فوق الزر **استقصاء الآن**.
   في مساحة عمل المجلد الفرعي **المجالات**، يتم عرض قائمة الأجهزة.
2. انقر فوق **استقصاء الآن**.
   تفتح نافذة خصائص المجال. إذا كنت ترغب، قم بتعديل إعدادات استقصاء شبكة Windows:

- **تمكين استقصاء شبكة Windows**

ويتم تحديد هذا الخيار بصورة افتراضية. إذا كنت لا ترغب في إجراء استقصاء شبكة Windows (على سبيل المثال، إذا كنت تعتقد أن استقصاء Active Directory كافيًا)، يمكنك إلغاء تحديد هذا الخيار.

- **تعيين جدول استقصاء سريع**

المدة الافتراضية هي 15 دقيقة.

أثناء إجراء استقصاء سريع، يقوم خادم الإدارة باسترداد المعلومات من قائمة أسماء NetBIOS الخاصة بالأجهزة في جميع مجالات الشبكة ومجموعات العمل فقط.

يتم استبدال البيانات التي يتم تلقيها في الاستقصاء التالي بالبيانات القديمة بشكل كامل.

تتوفر خيارات جدول الاستقصاء التالية:

- **كل N يومًا**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N دقيقة**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل خمس دقائق، بداية من الوقت الحالي للنظام.

- **حسب أيام الأسبوع**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 00:00:6 مساءً.

- **كل شهر في أيام معينة من الأسابيع المحددة**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكلٍ افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 00:00:6 مساءً.

- **تشغيل المهام الفائتة**

إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تمكين هذا الخيار افتراضيًا.

- **تعيين جدول استقصاء كامل**

المدة الافتراضية هي ساعة واحدة. يتم استبدال البيانات التي يتم تلقيها في الاستقصاء التالي بالبيانات القديمة بشكل كامل.

تتوفر خيارات جدول الاستقصاء التالية:

- **كل N يومًا**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N دقيقة**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل خمس دقائق، بداية من الوقت الحالي للنظام.

- **حسب أيام الأسبوع**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 00:00:6 مساءً.

- **كل شهر في أيام معينة من الأسابيع المحددة**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكلٍ افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 00:00:6 مساءً.

- **تشغيل المهام الفائتة**

إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تمكين هذا الخيار افتراضيًا.

إذا كنت ترغب في إجراء الاستقصاء فورًا، انقر فوق **استقصاء الآن**. سيبدأ كلا نوعي الاستقصاء.

من خادم الإدارة الافتراضي، يمكنك عرض إعدادات الاستقصاء الخاصة بشبكة Windows وتحريرها في نافذة خصائص نقطة التوزيع، في قسم **اكتشاف الأجهزة**.

استقصاء Active Directory

استخدم استقصاء Active Directory إذا كنت تستخدم Active Directory; خلافًا لذلك، فمن المستحسن أن تستخدم أنواع الاستقصاء الأخرى. إذا كنت تستخدم Active directory، إلا إن بعض الأجهزة المتصلة بالشبكة غير مدرجة كأعضاء، فإنه يتعذر على استقصاء Active Directory اكتشاف هذه الأجهزة.

يتم تخزين نتائج استطلاع Active Directory على خادم الإدارة لمدة 30 يومًا بغض النظر عن نتائج الاستطلاع اللاحق.

قبل أن تبدأ استقصاء الشبكة، تأكد من تمكين بروتوكول SMB. خلاف ذلك، يتعذر على Kaspersky Security Center اكتشاف الأجهزة في الشبكة التي تم استطلاعها. لتمكين بروتوكول SMB، اتبع الإرشادات الخاصة بنظام التشغيل الخاص بك.

عرض وتعديل إعدادات استقصاء Active Directory

لعرض وتعديل إعدادات استقصاء مجموعات Active Directory:

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **Active Directory**.

بدلًا من ذلك، يمكنك المتابعة من المجلد **الأجهزة غير المخصصة** إلى المجلد **اكتشاف الأجهزة** عن طريق النقر فوق الزر **استقصاء الآن**.

2. انقر فوق **تكوين الاستقصاء**.

تفتح نافذة خصائص Active Directory. إذا كنت ترغب، قم بتعديل إعدادات استقصاء مجموعة Active Directory:

- **تمكين استقصاء ActiveDirectory**

ويتم تحديد هذا الخيار بصورة افتراضية. ولن، إذا كنت لا تستخدم Active Directory، فإن الاستقصاء لن يقوم باسترداد أي نتائج. في هذه الحالة، يمكنك إلغاء تحديد هذا الخيار.

- **تعيين جدول الاستقصاء**

المدة الافتراضية هي ساعة واحدة.

تتوفر خيارات جدول الاستقصاء التالية:

- **كل N يومًا**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N دقيقة**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل خمس دقائق، بداية من الوقت الحالي للنظام.

- **حسب أيام الأسبوع**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 00:00:6 مساءً.

- **كل شهر في أيام معينة من الأسابيع المحددة**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكلٍ افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 00:00:6 مساءً.

- **تشغيل المهام الفائتة**

إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تمكين هذا الخيار افتراضيًا.

- **خيارات متقدمة**

يمكنك تحديد أي مجالات Active Directory التي سيتم استقصائها:

- مجال Active Directory الذي ينتمي إليه Kaspersky Security Center.
- المجال الرئيسي الذي ينتمي إليه Kaspersky Security Center.
- القائمة المحددة لمجالات Active Directory.

إذا قمت بتحديد هذا الخيار، فيمكنك إضافة المجالات إلى نطاق الاستقصاء:

  - انقر على زر **إضافة**.
  - في الحقول المقابلة، حدد عنوان وحدة التحكم بالمجال، والاسم، وكلمة المرور للحساب للوصول إليه.
  - انقر فوق **موافق** لحفظ التغييرات.

يمكنك تحديد عنوان وحدة التحكم بالمجال في القائمة، وانقر فوق الأزرار **تعديل** أو **إزالة** لتعديله أو إزالته.

- انقر فوق **موافق** لحفظ التغييرات.

إذا كنت ترغب في إجراء الاستقصاء فورًا، انقر فوق الزر **استقصاء الآن**.

من خادم الإدارة الافتراضي، يمكنك عرض إعدادات الاستقصاء الخاصة بمجموعات Active Directory وتحريرها في نافذة خصائص نقطة التوزيع في القسم **اكتشاف الأجهزة**.

استقصاء نطاق IP

يستقصي خادم الإدارة نطاقات IP المحددة باستخدام حزم ICMP أو بروتوكول NBNS ويجمع مجموعة كاملة من البيانات على الأجهزة ضمن نطاقات IP هذه. يتم تعطيل نوع الاستقصاء هذا افتراضيًا.

بالنسبة لجميع المضيفين المستندين إلى Linux ضمن وحدة تحكم المجال Microsoft Active Directory أو Samba، حدد معلمتي `netbios name` و `workgroup` في الملف `/etc/samba/smb.conf`. وإلا، فقد تحتوي نتائج الاستطلاع على مضيفين مكررين.

قبل أن تبدأ استقصاء الشبكة، تأكد من تمكين بروتوكول SMB. خلاف ذلك، يتعذر على Kaspersky Security Center اكتشاف الأجهزة في الشبكة التي تم استطلاعها. لتمكين بروتوكول SMB، اتبع الإرشادات الخاصة بنظام التشغيل الخاص بك.

عرض وتعديل إعدادات استقصاء نطاق IP

لعرض وتعديل إعدادات استقصاء مجموعات نطاق IP:

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **نطاقات IP**.

   يمكنك المتابعة من المجلد **الأجهزة غير المخصصة** إلى المجلد **اكتشاف الأجهزة** من خلال النقر فوق **استقصاء الآن**.

2. إذا كنت ترغب، انقر فوق **إضافة شبكة فرعية** في المجلد الفرعي **نطاقات IP**، لإضافة نطاق IP للاستقصاء، ثم انقر فوق **موافق**.

3. انقر فوق **تكوين الاستقصاء**.

   تفتح نافذة خصائص نطاقات IP. إذا كنت ترغب، قم بتعديل إعدادات استقصاء نطاق IP:

- **تمكين استقصاء نطاق IP**

  لا يتم تحديد هذا الخيار بصورة افتراضية. لا يوصى باستخدام هذا النوع من الاستقصاء إذا كنت تستخدم استقصاء شبكة Windows و/أو استقصاء Active Directory.

- **تعيين جدول الاستقصاء**

  الفترة الافتراضية هي 420 دقيقة. يتم استبدال البيانات التي يتم تلقيها في الاستقصاء التالي بالبيانات القديمة بشكل كامل.

  تتوفر خيارات جدول الاستقصاء التالية:

  - **كل N يومًا**

    يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

    بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

  - **كل N دقيقة**

    يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

    بشكلٍ افتراضي، يعمل الاستقصاء كل خمس دقائق، بداية من الوقت الحالي للنظام.

  - **حسب أيام الأسبوع**

    يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

    بشكلٍ افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 00:00:6 مساءً.

  - **كل شهر في أيام معينة من الأسابيع المحددة**

    يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

    بشكلٍ افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 00:00:6 مساءً.

  - **تشغيل المهام الفائتة**

    إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

    إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تمكين هذا الخيار افتراضيًا.

إذا كنت ترغب في إجراء الاستقصاء فورًا، انقر فوق **استقصاء الآن**. يكون هذا الزر متاحًا فقط في إذا قمت بتحديد **تمكين استقصاء نطاق IP**.

من خادم الإدارة الافتراضي، يمكنك عرض إعدادات استقصاء نطاق IP وتحريرها في نافذة خصائص نقطة التوزيع، في القسم **اكتشاف الأجهزة**. يتم عرض الأجهزة العميلة المكتشفة أثناء استقصاء نطاقات IP في المجلد **المجالات** الخاص بخادم الإدارة الافتراضي.

استطلاع شبكة لا تتطلب تكوينًا

نوع الاستقصاء هذا مدعوم فقط لنقاط التوزيع المستندة إلى Linux.

يمكن لنقطة التوزيع استطلاع الشبكات التي تحتوي على أجهزة بعناوين IPv6. في هذه الحالة، لا يتم تحديد نطاقات IP وتقوم نقطة التوزيع باستقصاء الشبكة بالكامل باستخدام شبكات التكوين الصفري (يشار إليها باسم شبكة لا تتطلب تكوينًا). لبدء استخدام شبكة لا تتطلب تكوينًا، يجب عليك تثبيت أداة استعراض avahi على نقطة التوزيع.

لتمكين استقصاء شبكة لا تتطلب تكوينًا:

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **نطاقات IP**.

   يمكنك المتابعة من المجلد **الأجهزة غير المخصصة** إلى المجلد **اكتشاف الأجهزة** من خلال النقر فوق **استقصاء الآن**.

2. انقر فوق **تكوين الاستقصاء**.

3. في نافذة خصائص نطاقات IP التي تفتح، حدد **تمكين الاستقصاء باستخدام تقنية شبكة لا تتطلب تكوينًا**.

بعد ذلك، تبدأ نقطة التوزيع في استقصاء شبكتك. في هذه الحالة، يتم تجاهل نطاقات IP المحددة.

العمل مع مجالات Windows. عرض وتغيير إعدادات المجال

لتعديل إعدادات المجال:

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **المجالات**.

2. حدد مجالاً وافتح النافذة خصائص بإحدى الطرق التالية:

   - بتحديد **خصائص** من قائمة سياق المجال.
   - بالنقر فوق الرابط **عرض خصائص المجموعة**.

   تفتح النافذة **خصائص: <اسم المجال>** حيث يمكنك تكوين المجال المحدد.

تكوين قواعد الاستبقاء للأجهزة غير المخصصة

بعد اكتمال استقصاء شبكة Windows، يتم وضع الأجهزة التي تم العثور عليها في مجموعات فرعية من مجموعة إدارة الأجهزة غير المخصصة. يمكن العثور على مجموعة الإدارة هذه في **خيارات متقدمة** ← **اكتشاف الأجهزة** ← **المجالات**. يمثل مجلد **مجالات** المجموعة الرئيسية. يحتوي على مجموعات فرعية تمت تسميتها باسم المجالات ومجموعات العمل المطابقة التي تم العثور عليها أثناء إجراء استقصاء الشبكة. قد تحتوي المجموعة الرئيسية أيضًا على مجموعة الإدارة للأجهزة المحمولة. يمكنك تكوين قواعد الاستبقاء للأجهزة غير المخصصة للمجموعة الرئيسية ولكل مجموعة من المجموعات الفرعية. لا تعتمد قواعد الاستبقاء على إعدادات استقصاء الشبكة وتعمل حتى إذا تم تعطيل استقصاء الشبكة.

قم بما يلي لتكوين قواعد الاستبقاء للأجهزة غير المخصصة:

1. من شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة** قم بواحدة من الخطوات التالية:

- لتكوين إعدادات المجموعة الرئيسية، انقر بزر الماوس الأيمن فوق المجلد الفرعي **المجالات** ثم حدد **خصائص**.

  تفتح نافذة خصائص المجموعة الرئيسية.

- لتكوين إعدادات مجموعة فرعية، انقر بزر الماوس الأيمن فوق اسمها وحدد **خصائص**.

  تفتح نافذة خصائص المجموعة الفرعية.

2. في القسم **الأجهزة**، حدد الإعدادات التالية:

- **إزالة الجهاز من المجموعة إذا ظل غير نشط لمدة تزيد عن (بالأيام)**

  إذا تم تمكين هذا الخيار، فيمكنك تحديد الفترة الزمنية التي يتم بعدها إزالة الجهاز تلقائيًا من المجموعة. يتم افتراضيًا توزيع هذا الخيار أيضًا على المجموعات الفرعية. الفاصل الزمني الافتراضي هو 7 أيام.

  يتم تمكين هذا الخيار افتراضيًا.

- **توريث من المجموعة الأصلية**

  إذا تم تمكين هذا الخيار، فإنه يتم توارث فترة الاستبقاء للأجهزة في المجموعة الحالية من المجموعة الرئيسية ولا يمكن تغييرها.

  هذا الخيار متاح فقط للمجموعات الفرعية.

  يتم تمكين هذا الخيار افتراضيًا.

- **فرض التوريث في المجموعات الفرعية**

  سيتم توزيع قيم الإعداد إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم قفل هذه الإعدادات.

  يتم تعطيل هذا الخيار افتراضيًا.

تم حفظ وتطبيق التغييرات الخاصة بك.

العمل مع نطاقات IP

يمكنك تخصيص نطاقات IP الموجودة وإنشاء نطاقات جديدة.

إنشاء نطاق IP

لإنشاء نطاق IP:

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **نطاقات IP**.
2. من قائمة سياق المجلد، حدد **جديد** ← **نطاق IP**.
3. في النافذة **نطاق IP جديد** التي تفتح، قم بإعداد نطاق IP الجديد.

   يظهر نطاق IP الجديد في المجلد **نطاقات IP**.

عرض إعدادات نطاق IP وتغييرها

لتعديل إعدادات نطاق IP:

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **نطاقات IP**.
2. حدد نطاق IP وافتح نافذة الخصائص الخاصة به بإحدى الطرق التالية:
   - بتحديد **خصائص** من قائمة سياق نطاق IP.
   - بالنقر فوق الرابط **عرض خصائص المجموعة**.

   تفتح النافذة **خصائص: <اسم نطاق IP>** حيث يمكنك تكوين خصائص نطاق IP المحدد.

العمل مع مجموعات Active Directory. عرض وتعديل إعدادات المجموعة

لتعديل إعدادات مجموعة Active Directory :

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **Active Directory**.
2. حدد مجموعة Active Directory وافتح النافذة خصائص بإحدى الطرق التالية:
   - بتحديد **خصائص** من قائمة سياق نطاق IP.
   - بالنقر فوق الرابط **عرض خصائص المجموعة**.

   تفتح النافذة **خصائص: <اسم مجموعة Active Directory>** حيث يمكنك تكوين مجموعة Active Directory المحددة.

إنشاء قواعد لنقل الأجهزة إلى مجموعات الإدارة تلقائيًا

يمكنك تكوين نقل الأجهزة تلقائيًا إلى مجموعات الإدارة بعد أن يتم اكتشافها أثناء الاستقصاء في شبكة الشركة.

لتكوين قواعد لنقل الأجهزة إلى مجموعات الإدارة تلقائيًا:

1. من شجرة وحدة التحكم، حدد المجلد **الأجهزة غير المخصصة**.

2. في مساحة عمل هذا المجلد، انقر فوق **تكوين القواعد**.

يؤدي ذلك لفتح نافذة **خصائص: الأجهزة غير المخصصة** . في القسم **تحريك الجهاز**، قم بتكوين قواعد نقل الأجهزة إلى مجموعات الإدارة تلقائيًا.

سيتم تطبيق أول قاعدة قابلة للتطبيق في القائمة (من أعلى القائمة إلى أسفلها) على جهاز.

استخدام الوضع الديناميكي VDI على الأجهزة العميلة

يمكن نشر بنية تحتية افتراضية على شبكة الشركة باستخدام أجهزة ظاهرية مؤقتة. يقوم Kaspersky Security Center باكتشاف الأجهزة الظاهرية المؤقتة وإضافة معلومات بشأنهم إلى قاعدة بيانات خادم الإدارة. عقب انتهاء المستخدم من استخدام جهاز ظاهري مؤقت، تتم إزالة هذا الجهاز من البنية التحتية الافتراضية. ومع ذلك، يمكن حفظ سجل بشأن الجهاز الظاهري الذي تمت إزالته في قاعدة بيانات خادم الإدارة. وأيضًا، يمكن عرض الأجهزة الظاهرية غير الموجودة في وحدة تحكم الإدارة.

لمنع حفظ معلومات بشأن أجهزة ظاهرية غير موجودة، يدعم Kaspersky Security Center وضع ديناميكي للبيئة الأساسية لسطح المكتب الافتراضي (VDI). يستطيع المسؤول تمكين دعم الوضع الديناميكي لـ VDI في خصائص حزمة التثبيت من عميل الشبكة ليتم تثبيتها على الجهاز الظاهري المؤقت.

عند تعطيل جهاز ظاهري مؤقت، يقوم عميل الشبكة بإخطار خادم الإدارة بأن الجهاز قد تم تعطيله. إذا تم تعطيل جهاز ظاهري بنجاح، فتتم إزالته من قائمة الأجهزة المتصلة بخادم الإدارة. إذا تم تعطيل جهاز ظاهري مع وجود أخطاء ولم يرسل عميل الشبكة إخطار عن الجهاز الظاهري المُعطل لخادم الإدارة، يتم استخدام سيناريو النسخ الاحتياطي. في هذا السيناريو، تتم إزالة الجهاز الظاهري من قائمة الأجهزة المتصلة بخادم الإدارة بعد ثلاث محاولات فاشلة في التزامن مع خادم الإدارة.

تمكين وضع VDI الديناميكي في خصائص حزمة تثبيت عميل الشبكة

لتمكين الوضع الديناميكي VDI:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.

2. في قائمة سياق حزمة تثبيت عميل الشبكة، حدد **خصائص**.

يتم فتح نافذة **خصائص: عميل شبكة Kaspersky Security Center**.

3. في نافذة **خصائص: عميل شبكة Kaspersky Security Center**، حدد قسم **خيارات متقدمة**.

4. في قسم **خيارات متقدمة**، حدد خيار **تمكين الوضع الديناميكي لـ VDI**.

سيصبح الجهاز الذي يتم تثبيت عميل الشبكة عليه جزءًا من VDI.

البحث عن الأجهزة التي تُعد جزءًا من VDI

للعثور على الأجهزة غير المعينة التي تُعد جزءًا من VDI:

1. حدد **بحث** من قائمة سياق المجلد **الأجهزة غير المخصصة**.

للاطلاع على قائمة بجميع الأجهزة التي تعد جزءًا من البنية التحتية لسطح المكتب الافتراضي، حدد **بحث** من قائمة السياق لمجلد **خادم الإدارة**.

2. في النافذة **بحث**، في علامة التبويب **الأجهزة الظاهرية**، حدد **نعم** في مجموعة إعدادات **جزء من البنية الأساسية لسطح المكتب الافتراضي**.

3. انقر على زر **بحث الآن**.

يتم عرض قائمة بالأجهزة غير المعينة التي تعد جزءًا من البنية التحتية لسطح المكتب الافتراضي.

نقل الأجهزة من VDI إلى مجموعة إدارة

لنقل الأجهزة التي تُعد جزءًا من VDI إلى مجموعة إدارة:

1. في مساحة عمل المجلد **الأجهزة غير المخصصة**، انقر فوق **تكوين القواعد**.
   يؤدي هذا إلى فتح نافذة خصائص المجلد **الأجهزة غير المخصصة**.

2. في نافذة خصائص المجلد **الأجهزة غير المخصصة**، في القسم **تحريك الجهاز**، انقر فوق الزر **إضافة**.
   يتم فتح النافذة **قاعدة جديدة**.

3. في النافذة **قاعدة جديدة**، حدد القسم **الأجهزة الظاهرية**.

4. في القائمة المنسدلة **هذا جهاز ظاهري**، حدد **نعم**.

قاعدة سيتم إنشاؤها لتغيير موقع الجهاز إلى مجموعة الإدارة.

مخزون المعدات

تتم تعبئة قائمة المكونات (**المستودعات ← الأجهزة**) التي تستخدمها لجرد المعدات بطريقتين: تلقائيًا ويدويًا. وبعد كل عملية استقصاء للشبكة، تتم إضافة جميع الأجهزة المكتشفة إلى القائمة تلقائيًا؛ ومع ذلك، يمكنك أيضًا إضافة الأجهزة يدويًا إذا كنت لا ترغب في استقصاء الشبكة. ويمكنك إضافة أجهزة أخرى إلى القائمة يدويًا، على سبيل المثال، أجهزة التوجيه أو الطابعات أو مكونات الأجهزة.

من خصائص جهاز يمكنك عرض معلومات مفصلة حول هذا الجهاز وتحريرها.

قد تحتوي قائمة الأجهزة المكتشفة على أنواع الأجهزة التالية:

- أجهزة الكمبيوتر
- الأجهزة الجوالة
- أجهزة الشبكة
- الأجهزة الظاهرية
- مكونات OEM
- أجهزة الكمبيوتر الطرفية
- الأجهزة المتصلة
- هواتف VoIP
- مستودعات الشبكة

يمكن للمسؤول تخصيص سمة أجهزة المؤسسة للأجهزة المكتشفة. ويمكن تخصيص هذه السمة يدويًا في خصائص جهاز، أو يمكن للمسؤول تحديد معايير للسمة التي سيتم تخصيصها تلقائيًا. في هذه الحالة، يتم تخصيص سمة أجهزة المؤسسة حسب نوع الجهاز.

يسمح Kaspersky Security Center بشطب الأجهزة. للقيام بذلك، حدد خيار **تم شطب الجهاز** في خصائص أحد الأجهزة. الجهاز غير معروض على قائمة الأجهزة.

يمكن للمسؤول إدارة قائمة عناصر التحكم المنطقية القابلة للبرمجة (PLC) في المجلد **الأجهزة**. تتوفر المعلومات المفصلة حول قائمة عناصر التحكم المنطقية البرمجية (PLC) في دليل مستخدم Kaspersky Industrial CyberSecurity for Nodes.

إضافة معلومات حول الأجهزة الجديدة

لإضافة معلومات حول الأجهزة الجديدة على الشبكة:

1. في مجلد **المستودعات** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة**.
2. في مساحة العمل الخاصة بمجلد **الأجهزة**، انقر فوق الزر **إضافة جهاز** لفتح نافذة **جهاز جديد**.

   يتم فتح نافذة **جهاز جديد**.
3. في النافذة **جهاز جديد** في القائمة المنسدلة **النوع** حدد نوع الجهاز الذي تريد إضافته.
4. انقر على**موافق**.

   تفتح نافذة خصائص الجهاز في القسم **عام**.
5. في القسم **عام** املأ حقول الإدخال بالبيانات الموجودة على الجهاز. يتضمن القسم **عام** الإعدادات التالية:
   - **جهاز المؤسسة**. حدد خانة الاختيار إذا كنت ترغب في تعيين سمة المؤسسة إلى الجهاز. باستخدام هذه الميزة، يمكنك البحث عن الأجهزة في مجلد **الأجهزة**.
   - **تم شطب الجهاز**. حدد خانة الاختيار إذا كنت لا ترغب في عرض الجهاز في قائمة الأجهزة في المجلد **الأجهزة**.
6. انقر على **تطبيق** .

   سيتم عرض الجهاز الجديد في مساحة عمل المجلد **الأجهزة**.

تكوين المعايير المستخدمة لتحديد أجهزة المؤسسة

لتكوين معايير اكتشاف أجهزة المؤسسة:

1. في مجلد **المستودعات** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة**.
2. في مساحة عمل المجلد **الأجهزة**، انقر فوق الزر **إجراءات إضافية** وحدد **إعداد قاعدة لأجهزة المؤسسة** في القائمة المنسدلة.

   تفتح نافذة خصائص الجهاز.

3. في نافذة خصائص الأجهزة، في القسم **أجهزة المؤسسة**، حدد طريقة لتعيين السمة المؤسسة إلى الجهاز:

- **تعيين سمة جهاز المؤسسة يدويًا للجهاز**. يتم تعيين سمة أجهزة المؤسسة" للجهاز يدويًا في نافذة خصائص الجهاز، في القسم **عام**.
- **تعيين سمة جهاز المؤسسة تلقائيًا للجهاز**. في كتلة الإعدادات **حسب نوع الجهاز**، حدد أنواع الأجهزة التي سيقوم التطبيق بتعيين سمة المؤسسة لها بصورة تلقائية.

يؤثر هذا الخيار فقط على الأجهزة التي تمت إضافتها من خلال استقصاء الشبكة. بالنسبة للأجهزة المضافة يدويًا، اضبط سمة المؤسسة يدويًا.

4. انقر على **موافق** .

تم تكوين معايير الكشف عن أجهزة المؤسسة.

تكوين الحقول المخصصة

لتكوين حقول مخصصة من الأجهزة:

1. في مجلد **المستودعات** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة**.
2. في مساحة عمل مجلد **الأجهزة** ، انقر على زر **إجراءات إضافية**وحدد **تكوين خانات البيانات المخصصة** في القائمة المنسدلة.
   تفتح نافذة خصائص الجهاز.
3. في النافذة خصائص الجهاز، حدد القسم **حقول مخصصة** ثم انقر فوق الزر **إضافة**.
   تفتح نافذة **إضافة حقل**.
4. في النافذة **إضافة حقل**، حدد اسم الحقل المخصص الذي سيتم عرضه في خصائص الجهاز.
   يمكنك إنشاء حقول مخصصة متعددة بأسماء فريدة.
5. انقر على **موافق** .

يتم عرض الحقول التي تمت إضافتها في القسم **حقول مخصصة** الخاص بخصائص الجهاز. يمكنك استخدام الحقول المخصصة لتقديم معلومات محددة حول الأجهزة. على سبيل المثال، قد يكون هذا رقم الطلب الداخلي لشراء الجهاز.

الترخيص

يقدم هذا القسم معلومات حول المفاهيم العامة المتعلقة بترخيص Kaspersky Security Center 15.1.

تم تجاوز حد أحداث الترخيص

يسمح لك Kaspersky Security Center بالحصول على معلومات عن الأحداث عند تجاوز بعض حدود الترخيص بواسطة تطبيقات Kaspersky المثبتة على أجهزة العملاء.

يتم تحديد مستوى أهمية هذه الأحداث عند تجاوز أحد قيود الترخيص وفقًا للقواعد التالية:

- إذا كان عدد الوحدات المستخدمة حاليًا والتي يشملها ترخيص مفرد تشكّل ما بين 90% و100% من إجمالي عدد الوحدات المشمولة بواسطة الترخيص نفسه، فسيتم نشر الحدث بمستوى الأهمية **معلومات**.
- إذا كان عدد الوحدات المستخدمة حاليًا والتي يشملها ترخيص مفرد تشكّل ما بين 100% و110% من إجمالي عدد الوحدات المشمولة بواسطة الترخيص نفسه، فسيتم نشر الحدث بمستوى الأهمية **تحذير**.
- إذا كان عدد الوحدات المستخدمة حاليًا والتي يشملها ترخيص مفرد يتجاوز 110% من إجمالي عدد الوحدات المشمولة بواسطة الترخيص نفسه، فيتم نشر الحدث بمستوى الأهمية **حدث حرج**.

حول الترخيص

يحتوي هذا القسم على معلومات عن ترخيص تطبيقات Kaspersky التي يديرها Kaspersky Security Center.

حول الترخيص

الترخيص هو حق محدود بفترة زمنية لاستخدام تطبيق Kaspersky Security Center، ويتم منحه بموجب شروط عقد الترخيص الموقع (اتفاقية ترخيص المستخدم النهائي).

يعتمد نطاق الخدمات وفترة الصلاحية على الترخيص الذي يتم بموجبه استخدام التطبيق.

يتم توفير أنواع التراخيص التالية:

- تجريبي

  ترخيص مجاني مُعد لتجريب التطبيق. يحتوي الترخيص التجريبي عادة على فترة ترخيص قصيرة.

  بمجرد انتهاء صلاحية ترخيص تجريبي، تصبح جميع مزايا Kaspersky Security Center معطلة. للاستمرار في استخدام التطبيق، يجب شراء ترخيص تجاري.

  يمكنك استخدام التطبيق بموجب ترخيص تجريبي لفترة تجريبية واحدة فقط.

- تجاري

  ترخيص مدفوع.

  عند انتهاء صلاحية ترخيص تجاري، يتم تعطيل الميزات الرئيسية للتطبيق. للاستمرار في استخدام Kaspersky Security Center، يجب عليك تجديد ترخيصك التجاري. وبعد انتهاء صلاحية ترخيص تجاري، لا يمكنك الاستمرار في استخدام التطبيق ويجب إزالته من جهازك.

  وننصح بتجديد ترخيصك قبل انتهاء صلاحيته لضمان الحماية المستمرة ضد جميع تهديدات الأمان.

حول اتفاقية ترخيص المستخدم النهائي

اتفاقية ترخيص المستخدم النهائي (المشار إليها باتفاقية ترخيص أو EULA) هي اتفاقية إلزامية بينك وبين AO Kaspersky Lab تحدد البنود التي يمكنك بموجبها استخدام التطبيق.

يرجى قراءة اتفاقية الترخيص بعناية قبل البدء في استخدام التطبيق.

يحتوي Kaspersky Security Center ومكوناته، على سبيل المثال، على عميل الشبكة، واتفاقية ترخيص المستخدم النهائي (EULA) الخاصة بهم.

يمكنك عرض شروط اتفاقية ترخيص المستخدم النهائي لـ Kaspersky Security Center باستخدام الطرق التالية:

- أثناء تثبيت Kaspersky Security Center.
- من خلال قراءتك لمستند license.txt المضمن في حزمة توزيع Kaspersky Security Center.
- من خلال قراءتك لمستند license.txt الموجود في مجلد تثبيت Kaspersky Security Center.
- عن طريق تنزيل ملف License.txt من موقع Kaspersky الإلكتروني .

يمكنك عرض شروط اتفاقية ترخيص المستخدم النهائي لعميل الشبكة الخاص بنظام التشغيل Windows وعميل الشبكة الخاص بنظام التشغيل Mac وعميل الشبكة الخاص بنظام التشغيل Linux باستخدام الطرق التالية:

- أثناء تنزيل حزمة توزيع عميل الشبكة من خوادم الويب من Kaspersky.
- أثناء تثبيت عميل الشبكة الخاص بنظام التشغيل Windows أو عميل الشبكة الخاص بنظام التشغيل Mac أو عميل الشبكة الخاص بنظام التشغيل Linux.
- من خلال قراءة وثيقة license.txt المدرجة في عميل الشبكة الخاص بحزمة توزيع نظام التشغيل Windows أو عميل الشبكة الخاص بحزمة توزيع نظام التشغيل Mac أو عميل الشبكة الخاص بحزمة توزيع نظام التشغيل Linux.
- عن طريق قراءة وثيقة license.txt في عميل الشبكة الخاص بمجلد تثبيت نظام التشغيل Windows أو عميل الشبكة الخاص بمجلد تثبيت نظام التشغيل Mac أو عميل الشبكة الخاص بمجلد تثبيت نظام التشغيل Linux.
- عن طريق تنزيل ملف License.txt من موقع Kaspersky الإلكتروني .

يتم قبول بنود اتفاقية ترخيص المستخدم النهائي عن طريق تأكيد موافقتك على اتفاقية ترخيص المستخدم النهائي عند تثبيت التطبيق. في حالة عدم الموافقة على بنود اتفاقية الترخيص، يجب عليك إلغاء تثبيت التطبيق وعدم استخدامه.

حول شهادة الترخيص

شهادة الترخيص هي المستند الذي تستلمه مع ملف مفتاح أو رمز تنشيط.

تحتوي شهادة الترخيص على المعلومات التالية بشأن الترخيص المُقدّم:

- معرف الترخيص أو رقم الطلب
- معلومات حول المستخدم الذي تم منحه الترخيص.
- معلومات حول التطبيق الممكن تنشيطه بموجب الترخيص المُقدّم.
- حد عدد وحدات الترخيص (على سبيل المثال، الأجهزة التي يمكن استخدام التطبيق عليها بموجب الترخيص المُقدّم)
- تاريخ بدء صلاحية الترخيص
- تاريخ انتهاء صلاحية الترخيص أو فترة الترخيص
- نوع الترخيص

حول مفتاح الترخيص

مفتاح الترخيص هو سلسلة من وحدات بت التي يمكنك تطبيقها لتفعيل التطبيق ومن ثم استخدامه وفقًا لشروط اتفاقية ترخيص المستخدم النهائي. يتم إنشاء مفاتيح الترخيص بواسطة أخصائيين في Kaspersky.

يمكنك إضافة مفتاح ترخيص إلى التطبيق باستخدام إحدى الطرق التالية: عن طريق تطبيق ملف المفتاح أو عن طريق إدخال رمز التنشيط. يتم عرض مفتاح الترخيص في واجهة التطبيق بمثابة تسلسل أبجدي رقمي فريد من نوعه بعد قيامك بإضافته إلى التطبيق.

يمكن منع مفتاح الترخيص بواسطة Kaspersky في حالة انتهاك شروط اتفاقية الترخيص. إذا تم منع مفتاح الترخيص، فيجب إضافة مفتاح آخر إذا كنت ترغب في استخدام التطبيق.

يمكن أن يكون مفتاح الترخيص نشطًا أو إضافيًا (أو احتياطيًا).

مفتاح الترخيص المفعّل هو مفتاح الترخيص الذي يستخدم حاليًا من قبل التطبيق. يمكن إضافة مفتاح ترخيص مفعل لترخيص تجريبي أو تجاري. لا يمكن أن يستخدم التطبيق أكثر من مفتاح ترخيص واحد مفعل.

مفتاح الترخيص الإضافي (أو الاحتياطي) هو مفتاح ترخيص يُعطي المستخدم الحق في استخدام التطبيق ولكن لا يتم استخدامه حاليًا. يُصبح مفتاح الترخيص الإضافي مفعلًا تلقائيًا عند انتهاء صلاحية الترخيص المرتبط بمفتاح الترخيص المفعل الحالي. لا يمكن إضافة مفتاح ترخيص إضافي إلا اذا كان قد تم بالفعل إضافة مفتاح ترخيص مفعل.

يمكن إضافة مفتاح الترخيص للترخيص التجريبي كمفتاح الترخيص المفعل. لا يمكن إضافة مفتاح الترخيص للترخيص التجريبي كمفتاح الترخيص الإضافي.

حول ملف المفتاح

ملف المفتاح هو ملف بامتداد .key مقدم لك من قبل Kaspersky. تم تصميم ملفات المفتاح لتفعيل التطبيق من خلال إضافة مفتاح ترخيص.

تتلقى ملف المفتاح الخاص بك عبر عنوان البريد الإلكتروني الذي حددته عند شراء Kaspersky Security Center أو عند طلب الإصدار التجريبي من Kaspersky Security Center.

لتنشيط التطبيق باستخدام ملف المفتاح، فأنت لست بحاجة إلى الاتصال بخوادم تنشيط Kaspersky.

إذا تم حذف ملف المفتاح عن طريق الخطأ، فيمكنك استعادته. قد تحتاج إلى ملف المفتاح لتسجيل حساب Kaspersky CompanyAccount، على سبيل المثال.

لاستعادة ملف المفتاح الخاص بك، قم بتنفيذ أحد الإجراءات التالية:

- اتصل ببائع الترخيص.
- استلم ملف مفتاح عبر موقع الويب الخاص بـ Kaspersky باستخدام رمز التنشيط المتوفر لديك.
- تصدير ملف مفتاح ترخيص من خادم إدارة آخر.

حول الاشتراك

إن الاشتراك في Kaspersky Security Center هو أمر لاستخدام التطبيق بموجب الإعدادات المحددة (تاريخ انتهاء صلاحية الاشتراك، وعدد الأجهزة المحمية). يمكنك تسجيل اشتراكك في Kaspersky Security Center مع موفر الخدمة الخاص بك (على سبيل المثال، موفر خدمة الإنترنت). يمكن تجديد الاشتراك يدويًا أو في الوضع التلقائي، وكذلك يمكنك إلغائه.

يمكن أن يكون الاشتراك محدودًا (على سبيل المثال، لمدة عام واحد) أو غير محدود (دون تاريخ انتهاء صلاحية). لمواصلة استخدام Kaspersky Security Center بعد انتهاء صلاحية اشتراك محدود، يتوجب عليك تجديده. يتم تجديد الاشتراك غير المحدود تلقائيًا في حالة الدفع المسبق لموفر الخدمة في المواعيد المحددة.

عند انتهاء صلاحية اشتراك محدود، قد يتم توفير فترة سماح للتجديد يستمر خلالها عمل التطبيق. يتم تحديد توافر ومدة فترة السماح من قبل موفر الخدمة.

لاستخدام Kaspersky Security Center بموجب اشتراك، يجب تطبيق رمز التنشيط الذي تلقيته من موفر الخدمة.

يمكنك تطبيق رموز تنشيط مختلفة لـ Kaspersky Security Center فقط عند انتهاء صلاحية الترخيص الخاص بك أو عند قيامك بإلغائه.

اعتمادًا على موفر الخدمة، قد تختلف مجموعة الإجراءات الخاصة بإدارة التطبيق. قد لا يقوم موفر الخدمة بتوفير فترة سماح لتجديد الاشتراك ولذلك يتوقف عمل التطبيق.

لا يمكن استخدام رموز التنشيط التي تم شراؤها بموجب الاشتراك لتفعيل إصدارات سابقة من Kaspersky Security Center.

عند استخدام التطبيق بموجب اشتراك، يحاول Kaspersky Security Center بشكل تلقائي الوصول إلى خادم التفعيل في فترات زمنية محددة حتى انتهاء صلاحية الاشتراك. ويضمن ذلك مزامنة المعلومات عن الاشتراك مع خادم التفعيل. إذا تعذر الوصول إلى الخادم باستخدام DNS النظام، يستخدم التطبيق خوادم DNS العام. يمكنك تجديد اشتراكك على موقع ويب موفر الخدمة.

يمكنك تحديث المعلومات عن الاشتراك يدويًا، دون انتظار وصول Kaspersky Security Center إلى خادم التفعيل. على سبيل المثال، قد يكون هذا مفيدًا عند تغيير إعدادات الاشتراك.

لتحديث المعلومات عن الاشتراك يدويًا:

1. في شجرة وحدة التحكم، حدد المجلد **Kaspersky Licenses**.
2. انقر فوق **إجراءات إضافية**، ومن القائمة المنسدلة حدد **مزامنة إعدادات الاشتراك مع خادم الترخيص**.

يتم تحديث المعلومات عن الاشتراك على خادم التفعيل.

حول رمز التنشيط

رمز التنشيط هو تسلسل فريد مكون من 20 حرفًا أبجديًا رقميًا. حيث تقوم بإدخال رمز تنشيط لإضافة مفتاح ترخيص الذي يقوم بدوره بتنشيط Kaspersky Security Center. تتلقى رمز التفعيل من خلال عنوان البريد الإلكتروني الذي قمت بتحديده عقب شراء Kaspersky Security Center أو عقب طلب الإصدار التجريبي من Kaspersky Security Center.

لتفعيل التطبيق باستخدام رمز التفعيل، ستحتاج إلى الوصول إلى الإنترنت لإنشاء اتصال مع خوادم تفعيل Kaspersky. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة.

إذا كان التطبيق مفعلاً برمز تنشيط، فإن التطبيق في بعض الحالات يرسل طلبات عادية لخوادم تنشيط Kaspersky للتحقق من الحالة الحالية لمفتاح الترخيص. يجب توفير عملية وصول التطبيق إلى الإنترنت ليكون من الممكن إرسال طلبات.

إذا فقدت رمز التنشيط بعد تثبيت التطبيق، فاتصل بشريك Kaspersky الذي اشتريت الترخيص منه.

لا يمكنك استخدام ملفات المفتاح لتفعيل التطبيقات المدارة؛ حيث يتم قبول رموز التنشيط فقط.

إلغاء الموافقة على اتفاقية ترخيص المستخدم النهائي

إذا قررت إيقاف حماية أجهزة العميل، فيمكنك إلغاء تثبيت تطبيقات Kaspersky المدارة وإلغاء اتفاقية ترخيص المستخدم النهائي (EULA) لهذه التطبيقات.

لإلغاء EULA لتطبيقات Kaspersky المُدارة:

1. في شجرة وحدة التحكم، حدد **خادم الإدارة** ← **خيارات متقدمة** ← **اتفاقيات ترخيص المستخدم النهائي المقبولة**.

يتم عرض قائمة اتفاقيات ترخيص المستخدم النهائي—المقبولة عند إنشاء حزم التثبيت أو عند التثبيت السلس للتحديثات أو عند نشر Kaspersky Security for Mobile.

2. في القائمة، حدد اتفاقية ترخيص المستخدم النهائي التي ترغب في إبطالها.

يمكنك عرض الخصائص التالية لاتفاقية المستخدم النهائي:

- تاريخ قبول اتفاقية المستخدم النهائي.
- اسم حساب المستخدم الذي قبل اتفاقية المستخدم النهائي.
- رابط إلى شروط اتفاقية ترخيص المستخدم النهائي.
- قائمة الكائنات المتصلة بـ EULA: أسماء حزم التثبيت وأسماء التحديثات السلسة وأسماء تطبيقات الأجهزة المحمولة.

3. انقر على زر **إبطال اتفاقية المستخدم النهائي**.

في النافذة التي يتم فتحها، يتم إعلامك بضرورة إلغاء تثبيت تطبيق Kaspersky المقابل لاتفاقية ترخيص المستخدم النهائي.

4. انقر على الزر لتأكيد الإبطال.

يتحقق Kaspersky Security Center من إلغاء تثبيت حزم التثبيت (المقابلة لتطبيق Kaspersky المُدار الذي تريد إبطال اتفاقية ترخيص المستخدم النهائي الخاص به).

يمكنك إبطال EULA فقط لتطبيق Kaspersky تتم إدارته، ويتم حذف حزم التثبيت الخاصة به.

تم إبطال اتفاقية ترخيص المستخدم النهائي. لا يتم عرضه في قائمة اتفاقيات ترخيص المستخدم النهائي في **خادم الإدارة** ← **خيارات متقدمة** ← قسم **اتفاقيات ترخيص المستخدم النهائي المقبولة**. لا يمكنك حماية أجهزة العميل باستخدام تطبيق Kaspersky الذي قمت بإبطال اتفاقية ترخيص المستخدم النهائي الخاصة به.

بخصوص تزويد البيانات

نقل البيانات إلى أطراف خارجية

عند استخدام إدارة الأجهزة المحمولة في البرامج، وبغرض تسليم الأوامر في الوقت المناسب إلى الأجهزة التي تعمل بنظام التشغيل Android من خلال آلية الإشعارات المباشرة، يتم استخدام خدمة Google Firebase Cloud Messaging service. إذا قام المستخدم بتكوين استخدام خدمة Google Firebase Cloud Messaging، فإن المستخدم يقبل تقديم المعلومات التالية إلى خدمة Google Firebase Cloud Messaging في الوضع التلقائي: معرفات التثبيت الخاصة بتطبيقات Kaspersky Endpoint Security for Android التي يجب إرسال إشعارات مباشرة إليها.

لحظر تبادل المعلومات مع خدمة Google Firebase Cloud Messaging، يجب على المستخدم إعادة تعيين إعدادات الاستخدام لخدمةGoogle Firebase Cloud Messaging إلى قيمها الأصلية.

عند استخدام إدارة الأجهزة المحمولة في البرامج، وبغرض تسليم الأوامر في الوقت المناسب إلى الأجهزة التي تعمل بنظام التشغيل iOS من خلال آلية الإشعارات المباشرة، يتم استخدام خدمة Apple Push Notification Service (APNs). إذا قام المستخدم بتثبيت شهادة أسماء نقاط الوصول (APNs) على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM وإنشاء ملف تعريف iOS MDM ومجموعة من الإعدادات لتوصيل الأجهزة المحمولة التي تعمل بنظام iOS بالبرنامج وتثبيت ملف التعريف هذا على الأجهزة المحمولة، فإن المستخدم يوافق بذلك على تزويد APNS بالمعلومات التالية في الوضع التلقائي:

- الرمز المميز—الرمز المميز المباشر للجهاز. يستخدم الخادم هذا الرمز المميز عند إرسال إشعارات مباشرة إلى الجهاز.
- PushMagic—سلسلة يجب تضمينها في الإشعارات المباشرة. يتم إنشاء قيمة السلسلة بواسطة الجهاز.

البيانات التي تتم معالجتها محليًا

تم تصميم Kaspersky Security Center للتنفيذ المركزي لمهام الإدارة والصيانة الأساسية في شبكة المؤسسة. يُمكّن برنامج Kaspersky Security Center المسؤول من الوصول إلى المعلومات المفصلة حول مستوى أمان شبكة المؤسسة؛ ويسمح Kaspersky Security Center للمسؤول بتكوين جميع مكونات الحماية بناءً على تطبيقات Kaspersky. يؤدي Kaspersky Security Center الوظائف الأساسية التالية:

- اكتشاف الأجهزة ومستخدميها في شبكة المؤسسة
- إنشاء تسلسل هرمي لمجموعات الإدارة لإدارة الجهاز
- تثبيت تطبيقات Kaspersky على الأجهزة
- إدارة إعدادات التطبيقات المُثبتة ومهامها
- إدارة التحديثات لتطبيقات Kaspersky وتطبيقات الأطراف الخارجية، والبحث عن الثغرات الأمنية وإصلاحها
- تنشيط تطبيقات Kaspersky على الأجهزة
- إدارة حسابات المستخدمين
- عرض معلومات حول تشغيل تطبيقات Kaspersky على الأجهزة
- عرض التقارير

يمكن لـ Kaspersky Security Center تلقي المعلومات التالية وتخزينها ومعالجتها من أجل تأدية وظائفه الرئيسية:

- معلومات حول الأجهزة الموجودة على شبكة المؤسسة التي تم تلقيها من خلال فحص مجال Windows أو Active Directory أو وحدات تحكم مجال Samba، أو من خلال فحص مجالات IP. يحصل خادم الإدارة على البيانات بشكل مستقل أو يتلقى البيانات من عميل الشبكة الذي يعمل كنقطة توزيع.
- معلومات من Active Directory وSamba حول الوحدات التنظيمية والمجالات والمستخدمين والمجموعات. ويحصل خادم الإدارة على البيانات بشكل مستقل أو يتلقى البيانات من عميل الشبكة الذي يعمل كنقطة توزيع.
- تفاصيل الأجهزة المُدارة. يقوم عميل الشبكة بنقل البيانات المُدرجة أدناه من الجهاز إلى خادم الإدارة. يقوم المستخدم بإدخال اسم العرض ووصف الجهاز في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console:
  - المواصفات الفنية للجهاز المُدار ومكوناته المطلوبة لتعريف الجهاز: اسم عرض الجهاز ووصفه، واسم مجال Windows ونوعه، واسم الجهاز في بيئة Windows، ومجال DNS واسم DNS، وعنوان IPv4، وعنوان IPv6، وموقع الشبكة، وعنوان MAC، والرقم التسلسلي، ونوع نظام التشغيل، سواء كان الجهاز عبارة عن جهاز افتراضي مع نوع برنامج Hypervisor، أو إذا كان الجهاز عبارة عن جهاز افتراضي ديناميكي كجزء من VDI.
  - المواصفات الأخرى للأجهزة المُدارة ومكوناتها المطلوبة لمراجعة الأجهزة المُدارة واتخاذ القرارات بشأن ما إذا كان هناك تصحيحات وتحديثات معينة قابلة للتطبيق: حالة وكيل تحديث Windows (WUA)، وبنية نظام التشغيل، وبائع نظام التشغيل، ورقم بناء نظام التشغيل، ومعرف إصدار نظام التشغيل، ومجلد موقع نظام التشغيل، وفي حال كون الجهاز جهازًا افتراضيًا—نوع الجهاز الافتراضي؛ اسم خادم الإدارة الافتراضي الذي يدير الجهاز؛ بيانات جهاز السحابة (منطقة السحابة، VPC، منطقة توفر السحابة، الشبكة الفرعية للسحابة، منطقة وضع السحابة.
  - تفاصيل الإجراءات على الأجهزة المُدارة: تاريخ ووقت آخر تحديث، ووقت آخر ظهور للجهاز في الشبكة، وحالة انتظار إعادة التشغيل، ووقت تشغيل الجهاز.
  - تفاصيل حسابات مستخدمي الأجهزة وجلسات عملهم.
- البيانات المستلمة عن طريق تشغيل التشخيصات عن بعد على جهاز مُدار: ملفات التتبع، ومعلومات النظام، وتفاصيل تطبيقات Kaspersky المثبتة على الجهاز، وملفات التفريغ، وسجلات الأحداث، ونتائج تشغيل البرامج النصية للتشخيص المستلمة من الدعم الفني في Kaspersky.
- إحصائيات عملية نقطة التوزيع إذا كان الجهاز يمثل نقطة توزيع. يقوم عميل الشبكة بنقل البيانات من الجهاز إلى خادم الإدارة.

- إعدادات نقطة التوزيع التي أدخلها المستخدم في وحدة تحكم الإدارة أو Kaspersky Security Center Web Console.
- البيانات اللازمة لتوصيل الأجهزة المحمولة بخادم الإدارة: الشهادة، ومنفذ الاتصال المحمول، وعنوان اتصال خادم الإدارة. يدخل المستخدم البيانات في وحدة تحكم الإدارة أو Kaspersky Security Center Web Console.
- تفاصيل الأجهزة المحمولة التي تم نقلها باستخدام بروتوكول iOS MDM. يتم نقل البيانات المُدرجة أدناه من الجهاز المحمول إلى خادم الإدارة:
  - المواصفات الفنية للجهاز المحمول ومكوناته المطلوبة لتعريف الجهاز: اسم الجهاز، والطراز، واسم نظام التشغيل، ورقم بنية نظام التشغيل، ورقم طراز الجهاز، ورقم IMEI، وUDID، وMEID، والرقم التسلسلي، ومقدار الذاكرة، وإصدار البرامج الثابتة للمودم، وعنوان MAC الخاص بـ Bluetooth، وعنوان MAC الخاص بشبكة Wi-Fi، وتفاصيل بطاقة SIM (ICCID كجزء من معرف بطاقة SIM).
  - تفاصيل شبكة الهاتف المحمول المُستخدمة من خلال الجهاز المُدار: نوع شبكة الهاتف المحمول، واسم شبكة الهاتف المحمول المُستخدمة حاليًا، واسم شبكة الهاتف المحمول المنزلية، وإصدار إعدادات مشغل شبكة الهاتف المحمول، وحالة خدمة التجوال الصوتي، وحالة خدمة تجوال البيانات، ورمز البلد الخاص بالشبكة المنزلية، ورمز بلد الإقامة، ورمز بلد الشبكة المستخدمة حاليًا، ومستوى التشفير.
  - إعدادات الأمان الخاصة بالجهاز المحمول: استخدام كلمة مرور وتوافقها مع إعدادات السياسة، وقائمة ملفات تعريف التكوين، وملفات تعريف التزويد المُستخدمة لتثبيت تطبيقات تابعة لجهات خارجية.
  - تاريخ إجراء آخر عملية مزامنة مع خادم الإدارة وحالة إدارة الجهاز.
- تفاصيل تطبيقات Kaspersky المُثبتة على الجهاز. ينقل التطبيق المُدار البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة:
  - إعدادات تطبيقات Kaspersky المثبتة على الجهاز المُدار: اسم تطبيق Kaspersky وإصداره، وحالته، وحالة الحماية في الوقت الحقيقي، وتاريخ ووقت آخر فحص للجهاز، وعدد التهديدات التي تم اكتشافها، وعدد العناصر التي لم يتم تطهيرها، وتوافر وحالة مكونات التطبيق، ووقت آخر تحديث، وإصدار قواعد بيانات مكافحة الفيروسات، وتفاصيل إعدادات ومهام تطبيق Kaspersky، ومعلومات حول مفاتيح الترخيص المفعلة والاحتياطية، وتاريخ تثبيت التطبيق، والمعرف.
  - إحصائيات تشغيل التطبيق: الأحداث المتعلقة بالتغييرات في حالة مكونات تطبيق Kaspersky على الجهاز المُدار وأداء المهام التي بدأتها مكونات البرامج.
  - حالة الجهاز المحددة من خلال تطبيق Kaspersky.
  - العلامات المعيّنة بواسطة تطبيق Kaspersky.
  - مجموعة من التحديثات المُثبتة والسارية لتطبيق Kaspersky.
- البيانات المُتضمنة في الأحداث من مكونات Kaspersky Security Center وتطبيقات Kaspersky المُدارة. يقوم عميل الشبكة بنقل البيانات من الجهاز إلى خادم الإدارة.
- البيانات الضرورية لتكامل Kaspersky Security Center مع نظام SIEM من أجل تصدير الحدث. يدخل المستخدم البيانات في وحدة تحكم الإدارة أو Kaspersky Security Center Web Console.
- إعدادات مكونات Kaspersky Security Center وتطبيقات Kaspersky المُدارة والمقدمة في السياسات وملفات تعريف السياسات. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.
- إعدادات مهام مكونات Kaspersky Security Center وتطبيقات Kasperskyالمُدارة. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.
- البيانات التي تمت معالجتها بواسطة ميزة إدارة الثغرات الأمنية والتصحيحات. يقوم عميل الشبكة بنقل البيانات المُدرجة أدناه من الجهاز إلى خادم الإدارة:
  - تفاصيل التطبيقات والتصحيحات المُثبتة على الأجهزة المُدارة (سجل التطبيقات).
  - معلومات حول الأجهزة المُكتشفة على الأجهزة المُدارة (سجل الأجهزة).

في حالة تثبيت عميل الشبكة على جهاز يعمل بنظام Windows، فإنه يرسل إلى خادم الإدارة المعلومات التالية عن أجهزة الجهاز:

- الذاكرة العشوائية
- أجهزة تخزين كبيرة السعة
- اللوحة الأم
- CPU
- محولات الشبكة
- الشاشات
- محول الفيديو
- بطاقة الصوت

في حالة تثبيت عميل الشبكة على جهاز يعمل بنظام Linux أو macOS، فإنه يرسل إلى خادم الإدارة المعلومات التالية فقط عن مكونات الجهاز، إذا وفر نظام التشغيل هذه المعلومات:

- إجمالي حجم RAM
- الحجم الإجمالي لأجهزة التخزين عالية السعة
- اللوحة الأم
- CPU
- محولات الشبكة

- تفاصيل الثغرات الأمنية في برامج طرف خارجي المُكتشفة على الأجهزة المُدارة.
- تفاصيل التحديثات المتوفرة لتطبيقات الأطراف الخارجية المُثبتة على الأجهزة المُدارة.
- تفاصيل تحديثات Microsoft التي تم العثور عليها بواسطة ميزة WSUS.
- قائمة تحديثات Microsoft التي عُثر عليها بواسطة ميزة WSUS التي يجب تثبيتها على الجهاز.

- البيانات المطلوبة لتنزيل التحديثات على خادم الإدارة المعزول لإصلاح الثغرات الأمنية بالبرامج الناجمة عن جهات خارجية على الأجهزة المدارة. يقوم المستخدم بإدخال البيانات ونقلها باستخدام الأداة المساعدة klscflag لخادم الإدارة.
- البيانات الضرورية لعمل Kaspersky Security Center في بيئات السحابة (Amazon Web Services وMicrosoft Azure وGoogle Cloud وYandex Cloud). يدخل المستخدم البيانات في وحدة تحكم الإدارة أو Kaspersky Security Center Web Console.
- فئات مستخدمي التطبيقات. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.
- قائمة الملفات التنفيذية التي تم اكتشافها في الأجهزة المُدارة بواسطة ميزة التحكم في التطبيقات. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.
- تفاصيل الملفات الموضوعة في النسخ الاحتياطي. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.
- تفاصيل الملفات الموضوعة في العزل. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- تفاصيل الملفات التي طلبها أخصائيون في Kaspersky لإجراء تحليل مفصل عليها. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- تفاصيل الحالة وتشغيل قواعد مراقبة عيوب التكيف. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- تفاصيل الأجهزة الخارجية (وحدات الذاكرة، وأدوات نقل المعلومات، وأدوات النسخ المطبوع للمعلومات، وحافلات التوصيل) المُثبتة أو المُتصلة بالجهاز المُدار والتي تم اكتشافها بواسطة ميزة التحكم في الجهاز. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- معلومات حول الأجهزة المُشفرة وحالة التشفير. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة.

- تفاصيل أخطاء تشفير البيانات على الأجهزة التي يتم تنفيذ العملية عليها باستخدام ميزة تشفير البيانات في تطبيقات Kaspersky. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- قائمة وحدات التحكم المنطقية المُدارة القابلة للبرمجة (PLC). يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- البيانات المطلوبة لإنشاء سلسلة تطوير للتهديد. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- معلومات عن محاولات موظفي المؤسسة الوصول إلى الخدمات السحابية. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- البيانات المطلوبة لتكامل برنامج Kaspersky Security Center مع خدمة Kaspersky Managed Detection and Response (وجوب تثبيت المكون الإضافي المخصص لبرنامج Kaspersky Security Center Web Console): رمز بدء التكامل، ورمز التكامل، ورمز جلسة المستخدم. يدخل المستخدم البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center Web Console. تنقل خدمة Kaspersky MDR رمز التكامل ورمز جلسة المستخدم عبر المكون الإضافي المخصص.

- تفاصيل رموز التنشيط التي تم إدخالها أو الملفات الرئيسية المحددة. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.

- حسابات المستخدمين: الاسم والوصف والاسم بالكامل وعنوان البريد الإلكتروني ورقم الهاتف الرئيسي وكلمة المرور والمفتاح السري الذي تم إنشاؤه بواسطة خادم الإدارة وإدخال كلمة المرور لمرة واحدة للتحقق المكون من خطوتين. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.

- البيانات التي تحتاجها إدارة الوصول والهوية للمصادقة المركزية ولتوفير تسجيل دخول أحادي (SSO) بين تطبيقات Kaspersky المدمجة مع Kaspersky Security Center: إعدادات التثبيت والتكوين لإدارة الوصول والهوية وجلسة مستخدم إدارة الوصول والهوية ورموز إدارة الوصول والهوية المميزة وحالات تطبيق العميل وحالات خادم الموارد. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.

- محفوظات مراجعة كائنات الإدارة. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.

- عنوان IP للجهاز الذي أنشأ المستخدم المراجعة عليه. يتم تحديد عنوان IP بواسطة خادم الإدارة تلقائيًا.

- سجل كائنات الإدارة المحذوفة. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.

- حزم التثبيت التي تم إنشاؤها من الملف، وكذلك إعدادات التثبيت. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.

- البيانات المطلوبة لعرض إعلانات Kaspersky في Kaspersky Security Center Web Console. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة برنامج Kaspersky Security Center Web Console.

- البيانات المطلوبة لتشغيل المكونات الإضافية للتطبيقات المُدارة في Kaspersky Security Center Web Console التي تحفظها المكونات الإضافية في قاعدة بيانات خادم الإدارة أثناء تشغيلها الروتيني. يتم توفير وصف وطرق توفير البيانات في ملفات المساعدة للتطبيق المقابل.

- إعدادات مستخدم Kaspersky Security Center Web Console: لغة الترجمة وسمة الواجهة، وإعدادات عرض لوحة المراقبة، ومعلومات عن حالة الإشعارات (تمت قراءتها بالفعل/ لم تتم قراءتها بعد)، وحالة الأعمدة في جداول البيانات (إظهار / إخفاء)، ومدى تقدم وضع التدريب. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة برنامج Kaspersky Security Center Web Console.

- سجل أحداث Kaspersky الخاص بمكونات Kaspersky Security Center والتطبيقات التي يديرها برنامج Kaspersky. يتم تخزين سجل أحداث Kaspersky على كل جهاز ولا يتم نقلها مطلقًا إلى خادم الإدارة.

- شهادة التوصيل الآمن للأجهزة المُدارة ومكونات Kaspersky Security Center. ويقوم المستخدم بإدخال البيانات باستخدام الأداة المساعدة klsetsrvcert لخادم الإدارة.

- شهادات لإنشاء الثقة لموارد الويب الداخلية للمؤسسة. يدخل المستخدم البيانات في واجهة وحدة تحكم الإدارة أو واجهة برنامج Kaspersky Security Center Web Console.

- البيانات المطلوبة لتشغيل برنامج Kaspersky Security Center في البيئات السحابية، مثل Amazon Web Services (AWS) وMicrosoft Azure وGoogle Cloud وYandex.Cloud. يتلقى خادم الإدارة البيانات من الجهاز الافتراضي الذي يعمل عليه.

- معلومات حول قبول المستخدم لشروط وأحكام الاتفاقيات القانونية في برنامج Kaspersky.

- بيانات خادم الإدارة التي يُدخلها المستخدم في المكونات التالية:

  - وحدة تحكم الإدارة

  - Kaspersky Security Center Web Console

  - محطة سطر الأوامر عند استخدام الأداة المساعدة klscflag

  - تتفاعل المكونات مع خادم الإدارة عبر كائنات أتمتة klakaut وKaspersky Security Center OpenAPI

- أي بيانات يدخلها المستخدم في واجهة تحكم الإدارة أو واجهة Kaspersky Security Center Web Console.

يمكن أن تكون البيانات المُدرجة أعلاه موجودة في Kaspersky Security Center في حالة تطبيق إحدى الطرق التالية:

- يقوم المستخدم بإدخال البيانات في واجهة المكونات التالية:

  - وحدة تحكم الإدارة

  - Kaspersky Security Center Web Console

  - محطة سطر الأوامر عند استخدام الأداة المساعدة klscflag

  - تتفاعل المكونات مع خادم الإدارة عبر كائنات أتمتة klakaut وKaspersky Security Center OpenAPI

- يقوم عميل الشبكة باستقبال البيانات من الجهاز ونقلها إلى خادم الإدارة تلقائيًا.

- يتلقى عميل الشبكة البيانات التي تم استردادها من خلال التطبيق المُدار بواسطة Kaspersky ويقوم بنقلها إلى خادم الإدارة. يتم توفير قوائم البيانات، التي تتم معالجتها بواسطة التطبيقات المُدارة بواسطة Kaspersky، في ملفات التعليمات للتطبيقات المقابلة.

- يحصل خادم الإدارة على معلومات عن الأجهزة المتصلة بالشبكة بشكل مستقل أو يتلقى معلومات من عميل شبكة يعمل كنقطة توزيع.

- يتم نقل البيانات من الجهاز المحمول إلى خادم الإدارة باستخدام بروتوكول iOS MDM.

يتم تخزين البيانات المُدرجة في قاعدة بيانات خادم الإدارة. يتم تخزين أسماء المستخدمين وكلمات المرور في صيغة مشفرة.

لا يمكن نقل جميع البيانات التي تتم معالجتها محليًا إلى برنامج Kaspersky إلا من خلال ملفات التفريغ أو ملفات التتبع أو ملفات السجل الخاصة بمكونات Kaspersky Security Center، بما في ذلك ملفات السجل التي تم إنشاؤها بواسطة أدوات التثبيت والأدوات المساعدة.

تحتوي ملفات التفريغ أو ملفات التتبع الخاصة بمكونات Kaspersky Security Center على بيانات عشوائية لخادم الإدارة، وعميل الشبكة، ووحدة تحكم الإدارة، وخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، وKaspersky Security Center Web Console. يمكن أن تحتوي هذه الملفات على بيانات شخصية وحساسة. يتم تخزين ملفات التفريغ وملفات التتبع وملفات السجل على الجهاز بشكل غير مشفر. لا يتم تلقائيًا نقل ملفات التفريغ وملفات التتبع إلى Kaspersky؛ إلا أنه يمكن للمسؤول نقل البيانات إلى Kaspersky يدويًا بناءً على طلب الدعم الفني لحل المشكلات في عملية Kaspersky Security Center.

باتباع الروابط في وحدة تحكم الإدارة أو Kaspersky Security Center Web Console، يوافق المستخدم على النقل التلقائي للبيانات التالية:

- رمز Kaspersky Security Center
- إصدار Kaspersky Security Center
- ترجمة Kaspersky Security Center
- معرف الترخيص
- نوع الترخيص
- ما إذا تم شراء الترخيص عن طريق شريك

تعتمد قائمة البيانات المقدمة عبر كل رابط على الغرض من الارتباط وموقعه.

تستخدم Kaspersky البيانات المُستلمة بصيغة مجهولة المصدر والبيانات الخاصة بالإحصائيات العامة فقط. يتم إنشاء إحصائيات موجزة تلقائيًا من المعلومات التي تم تلقيها في الأصل ولا تحتوي على أي بيانات شخصية أو سرية. بمجرد تجميع البيانات الجديدة، يتم مسح البيانات السابقة (مرة واحدة سنويًا). يتم تخزين إحصائيات موجزة إلى أجل غير مسمى.

تحمي شركة Kaspersky أي معلومات يتم استلامها وفقًا لقانون وقواعد Kaspersky المعمول بها. تم نقل البيانات عبر قناة آمنة.

خيارات ترخيص Kaspersky Security Center

من الممكن أن يعمل Kaspersky Security Center في الأوضاع التالية:

- **لا يوجد ترخيص (الوظيفة الأساسية)**

  يعمل Kaspersky Security Center في هذا الوضع قبل تفعيل التطبيق أو بعد انتهاء صلاحية الترخيص التجاري. يتم توفير Kaspersky Security Center مع دعم الوظائف الأساسية لوحدة الإدارة كجزء من تطبيقات Kaspersky لحماية الشبكات المشتركة. كما يمكنك تنزيله من الموقع الإلكتروني لـ Kaspersky .

- **الترخيص التجاري**

  إذا كنت بحاجة إلى وظائف إضافية غير مضمنة في الوظائف الأساسية لوحدة تحكم الإدارة، يجب عليك شراء ترخيص تجاري.

  عند إضافة مفتاح ترخيص في نافذة خصائص خادم الإدارة، تأكد من إضافة مفتاح ترخيص يتيح لك استخدام Kaspersky Security Center. يمكنك العثور على هذه المعلومات على موقع ويب Kaspersky. تحتوي كل صفحة ويب لحل على قائمة بالتطبيقات المضمنة في هذا الحل. قد يقبل خادم الإدارة مفاتيح الترخيص غير المدعومة، مثل مفتاح الترخيص لتطبيق Kaspersky Endpoint Security Cloud، لكن مفاتيح الترخيص هذه لا توفر ميزات جديدة بالإضافة إلى الوظائف الأساسية لوحدة تحكم الإدارة.

الميزة أو الملكية	وضع تشغيل Kaspersky Security Center	
	لا يوجد ترخيص	الترخيص التجاري
الوظائف الأساسية لوحدة الإدارة تتوفر الوظائف التالية: • إنشاء خوادم إدارة افتراضية يتم استخدامها لإدارة شبكة المكاتب البعيدة أو مؤسسات العميل • إنشاء ترتيب هرمي لمجموعات الإدارة لإدارة مجموعة أجهزة محددة ككيان فردي. • تثبيت التطبيقات عن بُعد. • التكوين المركزي للتطبيقات المثبتة على الأجهزة العميلة. • التحكم في حالة أمان مكافحة الفيروسات للمؤسسة • إدارة أدوار المستخدمين. • إحصاءات وتقارير حول تشغيل التطبيق، بالإضافة إلى إخطارات حول الأحداث الحرجة • عمليات التشغيل المركزية للملفات التي تم نقلها إلى العزل أو النسخ الاحتياطي والملفات ذات المعالجة المؤجلة • التشفير وإدارة حماية البيانات. • عرض وترخيص مجموعات التطبيقات المرخصة الموجودة. • العرض والتحرير اليدوي لقائمة مكونات الأجهزة التي تم اكتشافها بواسطة استقصاء الشبكة • عرض قائمة بصور نظام التشغيل المتوفرة للتثبيت عن بُعد.	✓	✓
إدارة الثغرات الأمنية والتصحيحات: الوظائف الأساسية لا تتطلب المهام التالية ترخيصًا تجاريًا: • البحث عن Find vulnerabilities and required updates خلال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المُكتشفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة المُدارة. • مهمة تثبيت تحديثات Windows Update يمكن استخدام هذه المهمة لتثبيت تحديثات Windows Update فقط. لاستخدام هذه المهمة ، يجب عليك تحديد التحديثات المطلوبة يدويًا في إعدادات المهمة. • مهمة إصلاح الثغرات الأمنية تستخدم المهمة إصلاح الثغرات الأمنية الإصلاحات الموصى بها لبرامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية. لاستخدام هذه المهمة، يجب عليك تحديد إصلاحات المستخدم لثغرات أمنية في إعدادات المهام يدويًا.	✓	✓
إدارة الثغرات الأمنية والتصحيحات: الوظائف المتقدمة تتوفر الوظائف التالية: • التثبيت عن بُعد لتحديثات البرامج وإصلاح الثغرات الأمنية تلقائيًا، وفقًا للقواعد التي تحددها. • استخدام خادم الإدارة كخادم Windows Server Update Services (WSUS) لتوفير تحديثات لخدمات Windows Update على الأجهزة في الوضع المركزي وبالتكرار المحدد.	—	✓

الميزة أو الملكية	وضع تشغيل Kaspersky Security Center	
	لا يوجد ترخيص	الترخيص التجاري
ميزة إدارة الأجهزة المحمولة في وحدة تحكم الإدارة المستندة إلى MMC تُستخدم ميزة إدارة الأجهزة المحمولة لإدارة أجهزة MDM التي تعمل بنظامي التشغيل iOS وAndroid. تتوفر الوظائف التالية لأجهزة iOS MDM: • إضافة أجهزة جديدة تحت إدارة Kaspersky Security Center. • إنشاء وتحرير ملفات تعريف التكوين، وتثبيت ملفات تعريف التكوين على الأجهزة المحمولة. • تثبيت التطبيقات على الأجهزة المحمولة إما من خلال App Store® أو باستخدام ملفات البيان (.plist) أو باستخدام حزم التثبيت للأجهزة المحمولة (.ipa). • تنفيذ الأوامر على أجهزة MDM التي تعمل بنظام iOS، بما في ذلك قفل الأجهزة المحمولة، وإعادة تعيين كلمة مرور الجهاز المحمول، وحذف جميع البيانات من الجهاز المحمول. تتوفر الوظائف التالية لأجهزة Android: • إضافة أجهزة جديدة تحت إدارة Kaspersky Security Center. • إدارة Kaspersky Endpoint Security for Android من خلال السياسة. • تنفيذ الأوامر على الأجهزة. وحدة الإدارة لإدارة الأجهزة المحمولة هي جهاز محمول. يتم وضع في الاعتبار إدارة جهاز محمول منذ اتصاله بخادم الأجهزة المحمولة.	—	✓ (يجب إضافة مفتاح ترخيص إلى خصائص خادم الإدارة.)
حماية الجهاز المحمول في Kaspersky Security Center Web Console يوفر لك Kaspersky Security Center Web Console الميزات التالية لإدارة الأجهزة المحمولة التي تعمل بنظام التشغيل Android وiOS: • إضافة أجهزة جديدة تحت إدارة Kaspersky Security Center. • إدارة Kaspersky Endpoint Security for Android وKaspersky Security for iOS من خلال السياسات. • إرسال الأوامر إلى الأجهزة المحمولة من خلال البروتوكولات ذات الصلة وتنفيذ الأوامر.	—	✓ (يجب إضافة مفتاح ترخيص على كل جهاز محمول.)
إدارة النظام تتوفر الوظائف التالية: • تثبيت نظم التشغيل والتطبيقات. يتيح لك Kaspersky Security Center إنشاء صور نظام التشغيل ونشرها على الأجهزة العميلة عبر الشبكة، وجراء تثبيت عن بُعد للتطبيقات بواسطة Kaspersky أو البائعين الآخرين. يمكنك التقاط صور نظام التشغيل من الأجهزة ونقل هذه الصور إلى خادم الإدارة. يتم تخزين صور أنظمة التشغيل على خادم الإدارة في مجلد مخصص. يمكن التقاط صورة نظام تشغيل جهاز مرجعي وإنشاؤها عن طريق مهمة إنشاء حزمة التثبيت. يمكنك استخدام الصور التي تم استلامها لنشرها على الأجهزة الجديدة المتصلة بالشبكة التي لم يتم تثبيت نظام تشغيل عليها بعد. يتم استخدام تقنية Preboot eXecution Environment (PXE) في هذه الحالة. • إدارة مجموعة التطبيقات المرخصة. • الإذن البعيد للاتصال بالأجهزة العميلة عبر مكون من Microsoft® Windows® يسمى اتصال سطح المكتب عن بُعد. • الاتصال بالأجهزة العميلة عن بُعد من خلال مشاركة سطح المكتب لـ Windows • الاتصال عن بعد من خلال **عارض جلسة سطح المكتب الجديد من Kaspersky**.	—	✓
الاندماج باستخدام البيئات السحابية Kaspersky Security Center لا يعمل مع الأجهزة الموجودة في موقع العمل فحسب، بل يوفر أيضًا ميزات خاصة للعمل في بيئة السحابة، مثل معالج تكوين بيئة السحابة. يعمل Kaspersky Security Center مع الأجهزة الافتراضية التالية: • مثيلات Amazon EC2 • أجهزة Microsoft Azure الافتراضية • مثيلات أجهزة Google Cloud الافتراضية • الأجهزة الافتراضية لخدمة Yandex.Cloud	—	✓
تصدير الأحداث إلى أنظمة إدارة معلومات الأمان والأحداث (SIEM): استخدام بروتوكول Syslog باستخدام بروتوكول Syslog، يمكنك ترحيل أي من الأحداث التي تحدث في خادم إدارة Kaspersky Security Center وفي تطبيقات Kaspersky المثبتة على الأجهزة المدارة. بروتوكول Syslog هو بروتوكول قياسي لتسجيل الرسائل. يمكنك استخدامه لتصدير الأحداث إلى أي نظام SIEM.	✓	✓

ميزات الترخيص الخاصة بـ Kaspersky Security Center والتطبيقات المدارة

يتضمن ترخيص خادم الإدارة والتطبيقات المدارة ما يلي:

- لا يمكنك إضافة إلا مفتاح ترخيص أو رمز تنشيط صالح إلى خادم الإدارة لتفعيل مزايا إدارة الثغرات الأمنية والتصحيحات أو إدارة الأجهزة المحمولة أو التكامل مع أنظمة SIEM. لا يمكن الوصول إلى بعض مزايا Kaspersky Security Center إلا اعتمادًا على ملفات المفاتيح المفعلة أو رموز التنشيط الصالحة المضافة إلى خادم الإدارة.

- يمكنك إضافة العديد من رموز التنشيط وملفات المفاتيح للتطبيقات المدارة إلى مستودع خادم الإدارة.

حول ترخيص Kaspersky Security Center

إذا قمت بتفعيل إحدى الميزات المرخصة (على سبيل المثال، إدارة الجهاز المحمول) باستخدام ملف المفتاح، ولكنك تريد أيضًا استخدام ميزة مرخصة أخرى (على سبيل المثال، إدارة الثغرات الأمنية والتصحيحات)، فإنه يجب عليك شراء ملف المفتاح يقوم بتفعيل كلتا الميزتين من مقدم الخدمة الذي تتعامل معه ويجب عليك تفعيل خادم الإدارة باستخدام ملف المفتاح هذا.

ميزات الترخيص الخاصة بالتطبيقات المدارة

لترخيص التطبيقات المدارة، يمكن نشر رمز التنشيط أو ملف المفتاح تلقائيًا أو بأي طريقة أخرى ملائمة. يمكن تطبيق الطرق التالية لنشر رمز تنشيط أو ملف المفتاح:

- النشر التلقائي

> إذا كنت تستخدم تطبيقات مدارة مختلفة وكان عليك نشر ملف مفتاح محدد أو رمز تنشيط للأجهزة، فقم باختيار طرق أخرى لنشر ملف المفتاح أو رمز التفعيل هذا.

يتيح لك Kaspersky Security Center نشر مفاتيح الترخيص المتاحة تلقائيًا إلى الأجهزة. على سبيل المثال، يتم تخزين ثلاثة مفاتيح ترخيص في مستودع خادم الإدارة. لقد حددت خانة الاختيار **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها** لجميع مفاتيح الترخيص الثلاثة. تطبيق أمان Kaspersky — على سبيل المثال، تم تثبيت Kaspersky Endpoint Security for Windows على أجهزة المؤسسة. تم اكتشاف الجهاز الجديد الذي يجب نشر المفتاح إليه. يحدد التطبيق على سبيل المثال، أنه يمكن تطبيق اثنين من مفاتيح التراخيص المتواجدة في المستودع إلى الجهاز وهما: مفتاح ترخيص باسم Key_1 ومفتاح ترخيص باسم Key_2. يتم نشر أحد هذين المفتاحين إلى الجهاز. وفي هذه الحالة، لا يمكن توقع مفتاح الترخيص الذي سيتم نشره إلى الجهاز لأن النشر التلقائي لمفاتيح التراخيص لا يسمح بإجراء أي نشاط للمسؤول.

عندما يتم نشر مفتاح ترخيص، تتم إعادة احتساب الأجهزة لمفتاح الترخيص هذا. ويجب عليك التأكد من أن عدد الأجهزة التي تم نشر مفتاح الترخيص إليها لا يتجاوز حد الترخيص. إذا تجاوز عدد الأجهزة حد الترخيص، فسيتم تعيين حالة جميع الأجهزة التي لم تكن مشمولة بالترخيص إلى الحالة حرج.

- إضافة ملف المفتاح أو رمز تنشيط إلى حزمة التثبيت الخاصة بتطبيق مُدار

إذا قمت بتثبيت تطبيق مدار باستخدام حزمة تثبيت، يمكنك تحديد رمز تنشيط أو ملف المفتاح في حزمة التثبيت هذه أو في السياسة الخاصة بالتطبيق. سيتم نشر مفتاح الترخيص إلى الأجهزة المُدارة عند إجراء المزامنة التالية للجهاز مع خادم الإدارة.

- النشر من خلال مهمة إضافة مفتاح الترخيص إلى تطبيق مُدار

إذا اخترت استخدام مهمة إضافة مفتاح الترخيص لتطبيق مُدار، يمكنك تحديد مفتاح الترخيص الذي يجب نشره إلى الأجهزة وتحديد الأجهزة بأية طريقة ملائمة، على سبيل المثال من خلال تحديد مجموعة إدارة أو تحديد جهاز.

- إضافة رمز التنشيط أو ملف المفتاح إلى الأجهزة يدويًا

تطبيقات Kaspersky. النشر المركزي

يبين هذا القسم طرق التثبيت عن بُعد لتطبيقات Kaspersky وإزالتها من الأجهزة المتصلة بالشبكة.

قبل نشر التطبيقات على الأجهزة العميلة، تأكد من توافق أجهزة وبرامج الأجهزة العميلة مع المتطلبات المعمول بها.

عميل الشبكة هو مكون يوفر اتصال خادم الإدارة بالأجهزة العميلة. ولذلك، يجب تثبيته على كل جهاز عميل ليتم توصيله بنظام التحكم المركزي عن بُعد. يستطيع الجهاز المثبت عليه خادم الإدارة استخدام إصدار الخادم من عميل الشبكة فقط. هذا الإصدار مضمن في خادم الإدارة كجزء يتم تثبيته وإزالته معه. لا يلزم تثبيت عميل الشبكة على ذلك الجهاز.

يمكن تثبيت عميل الشبكة عن بُعد أو محليًا مثل أي تطبيق. أثناء النشر المركزي لتطبيقات الأمان من خلال وحدة تحكم الإدارة، يمكنك تثبيت عميل الشبكة مع تطبيقات الأمان بشكل مشترك.

يمكن أن يختلف وكلاء الشبكة باختلاف تطبيقات Kaspersky التي تستخدمها معهم. في بعض الحالات، يمكن تثبيت عميل الشبكة محليًا فقط (للحصول على التفاصيل راجع الوثائق الخاصة بالتطبيقات المقابلة). لا يتعين عليك سوى تثبيت عميل الشبكة على جهاز عميل مرة واحدة.

تتم إدارة تطبيقات Kaspersky عبر وحدة تحكم الإدارة باستخدام مكونات الإدارة الإضافية. لذا، للوصول إلى واجهة إدارة التطبيق من خلال Kaspersky Security Center، يجب تثبيت مكون الإدارة الإضافي المقابل على محطة عمل المسؤول.

يمكنك تنفيذ مهمة التثبيت عن بُعد للتطبيقات من محطة عمل المسؤول من نافذة Kaspersky Security Center الرئيسية.

لتثبيت البرنامج عن بُعد، يجب إنشاء مهمة تثبيت عن بُعد.

ستبدأ مهمة التثبيت عن بُعد التي تن إنشاؤها وفقًا للجدول الخاص بها. يمكنك مقاطعة إجراءات التثبيت عن طريق إيقاف المهمة يدويًا.

إذا أعاد التثبيت عن بعد للتطبيق خطأً، فتأكد من استيفاء متطلبات إعداد الجهاز.

يمكنك تتبع تقدم التثبيت عن بُعد لتطبيقات Kaspersky على إحدى الشبكات باستخدام تقرير النشر.

للحصول على تفاصيل حول إدارة التطبيقات المسردة في Kaspersky Security Center، يرجى الرجوع إلى الوثائق الخاصة بالتطبيقات المقابلة.

استبدال تطبيقات الأمان من جهة خارجية

قد يتطلب تثبيت تطبيقات الأمان الخاصة بـ Kaspersky عبر Kaspersky Security Center إزالة برنامج الجهة الخارجية غير المتوافق مع التطبيق الذي يتم تثبيته. يوفر Kaspersky Security Center عدة طرق تتعلق بإزالة تطبيقات الجهات الخارجية.

إزالة التطبيقات غير المتوافقة من خلال استخدام برنامج التثبيت

يتوفر هذا الخيار فقط في وحدة تحكم الإدارة القائمة على وحدة تحكم Microsoft Management Console.

يتم دعم وسيلة برنامج التثبيت الخاصة بإزالة التطبيقات غير المتوافقة بواسطة أنواع التثبيت المختلفة. قبل تثبيت تطبيق الأمان، تتم إزالة كل التطبيقات غير المتوافقة تلقائيًا إذا كانت نافذة الخصائص الخاصة بحزمة التثبيت لتطبيق الأمان هذا (القسم **تطبيقات غير متوافقة**) تم تحديد خيار **إلغاء تثبيت التطبيقات غير المتوافقة تلقائيًا** بها.

إزالة التطبيقات غير المتوافقة عند تكوين التثبيت عن بُعد لأحد التطبيقات

يمكنك تمكين الخيار **إلغاء تثبيت التطبيقات غير المتوافقة تلقائيًا** عند تكوين التثبيت عن بُعد لأحد تطبيقات الأمان. في وحدة تحكم الإدارة القائمة على وحدة التحكم Microsoft Management Console (MMC)، يتوفر هذا الخيار في معالج التثبيت عن بُعد. في Kaspersky Security Center Web Console، يمكنك العثور على هذا الخيار في معالج نشر الحماية. عند تمكين هذا الخيار، يزيل Kaspersky Security Center التطبيقات غير المتوافقة قبل تثبيت تطبيق أمان على جهاز مُدار.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إزالة التطبيقات غير المتوافقة باستخدام معالج التثبيت عن بُعد
- Kaspersky Security Center Web Console: إزالة التطبيقات غير المتوافقة قبل التثبيت

إزالة التطبيقات غير المتوافقة من خلال مهمة محددة

لإزالة تطبيقات غير متوافقة، استخدم المهمة **إلغاء تثبيت التطبيق عن بُعد**. يجب أن تعمل هذه المهمة على الأجهزة قبل مهمة تثبيت تطبيق الأمان. على سبيل المثال، في مهمة التثبيت، يمكنك تحديد **عند إكمال مهمة أخرى** كنوع الجدول حيث تكون المهمة الأخرى هي **إلغاء تثبيت التطبيق عن بُعد**.

طريقة إلغاء التثبيت هذه مفيدة عند عدم تمكّن مثبت تطبيق الأمان من إزالة التطبيق غير متوافق بشكل صحيح.

تعليمات إرشادية لوحدة التحكم الإدارية: إنشاء مهمة .

تثبيت التطبيقات باستخدام مهمة التثبيت عن بُعد

يسمح لك Kaspersky Security Center بتثبيت التطبيقات على الأجهزة عن بُعد، باستخدام مهام التثبيت عن بُعد. ويتم إنشاء هذه المهام وتعيينها إلى الأجهزة من خلال المعالج المخصص. لتعيين مهمة بصورة أكثر سرعة وسهولة، يمكنك تحديد الأجهزة (حتى 1000 جهاز) في نافذة المعالج بأي طريقة من الطرق التالية:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة** . في هذه الحالة، يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**. يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.
- **تعيين مهمة إلى تحديد الجهاز** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في المجموعة المحددة التي تم إنشائها في وقت سابق. يمكنك تحديد المجموعة المحددة مسبقًا أو المجموعة المخصصة التي أنشأتها.
- **تعيين مهمة لمجموعة إدارة** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة تم إنشائها في وقت سابق.

لتجنب المشكلات التي قد تحدث أثناء تثبيت التطبيق على جهاز عميل بدون تثبيت عميل الشبكة، يجب عليك المتابعة كما هو موضح في النشر الإجباري عبر مهمة تثبيت عن بُعد من Kaspersky Security Center.

تثبيت تطبيق على الأجهزة المحددة

لتثبيت تطبيق على الأجهزة المحددة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. قم بتشغيل إنشاء المهمة بالنقر فوق الزر **إنشاء مهمة**.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

في نافذة **تحديد نوع المهمة** الخاصة بمعالج المهمة الجديدة، في القسم **خادم إدارة Kaspersky Security Center**، حدد **تثبيت التطبيق عن بُعد** كنوع المهمة.

ينشئ معالج المهمة الجديدة مهمة للتثبيت عن بُعد للتطبيق المحدد لأجهزة محددة. يتم عرض المهمة التي تم إنشاؤها حديثًا في مساحة عمل المجلد **المهام**.

3. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

عند إكمال مهمة التثبيت عن بُعد، سيتم تثبيت التطبيق المحدد على الأجهزة المحددة.

تثبيت تطبيق على الأجهزة العميلة في مجموعة الإدارة

لتثبيت تطبيق على أجهزة الكمبيوتر العميلة في مجموعة إدارة:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في مجموعة الإدارة ذات الصلة.

2. حدد مجموعة إدارة في شجرة وحدة التحكم.

3. في مساحة عمل المجموعة، حدد علامة التبويب **المهام**.

4. قم بتشغيل إنشاء المهمة بالنقر فوق الزر **إنشاء مهمة**.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

في نافذة **تحديد نوع المهمة** الخاصة بمعالج المهمة الجديدة، في القسم **خادم إدارة Kaspersky Security Center**، حدد **تثبيت التطبيق عن بُعد** كنوع المهمة.

ينشئ معالج المهمة الجديدة مهمة جماعية للتثبيت عن بُعد للتطبيق المحدد. تظهر المهمة الجديدة في مساحة عمل مجموعة الإدارة على علامة التبويب **المهام**.

5. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

عند إكمال مهمة التثبيت عن بُعد، سيتم تثبيت التطبيق المحدد على الأجهزة العميلة في مجموعة الإدارة.

تثبيت تطبيق من خلال سياسات مجموعة Active Directory

يتيح لك Kaspersky Security Center تثبيت تطبيقات Kaspersky على الأجهزة المدارة باستخدام سياسات مجموعة Active Directory. يجب أن يكون جهاز خادم الإدارة في المجال نفسه الخاص بالأجهزة المُدارة.

يمكنك تثبيت التطبيقات باستخدام سياسات مجموعة Active Directory من خلال حزم التثبيت التي تتضمن عامل الشبكة.

لتثبيت التطبيقات باستخدام سياسات مجموعة Active Directory:

1. ابدأ تكوين تثبيت التطبيق باستخدام معالج التثبيت عن بُعد.

2. في النافذة **تحديد إعدادات مهمة التثبيت عن بُعد** في معالج التثبيت عن بُعد، حدد الخيار **تعيين تثبيت الحزمة في سياسات مجموعة Active Directory**.

3. في النافذة **تحديد حسابات للوصول إلى الأجهزة** في معالج التثبيت عن بُعد، حدد الخيار **يُلزم وجود حساب (عميل الشبكة غير مستخدم)**.

4. أضف الحساب الذي يمتلك امتيازات المسؤول على الجهاز المثبت عليه Kaspersky Security Center أو الحساب المضمن مجموعة المجالGroup Policy Creator Owners.

5. منح الأذونات للحساب المحدد:

   a. انتقل إلى **لوحة التحكم** ← **الأدوات الإدارية** وافتح **إدارة سياسة المجموعة**.

   b. انقر فوق العقدة مع المجال المطلوب.

   c. انقر فوق قسم **التفويض**.

   d. في القائمة المنسدلة **الإذن**، حدد **ربط عناصر سياسة المجموعة**.

   e. انقر فوق **إضافة**.

   f. في نافذة **تحديد المستخدم أو الكمبيوتر أو المجموعة** التي تفتح، حدد الحساب المطلوب.

   g. انقر فوق **موافق** لإغلاق نافذة **تحديد مستخدم أو كمبيوتر أو مجموعة**.

   h. في قائمة **المجموعات والمستخدمين**، حدد الحساب الذي أضفته للتو وانقر فوق **إعدادات متقدمة** ← **إعدادات متقدمة**.

   i. في قائمة **إدخالات الأذونات**، انقر نقرًا مزدوجًا فوق الحساب الذي أضفته للتو.

   j. امنح الأذونات التالية:

   - **إنشاء عناصر المجموعة**
   - **حذف عناصر المجموعة**
   - **إنشاء كائنات مجموعة حاوية السياسة**
   - **حذف كائنات مجموعة حاوية السياسة**

   k. انقر فوق **موافق** لحفظ التغييرات.

6. حدد الإعدادات الأخرى باتباع تعليمات المعالج.

7. قم بتشغيل مهمة التثبيت عن بُعد يدويًا أو انتظر حتى تبدأ وفق جدولها.

تبدء سلسلة عمليات التثبيت عن بُعد التالية:

1. عندما تشغيل كل مهمة، يتم إنشاء الكائنات التالية في كل مجال يتضمن أي من الأجهزة العميلة من المجموعة المحددة:

   - كائن سياسة المجموعة (GPO) باسم **Kaspersky_AK{GUID}**.
   - مجموعة الأمان التي تتوافق مع GPO. تتضمن مجموعة الأمان هذه أجهزة عميلة مغطاة بواسطة المهمة. ويحدد محتوى مجموعة الأمان نطاق GPO.

2. يقوم Kaspersky Security Center بتثبيت تطبيقات Kaspersky المحددة على الأجهزة العميلة مباشرةً من KLSHARE، أي مجلد الشبكة المشترك للتطبيق. في مجلد تثبيت Kaspersky Security Center، سيتم إنشاء مجلد فرعي احتياطي يحتوي على ملف msi. لتثبيت التطبيق.

3. إذا تمت إضافة الأجهزة الجديدة إلى نطاق المهمة، تتم إضافتها إلى مجموعة الأمان بعد البدء التالي للمهمة. إذا تم تحديد الخيار **Run missed tasks** في جدول المهمة، تتم إضافة الأجهزة إلى مجموعة الأمان فورًا.

4. إذا تم حذف الأجهزة من نطاق المهمة، فيتم حذفها من مجموعة الأمان بعد البدء التالي للمهمة.

5. عند حذف مهمة من Active Directory، يتم أيضًا حذف GPO ورابط GPO ومجموعة الأمان المطابقة أيضًا.

إذا أردت تطبيق نظام تثبيت آخر باستخدام Active Directory، يمكنك تكوين الإعدادات المطلوبة يدويًا. على سبيل المثال، قد يكون هذا مطلوبًا في بعض الحالات:

- عندما لا يتمتع مسؤول الحماية ضد الفيروسات بالحقوق اللازمة لإجراء تغييرات على Active Directory لمجالات معينة.
- عندما يجب تخزين حزمة التثبيت الأصلية في مورد شبكة منفصل
- عندما يكون من الضروري ربط GPO بوحدات محددة في Active Directory

تتوفر الخيارات التالية لاستخدام نظام تثبيت بديل من خلال Active Directory:

- إذا كان المطلوب إجراء التثبيت مباشرةً من مجلد Kaspersky Security Center المشترك، ففي خصائص GPO، يجب عليك تحديد ملف msi. الموجود في المجلد الفرعي exec داخل مجلد حزمة التثبيت الخاصة بالتطبيق المطلوب.
- إذا كان يجب وضع حزمة التثبيت في مورد شبكة آخر، يجب عليك نسخ محتوى مجلد exec بالكامل إلى ذلك المورد، لأنه بالإضافة إلى الملف ذي الامتداد msi.، يحتوي المجلد على ملفات التكوين التي تم إنشاؤها عند إنشاء الحزمة. لتثبيت مفتاح الترخيص مع التطبيق، انسخ ملف المفتاح إلى هذا المجلد أيضًا.

تثبيت التطبيقات عن بُعد على أجهزة macOS

لتثبيت التطبيقات على الأجهزة التي تعمل بنظام التشغيل macOS باستخدام مهمة تثبيت عن بُعد:

1. أنشئ أرشيفًا يتكون من حزمة تثبيت وبرنامج نصي لتثبيت sh.

2. قم بتعطيل الخيار **تحقق من نوع نظام التشغيل قبل التنزيل** في معالج المهمة الجديدة.

بدلاً من ذلك، يمكنك استخدام مهمة **Execute scripts remotely**. توضح المقالة التالية كيفية تكوين الملفات لهذه المهمة: تثبيت التطبيقات عن بُعد على الأجهزة باستخدام مهمة تنفيذ البرامج النصية عن بُعد.

تثبيت التطبيقات على خوادم الإدارة الثانوية

لتثبيت تطبيق على خوادم الإدارة الثانوية:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في خوادم الإدارة الثانوية ذات الصلة.

2. تأكد من توفر حزمة التثبيت التي تتطابق مع التطبيق الجاري تثبيته على كل خادم من خوادم الإدارة الثانوية المحددة. في حالة عدم وجود حزمة التثبيت من أي خادم من الخوادم التابعة، قم بتوزيعها باستخدام مهمة توزيع حزمة التثبيت.

3. قم بإنشاء مهمة تثبيت التطبيق على خوادم الإدارة الثانوية باستخدام أي من الطرق التالية:

- إذا كنت ترغب في إنشاء مهمة لخوادم الإدارة الثانوية في مجموعة الإدارة المحددة، قم بإنشاء مهمة جماعية لتثبيت هذه المجموعة عن بُعد.
- إذا كنت ترغب في إنشاء مهمة لخوادم إدارة ثانوية محددة، فقم بإنشاء مهمة لتثبيت أجهزة محددة عن بُعد.

يبدأ معالج إنشاء مهمة النشر لإرشادك خلال عملية إنشاء مهمة التثبيت عن بُعد. اتبع إرشادات المعالج.

في النافذة **تحديد نوع المهمة** في معالج المهمة الجديدة، في القسم **خادم إدارة Kaspersky Security Center** في المجلد **خيارات متقدمة** حدد **تثبيت تطبيق خوادم الإدارة الثانوية عن بُعد** كنوع المهمة.

سيقوم معالج مهمة جديدة بإنشاء مهمة تثبيت عن بُعد للتطبيق المحدد على خوادم إدارة ثانوية محددة.

4. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

عند إكمال مهمة التثبيت عن بُعد، سيتم تثبيت التطبيق المحدد على خوادم الإدارة الثانوية.

تثبيت التطبيقات باستخدام معالج التثبيت عن بُعد

لتثبيت تطبيقات Kaspersky، يمكنك استخدام معالج التثبيت عن بُعد. يسمح لك معالج التثبيت عن بُعد بتثبيت للتطبيقات عن بُعد من خلال حزم التثبيت التي تم إنشائها بشكل خاص أو من خلال حزمة التوزيع بشكل مباشر.

للتشغيل الصحيح لمهمة التثبيت عن بُعد على جهاز عميل غير مثبت عليه عميل شبكة، يجب فتح المنافذ التالية: TCP 139 و445؛ UDP 137 و138. بشكل افتراضي، تكون هذه المنافذ مفتوحة لجميع الأجهزة المضمنة في المجال. وفي حالة وجود أخطاء في الشبكة، ارجع إلى قاعدة معارف Kaspersky Security Center.

لتثبيت تطبيق على أجهزة محددة باستخدام معالج الإعداد عن بُعد:

1. في شجرة وحدة التحكم، قم بتحديد موقع المجلد **التثبيت عن بُعد**، وحدد المجلد الفرعي **حزم التثبيت**.

2. في مساحة عمل المجلد، حدد حزمة تثبيت التطبيق التي يتعين عليك تثبيتها.

3. في قائمة السياق الخاصة بحزمة التثبيت، حدد **تثبيت التطبيق**.

يبدأ معالج التثبيت عن بُعد.

4. في النافذة **تحديد أجهزة للتثبيت**، يمكنك إنشاء قائمة بالأجهزة التي سيتم تثبيت التطبيق عليها:

- **قم بالتثبيت على مجموعة من الأجهزة المُدارة**

إذا تم تحديد هذا الخيار، فسوف يتم إنشاء مهمة التثبيت عن بُعد لمجموعة أجهزة.

- **تحديد أجهزة للتثبيت**

إذا تم تحديد هذا الخيار، فسوف يتم إنشاء مهمة التثبيت عن بُعد لأجهزة معينة. يمكن أن تتضمن هذه الأجهزة المحددة كلاً من الأجهزة المُدارة والأجهزة غير المعينة.

5. في النافذة **تحديد إعدادات مهمة التثبيت عن بُعد**، حدد إعدادات تثبيت التطبيق عن بُعد.

في مجموعة الإعدادات **تنزيل حزمة التثبيت الإجباري**، حدد كيفية توزيع الملفات المطلوبة لتثبيت التطبيق على الأجهزة العميلة:

- **استخدام عميل الشبكة**

إذا كان هذا الخيار مفعلاً، سيتم تسليم حزم التثبيت إلى الأجهزة العميلة بواسطة عميل الشبكة المثبت على الأجهزة العميلة هذه.

في حالة تعطيل هذا الخيار، يتم تسليم حزم التثبيت باستخدام أدوات نظام التشغيل للأجهزة العميلة.

ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة.

يتم تمكين هذا الخيار افتراضيًا.

- **استخدام موارد نظام التشغيل من خلال خادم الإدارة**

إذا تم تمكين هذا الخيار، يتم نقل الملفات إلى أجهزة العميل باستخدام أدوات نظام التشغيل لأجهزة العميل من خلال خادم الإدارة. يمكنك تفعيل هذا الخيار إذا لم يتم تثبيت عميل شبكة على الجهاز العميل، لكن الجهاز العميل موجود في نفس الشبكة الموجود عليها خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **استخدام موارد نظام التشغيل عبر نقاط التوزيع**

إذا تم تفعيل هذا الخيار، سيتم نقل حزم التثبيت إلى الأجهزة العميلة باستخدام أدوات نظام التشغيل من خلال نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت توجد نقطة توزيع واحدة على الأقل في الشبكة.

في حالة تفعيل هذا الخيار **استخدام عميل الشبكة**، يتم تسليم الملفات بواسطة أدوات نظام التشغيل فقط في حالة عدم توفر موارد عميل الشبكة.

يتم تفعيل هذا الخيار افتراضيًا لمهام التثبيت عن بُعد التي تم إنشاؤها على خادم إدارة افتراضي.

عندما تكون جميع نقاط التوزيع المخصصة للجهاز معطلة، فلن يتمكن الجهاز من تلقي التحديثات (قواعد بيانات مكافحة الفيروسات والتصحيحات) وحزم التثبيت.

- **عدد محاولات التثبيت**

عند تشغيل مهمة التثبيت عن بُعد، إذا فشل Kaspersky Security Center في تثبيت تطبيق على جهاز مُدار ضمن عدد عمليات تشغيل المثبتات المحددة من خلال المعلمة، فسيتوقف Kaspersky Security Center عن توصيل حزمة التثبيت إلى هذا الجهاز المُدار ولن يبدأ تشغيل المثبت على الجهاز مرةً أخرى.

خيار عدد محاولات التثبيت يتيح لك حفظ الموارد الخاصة بالجهاز المُدار، بالإضافة إلى تقليل حركة نقل البيانات (إلغاء التثبيت وتشغيل ملف MSI ورسائل الأخطاء).

قد تشير محاولات بدء تشغيل المهمة بشكل متكرر إلى وجود مشكلة في الجهاز تمنع عملية التثبيت. ينبغي على المسؤول حل المشكلة ضمن عدد محاولات التثبيت المحدد (على سبيل المثال، من خلال تخصيص مساحة كافية على القرص، أو إزالة التطبيقات غير المتوافقة، أو تعديل إعدادات التطبيقات الأخرى التي تمنع عملية التثبيت) وإعادة تشغيل المهمة (يدويًا أو بموجب جدول زمني).

إذا لم تتحقق عملية التثبيت في النهاية، فستعتبر المشكلة غير قابلة للحل وأي عمليات بدء تشغيل مهمة بعد ذلك ستعتبر مكلفة فيما يخص استهلاك الموارد وحركة المرور بلا داعي.

عند إنشاء المهمة، يتم تعيين عداد المحاولات على `0`. تزيد كل عملية بدء تشغيل للمثبت ينتج عنها أخطاء في الجهاز من قراءة العداد.

إذا تم تجاوز عدد المحاولات المحددة في المعلمة وكان الجهاز مستعدًا لعملية تثبيت التطبيق، يمكنك زيادة قيمة عدد محاولات تثبيت المعلمة وبدء تشغيل المهمة لتثبيت التطبيق. وبدلًا من ذلك، يمكنك إنشاء مهمة تثبيت عن بُعد جديدة.

حدد ما العمل مع أجهزة العميل المُدارة من قبل خادم إدارة آخر:

- **التثبيت على كل الأجهزة**

سيتم تثبيت التطبيق حتى على الأجهزة التي تدار بواسطة خوادم إدارة أخرى.

ويتم تحديد هذا الخيار بصورة افتراضية. لا يتعين عليك تغيير هذا الإعداد إذا كان لديك خادم إدارة واحد فقط في شبكتك.

- **يتم التثبيت فقط على الأجهزة المُدارة من خلال خادم الإدارة هذا**

سيتم تثبيت التطبيق فقط على الأجهزة التي تدار بواسطة خادم الإدارة هذا. حدد هذا الخيار إذا كان لديك أكثر من خادم إدارة واحد في الشبكة الخاصة بك وكنت ترغب في تجنب التعارض بينها.

حدد الإعدادات الإضافية:

- **لا تقم بإعادة تثبيت التطبيق إذا كان مثبتًا بالفعل**

إذا تم تفعيل هذا الخيار، لن يتم عادة تثبيت التطبيق المحدد إذا كان مثبتًا بالفعل على الجهاز العميل هذا.

إذا تم تفعيل هذا الخيار، سيتم تثبيت التطبيق بأية حال.

يتم تمكين هذا الخيار افتراضيًا.

- **تعيين تثبيت الحزمة في سياسات مجموعة Active Directory**

في حال تمكين هذا الخيار، سيتم تثبيت حزمة التثبيت باستخدام سياسات مجموعة Active Directory.

يتوفر هذا الخيار فقط إذا تم تحديد حزمة تثبيت عميل الشبكة.

يتم تعطيل هذا الخيار افتراضيًا.

6. في النافذة **تحديد مفتاح ترخيص**، حدد مفتاح ترخيص وطريقة توزيعه:

- **لا تضع المفتاح في حزمة التثبيت (مستحسن)**

يتم توزيع المفتاح تلقائيًا على كافة الأجهزة التي يتوافق معها:

- في حالة تمكين التوزيع التلقائي في خصائص المفتاح
- إذا تم إنشاء مهمة **إضافة مفتاح**.

- **ضع مفتاح في حزمة التثبيت**

يتم توزيع المفتاح على الأجهزة بالإضافة إلى حزمة التثبيت.

> لا نوصي بقيامك بتوزيع المفتاح باستخدام هذه الطريقة؛ لأن حقوق الوصول للقراءة المشتركة ممكّنة لمستودع حزم التثبيت.

تظهر النافذة **تحديد مفتاح ترخيص** إذا لم تشتمل حزمة التثبيت على أي مفتاح ترخيص.

إذا كانت حزمة التثبيت تحتوي على مفتاح ترخيص، تظهر النافذة **خصائص المفتاح** التي تشمل تفاصيل مفتاح الترخيص.

7. في النافذة **تحديد خيار إعادة تشغيل نظام التشغيل**، حدد ما إذا كان يجب إعادة تشغيل الأجهزة إذا كان يجب إعادة تشغيل نظام التشغيل أثناء تثبيت التطبيقات عليها أم لا:

- **لا تقم بإعادة تشغيل الجهاز**

في حالة تحديد هذا الخيار، لن يتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

- **أعد تشغيل الجهاز**

في حالة تحديد هذا الخيار، فستتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

- **مطالبة المستخدم باتخاذ إجراء**

في حالة تحديد هذا الخيار بعد تثبيت أحد تطبيقات الأمان، سيتم عرض إخطار للمستخدم، لإخطاره بضرورة إعادة تشغيل الجهاز. عن طريق استخدام الرابط **تعديل** يمكنك تعديل الرسائل النصية وفترة عرض الرسالة ووقت إعادة التشغيل التلقائي.

يتم تحديد هذا الخيار افتراضيًا.

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

إذا تم تمكين هذا الخيار، فسيتم فرض إغلاق التطبيقات المثبتة على الأجهزة المحظورة قبل إعادة تشغيل الجهاز.

يتم تعطيل هذا الخيار افتراضيًا.

8. في نافذة **تحديد حسابات للوصول إلى الأجهزة**، يمكنك إضافة حسابات يتم استخدامها لبدء مهمة التثبيت عن بُعد:

- **لا يلزم وجود حساب (تم تثبيت عميل الشبكة)**

إذا تم تحديد هذا الخيار، فلا يلزم تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

إذا لم يتم تثبيت عميل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

- **يُلزم وجود حساب (عميل الشبكة غير مستخدم)**

حدد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على الأجهزة التي قمت بتعيين مهمة التثبيت عن بُعد لها. في هذه الحالة، يمكنك تحديد حساب مستخدم أو شهادة SSH لتثبيت التطبيق.

- **Local Account**. إذا تم تحديد هذا الخيار، فحدد الحساب المستخدم الذي سيتم من خلاله تشغيل مثبت التطبيق. انقر على الزر **إضافة**، وحدد **Local Account**، ثم حدد بيانات اعتماد حساب المستخدم.

يمكنك تحديد عدة حسابات مستخدمين، على سبيل المثال، إذا لم يكن لدى أي منهم جميع الحقوق المطلوبة على جميع الأجهزة التي قمت بتعيين المهمة لها. في هذه الحالة، يتم استخدام جميع الحسابات المضافة لتشغيل المهمة، بترتيب متتالٍ، من أعلى إلى أسفل.

- **شهادة SSH**. إذا كنت ترغب في تثبيت تطبيق على جهاز عميل يستند إلى Linux ، فيمكنك تحديد شهادة SSH بدلاً من حساب المستخدم. انقر على زر **إضافة**، وحدد **شهادة SSH**، ثم حدد المفاتيح الخاصة والعامة للشهادة.

لإنشاء مفتاح خاص، يمكنك استخدام الأداة المساعدة ssh-keygen. لاحظ أن Kaspersky Security Center يدعم تنسيق PEM للمفاتيح الخاصة، لكن الأداة المساعدة ssh-keygen تنشئ مفاتيح SSH بتنسيق OPENSSH افتراضيًا. تنسيق OPENSSH غير مدعوم من قبل Kaspersky Security Center. ولإنشاء مفتاح خاص بتنسيق PEM المدعوم، أضف الخيار -m PEM في الأمر ssh-keygen. فمثلاً:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<البريد الالكتروني للمستخدم>"
```

9. في النافذة **بدء التثبيت**، انقر على زر **التالي** لإنشاء مهمة تثبيت عن بُعد وبدء تشغيلها على الأجهزة المحددة.

إذا كانت نافذة **بدء التثبيت** بها خيار **لا تقم بتشغيل المهمة بُعد اكتمال معالج التثبيت عن بُعد** محددًا، لن تبدأ مهمة التثبيت عن بُعد. يمكنك بدء المهمة يدويًا لاحقًا. تتطابق اسم المهمة مع اسم حزمة التثبيت الخاصة بالتطبيق **تثبيت <اسم حزمة التثبيت>**.

لتثبيت التطبيق على أجهزة في مجموعة إدارة باستخدام معالج التثبيت عن بُعد:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في مجموعة الإدارة ذات الصلة.

2. حدد مجموعة إدارة في شجرة وحدة التحكم.

3. في مساحة عمل المجموعة، انقر على زر **تنفيذ الإجراء** وحدد **تثبيت التطبيق** في القائمة المنسدلة.

سيؤدي هذا إلى بدء تشغيل معالج التثبيت عن بُعد. اتبع إرشادات المعالج.

4. عند الخطوة النهائية من المعالج، انقر على **التالي** لإنشاء وتشغيل مهمة التثبيت عن بُعد على الأجهزة المحددة.

عند انتهاء معالج التثبيت عن بُعد، ينفذ Kaspersky Security Center الإجراءات التالية:

- إنشاء حزمة تثبيت لتثبيت التطبيق (إذا لم يتم الإنشاء مسبقًا). توجد حزمة التثبيت في المجلد **التثبيت عن بُعد** داخل المجلد الفرعي **حزم التثبيت** ولها اسم مطابق لاسم التطبيق وإصداره. يمكنك استخدام حزمة التثبيت هذه لتثبيت التطبيق في المستقبل.

- تقوم بإنشاء مهمة التثبيت عن بُعد وتشغيلها لأجهزة محددة أو لإحدى مجموعات الإدارة. يتم تخزين مهمة التثبيت عن بُعد التي تم إنشاؤها حديثًا في المجلد **المهام** أو يتم إضافتها إلى مهام مجموعة الإدارة التي تم إنشاؤها من أجلها. يمكنك بدء المهمة يدويًا لاحقًا. تتطابق اسم المهمة مع اسم حزمة التثبيت الخاصة بالتطبيق **تثبيت <اسم حزمة التثبيت>**.

العمل مع المكونات الإضافية للإدارة

تتم إدارة تطبيقات Kaspersky عبر وحدة تحكم الإدارة باستخدام المكونات الإضافية للإدارة. كل تطبيق من تطبيقات Kaspersky التي يمكن إدارتها من خلال Kaspersky Security Center يشمل مكون الإدارة الإضافي. وباستخدام مكون الإدارة الإضافي للتطبيق، يمكنك القيام بالإجراءات التالية في وحدة تحكم الإدارة:

- إنشاء وتحرير سياسات التطبيقات وإعداداتها، بالإضافة إلى إعدادات مهام التطبيقات.

- الحصول على معلومات عن مهام التطبيقات وأحداث التطبيقات وإحصاءات تشغيل التطبيق المُستلمة من الأجهزة العميلة.

للتحقق من قائمة المكونات الإضافية المثبتة وإصداراتها:

1. في شجرة وحدة تحكم الإدارة، انقر بزر الماوس الأيمن فوق **خادم الإدارة <اسم الخادم>**، وحدد **خصائص** .

2. انقر فوق **خيارات متقدمة** ← **تفاصيل المكونات الإضافية المثبتة لإدارة التطبيق**.

تظهر قائمة المكونات الإضافية للإدارة المثبتة وإصداراتها في الجزء الأيسر.

يمكنك تثبيت المكونات الإضافية للتطبيقات المدارة عند تشغيل معالج البدء السريع لخادم الإدارة أثناء الإعداد الأولي لحل Kaspersky Security Center. ويمكنك أيضًا تثبيت المكونات الإضافية للإدارة يدويًا.

لتثبيت مكون إضافي للإدارة يدويًا:

1. قم بتنزيل المكون الإضافي للإدارة لتطبيق Kaspersky والإصدار المطلوب (على سبيل المثال، Kaspersky Endpoint Security for Windows 12.6) من صفحة ويب الدعم الفني من Kaspersky.

2. إذا كانت وحدة تحكم الإدارة قيد التشغيل، فأغلقها.

3. قم بفك ضغط ملف المكون الإضافي الذي تم تنزيله وقم بتشغيل ملف klcfginst.msi أو klcfginst.exe. واتبع تعليمات معالج التثبيت.

4. عند اكتمال التثبيت، قم بتشغيل وحدة تحكم الإدارة وتأكد من عرض المكون الإضافي في قائمة المكونات الإضافية المثبتة، كما هو موضح في الإجراء السابق.

عند تشغيل وحدة تحكم الإدارة بعد تثبيت البرنامج الإضافي للإدارة الذي يدعم معالج البدء السريع للتطبيق المُدار، يتم تشغيل هذا المعالج تلقائيًا. ويمكنك الاطلاع على خطوات معالج البدء السريع للتطبيق المُدار لإنشاء سياسات ومهام تطبيق Kaspersky الافتراضية. يبدأ المعالج تلقائيًا فقط عند تشغيل وحدة تحكم الإدارة بعد التثبيت الأولي للمكون الإضافي أو بعد تحديث المكون الإضافي للإدارة إلى إصدار متوافق مع إصدار آخر من تطبيق Kaspersky الذي لم يتم إنشاء مهام وسياسات له بعد. ويمكنك أيضًا بدء معالج البدء السريع لإدارة التطبيقات يدويًا.

لبدء تشغيل معالج البدء السريع لإدارة التطبيقات يدويًا:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

2. في قائمة السياق الخاصة بعقدة خادم الإدارة، حدد **All Tasks** ← **معالج البدء السريع لإدارة التطبيقات**.

3. يبدأ معالج البدء السريع لإدارة التطبيقات. اتبع خطوات المعالج لإنشاء سياسات ومهام تطبيق Kaspersky الافتراضية.

لإزالة مكون إضافي للإدارة:

1. إذا كانت وحدة تحكم الإدارة قيد التشغيل، فأغلقها.

2. افتح Windows Registry Editor.

3. ابحث عن المفتاح التالي:

- `Plugins\28\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE` لنظام 32 بت.
- `Plugins\28\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE` لنظام 64 بت.

يحتوي المفتاح على المكونات الإضافية للإدارة المثبتة. ولكل مكون إضافي، تحتوي القيمة `DisplayName` على اسم المكون الإضافي، وتحتوي القيمة `UninstallString` على الأمر الخاص بإلغاء تثبيت المكون الإضافي.

4. ابحث عن مفتاح المكون الإضافي الذي تريد إلغاء تثبيته، وانسخ القيمة `UninstallString` الخاصة به إلى الحافظة.

5. ألصق القيمة في سلسلة الأوامر وقم بتشغيلها باستخدام حقوق مسؤول النظام.

يجب ألا يكون إصدار المكون الإضافي للإدارة أقدم من إصدار تطبيق Kaspersky المُدار. إذا قمت بتحديث تطبيق Kaspersky على الأجهزة، فيجب عليك تثبيت المكون الإضافي للإدارة من الإصدار نفسه.

عند فتح السياسة التي تم إنشاؤها في إصدار سابق من المكون الإضافي، سيُطلب منك قبول بيان Kaspersky Security Network.

عند إلغاء تثبيت Kaspersky Security Center Web Console، يتم أيضًا إلغاء تثبيت جميع المكونات الإضافية للإدارة.

إذا فتحت السياسة وحفظتها في إصدار المكون الإضافي الأحدث من إصدار التطبيق المُدار، فسيتم تحديث السياسة، ولن تتمكن من فتحها في المكون الإضافي للإصدار السابق.

عرض تقرير نشر الحماية

يمكنك استخدام تقرير نشر الحماية لمراقبة تقدم نشر الحماية على الشبكة.

لعرض تقرير توزيع الحماية:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .

3. في المجلد **التقارير**، حدد قالب التقرير المسمى **تقرير نشر الحماية**.

تعرض مساحة العمل تقريرًا يحتوي على معلومات حول نشر الحماية على جميع الأجهزة الموجودة على الشبكة.

يمكنك إنشاء تقرير نشر حماية جديد وتحديد نوع البيانات التي ينبغي أن يتضمنها:

- لمجموعة إدارة
- لأجهزة محددة
- لمجموعة محددة من الأجهزة
- لجميع الأجهزة

يفترض Kaspersky Security Center أن الحماية منشورة على الجهاز إذا كان تطبيق الأمان مثبتًا والحماية في الوقت الحقيقي ممكنة.

إزالة التطبيقات عن بُعد

يسمح لك Kaspersky Security Center بإلغاء تثبيت التطبيقات من الأجهزة عن بُعد، باستخدام مهام إلغاء التثبيت عن بُعد. ويتم إنشاء هذه المهام وتعيينها إلى الأجهزة من خلال المعالج المخصص. لتعيين مهمة للأجهزة بصورة أكثر سرعة وسهولة، يمكنك تحديد الأجهزة في نافذة المعالج بأي طريقة من الطرق التالية:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة** . في هذه الحالة، يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**. يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.
- **تعيين مهمة إلى تحديد الجهاز** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في المجموعة المحددة التي تم إنشائها في وقت سابق. يمكنك تحديد المجموعة المحددة مسبقًا أو المجموعة المخصصة التي أنشأتها.
- **تعيين مهمة لمجموعة إدارة** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة تم إنشائها في وقت سابق.

مشاكل الإزالة عن بعد

عند إجراء إزالة عن بعد لتطبيقات جهة خارجية، قد يواجه المسؤولون تحذيرًا يقول "انتهت إزالة التطبيق عن بعد على هذا الجهاز مع تحذيرات: التطبيق المطلوب إزالته غير مثبت". وتظهر هذه المشكلة عادةً عندما يتم تثبيت التطبيق الذي يجب إزالته فقط للمستخدم الفردي الذي سجل الدخول حاليًا بواسطة المُثبت. وإذا لم يسجل المستخدم الدخول، يصبح هذا التطبيق غير مرئي ولا يمكن استهدافه للإزالة عن بعد.

يختلف هذا السلوك مع التطبيقات المخصصة للاستخدام من قبل مستخدمين متعددين على الجهاز نفسه، حيث تكون التطبيقات مرئية ويمكن الوصول إليها عالميًا من قبل جميع مستخدمي الأجهزة.

في Kaspersky Security Center، تتعامل خوارزمية سجل التطبيقات مع التطبيقات للمستخدمين الفرديين والتطبيقات لمستخدمين متعددين بشكل مختلف:

- يتم الاحتفاظ بالتطبيقات لمستخدمين متعددين في قائمة محدثة في الوقت الحقيقي للتطبيقات المثبتة.
- يتم مراقبة التطبيقات للمستخدمين الفرديين باستخدام آلية تخزين مؤقت.

  إذا سجل المستخدم الدخول في وقت اكتشاف التطبيق، يخزن Kaspersky Security Center المعلومات عن تطبيقات هذا المستخدم. وحتى إذا سجل المستخدم الخروج لاحقًا، يستمر Kaspersky Security Center في عرض هذه التطبيقات على أنها مثبتة استنادًا إلى البيانات المخزنة مؤقتًا، على الرغم من أنها لم تعد مرئية أو يمكن الوصول إليها على الجهاز.

قد يؤدي هذا التناقض إلى مواقف حيث يحدد Kaspersky Security Center تطبيقًا مثبتًا استنادًا إلى البيانات المخزنة مؤقتًا، لكن تفشل مهمة إزالة التطبيق لأن التطبيق لا يمكن الوصول إليه عندما يسجل المستخدم الخروج.

بشكل افتراضي، يتم تعيين عمر بيانات التطبيق المخزنة مؤقتًا على 30 يومًا. ويمكن للمسؤولين تعديل هذا الإعداد لتقليل مدة ذاكرة التخزين المؤقت، وبالتالي تقليل التناقضات بين البيانات المعروضة ورؤية التطبيق الفعلي على الأجهزة.

لضبط عمر ذاكرة التخزين المؤقت إلى ساعة واحدة (3600 ثانية)، قم بتشغيل الأمر التالي على خادم الإدارة:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

بعد تشغيل هذا الأمر، أعد تشغيل خادم الإدارة لتصبح التغييرات سارية المفعول.

مصدر المعلومات عن التطبيقات المثبتة

يسترد عميل الشبكة المعلومات عن البرامج المثبتة على أجهزة Windows من مفاتيح التسجيل التالية:

- Uninstall\CurrentVersion\Windows\Microsoft\Software\HKEY_LOCAL_MACHINE
  يحتوي على معلومات عن التطبيقات المثبتة لجميع المستخدمين.
- Uninstall\CurrentVersion\Windows\Microsoft\Wow6432Node\Software\HKEY_LOCAL_MACHINE
  يحتوي على معلومات عن التطبيقات المثبتة لجميع المستخدمين.
- Uninstall\CurrentVersion\Windows\Microsoft\Software\HKEY_CURRENT_USER
  يحتوي على معلومات عن التطبيقات المثبتة للمستخدم الحالي.
- Uninstall\CurrentVersion\Windows\Microsoft\Software\<...>HKEY_USER
  يحتوي على معلومات عن التطبيقات المُثبتة لمستخدمين معينين.

الإزالة عن بُعد لتطبيق من الأجهزة العميلة الخاصة بمجموعة الإدارة

لإزالة التطبيق عن بُعد من الأجهزة العميلة الخاصة بمجموعة الإدارة:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في مجموعة الإدارة ذات الصلة.
2. حدد مجموعة إدارة في شجرة وحدة التحكم.
3. في مساحة عمل المجموعة، حدد علامة التبويب **المهام**.
4. قم بتشغيل إنشاء المهمة بالنقر فوق الزر **New task**.

   سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

   في نافذة **تحديد نوع المهمة** في معالج المهمة الجديدة، في القسم **خادم إدارة Kaspersky Security Center**، في المجلد **خيارات متقدمة** حدد **إلغاء تثبيت التطبيق عن بُعد** كنوع المهمة.

   يقوم المعالج مهمة جديدة بإنشاء مهمة جماعية خاصة بالإزالة عن بُعد للتطبيق المحدد. تظهر المهمة الجديدة في مساحة عمل مجموعة الإدارة على علامة التبويب **المهام**.
5. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

   بمجرد إكمال مهمة الإزالة عن بُعد، ستتم إزالة التطبيق المحدد من الأجهزة العميلة في مجموعة الإدارة.

الإزالة عن بُعد للتطبيق من الأجهزة المحددة

لإزالة التطبيق عن بُعد من الأجهزة المحددة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. تشغيل إنشاء المهمة بالنقر فوق **مهمة جديدة**.

   سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

في نافذة **تحديد نوع المهمة** في معالج المهمة الجديدة، في القسم **خادم إدارة Kaspersky Security Center**، في المجلد **خيارات متقدمة** حدد **إلغاء تثبيت التطبيق عن بُعد** كنوع المهمة.

يقوم المعالج مهمة جديدة بإنشاء مهمة تتعلق بالإزالة عن بُعد للتطبيق المحدد من الأجهزة المحددة. يتم عرض المهمة التي تم إنشاؤها حديثًا في مساحة عمل المجلد **المهام**.

3. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

بمجرد إكمال مهمة الإزالة عن بُعد، ستتم إزالة التطبيق المحدد من الأجهزة المحددة

العمل باستخدام حزم التثبيت

عند إنشاء مهام تثبيت عن بُعد، يستخدم النظام حزم التثبيت التي تحتوي على مجموعات من المعلمات الضرورية لتثبيت البرنامج.

يمكن أن تحتوي حزم التثبيت على ملف المفتاح. نوصيك بتجنب مشاركة الوصول إلى حزم التثبيت التي تحتوي على ملف المفتاح.

يمكنك استخدام حزمة التثبيت عدة مرات.

يتم نقل حزم التثبيت التي تم إنشاؤها بواسطة خادم الإدارة إلى شجرة وحدة التحكم حيث توجد في المجلد **التثبيت عن بُعد**، في المجلد الفرعي **حزم التثبيت**. يتم تخزين حزم التثبيت على خادم الإدارة، في المجلد الفرعي للخدمة المسمى الحزم، ضمن المجلد المشترك المحدد.

إذا لزم الأمر، يمكنك حذف حزمة تثبيت من المجلد الفرعي **حزم التثبيت** باتباع الإرشادات الواردة في المقالة بعنوان حذف كائن.

تجنب تغيير محتويات حزم التثبيت في مجلد مشترك يدويًا. وإذا لزم الأمر، يمكنك إنشاء نسخة من حزمة تثبيت، وإجراء التغييرات اللازمة، وإنشاء مهام تثبيت جديدة.

إنشاء حزمة توزيع

تصف هذه المقالة إجراء إنشاء أنواع حزم التثبيت التالية:

- إنشاء حزمة تثبيت لتطبيق Kaspersky.
- حزمة التثبيت لملف تنفيذي محدد
- حزمة التثبيت لتطبيق من قاعدة بيانات Kaspersky

لا يتعين عليك إنشاء حزمة تثبيت يدويًا للتثبيت عن بُعد لعميل الشبكة. ويتم إنشاؤها تلقائيًا أثناء تثبيت Kaspersky Security Center ويتم تخزينها في المجلد **حزم التثبيت**. في حالة حذف حزمة التثبيت عن بُعد لعميل الشبكة، يمكنك إعادة إنشائها عن طريق تحديد الملف nagent.kud في مجلد NetAgent الخاص بحزمة توزيع Kaspersky Security Center.

لإنشاء حزمة تثبيت:

1. قم بالاتصال بخادم الإدارة المطلوب.

2. في شجرة وحدة التحكم، حدد **خيارات متقدمة** ← **التثبيت عن بُعد** ← **حزم التثبيت**.

3. ابدأ إنشاء حزمة تثبيت جديدة بإحدى الطرق التالية:

- انقر بزر الماوس الأيمن فوق المجلد **حزم التثبيت**، ثم حدد **New** ← **حزمة التثبيت** من قائمة السياق.
- انقر بزر الماوس الأيمن في المنطقة الفارغة من قائمة حزم التثبيت، ثم حدد **إنشاء** ← **حزمة التثبيت** من قائمة السياق.
- انقر فوق **إنشاء حزمة التثبيت** في قسم إدارة قائمة حزم التثبيت.

يبدأ معالج الحزمة الجديدة.

4. حدد أحد أنواع حزم التثبيت التالية من خلال النقر فوق الأيقونة المقابلة:

- حزمة التثبيت لتطبيق Kaspersky.
- حزمة التثبيت لملف تنفيذي محدد.
- حزمة التثبيت لتطبيق من قاعدة بيانات Kaspersky.

5. حدد اسم حزمة التثبيت التي سيتم إنشاؤها.

يمكنك تحديد أي اسم.

6. حدد التطبيق أو الملف التنفيذي الذي سيتم إنشاء حزمة التثبيت له، بإحدى الطرق التالية:

- انقر فوق الزر **استعراض**، وفي النافذة **فتح** القياسية في نظام التشغيل Windows، حدد حزمة التوزيع للتطبيق المطلوب الموجود على الأقراص المتوفرة.

  ينطبق هذا الخيار إذا اخترت إنشاء حزمة تثبيت لتطبيق Kaspersky أو لملف تنفيذي محدد.

- انقر فوق الزر **استعراض**، وفي النافذة **تحديد التطبيق**، حدد حزمة التوزيع للتطبيق المطلوب.

  ينطبق هذا الخيار إذا اخترت إنشاء حزمة تثبيت لتطبيق من قاعدة بيانات Kaspersky.

إذا كنت تنشئ حزمة تثبيت لخادم الإدارة، فحدد الملف sc.kud. ويوجد الملف sc.kud في المجلد الجذر لحزمة توزيع Kaspersky Security Center.

لا تقم بتحديد أي من التفاصيل للحسابات المميزة في معلمات حزم التثبيت.

7. راجع اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية.

عند إنشاء حزمة تثبيت لأحد التطبيقات، قد يُطلب منك عرض وقبول اتفاقية ترخيص المستخدم النهائي وسياسة الخصوصية لهذا التطبيق.

اقرأ كلا المستندين. وإذا كنت توافق على جميع شروط اتفاقية الترخيص وسياسة الخصوصية، فاقبلها عن طريق تحديد خانات الاختيار المقابلة.

تستمر عملية تثبيت التطبيق على جهازك، ويتم استئناف عملية إنشاء حزمة التثبيت.

إذا كنت تنشئ حزمة تثبيت لبرنامج Kaspersky Endpoint Security for Mac، فيمكنك اختيار لغة اتفاقية الترخيص وسياسة الخصوصية.

8. إذا لزم الأمر، قم بتمكين التثبيت التلقائي لمكونات النظام.

إذا كنت تقوم بإنشاء حزمة تثبيت لتطبيق من قاعدة بيانات Kaspersky، فيمكنك تمكين التثبيت التلقائي لمكونات النظام الضرورية. يعرض معالج الحزمة الجديدة قائمة بجميع مكونات النظام المتاحة للتطبيق المحدد. ويمكنك الوصول إلى هذه القائمة في أي وقت في خصائص حزمة التثبيت.

إذا كنت تنشئ حزمة تثبيت التصحيح، فستتضمن القائمة جميع مكونات النظام اللازمة لنشر هذا التصحيح.

9. انقر فوق الزر **إنهاء** لإكمال عملية إنشاء الحزمة.

بمجرد أن يكتمل معالج الحزمة الجديدة، ستظهر حزمة التثبيت الجديدة في مساحة العمل الخاصة بمجلد **حزم التثبيت**، والموجود في شجرة وحدة التحكم.

إنشاء حزم تثبيت مستقلة

يمكنك أنت ومستخدمو الجهاز في مؤسستك استخدام حزم التثبيت المستقلة لتثبيت التطبيقات على الأجهزة يدويًا.

حزمة التثبيت المستقلة عبارة عن ملف تنفيذي (installer.exe) يمكن إيجاده على خادم الويب أو في المجلد المشترك أو نقله إلى جهاز عميل بطريقة أخرى. كما يمكنك إرسال رابط إلى حزمة التثبيت المستقلة عبر البريد الإلكتروني. على الجهاز العميل، يمكن للمستخدم تشغيل الملف المستلم محليًا لتثبيت تطبيق دون تدخل Kaspersky Security Center.

تأكد من أن حزمة التثبيت المستقلة غير متاحة لأشخاص غير مصرح بهم.

يمكنك إنشاء حزم التثبيت المستقلة لتطبيقات Kaspersky وتطبيقات الجهات الخارجية لمنصات أنظمة التشغيل Windows وmacOS وLinux. لإنشاء حزمة تثبيت مستقلة لتطبيق جهة ثالثة، يجب عليك إنشاء حزمة تثبيت مخصصة أولاً.

مصدر إنشاء حزم التثبيت المستقل هو حزم التثبيت في قائمة الإنشاء على خادم الإدارة.

لإنشاء حزمة تثبيت مستقلة:

1. في شجرة وحدة التحكم، حدد **خادم الإدارة** ← **خيارات متقدمة** ← **التثبيت عن بُعد** ← **حزم التثبيت**.

   يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. في قائمة حزم التثبيت، حدد حزمة تثبيت التي تريد إنشاء حزمة مستقلة لها.

3. في قائمة السياق، حدد **إنشاء حزمة تثبيت مستقلة**.

   يبدأ معالج إنشاء حزمة التثبيت المستقلة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

4. في الصفحة الأولى من المعالج، إذا كنت قد حدد حزمة تثبيت لتطبيق Kaspersky وترغب في تثبيت عميل الشبكة مع التطبيق المحدد، تأكد أن خيار **تثبيت عميل الشبكة بالإضافة إلى هذا التطبيق** مفعل.

   يتم تمكين هذا الخيار افتراضيًا. ننصح بتمكين هذا الخيار إذا لم تكن متأكدًا من تثبيت عميل الشبكة على الجهاز من عدمه. إذا كان عميل الشبكة مثبتًا بالفعل على الجهاز، بعد تثبيت حزمة التثبيت المستقلة مع عميل الشبكة، سيتم تحديث عميل الشبكة إلى الإصدار الأحدث.

   إذا قمت بتعطيل هذا الخيار، فلن يتم تثبيت عميل الشبكة على الجهاز ولن تتم إدارة الجهاز.

   إذا كانت حزمة التثبيت المستقلة للتطبيق المحدد موجودة بالفعل على خادم الإدارة، يحيطك المعالج علمًا بهذه الحقيقة. في هذه الحالة، يجب عليك تحديد أحد الإجراءات التالية:

   - **إنشاء حزمة تثبيت مستقلة**. حدد هذا الخيار إذا كنت على سبيل المثال تريد إنشاء حزمة تثبيت مستقلة لإصدار تطبيق جديد وتريد أيضًا الاحتفاظ بحزمة تثبيت مستقلة قمت بإنشائها لإصدار تطبيق سابق. يتم وضع حزمة التثبيت المستقلة الجديدة في مجلد آخر.
   - **استخدام حزمة تثبيت مستقلة موجودة**. حدد هذا الخيار إذا أردت استخدام حزمة تثبيت مستقلة. لن يتم بدء عملية إنشاء الحزمة.
   - **إعادة بناء حزمة تثبيت مستقلة موجودة**. حدد هذا الخيار إذا أردت إنشاء حزمة تثبيت مستقلة للتطبيق نفسه مرة أخرى. يتم وضع حزمة التثبيت المستقلة في المجلد نفسه.

5. في الصفحة التالية من المعالج، حدد خيار **نقل الأجهزة غير المخصصة إلى هذه المجموعة** وحدد مجموعة إدارة تريد نقل الجهاز العميل إليها بعد تثبيت عميل الشبكة.

   بشكل افتراضي، يتم نقل الجهاز إلى مجموعة **الأجهزة المُدارة**.

   إذا كنت لا تريد نقل الجهاز العميل إلى مجموعة إدارة بعد تثبيت عميل الشبكة، حدد خيار **عدم نقل الأجهزة**.

6. في الصفحة التالية من المعالج، عند الانتهاء من عملية إنشاء حزمة التثبيت المستقلة، يتم عرض نتيجة إنشاء الحزمة المستقلة ومسار الحزمة المستقلة.

يمكنك النقر على الروابط والقيام بأي مما يلي:

- افتح المجلد مع حزمة التثبيت المستقلة.
- رابط البريد الإلكتروني إلى حزمة التثبيت المستقلة التي تم إنشاؤها. لتنفيذ هذا الإجراء، يجب أن يكون لديك تطبيق بريد إلكتروني قيد البدء.
- نموذج رمز HTML لنشر الرابط على موقع ويب. يتم إنشاء ملف نصي (TXT) وفتحه في تطبيق مرتبط بتنسيق TXT. في الملف، يتم عرض علامة HTML <a> مع السمات.

7. في الصفحة التالية من المعالج، إذا أردت فتح قائمة حزم التثبيت المستقلة، قم بتمكين خيار **فتح قائمة بالحزم المستقلة**.

8. انقر على زر **إنهاء**.

معالج إنشاء حزمة تثبيت مستقلة يغلق.

يتم إنشاء حزمة التثبيت المستقلة ووضعها في المجلد الفرعي PkgInst الخاص بـمجلد خادم الإدارة المشترك. يمكنك عرض قائمة الحزم المستقلة من خلال النقر على زر **عرض قائمة الحزم المستقلة** أعلى قائمة حزم التثبيت.

إنشاء حزمة توزيع مخصصة

يمكنك استخدام حزم التثبيت المخصصة للقيام بما يلي:

- لتثبيت أي تطبيق (مثل محرر نص) على جهاز عميل، على سبيل المثال، عبر مهمة.
- من أجل إنشاء حزمة تثبيت مستقلة.

حزمة التثبيت المخصصة عبارة عن مجلد به مجموعة من الملفات. المصدر لإنشاء حزمة تثبيت مخصصة هو ملف أرشيف. يحتوي ملف الأرشيف على ملف أو ملفات يجب تضمينها في حزمة التثبيت المخصصة. عند إنشاء حزمة تثبيت مخصصة، يمكنك تحديد معلمات سطر الأوامر، على سبيل المثال، لتثبيت التطبيق في وضع صامت.

لإنشاء حزمة تثبيت مخصصة:

1. في شجرة وحدة التحكم، حدد **خادم الإدارة** ← **متقدم** ← **التثبيت عن بُعد** ← **حزم التثبيت**.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. أعلى قائمة التثبيت، انقر على زر **إنشاء حزمة التثبيت**.

يبدأ معالج الحزمة الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. في صفحة المعالج، حدد **إنشاء حزمة تثبيت للملف التنفيذي المحدد**.

4. في الصفحة التالية من المعالج، حدد اسم حزمة التثبيت المخصصة.

5. في الصفحة التالية من المعالج، انقر على الزر **استعراض**، وفي النافذة **فتح** القياسية في نظام التشغيل Windows، اختر ملف أرشيف موجود على الأقراص المتوفرة لإنشاء حزمة تثبيت مخصصة.

يمكنك تحميل أرشيف ZIP أو CAB أو TAR أو TAR.GZ. لا يمكن إنشاء حزمة تثبيت من ملف SFX (أرشيف ذاتي الاستخراج).

يتم تنزيل الملفات إلى خادم إدارة Kaspersky Security Center.

6. في الصفحة التالية من المعالج، حدد معلمات سطر الأوامر لملف قابل للتنفيذ.

يمكنك تحديد معلمات سطر الأوامر لتثبيت التطبيق من حزمة التثبيت في وضع صامت. تحديد معلمات سطر الأوامر أمر اختياري.

إذا أردت ذلك، قم بتكوين الخيارات التالية:

- **نسخ المجلد بالكامل إلى حزمة التثبيت**

حدد هذا الخيار إذا كان الملف التنفيذي مصحوبًا بملفات إضافية مطلوبة لتثبيت التطبيق. قبل تمكين هذا الخيار، يُرجى التأكد من أن كل الملفات المطلوبة مخزّنة في المجلد نفسه. وفي حالة تمكين هذا الخيار، يُضيف التطبيق محتويات المجلد بالكامل، بما في ذلك الملف التنفيذي المحدد إلى حزمة التثبيت.

- **تحويل الإعدادات إلى القيم الموصى بها للتطبيقات التي تم التعرف عليها من قبل Kaspersky Security Center**

سيتم تثبيت التطبيق من خلال الإعدادات الموصى بها، إذا كانت المعلومات عن التطبيق المحدد مشتملة على قاعدة بيانات Kaspersky.

إذا أدخلتَ المعلمات في الحقل **سطر أوامر الملف التنفيذي**، تتم إعادة كتابتها باستخدام الإعدادات الموصى بها.

يتم تمكين هذا الخيار افتراضيًا.

قام محللو Kaspersky بإنشاء قاعدة بيانات Kaspersky وصيانتها. يحدد محللو Kaspersky إعدادات التثبيت المثلى لكل تطبيق تتم إضافته إلى قاعدة البيانات. يتم تحديد الإعدادات لضمان نجاح عملية التثبيت عن بُعد لتطبيق على الجهاز العميل. يتم تحديث قاعدة البيانات على خادم الإدارة تلقائيًا عند تنفيذ تنزيل التحديثات إلى مستودع مهمة خادم الإدارة.

تبدأ عملية إنشاء حزمة التثبيت المخصصة.

يحيطك المعالج علمًا عند الانتهاء من العملية.

إذا لم يتم إنشاء حزمة التثبيت المخصصة، يتم عرض رسالة مطلوبة.

7. انقر على زر **إنهاء** لإغلاق المعالج.

يتم تنزيل حزمة التثبيت التي قمت بإنشائها إلى مجلد الحزم الفرعي الخاص بـمجلد خادم الإدارة المشترك. بعد التنزيل، تظهر حزمة التثبيت المخصصة في قائمة حزم التثبيت.

في قائمة حزم التثبيت على خادم الإدارة، يمكنك عرض وتحرير خصائص حزمة التثبيت المخصصة.

عرض خصائص حزم التثبيت المخصصة وتحريرها

بعد قيامك بإنشاء حزمة تثبيت مخصصة، يمكنك عرض معلومات عامة حول حزمة التثبيت وتحديد إعدادات التثبيت في نافذة الخصائص.

لعرض وتحرير خصائص حزمة تثبيت مخصصة:

1. في شجرة وحدة التحكم، حدد **خادم الإدارة** ← **متقدم** ← **التثبيت عن بُعد** ← **حزم التثبيت**.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. في قائمة السياق الخاصة بحزمة تثبيت، حدد **خصائص**.

يتم فتح نافذة الخصائص الخاصة بحزمة التثبيت المحددة.

3. عرض المعلومات التالية:

- اسم حزمة التثبيت
- اسم التطبيق في حزمة التثبيت المخصصة
- إصدار التطبيق
- تاريخ إنشاء حزمة التثبيت
- المسار إلى حزمة التثبيت المخصصة على خادم الإدارة
- سطر أوامر الملف التنفيذي

4. حدد الإعدادات التالية:

- اسم حزمة التثبيت
- **تثبيت مكونات النظام العام المطلوبة**

إذا تم تمكين هذا الخيار، قبل تثبيت التحديث، يقوم التطبيق تلقائيًا بتثبيت كافة مكونات النظام العامة (المتطلبات الأساسية) اللازمة لتثبيت التحديث. على سبيل المثال، يمكن أن تكون تلك المتطلبات الأساسية عبارة عن تحديثات نظام التشغيل.

إذا تم تعطيل هذا الخيار، فقط يتعين عليك تثبيت المتطلبات الأساسية يدويًا.

يتم تعطيل هذا الخيار افتراضيًا.

لا يتوفر هذا الخيار إلا عندما يتعرف Kaspersky Security Center على التطبيق المُضاف إلى حزمة التثبيت.

- **سطر أوامر الملف التنفيذي**

إذا كان التطبيق يتطلب معلمات إضافية للتثبيت الصامت، فيرجى تحديدها في هذا الحقل. راجع وثائق البائع للاطلاع على التفاصيل.

يمكنك أيضًا إدخال معلمات أخرى.

هذا الخيار متاح فقط للحزم التي لم يتم إنشاؤها على أساس تطبيقات Kaspersky.

5. انقر على زر **موافق** أو زر **تطبيق** لحفظ التغييرات، إن وجدت.

يتم حفظ الإعدادات الجديدة.

الحصول على حزمة تثبيت عميل الشبكة من مجموعة توزيع Kaspersky Security Center

يمكنك الحصول على حزمة تثبيت عميل الشبكة من مجموعة توزيع Kaspersky Security Center، دون الحاجة إلى تثبيت Kaspersky Security Center. ثم يمكنك استخدام حزمة التثبيت لتثبيت عميل الشبكة على أجهزة العميل.

للحصول على حزمة تثبيت عميل الشبكة من مجموعة توزيع Kaspersky Security Center:

1. قم بتشغيل ksc_<version number>. <build number>_ممتلىء_<localization language> ملف. exe قابل للتنفيذ من ملف مجموعة توزيع Kaspersky Security Center.

2. في النافذة التي تفتح ، انقر على الرابط **استخراج حزم التثبيت**.

3. في قائمة حزم التثبيت، حدد مربع الاختيار بجوار حزمة تثبيت عميل الشبكة، ثم انقر فوق الزر **التالي**.

4. إذا لزم الأمر، انقر فوق **استعراض** لتغيير المجلد المعروض لاستخراج حزمة التثبيت إليه.

5. انقر فوق زر **استخراج**.

يستخرج التطبيق حزمة تثبيت عميل الشبكة.

6. عند اكتمال العملية ، انقر فوق الزر **إغلاق**.

يتم استخراج حزمة تثبيت عميل الشبكة إلى المجلد المحدد.

يمكنك استخدام حزمة التثبيت لتثبيت عميل الشبكة بإحدى الطرق التالية:

- محليا عن طريق تشغيل ملف setup.exe من المجلد المستخرج
- من خلال التثبيت الصامت
- النشر باستخدام سياسات المجموعة الخاصة بـ Microsoft Windows

توزيع حزم التثبيت على خوادم الإدارة الثانوية

لتوزيع حزم التثبيت على خوادم الإدارة الثانوية:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في خوادم الإدارة الثانوية ذات الصلة.
2. إنشاء مهمة توزيع حزمة تثبيت إلى خوادم الإدارة الثانوية باستخدام أحد الطرق التالية:
   - إذا كنت ترغب في إنشاء مهمة لخوادم الإدارة الثانوية في مجموعة الإدارة المحددة، قم ببدء تشغيل مهمة جماعية لهذه المجموعة.
   - إذا كنت ترغب في إنشاء مهمة لخوادم إدارة ثانوية محددة، فقم ببدء تشغيل إنشاء مهمة للأجهزة المحددة.

   سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

   في نافذة **تحديد نوع المهمة** في معالج المهمة الجديدة، في القسم **خادم إدارة Kaspersky Security Center**، في المجلد **خيارات متقدمة** حدد **توزيع تثبيت الحزمة** كنوع المهمة.

   سيقوم معالج مهمة جديدة بإنشاء مهمة توزيع حزم التثبيت المحددة على خوادم إدارة ثانوية محددة.
3. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

   سيتم نسخ حزم التثبيت المحددة إلى خوادم الإدارة الثانوية المحددة.

توزيع حزم التثبيت بواسطة نقاط التوزيع

يمكنك استخدام نقاط التوزيع لتوزيع حزم التثبيت ضمن مجموعة إدارة.

بعد أن يتم استلام حزم التثبيت من خادم الإدارة، تقوم نقاط التوزيع تلقائيًا بتوزيعها على الأجهزة العميلة باستخدام البث المتعدد لـ IP. تحدث عملية الإرسال المتعدد لعنوان IP لحزم التثبيت الجديدة ضمن مجموعة إدارة لمرة واحدة. في حالة قطع اتصال جهاز عميل من شبكة الشركة أثناء عملية التوزيع، سيقوم عميل الشبكة (على الجهاز العميل) بالتنزيل التلقائي لحزمة التثبيت المطلوبة من نقطة التوزيع عندما تبدأ مهمة التثبيت.

نقل نتائج تثبيت التطبيق إلى Kaspersky Security Center

بعد إنشاء حزمة تثبيت التطبيق، يمكنك تكوينها ومن ثم يمكن نقل جميع معلومات التشخيص حول نتائج تثبيت التطبيق إلى Kaspersky Security Center. بالنسبة لحزم تثبيت تطبيقات Kaspersky، يتم تكوين عملية نقل معلومات التشخيص حول نتائج تثبيت التطبيق بشكل افتراضي، ولا يلزم إجراء تكوين إضافي.

لتكوين نقل معلومات التشخيص الخاصة بنتائج تثبيت التطبيق إلى Kaspersky Security Center:

1. انتقل إلى مجلد حزمة التثبيت الذي تم إنشاؤه باستخدام Kaspersky Security Center للتطبيق المحدد. يمكن العثور على الملف في المجلد المشترك المحدد أثناء تثبيت Kaspersky Security Center.

2. افتح الملف الذي له الامتداد .kpd أو .kud للتحرير (على سبيل المثال، في محرر مفكرة Microsoft Windows).

   يمتلك الملف التنسيق العادي لملف التكوين .ini.

3. قم بإضافة الأسطر التالية إلى الملف:

```
[SetupProcessResult]
1=Wait
```

   يقوم هذا الأمر بتكوين Kaspersky Security Center حتى ينتظر إكمال إعداد التطبيق الذي تم إعداد حزمة التثبيت من أجله ولتحليل رمز إرجاع برنامج المثبت إذا كان عليك تعطيل نقل بيانات التشخيص، فقم بتعيين قيمة مفتاح الانتظار إلى 0.

4. أضف وصفًا إلى رموز الإرجاع الخاصة بالتثبيت الناجح. لتنفيذ هذا الأمر، أضف الأسطر التالية إلى الملف:

```
[SetupProcessResult_SuccessCodes]
[<description>]=<return code>
[<description>]=<return code 1>
...
```

> تحتوي الأقواس المربعة على مفاتيح اختيارية.

   بناء الجملة الخاص بهذه الأسطر:

   - `<return code>`. أي رقم مقابل لرمز إرجاع المثبت. يمكن تغيير عدد رموز الإرجاع.
   - `<description>`. الوصف النصي لنتائج التثبيت. يمكن حذف الوصف.

5. إضافة وصف لرموز الإرجاع لعمليات التثبيت الفاشلة. لتنفيذ هذا الأمر، أضف الأسطر التالية إلى الملف:

```
[SetupProcessResult_ErrorCodes]
[<description>]=<return code>
[<description>]=<return code 1>
...
```

   يتطابق بناء جملة هذه الأسطر مع بناء الجملة الخاص برموز إرجاع الإعداد الناجح.

6. قم بإغلاق ملف .kpd أو .kud عن طريق حفظ جميع التغييرات.

سيتم تسجيل المعلومات الخاصة بنتائج تثبيت التطبيق المعرف بواسطة المستخدم في سجلات Kaspersky Security Center، وستظهر في قائمة الأحداث في التقارير وسجلات المهام.

تحديد عنوان خادم وكيل KSN لحزم التثبيت

في حال تغيير العنوان أو مجال خادم الإدارة، يمكنك تحديد عنوان خادم وكيل KSN لحزمة التثبيت.

لتحديد عنوان خادم وكيل KSN لحزمة التثبيت:

1. في شجرة وحدة التحكم، في مجلد **التثبيت عن بُعد**، انقر نقرًا مزدوجًا فوق الملف الفرعي **حزم التثبيت**.

2. في القائمة التي تفتح، حدد **الخصائص**.

3. في نافذة الخصائص التي تفتح، حدد القسم الفرعي **عام**.

4. في القسم الفرعي **عام** من نافذة الخصائص، أدخل عنوان خادم وكيل KSN.

ستستخدم حزم التثبيت هذا العنوان كعنوان افتراضي.

تلقي إصدارات التطبيقات المُحدَّثة

يسمح لك Kaspersky Security Center بتلقي إصدارات تطبيقات الشركة المُحدَّثة التي يتم تخزينها على خوادم Kaspersky.

لتلقي الإصدارات المُحدَّثة من تطبيقات شركة Kaspersky:

1. قم بأحد الإجراءات التالية:

- في شجرة وحدة التحكم، حدد الجزء الذي يحمل اسم خادم الإدارة المطلوب، وتأكد من تحديد علامة التبويب **المراقبة**، وفي قسم **النشر**، انقر على رابط **توجد إصدارات جديدة من تطبيقات Kaspersky متاحة**.

> يصبح رابط **توجد إصدارات جديدة من تطبيقات Kaspersky متاحة** متاحًا عندما يعثر خادم الإدارة على إصدار جديد لأحد تطبيقات الشركة على خادم Kaspersky.

- في شجرة وحدة التحكم، حدد **خيارات متقدمة** ← **التثبيت عن بُعد** ← **حزم التثبيت**، وفي مساحة العمل انقر فوق **إجراءات إضافية** ومن القائمة المنسدلة حدد **عرض الإصدار الحالي لتطبيقات Kaspersky**.

يتم عرض قائمة الإصدار الحالي من تطبيقات Kaspersky.

2. يمكنك تصفية قائمة تطبيقات Kaspersky لتبسيط البحث عن التطبيق المطلوب.

في الجزء العلوي من نافذة **إصدارات التطبيق الحالية**، انقر على رابط **عامل التصفية** لتصفية قائمة الطلبات حسب المعايير التالية:

- **المكونات**. استخدم هذا المعيار لتصفية قائمة تطبيقات Kaspersky حسب مناطق الحماية المستخدمة على شبكتك.
- **نوع البرنامج الذي تم تنزيله**. استخدم هذا المعيار لتصفية قائمة تطبيقات Kaspersky حسب نوع التطبيق.
- **منتجات البرامج والتحديثات التي سيتم عرضها**. استخدم هذا المعيار لعرض تطبيقات Kaspersky المتاحة بإصدارات محددة.
- **اللغات المعروضة للبرامج والتحديثات**. استخدم هذا المعيار لعرض تطبيقات Kaspersky بلغة ترجمة محددة.

انقر على زر **تطبيق** لتطبيق عوامل التصفية المحددة.

3. حدد التطبيق المطلوب من القائمة.

4. تنزيل حزمة توزيع التطبيق عن طريق النقر فوق الرابط الموجود في السلسلة **عنوان الويب لحزمة التوزيع**.

تحديثات التطبيقات المُدارة قد يتطلب تثبيت إصدار أدنى محدد من Kaspersky Security Center. إذا كان هذا الإصدار أحدث من إصدارك الحالي، يتم عرض هذه التحديثات لكن لا يمكن الموافقة عليها. أيضًا لا يمكن إنشاء حزم تثبيت من هذه التحديثات حتى تقوم بترقية Kaspersky Security Center. سيُطلب منك ترقية مثيلك من Kaspersky Security Center إلى الإصدار الأدنى المطلوب.

في حالة عرض زر **تنزيل التطبيقات وإنشاء حزم تثبيت** للتطبيق المحدد، يمكنك النقر فوق هذا الزر لتنزيل حزمة توزيع التطبيق وإنشاء حزمة تثبيت تلقائيًا. يقوم Kaspersky Security Center بتنزيل حزمة توزيع التطبيق لخادم الإدارة إلى المجلد المشترك المحدد أثناء تثبيت Kaspersky Security Center. يتم عرض حزمة التثبيت التي تم إنشاؤها تلقائيًا في المجلد **التثبيت عن بُعد** في شجرة وحدة التحكم، في المجلد الفرعي **حزم التثبيت**.

بعد إغلاق نافذة **إصدارات التطبيق الحالية**، يختفي رابط **توجد إصدارات جديدة من تطبيقات Kaspersky متاحة** من القسم **النشر** .

يمكنك إنشاء حزم تثبيت للإصدارات الجديدة من التطبيقات وإدارة حزم التثبيت التي تم إنشاؤها حديثًا في المجلد **التثبيت عن بُعد** في شجرة وحدة التحكم، في المجلد الفرعي **حزم التثبيت**.

يمكنك أيضًا فتح نافذة **إصدارات التطبيق الحالية** بالنقر على رابط **عرض الإصدار الحالي لتطبيقات Kaspersky** في مساحة عمل المجلد **حزم التثبيت**.

تحضير جهاز يعمل بنظام Windows للتثبيت عن بُعد

تثبيت التطبيق عن بعُد على الجهاز العميل قد يرجع خطأ للأسباب التالية:

- تم تنفيذ هذه المهمة بالفعل بنجاح على هذا الجهاز.

  في هذه الحالة، لا توجد حاجة لتنفيذ المهمة مرة أخرى.

- عند بدء المهمة، يتم إيقاف تشغيل الجهاز.

  في هذه الحالة، قم بتشغيل الجهاز وأعد تشغيل المهمة.

- لا يوجد اتصال بين خادم الإدارة وعميل الشبكة المثبت على الجهاز العميل.

  لتحديد سبب المشكلة، استخدم الأداة المساعدة المصممة لتشخيص الأجهزة العميلة عن بعُد (klactgui).

- إذا لم يتم تثبيت عميل الشبكة على الجهاز، قد تحدث المشاكل التالية أثناء التثبيت عن بُعد:
  - تم تمكين **تعطيل مشاركة الملفات البسيطة** في الجهاز العميل.
  - لا تعمل خدمة الخادم على الجهاز العميل.
  - غلق المنافذ المطلوبة على الجهاز العميل.
  - الحساب المستخدم لتنفيذ المهمة لا يمتلك الامتيازات الكافية.

لتجنب المشكلات التي قد تحدث أثناء تثبيت التطبيق على جهاز عميل بدون تثبيت عميل الشبكة، يجب عليك المتابعة كما هو موضح في النشر الإجباري عبر مهمة تثبيت عن بُعد من Kaspersky Security Center.

في السابق، تم استخدام الأداة المساعدة riprep لإعداد جهاز للتثبيت عن بعد. ويُعتبر هذا الآن طريقة قديمة لتكوين أنظمة التشغيل. ولا يُنصح باستخدام أداة riprep على أنظمة التشغيل الأحدث من Windows XP وWindows Server 2003 R2.

تحضير جهاز Linux وتثبيت عميل الشبكة على جهاز Linux عن بُعد

يتكون تثبيت عميل الشبكة من خطوتين:

- تحضير جهاز Linux
- تثبيت عميل الشبكة عن بُعد

تحضير جهاز Linux

لإعداد جهاز يعمل بنظام Linux لتثبيت عميل الشبكة عن بُعد:

1. تأكد أن الجهاز الذي ترغب في تثبيت عميل الشبكة عليه يعمل بإحدى توزيعات Linux المدعومة.
2. قم بتنزيل حزمة تثبيت عميل الشبكة باستخدام واجهة التطبيق أو من موقع ويب Kaspersky.
3. تأكد من تثبيت البرنامج التالي على جهاز Linux الهدف:
   - Sudo (لنظام التشغيل Ubuntu 10.04، إصدار Sudo هو 1.7.2p1 أو أحدث)
   - إصدار مترجم لغة Perl الإصدار 5.10 أو أحدث
   - أداة حالة العملية
4. قم باختبار تكوين الجهاز:
   a. تحقق مما إذا كان يمكنك الاتصال بالجهاز عبر عميل SSH (مثل PuTTY).
   إذا لم تتمكن من توصيل الجهاز، فافتح الملف `etc/ssh/sshd_config/` وتأكد من وجود القيم المدرجة أدناه للإعدادات التالية:
   ```
   PasswordAuthentication no
   ChallengeResponseAuthentication yes
   ```

> لا تقم بتعديل ملف /etc/ssh/sshd_config إذا كان بإمكانك الاتصال بالجهاز دون مشاكل؛ وخلافًا لذلك، قد تواجه فشل مصادقة SSH عند تشغيل مهمة التثبيت عن بُعد.

   احفظ الملف (إذا لزم الأمر) ثم أعد تشغيل خدمة SSH باستخدام الأمر `sudo service ssh restart`.

   b. تأكد من أن منفذ TCP 22 مفتوح وتتوفر إمكانية الوصول إليه على جهاز Linux من الأجهزة غير المخصصة. ويجب أن يتوفر منفذ TCP 22 للتثبيت الناجح لعميل الشبكة لنظام التشغيل Linux.

   c. قم بتعطيل كلمة مرور sudo الخاصة بحساب المستخدم الذي سيتم توصيل الجهاز بموجبه.

   d. استخدم الأمر `visudo` في برنامج sudo لفتح ملف تكوين sudoers.
   في الملف الذي فتحته، أضف السطر التالي إلى نهاية الملف: `ALL :NOPASSWD (ALL) = ALL <username>`. في هذه الحالة، يكون `<username>` عبارة عن حساب المستخدم الذي يجب استخدامه لاتصال الجهاز باستخدام SSH. إذا كنت تستخدم نظام التشغيل Astra Linux، في ملف /etc/sudoers، أضف السطر الأخير مع النص التالي: `ALL :NOPASSWD (ALL:ALL)=astra-admin ALL%`

e. احفظ ملف sudoers ثم أغلقه.

f. اتصل بالجهاز مجددًا عبر SSH وتأكد من عدم مطالبة خدمة Sudo بإدخال كلمة المرور؛ ويمكنك القيام بذلك باستخدام الأمر `sudo whoami`.

5. افتح الملف `/etc/systemd/logind.conf`، ثم قم بأحد الإجراءات التالية:

- حدد "لا" كقيمة لإعداد KillUserProcesses: `KillUserProcesses=no`.
- بالنسبة لإعداد KillExcludeUsers، اكتب اسم مستخدم الحساب الذي سيتم تنفيذ التثبيت عن بُعد فيه، على سبيل المثال، `KillExcludeUsers=root`.

إذا كان الجهاز المستهدف يعمل بنظام Astra Linux، أضف السلسلة `PATH=/usr/local/bin/:/usr/local/sbin/:/usr/bin/:/usr/sbin/:bin/:sbin` في `/home/<username>/.bashrc`، حيث `<username>` هو حساب المستخدم الذي سيتم استخدامه لتوصيل الجهاز باستخدام SSH.

لتطبيق الإعداد الذي تم تغييره، أعد تشغيل جهاز Linux أو نفّذ الأمر التالي:

```
sudo systemctl restart systemd-logind.service
```

6. إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تعمل بنظام التشغيل SUSE Linux Enterprise Server 15، فثبت أول حزمة insserv-Compatible لتكوين عميل الشبكة.

7. إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تعمل بنظام التشغيل Astra Linux التي تعمل في وضع بيئة البرنامج المغلق، نفذ الخطوات الإضافية لإعداد أجهزة Astra Linux.

8. إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تستخدم نظام التشغيل RED OS 7.3.4 أو أحدث أو MSVSPHERE 9.2 أو أحدث، فقم بتثبيت حزمة libxcrypt-compat لكي يعمل عميل الشبكة بشكل صحيح.

تثبيت عميل الشبكة عن بُعد

لتثبيت عميل الشبكة على أجهزة Linux عن بُعد:

1. تنزيل وإنشاء حزمة تثبيت:

a. قبل تثبيت الحزمة على الجهاز، تأكد من أن كل التبعيات مثبتة بالفعل (البرامج والمكتبات) لهذه الحزمة.

يمكنك عرض التبعيات لكل حزمة بنفسك، باستخدام الأدوات المساعدة المحددة للتوزيع على نظام Linux المراد تثبيت الحزمة عليه. للاطلاع على تفاصيل حول الأدوات المساعدة، يرجى الرجوع إلى وثائق نظام التشغيل.

b. لإنشاء حزمة تثبيت عن بُعد، استخدم الملفات التالية:

- klnagent.kpd
- akinstall.sh
- حزمة DEB أو RPM لعميل الشبكة

2. أنشئ مهمة تثبيت عن بُعد باستخدام الإعدادات التالية:

- في صفحة **الإعدادات** الخاصة بمعالج المهمة الجديدة، انقر على زر **استخدام موارد نظام التشغيل من خلال خادم الإدارة**. قم بإلغاء جميع خانات الاختيار الأخرى.
- في الصفحة **تحديد حساب لتشغيل المهمة**، حدد إعدادات حساب المستخدم الذي سيتم استخدامه لتوصيل الجهاز عبر SSH.

3. وقم بتشغيل مهمة التثبيت عن بُعد. استخدم خيار الأمر `su` للحفاظ على البيئة: `-m, -p, --preserve-environment`.

تحضير جهاز يقوم بتشغيل SUSE Linux Enterprise Server 15 لتثبيت عميل الشبكة

لتثبيت عميل الشبكة على جهاز يعمل بنظام التشغيل SUSE Linux Enterprise Server 15،

قبل تثبيت عميل الشبكة، قم بتشغيل الأمر التالي:

```
sudo zypper install insserv-compat
```

يمكّنك هذا من تثبيت حزمة insserv-Compatible وتكوين عميل الشبكة بشكل صحيح.

قم بتشغيل `rpm -q insserv-compat` الأمر للتحقق مما إذا كانت الحزمة مثبتة بالفعل.

إذا كانت شبكتك تتضمن الكثير من الأجهزة التي تعمل بنظام SUSE Linux Enterprise Server 15، فيمكنك استخدام البرنامج الخاص لتكوين وإدارة البنية التحتية للشركة. باستخدام هذا البرنامج، يمكنك تثبيت حزمة insserv-Compatible تلقائيًا على جميع الأجهزة الضرورية مرة واحدة. على سبيل المثال، يمكنك استخدام Puppet أو Ansible أو Chef أو يمكنك إنشاء البرنامج النصي الخاص بك-استخدم أي طريقة مناسبة لك.

إذا لم يكن الجهاز يحتوي على مفاتيح توقيع GPG لنظام SUSE Linux Enterprise، فقد تواجه التحذير التالي: `Package header is not signed!` حدد الخيار `i` لتجاهل التحذير.

إلى جانب تثبيت حزمة insserv-Compatible، تأكد من أنك قد أعدت أجهزة Linux الخاصة بك. بعد ذلك، نشر وتثبيت عميل الشبكة.

إعداد جهاز macOS يعمل لتثبيت عميل الشبكة عن بُعد

لإعداد جهاز macOS لتثبيت عميل الشبكة عن بُعد:

1. تأكد من تثبيت sudo على جهاز الهدف macOS.

2. قم باختبار تكوين الجهاز:

a. تأكد من فتح المنفذ 22 على جهاز العميل. للقيام بذلك، في **تفضيلات النظام**، افتح جزء **المشاركة**، ثم تأكد من أن خانة اختيار **الدخول عن بعد** محددة.

يمكنك الاتصال بجهاز العميل عبر Secure Shell (SSH) فقط من خلال المنفذ 22. لا يمكنك تغيير رقم المنفذ.

يمكنك استخدام أمر `ssh <device_name>` لتسجيل الدخول إلى جهاز macOS عن بُعد. في جزء **المشاركة**، يمكنك استخدام خيار **السماح بخيار الوصول** لتعيين نطاق المستخدمين المسموح لهم بالوصول إلى جهاز macOS.

b. قم بتعطيل كلمة مرور sudo الخاصة بحساب المستخدم الذي سيتم توصيل الجهاز بموجبه.

استخدم الأمر `sudo visudo` في برنامج sudo لفتح ملف تكوين sudoers. في الملف الذي فتحته، في إدخال مواصفات امتياز المستخدم حدد ما يلي: `ALL :NOPASSWD (ALL) = username ALL`. في هذه الحالة، يكون `username` هو حساب المستخدم، الذي يجب استخدامه لاتصال الجهاز باستخدام SSH.

c. احفظ ملف sudoers ثم أغلقه.

d. اتصل بالجهاز مجددًا عبر SSH وتأكد من عدم مطالبة خدمة Sudo بإدخال كلمة مرور؛ ويمكنك القيام بذلك باستخدام الأمر `sudo whoami`.

3. تنزيل وإنشاء حزمة تثبيت:

a. قم بتنزيل حزمة تثبيت عميل الشبكة باستخدام إحدى الطرق التالية:

- في شجرة وحدة التحكم، عن طريق فتح قائمة السياق في **التثبيت عن بُعد** ← **حزم التثبيت** وتحديد **عرض إصدارات التطبيق الحالية** للاختيار من الحزم المتوفرة
- عن طريق تنزيل الإصدار ذي الصلة من عميل الشبكة من موقع ويب الدعم الفني على https://support.kaspersky.com/
- عن طريق طلب حزمة التثبيت من أخصائيي الدعم الفني

b. لإنشاء حزمة تثبيت عن بُعد، استخدم الملفات التالية:

- klnagent.kud
- install.sh
- klnagentmac.dmg

4. إنشاء مهمة تثبيت عن بُعد بالإعدادات التالية:

- في صفحة **إعدادات** الخاصة بمعالج المهمة الجديدة، انقر على زر **استخدام موارد نظام التشغيل من خلال خادم الإدارة**. قم بإلغاء جميع خانات الاختيار الأخرى.
- في صفحة **تحديد حساب لتشغيل المهمة**، ولتشغيل المهمة؛ حدد إعدادات حساب المستخدم الذي سيتم استخدامه لاتصال الجهاز عبر SSH.

جهاز العميل جاهز للتثبيت عن بُعد لعميل الشبكة من خلال المهمة المقابلة التي قمت بإنشائها.

تطبيقات Kaspersky: الترخيص والتنشيط

يوضح هذا القسم ميزات Kaspersky Security Center المتعلقة بالتعامل مع مفاتيح الترخيص لتطبيقات Kaspersky المُدارة.

يسمح لك Kaspersky Security Center بإجراء توزيع مركزي لمفاتيح الترخيص الخاصة بتطبيقات Kaspersky على الأجهزة العميلة ومراقبة استخدامها وتجديد تراخيصها.

عند إضافة مفتاح ترخيص باستخدام Kaspersky Security Center، يتم حفظ إعدادات مفتاح الترخيص على خادم الإدارة. وبناءً على هذه المعلومات، يصدر التطبيق تقريرًا حول استخدام مفتاح الترخيص ويقوم بإخطار المسؤول بانتهاء صلاحية الترخيص وانتهاك قيود الترخيص المحددة في خصائص مفاتيح التراخيص. يمكنك تكوين إخطارات استخدام مفاتيح التراخيص في إعدادات خادم الإدارة.

ترخيص التطبيقات المُدارة

يجب إصدار ترخيص لتطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال تطبيق ملف المفتاح أو رمز التفعيل على كل تطبيق من التطبيقات. يمكن نشر ملف المفتاح أو رمز التفعيل بالطرق التالية:

- النشر التلقائي
- حزمة تثبيت التطبيق المُدار

- المهمة إضافة مفتاح الترخيص لتطبيق مُدار
- التفعيل اليدوي للتطبيق المُدار

يمكنك إضافة مفتاح ترخيص نشط أو احتياطي جديد بأي من الطرق المذكورة أعلاه. يستخدم تطبيق Kaspersky مفتاحًا نشطًا في الوقت الحالي ويخزن مفتاح احتياطي لتطبيقه بعد انتهاء صلاحية المفتاح النشط. يحدد التطبيق الذي تضيف مفتاح ترخيص له ما إذا كان المفتاح نشطًا أم احتياطيًا. لا يعتمد تعريف المفتاح على الطريقة التي تستخدمها لإضافة مفتاح ترخيص جديد.

النشر التلقائي

إذا كنت تستخدم تطبيقات مدارة مختلفة وكان عليك نشر ملف مفتاح محدد أو رمز تنشيط للأجهزة، فقم باختيار طرق أخرى لنشر ملف المفتاح أو رمز التفعيل هذا.

يتيح لك Kaspersky Security Center نشر مفاتيح الترخيص المتاحة تلقائيًا إلى الأجهزة. على سبيل المثال، يتم تخزين ثلاثة مفاتيح ترخيص في مستودع خادم الإدارة. لقد حددت خانة الاختيار **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها** لجميع مفاتيح الترخيص الثلاثة. تطبيق أمان Kaspersky— على سبيل المثال، تم تثبيت — Kaspersky Endpoint Security for Windows على أجهزة المؤسسة. تم اكتشاف الجهاز الجديد الذي يجب نشر المفتاح إليه. يحدد التطبيق على سبيل المثال، أنه يمكن نشر اثنين من مفاتيح التراخيص المتواجدة في المستودع إلى الجهاز وهما: مفتاح ترخيص باسم Key_1 ومفتاح ترخيص باسم Key_2. يتم نشر أحد هذين المفتاحين إلى الجهاز. وفي هذه الحالة، لا يمكن توقع مفتاح الترخيص الذي سيتم نشره إلى الجهاز لأن النشر التلقائي لمفاتيح التراخيص لا يسمح بإجراء أي نشاط للمسؤول.

عندما يتم نشر مفتاح ترخيص، تتم إعادة احتساب الأجهزة لمفتاح الترخيص هذا. ويجب عليك التأكد من أن عدد الأجهزة التي تم نشر مفتاح الترخيص إليها لا يتجاوز حد الترخيص. إذا تجاوز عدد الأجهزة حد الترخيص، فسيتم تعيين حالة جميع الأجهزة التي لم تكن مشمولة بالترخيص إلى الحالة حرج.

قبل النشر، يجب إضافة ملف المفتاح أو رمز التفعيل إلى مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - التوزيع التلقائي لمفتاح الترخيص

أو

- Kaspersky Security Center Web Console:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - التوزيع التلقائي لمفتاح الترخيص

لاحظ أنه قد لا يتم عرض مفتاح الترخيص الموزع تلقائيًا في مستودع خادم الإدارة الافتراضي في الحالات التالية:

- مفتاح الترخيص غير صالح للتطبيق.
- لا يحتوي خادم الإدارة الافتراضي على أجهزة مُدارة.
- تم استخدام مفتاح الترخيص بالفعل للأجهزة المُدارة بواسطة خادم إدارة افتراضي آخر وتم الوصول إلى الحد الأقصى لعدد الأجهزة.

إضافة ملف المفتاح أو رمز تنشيط إلى حزمة التثبيت الخاصة بتطبيق مُدار

لأسباب تتعلق بالأمان، لا يوصى باستخدام هذا الخيار. قد يتم اختراق ملف المفتاح أو رمز التفعيل المُضاف إلى حزمة التثبيت.

إذا قمت بتثبيت تطبيق مدار باستخدام حزمة تثبيت، يمكنك تحديد رمز تنشيط أو ملف المفتاح في حزمة التثبيت هذه أو في السياسة الخاصة بالتطبيق. سيتم نشر مفتاح الترخيص إلى الأجهزة المُدارة عند إجراء المزامنة التالية للجهاز مع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إنشاء حزمة توزيع
  - تثبيت التطبيقات على الأجهزة العميلة

أو

- Kaspersky Security Center Web Console: إضافة مفتاح ترخيص إلى حزمة تثبيت

النشر من خلال مهمة إضافة مفتاح الترخيص لتطبيق مُدار

إذا اخترت استخدام مهمة إضافة مفتاح الترخيص لتطبيق مُدار، يمكنك تحديد مفتاح الترخيص الذي يجب نشره إلى الأجهزة وتحديد الأجهزة بأية طريقة ملائمة، على سبيل المثال من خلال تحديد مجموعة إدارة أو تحديد جهاز.

قبل النشر، يجب إضافة ملف المفتاح أو رمز التنشيط إلى مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - نشر مفتاح ترخيص على الأجهزة العميلة

أو

- Kaspersky Security Center Web Console:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - نشر مفتاح ترخيص على الأجهزة العميلة

إضافة رمز التفعيل أو ملف المفتاح إلى الأجهزة يدويًا

يمكنك تنشيط تطبيق Kaspersky المثبّت محليًا من خلال استخدام الأدوات المتوفرة في واجهة التطبيق. يرجى الرجوع إلى وثائق التطبيق المثبّت.

عرض معلومات حول مفاتيح التراخيص قيد الاستخدام

لعرض معلومات حول مفاتيح التراخيص قيد الاستخدام،

في شجرة وحدة التحكم، حدد المجلد **تراخيص Kaspersky**.

تعرض مساحة عمل المجلد قائمة بمفاتيح التراخيص المُستخدمة على الأجهزة العميلة.

يظهر رمز بجوار كل مفاتيح التراخيص يطابق نوع الاستخدام:

- —يتم تلقي معلومات عن مفتاح الترخيص المُستخدم من الجهاز العميل المتصل بخادم الإدارة. ويتم تخزين ملف مفتاح الترخيص هذا خارج خادم الإدارة.
- —يتم تخزين مفتاح الترخيص في مستودع خادم الإدارة. ويتم تعطيل التوزيع التلقائي لمفتاح الترخيص هذا.
- —يتم تخزين مفتاح الترخيص في مستودع خادم الإدارة. ويتم تمكين التوزيع التلقائي لمفتاح الترخيص هذا.

يمكنك عرض معلومات حول مفاتيح التراخيص المُستخدمة لتفعيل التطبيق على جهاز عميل من خلال فتح القسم **التطبيقات** في النافذة خصائص الجهاز العميل.

لتحديد الإعدادات المحدثة لمفاتيح ترخيص خادم الإدارة، يقوم خادم الإدارة بإرسال طلب إلى خوادم تفعيل Kaspersky مرة واحدة يوميًا على الأقل. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة.

في حالة استلام مفتاح ترخيص من جهاز عميل، فلا يمكنك تصديره كملف.

إضافة مفتاح ترخيص إلى مستودع خادم الإدارة

لإضافة مفتاح ترخيص إلى مستودع خادم الإدارة:

1. في شجرة وحدة التحكم، حدد المجلد **تراخيص Kaspersky** .
2. ابدأ مهمة إضافة مفتاح الترخيص بإحدى الطرق التالية:
   - حدد **إضافة ملف المفتاح أو رمز التنشيط** من قائمة سياق مفتاح الترخيص.
   - انقر فوق الرابط **إضافة ملف المفتاح أو رمز التنشيط** في مساحة العمل الخاصة بقائمة مفاتيح التراخيص.
   - انقر فوق زر **إضافة ملف المفتاح أو رمز التنشيط**.

   سيبدأ إضافة معالج مفتاح الترخيص.
3. حدد كيف تريد تنشيط خادم الإدارة: باستخدام رمز تنشيط أو باستخدام ملف مفتاح.

4. حدد رمز التفعيل الخاص بك أو ملف مفتاح الترخيص.

5. حدد خيار **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها** إذا كنت تريد توزيع مفتاح ترخيص ذي صلة على شبكتك على الفور. إذا لم تحدد هذا الخيار، فيمكنك يدويًا توزيع مفتاح الترخيص في وقت لاحق.

نتيجة لذلك، يتم تنزيل ملف المفتاح وينتهي إضافة معالج مفتاح الترخيص. يمكنك الآن رؤية مفتاح الترخيص المضاف في قائمة تراخيص Kaspersky.

إزالة مفتاح ترخيص خادم الإدارة

لإزالة مفتاح ترخيص خادم الإدارة:

1. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

2. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **المفاتيح**.

3. قم بإزالة مفتاح الترخيص عن طريق النقر على الزر **إزالة**.

يؤدي هذا إلى إزالة مفتاح الترخيص.

في حالة إضافة مفتاح ترخيص احتياطي، يصبح مفتاح الترخيص الاحتياطي تلقائيًا مفتاح الترخيص المفعل بعد إزالة مفتاح الترخيص المفعل السابق.

بعد إزالة مفتاح الترخيص المفعل لخادم الإدارة، لا تتوفر إدارة الثغرات الأمنية والتصحيحات وإدارة الجهاز المحمول. يمكنك إضافة مفتاح تمت إزالته مرة أخرى أو إضافة مفتاح ترخيص جديد.

نشر مفتاح ترخيص على الأجهزة العميلة

يسمح لك Kaspersky Security Center بتوزيع مفتاح ترخيص على الأجهزة العميلة من خلال مهمة توزيع مفتاح الترخيص.

قبل النشر، أضف مفتاح ترخيص إلى مستودع خادم الإدارة.

لتوزيع مفتاح ترخيص على الأجهزة العميلة:

1. في شجرة وحدة التحكم، حدد المجلد **تراخيص Kaspersky** .

2. في مساحة عمل قائمة مفاتيح التراخيص، انقر فوق الزر **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها**.
يبدأ تشغيل **معالج إنشاء مهمة تفعيل التطبيق**. انتقل عبر المعالج باستخدام زر **التالي**.

3. في قائمة التطبيقات، حدد التطبيق الذي ترغب في إنشاء مهمة له.

4. في خطوة **إضافة المفتاح** في المعالج، أضف مفتاح الترخيص باستخدام أحد الخيارات التالية:

- حدد الخيار **رمز التنشيط** لإضافة رمز تفعيل من مستودع Kaspersky Security Center.
انقر فوق **تحديد**. في النافذة التي تفتح، حدد رمز التفعيل، ثم انقر فوق **موافق** .

- حدد الخيار **Key file or key**، ثم نفذ ما يلي:

a. انقر فوق **تحديد**.

b. في قائمة السياق، حدد أحد الخيارات:

- **ملف المفتاح من المجلد**.

  في النافذة التي تفتح، حدد ملف المفتاح من الجهاز الخاص بك، ثم انقر فوق **فتح**.

- **مفتاح من مستودع Kaspersky Security Center**.

  في النافذة التي تفتح، حدد المفتاح من مستودع Kaspersky Security Center، ثم انقر فوق **موافق**.

5. إذا كنت تريد استبدال مفتاح الترخيص النشط الحالي، فقم بإلغاء تحديد خانة الاختيار **استخدام كمفتاح احتياطي**.

على سبيل المثال، يكون ذلك مطلوبًا عندما تتغير المؤسسة، ويكون مفتاح مؤسسة أخرى مطلوبًا على الجهاز؛ أو إذا تمت إعادة إصدار المفتاح، وتنتهي صلاحية الترخيص الجديد قبل الترخيص الحالي. ولتجنب الأخطاء، يجب عليك إلغاء تحديد خانة الاختيار **استخدام كمفتاح احتياطي**.

إذا كنت ترغب في معرفة المزيد من المعلومات عن المشكلات التي قد تحدث عند إضافة مفتاح ترخيص إلى Kaspersky Security Center Windows وطرق حلها، فارجع إلى قاعدة معارف Kaspersky Security Center.

6. تحقق من معلومات مفتاح الترخيص، ثم انقر فوق **التالي**.

7. في هذه الخطوة من المعالج، حدد الأجهزة التي تريد تعيين مهمة إضافة مفتاح إليها. يمكنك تحديد الأجهزة (حتى 1000 جهاز) بإحدى الطرق التالية:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة** . في هذه الحالة، يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.

- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**. يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

- **تعيين مهمة إلى تحديد الجهاز** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في المجموعة المحددة التي تم إنشائها في وقت سابق. يمكنك تحديد المجموعة المحددة مسبقًا أو المجموعة المخصصة التي أنشأتها.

- **تعيين مهمة لمجموعة إدارة** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في مجموعة الإدارة التي تم إنشائها في وقت سابق.

8. في خطوة **تكوين جدول المهمة** في المعالج، أنشئ جدولاً لبدء المهمة:

- **البدء المُجدول**:

  - **مرة**

  يتم تشغيل المهمة مرة واحدة، في التاريخ والوقت المحددين (افتراضيًا، في اليوم الذي تم إنشاء المهمة فيه).

  - **يدويًا**

  لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

  يتم تحديد هذا الخيار افتراضيًا.

- **عند تنزيل تحديثات جديدة إلى المستودع**

تعمل المهمة بعد تنزيل التحديثات إلى المستودع. على سبيل المثال، قد ترغب في استخدام هذا الجدول للبحث عن الثغرات الأمنية ومهمة التحديثات المطلوبة.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

9. في الخطوة **حدد اسم المهمة** في المعالج، حدد اسم المهمة. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة (*"<>?\:|).

10. في خطوة **إنهاء عملية إنشاء المهمة** في المعالج انقر فوق الزر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار **Run the task after the wizard finishes**.

المهام التي يتم إنشاؤها باستخدام **معالج إنشاء مهمة تفعيل التطبيق** هي مهام لأجهزة محددة مخزنة في المجلد **المهام** في شجرة وحدة التحكم.

ويمكنك أيضًا إنشاء مجموعة أو مهمة توزيع مفتاح ترخيص محلية عبر "معالج إنشاء مهمة" لمجموعة إدارة ولجهاز عميل.

التوزيع التلقائي لمفتاح الترخيص

يتيح Kaspersky Security Center إمكانية التوزيع التلقائي لمفاتيح الترخيص على الأجهزة المدارة في حالة وجودها في مستودع مفاتيح التراخيص على خادم الإدارة. لا ينطبق التوزيع التلقائي لمفاتيح الترخيص على الأجهزة الموجودة في مجلد **الأجهزة غير المخصصة**.

لتوزيع أحد مفاتيح التراخيص إلى الأجهزة المدارة تلقائيًا:

1. في شجرة وحدة التحكم، حدد المجلد **تراخيص Kaspersky** .
2. في مساحة عمل المجلد، حدد مفتاح الترخيص الذي تريد توزيعه إلى الأجهزة تلقائيًا.
3. افتح نافذة خصائص مفتاح الترخيص المحدد باستخدام إحدى الطرق التالية:
   - من خلال تحديد **خصائص** من قائمة سياق مفتاح الترخيص.
   - من خلال النقر فوق الرابط **عرض خصائص المفتاح** في خانة المعلومات الخاصة بمفتاح الترخيص المحدد.
4. من نافذة خصائص مفتاح الترخيص التي يتم فتحها، حدد خانة اختيار **مفتاح موزع تلقائيًا**. أغلق نافذة خصائص مفتاح الترخيص.

   سيتم توزيع مفتاح الترخيص تلقائيًا على جميع الأجهزة المتوافقة.

يتم توزيع مفتاح الترخيص من خلال وسائل عميل الشبكة. لم يتم إنشاء مهام توزيع مفتاح الترخيص للتطبيق.

أثناء التوزيع التلقائي لمفتاح الترخيص، يتم أخذ حد الترخيص على عدد الأجهزة في الاعتبار. (تم تعيين حد الترخيص في خصائص مفتاح الترخيص.) في حالة الوصول إلى حد الترخيص، يتوقف توزيع مفتاح الترخيص هذا على الأجهزة تلقائيًا.

يوزع خادم الإدارة الافتراضي تلقائيًا مفاتيح الترخيص من مخزنه ومن مستودع خادم الإدارة. نوصيك بما يلي:

- استخدم مهمة إضافة مفتاح الترخيص لتحديد مفتاح الترخيص الذي يجب نشره على الأجهزة.
- تجنب تعطيل الخيار **Allow automatic deployment of license keys from this virtual Administration Server to its devices** في إعدادات خادم الإدارة الافتراضي. وبخلاف ذلك، لن يوزع خادم الإدارة الافتراضي مفاتيح الترخيص على الأجهزة، بما في ذلك مفاتيح الترخيص من مستودع خادم الإدارة.

إذا حددت خانة الاختيار **مفتاح موزع تلقائيًا** في نافذة خصائص مفتاح الترخيص، فسيتم توزيع مفتاح ترخيص على شبكتك على الفور. إذا لم تحدد هذا الخيار، فيمكنك يدويًا توزيع مفتاح الترخيص في وقت لاحق.

إنشاء تقرير حول استخدام مفتاح الترخيص وعرضه

لإنشاء تقرير حول استخدام مفاتيح التراخيص على الأجهزة العميلة:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .
3. حدد قالب التقرير الذي يحمل الاسم **تقرير استخدام مفتاح الترخيص**، أو قم بإنشاء قالب تقرير جديد من نفس النوع.

تعرض مساحة العمل لتقرير حول استخدام مفتاح الترخيص معلومات حول مفاتيح الترخيص المفعلة والإضافية المُستخدمة على أجهزة العملاء. ويحتوي التقرير أيضًا على معلومات حول الأجهزة التي تُستخدم بها مفاتيح التراخيص، وحول التقييدات المحددة في خصائص مفاتيح التراخيص هذه.

عرض معلومات حول مفاتيح ترخيص التطبيق

لمعرفة مفاتيح الترخيص المستخدمة لتطبيق Kaspersky:

1. في شجرة وحدة التحكم Kaspersky Security Center، حدد العقدة **الأجهزة المُدارة** وانتقل إلى علامة التبويب **الأجهزة**.
2. انقر بزر الماوس الأيمن لفتح قائمة سياق الجهاز ذي الصلة وحدد **خصائص**.
3. في النافذة خصائص الجهاز التي تُفتح، حدد القسم **التطبيقات**.
4. في قائمة التطبيقات التي تظهر، حدد التطبيق الذي تريد عرض مفاتيح ترخيصه، ثم انقر فوق الزر **خصائص**.
5. في نافذة خصائص التطبيق التي تفتح، حدد قسم **مفاتيح الترخيص**.

   يتم عرض المعلومات في مساحة العمل الخاصة بهذا القسم.

تصدير ملف مفتاح الترخيص

إذا تم حذف مفتاح الترخيص الخاص بك عن طريق الخطأ وتريد استعادته، فيمكنك تصدير ملف مفتاح الترخيص من خادم إدارة آخر.

لتصدير ملف مفتاح ترخيص، يجب أن يكون لديك **تصدير ملف المفتاح** مباشرةً في منطقة وظائف **المزايا العامة: Key management**.

إذا تم استلام مفتاح ترخيص من جهاز عميل، فلا يمكنك تصديره.

لتصدير مفتاح ترخيص:

1. في شجرة وحدة التحكم، حدد المجلد **تراخيص Kaspersky** .
2. في القائمة، حدد مفتاح الترخيص الذي تريد تصديره كملف.

3. في مربع المعلومات الذي يتم فتحه، انقر على الرابط **تصدير ملف المفتاح**.

4. في النافذة التي تفتح، حدد المسار إلى المجلد الذي تريد حفظ ملف مفتاح الترخيص فيه، ثم حدد اسمًا للملف. بعد ذلك، انقر فوق **حفظ**.

يتم تصدير ملف مفتاح الترخيص بتنسيق .key إلى المجلد المحدد.

إذا كان مفتاح الترخيص الذي قمت بتصدير ملفه قم تم إضافته إلى مستودع خادم الإدارة كرمز تفعيل، وتريد إضافة ملف مفتاح الترخيص الذي تم تصديره إلى مستودع خادم إدارة آخر، فيجب عليك إضافته كرمز تفعيل، وليس كملف مفتاح. وإلا، سيحدث خطأ. ويتعين عليك فتح ملف مفتاح الترخيص الذي تم تصديره في أي محرر نصوص مناسب، ثم نسخ رمز التفعيل.

تكوين حماية الشبكة

يحتوي هذا القسم على معلومات حول التكوين اليدوي للسياسات والمهام، ومعلومات حول أدوار المستخدم، ومعلومات حول بناء هيكل مجموعة الإدارة والتسلسل الهرمي للمهام.

السيناريو: تكوين حماية الشبكة

ينشئ معالج البدء السريع سياسات ومهام باستخدام الإعدادات الافتراضية. قد يتبين أن هذه الإعدادات دون المستوى الأمثل أو حتى غير مسموح بها من قِبل المؤسسة. لذلك، نوصي بضبط هذه السياسات والمهام وإنشاء سياسات ومهام أخرى، إذا كانت ضرورية للشبكة لديك.

المتطلبات الأساسية

قبل البدء، تأكد من إجرائك لما يلي:

- خادم إدارة Kaspersky Security Center المُثبت
- Kaspersky Security Center Web Console المُثبت (اختياري)
- تم إكمال سيناريو التثبيت الرئيسي لـ Kaspersky Security Center
- عند اكتمال معالج البدء السريع أو إنشاء السياسات والمهام التالية يدويًا في مجموعة إدارة **الأجهزة المُدارة**:
  - سياسة Kaspersky Endpoint Security
  - مهمة جماعية لتحديث Kaspersky Endpoint Security
  - سياسة عميل الشبكة
  - البحث عن الثغرات الأمنية ومهمة التحديثات المطلوبة

يجري تكوين حماية الشبكة على المراحل التالية:

1. **إعداد ونشر سياسات وملفات تعريف السياسة لتطبيق Kaspersky**

لتكوين ونشر إعدادات لتطبيقات Kaspersky المثبتة على الأجهزة المُدارة، يمكنك استخدام نهجين مختلفين لإدارة الأمان- نهج مرتكز على الجهاز أو نهج مرتكز على المستخدم. يمكن الجمع بين هذين النهجين. لتنفيذ إدارة الأمان المرتكزة على الجهاز، يمكنك استخدام الأدوات المتوفرة في وحدة تحكم الإدارة التي تعمل في Microsoft Management Console أو Kaspersky Security Center Web Console. يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال Kaspersky Security Center Web Console فقط.

2. **تكوين المهام للإدارة عن بُعد لتطبيقات Kaspersky**

تحقق من المهام التي تم إنشاؤها بواسطة معالج البدء السريع وقم بضبطهم إذا لزم الأمر.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - يجري إعداد مهمة جماعية لتحديث Kaspersky Endpoint Security
  - جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
- Kaspersky Security Center Web Console:
  - يجري إعداد مهمة جماعية لتحديث Kaspersky Endpoint Security
  - البحث عن الثغرات الأمنية والإعدادات المطلوبة لمهمة التحديثات

إذا لزم الأمر، قم بإنشاء مهام إضافية لإدارة تطبيقات Kaspersky المثبتة على الأجهزة العميلة.

3. **تقييم وتقييد تحميل الحدث على قاعدة البيانات**

يتم نقل المعلومات حول الأحداث التي تحدث أثناء تشغيل التطبيقات المُدارة من جهاز عميل ويتم تسجيلها بقاعدة بيانات خادم الإدارة. لتقييد التحميل على خادم الإدارة، قم بتقييم وتقليل أقصى عدد من الأحداث التي يمكن تخزينها في قاعدة البيانات.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تعيين الحد الأقصى لعدد الأحداث
- Kaspersky Security Center Web Console: تعيين الحد الأقصى لعدد الأحداث

النتائج

عند إكمال هذا السيناريو، ستتم حماية شبكتك عن طريق تكوين تطبيقات ومهام وأحداث Kaspersky التي يتلقاها خادم الإدارة:

- يتم تكوين تطبيقات Kaspersky وفقًا للسياسات وملفات تعريف السياسة.
- تتم إدارة التطبيقات من خلال مجموعة من المهام.
- يتم تعيين الحد الأقصى لعدد الأحداث التي يمكن تخزينها في قاعدة البيانات.

عند إكمال تكوين حماية الشبكة، يمكنك متابعة تكوين التحديثات المنتظمة للتطبيقات وقواعد بيانات Kaspersky.

للحصول على تفاصيل حول كيفية تكوين الاستجابات التلقائية للتهديدات التي اكتشفها Kaspersky Sandbox، يرجى الإشارة إلى تعليمات Kaspersky Sandbox 2.0 عبر الإنترنت.

نشر وإعداد السياسة: نهج مرتكز على الجهاز

عند قيامك بإكمال هذا السيناريو، سيتم تكوين التطبيقات على جميع الأجهزة المُدارة وفقًا لسياسات التطبيق وملفات تعريف السياسة التي تحددها.

المتطلبات الأساسية

قبل البدء، تأكد من تثبيت خادم إدارة Kaspersky Security Center وKaspersky Security Center Web Console (اختياري). إذا قمت بتثبيت Kaspersky Security Center Web Console، فقد ترغب أيضًا في اعتبار إدارة الأمان المعتمد على المستخدم كخيار بديل أو إضافي للنهج المرتكز على الجهاز.

المراحل

يتكون سيناريو الإدارة المرتكزة على الجهاز لتطبيقات Kaspersky من الخطوات التالية:

1. **تكوين سياسات التطبيق**

قم بتكوين إعدادات تطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال إنشاء سياسة لكل تطبيق. سيتم نشر مجموعة السياسات إلى الأجهزة العميلة.

عند تكوين حماية شبكتك في معالج البدء السريع، سيُنشئ Kaspersky Security Center السياسة الافتراضية للتطبيقات التالية:

- Kaspersky Endpoint Security for Windows — للأجهزة العميلة المستندة إلى Windows
- Kaspersky Endpoint Security for Linux—للأجهزة العميلة المستندة إلى Linux

إذا قمت باستكمال عملية التكوين باستخدام هذا المعالج، فليس عليك إنشاء سياسة جديدة لهذا التطبيق. الانتقال إلى الإعداد اليدوي لسياسة Kaspersky Endpoint Security.

إذا كانت لديك بنية هرمية للعديد من خوادم الإدارة و/أو مجموعات الإدارة، فإن خوادم الإدارة الثانوية ومجموعات الإدارة الفرعية ترث السياسات من خادم الإدارة الرئيسي بشكلٍ افتراضي. يمكنك فرض الوراثة من خلال المجموعات الفرعية وخوادم الإدارة الثانوية لمنع أي تعديلات في الإعدادات المكونة في سياسة المنبع. إذا كنت تريد فقط أن يتم توريث جزء من الإعدادات بالقوة، فيمكنك قفلها في سياسة المنبع. ستكون بقية الإعدادات غير المقفلة متاحة للتعديل في السياسات التالية. سوف يتيح لك التسلسل الهرمي للسياسات الذي قمت بإنشائه إدارة الأجهزة بفعالية في مجموعات الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء سياسة
- Kaspersky Security Center Web Console: إنشاء سياسة

2. **إنشاء ملفات تعريف السياسة (اختياري)**

إذا أردت تشغيل الأجهزة الموجودة ضمن مجموعة إدارة واحدة ضمن إعدادات سياسة مختلفة، فقم بإنشاء ملفات تعريف سياسة لهذه الأجهزة. ملف تعريف السياسة هو مجموعة فرعية مسمّاة لإعدادات السياسة. يتم توزيع هذه المجموعة الفرعية على الأجهزة المستهدفة بالإضافة إلى السياسة، وتلحقها في حالة خاصة تُسمى شرط تفعيل ملف التعريف. تحتوي ملفات التعريف فقط على الإعدادات التي تختلف عن السياسة "الأساسية"، والتي تكون نشطة على الجهاز المُدار.

باستخدام شروط تنشيط ملف التعريف، يمكنك تطبيق ملفات تعريف سياسة مختلفة، على سبيل المثال، على الأجهزة الموجودة في وحدة محددة أو مجموعة أمان في Active Directory، مع وجود تكوين محدد للمكونات، أو تحمل علاماتمحددة. استخدم العلامات لتصفية الأجهزة التي تستوفي معايير محددة. على سبيل المثال، يمكنك إنشاء علامة تسمى Windows، وتحديد على جميع الأجهزة التي تعمل بنظام تشغيل Windows باستخدام هذه العلامة، ثم تحديد هذه العلامة كشرط تفعيل لملف تعريف سياسة. ونتيجة لذلك، ستتم إدارة تطبيقات Kaspersky المثبتة على جميع الأجهزة التي تعمل بنظام Windows عن طريق ملف تعريف السياسة الخاص بها.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إنشاء ملف تعريف سياسة
  - إنشاء قاعدة تفعيل ملف تعريف سياسة
- Kaspersky Security Center Web Console:
  - إنشاء ملف تعريف سياسة
  - إنشاء قاعدة تفعيل ملف تعريف سياسة

3 **نشر السياسات وملفات تعريف السياسة على الأجهزة المدارة**

بشكل افتراضي، يعمل خادم الإدارة تلقائيًا على المزامنة مع الأجهزة المُدارة كل 15 دقيقة. يمكنك تجنب المزامنة التلقائية وتشغيل المزامنة يدويًا باستخدام الأمر فرض المزامنة. كما يتم فرض التزامن بعد إنشاء أو تغيير سياسة أو ملف تعريف سياسة. وأثناء المزامنة، يتم نشر السياسات وملفات تعريف السياسة الجديدة أو التي تم تغييرها إلى الأجهزة المُدارة.

إذا كنت تستخدم Kaspersky Security Center Web Console، يمكنك التحقق مما إذا كان قد تم تسليم السياسات وملفات تعريف السياسة إلى جهاز. يحدد Kaspersky Security Center تاريخ ووقت التسليم في خصائص الجهاز.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: المزامنة المفروضة
- Kaspersky Security Center Web Console: المزامنة المفروضة

النتائج

عند اكتمال السيناريو المرتكز على الجهاز، يتم تكوين تطبيقات Kaspersky وفقًا للإعدادات التي تم تحديدها ونشرها من خلال التسلسل الهرمي للسياسات.

سيتم تلقائيًا تطبيق سياسات التطبيق الذي تم تكوينه وملفات تعريف السياسة على الأجهزة الجديدة المُضافة إلى مجموعات الإدارة.

حول نُهج إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم

يمكنك إدارة إعدادات الأمان من منطلق مزايا الجهاز ومن منطلق أدوار المستخدم. يُطلق على النهج الأول إدارة الأمان المرتكزة على الجهاز ويُطلق على النهج الثاني إدارة الأمان المرتكزة على المستخدم. لتطبيق إعدادات تطبيق مختلفة على أجهزة مختلفة، يمكنك استخدام أي من نوعي الإدارة أو كليهما معًا. لتنفيذ إدارة الأمان المرتكزة على الجهاز، يمكنك استخدام الأدوات المتوفرة في وحدة تحكم الإدارة التي تعمل في Microsoft Management Console أو Kaspersky Security Center Web Console. يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال Kaspersky Security Center Web Console فقط.

تمكنك إدارة الأمان المرتكزة على الجهاز من تطبيق إعدادات تطبيق الأمان المختلفة على الأجهزة المدارة اعتمادًا على الميزات الخاصة بالجهاز. على سبيل المثال، يمكنك تطبيق إعدادات مختلفة على الأجهزة المخصصة في مجموعات الإدارة المختلفة. يمكنك أيضًا التمييز بين الأجهزة باستخدام تلك الأجهزة فيActive Directory أو مواصفات أجهزتهم.

تمكنك إدارة الأمان المرتكزة على المستخدم من تطبيق إعدادات تطبيق الأمان المختلفة على أدوار المستخدم المختلفة. يمكنك إنشاء عدة أدوار للمستخدم وتعيين دور مستخدم مناسب لكل مستخدم وتحديد إعدادات التطبيق المختلفة للأجهزة التي يملكها المستخدمون ذوي الأدوار المختلفة. على سبيل المثال، قد ترغب في تطبيق إعدادات تطبيق مختلفة على أجهزة المحاسبين والمتخصصين في قسم الموارد البشرية. ونتيجة لذلك، عند تنفيذ إدارة الأمان المرتكزة على المستخدم، فكل قسم من—أقسام الحسابات و الموارد البشرية—لديه تكوين الإعدادات الخاصة به لتطبيقات Kaspersky. يحدد تكوين الإعدادات إعدادات التطبيق التي يمكن تغييرها عن طريق المستخدمين والتي يتم تحديدها وقفلها بالقوة عن طريق المسؤول.

باستخدامك لنهج إدارة الأمان المرتكز على المستخدم يمكنك تطبيق إعدادات التطبيق المحددة للمستخدمين الفرديين. قد يكون هذا مطلوبًا عندما يكون للموظف دورًا فريدًا في الشركة أو عندما تريد مراقبة مشاكل الأمان المتعلقة بأجهزة شخص معين. اعتمادًا على دور هذا الموظف في الشركة، يمكنك توسيع أو تقييد حقوق هذا الشخص لتغيير إعدادات التطبيق. على سبيل المثال، قد ترغب في توسيع حقوق مسؤول النظام الذي يدير الأجهزة العميلة في مكتب محلي.

يمكنك أيضًا الجمع بين أساليب إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم. على سبيل المثال، يمكنك تكوين سياسة تطبيق محددة لكل مجموعة إدارة، ثم إنشاء ملفات تعريف السياسة لدور مستخدم واحد أو عدة أدوار مستخدم في مؤسستك. في هذه الحالة يتم تطبيق السياسات وملفات تعريف السياسة بالترتيب التالي:

1. يتم تطبيق السياسات التي تم إنشاؤها لإدارة الأمان المرتكزة على الجهاز.
2. يتم تعديلهم بواسطة ملفات تعريف السياسة وفقًا لأولويات ملف تعريف السياسة.
3. يتم تعديل السياسات بواسطة ملفات تعريف السياسة المرتبطة بأدوار المستخدم.

الإعداد اليدوي لسياسة Kaspersky Endpoint Security

يقدم هذا القسم اقتراحات حول كيفية تكوين سياسة Kaspersky Endpoint Security، التي يتم إنشاؤها بواسطة معالج البدء السريع. يمكنك إجراء الإعداد في نافذة خصائص السياسة.

عند تحرير إعداد ما، ضع في الاعتبار أنه يجب عليك النقر على أيقونة القفل فوق الإعداد ذي الصلة للسماح باستخدام القيمة الخاصة به على محطة عمل.

تكوين السياسة في قسم الحماية من التهديدات المتقدمة

للحصول على وصف كامل للإعدادات الموجودة في هذا القسم، فبرجاء الرجوع إلى وثائق Kaspersky Endpoint Security for Windows.

في قسم **الحماية من التهديدات المتقدمة**، يمكنك تكوين استخدام Kaspersky Security Network لتطبيق Kaspersky Endpoint Security for Windows. كما يمكنك تكوين وحدات Kaspersky Endpoint Security for Windows النمطية، مثل اكتشاف السلوك ومنع الاستغلال ومنع اختراق المضيف ومحرك المعالجة.

في القسم الفرعي **Kaspersky Security Network**، نوصيك بتمكين الخيار **Kaspersky Security Network**. يساعد استخدام هذا الخيار في إعادة توزيع وتحسين حركة المرور على الشبكة. إذا كان خيار **Kaspersky Security Network** معطلاً، فيمكنك تمكين استخدام خوادم KSN مباشرةً.

تكوين السياسة في قسم الحماية من التهديدات الأساسية

للحصول على وصف كامل للإعدادات الموجودة في هذا القسم، فبرجاء الرجوع إلى وثائق Kaspersky Endpoint Security for Windows.

في قسم **الحماية من التهديدات الأساسية** في نافذة خصائص السياسة، نوصي بتحديد إعدادات إضافية في القسمين الفرعيين **جدار الحماية** و**الحماية من تهديدات الملفات**.

يحتوي القسم الفرعي **جدار الحماية** على إعدادات تسمح لك بالتحكم في نشاط الشبكة للتطبيقات على أجهزة العميل. يستخدم جهاز العميل شبكة تم تعيين إحدى الحالات التالية لها: عامة أو محلية أو موثوقة. اعتمادًا على حالة الشبكة، يمكن أن يسمح Kaspersky Endpoint Security بنشاط الشبكة على الجهاز أو يرفضه. عند إضافة شبكة جديدة إلى مؤسستك، يجب عليك تعيين حالة شبكة مناسبة لها. على سبيل المثال، إذا كان جهاز العميل عبارة عن كمبيوتر محمول ، فإننا نوصي بأن يستخدم هذا الجهاز الشبكة العامة أو الموثوقة، لأن الكمبيوتر المحمول غير متصل دائمًا بالشبكة المحلية. في القسم الفرعي **جدار الحماية**، يمكنك التحقق مما إذا كنت قد قمت بتعيين الحالات بشكل صحيح للشبكات المستخدمة في مؤسستك.

للتحقق من قائمة الشبكات:

1. في نافذة خصائص السياسة، انتقل إلى **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

2. في قسم **الشبكات المتاحة**، انقر فوق الزر **الإعدادات**.

3. في نافذة **جدار الحماية** التي تفتح، انتقل إلى علامة التبويب **شبكات الاتصال** لعرض قائمة الشبكات.

في القسم الفرعي **الحماية من تهديدات الملفات**، يمكنك تعطيل فحص محركات أقراص الشبكة. من الممكن يتسبب فحص محركات أقراص الشبكة إلى تطبيق حمل كبير على محركات أقراص الشبكة. إجراء فحص غير مباشر على خوادم الملفات هو السلوك الأكثر ملاءمة.

لتعطيل فحص محركات أقراص الشبكة:

1. في خصائص السياسة، انتقل إلى **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.

2. قي قسم **مستوى الأمان**، انقر فوق الزر **الإعدادات**.

3. في النافذة **الحماية من تهديدات الملفات** التي تفتح، في علامة التبويب **عام** امسح خانة الاختيار **كل محركات أقراص الشبكة**.

تكوين السياسة في قسم الإعدادات العامة

للحصول على وصف كامل للإعدادات الموجودة في هذا القسم، فبرجاء الرجوع إلى وثائق Kaspersky Endpoint Security for Windows.

في قسم **General settings** في نافذة خصائص السياسة، نوصي بتحديد إعدادات إضافية في القسمين للفرعيين **التقارير والمخزن** و**الواجهة**.

في القسم الفرعي **التقارير والمخزن**، انتقل إلى قسم **Data transfer to Administration Server**. تحدد خانة الاختيار **About started applications** ما إذا كانت قاعدة بيانات خادم الإدارة تحفظ معلومات حول جميع إصدارات كل وحدات البرامج على الأجهزة المتصلة بالشبكة. إذا تم تحديد خانة الاختيار هذه، قد تتطلب هذه المعلومات المحفوظة مساحة كبيرة من مساحة القرص في قاعدة بيانات Kaspersky Security Center (عشرات الجيجا بايت). امسح خانة الاختيار **About started applications** إذا كانت محددة في سياسة المستوى الأعلى.

إذا كانت وحدة تحكم الإدارة تدير الحماية من التهديد على شبكة المؤسسة في الوضع المركزي، فقم بتعطيل عرض واجهة مستخدم Kaspersky Endpoint Security for Windows على محطات العمل. لفعل ذلك، في القسم الفرعي **الواجهة**، انتقل إلى قسم **Interaction with user**، ثم حدد الخيار **Do not display user interface**.

لتمكين الحماية بكلمة مرور على محطات العمل، في القسم الفرعي **الواجهة**، انتقل إلى قسم **الحماية بكلمة مرور**، وانقر فوق الزر **الإعدادات**، ثم حدد خانة الاختيار **تمكين الحماية بكلمة مرور**.

تكوين السياسة في القسم تكوين الحدث

في القسم **تكوين الحدث**، ينبغي عليك تعطيل حفظ أي أحداث على خادم الإدارة ماعدا الأحداث التالية:

- في علامة التبويب **حرج**:
  - تم تعطيل التشغيل التلقائي للتطبيق
  - تم رفض الوصول
  - تم حظر بدء تشغيل التطبيق
  - يتعذر التنظيف

- تم انتهاك اتفاقية ترخيص المستخدم النهائي
- تعذر تحميل وحدة التشفير النمطية
- تعذر بدء مهمتين في نفس الوقت
- تم اكتشاف تهديد نشط. يجب بدء التنظيف المتقدم
- تم اكتشاف هجوم عبر الشبكة
- لم يتم تحديث كافة المكونات
- خطأ في التفعيل
- خطأ في تمكين الوضع المحمول
- حدث خطأ في التفاعل مع Kaspersky Security Center
- خطأ في تعطيل الوضع المحمول
- حدث خطأ في تغيير مكونات التطبيق
- خطأ في تطبيق قواعد تشفير / فك تشفير الملفات
- لا يمكن تطبيق السياسة
- تم إنهاء العملية
- تم منع نشاط الشبكة

- في علامة التبويب **خلل وظيفي**: إعدادات غير صالحة للمهمة. لم يتم تطبيق الإعدادات
- في علامة التبويب **تحذير**:
  - تم تعطيل الدفاع الذاتي
  - المفتاح الاحتياطي غير صحيح
  - انسحب المستخدم من سياسة التشفير
- في علامة التبويب **معلومات**: تم حظر بدء تشغيل التطبيق في وضع الاختبار

الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security

إن خيار الجدولة الأمثل والموصى به لإصدار Kaspersky Endpoint Security versions 10 والإصدارات الأحدث هو **عند تنزيل تحديثات جديدة إلى المستودع** عندما تكون خانة الاختيار **استخدم التأخير العشوائي لبدء المهام تلقائيًا** محددة.

الإعداد اليدوي للمهمة الجماعية لفحص جهاز باستخدام Kaspersky Endpoint Security

ينشئ معالج البدء السريع مهمة جماعية لفحص جهاز. بشكل افتراضي، يتم تعيين الجدول **تشغيل في أيام الجمعة الساعة 00:7 م** للمهمة بعشوائية تلقائية، مع إلغاء تحديد خانة الاختيار **تشغيل المهام الفائتة**.

وهذا يعني أنه في حالة إيقاف تشغيل الأجهزة الموجودة في مؤسسة ما في أيام الجمعة على سبيل المثال في 30:6 م، فلن يتم تشغيل مهمة فحص الجهاز أبدًا. يجب عليك إعداد الجدول الأكثر ملاءمةً لهذه المهمة بناءً على قواعد مكان العمل التي تتبناها المؤسسة.

جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة

ينشئ معالج البدء السريع مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة لعميل الشبكة. بشكل افتراضي، يتم تعيين الجدول **تشغيل في أيام الثلاثاء الساعة 00:7 م** للمهمة بعشوائية تلقائية، مع تحديد خانة الاختيار **تشغيل المهام الفائتة**.

إذا كانت قواعد مكان العمل الخاصة بالمؤسسة تعمل على إيقاف تشغيل جميع الأجهزة في هذا الوقت، سيتم تشغيل مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة بعد تشغيل الأجهزة مرة أخرى، وسيكون هذا في صباح يوم الأربعاء. قد يكون مثل هذا النشاط غير مرغوب فيه لأن عملية فحص الثغرات لأمنية قد تزيد من الحمل على وحدات المعالجة المركزية والأنظمة الفرعية للقرص. يجب عليك إعداد الجدول الأكثر ملاءمةً للمهمة بناءً على قواعد مكان العمل التي تتبناها المؤسسة.

الإعداد اليدوي للمهمة الجماعية لتثبيت التحديثات وإصلاح الثغرات الأمنية

ينشئ معالج البدء السريع مهمة جماعية لتثبيت التحديثات وإصلاح الثغرات الأمنية لعميل الشبكة. بشكل افتراضي، يتم إعداد المهمة للتشغيل كل يوم الساعة 00:01 ص، بعشوائية تلقائية، مع إلغاء تمكين خيار **تشغيل المهام الفائتة**.

إذا كانت قواعد مكان العمل الخاصة بالمؤسسة تعمل على إيقاف تشغيل الأجهزة أثناء الليل، فلن يتم تشغيل تثبيت التحديثات أبدًا. يجب عليك إعداد الجدول الأكثر ملاءمةً لمهمة فحص الثغرات الأمنية بناءً على قواعد مكان العمل التي تتبناها المؤسسة. من المهم أيضًا أن تضع في اعتبارك أن تثبيت التحديثات قد يتطلب إعادة تشغيل الجهاز.

تعيين الحد الأقصى لعدد الأحداث في مستودع الأحداث

من القسم **مستودع الأحداث** في النافذة خصائص خادم الإدارة، يمكنك تحرير إعدادات تخزين الأحداث في قاعدة بيانات خادم الإدارة من خلال تقييد عدد سجلات الأحداث أو مدة تخزين السجل. عندما تحدد الحد الأقصى لعدد الأحداث، يقوم التطبيق بحساب مقدار تقريبي لمساحة التخزين المطلوبة للرقم المحدد. يمكنك استخدام هذا الحساب التقريبي لتقييم ما إذا كانت لديك مساحة خالية كافية على القرص لتجنب تجاوز سعة قاعدة البيانات. السعة الافتراضية لقاعدة بيانات خادم الإدارة هي 400 000 حدث. أقصى سعة موصى بها لقاعدة البيانات هي 45 مليون حدث.

يتحقق التطبيق من قاعدة البيانات كل 10 دقائق. وإذا وصل عدد الأحداث إلى القيمة القصوى المحددة بالإضافة إلى 10 000، فسوف يحذف التطبيق الأحداث الأقدم بحيث يبقى الحد الأقصى لعدد الأحداث المحدد فقط.

عند قيام خادم الإدارة بحذف الأحداث القديمة، فلا يمكن حفظ الأحداث الجديدة في قاعدة البيانات. وأثناء هذه الفترة الزمنية، تتم كتابة معلومات حول الأحداث المرفوضة في سجل أحداث Kaspersky. يتم وضع الأحداث الجديدة في قائمة الانتظار ثم حفظها في قاعدة البيانات بعد اكتمال عملية الحذف.

لتقييد عدد الأحداث التي يمكن تخزينها في مستودع الأحداث بخادم الإدارة:

1. وانقر بزر الماوس الأيمن فوق خادم الإدارة، ثم حدد **الخصائص**.

   تفتح نافذة خصائص خادم الإدارة.

2. في مساحة عمل القسم **مستودع الأحداث**، حدد الحد الأقصى لعدد الأحداث المخزّنة في قاعدة البيانات.

3. انقر على**موافق**.

بالإضافة إلى ذلك، يمكنك تغيير إعدادات أي مهمة لحفظ الأحداث المتعلقة بتقدم المهمة، أو حفظ نتائج تنفيذ المهمة فقط. عند فعل ذلك، ستقلل من عدد الأحداث الموجودة في قاعدة البيانات، وتزيد من سرعة تنفيذ السيناريوهات المرتبطة بتحليل جدول الأحداث في قاعدة البيانات وخفض خطر الكتابة فوق الأحداث الحرجة بواسطة عدد كبير من الأحداث.

تحديد فترة التخزين القصوى للمعلومات حول الثغرات الأمنية الثابتة

لتعيين الحد الأقصى لفترة التخزين في قاعدة البيانات للحصول على معلومات حول الثغرات الأمنية التي تم إصلاحها بالفعل على الأجهزة المُدارة:

1. وانقر بزر الماوس الأيمن فوق خادم الإدارة، ثم حدد **الخصائص**.

   تفتح نافذة خصائص خادم الإدارة.

2. في مساحة عمل قسم **مستودع الأحداث** حدد فترة التخزين القصوى للمعلومات حول الثغرات الأمنية الثابتة في قاعدة البيانات.

   فترة التخزين الافتراضية هي 90 يومًا.

3. انقر على**موافق**.

فترة التخزين القصوى للمعلومات حول الثغرات الأمنية التي تم إصلاحها محدودة بعدد الأيام المحدد. بعد ذلك، ستحذف مهمة صيانة خادم الإدارة المعلومات القديمة من قاعدة البيانات.

إدارة المهام

يقوم Kaspersky Security Center بإدارة التطبيقات المثبتة على الأجهزة عن طريق إنشاء العديد من المهام وتشغيلها. يلزم وجود المهام من أجل تثبيت التطبيقات، وبدء تشغيلها، وإيقافها، وفحص الملفات، وتحديث قواعد البيانات والوحدات النمطية للبرامج، واتخاذ إجراءات أخرى بشأن التطبيقات.

وتُقسّم المهام تقسيمًا فرعيًا إلى الأنواع التالية:

- مهام المجموعة. وهي المهام التي تتم على الأجهزة في مجموعة الإدارة المحددة.
- مهام خادم الإدارة. وهي المهام التي تتم على خادم الإدارة.
- مهام الأجهزة الخاصة. وهي المهام التي تتم على أجهزة محددة بصرف النظر عما إذا كانت مضمنة في أية مجموعة إدارة أم لا.
- المهام المحلية. وهي المهام التي تتم على جهاز محدد.

لا يمكن إنشاء مهمة تطبيق إلا إذا كانت الأداة الإضافية للإدارة الخاصة بذلك التطبيق مثبتة على محطة عمل المسؤول.

يمكنك تجميع قائمة بالأجهزة (حتى 1000 جهاز) التي سيتم إنشاء مهمة لها بإحدى الطرق التالية:

- بتحديد الأجهزة المتصلة بالشبكة التي تم اكتشافها بواسطة خادم الإدارة.
- بتحديد قائمة بالأجهزة يدويًا. يمكنك استخدام عنوان IP (أو نطاق IP)، أو اسم NetBIOS أو اسم DNS كعنوان الجهاز.
- قم باستيراد قائمة بالأجهزة من ملف .txt يحتوي على عناوين الأجهزة التي يجب إضافتها (يجب وضع كل عنوان في سطر منفرد).

  إذا قمت باستيراد قائمة بالأجهزة من ملف أو قمت بإنشاء قائمة يدويًا وتم تحديد الأجهزة بأسمائها، فيمكن فقط أن تحتوي القائمة على الأجهزة التي تم إدخال معلوماتها في قاعدة بيانات خادم الإدارة عند اتصال تلك الأجهزة أو أثناء اكتشاف الأجهزة.

ويمكنك إنشاء أي عدد من مهام المجموعة أو مهام الأجهزة الخاصة أو المهام المحلية، وذلك لكل تطبيق.

يتم تنفيذ تبادل المعلومات المتعلقة بالمهمة بين التطبيق المُثبت على جهاز وبين قاعدة بيانات Kaspersky Security Center عندما يتم توصيل عميل الشبكة بخادم الإدارة.

ويمكنك إجراء تغييرات على إعدادات المهام، وعرض مستوى تقدمها، ونسخها، وتصديرها، واستيرادها، وحذفها.

ولا يتم بدء تشغيل المهام على جهاز إلا إذا كان التطبيق الذي تم إنشاء المهمة له قيد التشغيل. وعندما لا يكون التطبيق قيد التشغيل، يتم إلغاء جميع المهام المُشغلة.

يتم حفظ نتائج المهام المكتملة في سجلات مهام Microsoft Windows و Kaspersky Security Center، بشكل مركزي لكل منهما على خادم الإدارة ومحليًا على كل جهاز.

لا تقم بتضمين بيانات خاصة في إعدادات المهمة. على سبيل المثال، تجنّب تخصيص كلمة مرور مسؤول المجال.

تفاصيل إدارة المهام للتطبيقات التي تتمتع بدعم التشغيل المتعدد

يتم تطبيق مهمة جماعية لتطبيق يتمتع بدعم التشغيل المتعدد بناءً على التسلسل الهرمي لخوادم الإدارة والأجهزة العميلة. يجب أن يكون خادم الإدارة الافتراضي الذي تم إنشاء المهمة منه في نفس مجموعة الإدارة أو في مستوي أقل من الجهاز العميل الذي تم تثبيت التطبيق عليه.

في الأحداث التي تتناسب مع نتائج تنفيذ المهمة، يقوم مسؤول موفر الخدمة بعرض المعلومات حول الجهاز الذي تم تنفيذ المهمة عليه. وعلى عكس ذلك، تظهر إدارة المستأجر **عقدة المؤسسات المتعددة**.

إنشاء مهمة

في وحدة تحكم الإدارة، يمكنك إنشاء المهام مباشرة في المجلد الخاص بمجموعة الإدارة التي سيتم إنشاء مهمة جماعية لها، أو في مساحة عمل مجلد **المهام**.

لإنشاء مهمة جماعية في المجلد خاص بمجموعة إدارة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي تريد إنشاء مهمة لها.
2. في مساحة عمل المجموعة، حدد علامة التبويب **المهام**.
3. قم بتشغيل إنشاء المهمة بالنقر فوق الزر **إنشاء مهمة**.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

لإنشاء مهمة في مساحة عمل المجلد **المهام**:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. قم بتشغيل إنشاء المهمة بالنقر فوق الزر **إنهاء**.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

لا تقم بتضمين بيانات خاصة في إعدادات المهمة. على سبيل المثال، تجنّب تخصيص كلمة مرور مسؤول المجال.

إنشاء مهمة خادم الإدارة

يقوم خادم الإدارة بالمهام التالية:

- تسليم التقارير
- تنزيل التحديثات إلى مستودع خادم الإدارة
- النسخ الاحتياطي لبيانات خادم الإدارة
- صيانة خادم الإدارة
- مزامنة Windows Update
- إنشاء حزمة التثبيت على مرجع صورة نظام التشغيل للجهاز
- تثبيت التطبيق عن بُعد
- إلغاء تثبيت التطبيق عن بُعد
- توزيع حزم التثبيت
- تثبيت التطبيق على خوادم الإدارة الثانوية عن بُعد

على خادم الإدارة الافتراضي، تتوفر فقط مهمة تسليم التقارير التلقائية ومهمة إنشاء حزمة التثبيت بناءً على صورة نظام التشغيل للجهاز المرجعي. مستودع خادم الإدارة الافتراضي يعرض التحديثات المنزّلة على خادم الإدارة الرئيسي. يتم إجراء النسخ الاحتياطي لبيانات الخادم الافتراضي بجانب النسخ الاحتياطي لبيانات خادم الإدارة الرئيسي.

لإنشاء مهمة خادم الإدارة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. بدء إنشاء المهمة بإحدى الطرق التالية:

- عن طريق تحديد **جديد** ← **مهمة** في قائمة سياق المجلد **المهام** في شجرة وحدة التحكم.
- بالنقر فوق الزر **إنشاء مهمة** في مساحة عمل المجلد **المهام**.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

يمكن إنشاء مهام تنزيل التحديثات إلى مستودع خادم الإدارة، وإجراء مزامنة Windows Update، وصيانة خادم الإدارة، والنسخ الاحتياطي لبيانات خادم الإدارة مرة واحدة فقط. إذا تم إنشاء مهام تنزيل التحديثات إلى مستودع خادم الإدارة، وصيانة خادم الإدارة، والنسخ الاحتياطي لبيانات خادم الإدارة، وتنفيذ مهام مزامنة Windows Update بالفعل لخادم الإدارة، فلن يتم عرضها في نافذة تحديد نوع المهمة لمعالج المهمة الجديدة.

إنشاء مهمة لأجهزة محددة

في Kaspersky Security Center، يمكنك إنشاء مهام لأجهزة خاصة. الأجهزة الموجودة في مجموعة يمكن أن تكون مضمنة في مجموعات إدارة متعددة أو البقاء خارج أي مجموعة إدارة. ويمكن لتطبيق Kaspersky Security Center القيام بالمهام الرئيسية التالية لأجهزة خاصة:

- تثبيت تطبيق عن بُعد
- إرسال رسالة إلى المستخدم
- تغيير خادم الإدارة
- إدارة الأجهزة
- التحقق من التحديثات
- توزيع حزم التثبيت
- تثبيت التطبيق على خوادم الإدارة الثانوية عن بُعد
- إلغاء تثبيت تطبيق عن بُعد

لإنشاء مهمة لأجهزة خاصة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. بدء إنشاء المهمة بإحدى الطرق التالية:

- عن طريق تحديد **جديد** ← **مهمة** في قائمة سياق مجلد **المهام** في شجرة وحدة التحكم.
- بالنقر فوق الزر **إنشاء مهمة** في مساحة عمل المجلد **المهام**.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

إنشاء مهمة محلية

لإنشاء مهمة محلية لأحد الأجهزة:

1. حدد علامة التبويب **الأجهزة** في مساحة عمل المجموعة التي تتضمن الجهاز.
2. من قائمة الأجهزة الموجودة بعلامة التبويب **الأجهزة**، حدد الجهاز الذي يجب إنشاء المهمة المحلية له.
3. ابدأ في إنشاء المهمة للجهاز المحدد بإحدى الطرق التالية:
   - انقر فوق الزر **تنفيذ الإجراء** وحدد **إنشاء مهمة** في القائمة المنسدلة.
   - انقر فوق الرابط **إنشاء مهمة** في مساحة عمل الجهاز.
   - استخدم خصائص الجهاز على النحو التالي:
     a. في قائمة السياق الخاصة بالجهاز، حدد **خصائص**.
     b. في نافذة خصائص الجهاز التي تفتح، حدد القسم **المهام** وانقر فوق **إضافة**.

   سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

تتوفر إرشادات تفصيلية حول كيفية إنشاء وتكوين المهام المحلية في أدلة تطبيقات Kaspersky المعنية.

عرض مهمة جماعية موروثة في مساحة عمل لمجموعة متداخلة

لتمكين عرض المهام الموروثة لمجموعة متداخلة في مساحة العمل:

1. حدد علامة التبويب **المهام** في مساحة عمل المجموعة المتداخلة.
2. في مساحة عمل علامة التبويب **المهام**، انقر فوق الزر **إظهار المهام الموروثة**.

   يتم عرض المهام الموروثة في قائمة المهام متضمنةً أحد الموز التالية:

- —إذا كانت موروثة من مجموعة تم إنشاؤها على خادم إدارة أساسي.
- —إذا كانت موروثة من مجموعة مستوى أعلى.

في حالة تمكين وضع التوريث، لا يمكن تحرير المهام الموروثة إلا في المجموعة التي تم إنشاء تلك المهام فيها. ولا يمكن تحرير المهام الموروثة في المجموعة التي ترث المهام.

تشغيل الأجهزة تلقائيًا قبل بدء المهمة

لا يشغل Kaspersky Security Center المهام على الأجهزة التي تم إيقاف تشغيلها. يمكنك تكوين Kaspersky Security Center لتشغيل هذه الأجهزة تلقائيًا قبل بدء مهمة باستخدام وظيفة Wake-on-LAN.

لتكوين بدء التشغيل التلقائي للأجهزة قبل بدء المهمة:

1. في نافذة خصائص المهمة، حدد القسم **الجدول**.

2. لتكوين الإجراءات على الأجهزة ، انقر فوق الارتباط **خيارات متقدمة**.

3. في نافذة **خيارات متقدمة** التي يتم فتحها، حدد خانة **قم بتشغيل الأجهزة باستخدام وظيفة Wake-on-LAN قبل بدء المهمة (دقيقة)**، ثم حدد الفاصل الزمني بالدقائق.

نتيجة لذلك، وفقًا لعدد الدقائق المحدد قبل بدء المهمة، يقوم Kaspersky Security Center بتشغيل الأجهزة وتحميل نظام التشغيل عليها باستخدام وظيفة Wake-on-LAN. بعد اكتمال المهمة، يتم إيقاف تشغيل الأجهزة تلقائيًا إذا لم يقم مستخدمي الجهاز بتسجيل الدخول إلى النظام. لاحظ أن Kaspersky Security Center يقوم تلقائيًا بإيقاف تشغيل الأجهزة التي تم تشغيلها فقط باستخدام وظيفة Wake-on-LAN.

يمكن لـ Kaspersky Security Center بدء تشغيل أنظمة التشغيل تلقائيًا فقط على الأجهزة التي تدعم معيار Wake-on-LAN (WoL).

إيقاف تشغيل جهاز تلقائيًا بعد اكتمال مهمة

يتيح لك Kaspersky Security Center مهمة بطريقة يتم إيقاف تشغيل الأجهزة التي يتم توزيعها عليها تلقائيًا بعد اكتمال المهمة.

لإيقاف تشغيل جهاز تلقائيًا بعد اكتمال مهمة:

1. في نافذة خصائص المهمة، حدد القسم **الجدول**.

2. انقر فوق الرابط **خيارات متقدمة** لفتح نافذة تكوين الإجراءات على الأجهزة.

3. في النافذة **خيارات متقدمة** التي تفتح، حدد خانة الاختيار **أغلق الأجهزة بعد الانتهاء من المهمة**.

تحديد وقت تشغيل المهمة

لتقييد الوقت المستغرق خلال تشغيل مهمة على الأجهزة:

1. في نافذة خصائص المهمة، حدد القسم **الجدول**.

2. افتح النافذة المخصصة لتكوين الإجراءات على الأجهزة العميلة بالنقر فوق **خيارات متقدمة**.

3. في نافذة **خيارات متقدمة** التي يتم فتحها، حدد **أوقف المهمة إذا كانت أطول من (دقيقة)** وحدد الفاصل الزمني بالدقائق.

إذا لم تكتمل المهمة على الجهاز عند انتهاء الفاصل الزمني المحدد، فسيوقف Kaspersky Security Center تشغيل المهمة تلقائيًا.

تصدير مهمة

يمكنك تصدير مهام مجموعة أو مهام لأجهزة خاصة إلى ملف. لا يتوفر تصدير مهام خادم الإدارة.

لتصدير مهمة:

1. من قائمة سياق المهمة، حدد **جميع& المهام** ← **تصدير**.

2. في النافذة **حفظ باسم** التي تفتح، حدد مسار اسم الملف.

3. انقر على زر **حفظ**.

لا يتم تصدير حقوق المستخدمين المحليين.

استيراد مهمة

يمكنك استيراد مهام مجموعة ومهام لأجهزة خاصة. لا يتوفر استيراد مهام خادم الإدارة.

لاستيراد مهمة:

1. حدد القائمة التي يجب استيراد المهمة لها:

- إذا كنت تريد استيراد المهمة إلى قائمة مهام مجموعة في مساحة عمل مجموعة الإدارة ذات الصلة، حدد علامة التبويب **المهام**.
- إذا كنت تريد استيراد مهمة في قائمة المهام لأجهزة خاصة، فحدد المجلد **المهام** من شجرة وحدة التحكم.

2. حدد أحد الخيارات التالية لاستيراد المهمة:

- من قائمة السياق الخاصة بقائمة المهام، حدد **جميع& المهام** > **استيراد**.
- انقر فوق الرابط **استيراد مهمة من ملف** في كتلة إدارة قائمة المهام.

3. في النافذة التي تفتح، حدد المسار إلى الملف الذي تريد استيراد المهمة منه.

4. انقر فوق الزر **فتح**.

يتم عرض المهمة في قائمة المهام.

إذا كانت المهمة المستوردة حديثًا لها اسم مماثل لمهمة موجودة، فسيتم توسيع اسم المهمة المستوردة بامتداد **(<next sequence number>)** الفهرس، على سبيل المثال: **(1)** و **(2)**.

تحويل المهام

يمكنك استخدام Kaspersky Security Center لتحويل المهام من الإصدارات الأقدم لتطبيقات Kaspersky إلى تلك الإصدارات الأحدث للتطبيقات.

يتوفر التحويل لمهام التطبيقات التالية:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows.
- Kaspersky Endpoint Security 10 for Windows.

لتحويل المهام:

1. من شجرة وحدة التحكم قم بتحديد خادم الإدارة الذي تريد أن تقوم بتحويل المهام إليه.

2. في القائمة سياق خادم الإدارة، حدد **جميع المهام** ← **معالج تحويل تصحيح المهام والسياسات**.

يبدأ معالج تحويل تصحيح المهام والسياسات. اتبع إرشادات المعالج.

بعد أن ينهي المعالج عملياته، يتم إنشاء مهام جديدة تستخدم إعدادات المهام من إصدارات أقدم من التطبيقات.

بدء تشغيل مهمة وإيقافها يدويًا

يمكنك بدء وإيقاف المهام يدويًا باستخدام أي من الطريقتين التاليتين: من خلال قائمة السياق للمهمة أو من خلال نافذة خصائص الجهاز العميل الذي تم تعيين المهمة إليه.

يسمح فقط ببدء مهمة جماعية من قائمة سياق الجهاز للمستخدمين المضمنين في مجموعة KLAdmins.

لبدء أو إيقاف مهمة من قائمة السياق أو من نافذة خصائص المهمة:

1. في قائمة المهام، حدد مهمة.

2. بدء تشغيل المهمة أو إيقافها بإحدى الطرق التالية:

- بتحديد **بدء** أو **إيقاف** من قائمة سياق المهمة.
- من خلال النقر فوق **بدء** أو **إيقاف** في القسم **عام** بنافذة خصائص المهمة.

لبدء أو إيقاف مهمة من قائمة السياق أو من نافذة خصائص الجهاز العميل:

1. في قائمة الأجهزة، حدد الجهاز.

2. بدء تشغيل المهمة أو إيقافها بإحدى الطرق التالية:

- بتحديد **جميع& المهام** ← **تشغيل مهمة** في قائمة السياق الخاصة بالجهاز. حدد المهمة ذات الصلة من قائمة المهام.
  سيتم استبدال قائمة الأجهزة التي تم تعيين المهمة إليها بالجهاز الذي قمت بتحديده. تبدأ المهمة.
- من خلال النقر فوق الزر بدء ( ) أو الزر إيقاف ( ) في القسم **المهام** في نافذة خصائص الجهاز.

إيقاف المهمة مؤقتًا واستئنافها يدويًا

لإيقاف مهمة جاري تنفيذها مؤقتًا أو استئنافها يدويًا:

1. في قائمة المهام، حدد مهمة.
2. إيقاف المهمة مؤقتًا أو استئنافها بإحدى الطرق التالية:
   - بتحديد **إيقاف مؤقت** أو **استئناف**من قائمة سياق المهمة.
   - بتحديد القسم **عام** في نافذة خصائص المهام والنقر فوق **إيقاف مؤقت** أو **استئناف**.

مراقبة تنفيذ المهمة

لمراقبة تنفيذ المهمة،

في نافذة خصائص المهمة، حدد قسم **عام**.

في الجزء الأوسط للقسم **عام**، يتم عرض الحالة الحالية للمهمة.

عرض نتائج تشغيل المهمة المخزنة على خادم الإدارة

يتيح لك Kaspersky Security Center عرض نتائج المهام الجماعية ومهام الأجهزة المحددة ومهام خادم الإدارة.

لعرض نتائج المهام:

1. في نافذة خصائص المهمة، حدد قسم **عام**.
2. انقر فوق الرابط **النتائج** لفتح النافذة **Task results**.

لعرض نتائج المهام لخادم إدارة ثانوي:

1. في نافذة خصائص المهمة، حدد قسم **عام**.
2. انقر فوق الرابط **النتائج** لفتح النافذة **Task results**.
3. انقر فوق **Statistics from secondary Servers**.
4. حدد الخادم الثانوي الذي تريد عرض نافذة **Task results** الخاصة به.

تكوين تصفية المعلومات بشأن نتائج تشغيل المهمة

يتيح لك Kaspersky Security Center تصفية المعلومات بشأن نتائج المهام الجماعية، ومهام الأجهزة المحددة ومهام خادم الإدارة. لا تتوفر تصفية للمهام المحلية.

لإعداد تصفية معلومات بشأن نتائج تشغيل المهمة:

1. في نافذة خصائص المهمة، حدد قسم **عام**.

2. انقر فوق الرابط **النتائج** لفتح النافذة **نتائج المهمة**.

يحتوي الجدول الموجود في الجزء العلوي على قائمة بكل الأجهزة التي تم إسناد المهمة من أجلها. يعرض الجدول الموجود في الجزء السفلي نتائج المهمة التي تم تنفيذها على الجهاز المحدد.

3. انقر بزر الماوس الأيمن فوق الجدول ذي الصلة لفتح قائمة السياق وحدد **عامل التصفية**.

4. في النافذة **تعيين عامل تصفية** التي تفتح، حدد إعدادات عامل التصفية في أقسام **الأحداث**، و**الأجهزة**، و**الوقت**. انقر على**موافق**.

تعرض النافذة **نتائج المهمة** المعلومات التي تفي بالإعدادات المحددة في عامل التصفية.

تعديل مهمة. التراجع عن التغييرات

لتعديل مهمة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. في مساحة عمل المجلد **المهام**، حدد مهمة ثم تابع إلى النافذة خصائص المهمة باستخدام قائمة السياق.

3. قم بعمل التغييرات اللازمة.

في القسم **الاستثناءات من نطاق المهمة**، يمكنك إعداد قائمة بالمجموعات الفرعية التي لا يتم تطبيق المهمة عليها.

4. انقر على **تطبيق** .

سيتم حفظ التغييرات التي تم إجراؤها على المهمة في نافذة خصائص المهمة، في القسم **سجل المراجعة**.

وإذا لزم الأمر، يمكنك التراجع عن التغييرات التي تم إجراؤها على المهمة.

للتراجع عن التغييرات التي تم إجراؤها على المهمة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. حدد المهمة التي يجب التراجع عن التغييرات التي تم إجراؤها فيها، ثم تابع إلى نافذة خصائص المهمة باستخدام قائمة السياق.

3. في النافذة خصائص المهمة، حدد قسم **سجل المراجعة**.

4. في قائمة مراجعات المهمة، حدد رقم المراجعة التي تريد التراجع عن التغييرات لها.

5. انقر فوق الزر **خيارات متقدمة** وحدد القيمة **التراجع** في القائمة المنسدلة.

مقارنة المهام

يمكنك المقارنة بين مهام من النوع نفسه: على سبيل المثال، يمكنك المقارنة بين مهمتين لفحص البرامج الضارة، لكن لا يمكنك مقارنة مهمة لفحص البرامج الضارة ومهمة تثبيت تحديث. بعد إجراء المقارنة، ستحصل على تقرير يعرض الإعدادات المتطابقة والمختلفة في المهمتين. يمكنك طباعة تقرير مقارنة المهام أو حفظه في صورة ملف. قد تحتاج إلى مقارنة المهام عند تعيين مهام متعددة من نفس النوع إلى وحدات مختلفة في الشركة. على سبيل المثال، يتولى موظفو قسم الحسابات تنفيذ مهمة فحص البرامج الضارة على الأقراص المحلية لأجهزتهم فقط، ونظرًا لأن موظفو قسم المبيعات يتواصلون مع العملاء فإنهم يتولون مهمة فحص الأقراص المحلية والبريد الإلكتروني. ليس عليك عرض جميع إعدادات المهام لملاحظة هذا الاختلاف بسرعة، ويمكنك بكل بساطة مقارنة المهام بدلاً من ذلك.

يمكن فقط مقارنة مهام من نفس النوع.

يمكن مقارنة المهام بصورة مزدوجة فقط.

يمكنك مقارنة المهام بإحدى الطرق التالية: عن طريق تحديد مهمة ومقارنتها بمهمة أخرى، أو عن طريق المقارنة بين أي مهمتين من قائمة المهام.

لتحديد مهمة ومقارنتها بمهمة أخرى:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. في مساحة عمل المجلد **المهام**، حدد المهمة التي تريد مقارنتها بمهمة أخرى.
3. من قائمة سياق المهمة، حدد **جميع& المهام** ← **مقارنة بمهمة أخرى**.
4. في النافذة **تحديد مهمة**، حدد المهمة للمقارنة.
5. انقر على**موافق**.

يتم عرض تقرير بتنسيق HTML يقارن بين المهمتين.

للمقارنة بين أي مهمتين من قائمة المهام:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. في مجلد **المهام**، في قائمة المهام، اضغط على مفتاح **Shift** أو مفتاح **Ctrl** لتحديد مهمتين من نفس النوع.
3. في قائمة السياق، حدد **مقارنة**.

يتم عرض تقرير بتنسيق HTML يقارن بين المهام المحددة.

عند مقارنة المهام، إذا كانت كلمات المرور مختلفة، ستظهر علامات النجمة (******) في تقرير مقارنة المهمة.

إذا تم تغيير كلمة المرور في خصائص المهمة، ستظهر علامات النجمة (******) في تقرير مقارنة المراجعات (******).

الحسابات التي ستقوم ببدء المهام

يمكنك تحديد الحساب الذي سيتم تشغيل المهمة من خلاله.

على سبيل المثال، لتنفيذ مهمة فحص عند الطلب، تحتاج إلى امتلاك حقوق الوصول إلى الكائن الذي سيتم فحصه، وليتم تنفيذ مهمة التحديث، يجب أن تمتلك حقوق مستخدم الخادم الوكيل المرخص. تتيح لك القدرة على تحديد حساب لتشغيل المهمة تجنب المشاكل المرتبطة بمهام الفحص عند الطلب ومهام التحديث في حالة أن المستخدم يقوم بتشغيل مهمة لا تمتلك حقوق الوصول المطلوبة.

يتم استخدام الحساب المحدد أثناء تنفيذ مهام التثبيت/إزالة التثبيت عن بُعد لتنزيل الملفات المطلوبة إلى الأجهزة العميلة لتثبيت / إلغاء تثبيت أحد التطبيقات في حالة عدم تثبيت عميل الشبكة أو عدم توفره. إذا تم تثبيت عميل الشبكة وتوفره، فسيتم استخدام الحساب وفقًا لإعدادات المهام وسيتم إجراء تسليم الملفات باستخدام أدوات المساعدة لـ Microsoft Windows من المجلد المشترك فقط. في هذه الحالة، يجب أن يكون للحساب الحقوق التالية على الجهاز:

- حق بدء تشغيل التطبيقات عن بُعد.
- حق استخدام مورد Admin$.
- حق تسجيل الدخول كخدمة.

إذا تم تسليم الملفات إلى الأجهزة بواسطة عميل الشبكة، فلن يتم استخدام الحساب. وسيتم إجراء جميع عمليات النسخ والتثبيت للملف بعد ذلك بواسطة **عميل الشبكة (حساب النظام المحلي)**.

تصدير سجل تنفيذ المهمة

إذا واجهت أي مشكلات مع إحدى المهام، فقد تحتاج إلى التحقق من الأسباب الكامنة وراء ذلك. ولفعل ذلك، يمكنك تصدير سجل تنفيذ المهمة وتحليله بشكل أكبر.

لتصدير سجل تنفيذ المهمة:

1. أنشئ ملف TXT فارغًا في دليل على جهازك.
   سيتم تصدير سجل تنفيذ المهمة إلى هذا الملف.
2. افتح نافذة نتائج المهمة.
3. في الجزء العلوي من نافذة نتائج المهمة، حدد الجهاز الذي يواجه مشكلات.
4. في الجزء السفلي من نافذة نتائج المهمة، حيث يتم عرض سجل التنفيذ للجهاز المحدد، حدد حدثًا واحدًا أو أكثر.
   لتحديد عدة أحداث، استخدم مفتاح **Shift** أو **Ctrl**.
5. انقر بزر الماوس الأيمن فوق الحدث (الأحداث) المحدد(ة) لفتح قائمة السياق وحدد **تصدير**.
   يبدأ معالج تصدير الأحداث.
6. في خطوة **تصدير ملف** في المعالج، انقر فوق الزر **استعراض**، ثم حدد ملف TXT الذي أنشأته لتصدير سجل تنفيذ المهمة.
   إذا كنت تريد تصدير الأحداث المحددة فقط، فقم بتمكين الخيار **تصدير الأحداث المحددة فقط**.
   إذا كنت تريد تصدير سجل تنفيذ المهمة بالكامل (كل الأحداث)، فإن الخيار **تصدير الأحداث المحددة فقط** يجب تعطيله.
7. انقر على الزر **Next**.
8. في خطوة **تنسيق التصدير** في المعالج، قم بتمكين أحد الخيارات التالية:

- **التصدير كنص Unicode محدد بعلامات جدولة**

قم بتمكين هذا الخيار إذا كانت البيانات التي يتم تصديرها تتضمن أحرفًا ورموزًا خاصة من عدة لغات وتحتاج إلى التأكد من الحفاظ على جميع الأحرف بدقة عند فتح ملف TXT الذي يحتوي على البيانات التي يتم تصديرها في تطبيقات مختلفة.

- **التصدير كنص محدد بعلامات جدولة**

قم بتمكين هذا الخيار إذا كنت تريد الحفاظ على التوافق مع الأنظمة أو التطبيقات القديمة التي قد لا تدعم Unicode.

9. انقر على زر **Next** لإنهاء المعالج.

يتم تصدير سجل تنفيذ المهمة إلى ملف TXT المحدد.

معالج تغيير كلمة مرور المهام

بالنسبة إلى مهمة غير محلية، يمكنك تحديد حساب الذي بموجبه يجب تشغيل المهمة. يمكنك تحديد الحساب أثناء إنشاء المهمة أو في خصائص مهمة موجودة. إذا تم استخدام الحساب المحدد وفقًا لتعليمات الأمان للمنظمة، قد تتطلب هذه التعليمات تغيير كلمة مرور الحساب من وقت لآخر. عند انتهاء صلاحية كلمة مرور الحساب وتعيينك لكلمة مرور جديدة، لن تبدأ المهام حتى تحدد كلمة المرور الجديدة الصالحة في خصائص المهمة.

يمكّنك "معالج تغيير كلمة مرور المهام" من استبدال كلمة المرور القديمة تلقائيًا بكلمة مرور جديدة في جميع المهام التي يتم فيها تحديد الحساب. بدلاً من ذلك، يمكنك القيام بذلك يدويًا في خصائص كل مهمة.

لبدء تشغيل معالج تغيير كلمة مرور المهام:

1. في شجرة وحدة التحكم، حدد جزء **المهام**.

2. في قائمة السياق الخاصة بالجزء، حدد **معالج تغيير كلمة مرور المهام**.

اتبع إرشادات المعالج.

الخطوة 1. تحديد بيانات الاعتماد

في حقول **الحساب** و**كلمة المرور**، حدد بيانات اعتماد جديدة صالحة حاليًا في نظامك (على سبيل المثال، في Active Directory). عندما تقوم بالتبديل إلى الخطوة التالية من المعالج، يتحقق Kaspersky Security Center ما إذا كان اسم الحساب المحدد مطابقًا لاسم الحساب في خصائص كل مهمة غير المحلية. في حالة تطابق أسماء الحساب، يتم استبدال كلمة المرور في خصائص المهمة تلقائيًا بكلمة المرور الجديدة.

إذا قمت بملء الحقل **كلمة المرور القديمة (اختياري)**، فإن Kaspersky Security Center يستبدل كلمة المرور فقط لتلك المهام التي يتم فيها العثور على كل من اسم الحساب وكلمة المرور القديمة. يتم إجراء الاستبدال تلقائيًا. في جميع الحالات الأخرى، ستحتاج إلى اختيار إجراء لاتخاذه في الخطوة التالية من المعالج.

الخطوة 2. اختيار إجراء لاتخاذه

إذا لم تحدد كلمة المرور القديمة في الخطوة الأولى من المعالج أو لم تتطابق كلمة المرور القديمة المحددة مع كلمات المرور في المهام، يجب عليك اختيار إجراء لاتخاذه للمهام التي تم العثور عليها.

لكل مهمة تتسم بحالة تتطلب العملية موافقة، حدد ما إذا كنت تريد إزالة كلمة المرور في خصائص المهمة أو استبدالها بكلمة المرور الجديدة. إذا اخترت إزالة كلمة المرور، يتم تبديل المهمة لتعمل بموجب الحساب الافتراضي.

الخطوة 3. عرض النتائج

في الخطوة الأخيرة من المعالج، قم بعرض النتائج لكل مهمة تم العثور عليها. لإكمال المعالج، انقر على زر **إنهاء**.

إنشاء تسلسل هرمي لمجموعات الإدارة التابعة لخادم إدارة افتراضي

بعد أن يتم إنشاء خادم الإدارة الافتراضي، سيحتوي بشكل افتراضي على مجموعة إدارة باسم **الأجهزة المدارة**.

يتطابق إجراء إنشاء تسلسل هرمي لمجموعات الإدارة التابعة لخادم الإدارة الافتراضي مع الإجراء الخاص بإنشاء تسلسل هرمي لمجموعات الإدارة التابعة لـ خادم الإدارة الفعلي.

لا يمكنك إضافة خوادم إدارة ثانوية وظاهرية إلى مجموعات الإدارة التابعة بخادم افتراضي. يرجع ذلك إلى القيود المفروضة على خوادم الإدارة الافتراضية.

السياسات وملفات تعريف السياسة

يمكنك في Kaspersky Security Center Web Console إنشاء سياسات لتطبيقات Kaspersky. يصف هذا القسم السياسات وملفات تعريف السياسة، كما يوفر تعليمات حول إنشائها وتعديلها.

التسلسل الهرمي للسياسات، واستخدام ملفات تعريف السياسة

يُقدم هذا القسم معلومات حول كيفية تطبيق السياسات على الأجهزة في مجموعات الإدارة. يوفر هذا القسم أيضًا معلومات حول ملفات تعريف السياسة.

التسلسل الهرمي للسياسات

في Kaspersky Security Center، أنت تستخدم سياسات لتحديد مجموعة فردية من الإعدادات لأجهزة متعددة. على سبيل المثال، نطاق السياسة للتطبيق P المحددة لمجموعة الإدارة G يتضمن أجهزة مدارة مثبت عليها التطبيق P الذي تم نشره في المجموعة G وكل مجموعاتها الفرعية، باستثناء المجموعات الفرعية التي تم إلغاء تحديد خانة الاختيار **توريث من المجموعة الأصلية** في خصائصها.

تتميز السياسة عن أي إعداد محلي بوجود رموز قفل (🔒) بجانب إعداداتها. في حالة قفل إعداد ما (أو مجموعة إعدادات) في خصائص السياسة، يجب عليك أولاً استخدام هذا الإعداد (أو مجموعة الإعدادات) عند إنشاء إعدادات فعالة، وثانيًا يجب كتابة الإعدادات أو مجموعة الإعدادات في سياسة انتقال البيانات من الخادم.

يمكن وصف إنشاء الإعدادات الفعالة على جهاز ما كما يلي: يتم الحصول على قيم كل الإعدادات التي لم يتم قفلها من السياسة، ثم يتم الكتابة عليها باستخدام قيم الإعدادات المحلية، ثم يتم الكتابة على المجموعة الناتجة باستخدام قيم الإعدادات التي تم قفلها والتي تم الحصول عليها من السياسة.

تؤثر السياسات الخاصة بالتطبيق نفسه على بعضها البعض عبر من خلال الترتيب الهرمي لمجموعات الإدارة: الإعدادات التي تم قفلها من سياسة انتقال البيانات إلى الخادم تقوم بالكتابة فوق الإعدادات نفسها من سياسة انتقال البيانات من الخادم.

توجد سياسة خاصة للمستخدمين خارج المكتب. تسري هذه السياسة على الجهاز عندما يتحول إلى وضع الوجود خارج المكتب. لا تؤثر سياسات خارج المكتب على السياسات الأخرى من خلال الترتيب الهرمي لمجموعات الإدارة.

ملفات تعريف السياسة

قد يكون تطبيق السياسات على الأجهزة من خلال الترتيب الهرمي لمجموعات الإدارة فقط غير ملائم في كثير من الحالات. قد يكون من الضروري إنشاء مثيلات متعددة لسياسة واحدة ما تختلف بإعداد واحد أو اثنين لمجموعات إدارة مختلفة، ومزامنة المحتويات الخاصة بهذه السياسات في المستقبل.

لمساعدتك في تجنب مثل هذه المشاكل، يدعم Kaspersky Security Center ملفات تعريف السياسة. ملف تعريف السياسة هو مجموعة فرعية مسمّاة لإعدادات السياسة. يتم توزيع هذه المجموعة الفرعية على الأجهزة المستهدفة بالإضافة إلى السياسة، وتلحقها في حالة خاصة تُسمى شرط تفعيل ملف التعريف. تحتوي ملفات التعريف فقط على الإعدادات التي تختلف عن السياسة "الأساسية" والتي تكون نشطة على الجهاز العميل (كمبيوتر أو جهاز محمول). يؤدي تنشيط ملف التعريف إلى تعديل إعدادات السياسة التي كانت نشطة على الجهاز قبل أن يتم تنشيط ملف التعريف. هذه الإعدادات تأخذ القيم التي تم تحديدها في ملف التعريف.

يتم فرض القيود التالية حاليًا على ملفات تعريف السياسة:

- يمكن أن تتضمن سياسة ما على 100 ملف تعريف بحد أقصى.
- لا يمكن أن يحتوي ملف تعريف سياسة على ملفات تعريف أخرى
- لا يمكن أن يحتوي ملف تعريف السياسة على إعدادات الإخطار.

محتويات ملف التعريف

يحتوي ملف تعريف السياسة على الأجزاء التأسيسية التالية:

- الاسم. تؤثر ملفات التعريف ذات الأسماء المتشابهة على بعضها البعض عبر الترتيب الهرمي لمجموعات الإدارة ذات القواعد المشتركة.
- مجموعة فرعية من إعدادات السياسة. على عكس السياسة، التي تحتوي على كل الإعدادات، يحتوي ملف التعريف على الإعدادات المطلوبة فعليًا فقط (الإعدادات المقفولة).
- شرط التعريف هو تعبير منطقي باستخدام خصائص الجهاز. يكون ملف التعريف نشطًا (يلحق بالسياسة) فقط عندما يتحقق شرط تنشيط ملف التعريف. في كل الحالات الأخرى، يكون ملف التعريف غير نشط ويتم تجاهله. يمكن تضمين خصائص الجهاز التالية في هذا التعبير المنطقي:
  - حالة وضع الوجود خارج المكتب.
  - خصائص بيئة الشبكة—اسم القاعدة المفعلة لـ اتصال عميل الشبكة.
  - وجود أو غياب علامات محددة على الجهاز
  - موقع الجهاز في وحدة Active Directory: بشكل صريح (يوجد الجهاز في الوحدة التنظيمية المحددة) أو ضمنيًا (يوجد الجهاز في وحدة تنظيمية ما، والذي يوجد ضمن الوحدة التنظيمية المحددة على أي مستوى من التداخل)
  - عضوية الجهاز في مجموعة أمن Active Directory (بشكل صريح أو ضمني)
  - عضوية مالك الجهاز في مجموعة أمن Active Directory (بشكل صريح أو ضمني)
- خانة اختيار تعطيل ملف التعريف. دائمًا ما يتم تجاهل ملفات التعريف المعطلة ولا يتم التحقق من شروط التنشيط الخاصة بها.
- أولوية ملف التعريف. شروط التنشيط الخاصة بملفات التعريف المختلفة مستقلة، وبذلك يمكن تنشيط العديد من ملفات التعريف في الوقت نفسه. إذا كانت ملفات التعريف المفعلة لا تحتوي على مجموعات إعدادات متداخلة، فلن تحدث أي مشكلة. ولكن، إذا كان ملفا تعريف نشطان يحتويان على قيم مختلفة للإعداد نفسه، فسيحدث التباس. يمكن تجنب هذا الالتباس عبر خصائص ملف التعريف: سيتم الحصول على قيمة المتغير الملتبسة من ملف التعريف الذي يملك الأولوية الأعلى (وهو الملف ذي التصنيف الأعلى في قائمة ملفات التعريف).

سلوك ملفات التعريف عندما تؤثر السياسات على بعضها البعض عبر الترتيب الهرمي

يتم دمج ملفات التعريف التي لها الاسم نفسه طبقًا لقواعد الدمج الخاصة بالسياسة. تملك ملفات التعريف الخاصة بسياسة نقل البيانات إلى الخادم أولوية أعلى من ملفات تعريف سياسة نقل البيانات من الخادم. في حالة حظر إعدادات التحرير في سياسة نقل البيانات إلى الخادم (تم قفلها)، تستخدم سياسة نقل البيانات من الخادم شروط تفعيل ملف التعريف من سياسة نقل البيانات إلى الخادم. في حالة السماح بإعدادات التحرير في سياسة نقل البيانات إلى الخادم، يتم استخدام شروط تنشيط ملف التعريف من سياسة نقل البيانات من الخادم.

حيث إن ملف تعريف السياسة قد يحتوي على الخاصية **الجهاز غير متصل** في شرط التنشيط الخاص به، فإن ملفات التعريف تستبدل تمامًا ميزة السياسات للمستخدمين خارج المكتب، والتي لن تعد مدعومة.

قد تحتوي سياسة خاصة بالمستخدمين خارج المكتب على ملفات تعريف، ولكن يمكن تنشيط ملفات تعريفها فقط بعدما يتحول الجهاز إلى وضع الوجود خارج المكتب.

توريث إعدادات السياسة

يتم تحديد سياسة مجموعة الإدارة. يمكن توريث إعدادات السياسة التي تم استلامها في المجموعات الفرعية (المجموعات التابعة) لمجموعة الإدارة التي تم تعيين الإعدادات من أجلها. فيما يلي، تتم الإشارة إلى سياسة المجموعة الأصلية أيضًا بالسياسة الأصلية.

يمكنك تمكين أو تعطيل خيارين من خيارات التوريث وهما: **توريث الإعدادات في السياسة الأصلية** و**فرض توريث الإعدادات في السياسات الفرعية**:

- في حالة تمكين إعدادات **التوريث من السياسة الأصلية** لسياسة تابعة وقفل بعض الإعدادات في السياسة الأصلية، لا يمكنك بالتالي تغيير هذه الإعدادات للمجموعة التابعة. ومع ذلك، يمكنك تغيير الإعدادات التي لم يتم "قفلها" في السياسة الأصلية.
- أما في حالة تعطيل إعدادات **التوريث من السياسة الأصلية** لسياسة تابعة، فيمكنك بالتالي تغيير كل الإعدادات في المجموعة التابعة حتى في حالة "قفل" بعض الإعدادات في السياسة الأصلية.
- في حالة تمكين **فرض توريث الإعدادات في السياسات الفرعية** في المجموعة الأصلية، يؤدي ذلك إلى تمكين **توريث الإعدادات من السياسة الأصلية** لكل سياسة تابعة. وفي هذه الحالة، لا يمكنك تعطيل هذا الخيار لأية سياسة تابعة. ويتم فرض توريث كل الإعدادات التي تم قفلها في السياسة الأصلية في المجموعات التابعة ولا يمكنك تغيير هذه الإعدادات في المجموعات التابعة.
- في سياسات مجموعة **الأجهزة المُدارة**، لا يؤثر الخيار **توريث الإعدادات من السياسة الأصلية** على أي إعدادات لأن مجموعة **الأجهزة المُدارة** لا تتضمن أية مجموعات مصدر، وبالتالي لا تقوم بتوريث أية سياسات.

يتم افتراضيًا تمكين الخيار **توريث الإعدادات من السياسة الأصلية** للسياسة الجديدة.

إذا كانت السياسة تتضمن ملفات تعريف، فتقوم السياسات التابعة بتوريث ملفات التعريف هذه.

إدارة السياسات

يتم تكوين التطبيقات المثبتة على الأجهزة العميلة بشكل مركزي من خلال تحديد السياسات.

وتُعرض السياسات المنشأة للتطبيقات الموجودة في مجموعة الإدارة في مساحة العمل، ضمن علامة التبويب **السياسات**. ويظهر قبل اسم كل سياسة رمز يدل على حالتها.

بعد حذف السياسة أو إلغائها، تتابع التطبيقات العمل بالإعدادات المحددة في السياسة. ويمكن تعديل تلك الإعدادات يدويًا فيما بعد.

يتم تطبيق السياسة كما يلي: في حالة تشغيل الجهاز مهام قائمة (مهام الحماية في الوقت الحقيقي)، فإن هذه المهام تواصل تشغيلها باستخدام قيم الإعدادات الجديدة. وتستمر أي مهام دورية (الفحص حسب الطلب، وتحديث قواعد بيانات التطبيق) تم بدء تشغيلها دون تغيير في القيم. في المرة القادمة، سيتم تشغيلها بقيم الإعدادات الجديدة.

يتم توريث السياسات والتطبيقات التي تتمتع بدعم التشغيل المتعدد لمجموعات إدارة منخفضة المستوى وكذلك إلى مجموعات إدارة عالية المستوى: يتم نشر السياسة على كافة الأجهزة العميلة التي يتم تثبيت التطبيق عليها.

إذا تم ترتيب خوادم الإدارة في تسلسل هرمي، فإن خوادم الإدارة الثانوية تتلقى السياسات من خادم الإدارة الرئيسي وتقوم بتوزيعها على الأجهزة العميلة. عند تمكين الوراثة، يمكن تعديل إعدادات السياسة على خادم الإدارة الرئيسي. وبعد ذلك، يتم نشر أي تغييرات أُجريت على إعدادات السياسة في السياسات الموروثة على خوادم الإدارة الثانوية.

إذا تم إنهاء الاتصال بين خوادم الإدارة الأساسية والتابعة، فإن السياسة الخاص بالخادم التابع تستمر باستخدام الإعدادات المُطبقة. إعدادات السياسة المعدّلة الموجودة على خادم الإدارة الرئيسي يتم توزيعها على خادم إدارة تابع بعد إعادة إنشاء الاتصال.

في حالة تعطيل الوراثة، يمكن تعديل إعدادات السياسة الخاصة بخادم الإدارة الثانوي بشكل مستقل من خادم الإدارة الرئيسي.

إذا تم قطع الاتصال بين خادم الإدارة والجهاز العميل، فيبدأ الجهاز العميل في العمل بسياسة الوجود خارج المكتب (إذا تم تحديدها) أو يستمر تشغيل السياسة باستخدام الإعدادات المطبّقة إلى أن يتم إعادة إنشاء الاتصال.

تُعرض نتائج توزيع السياسة على خادم الإدارة الثانوي في نافذة خصائص السياسة بوحدة التحكم على خادم الإدارة الرئيسي.

وتُعرض نتائج توزيع السياسات على الأجهزة العميلة في نافذة خصائص السياسة بخادم الإدارة التي تتصل به.

لا تستخدم بيانات خاصة في إعدادات السياسة. على سبيل المثال، تجنّب تخصيص كلمة مرور مسؤول المجال.

إنشاء سياسة

في وحدة تحكم الإدارة، يمكنك إنشاء سياسات مباشرة في المجلد الخاص بمجموعة الإدارة التي سيتم إنشاء سياسة لها، أو في مساحة عمل المجلد **السياسات**.

لإنشاء سياسة في مجلد خاص بمجموعة إدارة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي تريد إنشاء سياسة لها.
2. في مساحة العمل الخاصة بالمجموعة، حدد علامة التبويب **السياسات**.
3. قم بتشغيل معالج السياسة الجديدة عن طريق النقر فوق الزر **سياسة جديدة**.

   يبدأ معالج السياسة الجديدة. اتبع إرشادات المعالج.

لإنشاء سياسة في مساحة عمل المجلد **السياسات**:

1. من شجرة وحدة التحكم، حدد مجلد **السياسات**.
2. قم بتشغيل معالج السياسة الجديدة عن طريق النقر فوق الزر **سياسة جديدة**.

   يبدأ معالج السياسة الجديدة. اتبع إرشادات المعالج.

يمكنك إنشاء عدة سياسات لتطبيق واحد من المجموعة، ولكن لا يكون هناك إلا سياسة واحدة فقط نشط في كل مرة. عند إنشاء سياسة جديدة نشطة، تصبح السياسة المفعلة السابقة غير نشطة.

عند إنشاء سياسة، يمكنك تحديد مجموعة على الأقل من المعلمات المطلوبة لكي يعمل التطبيق بشكل سليم. يتم تعيين جميع القيم الأخرى إلى القيم الافتراضية المطبّقة أثناء التثبيت المحلي للتطبيق. ويمكنك تغيير السياسة بعد إنشائها.

لا تستخدم بيانات خاصة في إعدادات السياسة. على سبيل المثال، تجنّب تخصيص كلمة مرور مسؤول المجال.

يتم توضيح إعدادات تطبيقات Kaspersky التي تم تغييرها بعد تطبيق السياسات بالتفصيل في الأدلة المعنية.

بعد إنشاء السياسة، يتم تطبيق الإعدادات التي تم منع تحريرها (تم تمييزها بأيقونة القفل()) على الأجهزة العميلة بغض النظر عن أي الإعدادات التي تم تحديدها مسبقًا للتطبيق.

عرض سياسة موروثة في مجموعة فرعية

لتمكين عرض السياسات الموروثة لمجموعة إدارة متداخلة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي ينبغي عرض السياسات الموروثة لها.
2. في مساحة عمل المجموعة المحددة، حدد علامة التبويب **السياسات**.
3. في قائمة السياق الخاصة بقائمة السياسات، حدد **عرض** > **السياسات الموروثة**.

يتم عرض السياسات الموروثة في قائمة السياسات متضمنةً الرمز التالي:

- —إذا كانت موروثة من مجموعة تم إنشاؤها على خادم إدارة أساسي.
- —إذا كانت موروثة من مجموعة مستوى أعلى.

عند تمكين وضع توريث الإعدادات، تتوفر إمكانية تعديل السياسات الموروثة في المجموعة التي تم إنشاؤها فيها فقط. ولا تتوفر إمكانية تعديل تلك السياسات الموروثة في المجموعة التي قامت بوراثتها.

تنشيط سياسة

لتنشيط سياسة للمجموعة المحددة:

1. في مساحة عمل المجموعة، من علامة التبويب **السياسات**، حدد السياسة التي يتعين عليك تنشيطها.
2. لتنشيط السياسة، قد بأحد الإجراءات التالية:
   - في قائمة السياق للسياسة، حدد **سياسة نشطة**.
   - في نافذة خصائص السياسة، افتح القسم **عام** وحدد **سياسة نشطة** من مجموعة إعدادات **حالة السياسة**.

تصبح السياسة نشطة لمجموعة الإدارة المحددة.

عندما يتم تطبيق سياسة على عدد كبير من الأجهزة العميلة، يزيد الحمل على كل من خادم الإدارة وحركة مرور الشبكة بشكل كبير لفترة من الوقت.

تنشيط سياسة تلقائيًا بعد حدث انتشار الفيروسات

لجعل السياسة تقوم بعملية التنشيط تلقائيًا عند حدوث حدث انتشار الفيروسات:

1. في نافذة خصائص خادم الإدارة، افتح القسم **انتشار الفيروسات**.
2. افتح النافذة **تنشيط السياسة** بالنقر فوق الرابط **تكوين السياسات ليتم تفعيلها عند وقوع حدث انتشار الفيروسات** وأضف السياسة إلى القائمة المحددة للسياسات التي يتم تنشيطها عند اكتشاف انتشار الفيروس.

إذا تم تنشيط سياسة عند حدث انتشار فيروسات، يمكنك العودة إلى السياسة السابقة فقط باستخدام الوضع اليدوي.

تطبيق سياسة الوجود خارج المكتب

تصبح سياسة الوجود خارج المكتب فعالة على الجهاز إذا تم قطع اتصاله عن شبكة الشركة.

لتطبيق سياسة الوجود خارج المكتب:

في نافذة خصائص السياسة، افتح القسم **عام**، ومن مجموعة إعدادات **حالة السياسة**، حدد **سياسة الوجود خارج المكتب**.

سيتم تطبيق سياسة الوجود خارج المكتب على الأجهزة إذا تم قطع اتصالها عن شبكة الشركة.

تعديل سياسة. التراجع عن التغييرات

لتعديل سياسة:

1. من شجرة وحدة التحكم، حدد مجلد **السياسات**.
2. في مساحة عمل المجلد **السياسات**، حدد سياسة وتابع إلى نافذة خصائص السياسة عبر استخدام قائمة السياق.
3. قم بعمل التغييرات اللازمة.
4. انقر على **تطبيق** .

وسيتم حفظ التغييرات التي تم إجراؤها على السياسة في خصائص السياسة، في القسم **سجل المراجعة**.

وإذا لزم الأمر، يمكنك التراجع عن التغييرات التي تم إجراؤها على السياسة.

للتراجع عن التغييرات التي تم إجراؤها على السياسة:

1. من شجرة وحدة التحكم، حدد مجلد **السياسات**.
2. حدد السياسة التي يجب التراجع عن التغييرات التي تم إجراؤها فيها، ثم تابع إلى نافذة خصائص السياسة باستخدام قائمة السياق.
3. في النافذة خصائص السياسة، حدد القسم **سجل المراجعة**.
4. في قائمة محفوظات المراجعات، حدد رقم المراجعة التي ترغب في التراجع عن التغييرات لها.
5. انقر فوق الزر **خيارات متقدمة** وحدد القيمة **التراجع** في القائمة المنسدلة.

مقارنة السياسات

يمكنك المقارنة بين سياستين لتطبيق مدار واحد. بعد إجراء المقارنة، ستحصل على تقرير يعرض أي من إعدادات السياسة متطابقة وأيها مختلفة. قد يتعين عليك، على سبيل المثال، مقارنة السياسات إذا قام المسؤولون بإنشاء سياسات متعددة لتطبيق مدار واحد في المكاتب الخاصة بهم، أو إذا تم توريث سياسة واحدة عالية المستوى بواسطة كل المكاتب المحلية أو إذا تم تعديلها لكل مكتب. يمكنك مقارنة السياسات بإحدى الطرق التالية: عن طريق تحديد سياسة ومقارنتها بالأخرى، أو عن طريق مقارنة سياستين من قائمة السياسات.

يمكنك فقط مقارنة السياسات التي تحتوي على مراجعات حالية في سجل المراجعة.

لمقارنة سياسة بأخرى:

1. من شجرة وحدة التحكم، حدد مجلد **السياسات**.

2. في مساحة عمل المجلد **السياسات**، حدد السياسة التي تحتاج لمقارنتها بسياسة أخرى.

3. في قائمة السياق الخاصة بالسياسة، حدد **مقارنة سياسة بسياسة أخرى**.

4. في النافذة **تحديد سياسة**، حدد السياسة التي ستتم مقارنتها بسياستك.

5. انقر على**موافق**.

يتم عرض تقرير بتنسيق HTML لمقارنة سياستين لنفس التطبيق.

لمقارنة أي سياستين من قائمة السياسات:

1. في مجلد **السياسات**، في قائمة السياسات، استخدم المفتاح **Shift** أو **Ctrl** لتحديد سياستين لتطبيق مُدار واحد.

2. في قائمة السياق، حدد **مقارنة**.

يتم عرض تقرير بتنسيق HTML لمقارنة سياستين لنفس التطبيق.

يقدم أيضًا التقرير المعني بمقارنة إعدادات السياسة لتطبيق Kaspersky Endpoint Security for Windows تفاصيل مقارنة ملفات تعريف السياسات. يمكنك تصغير نتائج مقارنة ملف تعريف السياسة. لتصغير القسم، انقر فوق أيقونة السهم (▲) بجوار اسم القسم.

عرض مخطط حالة توزيع السياسة

في Kaspersky Security Center، يمكنك عرض نتائج تطبيق السياسة على كل جهاز.

لعرض مخطط حالة توزيع السياسة على كل جهاز:

1. في مساحة عمل المجموعة، في علامة التبويب **السياسات**، حدد السياسة التي تريد عرض حالة التوزيع لها.
   يعرض المخطط الموجود في الجزء الأيسر نظرة عامة حول فرض السياسة.

2. انقر فوق **Details**.
   تفتح النافذة **نتائج تطبيق السياسة**.
   يمكنك تصدير نتائج فرض السياسة إلى ملف CSV أو TXT.

حذف سياسة

لحذف سياسة:

1. في مساحة عمل مجموعة إدارة، من علامة التبويب **السياسات**، حدد السياسة التي تريد حذفها.

2. يمكنك حذف السياسة بإحدى الطرق التالية:

- بتحديد **حذف** في قائمة السياق للسياسة.

- من خلال النقر فوق الرابط **حذف سياسة** في خانة المعلومات الخاصة بالسياسة المحددة.

نسخ سياسة

لنسخ سياسة:

1. في مساحة عمل المجموعة المطلوبة، من علامة التبويب **السياسات** حدد إحدى السياسات.

2. في قائمة السياق للسياسة، حدد **نسخ**.

3. في شجرة وحدة التحكم، حدد المجموعة التي تريد نسخ السياسة إليها.
   ويمكنك إضافة سياسة إلى المجموعة التي تم نسخ السياسة منها.

4. من قائمة السياق الخاصة بقائمة سياسات المجموعة المحددة، في علامة التبويب **السياسات** حدد **لصق**.

يتم نسخ السياسة مع جميع الإعدادات الخاصة بها ويتم تطبيقها على الأجهزة الموجودة ضمن المجموعة التي تم نسخها فيها. إذا قمت بلصق السياسة في نفس المجموعة التي قمت بنسخها منها، تتم إضافة المؤشر الدلالي **(<رقم التسلسل التالي>)** إلى اسم السياسة تلقائيًا: على سبيل المثال **(1)**, **(2)**.

وتصبح السياسة المفعلة أثناء نسخها غير نشطة. وإذا لزم الأمر، يمكنك جعلها نشطة.

تصدير سياسة

لتصدير سياسة:

1. استخدام إحدى الطرق التالية لتصدير سياسة:

   - بتحديد **جميع& المهام** ← **تصدير** في قائمة السياق للسياسة.
   - من خلال النقر على ارتباط **تصدير السياسة إلى ملف** في مربع المعلومات الخاص بالنهج المحدد.

2. في النافذة **حفظ باسم** التي تفتح، حدد اسم ملف السياسة والمسار إليه. انقر على زر **حفظ**.

استيراد سياسة

لاستيراد سياسة:

1. في مساحة عمل المجموعة ذات الصلة، من علامة التبويب **السياسات** حدد إحدى الطرق التالية لاستيراد السياسات:

   - عن طريق تحديد **جميع& المهام** ← **استيراد** في قائمة السياق الخاصة بقائمة السياسات.
   - بالنقر فوق الزر **استيراد سياسة من ملف** الموجود في كتلة الإدارة الخاصة بقائمة السياسات.

2. في النافذة التي تفتح، حدد مسار الملف الذي تريد استيراد السياسة منه. انقر فوق الزر **فتح**.

يتم عرض السياسة المستوردة في قائمة السياسات. يتم أيضًا استيراد إعدادات وملفات تعريف السياسة. بغض النظر عن حالة السياسة التي تم تحديدها أثناء التصدير، فإن السياسة المستوردة غير نشطة. يمكنك تغيير حالة السياسة في خصائص السياسة.

إذا كانت السياسة المستوردة حديثًا لها اسم مطابق لاسم سياسة موجودة، فسيتم توسيع اسم السياسة المستوردة بامتداد فهرس **(<next sequence number>)** ، على سبيل المثال: **(1)** و **(2)**.

تحويل السياسات

يستطيع Kaspersky Security Center تحويل السياسات من الإصدارات السابقة لتطبيقات Kaspersky المُدارة إلى الإصدارات المحدثة من التطبيقات نفسها. تحافظ السياسات المحولة على إعدادات المسؤول الحالية المحددة قبل التحديث، بالإضافة إلى تضمين الإعدادات الجديدة من الإصدارات الحديثة للتطبيقات. وإذا تم تحويل سياسة إلى إصدار محدث من تطبيق Kaspersky مُدار، فلن تتمكن من فتح السياسة على خادم إدارة التطبيق الذي يحتوي على إصدار سابق مُثبت من المكون الإضافي للتطبيق. تحدد المكونات الإضافية للإدارة لتطبيقات Kaspersky ما إذا كان التحويل متاحًا لسياسات هذه التطبيقات. للحصول على معلومات حول سياسات التحويل لكل تطبيق من تطبيقات Kaspersky المدعومة، راجع التعليمات ذات الصلة من القائمة التالية:

- **تطبيقات Kaspersky لمحطات العمل:**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security لنظام Windows
- **الأمن الإلكتروني الصناعي من Kaspersky:**
  - الأمن الإلكتروني الصناعي من Kaspersky للعقد
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (النشر المركزي غير مدعوم)
- **تطبيقات Kaspersky للأجهزة المحمولة:**
  - Kaspersky Endpoint Security for Android:
  - Kaspersky Security لأجهزة iOS
- **تطبيقات Kaspersky لخوادم الملفات:**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **تطبيقات Kaspersky للأجهزة الافتراضية:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless

- **تطبيقات Kaspersky لاكتشاف الهجمات المستهدفة:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **تطبيقات Kaspersky لأجهزة KasperskyOS:**
  - بوابة Kaspersky IoT الآمنة
  - Kaspersky Security Management Suite (مكون إضافي لـ Kaspersky Thin Client)

لتحويل السياسات:

1. من شجرة وحدة التحكم، حدد خادم الإدارة الذي تريد أن تقوم بتحويل السياسات إليه.
2. في القائمة سياق خادم الإدارة، حدد **جميع المهام** ← **معالج تحويل تصحيح المهام والسياسات**.

   يبدأ معالج تحويل تصحيح المهام والسياسات. اتبع إرشادات المعالج.

بعد اكتمال المعالج، يتم إنشاء سياسات جديدة تستخدم إعدادات سياسات المسؤول الحالية والإعدادات الجديدة من الإصدارات المحدثة من تطبيقات Kaspersky.

إدارة ملفات تعريف السياسة

يُعد ملف تعريف السياسة مجموعة مسماة من الإعدادات لسياسة تم تفعيلها على جهاز عميل (كمبيوتر أو جهاز محمول) عندما يفي الجهاز بـ قواعد تفعيل محددة. يؤدي تنشيط ملف التعريف إلى تعديل إعدادات السياسة التي كانت نشطة على الجهاز قبل أن يتم تنشيط ملف التعريف. هذه الإعدادات تأخذ القيم التي تم تحديدها في ملف التعريف.

إن ملفات تعريف السياسة تُعد ضرورية للسماح بتشغيل الأجهزة الموجودة ضمن مجموعة إدارة واحدة بموجب إعدادات سياسة مختلفة. على سبيل المثال، قد يطرأ شيء ما عند الاضطرار لتعديل إعدادات السياسة لبعض الأجهزة في إحدى مجموعات الإدارة. في هذه الحالة، يمكنك تكوين ملفات تعريف السياسة لهذه السياسة، مما يتيح لك تحرير إعدادات السياسة للأجهزة المحددة في مجموعة الإدارة. على سبيل المثال، تحظر السياسة تشغيل برنامج تحديد الموقع GPS على جميع الأجهزة في مجموعة الإدارة "المستخدمين". يلزم وجود برنامج تحديد الموقع GPS على جهاز واحد في مجموعة الإدارة "المستخدمين"، وهو الجهاز المملوك لمستخدم يعمل بوظيفة "ساع". يمكنك بكل بساطة وضع علامة "البريد السريع" على هذا الجهاز وإعادة تكوين ملف تعريف السياسة لتتيح تشغيل برنامج تحديد الموقع GPS على الجهاز ذو العلامة "البريد السريع" فقط، مع الحفاظ على جميع إعدادات السياسة المتبقية. وفي هذه الحالة، إذا ظهر جهاز يحمل العلامة "البريد السريع" في مجموعة الإدارة "المستخدمين"، فسيتاح له تشغيل برنامج تحديد الموقع GPS. سيستمر حظر تشغيل برنامج تحديد الموقع GPS على الأجهزة الأخرى في مجموعة الإدارة "المستخدمين" إلا إذا كانت تحمل العلامة "البريد السريع" كذلك.

ملفات التعريف مدعومة فقط من السياسات التالية:

- سياسات Kaspersky Endpoint Security for Windows
- سياسات Kaspersky Endpoint Security for Mac.
- سياسات المكون الإضافي لـ Kaspersky Mobile Device Management تتراوح بين الإصدار 10 Service Pack 1 والإصدار 10 Service Pack 3 Maintenance Release 1
- سياسات المكون الإضافي لـ Kaspersky Device Management for iOS
- سياسات Kaspersky Security for Virtualization 5.1 Light Agent for Windows
- سياسات Kaspersky Security for Virtualization 5.1 Light Agent for Linux

تقوم ملفات تعريف السياسة بتبسيط إدارة الأجهزة العميلة التي يتم تطبيق السياسات عليها:

- قد تختلف إعدادات ملف تعريف السياسة عن إعدادات السياسة.
- ليس عليك المحافظة على عدة حالات لسياسة واحدة تختلف فقط بمقدار عدد قليل من الإعدادات أو تطبيقها يدويًا.
- ليس عليك تخصيص سياسة منفصلة للمستخدمين خارج المكتب.
- يمكنك تصدير ملفات تعريف السياسة واستيرادها، وكذلك إنشاء ملفات تعريف سياسة جديدة وفقًا لملفات تعريف موجودة بالفعل.
- يمكن أن تمتلك سياسة واحدة العديد من ملفات تعريف السياسة المفعلة. فقط ملفات التعريف التي تفي بقواعد التفعيل السارية على الجهاز سيتم تطبيقها على ذلك الجهاز.
- تخضع ملفات التعريف للتسلسل الهرمي للسياسات. تحتوي سياسة موروثة على جميع ملفات التعريف الخاصة بالسياسة من المستوى الأعلى.

أولويات ملفات التعريف.

يتم ترتيب ملفات التعريف التي تم إنشاؤها لسياسة ترتيب تنازلي حسب الأولوية. على سبيل المثال، إذا كان ملف التعريف (أ) يقع في مرتبة أعلى من ملف التعريف (ب) في قائمة ملفات التعريف، فيكون لملف التعريف (أ) أولوية أعلى من ملف التعريف (ب). يمكن تطبيق العديد من ملفات التعريف على جهاز واحد في نفس الوقت. في حالة اختلاف قيم أحد الإعدادات في ملفات تعريف مختلفة، فيتم تطبيق القيمة من ملف التعريف الأعلى أولوية على الجهاز.

قواعد تفعيل ملف تعريف

يتم تنشيط ملف تعريف سياسة على جهاز عميل عند تشغيل قاعدة تفعيل. قواعد التفعيل هي مجموعة من الشروط التي تؤدي إلى، عند الوفاء بها، بدء ملف تعريف السياسة على الجهاز. قد تحتوي قاعدة التنشيط على الشروط التالية:

- اتصال عميل الشبكة على كمبيوتر عميل بخادم الإدارة الذي يمتلك مجموعة محددة من إعدادات الاتصال، مثل عنوان خادم الإدارة ورقم المنفذ، وما إلى ذلك.
- الجهاز العميل غير متصل بالإنترنت.
- تم تعيين علامات محددة للجهاز العميل.
- الجهاز العميل يوجد بشكل صريح (الجهاز يوجد مباشرةً في وحدة محددة) أو بشكل ضمني (الجهاز يوجد في وحدة توجد في الوحدة المحددة على أي مستوى من التداخل) في وحدة محددة من Active Directory®، الجهاز أو مالكه يوجد في مجموعة أمان من Active Directory.
- الجهاز العميل ينتمي لمالك محدد، أو تم تضمين مالك الجهاز في مجموعة أمان داخلية خاصة بـ Kaspersky Security Center.
- تم تعيين دور محدد لمالك الجهاز العميل.

ملفات التعريف في التسلسل الهرمي لمجموعات الإدارة

إذا كنت تقوم بإنشاء سياسة في مجموعة إدارة من المستوى المنخفض، فترث هذه السياسة الجديدة جميع ملفات التعريف الخاصة بالسياسة المفعلة من المجموعة من المستوى الأعلى. ويتم دمج ملفات التعريف ذات الأسماء المتطابقة. ويكون لملفات تعريف السياسة من المجموعة ذات المستوى الأعلى الأولوية الأعلى. على سبيل المثال، في مجموعة الإدارة A، السياسة P(A) لديها ملفات تعريف X1 وX2 وX3 (في ترتيب تنازلي حسب الأولوية). في مجموعة الإدارة B، والتي تكون مجموعة فرعية من مجموعة الإدارة A، تم إنشاء السياسة P(B) بملفات التعريف X2 وX4 وX5. سيتم تعديل السياسة P(B) مع السياسة P(A) بحيث تظهر قائمة ملفات التعريف في السياسة P(B) على النحو التالي: X1، X2, X3, X4، X5 (بترتيب تنازلي من حيث درجة الأولوية). سوف تعتمد أولوية ملف التعريف X2 على الحالة الأولية لـ X2 للسياسة P(B) وX2 للسياسة P(A). بعد إنشاء السياسة P(B)، لا يتم عرض السياسة P(A) في المجموعة الفرعية B.

يتم إعادة حساب السياسة المفعلة عند كل عملية تشغيل لعميل الشبكة، أو تمكين وتعطيل وضع غير متصل، أو تحرير قائمة العلامات المُعينة للجهاز العميل. على سبيل المثال، عند زيادة حجم ذاكرة الوصول العشوائي (RAM) على الجهاز، يؤدي ذلك إلى تفعيل ملف تعريف السياسة الذي يتم تطبيقه على الأجهزة ذات حجم RAM مرتفع.

خصائص وقيود ملفات تعريف السياسة

لدى ملفات التعريف الخصائص التالية:

- ليس لملفات تعريف السياسة غير المفعلة أي تأثير على الأجهزة العميلة.
- إذا تم تعيين السياسة إلى الحالة **سياسة الوجود خارج المكتب**، فسيتم تطبيق ملفات تعريف السياسة أيضًا عند قطع اتصال الجهاز من شبكة الشركة.
- ملفات التعريف لا تدعم التحليل الثابت للوصول إلى الملفات التنفيذية.
- لا يمكن أن يحتوي ملف تعريف السياسة على أيٍ من إعدادات إخطارات الأحداث.
- إذا تم استخدام المنفذ UDP 15000 لاتصال جهاز بخادم الإدارة، فيتم تنشيط ملف التعريف المناظر له في غضون دقيقة واحدة بعد تعيين علامة إلى الجهاز.
- يمكنك استخدام قواعد اتصال عميل الشبكة بخادم الإدارة، عند إنشاء قواعد تفعيل ملف تعريف السياسة.

إنشاء ملف تعريف سياسة

إنشاء ملف التعريف متاح فقط لسياسات التطبيقات التالية:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows والإصدارات الأحدث
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- سياسات المكون الإضافي لإدارة Kaspersky Mobile Device الإصدار 10 Service Pack 1 إلى الإصدار 10 Service Pack 3 Maintenance Release 1
- المكون الإضافي لـ Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows and Linux

لإنشاء ملف تعريف سياسة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي يجب إنشاء ملف تعريف سياسة للسياسة الخاصة بها.
2. في مساحة العمل الخاصة بمجموعة الإدارة، حدد علامة التبويب **السياسات**.
3. قم بتحديد سياسة ثم انتقل إلى نافذة خصائص السياسة باستخدام قائمة السياق.
4. قم بفتح القسم **ملفات تعريف السياسة** في نافذة خصائص السياسة وانقر فوق الزر **إضافة**.
   يبدأ معالج ملف تعريف السياسة الجديدة.
5. في نافذة المعالج **اسم ملف تعريف السياسة**، حدد التالي:
   a. اسم ملف تعريف السياسة
   لا يمكن أن يتضمن اسم ملف التعريف أكثر من 100 حرف.

b. حالة ملف تعريف السياسة (تم التمكين أو معطل).

ننصحك بإنشاء ملفات تعريف السياسة غير المفعلة وتمكينها وذلك فقط بعد الانتهاء بشكل كامل من إعدادات وحالات تفعيل ملف تعريف السياسة.

6. حدد خانة الاختيار **بعد إغلاق معالج ملف تعريف السياسة الجديدة، انتقل إلى تكوين قاعدة تفعيل ملف تعريف السياسة** لبدء تشغيل معالج قاعدة تفعيل ملف تعريف السياسة الجديد. اتبع خطوات المعالج.

7. قم بتحرير إعدادات ملف تعريف السياسة في نافذة خصائص ملف تعريف السياسة، بالطريقة التي تطلبها.

8. قم بحفظ التغييرات بالنقر فوق **موافق**.

تم حفظ ملف التعريف. سيتم تفعيل ملف التعريف على الأجهزة التي تستوفي قواعد التفعيل.

يمكنك إنشاء ملفات تعريف متعددة لسياسة واحدة. يتم عرض ملفات التعريف التي تم إنشاؤها لسياسة في خصائص السياسة، في القسم **ملفات تعريف السياسة**. يمكنك تعديل ملف تعريف سياسة وتغيير أولوية ملف التعريف، وكذلك إزالة ملف التعريف.

تعديل ملف تعريف سياسة

تحرير إعدادات ملف تعريف سياسة

تتوفر القدرة على تحرير ملف تعريف سياسة لسياسات Kaspersky Endpoint Security for Windows فقط.

لتعديل ملف تعريف سياسة

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي يجب تعديل ملف تعريف السياسة لها.

2. في مساحة العمل الخاصة بالمجموعة، حدد علامة التبويب **السياسات**.

3. قم بتحديد سياسة ثم انتقل إلى نافذة خصائص السياسة باستخدام قائمة السياق.

4. افتح القسم **ملفات تعريف السياسة** في خصائص السياسة.

يحتوي هذا القسم على قائمة بملفات التعريف التي تم إنشاؤها للسياسة. يتم عرض ملفات التعريف في القائمة وفقًا لأولوياتها.

5. حدد ملف تعريف سياسة وانقر فوق الزر **خصائص**.

6. قم بتكوين ملف التعريف في نافذة الخصائص:

- إذا لزم الأمر، في القسم **عام**، قم بتغيير اسم ملف التعريف ثم قم بتمكين أو تعطيل ملف التعريف باستخدام خانة الاختيار **تمكين ملف التعريف**.
- في القسم **قواعد التفعيل**، قم بتحرير قواعد تفعيل ملف التعريف.
- قم بتحرير إعدادات السياسة في الأقسام المقابلة.

7. انقر على**موافق**.

سوف يتم تطبيق الإعدادات التي قمت بتعديلها إما بعد مزامنة الجهاز مع خادم الإدارة (إذا كان ملف تعريف السياسة نشطًا)، أو بعد تشغيل قاعدة تفعيل (إذا كان ملف التعريف غير نشط).

تغيير أولوية ملف تعريف سياسة

تحدد أولوية ملفات تعريف السياسة ترتيب تنشيط ملفات التعريف على جهاز عميل. يتم استخدام الأولويات إذا تم تعيين قواعد تنشيط متماثلة لمختلف ملفات تعريف السياسة.

على سبيل المثال، تم إنشاء ملفين تعريف سياسة: ملف التعريف 1 وملف التعريف 2والذي يختلف بواسطة القيم الخاصة لإعداد واحد (القيمة 1 والقيمة 2). أولوية ملف التعريف 1 أعلى من ملف التعريف 2. علاوة على ذلك، يوجد ملفات تعريف ذات أولوية أقل من ملف التعريف 2. تكون قواعد تنشيط ملفات التعريف تلك متماثلة.

عند تشغيل قاعدة تفعيل، سيتم تفعيل ملف التعريف 1. وسوف يأخذ الإعداد على الجهاز القيمة 1. إذا قمت بإزالة ملف التعريف 1، فإن ملف التعريف 2 له الأولوية القصوى، وسوف يأخذ الإعداد القيمة 2.

في قائمة ملفات تعريف السياسة، يتم عرض ملفات التعريف وفقًا لأولويات كل منها. يأتي ملف التعريف ذو الأولوية القصوى في المرتبة الأولى. يمكنك تغيير أولوية ملف التعريف باستخدام زري السهم لأعلى والسهم لأسفل.

إزالة ملف تعريف سياسة

لحذف ملف تعريف سياسة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي ترغب في حذف ملف تعريف سياسة لها.
2. في مساحة العمل الخاصة بمجموعة الإدارة، حدد علامة التبويب **السياسات**.
3. قم بتحديد سياسة ثم انتقل إلى نافذة خصائص السياسة باستخدام قائمة السياق.
4. افتح القسم **ملفات تعريف السياسة** في خصائص سياسة Kaspersky Endpoint Security.
5. حدد ملف تعريف السياسة الذي ترغب في إزالته وانقر فوق الزر **حذف**.

سيتم حذف ملف تعريف السياسة. سيتم تمرير الحالة المفعلة إما لملف تعريف سياسة آخر الذي سيتم تشغيل قواعد تنشيطه على الجهاز، أو إلى السياسة.

إنشاء قاعدة تفعيل ملف تعريف سياسة

لإنشاء قاعدة تفعيل ملف تعريف سياسة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي يتعين عليك إنشاء قاعدة تفعيل ملف تعريف سياسة لها.
2. في مساحة العمل الخاصة بالمجموعة، حدد علامة التبويب **السياسات**.
3. قم بتحديد سياسة ثم انتقل إلى نافذة خصائص السياسة باستخدام قائمة السياق.
4. حدد القسم **ملفات تعريف السياسة** في النافذة خصائص السياسة.
5. حدد ملف تعريف السياسة الذي تحتاج إلي إنشاء قاعدة تفعيل لها، وانقر فوق الزر **خصائص**.

   يتم فتح نافذة خصائص ملف تعريف السياسة.

   إذا كانت قائمة ملفات تعريف السياسة فارغة، يمكنك إنشاء ملف تعريف سياسة.
6. حدد القسم **قواعد التفعيل**، وانقر فوق الزر **إضافة**.

   سيبدأ تشغيل معالج قاعدة تفعيل ملف تعريف سياسة جديدة.
7. في النافذة **قواعد تفعيل ملف تعريف السياسة**، حدد خانات الاختيار المجاورة للشروط التي يجب أن تؤثر على تفعيل ملف تعريف السياسة الذي تقوم بإنشائه:

- **القواعد العامة لتفعيل ملف تعريف السياسة**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناءً على حالة الوضع غير المتصل بالإنترنت للجهاز وقاعدة الاتصال بخادم الإدارة والعلامات المعينة للجهاز.

- **قواعد استخدام Active Directory**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناء على وجود الجهاز في الوحدة التنظيمية لـ Active Directory، أو عضوية الجهاز (أو عضوية مالكه) في مجموعة أمن Active Directory.

- **قواعد مالك جهاز معين**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناءً على مالك الجهاز.

- **قواعد مواصفات الأجهزة**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناءً على حجم الذاكرة وعدد المعالجات المنطقية.

يعتمد عدد الصفحات الإضافية للمعالج على الإعدادات التي تحددها في الخطوة الأولى. يمكنك تعديل قواعد تفعيل ملف تعريف السياسة في وقت لاحق.

8. في النافذة **الشروط العامة**، حدد الإعدادات التالية:

- في حقل **الجهاز غير متصل**، في القائمة المنسدلة، حدد الشرط الخاص بوجود الجهاز على الشبكة:

  - **نعم**

  الجهاز موجود في شبكة خارجية، وهذا يعني أن خادم الإدارة غير متاح.

  - **لا**

  الجهاز موجود على الشبكة، لذا يتوفر خادم الإدارة.

  - **لم يتم تحديد قيمة**

  لن يتم تطبيق المعيار.

- في الخانة **الجهاز في موقع الشبكة المحدد**، استخدم القوائم المنسدلة لإعداد تفعيل ملف تعريف السياسة في حالة تنفيذ/عدم تنفيذ قاعدة الاتصال بخادم الإدارة على هذا الجهاز:

  - **تم التنفيذ / لم يتم التنفيذ**

  الشرط الخاص بتفعيل ملف تعريف السياسة (سواء تم تنفيذ القاعدة أو لم يتم تنفيذها).

  - **اسم القاعدة**

  وصف موقع الشبكة للجهاز للاتصال بخادم الإدارة، والذي يجب استيفاء شروطه (أو عدم استيفاء شروطه) لتفعيل ملف تعريف السياسة.

  يمكن إنشاء وصف موقع شبكة الأجهزة للاتصال بخادم الإدارة أو تكوينه في قاعدة نقل عميل شبكة.

يتم عرض النافذة **الشروط العامة** في حالة تحديد خانة الاختيار **القواعد العامة لتفعيل ملف تعريف السياسة**.

9. في نافذة **الشروط التي تستخدم العلامات**، حدد الإعدادات التالية:

- **قائمة العلامات**

في قائمة العلامات، حدد قاعدة لتضمين الجهاز في ملف تعريف السياسة عن طريق تحديد خانات الاختيار المقابلة للعلامات ذات الصلة.

يمكنك إضافة علامات جديدة إلى القائمة عن طريق إدخالها في الحقل الموجود أعلى القائمة والنقر فوق الزر **إضافة**.

يتضمن الملف التعريفي للسياسة أجهزة بها أوصاف تحتوي جميع العلامات المحددة. إذا تم إلغاء خانات الاختيار، لن يتم تطبيق المعيار. بشكل افتراضي، خانات الاختيار هذه غير محددة.

- **التطبيق على الأجهزة بدون العلامات المحددة**

مكّن هذا الخيار إذا كان يتعين عليك عكس تحديد علاماتك.

في حال تمكين هذا الخيار، سيتضمن ملف تعريف السياسة أجهزة بها أوصاف لا تحتوي على أي من العلامات المحددة. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار.

يتم تعطيل هذا الخيار افتراضيًا.

يتم عرض النافذة **الشروط التي تستخدم العلامات** إذا تم تحديد خانة الاختيار **القواعد العامة لتفعيل ملف تعريف السياسة**.

10. في نافذة **شروط استخدام Active Directory**، حدد الإعدادات التالية:

- **عضوية مالك الجهاز في مجموعة أمان Active Directory**

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز الذي يكون مالكه عضوًا في مجموعة الأمان المحددة. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **عضوية الجهاز في مجموعة أمان Active Directory**

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف تعريف السياسة على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **تخصيص الجهاز في الوحدة التنظيمية لـ Active Directory**

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف تعريف السياسة على الجهاز المدمج في الوحدة التنظيمية المحددة لـ Active Directory. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف.

يتم تعطيل هذا الخيار افتراضيًا.

يتم عرض **شروط استخدام Active Directory** إذا تم تحديد خيار **قواعد استخدام Active Directory**.

11. في **شروط استخدام مالك الجهاز**، حدد الإعدادات التالية:

- **مالك الجهاز**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف وتمكينها على الجهاز وفقًا لمالكه. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- الجهاز ينتمي للمالك المحدد (العلامة "=").
- الجهاز لا ينتمي للمالك المحدد (العلامة"#").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد مالك الجهاز عندما يتم تحديد هذا الخيار. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **مالك الجهاز مدرج في مجموعة أمان داخلية**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة عضوية المالك في مجموعة أمان داخلية خاصة بـ Kaspersky Security Center. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- مالك الجهاز عضو في مجموعة الأمان الداخلية المحددة (الرمز "=").
- مالك الجهاز ليس عضوًا في مجموعة الأمان الداخلية المحددة (العلامة "#").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد مجموعة أمان من Kaspersky Security Center. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **تفعيل ملف تعريف السياسة من خلال دور محدد لمالك الجهاز**

حدد هذا الخيار لتكوين وتمكين قاعدة تفعيل ملف التعريف على الجهاز بناءً على دور المالك. قم بإضافة الدور يدويًا من قائمة الأدوار الموجودة.

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه.

يتم عرض النافذة **شروط استخدام مالك الجهاز** إذا تم تحديد خانة الاختيار **قواعد مالك جهاز معين**.

12. في **شروط استخدام مواصفات المعدات**، حدد الإعدادات التالية:

- **حجم ذاكرة الوصول العشوائي RAM، بالميجابايت**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة حجم ذاكرة الوصول العشوائي على ذلك الجهاز. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- حجم ذاكرة الوصول العشوائي للجهاز أصغر من القيمة المحددة (علامة "<").
- حجم ذاكرة الوصول العشوائي للجهاز أكبر من القيمة المحددة (علامة ">").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد حجم ذاكرة الوصول العشوائي على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **عدد المعالجات المنطقية**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة عدد المعالجات المنطقية على ذلك الجهاز. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- عدد المعالجات المنطقية على الجهاز أقل من أو يساوي القيمة المحددة العلامة ("<").
- عدد المعالجات المنطقية على الجهاز أكبر من أو يساوي القيمة المحددة (العلامة ">").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد عدد المعالجات المنطقية على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

يتم عرض **شروط استخدام مواصفات المعدات** إذا تم تحديد خيار **قواعد مواصفات الأجهزة**.

13. في النافذة **اسم قاعدة تفعيل الخاصة بملف تعريف السياسية**، في الحقل **اسم القاعدة**، حدد اسم للقاعدة.

سيتم حفظ ملف التعريف. سيتم تفعيل ملف التعريف على الجهاز عند تشغيل قواعد التنشيط.

يتم عرض قواعد تفعيل ملف تعريف السياسة التي تم إنشاؤها لملف التعريف في خصائص ملف تعريف السياسة في القسم **قواعد التفعيل**. يمكنك تعديل أي من قواعد تفعيل ملف تعريف السياسة أو إزالتها.

يمكن تشغيل العديد من قواعد التفعيل في آن واحد.

قواعد نقل الجهاز

نوصي بأتمتة تخصيص الأجهزة لمجموعات الإدارة من خلال قواعد نقل الجهاز. تتكون قاعدة نقل جهاز ما من ثلاثة أجزاء رئيسية: اسم وشرط تنفيذ (تعبير منطقي باستخدام سمات الجهاز) ومجموعة إدارة مستهدفة. تقوم قاعدة ما بنقل جهاز ما إلى مجموعة الإدارة الهدف إذا توافقت سمات الجهاز مع شرط تنفيذ القاعدة.

كل قواعد نقل الأجهزة تحتوي على أولويات. يتحقق خادم الإدارة مما إذا كانت سمات الجهاز تفي بشرط تنفيذ كل قاعدة، بترتيب تصاعدي للأولوية. إذا توافقت سمات الجهاز مع شرط تنفيذ قاعدة ما، يتم نقل الجهاز إلى المجموعة الهدف، وبذلك تكتمل معالجة القاعدة لهذا الجهاز. إذا توافقت سمات الجهاز مع شروط قواعد متعددة، يتم نقل الجهاز إلى المجموعة الهدف الخاصة بالقاعدة ذات الأولوية الأعلى (أي التي لها أعلى رتبة في قائمة القواعد).

يمكن إنشاء قواعد نقل الجهاز ضمنيًا. على سبيل المثال، في خصائص حزمة تثبيت ما أو مهمة تثبيت عن بُعد، يمكنك تحديد مجموعة الإدارة التي يجب نقل الجهاز إليها بعد تثبيت عميل الشبكة عليه. كما يمكن إنشاء قواعد نقل الجهاز بشكل صريح بواسطة مسؤول Kaspersky Security Center، في قائمة قواعد النقل. توجد القائمة في وحدة تحكم الإدارة، في خصائص مجموعة **الأجهزة غير المخصصة**.

بشكل افتراضي، تكون قاعدة نقل جهاز مصممة للتخصيص الأولي للأجهزة إلى مجموعات الإدارة لمرة واحدة. تنقل القاعدة الأجهزة من مجموعة **الأجهزة غير المخصصة** مرة واحدة فقط. في حالة نقل جهاز مرة واحدة بواسطة هذه القاعدة، فلن تنقله القاعدة مرة أخرى أبدًا، حتى وإن قمت بإعادة الجهاز إلى مجموعة **الأجهزة غير المخصصة** يدويًا. هذه هي الطريقة المستحسنة لتطبيق قواعد النقل.

يمكنك نقل الأجهزة التي تم تخصيصها بالفعل لبعض مجموعات الإدارة. للقيام بذلك، من خصائص القاعدة، قم بإلغاء تحديد خانة الاختيار **نقل الأجهزة فقط التي لا تنتمي لمجموعة إدارة**.

يؤدي تطبيق قواعد النقل على الأجهزة التي تم تخصيصها بالفعل لبعض مجموعات الإدارة إلى زيادة الحمل بشكل كبير على خادم الإدارة.

يتم قفل خانة الاختيار **نقل الأجهزة فقط التي لا تنتمي لمجموعة إدارة** في خصائص قواعد النقل التي تم إنشاؤها تلقائيًا. ويتم إنشاء هذه القواعد عند إضافة مهمة تثبيت التطبيق عن بُعد أو إنشاء حزمة تثبيت مستقلة.

يمكنك إنشاء قاعدة نقل من شأنها التأثير على جهاز واحد بشكل متكرر.

ننصح بشدة أن تتجنب نقل جهاز واحد من مجموعة إلى أخرى بشكل متكرر (على سبيل المثال، لتطبيق سياسة محددة على هذا الجهاز، قم بتشغيل مهمة جماعية محددة أو قم بتحديث الجهاز عبر نقطة توزيع محددة).

مثل هذا السيناريو غير مدعوم لأنه يزيد الحمل على خادم الإدارة وحركة مرور الشبكة إلى الدرجة القصوى. تتعارض هذه السيناريوهات أيضًا مع مبادئ تشغيل Kaspersky Security Center (وبخاصةً في مناطق حقوق الوصول والأحداث والتقارير). يجب العثور على حل أخر، على سبيل المثال، من خلال استخدام ملفات تعريف السياسة، والمهام الخاصة بـ تحديدات الأجهزة، وتعيين عملاء الشبكة حسب السيناريو القياسي.

نسخ قواعد نقل الجهاز

عندما يتوجب عليك إنشاء قواعد متعددة لنقل الجهاز ذات إعدادات متشابهة، يمكنك نسخ قاعدة موجودة ثم تغيير الإعدادات للقاعدة المنسوخة. على سبيل المثال، يكون الأمر مفيدًا عندما يتوجب عليك امتلاك قواعد متعددة ومتطابقة لنقل الجهاز والتي تكون ذات نطاقات IP ومجموعات مستهدفة مختلفة.

لنسخ قاعدة نقل الجهاز:

1. افتح نافذة التطبيق الرئيسية.
2. في المجلد **الأجهزة غير المخصصة**، انقر فوق **تكوين القواعد**.

   تفتح نافذة **الخصائص: الأجهزة غير المخصصة**.
3. في القسم **تحريك الجهاز**، حدد قاعدة نقل الجهاز التي ترغب في نسخها.
4. انقر على **قاعدة النسخة**.

   ستتم إضافة نسخ القاعدة المحددة لنقل الجهاز في نهاية القائمة.

سيتم إنشاء قاعدة جديدة في حالة معطلة. يمكنك تحرير وتمكين القاعدة في أي وقت.

تصنيف البرنامج

الأداة الرئيسية لتشغيل التطبيقات هي فئات Kaspersky (يُشار إليها فيما بعد باسم فئات KL). تساعد فئات KL مسؤولي Kaspersky Security Center في تبسيط دعم تصنيف البرامج وتقليل حركة المرور المتوجهة إلى الأجهزة المدارة لأدنى حد.

يجب إنشاء فئات المستخدم فقط للتطبيقات التي لا يمكن تصنيفها في أي من فئات KL (على سبيل المثال البرامج المعدّة حسب الطلب). يتم إنشاء فئات المستخدم على أساس حزمة التثبيت الخاصة بتطبيق ما (MSI) أو مجلد يحتوي على حزمة التثبيت.

في حالة توفر مجموعة كبيرة من البرامج، والتي لم يتم تصنيفها عبر فئات KL، فقد يكون من المفيد إنشاء فئة يتم تحديثها تلقائيًا. ستتم إضافة المجاميع الاختبارية للملفات التنفيذية إلى هذه الفئة عند كل تعديل للمجلد الذي يحتوي على حزم التوزيع.

لا تنشئ فئات برامج محدثة تلقائيًا للمجلدات My Documents و%windir% و%ProgramFiles% و%ProgramFiles(x86)%. تخضع مجموعة الملفات الموجودة في هذه المجلدات لتغييرات متكررة، والتي تؤدي إلى حمل زائد على خادم الإدارة وحركة مرور الشبكة. يجب عليك إنشاء مجلد مخصص لمجموعة البرامج وإضافة عناصر جديدة إليه بشكل دوري.

المتطلبات الأساسية لتثبيت التطبيقات على أجهزة المؤسسة العميلة

تطابق عملية التثبيت عن بُعد للتطبيقات على أجهزة المؤسسة العميلة عملية التثبيت عن بُعد داخل المؤسسة.

لتثبيت التطبيقات على أجهزة خاصة بمنظمة العميل، يجب تنفيذ الإجراءات التالية:

- قبل تثبيت التطبيقات على أجهزة المؤسسة العميلة لأول مرة، قم بتثبيت عميل الشبكة عليهم.

عند تكوين حزمة تثبيت عميل الشبكة بواسطة موفر الخدمة في Kaspersky Security Center، اضبط الإعدادات التالية في نافذة الخصائص الخاصة بحزمة التثبيت:

- في القسم **الاتصال** في السلسلة **خادم الإدارة**، حدد عنوان نفس خادم الإدارة الافتراضي الذي تم تحديده أثناء التثبيت المحلي لعميل الشبكة على نقطة التوزيع.
- في القسم **خيارات متقدمة**، حدد خيار **الاتصال بخادم الإدارة باستخدام بوابة الاتصال**. في سلسلة **عنوان بوابة الاتصال**، حدد عنوان نقطة التوزيع. يمكنك استخدام عنوان IP أو اسم الجهاز في شبكة Windows.
- حدد **استخدام موارد نظام التشغيل عبر نقاط التوزيع** كوسيلة التنزيل المُستخدمة مع حزمة تثبيت عميل الشبكة. يمكنك تحديد طريقة التنزيل على النحو التالي:
  - إذا قمت بتثبيت التطبيق باستخدام مهمة التثبيت عن بُعد، فيمكنك تحديد طريقة التنزيل بإحدى الطرق التالية:
    - عند إنشاء مهمة تثبيت عن بُعد في النافذة **إعدادات**.
    - في نافذة خصائص مهمة التثبيت عن بُعد، من خلال القسم **إعدادات**.
  - إذا قمت بتثبيت التطبيقات باستخدام معالج التثبيت عن بُعد، يمكنك تحديد طريقة التنزيل في نافذة **الإعدادات** الخاصة بهذا المعالج.
- يجب أن يمتلك الحساب المستخدم بواسطة نقطة التوزيع للتخويل إمكانية الوصول إلى مورد Admin$ على جميع الأجهزة العميلة.

عرض الإعدادات المحلية للتطبيق وتحريرها

يتيح لك نظام إدارة Kaspersky Security Center بإدارة الإعدادات المحلية للتطبيق عن بُعد على الأجهزة من خلال وحدة تحكم الإدارة.

الإعدادات المحلية للتطبيق هي إعدادات التطبيق المخصصة لجهاز محدد. ويمكنك استخدام Kaspersky Security Center لتعيين الإعدادات المحلية للتطبيق للأجهزة في مجموعات الإدارة.

وتتوفر أوصاف تفصيلية لإعدادات تطبيقات Kaspersky في الأدلة المعنية.

لعرض الإعدادات المحلية لتطبيق ما أو تغييرها:

1. في مساحة عمل المجموعة التي ينتمي إليها الجهاز ذو الصلة، حدد علامة التبويب **الأجهزة**.

2. في نافذة خصائص الجهاز، من القسم **التطبيقات**، حدد التطبيق ذا الصلة.

3. افتح نافذة خصائص التطبيق بالنقر المزدوج فوق اسم التطبيق أو النقر فوق الزر **خصائص**.

تفتح نافذة الإعدادات المحلية للتطبيق المحدد لكي تتمكن من عرض هذه الإعدادات وتحريرها.

يمكنك تغيير قيم الإعدادات التي لم يكن تعديلها محظورًا بواسطة سياسة مجموعة (أي غير المميزة بأيقونة القفل (🔒) في سياسة).

تحديث Kaspersky Security Center والتطبيقات التطبيقات المدارة

يصف هذا القسم الخطوات الواجب عليك اتخاذها لتحديث Kaspersky Security Center والتطبيقات المدارة.

السيناريو: تحديث منتظم لقواعد بيانات Kaspersky وتطبيقاتها

يوفر هذا القسم سيناريو للتحديث المنتظم لقواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. بعد أن تكمل تكوين سيناريو حماية الشبكة، يجب أن تحافظ على موثوقية نظام الحماية للتأكد أن خوادم الإدارة والأجهزة المُدارة تبقى محمية من مختلف التهديدات، مثل الفيروسات وهجمات الشبكة وهجمات التصيد الاحتيالي.

تبقى حماية الشبكة محدثة بالتحديثات المنتظمة لما يلي:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج
- تطبيقات Kaspersky المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

عند إكمالك لهذا السيناريو، يمكنك التأكد مما يلي:

- شبكتك محمية بأحدث برامج Kaspersky، وهذه تشمل مكونات Kaspersky Security Center وتطبيقات الأمان.
- قواعد بيانات مكافحة الفيروسات وقواعد بيانات Kaspersky الأخرى ضرورية للغاية لأمان الشبكة تبقى محدثة.

المتطلبات الأساسية

يجب أن تكون الأجهزة المُدارة متصلة بخادم الإدارة. إذا كانت غير متصلة، فكر في تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات يدويًا أو مباشرةً من خوادم تحديث Kaspersky.

يجب أن يكون خادم الإدارة متصلاً بالإنترنت.

قبل البدء، تأكد من إجرائك لما يلي:

1. نشرت تطبيقات أمان Kaspersky على الأجهزة المُدارة وفق سيناريو نشر تطبيقات Kaspersky عبر Kaspersky Security Center Web Console.

2. أنشأت وكونت جميع السياسات المطلوبة وملفات تعريف السياسة والمهام وفق سيناريو تكوين حماية الشبكة.

3. خصصت كمية مناسبة من نقاط التوزيع وفق عدد الأجهزة المُدارة ومخطط الشبكة.

تحديث قواعد بيانات Kaspersky وتطبيقاته يسري عبر بضعة مراحل:

1 اختيار مخطط تحديث

يوجد عدة مخططات يمكنك استخدامها في تثبيت التحديثات لمكونات Kaspersky Security Center وتطبيقات الأمان. اختر المخطط أو عدة مخططات تلبي متطلبات شبكتك بصورة مثالية.

2 إنشاء مهمة لتنزيل التحديثات إلى مستودع خادم الإدارة

يتم إنشاء هذه المهمة تلقائيًا من خلال معالج البدء السريع في Kaspersky Security Center. إذا لم تشغِّل "المعالج"، قم بإنشاء المهمة الآن.

المهمة مطلوبة لتنزيل التحديثات من خوادم تحديث Kaspersky إلى مستودع خادم الإدارة وكذلك لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج لـ Kaspersky Security Center. بعد تنزيل التحديثات، يمكن نشرها على الأجهزة المُدارة.

إذا كانت شبكتك قد خصصت نقاط التوزيع، يتم تنزيل التحديثات تلقائيًا من مستودع خادم الإدارة إلى مستودعات نقاط التوزيع. في هذه الحالة، تقوم الأجهزة المُدارة المضمّنة في نطاق نقطة التوزيع بتنزيل التحديثات من مستودع نقطة التوزيع بدلاً من مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة
- Kaspersky Security Center Web Console: إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة

3 إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع (اختياري)

يتم تنزيل التحديثات بشكل افتراضي إلى نقاط التوزيع من خادم الإدارة. يمكنك تكوين Kaspersky Security Center لتنزيل التحديثات إلى نقاط التوزيع مباشرةً من خوادم تحديث Kaspersky. ومن الأفضل التنزيل إلى مستودعات نقاط التوزيع إذا كانت تكلفة حركة المرور بين خادم الإدارة ونقاط التوزيع أكثر من حركة المرور بين نقاط التوزيع وخوادم تحديث Kaspersky أو إذا لم يتمتع خادم الإدارة بإمكانية الوصول إلى الإنترنت.

عند تخصيص شبكتك لنقاط التوزيع وعند إنشاء مهمة Download updates to the repositories of distribution points، تقوم نقاط التوزيع بتنزيل التحديثات من خوادم تحديث Kaspersky وليس من مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع
- Kaspersky Security Center Web Console: إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

4 تكوين نقاط التوزيع

عندما تقوم شبكتك بتخصيص نقاط توزيع، تأكد أن خيار **Deploy updates** مفعل في جميع نقاط التوزيع المطلوبة. عندما يكون هذا الخيار معطلاً لنقطة التوزيع، يتم إدراج الأجهزة في نطاق تنزيل تحديثات نقطة التوزيع من مستودع خادم الإدارة.

إذا كنت ترغب في أن تتلقى الأجهزة المُدارة تحديثات من نقاط التوزيع فقط، قم بتفعيل خيار **Distribute files through distribution points only** في سياسة عميل الشبكة.

5 تحسين عملية التحديث باستخدام النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديث أو ملفات diff (اختياري)

يمكنك تحسين عملية التحديث باستخدام النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات (مفعل بشكل افتراضي) أو باستخدام ملفات diff. لكل قطاع شبكة، عليك اختيار ما ستفعله من هاتين الميزتين لأنهما لا يعملان في الوقت نفسه.

عند تفعيل النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات، يقوم عميل الشبكة بتنزيل التحديثات المطلوبة إلى الجهاز المُدار بمجرد تنزيل التحديثات إلى مستودع خادم الإدارة قبل أن يطلب تطبيق الأمان التحديثات. يعزز هذا من موثوقية عملية التحديث. لاستخدام هذه الميزة، قم بتمكين خيار **Download updates and anti-virus databases from Administration Server in advance (recommended)** في سياسة عميل الشبكة.

إذا لم تستخدم النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات، يمكنك تحسين حركة المرور بين خادم الإدارة والأجهزة المُدارة باستخدام ملفات diff. عند تفعيل هذه الميزة، يقوم خادم الإدارة أو نقطة التوزيع بتنزيل ملفات diff بدلاً من كامل ملفات قواعد بيانات Kaspersky أو الوحدات النمطية للبرامج. يصف ملف diff الاختلافات بين نسختين من ملف قاعدة البيانات أو الوحدة النمطية للبرامج. وبالتالي يشغل ملف diff مساحة أقل من ملف كامل. يتسبب هذا في انخفاض حركة المرور بين خادم الإدارة أو نقاط التوزيع والأجهزة المُدارة. لاستخدام هذه الميزة، قم بتفعيل خيار **Download diff files** في خصائص مهمة Download updates to the Administration Server repository و/أو مهمة Download updates to the repositories of distribution points.

تعليمات للمساعدة:

- استخدام ملفات diff لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج
- وحدة تحكم الإدارة: تمكين النموذج غير المتصل بالإنترنت لتنزيل التحديثات وتعطيله
- Kaspersky Security Center Web Console: تمكين النموذج غير المتصل بالإنترنت لتنزيل التحديثات وتعطيله

6 التحقق من التحديثات المُنزّلة (اختياري)

قبل تثبيت التحديثات التي تم تنزيلها، يمكنك التحقق من صحة التحديث من خلال مهمة تحديث التحقق. تعمل هذه المهمة على تشغيل مهام تحديث الجهاز ثم مهام فحص البرامج الضارة التي تم تكوينها عبر الإعدادات الخاصة بمجموعة محددة من أجهزة الاختبار. عند الحصول على نتائج المهمة، يبدأ خادم الإدارة نشر التحديث إلى الأجهزة الباقية أو يحظره.

يمكن إجراء مهمة التحقق من صحة التحديث كجزء من مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، قم بتمكين الخيار **التحقق من صحة التحديثات قبل التوزيع** في وحدة تحكم الإدارة أو خيار **Run update verification** في Kaspersky Security Center Web Console.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: التحقق من التحديثات المُنزّلة
- Kaspersky Security Center Web Console: التحقق من التحديثات المُنزّلة

7 اعتماد ورفض تحديثات البرنامج

بشكل افتراضي، يكون لتحديثات البرامج التي تم تنزيلها حالة غير محددة. يمكنك تغيير الحالة إلى مقبولة أو مرفوضة. يتم تثبيت التحديثات المقبولة دائمًا. إذا تطلب التحديث مراجعة وقبول شروط اتفاقية ترخيص المستخدم النهائي، أنت بحاجة أولاً إلى قبول الشروط. يمكن بعد ذلك نشر التحديث على الأجهزة المُدارة. لا يمكن تثبيت التحديثات غير المحددة إلا على عميل الشبكة ومكونات Kaspersky Security Center الأخرى وفق إعدادات سياسة عميل الشبكة. لن يتم تثبيت التحديثات التي تحدد لها حالة مرفوضة. في حالة وجود تحديث مرفوض لتطبيق قد تم تثبيته مسبقًا، سيحاول Kaspersky Security Center إلغاء تثبيت ذلك التحديث من جميع الأجهزة.

تتوفر إمكانية الموافقة على التحديثات أو رفضها فقط لعميل الشبكة وتطبيقات Kaspersky المُدارة المثبتة على أجهزة العميل المستندة إلى نظام Windows والمستندة إلى نظام Linux. لا يتم دعم التحديث السلس لخادم الإدارة وKaspersky Security Center Web Console والمكونات الإضافية لإدارة الويب.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: الموافقة على تحديثات البرامج ورفضها
- Kaspersky Security Center Web Console: الموافقة على تحديثات البرامج ورفضها

8 تكوين التثبيت التلقائي للتحديثات والتصحيحات المخصصة لمكونات Kaspersky Security Center

يتم تلقائيًا تثبيت التحديثات والتصحيحات المنزلة لعميل الشبكة ومكونات Kaspersky Security Center الأخرى. إذا تركت خيار **Automatically install applicable updates and patches for components that have the Undefined status** مفعلاً في خصائص عميل الشبكة، عندها سيتم جميع التحديثات تلقائيًا بعد أن يتم تنزيلها إلى المستودع (أو عدة مستودعات). إذا تم تعطيل هذا الخيار، فسوف يتم تثبيت تصحيحات Kaspersky التي تم تنزيلها وتعيين الحالة غير محددة لها فقط بعد أن تقوم بتغيير حالتها إلى معتمدة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center
- Kaspersky Security Center Web Console: تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center

9 **تثبيت التحديثات لخادم الإدارة**

تحديثات البرامج لخادم الإدارة لا تعتمد على حالات التحديث. لم يتم تثبيتها تلقائيًا ويجب أن تتم الموافقة عليها بشكل مبدئي من قبل المسؤول في تبويب **المراقبة** في وحدة تحكم الإدارة (**خادم الإدارة** ← **المراقبة**) أو في قسم **Notifications** في Kaspersky Security Center Web Console (**Monitoring & reporting** ← **Notifications**). يجب أن يقوم المدير بعد ذلك بتشغيل تثبيت التحديثات بشكل صريح.

10 **تكوين التثبيت التلقائي لتحديثات تطبيقات الأمان.**

قم بإنشاء مهام التحديث للتطبيقات المُدارة لتوفير التحديثات في الوقت المناسب للتطبيقات والوحدات النمطية للبرامج وقواعد بيانات Kaspersky، بما في ذلك قواعد بيانات مكافحة الفيروسات. لضمان التحديثات في الوقت المناسب، نوصي بتحديد خيار **When new updates are downloaded to the repository** أثناء تكوين جدول المهام.

إذا كانت شبكتك تتضمن أجهزة IPv6 فقط وترغب في تحديث تطبيقات الأمان المثبتة على هذه الأجهزة بانتظام، فتأكد من تثبيت خادم الإدارة (الإصدار الأقدم من 13.2) وعميل الشبكة (الإصدار الأقدم من 13.2) على الإدارة الأجهزة.

بشكل افتراضي، لا يتم تثبيت تحديثات Kaspersky Endpoint Security for Windows وKaspersky Endpoint Security for Linux إلا بعد أن تغير حالة التحديث إلى مقبولة. يمكنك تغيير إعدادات التحديث في مهمة التحديث.

إذا تطلب التحديث مراجعة وقبول شروط اتفاقية ترخيص المستخدم النهائي، أنت بحاجة أولاً إلى قبول الشروط. يمكن بعد ذلك نشر التحديث على الأجهزة المُدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: التثبيت التلقائي لتحديثات Kaspersky Endpoint Security على الأجهزة
- Kaspersky Security Center Web Console: التثبيت التلقائي لتحديثات Kaspersky Endpoint Security على الأجهزة

النتائج

عند إكمال السيناريو، يتم تكوين Kaspersky Security Center لتحديث قواعد بيانات Kaspersky وتطبيقات Kaspersky المثبتة بعد تنزيل التحديثات إلى مستودع خادم الإدارة أو مستودعات نقاط التوزيع. يمكنك بعد ذلك التقدم إلى مراقبة حالة الشبكة.

حول تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات

للتأكد من تحديث حماية خوادم الإدارة والأجهزة المُدارة لديك، يجب عليك توفير تحديثات لما يلي في الوقت المحدد:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج

قبل تنزيل قواعد بيانات Kaspersky ووحدات البرامج النمطية، يتحقق Kaspersky Security Center من إمكانية الوصول إلى خوادم Kaspersky. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة. يُعد ذلك ضروريًا للتأكد من تحديث قواعد بيانات مكافحة الفيروسات والحفاظ على مستوى الأمان للأجهزة المُدارة.

- تطبيقات Kaspersky المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

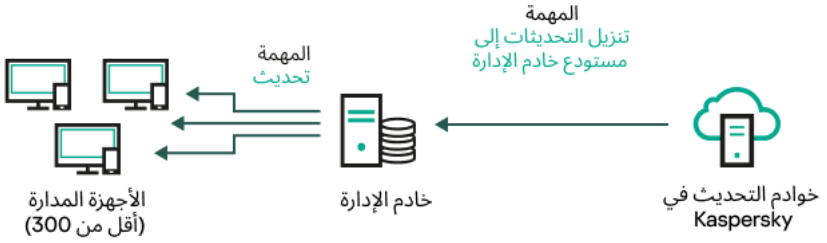
يتيح لك Kaspersky Security Center تحديث عميل الشبكة وتطبيقات Kaspersky المثبتة على أجهزة العميل المستندة إلى Windows وLinux تلقائيًا. لا يتم دعم التحديث السلس لخادم الإدارة وKaspersky Security Center Web Console والمكونات الإضافية لإدارة الويب. لتحديث هذه المكونات، يجب عليك تنزيل أحدث الإصدارات من موقع ويب Kaspersky ، ثم تثبيتها يدويًا.

بناءً على تكوين شبكتك، يمكنك استخدام المخططات التالية الخاصة بتنزيل التحديثات اللازمة وتوزيعها للأجهزة المُدارة:

- باستخدام مهمة واحدة: تنزيل التحديثات إلى مستودع خادم الإدارة
- باستخدام مهمتين:
  - مهمة تنزيل التحديثات إلى مستودع خادم الإدارة
  - مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع
- يدويًا من خلال مجلد محلي أو مجلد مشترك أو خادم FTP
- مباشرة من خوادم تحديث Kaspersky إلى Kaspersky Endpoint Security على الأجهزة المُدارة
- من خلال مجلد محلي أو شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة

في هذا المخطط، يقوم Kaspersky Security Center بتنزيل التحديثات من خلال مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وفي الشبكات الصغيرة التي تحتوي على أقل من 300 جهاز مُدار في مقطع شبكة واحد أو أقل من 10 أجهزة مُدارة في كل مقطع للشبكة، يتم توزيع التحديثات إلى الأجهزة المُدارة مباشرة من مستودع خادم الإدارة (انظر الشكل أدناه).

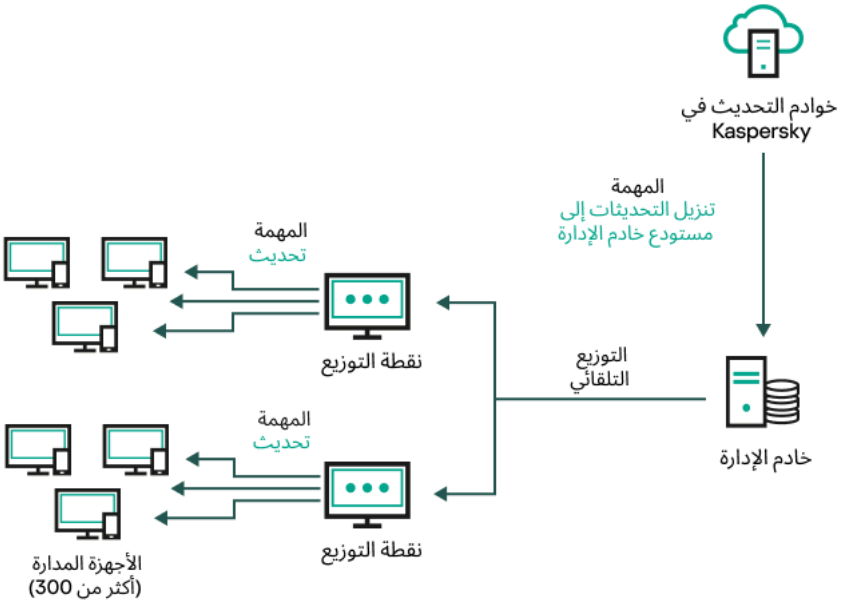


التحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة دون نقاط توزيع

يتصل خادم الإدارة افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة لاستخدام بروتوكول HTTP بدلاً من HTTPS.

إذا كانت شبكتك تحتوي على أكثر من 300 جهاز مُدار في مقطع شبكة واحد أو إذا كانت شبكتك تتكون من مقاطع شبكات متعددة تحتوي على أكثر من 9 أجهزة مُدارة في كل مقطع شبكة، فنوصيك باستخدام نقاط التوزيع لنشر التحديثات إلى الأجهزة المُدارة (انظر الشكل أدناه). وتقلل نقاط التوزيع من التحميل الموجود على خادم الإدارة ويعمل على تحسين حركة المرور بين خادم الإدارة والأجهزة المُدارة. يمكنك حساب عدد نقاط التوزيع لمطلوبة لشبكتك وتكوينها.

وفي هذا المخطط، يتم تنزيل التحديثات تلقائيًا من مستودع خادم الإدارة إلى مستودعات نقاط التوزيع. تقوم الأجهزة المُدارة المضمّنة في نطاق نقطة التوزيع بتنزيل التحديثات من مستودع نقطة التوزيع بدلاً من مستودع خادم الإدارة.



التحديث باستخدام مهمة تنزيل التحديثات إلى مستودع خادم الإدارة مع نقاط توزيع

عند اكتمال المهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يتم تنزيل التحديثات التالية إلى مستودع خادم الإدارة:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج لـ Kaspersky Security Center

  يتم تثبيت هذه التحديثات تلقائيًا.

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج لتطبيقات الأمان على الأجهزة المُدارة

  يتم تثبيت هذه التحديثات من خلال مهمة تحديث لتطبيق Kaspersky Endpoint Security for Windows.

- تحديثات خادم الإدارة

  لا يتم تثبيت هذه التحديثات تلقائيًا. ويجب على المسؤول الموافقة صراحة على تثبيت التحديثات وتشغيلها.

> تلزم حقوق المسؤول المحلي لتثبيت التصحيحات على خادم الإدارة.

- تحديثات مكونات Kaspersky Security Center

  يتم افتراضيًا تثبيت هذه التحديثات تلقائيًا. ويمكنك تغيير الإعدادات في سياسة عميل الشبكة.

- تحديثات تطبيقات الأمن

  بشكل افتراضي، لا يثبت Kaspersky Endpoint Security for Windows إلا التحديثات التي توافق عليها. (يمكنك الموافقة على التحديثات عبر وحدة تحكم الإدارة أو عبر Kaspersky Security Center Web Console). ويتم تثبيت التحديثات من خلال المهمة تحديث ويمكن تكوينها في خصائص هذه المهمة.

> لا تتوفر مهمة تنزيل التحديثات إلى مستودع مهمة خادم الإدارة على خوادم الإدارة الافتراضية. مستودع خادم الإدارة الافتراضي يعرض التحديثات المنزّلة على خادم الإدارة الرئيسي.

ويمكنك تكوين التحديثات للتحقق من التشغيل والأخطاء بمجموعة من الأجهزة الاختبارية. وفي حالة نجاح عملية التحقق، يتم توزيع التحديثات إلى الأجهزة المُدارة الأخرى.

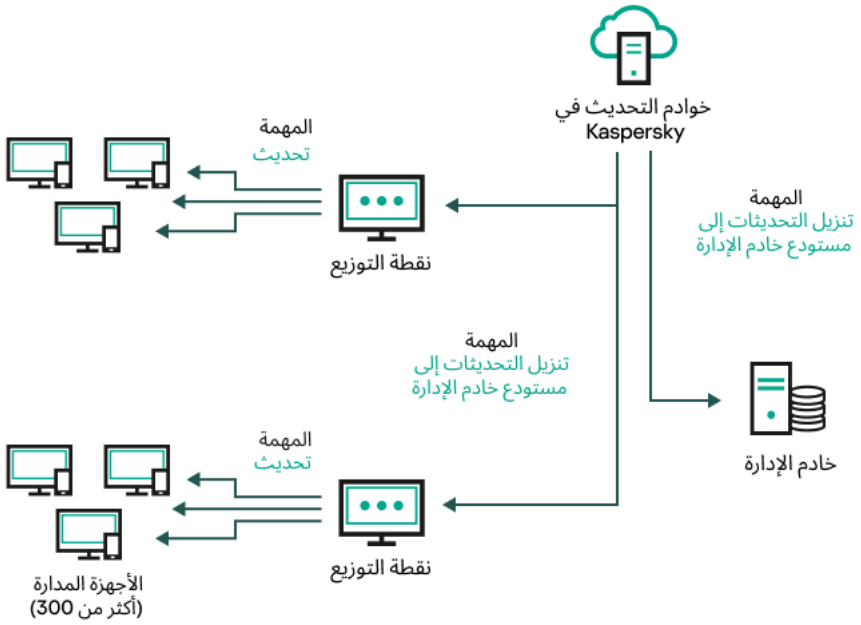
يتطلب كل تطبيق من تطبيقات Kaspersky تحديثات من خادم الإدارة. قام خادم الإدارة بتجميع تلك الطلبات وتنزيل التحديثات التي تم طلبها من قبل التطبيق فقط. يضمن هذا عدم تنزيل نفس التحديثات عدة مرات وعدم تنزيل التحديثات غير الضرورية أبدًا. عند تشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يرسل خادم الإدارة المعلومات التالية إلى خوادم تحديث Kaspersky تلقائيًا لضمان تنزيل إصدارات ذات صلة بقواعد بيانات Kaspersky والوحدات النمطية للبرامج:

- معرف التطبيق وإصداره
- معرف تثبيت التطبيق
- معرف المفتاح المفعل
- معرف تشغيل تنزيل التحديثات إلى مستودع مهمة خادم الإدارة

لا تحتوي أيٌ من المعلومات المنقولة على تفاصيل شخصية أو بيانات سرية أخرى. يحمي AO Kaspersky Lab المعلومات وفقًا للمتطلبات التي ينص عليها القانون.

باستخدام المهمتين: المهمة تنزيل التحديثات إلى مستودع خادم الإدارة والمهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع

يمكنك تنزيل التحديثات إلى مستودعات نقاط التوزيع مباشرة من خوادم تحديث Kaspersky بدلاً من مستودع خادم الإدارة، ثم توزيع التحديثات على الأجهزة المُدارة (انظر الشكل أدناه). ومن الأفضل التنزيل إلى مستودعات نقاط التوزيع إذا كانت تكلفة حركة المرور بين خادم الإدارة ونقاط التوزيع أكثر من حركة المرور بين نقاط التوزيع وخوادم تحديث Kaspersky أو إذا لم يتمتع خادم الإدارة بإمكانية الوصول إلى الإنترنت.



تحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة والمهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع

يتصل خادم الإدارة ونقاط التوزيع افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة و/أو نقاط التوزيع لاستخدام بروتوكول HTTP بدلاً من HTTPS.

لتنفيذ هذا المخطط، قم بإنشاء مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيعبالإضافة إلى مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وبعد ذلك، ستقوم نقاط التوزيع بتنزيل التحديثات من خوادم تحديث Kaspersky وليس من مستودع خادم الإدارة.

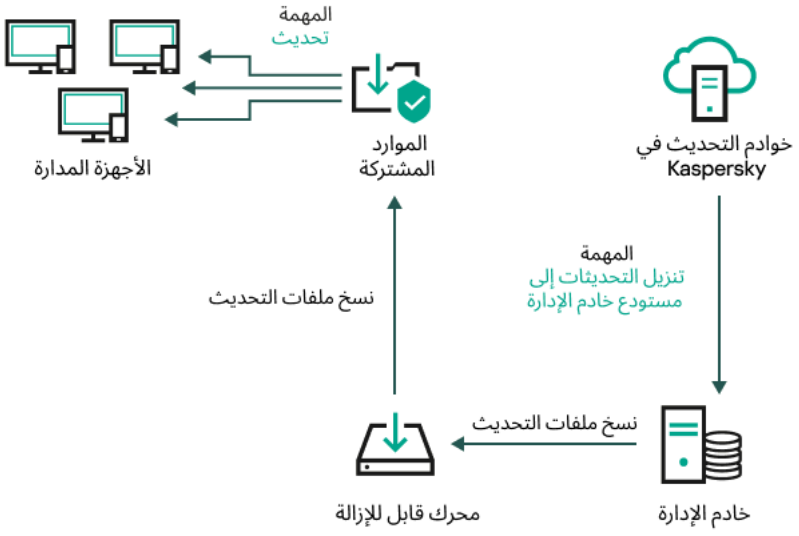
لا يمكن لأجهزة نقاط التوزيع التي تعمل بنظام macOS تنزيل التحديثات من خوادم تحديث Kaspersky.

في حالة وجود جهاز أو أكثر من الأجهزة التي تعمل بنظام macOS داخل نطاق مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع ، تكون المهمة مكتملة مع إظهار حالة فشل ، حتى إذا تم إكمالها بنجاح على جميع أجهزة Windows.

كما يلزم توفير مهمة تنزيل التحديثات إلى مستودع خادم الإدارة في هذا المخطط، نظرًا لاستخدام هذه المهمة في تنزيل قواعد بيانات Kaspersky والوحدات النمطية للبرامج في Kaspersky Security Center.

يدويًا من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

إذا لم تتمتع الأجهزة العميلة باتصال بخادم الإدارة، يمكنك استخدام مجلد محلي أو مورد مشترك كمصدر لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. وفي هذا المخطط، تحتاج إلى نسخ التحديثات اللازمة من مستودع خادم الإدارة إلى محرك الأقراص القابل للإزالة ونسخ التحديثات إلى المجلد المحلي أو المورد المشترك المحدد كمصدر تحديث في إعدادات Kaspersky Endpoint Security (انظر الشكل أدناه).



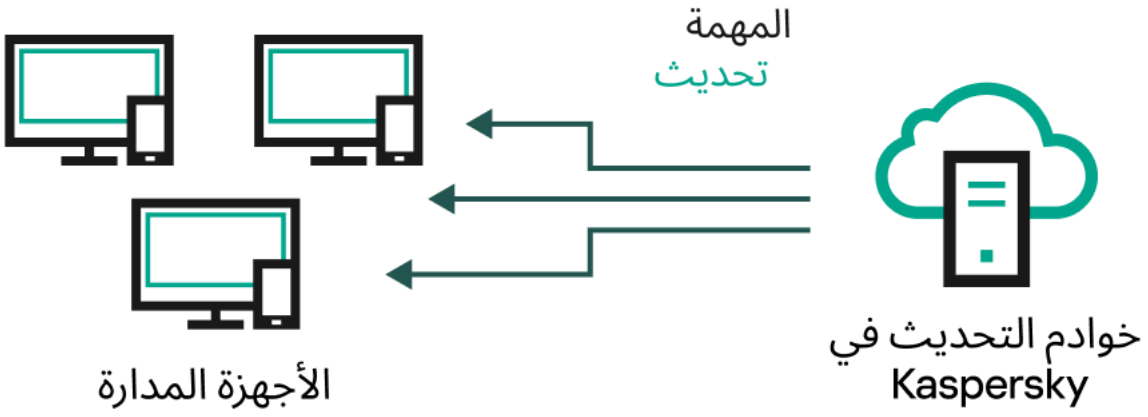
التحديث من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

لمزيد من المعلومات حول مصادر التحديثات في Kaspersky Endpoint Security ، راجع المساعدة التالية:

- تعليمات Kaspersky Endpoint Security for Windows
- دعم Kaspersky Endpoint Security for Linux

مباشرة من خوادم تحديث Kaspersky إلى Kaspersky Endpoint Security على الأجهزة المُدارة

على الأجهزة المُدارة، يمكنك تكوين Kaspersky Endpoint Security لتلقي التحديثات مباشرة من خوادم تحديث Kaspersky (انظر الشكل أدناه).



تحديث تطبيقات الأمن مباشرة من خوادم تحديث Kaspersky

في هذا المخطط، لا يستخدم تطبيق الأمن المستودعات المتوفرة من Kaspersky Security Center. ولتلقي التحديثات مباشرة من خوادم تحديث Kaspersky، حدد خوادم تحديث Kaspersky كمصدر تحديث في واجهة تطبيق الأمان. لمزيد من المعلومات حول هذه الإعدادات، راجع المساعدة التالية:

- تعليمات Kaspersky Endpoint Security for Windows
- دعم Kaspersky Endpoint Security for Linux

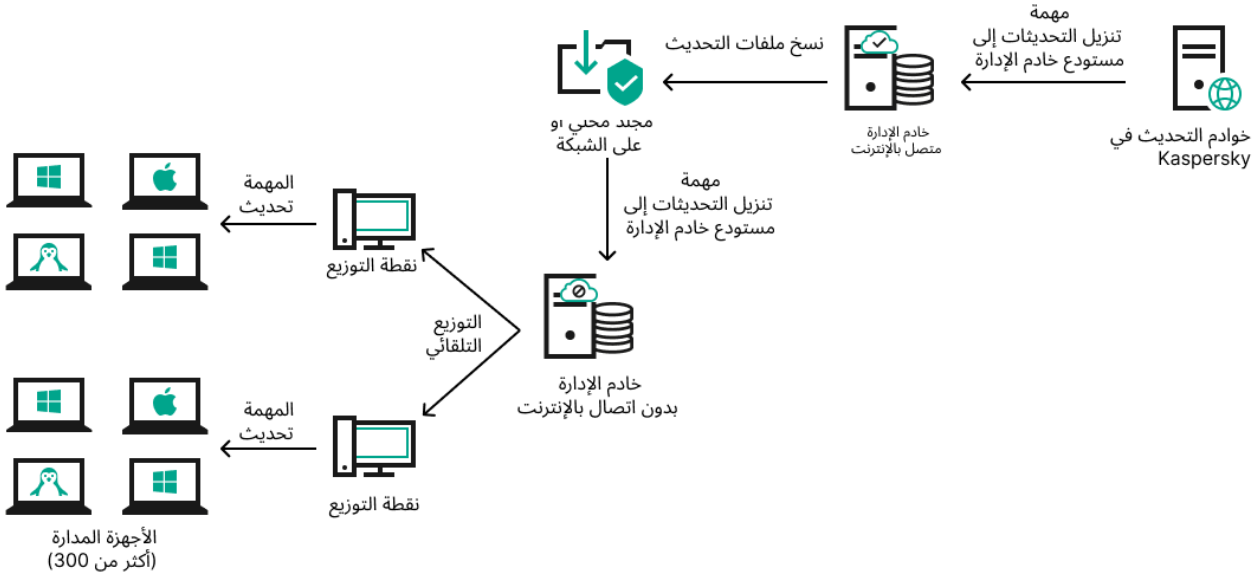
من خلال مجلد محلي أو شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت، فيمكنك تكوين مهمة تنزيل التحديثات إلى مستودع خادم الإدارة لتنزيل التحديثات من مجلد محلي أو مجلد شبكة. في هذه الحالة، يجب عليك نسخ ملفات التحديث المطلوبة إلى المجلد المحدد من وقت لآخر. على سبيل المثال، يمكنك نسخ ملفات التحديث المطلوبة من أحد المصادر التالية:

- خادم الإدارة الذي لديه اتصال بالإنترنت (انظر الشكل أدناه)

  نظرًا لأن خادم الإدارة يقوم بتنزيل التحديثات التي تطلبها تطبيقات الأمان فقط، فيجب أن تتطابق مجموعات تطبيقات الأمان التي تتم إدارتها بواسطة خوادم الإدارة – تلك التي تحتوي على اتصال بالإنترنت وتلك التي لا تحتوي على ذلك –.

إذا كان خادم الإدارة الذي تستخدمه لتنزيل التحديثات يحتوي على الإصدار 13.2 أو إصدار أقدم، فافتح خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، ثم قم بتمكين خيار **تنزيل التحديثات باستخدام النظام القديم** .



التحديث من خلال مجلد محلي أو مجلد شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

- Kaspersky Update Utility

نظرًا لأن هذه الأداة تستخدم النظام القديم لتنزيل التحديثات، افتح خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، ثم قم بتمكين خيار **تنزيل التحديثات باستخدام النظام القديم** .

حول استخدام ملفات diff لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج

عندما يقوم Kaspersky Security Center بتنزيل التحديثات من خوادم تحديث Kaspersky، فإنه يعمل على تحسين حركة المرور باستخدام ملفات diff. يمكنك أيضًا تمكين استخدام ملفات diff بواسطة الأجهزة (خوادم الإدارة، ونقاط التوزيع، والأجهزة العميلة) التي تستقبل التحديثات من الأجهزة الأخرى على شبكتك.

حول ميزة تنزيل ملفات diff

يصف ملف diff الاختلافات بين نسختين من ملف قاعدة البيانات أو الوحدة النمطية للبرامج. إن استخدام ملفات diff يحفظ حركة المرور داخل شبكة شركتك لأن ملفات diff تحتل مساحة أقل من الملفات الكاملة لقواعد البيانات والوحدات النمطية للبرامج. إذا تم تمكين ميزة تنزيل ملفات تفاضلية على خادم الإدارة أو نقطة توزيع، فإنه يتم حفظ الملفات التفاضلية على خادم الإدارة هذا أو نقطة التوزيع. ونتيجة لذلك، يمكن للأجهزة التي تأخذ التحديثات من خادم الإدارة أو نقطة التوزيع هذه استخدام ملفات diff المحفوظة لتحديث قواعد البيانات والوحدات النمطية للبرامج الخاصة بها.

لتحسين استخدام ملفات diff، نوصيك بمزامنة جدول تحديث الأجهزة مع جدول تحديث خادم الإدارة أو نقطة التوزيع التي تأخذ الأجهزة منها التحديثات. ومع ذلك، يمكن حفظ حركة المرور حتى إذا تم تحديث الأجهزة بعدد مرات أقل من خادم الإدارة أو نقطة التوزيع التي تأخذ الأجهزة منه التحديثات.

يمكن تمكين ميزة تنزيل ملفات diff فقط على خوادم الإدارة ونقاط التوزيع للإصدارات بدءًا من الإصدار 11. لحفظ ملفات diff على خوادم الإدارة ونقاط توزيع الإصدارات القديمة، قم بترقيتها إلى الإصدار 11 أو أحدث.

ميزة تنزيل ملفات diff غير متوافقة مع الوضع "غير متصل بالإنترنت" الخاص بتنزيل التحديثات. هذا الأمر يعني أن عملاء الشبكة الذين يستخدمون الوضع غير متصل بالإنترنت الخاص بتنزيل التحديثات لا يقومون بتنزيل ملفات diff حتى إذا تم تمكين ميزة تنزيل ملفات diff على خادم الإدارة أو نقطة التوزيع التي توفر تحديثات لعملاء الشبكة هؤلاء.

لا تستخدم نقاط التوزيع الإرسال المتعدد لـ IP من أجل التوزيع التلقائي لملفات diff.

تمكين ميزة تنزيل ملفات diff

المتطلبات الأساسية

المتطلبات الأساسية لهذا السيناريو كالتالي:

- تمت ترقية خوادم الإدارة ونقاط التوزيع إلى الإصدار 11 أو أحدث.
- تم تعطيل الوضع "غير متصل بالإنترنت" الخاص بتنزيل التحديثات في إعدادات سياسة عميل الشبكة.

المراحل

1. **تمكين الميزة على خادم الإدارة**

   قم بتمكين الميزة في إعدادات تنزيل التحديثات إلى مستودع مهمة خادم الإدارة.

2. **تمكين الميزة لنقطة توزيع**

   قم بتمكين الميزة لنقطة التوزيع التي تستقبل التحديثات عن طريق مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع.

   ثم قم بتمكين الميزة لنقطة التوزيع التي تستقبل التحديثات من خادم الإدارة.

   يتم تمكين الميزة في إعدادات سياسة عميل الشبكة و—إذا تم تعيين نقاط التوزيع يدويًا، وإذا كنت تريد تجاوز إعدادات السياسة—في قسم **نقاط التوزيع** في خصائص خادم الإدارة.

للتحقق من أنه تم تمكين ميزة تنزيل ملفات diff بنجاح، يمكنك قياس حركة المرور الداخلية قبل وبعد تنفيذ السيناريو.

إنشاء مهمة لتنزيل التحديثات إلى مستودع خادم الإدارة

يتم إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة الخاص بخادم الإدارة تلقائيًا بواسطة معالج البدء السريع في Kaspersky Security Center. يمكنك إنشاء مهمة واحدة فقط لتنزيل التحديثات إلى مستودع مهمة خادم الإدارة. ولهذا السبب، يمكنك إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة فقط في حالة إزالة هذه المهمة من قائمة مهام خادم الإدارة.

لإنشاء تنزيل تحديثات إلى مستودع مهمة خادم الإدارة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. بدء إنشاء المهمة بإحدى الطرق التالية:

- من قائمة سياق المجلد **المهام** في شجرة وحدة التحكم، حدد **جديد** ← **مهمة**.
- في مساحة عمل المجلد **المهام**، انقر على زر **إنشاء مهمة**.

سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. في صفحة المعالج **تحديد نوع المهمة**، وحدد **تنزيل التحديثات إلى مستودع خادم الإدارة**.

4. في صفحة **إعدادات** المعالج، حدد إعدادات المهمة كما يلي:

- **مصادر التحديثات**

ويمكن استخدام الموارد التالية كمصدر للتحديثات لخادم الإدارة:

- خوادم تحديث Kaspersky

خوادم HTTP(S) في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق. يتصل خادم الإدارة افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة لاستخدام بروتوكول HTTP بدلاً من HTTPS.

يتم تحديده بصورة افتراضية.

- خادم الإدارة الأساسي

ينطبق هذا المصدر على المهام التي يتم إنشاؤها لخادم الإدارة الثانوي أو الافتراضي.

- المجلد المحلي أو مجلد الشبكة

مجلد شبكة أو مجلد محلي يحتوي على آخر التحديثات. يمكن أن يكون مجلد الشبكة إما خادم FTP أو خادم HTTP أو مشاركة SMB. إذا تطلب مجلد الشبكة المصادقة، فسيتم دعم بروتوكول SMB فقط. عند تحديد مجلد محلي، يجب عليك تحديد مجلد موجود على الجهاز المُثبت عليه خادم الإدارة.

> يجب أن يحتوي مجلد الشبكة أو خادم FTP أو HTTP المستخدم من قبل مصدر التحديث على بنية مجلدات (مع تحديثات) تتطابق مع البنية التي تم إنشاؤها عند استخدام خوادم تحديث Kaspersky.

- **إعدادات أخرى**:

- **فرض التحديث لخوادم الإدارة الثانوية**

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة بتشغيل مهام التحديث على خوادم الإدارة الثانوية بمجرد أن يتم تنزيل التحديثات الجديدة. تبدأ مهام التحديث باستخدام مصدر التحديث الذي تم تكوينه في خصائص المهمة على خوادم الإدارة الثانوية.

إذا تم تعطيل هذا الخيار، فستبدأ مهام التحديث على خوادم الإدارة الثانوية وفقًا لجداولها الزمنية.

يتم تعطيل هذا الخيار افتراضيًا.

- **نسخ التحديثات التي تم تنزيلها إلى مجلدات إضافية**

بعد تلقي خادم الإدارة للتحديثات، يقوم بنسخها إلى المجلدات المحددة. استخدم هذا الخيار في حال رغبت في إدارة توزيع التحديثات يدويًا على الشبكة الخاصة بك.

على سبيل المثال، قد ترغب في استخدام هذا الخيار في الموقف التالي: تتكون شبكة المؤسسة الخاصة بك من العديد من الشبكات الفرعية المستقلة، ولا تمتلك الأجهزة على كل شبكة فرعية إمكانية الوصول إلى الشبكات الفرعية الأخرى. ومع ذلك فإن جميع الأجهزة في جميع الشبكات الفرعية تمتلك إمكانية الوصول إلى مشاركة الشبكة العامة. في هذه الحالة، قم بتعيين خادم الإدارة في واحدة من الشبكات الفرعية لتنزيل التحديثات من خوادم تحديث Kaspersky، وقم بتمكين هذا الخيار ثم حدد مشاركة الشبكة هذه. من تنزيل التحديثات إلي مستودع المهام لخوادم إدارة أخرى، قم بتحديد نفس مشاركة الشبكة كمصدر تحديث.

إذا حددت نسخ التحديثات التي تم تنزيلها إلى مجلد محلي، فيجب عليك تحديد مجلد على الجهاز الذي تم تثبيت خادم الإدارة عليه. ويعتمد المسار إلى المجلد على نظام تشغيل الجهاز. ونظرًا لوجود المجلد المحلي على خادم الإدارة المستند إلى نظام Linux، فيجب عليك تحديد مسار POSIX، على سبيل المثال: /path/to/dir.

عند تحديد مجلد شبكة موجود على خادم الإدارة المستند إلى نظام Linux، يجب عليك التأكد من إمكانية الوصول إلى مجلد الشبكة مسبقًا من الجهاز المُثبت عليه خادم الإدارة عن طريق تحميل المجلد. ويتم تنفيذ الوصول إلى المجلد باستخدام بروتوكول SMB.

يتم تعطيل هذا الخيار افتراضيًا.

- **لا تفرض تحديث الأجهزة وخوادم الإدارة الثانوية إلا عند اكتمال النسخ**

تبدأ مهام تنزيل التحديثات على الأجهزة العميلة وخوادم الإدارة الثانوية فقط بعد نسخ تلك التحديثات من مجلد التحديث الرئيسي إلى مجلدات التحديث الإضافية.

يجب تمكين هذا الخيار إذا كانت الأجهزة العميلة وخوادم الإدارة الثانوية تقوم بتنزيل تحديثات من مجلدات شبكة إضافية.

يتم تعطيل هذا الخيار افتراضيًا.

- **تنزيل التحديثات باستخدام النظام القديم**

بدءًا من الإصدار 14، يقوم Kaspersky Security Center بتنزيل تحديثات قواعد البيانات ووحدات البرامج باستخدام النظام الجديد. لكي يقوم التطبيق بتنزيل التحديثات باستخدام النظام الجديد، يجب أن يحتوي مصدر التحديث على ملفات تحديث ببيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث ببيانات أولية متوافقة مع النظام القديم فقط، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم**. خلاف ذلك، ستفشل مهمة تنزيل التحديث.

على سبيل المثال، يجب تمكين هذا الخيار عند تحديد مجلد محلي أو مجلد شبكة كمصدر تحديث، ويتم تنزيل ملفات التحديث الموجودة في هذا المجلد بواسطة أحد التطبيقات التالية:

- Kaspersky Update Utility

تقوم هذه الأداة بتنزيل التحديثات باستخدام النظام القديم.

- Kaspersky Security Center 13.2 أو إصدار سابق

على سبيل المثال، خادم الإدارة 1 ليس به اتصال بالإنترنت. في هذه الحالة، يمكنك تنزيل التحديثات باستخدام خادم الإدارة 2 الذي يحتوي على اتصال بالإنترنت، ثم وضع التحديثات على مجلد محلي أو مجلد شبكة لاستخدامه كمصدر تحديث لخادم الإدارة 1. إذا كان خادم الإدارة 2 يحتوي على الإصدار 13.2 أو إصدار أقدم، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم** في مهمة خادم الإدارة 1.

يتم تعطيل هذا الخيار افتراضيًا.

5. في صفحة **تكوين جدول المهمة** للمعالج، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.
  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

6. في صفحة المعالج **حدد اسم المهمة**، حدد اسم المهمة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

7. في صفحة **إنهاء عملية إنشاء المهمة** في المعالج، انقر على زر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

بعد انتهاء المعالج، يظهر **تنزيل التحديثات إلى مستودع خادم الإدارة** في قائمة مهام خادم الإدارة في مساحة العمل.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عندما ينفذ خادم الإدارة مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يتم تنزيل تحديثات قواعد البيانات والوحدات النمطية للبرنامج من مصدر التحديثات وتخزينها في مجلد خادم الإدارة المشترك. إذا قمت بإنشاء هذه المهمة لإحدى مجموعات الإدارة، فسيتم تطبيقها فقط على عملاء الشبكة المحددين في مجموعة الإدارة المحددة.

يتم توزيع التحديثات على الأجهزة العميلة وخوادم الإدارة الثانوية من المجلد المشترك لخادم الإدارة.

إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

لا يمكن لأجهزة نقاط التوزيع التي تعمل بنظام macOS تنزيل التحديثات من خوادم تحديث Kaspersky.

في حالة وجود جهاز أو أكثر من الأجهزة التي تعمل بنظام macOS داخل نطاق مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع ، تكون المهمة مكتملة مع إظهار حالة فشل ، حتى إذا تم إكمالها بنجاح على جميع أجهزة Windows.

يمكنك إنشاء مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع لمجموعة إدارة. سيتم تشغيل هذه المهمة لنقاط التوزيع المضمنة في مجموعة الإدارة المحددة.

يمكنك استخدام هذه المهمة على سبيل المثال إذا كانت حركة المرور بين خادم الإدارة ونقطة (نقاط) التوزيع أكثر تكلفة من حركة المرور بين نقطة (نقاط) التوزيع وخوادم تحديث Kaspersky أو إذا لم يكن لدى خادم الإدارة الخاص بك اتصال بالإنترنت. إذا كانت نقطة التوزيع تتصل بالإنترنت باستخدام خادم وكيل، فيجب عليك تحديد الإعدادات المقابلة في سياسة عميل الشبكة.

لإنشاء مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط توزيع مجموعة إدارة محددة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. في مساحة عمل هذا المجلد، انقر على الزر **مهمة جديدة**.

سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. في صفحة المعالج **تحديد نوع المهمة**، حدد القسم **Kaspersky Security Center Administration Server** وقم بتوسيع المجلد **خيارات متقدمة**، ثم حدد المهمة **تنزيل التحديثات إلى مستودعات نقاط التوزيع**.

4. في صفحة **إعدادات** المعالج، حدد إعدادات المهمة كما يلي:

- **مصادر التحديثات**

يمكن استخدام الموارد التالية كمصدر لتحديثات نقطة التوزيع:

- خوادم تحديث Kaspersky

خوادم (S)HTTP في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق.

ويتم تحديد هذا الخيار بصورة افتراضية.

- المجلد المحلي أو مجلد الشبكة

مجلد شبكة أو مجلد محلي يحتوي على آخر التحديثات. يمكن أن يكون مجلد الشبكة إما خادم FTP أو خادم HTTP أو مشاركة SMB. إذا تطلب مجلد الشبكة المصادقة، فسيتم دعم بروتوكول SMB فقط. عند تحديد مجلد محلي، يجب عليك تحديد مجلد موجود على الجهاز المُثبت عليه خادم الإدارة.

يجب أن يحتوي مجلد الشبكة أو خادم FTP أو HTTP المستخدم من قبل مصدر التحديث على بنية مجلدات (مع تحديثات) تتطابق مع البنية التي تم إنشاؤها عند استخدام خوادم تحديث Kaspersky.

- **مجلد لتخزين التحديثات**

المسار إلى المجلد المحدد لتخزين التحديثات المحفوظة. يمكنك نسخ مسار المجلد المحدد إلى الحافظة. لا يمكنك تغيير المسار إلى مجلد محدد لمهمة جماعية.

- **تنزيل التحديثات باستخدام النظام القديم**

بدءًا من الإصدار 14، يقوم Kaspersky Security Center بتنزيل تحديثات قواعد البيانات ووحدات البرامج باستخدام النظام الجديد. لكي يقوم التطبيق بتنزيل التحديثات باستخدام النظام الجديد، يجب أن يحتوي مصدر التحديث على ملفات تحديث ببيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث ببيانات أولية متوافقة مع النظام القديم فقط، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم**. خلاف ذلك، ستفشل مهمة تنزيل التحديث.

على سبيل المثال، يجب تمكين هذا الخيار عند تحديد مجلد محلي أو مجلد شبكة كمصدر تحديث، ويتم تنزيل ملفات التحديث الموجودة في هذا المجلد بواسطة أحد التطبيقات التالية:

- Kaspersky Update Utility

تقوم هذه الأداة بتنزيل التحديثات باستخدام النظام القديم.

- Kaspersky Security Center 13.2 أو إصدار سابق

على سبيل المثال، تم تكوين نقطة توزيع لأخذ التحديثات من مجلد محلي أو مجلد شبكة. في هذه الحالة، يمكنك تنزيل التحديثات باستخدام خادم إدارة متصل بالإنترنت، ثم وضع التحديثات للمجلد المحلي في نقطة التوزيع. إذا كان خادم الإدارة يحتوي على الإصدار 13.2 أو إصدار أقدم ، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم** في مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع.

يتم تعطيل هذا الخيار افتراضيًا.

5. في صفحة المعالج **تحديد مجموعة الإدارة**، وانقر فوق **استعراض** وقم بتحديد مجموعة الإدارة التي يتم تطبيق المهمة عليها.

6. في صفحة **تكوين جدول المهمة** للمعالج، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

7. في صفحة المعالج **حدد اسم المهمة**، حدد اسم المهمة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

8. في صفحة **إنهاء عملية إنشاء المهمة** في المعالج، انقر على زر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

عندما ينتهي المعالج من عمليته، يظهر **تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع** في قائمة مهام عميل الشبكة في مجموعة الإدارة المستهدفة وفي مساحة العمل **المهام** بوحدة التحكم.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عند تنفيذ مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع، يتم تنزيل تحديثات قواعد البيانات والوحدات النمطية للبرنامج من مصدر التحديث ويتم تخزينها في المجلد المشترك. سيتم استخدام التحديثات التي تم تنزيلها فقط بواسطة نقاط التوزيع المضمنة في مجموعة الإدارة المحددة وتلك التي لم يتم تعيين مهمة تنزيل تحديث لها بشكل صريح.

من النافذة خصائص خادم الإدارة، في الجزء **الأقسام**، حدد **نقاط التوزيع**. في خصائص كل نقطة توزيع، في القسم **تحديث المصدر**، يمكنك تحديد مصدر التحديث (**الاستعادة من خادم الإدارة** أو **استخدام مهمة فرض تنزيل التحديثات**). بشكل افتراضي، يتم تحديد الخيار **الاستعادة من خادم الإدارة** لنقطة التوزيع التي يتم تعيينها يدويًا أو تلقائيًا. ستستخدم نقاط التوزيع هذه نتائج مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع.

تحدد خصائص كل نقطة توزيع مجلد الشبكة الذي تم إعداده لها بشكل فردي. قد تتنوع أسماء المجلدات حسب نقاط التوزيع المختلفة. لهذا السبب، لا نوصيك بتغيير مجلد الشبكة في خصائص المهمة إذا تم إنشاء المهمة لمجموعة من الأجهزة.

يمكنك تغيير مجلد الشبكة الذي يحتوي على تحديثات من خصائص مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع إذا كنت تقوم بإنشاء مهمة محلية لجهاز ما.

تكوين تنزيل التحديثات إلى مستودع مهمة خادم الإدارة

لتكوين تنزيل التحديثات إلى مستودع مهمة خادم الإدارة:

1. في مساحة عمل المجلد **المهام** الخاص بشجرة وحدة التحكم، حدد **تنزيل التحديثات إلى مستودع خادم الإدارة** من قائمة المهام.

2. افتح نافذة خصائص المهمة بإحدى الطرق التالية:

- عن طريق تحديد **خصائص** من قائمة سياق المهمة.
- من خلال النقر فوق الرابط **تكوين المهمة** الموجود في خانة معلومات المهمة المحددة.

يتم فتح نافذة خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. في هذه النافذة، يمكنك تكوين طريقة تنزيل التحديثات إلى مستودع خادم الإدارة.

التحقق من التحديثات المُنزّلة

قبل تثبيت التحديثات على الأجهزة المدارة، يمكنك أولاً التحقق من التحديث للتأكد من قابلية التشغيل والأخطاء من خلال مهمة التحقق من صحة التحديث. يتم تنفيذ مهمة التحقق من صحة التحديث تلقائيًا كجزء من مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. يقوم خادم الإدارة بتنزيل التحديثات من المصدر ويحفظها في المستودع المؤقت، ويقوم بتشغيل مهمة التحقق من صحة التحديث. إذا اكتملت المهمة بنجاح، سيتم نسخ التحديثات من المستودع المؤقت إلى المجلد المشترك لخادم الإدارة (<Kaspersky Security Center installation folder>\Share\Updates). يتم توزيعها على جميع أجهزة العميل التي يكون فيها خادم الإدارة هو مصدر التحديثات.

كنتيجة لمهمة التحقق من صحة التحديث، إذا كانت التحديثات الموجودة في المستودع المؤقت غير صحيحة أو إذا اكتملت مهمة التحقق من صحة التحديث مع وجود خطأ، لن يتم نسخ هذه التحديثات إلى المجلد المشترك. يحتفظ خادم الإدارة بالمجموعة السابقة من التحديثات. أيضًا لن يتم بدء الهام ذات نوع الجدول **عند تنزيل تحديثات جديدة إلى المستودع** بعد. يتم إجراء هذه العمليات في البداية التالية لمهمة تنزيل التحديثات إلى مستودع خادم الإدارة إذا اكتمل فحص التحديثات الجديدة بنجاح.

تعتبر مجموعة التحديثات غير صالحة في حالة الوفاء بأحد الشروط التالية على جهاز اختبار واحد على الأقل:

- حدث خطأ في مهمة تحديث.
- تغيير حالة الحماية في الوقت الحقيقي لتطبيق الأمن بعد تطبيق التحديثات.
- تم اكتشاف كائن مصاب أثناء تشغيل مهمة الفحص عند الطلب.
- حدث خطأ في وقت تشغيل تطبيق Kaspersky.

إذا لم يكن أي من الشروط المدرجة في القائمة صحيحًا لأي جهاز اختبار، تعتبر مجموعة التحديثات صالحة وتعتبر مهمة التحقق من صحة التحديث مكتملة بنجاح.

قبل أن تبدأ في إنشاء مهمة التحقق من صحة التحديث، نفذ المتطلبات الأساسية:

1. إنشاء مجموعة الإدارة مع العديد من أجهزة الاختبار. ستحتاج إلى هذه المجموعة للتحقق من التحديثات عليها.

   نُوصى باستخدام الأجهزة التي تتمتع بحماية موثوقة وتكوين التطبيق الشائع عبر الشبكة. يزيد هذا النهج من جودة واحتمالية اكتشاف الفيروسات أثناء عمليات الفحص، ويقلل من مخاطر الإيجابيات الكاذبة. إذا تم اكتشاف الفيروسات على أجهزة الاختبار، تعتبر مهمة التحقق من صحة التحديث غير ناجحة.

2. أنشئ مهتمي تحديث وفحص البرامج الضارة لتطبيق مدعوم بواسطة Kaspersky Security Center، على سبيل المثال، Kaspersky Endpoint Security for Windows أو Kaspersky Security for Windows Server. عند إنشا مهتمي تحديث وفحص البرامج الضارة، حدد مجموعة الإدارة مع أجهزة الاختبار.

   تقوم مهمة التحقق من صحة التحديث بتشغيل مهمتي تحديث وفحص البرامج الضارة بالتتابع على أجهزة الاختبار للتحقق من صلاحية جميع التحديثات. بالإضافة إلى ذلك، عند إنشاء مهمة التحقق من صحة التحديث ، تحتاج إلى تحديد مهمتي تحديث وفحص البرامج الضارة.

3. إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة.

لجعل التطبيق Kaspersky Security Center يتحقق من التحديثات التي تم تنزيلها قبل توزيعها إلى الأجهزة العميلة:

1. في مساحة عمل مجلد **المهام**، حدد مهمة تنزيل التحديثات إلى مستودع خادم الإدارة في قائمة المهام.
2. افتح نافذة خصائص المهمة بإحدى الطرق التالية:
   - عن طريق تحديد **خصائص** من قائمة سياق المهمة.
   - بالنقر فوق رابط **تكوين المهمة** في خانة معلومات المهمة المحددة.
3. إذا كانت مهمة التحقق من صحة التحديث موجودة، انقر فوق الزر **استعراض**. في النافذة التي تفتح، حدد مهمة التحقق من صحة التحديث في مجموعة الإدارة مع أجهزة الاختبار.
4. إذا لم تكن قد أنشأت مهمة التحقق من صحة التحديث من قبل، انقر فوق الزر **إنشاء**.

   يبدأ معالج مهمة التحقق من صحة التحديث. اتبع إرشادات المعالج.
5. انقر على **موافق** لإغلاق نافذة الخصائص لمهمة تنزيل التحديثات إلى مستودع خادم الإدارة.

يتم تفعيل التحقق التلقائي من التحديثات. يمكنك الآن تشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة وستبدأ التحقق من التحديث.

تكوين سياسات الاختبار والمهام الإضافية

عند إنشاء مهمة التحقق من صحة التحديث، ينشئ خادم الإدارة سياسات الاختبار ومهام تحديث المجموعة الإضافية ومهام الفحص عند الطلب.

يستغرق تحديث المجموعة الإضافية ومهام الفحص حسب الطلب بعض الوقت. يتم القيام بهذه المهام عند تنفيذ مهمة التحقق من صحة التحديث. يتم تنفيذ مهمة Update verification أثناء تنفيذ مهمة Download updates to the repository. تتضمن مدة مهمة Download updates to the repository تحديث المجموعة الفرعية ومهام الفحص عند الطلب.

يمكنك تغيير إعدادات سياسات الاختبار والمهام الإضافية.

لتغيير إعدادات سياسة اختبار أو مهمة إضافية:

1. في شجرة وحدة التحكم، حدد مجموعة يتم إنشاء مهمة التحقق من صحة التحديث لها.
2. في مساحة عمل المجموعة، حدد إحدى علامات التبويب التالية:
   - **السياسات**، إذا كنت تريد تحرير إعدادات سياسة الاختبار.
   - **المهام**، إذا كنت تريد تغيير إعدادات المهمة الإضافية.
3. في مساحة عمل علامة التبويب، حدد السياسة أو المهمة، التي تريد تغيير إعداداتها.
4. افتح نافذة خصائص السياسة (المهمة) بإحدى الطرق التالية:
   - عن طريق تحديد **خصائص** من قائمة سياق السياسة (المهمة).
   - من خلال النقر فوق الرابط **تكوين السياسة (تكوين المهمة)** في خانة معلومات السياسة المحددة (المهمة).

للتحقق من التحديثات بشكل صحيح، قم بتعيين القيود التالية على تعديل سياسات الاختبار والمهام الإضافية:

- في إعدادات المهمة الإضافية:
  - حفظ جميع المهام ذات مستويات الأهمية **حدث حرج** و**خلل وظيفي**على خادم الإدارة. يحلل خادم الإدارة باستخدام الأحداث من هذه النوعية تشغيل التطبيقات.
  - استخدم خادم الإدارة كمصدر للتحديثات.
  - حدد نوع جدولة المهمة: **يدويًا**.
- في إعدادات سياسات الاختبار:
  - تعطيل تقنيات تسريع المسح الضوئي iChecker وiSwift (**الحماية الأساسية من التهديدات** ← **الحماية من تهديدات الملفات** ← **الإعدادات** ← **إضافي** ← **تقنيات المسح الضوئي**).
  - حدد الإجراءات على الكائنات المصابة: **التنظيف؛ حذف إذا فشل التنظيف؛** / **التنظيف؛ حظر إذا فشل التنظيف** / **حظر**. (**الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات** ← **الإجراء عند اكتشاف تهديد**).
- في إعدادات سياسات الاختبار والمهام الإضافية:

إذا تطلب الجهاز إعادة تشغيل بعد تثبيت تحديثات الوحدات النمطية للبرامج، فيجب القيام بذلك على الفور. إذا لم تتم إعادة تشغيل الجهاز، فمن المستحيل اختبار هذا النوع من التحديثات. لبعض التطبيقات، ربما يتم حظر تثبيت التحديثات التي تتطلب إعادة التشغيل أو تهيئتها لمطالبة المستخدم بالتأكيد أولاً. ينبغي تعطيل هذه القيود في إعدادات سياسات الاختبار والمهام الإضافية.

عرض التحديثات المُنزّلة

لعرض قائمة التحديثات المنزّلة:

في شجرة وحدة التحكم، في مجلد **المستودعات**، حدد المجلد الفرعي **تحديثات قواعد بيانات Kaspersky ووحدات البرامج النمطية** .

تعرض مساحة عمل المجلد **تحديثات قواعد بيانات Kaspersky ووحدات البرامج النمطية** قائمة بالتحديثات المحفوظة على خادم الإدارة.

التثبيت التلقائي لتحديثات Kaspersky Endpoint Security على الأجهزة

يمكنك تكوين التحديثات التلقائية لقواعد البيانات والوحدات النمطية للبرامج الخاصة بـ Kaspersky Endpoint Security على الأجهزة العميلة.

لتكوين التنزيل والتثبيت التلقائي لتحديثات Kaspersky Endpoint Security على الأجهزة :

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. قم بإنشاء مهمة **تحديث** بإحدى الطرق التالية:
   - عن طريق تحديد **جديد** ← **مهمة** في قائمة سياق المجلد **المهام** في شجرة وحدة التحكم.
   - بالنقر فوق الزر **مهمة جديدة** في مساحة عمل المجلد **المهام**.

   سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.
3. في صفحة المعالج **تحديد نوع المهمة**، حدد **Kaspersky Endpoint Security** كنوع المهمة، ثم حدد **تحديث** كالنوع الفرعي للمهمة.
4. اتبع بقية تعليمات المعالج.

   بعد انتهاء المعالج، يتم إنشاء مهمة تحديث لـ Kaspersky Endpoint Security. يتم عرض المهمة التي تم إنشاؤها حديثًا في قائمة المهام في مساحة عمل المجلد **المهام**.
5. في مساحة عمل المجلد **المهام**، حدد مهمة التحديث التي قمت بإنشائها.
6. من قائمة سياق المهمة، حدد **خصائص**.
7. من نافذة خصائص المهمة التي تفتح، في الجزء **الأقسام**، حدد **الخيارات**.

   في القسم **إعدادات**، يمكنك تحديد إعدادات مهمة التحديث في الوضع المحلي أو الجهاز المحمول:
   - **إعدادات التحديث للوضع المحلي**: تم إنشاء الاتصال بين الجهاز وخادم الإدارة.
   - **إعدادات التحديث لوضع الجهاز المحمول**: لم يتم إنشاء اتصال بين Kaspersky Security Center والجهاز (على سبيل المثال، عندما لا يكون الجهاز متصل بالإنترنت).
8. انقر فوق الزر **إعدادات** لتحديد مصدر التحديث.
9. حدد خيار **تنزيل تحديثات الوحدة النمطية للتطبيق** لتنزيل تحديثات الوحدة النمطية للبرنامج وتثبيتها جنبًا إلى جنب مع قواعد بيانات التطبيق.

إذا تم تحديد خانة الاختيار، يقوم Kaspersky Endpoint Security بإخطار المستخدم حول تحديثات الوحدة النمطية للبرنامج المتوفرة وتضمين تحديثات الوحدة النمطية للبرنامج في حزمة التحديثات أثناء تشغيل مهمة التحديث. تكوين استخدام الوحدات النمطية للتحديث:

- **تثبيت التحديثات الحيوية والمعتمدة**. إذا توافرت أي تحديثات للوحدات النمطية للبرنامج، يقوم Kaspersky Endpoint Security بتثبيت التحديثات التي حالتها حرج تلقائيًا؛ وسيتم تثبيت التحديثات المتبقية بعد الحصول على موافقتك.

- **تثبيت التحديثات المعتمدة فقط**. إذا توافرت أي تحديثات للوحدات النمطية للبرنامج، فإن Kaspersky Endpoint Security يقوم بتثبيتها بعد الموافقة على تثبيتها؛ ويتم تثبيتها محليًا من خلال واجهة التطبيق أو عبر Kaspersky Security Center.

إذا تطلب تحديث الوحدة النمطية للبرنامج مراجعة بنود اتفاقية الترخيص وسياسة الخصوصية والموافقة عليها، فإن التطبيق يقوم بتثبيت التحديثات بعد الموافقة على بنود اتفاقية الترخيص وسياسة الخصوصية من قبل المستخدم.

10. حدد خيار **نسخ التحديثات إلى مجلد** لكي يقوم التطبيق بحفظ التحديثات التي تم تنزيلها إلى مجلد، ثم انقر فوق الزر **استعراض** لتحديد المجلد.

11. انقر فوق **موافق**.

عند تشغيل المهمة **تحديث**، يرسل التطبيق طلبات إلى خوادم تحديث Kaspersky.

تتطلب بعض التحديثات تثبيت أحدث إصدارات مكونات الإدارة الإضافية.

النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات

قد لا يتصل عميل الشبكة على الأجهزة المُدارة بخادم الإدارة لتلقي التحديثات في بعض الأحيان. على سبيل المثال، قد يكون عميل الشبكة قد تم تثبيته على جهاز كمبيوتر محمول لا يكون متصلاً بالإنترنت في بعض الأحيان ولا يتوفر له الوصول إلى شبكة محلية. وعلاوة على ذلك، قد يقلل المسؤول وقت اتصال الأجهزة بالشبكة. في مثل هذه الحالات، لا يمكن للأجهزة المثبت عليها عميل الشبكة تلقي التحديثات من خادم الإدارة بناءً على الجدولة الموجودة. إذا قمت بتكوين تحديث التطبيقات المُدارة (مثل Kaspersky Endpoint Security) باستخدام عميل الشبكة، فسوف يتطلب كل تحديث وجود اتصال بخادم الإدارة. عند تعذّر إنشاء أي اتصال بين عميل الشبكة وخادم الإدارة، يكون التحديث مستحيلاً. ويمكنك تكوين الاتصال بين عميل الشبكة وخادم الإدارة بحيث يتصل عميل الشبكة بخادم الإدارة على فترات زمنية محددة. وفي أسوأ الأحوال، إذا تزامنت الفترات الزمنية المحددة للاتصال مع فترات لا يتوفر فيها أي اتصال، فلن يتم تحديث قواعد البيانات. بالإضافة إلى ذلك، قد تحدث مشكلات عند محاولة تطبيقات مدارة متعددة الوصول في وقتٍ واحد إلى خادم الإدارة لتلقي التحديثات. في هذه الحالة، قد يتوقف خادم الإدارة عن الاستجابة للطلبات (وبالمثل لهجوم DDoS).

لتجنب حدوث مشكلات كتلك التي تم وصفها في الأعلى، يتم تطبيق الوضع "غير متصل بالإنترنت" لتنزيل التحديثات والوحدات النمطية للتطبيقات المُدارة في Kaspersky Security Center. يوفر هذا النموذج آلية لتوزيع التحديثات، بغض النظر عن المشاكل المؤقتة الناجمة عن عدم إمكانية الوصول إلى قنوات اتصال خادم الإدارة. يقلل النموذج أيضًا الحمل على خادم الإدارة.

كيفية عمل النموذج غير متصل لتنزيل التحديثات

عند تلقي خادم الإدارة للتحديثات، يقوم بإخطار عميل الشبكة (على الأجهزة المثبت عليها) بالتحديثات المطلوبة للتطبيقات المُدارة. وعندما يتلقى عميل الشبكة معلومات حول هذه التحديثات، يقوم بتنزيل الملفات ذات الصلة من خادم الإدارة بشكلٍ مسبق. وعند أول اتصال مع عميل الشبكة، يبدأ خادم الإدارة بتنزيل التحديث. بعد أن يقوم عميل الشبكة بتنزيل جميع التحديثات إلى جهاز عميل، تصبح التحديثات متاحة للتطبيقات على هذا الجهاز.

عندما يحاول تطبيق مُدار على جهاز عميل الوصول إلى عميل الشبكة للحصول على تحديثات، يقوم عميل الشبكة بالتحقق مما إذا كانت جميع التحديثات المطلوبة متوفرة. إذا تم تلقي التحديثات من خادم الإدارة قبل فترة لا تزيد عن 25 ساعة من طلبها بواسطة تطبيق مُدار، فلن يتصل عميل الشبكة بخادم الإدارة ولكنه سيوفر بدلًا من ذلك تحديثات للتطبيق المُدار من خلال ذاكرة التخزين المؤقت المحلية. وقد يتعذر إنشاء اتصال بخادم الإدارة عند توفير عميل الشبكة لتحديثات للتطبيقات الموجودة على الأجهزة العميلة، إلا إن الاتصال غير مطلوب للتحديث.

لتوزيع الحمل على خادم الإدارة، يتصل عميل الشبكة على أحد الأجهزة بخادم الإدارة ويقوم بتنزيل التحديثات عشوائيًا أثناء الفترات الزمنية المحددة من قِبل خادم الإدارة. ويعتمد هذا الفاصل الزمني على عدد الأجهزة المثبت عليها عميل الشبكة الذين يقومون بتنزيل التحديثات وعلى حجم تلك التحديثات. لتقليل الحمل على خادم الإدارة، يمكنك استخدام عميل الشبكة كنقاط توزيع.

إذا تم تعطيل الوضع "غير متصل بالإنترنت" لتنزيل التحديث، فإنه يتم توزيع التحديثات وفقًا لجدول مهمة تنزيل التحديث.

بشكل افتراضي، يتم تمكين النموذج غير متصل لتنزيل التحديثات.

يتم استخدام الوضع "غير متصل بالإنترنت" لتنزيل التحديث فقط مع الأجهزة المُدارة التي يكون خيار **عند تنزيل تحديثات جديدة إلى المستودع** لمهمة استرداد التحديثات بواسطة التطبيقات المُدارة محددًا عليها كنوع للجدولة. بالنسبة للأجهزة المُدارة الأخرى، يتم استخدام النظام القياسي لاسترداد التحديثات من خادم الإدارة في وضع الوقت الحقيقي.

نوصي بتعطيل الوضع غير متصل بالإنترنت الخاص بتنزيل التحديثات باستخدام إعدادات سياسات عميل الشبكة لمجموعات الإدارة ذات الصلة في هذه الحالات: إذا كانت التطبيقات المُدارة تتمتع بخاصية استرداد مجموعة التحديثات ولكن ليس من خادم الإدارة بل من خوادم Kaspersky أو من مجلد الشبكة، وإذا كانت مهمة تنزيل التحديثات محدد بها الخيار **عند تنزيل تحديثات جديدة إلى المستودع** كنوع من الجدولة.

تمكين النموذج غير متصل بالإنترنت لتنزيل التحديثات وتعطيله

ننصحك بتجنب تعطيل نموذج عدم الاتصال لتنزيل التحديثات. قد يسبب تعطيله إخفاقات في تسليم التحديث إلى الأجهزة. في بعض الحالات، قد ينصحك متخصص الدعم الفني من Kaspersky بإلغاء تحديد خانة اختيار **تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة بشكل مسبق**. لذلك، سيتعين عليك التأكد من إعداد مهمة استلام التحديثات لتطبيقات Kaspersky.

لتمكين وتعطيل نموذج غير متصل لتنزيل التحديثات لمجموعة إدارة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي تريد لأجلها تمكين نموذج غير متصل لتنزيل التحديثات.
2. في مساحة عمل المجموعة، افتح علامة التبويب **السياسات**.
3. في علامة التبويب **السياسات**، حدد سياسة عميل الشبكة.
4. في قائمة السياق للسياسة، حدد **خصائص**.

   افتح نافذة خصائص سياسة عميل الشبكة.
5. في نافذة خصائص السياسة ، حدد قسم **إدارة التصحيحات والتحديثات**.
6. قم بتحديد أو إلغاء خانة الاختيار **تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة مقدمًا (مستحسن)** لتمكين وضع غير متصل بالإنترنت أو تعطيله على التوالي.

   بشكل افتراضي، يتم تمكين النموذج غير متصل لتنزيل التحديثات.

   سيتم تمكين نموذج غير متصل لتنزيل التحديثات أو تعطيله.

التحديث والتصحيح التلقائيان لمكونات Kaspersky Security Center

بشكل افتراضي يتم التثبيت التلقائي لأي من التحديثات والتصحيحات التي تم تنزيلها لمكونات التطبيقات التالية:

- عميل الشبكة لنظام التشغيل Windows
- وحدة تحكم الإدارة
- خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يتوفر التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center فقط للأجهزة التي تعمل بنظام التشغيل Windows. يمكنك تعطيل التحديث والتصحيح التلقائيين لهذه المكونات. وفي هذه الحالة، لن يتم تثبيت أي من التحديثات والتصحيحات التي تم تنزيلها إلا بعد أن تغير حالتها إلى تمت الموافقة. لن يتم تثبيت التحديثات والتصحيحات ذات الحالة غير محددة.

تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center.

يتم تمكين التثبيت التلقائي لتحديثات وتصحيحات مكونات Kaspersky Security Center بشكل افتراضي أثناء تثبيت عميل الشبكة على الجهاز. ويمكنك تعطيله أثناء تثبيت عميل الشبكة، أو تعطيله في وقت لاحق باستخدام سياسة.

لتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center أثناء التثبيت المحلي لعميل الشبكة على الجهاز:

1. ابدأ التثبيت المحلي لعميل الشبكة على الجهاز.
2. في الخطوة **الإعدادات المتقدمة**، قم بإلغاء تحديد خانة الاختيار **تثبيت التحديثات والتصحيحات القابلة للتطبيق تلقائيًا للمكونات بالحالة غير محددة**.
3. اتبع إرشادات المعالج.

سيتم تثبيت عميل الشبكة الذي تم تعطيل التثبيت والتصحيح التلقائيين لمكونات Kaspersky Security Center له على الجهاز. يمكنك تمكين التحديث والتصحيح التلقائيين في وقت لاحق باستخدام سياسة.

لتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center أثناء تثبيت عميل الشبكة على الجهاز من خلال حزمة تثبيت:

1. في شجرة وحدة التحكم، حدد المجلد **التثبيت عن بُعد** ← **حزم التثبيت**.
2. في قائمة سياق الحزمة **عميل شبكة Kaspersky Security Center <رقم الإصدار>**، حدد **خصائص**.
3. في خصائص حزمة التثبيت، في القسم **إعدادات** قم بإلغاء تحديد خانة الاختيار **التثبيت التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة**.

سيتم تثبيت عميل الشبكة الذي تم تعطيل التثبيت والتصحيح التلقائيين لمكونات Kaspersky Security Center له من هذه الحزمة. يمكنك تمكين التحديث والتصحيح التلقائيين في وقت لاحق باستخدام سياسة.

في حالة تحديد خانة الاختيار هذه (أو إلغاء تحديدها) أثناء تثبيت عميل الشبكة على الجهاز، يمكنك بعد ذلك تمكين (أو تعطيل) التحديث التلقائي باستخدام سياسة عميل الشبكة.

لتمكين أو تعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center باستخدام سياسة عميل الشبكة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي يتعين عليك تمكين أو تعطيل التحديث والتصحيح التلقائيين لها.
2. في مساحة عمل المجموعة، افتح علامة التبويب **السياسات**.
3. في علامة التبويب **السياسات**، حدد سياسة عميل الشبكة.
4. في قائمة السياق للسياسة، حدد **خصائص**.

   افتح نافذة خصائص سياسة عميل الشبكة.
5. في نافذة خصائص السياسة ، حدد قسم **إدارة التصحيحات والتحديثات**.
6. حدد أو ألغ تحديد خانة الاختيار **التثبيت التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة** لتمكين أو تعطيل التحديث والتصحيح تلقائيًا على التوالي.
7. عيّن القفل لخانة الاختيار هذه.

سيتم تطبيق السياسة على الأجهزة المحددة، وسيتم تمكين (أو تعطيل) التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center على هذه الأجهزة.

التوزيع التلقائي للتحديثات

يسمح Kaspersky Security Center بتوزيع التحديثات تلقائيًا وتثبيتها على الأجهزة العميلة وخوادم الإدارة الثانوية.

توزيع التحديثات تلقائيًا على الأجهزة العميلة

لتوزيع تحديثات التطبيق المحدد تلقائيًا على الأجهزة العميلة مباشرة بعد تنزيلها إلى مستودع خادم الإدارة:

1. اتصل بخادم الإدارة الذي يتولى إدارة الأجهزة العميلة.

2. قم بإنشاء مهمة نشر تحديث للأجهزة العميلة المحددة باستخدام إحدى الطرق التالية:

- إذا كنت تريد توزيع التحديثات على الأجهزة العميلة التي تنتمي إلى مجموعة إدارة محددة، فقم بإنشاء مهمة للمجموعة المحددة.
- وإذا كنت تريد توزيع التحديثات على الأجهزة العميلة التي تنتمي إلى مجموعات إدارة مختلفة أو لا تنتمي إلى أي مجموعات إدارة على الإطلاق، فقم بإنشاء مهمة لأجهزة محددة.

سيبدأ معالج المهمة الجديدة. اتبع تعليماته ونفّذ الإجراءات التالية:

a. في نافذة معالج **نوع المهمة**، في عقدة التطبيق المطلوب، حدد مهمة نشر التحديثات.

يعتمد اسم مهمة نشر التحديثات في نافذة **نوع المهمة** على التطبيق الذي تقوم بإنشاء هذه المهمة له. للاطلاع على معلومات مفصلة حول أسماء مهام التحديث لتطبيقات Kaspersky المحددة، انظر الأدلة المقابلة.

b. في نافذة معالج **جدول**، في حقل **البدء المُجدول**، حدد **عند تنزيل تحديثات جديدة إلى المستودع**.

ستبدأ مهمة توزيع التحديثات التي تم إنشاؤها حديثًا للأجهزة المحددة في كل مرة يتم فيها تنزيل أي تحديثات إلى مستودع خادم الإدارة.

في حالة إنشاء مهمة توزيع تحديثات تخص التطبيق المطلوب للأجهزة المحددة، فلكي تقوم بتوزيع التحديثات تلقائيًا على الأجهزة العميلة، في نافذة خصائص المهمة في القسم **جدول**، حدد **عند تنزيل تحديثات جديدة إلى المستودع** كخيار البدء في الحقل **البدء المُجدول**.

توزيع التحديثات تلقائيًا على خوادم الإدارة الثانوية

لتوزيع تحديثات التطبيقات المحددة على خوادم الإدارة الثانوية بعد تنزيل التحديثات مباشرةً إلى مستودع خادم الإدارة الرئيسي:

1. ضمن شجرة وحدة التحكم، في عقدة خادم الإدارة الرئيسي، حدد المجلد **المهام**.

2. في قائمة المهام في مساحة العمل، حدد تنزيل التحديثات إلى مستودع مهمة خادم الإدارة الخاص بخادم الإدارة.

3. افتح القسم **إعدادات** للمهمة المحددة بإحدى الطرق التالية:

- بتحديد **خصائص** من قائمة سياق المهمة.
- من خلال النقر فوق رابط **تحرير الخصائص** الموجود في خانة معلومات المهمة المحددة.

4. في القسم **إعدادات** من نافذة خصائص المهمة، حدد القسم الفرعي **إعدادات أخرى** وانقر بعد ذلك فوق الرابط **تكوين**.

5. من نافذة **إعدادات أخرى** التي تفتح، حدد خانة الاختيار **إجبار تحديث خوادم الإدارة الثانوية**.

6. ضمن إعدادات مهمة تنزيل التحديثات الخاصة بخادم الإدارة، في علامة التبويب **إعدادات** نافذة خصائص المهمة، حدد خانة الاختيار **إجبار تحديث خوادم الإدارة الثانوية**.

وبعد أن يستعيد خادم الإدارة الرئيسي التحديثات، تبدأ مهمة تنزيل التحديثات تلقائيًا على خوادم الإدارة الثانوية بصرف النظر عن جدولها.

ويقوم خادم الإدارة الأساسي بتحديث قواعد بيانات مكافحة الفيروسات، وفقًا للتطبيقات المثبتة على خوادم الإدارة الثانوية. وليس من الضروري تثبيت المكونات الإضافية وإنشاء حزم التثبيت على خادم الإدارة الأساسي.

تعيين نقاط التوزيع تلقائيًا

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. حينئذ، سيحدد Kaspersky Security Center بنفسه الأجهزة التي يجب تعيين نقاط التوزيع لها.

لتعيين نقاط التوزيع تلقائيًا:

1. افتح نافذة التطبيق الرئيسية.

2. في شجرة وحدة التحكم، حدد الجزء الذي يحمل اسم خادم الإدارة الذي تريد تعيين نقاط التوزيع له.

3. في قائمة السياق لخادم الإدارة، انقر على **خصائص**.

4. من النافذة خصائص خادم الإدارة، في الجزء **الأقسام**، حدد **نقاط التوزيع**.

5. في الجزء الأيمن من النافذة، حدد خيار **تعيين نقاط التوزيع تلقائيًا**.

في حالة تمكين التعيين التلقائي للأجهزة كنقاط توزيع، سيتعذر عليك تكوين نقاط التوزيع يدويًا أو تحرير قائمة نقاط التوزيع.

6. انقر فوق **موافق**.

يقوم خادم الإدارة بتعيين نقاط التوزيع وتكوينهم تلقائيًا.

تعيين نقطة توزيع لجهاز يدويًا

يتيح لك Kaspersky Security Center تعيين أجهزة للعمل كنقاط توزيع.

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. في هذه الحالة، سيحدد Kaspersky Security Center بنفسه الأجهزة التي سيتم تعيين نقاط التوزيع لها. ولكن، إذا كان يتعين عليك إلغاء الاشتراك في تعيين نقاط التوزيع تلقائيًا لأي سبب (على سبيل المثال، إذا كنت ترغب في استخدام خوادم معيّنة حصريًا) فيمكنك تعيين نقاط التوزيع يدويًا بعد قيامك بحساب عددهم وتكوينهم.

يجب أن تكون الأجهزة التي تعمل كنقاط توزيع محمية، بما في ذلك الحماية الفعلية، وضد أي وصول غير مصرح به.

لتعيين جهاز للعمل كنقطة توزيع يدويًا:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في النافذة خصائص خادم الإدارة، حدد القسم **نقاط التوزيع** وانقر فوق الزر **إضافة**. يتوفر هذا الزر إذا تم تحديد **تعيين نقاط التوزيع يدويًا**.
يتم فتح نافذة **إضافة نقطة توزيع**.

4. في النافذة **إضافة نقطة توزيع**، قم بتنفيذ الإجراءات التالية:

a. حدد جهاز للعمل كنقطة توزيع (حدد جهاز في مجموعة الإدارة، أو حدد عنوان IP الخاص بالجهاز). عند تحديد جهاز، فيجب مراعاة ميزات تشغيل نقاط التوزيع والمتطلبات المحددة للجهاز الذي يعمل كنقطة توزيع.

b. حدد الأجهزة المحددة التي ستقوم نقطة التوزيع بتوزيع التحديثات إليها. يمكنك تحديد مجموعة إدارة أو وصف موقع الشبكة.

5. انقر على**موافق**.
سيتم عرض نقطة التوزيع التي أضفتها في قائمة نقاط التوزيع، في القسم **نقاط التوزيع**.

6. حدد نقطة التوزيع التي تمت إضافتها مؤخرًا في القائمة وانقر فوق الزر **خصائص** لفتح نافذة خصائصه.

7. قم بتكوين نقطة التوزيع في نافذة الخصائص:

- يحتوي القسم **عام** على إعدادات تفاعل نقطة التوزيع مع أجهزة العميل.

- **منفذ SSL**

رقم منفذ SSL للاتصال المشفر بين الأجهزة العميلة ونقطة التوزيع باستخدام SSL.

يتم استخدام المنفذ 13000 بشكل افتراضي.

- **استخدام الإرسال المتعدد**

إذا تم تمكين هذا الخيار، فسوف يتم استخدام البث المتعدد لـ IP في التوزيع التلقائي لحزم التثبيت على أجهزة العميل داخل المجموعة.

يقلل الإرسال المتعدد لعنوان IP الوقت اللازم لتثبيت تطبيق من حزمة تثبيت على مجموعة من أجهزة العملاء، ولكنه يزيد من وقت التثبيت عند تثبيت تطبيق على جهاز عميل واحد.

- **عنوان IP للإرسال المتعدد**

عنوان IP الذي سيتم استخدامه للإرسال المتعدد. يمكنك تحديد عنوان IP في نطاق 224.0.0.0 – 239.255.255.255

بشكل افتراضي، يقوم تطبيق Kaspersky Security Center تلقائيًا بتعيين عنوان IP متعدد الإرسال فريد ضمن النطاق المحدد.

- **رقم منفذ الإرسال المتعدد IP**

رقم منفذ الإرسال المتعدد لعنوان IP.

رقم المنفذ هو 15001 بشكل افتراضي. في حالة تحديد الجهاز المثبت عليه خادم الإدارة كنقطة التوزيع، فسيتم بشكل افتراضي استخدام المنفذ 13001 لاتصال SSL.

- **نشر التحديثات**

يتم توزيع التحديثات على الأجهزة المدارة من المصادر التالية:

- نقطة التوزيع هذه، إذا تم تمكين هذا الخيار.

- نقاط التوزيع الأخرى أو خادم الإدارة أو خوادم تحديث Kaspersky، إذا تم تعطيل هذا الخيار.

إذا كنت تستخدم نقاط التوزيع لنشر التحديثات، فيمكنك حفظ حركة المرور لأنك تقلل عدد التنزيلات. يمكنك أيضًا تخفيف الحمل على خادم الإدارة ونقل الحمل بين نقاط التوزيع. يمكنك حساب عدد نقاط التوزيع لشبكتك لتحسين حركة البيانات والتحميل.

إذا قمت بتعطيل هذا الخيار، فقد يزيد عدد تنزيلات التحديث وتحميلها على خادم الإدارة. يتم تمكين هذا الخيار افتراضيًا.

- **نشر حزم التثبيت**

يتم توزيع حزم التثبيت على الأجهزة المُدارة من المصادر التالية:

- نقطة التوزيع هذه، إذا تم تمكين هذا الخيار.
- نقاط التوزيع الأخرى أو خادم الإدارة أو خوادم تحديث Kaspersky، إذا تم تعطيل هذا الخيار.

إذا كنت تستخدم نقاط التوزيع لنشر حزم التثبيت، فيمكنك توفير حركة البيانات لأنك تقلل عدد التنزيلات. يمكنك أيضًا تخفيف الحمل على خادم الإدارة ونقل الحمل بين نقاط التوزيع. يمكنك حساب عدد نقاط التوزيع لشبكتك لتحسين حركة البيانات والتحميل.

إذا قمت بتعطيل هذا الخيار، فقد يزيد عدد تنزيلات حزمة التثبيت وتحميلها على خادم الإدارة. يتم تمكين هذا الخيار افتراضيًا.

- **استخدم نقطة التوزيع هذه كخادم إرسال**

في Kaspersky Security Center، يمكن أن تعمل نقطة التوزيع كخادم إرسال للأجهزة المدارة من خلال بروتوكول الهاتف المحمول. على سبيل المثال، يجب تمكين خادم الإرسال إذا كنت تريد أن تكون قادرًا على فرض المزامنة لأجهزة KasperskyOS المزودة بخادم الإدارة. خادم الإرسال لديه نفس نطاق الأجهزة المدارة التي تعمل كنقطة التوزيع حيث يتم فيها تمكين خادم الإرسال. إذا كان لديك العديد من نقاط التوزيع المخصصة لمجموعة الإدارة نفسها، فيمكنك تمكين خادم الإرسال في كل نقطة من نقاط التوزيع. في هذه الحالة، يوازن خادم الإدارة التحميل بين نقاط التوزيع.

إذا كنت تدير أجهزة مثبت عليها KasperskyOS، أو تخطط للقيام بذلك، فيجب عليك استخدام نقطة توزيع كخادم إرسال. يمكنك أيضًا استخدام نقطة توزيع كخادم إرسال، إذا كنت ترغب في إرسال إشعارات إلى أجهزة العميل.

- **منفذ خادم الإرسال**

المنفذ الموجود في نقطة التوزيع التي ستستخدمها الأجهزة العميلة في الاتصال. يتم استخدام المنفذ 13295 بشكل افتراضي.

- في القسم **النطاق**، حدد النطاق الذي ستقوم فيه نقطة التوزيع بتوزيع التحديثات إليه (مجموعات الإدارة و/أو موقع الشبكة).
- من القسم **وكيل KSN**، يمكنك تكوين التطبيق لاستخدام نقطة التوزيع لإعادة توجيه طلبات KSN من الأجهزة المدارة.

- **تمكين وكيل KSN على جانب نقطة التوزيع**

تعمل خدمة وكيل KSN على الجهاز المستخدم كنقطة توزيع. استخدم هذه الميزة لإعادة توزيع حركة مرور البيانات في الشبكة وتحسينها.

ترسل نقطة التوزيع إحصاءات KSN المُدرجة في بيان Kaspersky Security Network إلى Kaspersky.

يتم تعطيل هذا الخيار افتراضيًا. يسري تمكين هذا الخيار فقط في حالة تمكين الخيارين **Use Administration Server as a proxy** و**I agree to use Kaspersky Security Network** في نافذة خصائص خادم الإدارة.

يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل خادم KSN على هذه العقدة.

- **إعادة توجيه طلبات KSN إلى خادم الإدارة**

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المدارة إلى خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **الوصول إلى KSN Cloud/KPSN مباشرة عبر الإنترنت**

تعيد نقطة التوزيع توجيه طلبات KSN من الأجهزة المُدارة إلى KSN Cloud أو KPSN. يتم أيضًا إرسال طلبات KSN – التي تم إنشاؤها على نقطة التوزيع نفسها – مباشرةً إلى KSN Cloud أو PKSN.

لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى KPSN مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KPSN، فقم بتمكين خيار **توجيه طلبات KSN إلى خادم الإدارة** لكل نقطة توزيع.

لا يمكن لنقاط التوزيع التي لديها الإصدار 12 المثبت من Network Agent (أو إصدار أقدم)، الوصول إلى KPSN مباشرةً.

- **تجاهل إعدادات الخادم الوكيل عند الاتصال بشبكة KPSN**

قم بتمكين هذا الخيار، إذا كانت إعدادات الخادم الوكيل مكوّنة في خصائص نقطة التوزيع أو في سياسة عميل الشبكة، لكن كانت بنية شبكتك تتطلب استخدام شبكة KPSN مباشرةً. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المُدارة إلى شبكة KPSN.

يتوفر هذا الخيار إذا حددت الخيار **Access KSN Cloud/KPSN directly over the internet**.

- **منفذ TCP**

رقم منفذ TCP الذي ستستخدمه الأجهزة المُدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

- **منفذ UDP.**

إذا كنت بحاجة إلى عميل الشبكة للاتصال بخادم الإدارة من خلال منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد **رقم منفذ UDP**. يتم تمكين هذا الخيار افتراضيًا. ويكون منفذ UDP الافتراضي للاتصال بخادم الإدارة هو 15000.

- **منفذ HTTPS**

إذا كنت تريد أن تتصل الأجهزة المُدارة بخادم وكيل لشبكة KSN من خلال منفذ HTTPS، فقم بتمكين خيار **استخدام HTTPS** وحدد **HTTPS من خلال رقم المنفذ**. والمنفذ الافتراضي لبروتوكول HTTPS للاتصال بخادم وكيل لشبكة KSN هو 17111.

- في القسم **اكتشاف الأجهزة**، قم بتكوين استقصاء مجالات Windows، وActive Directory، ونطاقات IP بواسطة نقطة التوزيع.

- **مجالات Windows**

يمكنك تمكين اكتشاف الأجهزة لمجالات Windows وتعيين الجدول للاكتشاف.

- **Active Directory**

يمكنك تمكين استقصاء الشبكة لـActive Directory وتعيين الجدول للاستقصاء.

إذا كنت تستخدم نقطة توزيع Windows، يمكنك تحديد أحد الخيارات التالية:

- **استقصاء مجال Active Directory الحالي**.
- **استقصاء مجال Active Directory الرئيسي**.
- **استقصاء مجالات Active Directory المحددة فقط**. إذا قمت بتحديد هذا الخيار، فقم بإضافة واحد أو أكثر من مجالات Active Directory إلى هذه القائمة.

إذا كنت تستخدم نقطة توزيع Linux مُثبت عليها الإصدار 15 من عميل الشبكة، يمكنك استقصاء نطاقات Active Directory فقط التي تحدد لها العنوان وبيانات اعتماد المستخدم. لا يتوفر استقصاء مجال Active Directory الحالي ومجال Active Directory الرئيسي.

- **نطاقات IP**

يمكنك تمكين اكتشاف الجهاز لنطاقات IPv4 وشبكات IPv6.

إذا مكنت خيار **تمكين استقصاء النطاق** ، فيمكنك إضافة نطاقات ممسوحة ضوئيًا وتعيين الجدول الزمني لها. يمكنك إضافة نطاقات IP لقائمة النطاقات التي تم فحصها.

إذا قمت بتمكين الخيار **Use Zeroconf to poll IPv6 networks**، ستقوم نقطة التوزيع تلقائيًا باستقصاء شبكة IPv6 باستخدام شبكات التكوين الصفري (يشار إليها أيضًا باسم شبكة لا تتطلب تكوينًا). في هذه الحالة، يتم تجاهل نطاقات IP المحددة لأن نقطة التوزيع تستقصي الشبكة بالكامل. يتوفر الخيار **Use Zeroconf to poll IPv6 networks** إذا كانت نقطة التوزيع تعمل بنظام Linux. لاستخدام استقصاء IPv6 لشبكة لا تتطلب تكوينًا، يجب عليك تثبيت أداة استعراض avahi على نقطة التوزيع.

- في القسم **خيارات متقدمة**، حدد المجلد الذي يجب أن تستخدمه نقطة التوزيع لتخزين البيانات التي تم توزيعها.

- **استخدام المجلد الافتراضي**

إذا حددت هذا الخيار، سيستخدم التطبيق مجلد تثبيت عميل الشبكة على نقطة التوزيع.

- **استخدام المجلد المعين**

في حالة تحديد هذا الخيار، يمكنك تحديد المسار الخاص بالمجلد في الحقل الموجود أدناه. قد يكون مجلد محلي على نقطة التوزيع أو يمكن أن يكون مجلد على أي جهاز في شبكة الشركة.

يجب أن يمتلك حساب المستخدم الذي يتم استخدامه على نقطة التوزيع لتشغيل عميل الشبكة وصولاً إلى المجلد المحدد للقراءة والكتابة.

تعمل الأجهزة المحددة كنقاط توزيع.

يمكن للأجهزة التي تعمل بنظام تشغيل Windows فقط تحديد موقع شبكتها. لا يمكن تحديد موقع الشبكة للأجهزة التي تعمل بأنظمة تشغيل أخرى.

إزالة جهاز من قائمة نقاط التوزيع

لإزالة جهاز من قائمة نقاط التوزيع:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في النافذة خصائص خادم الإدارة، في القسم **نقاط التوزيع**، حدد الجهاز الذي يعمل كنقطة توزيع، وانقر فوق الزر **إزالة**.

سيتم إزالة الجهاز من قائمة نقاط التوزيع وسيتوقف عن العمل كنقطة توزيع.

لا يمكن إزالة جهاز من قائمة نقاط التوزيع إذا كان قد تم تعيينه بواسطة خادم الإدارة تلقائيًا.

تنزيل التحديثات عن طريق نقاط التوزيع

يتيح Kaspersky Security Center لنقاط التوزيع تلقي التحديثات من خادم الإدارة، أو خوادم Kaspersky، أو من مجلد شبكة أو مجلد محلي.

إذا لم تكن بحاجة إلى تحديد مصدر تحديث، فنوصيك باستخدام مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع لمجموعة إدارة. راجع الموضوع التالي للحصول على التفاصيل: إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع.

لتكوين تنزيل التحديث لنقطة توزيع:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة خصائص خادم الإدارة، في قسم **نقاط التوزيع**، حدد نقطة التوزيع التي سيتم تسليم التحديثات عبرها إلى أجهزة العميل في المجموعة.
4. انقر فوق الزر **خصائص** لفتح نافذة خصائص نقطة التوزيع المحددة.
5. في النافذة خصائص نقطة التوزيع، حدد القسم **مصادر التحديثات**.

6. تحديد مصدر تحديث لنقطة التوزيع:

- للسماح لنقطة التوزيع بتلقي التحديثات من خادم الإدارة، حدد **الاستعادة من خادم الإدارة**.
- **تنزيل ملفات diff**

  يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.

  يتم تمكين هذا الخيار افتراضيًا.
- للسماح لنقطة التوزيع بتلقي التحديثات باستخدام مهمة، حدد **استخدام مهمة فرض تنزيل التحديثات**:
- انقر فوق زر **استعراض** في حالة وجود مثل هذه المهمة بالفعل على الجهاز، وحدد المهمة من القائمة التي ستظهر.
- انقر على زر **مهمة جديدة** لإنشاء مهمة في حالة عدم وجود مثل هذه المهمة على الجهاز. سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

تعتبر مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع مهمة محلية. يجب عليك إنشاء مهمة جديدة لكل جهاز يعمل كنقطة توزيع.

ستتلقى نقطة التوزيع التحديثات من المصدر المحدد.

حذف تحديثات البرامج من المستودع

لحذف تحديثات البرامج من مستودع خادم الإدارة:

1. في مجلد **خيارات متقدمة** ← **إدارة التطبيق** في شجرة وحدة التحكم، حدد المجلد الفرعي**تحديثات البرنامج** .
2. في مساحة عمل المجلد **تحديثات البرنامج**، حدد التحديث الذي ترغب في حذفه.
3. في قائمة سياق التحديث، حدد **حذف ملفات التحديث**.

سيتم حذف تحديثات البرامج من مستودع خادم الإدارة.

تثبيت تصحيح خاص بتطبيق Kaspersky في وضع المجموعة

يدعم Kaspersky Security Center فقط التثبيت اليدوي للتصحيحات الخاصة بتطبيقات Kaspersky في وضع المجموعة.

لتثبيت تصحيح خاص بتطبيق Kaspersky:

1. قم بتنزيل التصحيح لكل عقدة في المجموعة.
2. قم بتشغيل تثبيت التصحيح على العقدة المفعلة.
3. انتظر حتى اكتمال تثبيت التصحيح بنجاح.
4. قم بتشغيل التصحيح على كل العقد الفرعية في المجموعة تباعًا.

   في حالة تشغيل التصحيح من سطر الأوامر، استخدم المفتاح `--CLUSTER_SECONDARY_NODE`

التصحيح غير مثبت الآن على كل العُقد في المجموعة.

5. قم بتشغيل خدمات المجموعة من Kaspersky يدويًا.

يتم عرض كل عقدة من المجموعة في وحدة تحكم الإدارة كجهاز مثبت عليه عميل الشبكة.

للحصول على معلومات حول تثبيت التصحيحات، انظر مجلد **تحديثات البرنامج** أو التقرير حول إصدارات تحديثات وحدات البرامج النمطية لتطبيقات Kaspersky.

إدارة تطبيقات الجهات الخارجية على أجهزة العميل

يتيح لك Kaspersky Security Center إدارة التطبيقات المثبتة على الأجهزة العميلة بواسطة Kaspersky والموردين الآخرين.

يمكن للمسؤول القيام بالإجراءات التالية:

- إنشاء فئات التطبيقات استنادًا إلى المعايير المحددة.
- إدارة فئات التطبيقات باستخدام القواعد المنشأة خصيصًا.
- إدارة التطبيقات على الأجهزة.
- تنفيذ المخزون والحفاظ على سجل البرامج المثبتة على الأجهزة.
- إصلاح الثغرات الأمنية في البرامج المثبتة على الأجهزة.
- تثبيت التحديثات من Windows Update وصانعي البرامج الآخرين على الأجهزة.
- مراقبة استخدام مفاتيح الترخيص لمجموعات التطبيقات المرخصة.

حول تطبيقات الجهات الخارجية

يمكن أن يساعدك Kaspersky Security Center على تحديث برامج الجهات الخارجية المثبتة على أجهزة العميل وإصلاح الثغرات الأمنية في برنامج الجهة الخارجية. يمكن لـ Kaspersky Security Center تحديث برامج الجهات الخارجية من الإصدار الحالي إلى الإصدار الأحدث فقط.

يمكن تغيير قائمة برامج الجهات الخارجية وتحديثها ديناميكيًا. ويمكنك التحقق مما إذا كان بإمكانك تحديث برنامج الجهة الخارجية (المثبت على أجهزة المستخدمين) باستخدام Kaspersky Security Center من خلال عرض قائمة التحديثات المتوفرة في وحدة تحكم الإدارة القائمة على MMC وKaspersky Security Center Web Console.

الإجراء الموضح أدناه مخصص فقط لعرض قائمة برامج الطرف الخارجي التي يمكن تحديثها باستخدام Kaspersky Security Center. ويتم إتباع الخطوات للوصول إلى المعلومات ذات الصلة دون بدء أي مهام.

لعرض قائمة برامج الجهات الخارجية التي يمكنك تحديثها باستخدام Kaspersky Security Center في Kaspersky Security Center Web Console:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

3. في خطوة **New task settings** في المعالج، حدد الإعدادات التالية:

a. في القائمة المنسدلة **Application**، حدد **Kaspersky Security Center**.

b. في حقل **Task type**، حدد **Install required updates and fix vulnerabilities**.

4. في خطوة **Task scope** في المعالج، حدد الخيار **Managed Devices**.

5. في خطوة **Specify rules for installing updates** في المعالج، انقر فوق الزر **Add**.
يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام زر **Next**.

6. في خطوة **Select rule type** في المعالج، حدد الخيار **Rule for third-party updates**.

7. في خطوة **المعايير العامة** في المعالج، حدد الخيار **Install all updates (except declined)**، ثم انقر فوق **Next**.

يتم عرض قائمة برامج الجهات خارجية.

لعرض قائمة ببرامج الجهات الخارجية التي يمكنك تحديثها باستخدام Kaspersky Security Center في وحدة التحكم القائمة على MMC، فإنك بحاجة إلى ترخيص إدارة الثغرات الأمنية والتصحيحات. وبخلاف ذلك، لن تتوفر مهمة **Install required updates and fix vulnerabilities**.

1. في شجرة وحدة التحكم، افتح المجلد **الأجهزة المُدارة**.

2. في مساحة عمل المجموعة، حدد علامة تبويب **المهام**.

3. انقر فوق الزر **إنشاء مهمة** لتشغيل معالج المهمة الجديدة. اتبع خطوات المعالج.

4. في صفحة المعالج **تحديد نوع المهمة**، حدد **Install required updates and fix vulnerabilities**.

5. في خطوة **Specify rules for installing updates** في المعالج، انقر فوق الزر **Add**.
يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام زر **Next**.

6. في خطوة **Select rule type** في المعالج، حدد الخيار **Rule for third-party updates**.

7. في خطوة **المعايير العامة** في المعالج، حدد الخيار **Install all updates (except declined)**، ثم انقر فوق **Next**.

يتم عرض قائمة برامج الجهات خارجية.

تثبيت تحديثات برامج الجهات الخارجية

يتيح Kaspersky Security Center لك إدارة تحديثات البرامج المثبتة على الأجهزة العميلة وإصلاح الثغرات الأمنية في تطبيقات Microsoft ومنتجات الصناع الآخرين للبرامج من خلال تثبيت التحديثات المطلوبة.

يبحث Kaspersky Security Center عن التحديثات من خلال مهمة البحث عن التحديثات وتنزيلها إلى مخزن التحديثات. بعد الانتهاء من البحث عن التحديثات، يزود التطبيق المسؤول بمعلومات حول التحديثات المتوفرة والثغرات الأمنية الموجودة في التطبيقات والتي يمكن إصلاحها باستخدام هذه التحديثات.

يتم تقديم معلومات حول التحديثات المتوفرة لـ Microsoft Windows بواسطة خدمة Windows Update. يمكن استخدام خادم الإدارة كخادم Windows Server Update Services (WSUS). لاستخدام خادم الإدارة كخادم (WSUS)، ينبغي تكوين مزامنة التحديثات مع Windows Update. بعد تكوين مزامنة البيانات مع Windows Update، يوفر خادم الإدارة تحديثات لخدمات Windows Update على الأجهزة في الوضع المركزي ومع التكرار المضبوط.

يمكنك أيضًا إدارة تحديثات البرامج من خلال سياسة عميل الشبكة. للقيام بذلك، ينبغي إنشاء سياسة عميل الشبكة وتكوين تحديث البرنامج في النوافذ المقابلة لمعالج السياسة الجديدة.

يمكن للمسؤول عرض قائمة بالتحديثات المتوفرة في المجلد الفرعي **تحديثات البرنامج** المضمن في المجلد **إدارة التطبيق**. يحتوي هذا المجلد على قائمة بالتحديثات لتطبيقات Microsoft ومنتجات صانعي البرامج الآخرين المستردة بواسطة خادم الإدارة الذي يمكن توزيعه على الأجهزة. بعد عرض معلومات حول التحديثات المتوفرة، يمكن للمسؤول تثبيتها على الأجهزة.

يقوم Kaspersky Security Center بتحديث بعض التطبيقات عن طريق إزالة الإصدار السابق للتطبيق وتثبيت الإصدار الجديد.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

تأكد من تمكين الخيار **عرض إدارة الثغرات الأمنية والتصحيح في النافذة تكوين الواجهة** لخوادم الإدارة الرئيسية والثانوية. بخلاف ذلك، تتعامل مهمة البحث عن التحديثات مع تحديثات WSUS فقط.

لأسباب تتعلق بالأمان، يتم تلقائيًا فحص أي تحديثات برامج، تابعة لطرف ثالث، تقوم بتثبيتها باستخدام ميزة إدارة الثغرات الأمنية والتصحيحات بحثًا عن البرامج الضارة بواسطة تقنيات Kaspersky. تُستخدم هذه التقنيات لعمليات فحص الملفات بشكل تلقائي، وتتضمن فحص الفيروسات، وتحليلًا ثابتًا، وتحليلًا ديناميكيًا، وتحليل السلوك في بيئة وضع الحماية والتعلم الآلي.

لا يقوم خبراء Kaspersky بإجراء تحليل يدوي لتحديثات برامج الجهات الخارجية التي يمكن تثبيتها من خلال استخدام ميزة إدارة الثغرات الأمنية والتصحيحات. بالإضافة إلى ذلك، لا يبحث خبراء Kaspersky عن الثغرات الأمنية (المعروفة أو غير المعروفة) أو الميزات غير الموثقة في مثل هذه التحديثات، ولا يجرون أنواعًا أخرى من تحليل التحديثات بخلاف تلك المحددة في الفقرة أعلاه.

قبل تثبيت التحديثات على جميع الأجهزة العميلة، يمكنك إجراء اختبار تثبيت للتأكد من أن التحديثات المثبتة لن تُحدث أعطال لعملية تشغيل التطبيقات الموجودة على الأجهزة.

السيناريو: تحديث برامج الجهات الخارجية

يوفر هذا القسم سيناريو لتحديث برامج الأطراف الخارجية المثبتة على أجهزة العميل. برنامج الجهة الخارجية يشتمل على تطبيقات من Microsoft وبائعي البرامج الآخرين. يتم توفير تحديثات تطبيقات Microsoft عبر خدمة Windows Update.

المتطلبات الأساسية

يجب أن يكون خادم الإدارة متصلاً بالإنترنت من أجل تثبيت تحديثات تطبيقات الأطراف الخارجية غير تطبيقات Microsoft.

بشكل افتراضي، لا يلزم اتصال خادم الإدارة بالإنترنت لتثبيت تحديثات برامج Microsoft على الأجهزة المدارة. على سبيل المثال، يمكن للأجهزة المدارة تنزيل تحديثات برامج Microsoft مباشرة من خوادم تحديث Microsoft أو من خادم Windows وخدمات تحديث خادم Microsoft Windowsالمنتشرة في شبكة مؤسستك. يجب أن يكون خادم الإدارة متصلاً بالإنترنت عند استخدامك لخادم الإدارة كخادم WSUS.

المراحل

تحديث برامج الجهات الخارجية يسري عبر مراحل:

1. **البحث عن التحديثات المطلوبة**

   للعثور على تحديثات برامج الأطراف الخارجية المطلوبة للأجهزة المُدارة، قم بتشغيل مهمة Find vulnerabilities and required updates. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المُكتشَفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

يتم إنشاء مهمة Find vulnerabilities and required updates تلقائيًا بواسطة معالج البدء السريع لخادم الإدارة. إذا لم تشغِّل المعالج، فقم بإنشاء المهمة أو تشغيل معالج البدء السريع الآن.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: فحص التطبيقات بحثًا عن الثغرات الأمنية، وجدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
- Kaspersky Security Center Web Console: إنشاء Find vulnerabilities and required updates المهمة، والبحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة

2 تحليل قائمة التحديثات التي تم العثور عليها

اعرض قائمة **Software updates** وحدد التحديثات التي ترغب في تثبيتها. لعرض معلومات تفصيلية حول كل تحديث، انقر على اسم التحديث في القائمة. لكل تحديث في القائمة، يمكنك أيضًا عرض إحصاءات حول تثبيت التحديث على أجهزة العميل.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: عرض معلومات حول التحديثات المتوفرة
- Kaspersky Security Center Web Console: عرض معلومات حول تحديثات برامج الجهات الخارجية المتوفرة

3 تكوين تثبيت التحديثات

عندما استلم Kaspersky Security Center قائمة تحديثات برامج الأطراف الخارجية، يمكنك تثبيتها على أجهزة العميل باستخدام مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو مهمة تثبيت تحديثات Windows Update. قم بإنشاء إحدى المهام التالية. يمكنك إنشاء هذه المهام في تبويب **Tasks** أو باستخدام قائمة **Software updates**.

تُستخدم مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية في تثبيت التحديثات لتطبيقات Microsoft، بما في ذلك التحديثات التي توفرها خدمة Windows Update وتحديثات برامج البائعين الآخرين. لاحظ أنه لا يمكن إنشاء هذه المهمة إلا إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات.

لا تتطلب مهمة تثبيت تحديثات Windows Update ترخيصًا، ولكن يمكن استخدامها لتثبيت تحديثات Windows Update فقط.

لتثبيت بعض تحديثات البرامج، يجب أن توافق على اتفاقية ترخيص المستخدم النهائي لبرنامج التثبيت. إذا رفضت اتفاقية ترخيص المستخدم النهائي، لن يتم تثبيت تحديث البرنامج.

يمكنك بدء مهمة تثبيت التحديث بالجدول. عند تحديد جدول المهام، تأكد من بدء مهمة تثبيت التحديث بعد اكتمال مهمة Find vulnerabilities and required updates.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إصلاح الثغرات الأمنية في التطبيقات، عرض معلومات حول التحديثات المتوفرة
- Kaspersky Security Center Web Console: إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، إنشاء مهمة تثبيت تحديثات Windows Update، عرض معلومات حول تحديثات برامج الجهات الخارجية المتوفرة

4 جدولة المهام

للتأكد من أن قائمة التحديث مُحدَّثة دائمًا، قم بجدولة مهمة Find vulnerabilities and required updates لتشغيل المهمة تلقائيًا من وقتٍ لآخر. بشكل افتراضي، يتم تحديد مهمة Find vulnerabilities and required updates لكي تبدأ يدويًا.

إذا كنت قد أنشأت مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك جدولتها لتعمل بالتكرار نفسه الذي تعمل به مهمة Find vulnerabilities and required updates أو أقل منه. عند جدولة مهمة تثبيت تحديثات Windows Update، لاحظ أنه من أجل هذه المهمة يجب أن تحدد قائمة التحديثات في كل مرة قبل بدء هذه المهمة.

عند جدولة المهام، تأكد من بدء مهمة تثبيت التحديث بعد اكتمال مهمة Find vulnerabilities and required updates.

5 الموافقة على تحديثات البرامج ورفضها (اختياري)

إذا كنت قد أنشأت مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك تحديد قواعد تثبيت التحديثات في خصائص المهمة. إذا كنت قد أنشأت مهمة تثبيت تحديثات Windows Update، يمكنك تخطي هذه الخطوة.

يمكنك لكل قاعدة تحديد التحديثات المراد تثبيتها اعتمادًا على حالة التحديث: غير محدد أو مقبول أو مرفوض. قد ترغب على سبيل المثال في إنشاء مخمة محددة للخوادم ووضع قاعدة لهذه المهمة من أجل السماح بتثبيت تحديثات Windows Update وفقط التحديثات التي بحالة مقبول. بعدها أنت تقوم يدويًا بتعيين حالة مقبول للتحديثات التي ترغب في تثبيتها. في هذه الحالة، لن يتم تثبيت تحديثات Windows Update التي بحالة غير محدد أو مرفوض على الخوادم التي حددتها في المهمة.

استخدام حالة مقبول لإدارة تثبيت التحديث أمر فعال لعدد صغير من التحديثات. لتثبيت عدة تحديثات، استخدم القواعد التي يمكنك تكوينها في مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. نوصي بتعيين حالة الموافقة لتلك التحديثات المحددة التي لا تفي بالمعايير المحددة في القواعد. عند الموافقة بشكل يدوي على عدد كبير من التحديثات، ينخفض أداء خادم الإدارة مما قد ينتج عنه التحميل الزائد على الخادم.

بشكل افتراضي، يكون لتحديثات البرامج التي تم تنزيلها حالة غير محددة. يمكنك تغيير الحالة إلى مقبول أو مرفوض في قائمة **Software updates** (**Operations ← Patch management ← Software updates**).

تعليمات للمساعدة:

- وحدة تحكم الإدارة: الموافقة على تحديثات البرامج ورفضها
- Kaspersky Security Center Web Console: الموافقة على تحديثات برامج الأطراف الخارجية ورفضها

6 **تكوين خادم الإدارة للعمل كخادم Windows Server Update Services (WSUS) (اختياري)**

يتم تنزيل تحديثات Windows Update بشكل افتراضي إلى الأجهزة المُدارة من خوادم Microsoft. يمكنك تغيير هذا الإعداد لاستخدام خادم الإدارة كخادم WSUS. يقوم خادم الإدارة في هذه الحالة بمزامنة بيانات التحديث مع Windows Update بالتكرار المحدد ويوفر تحديثات في وضع مركزي إلى Windows Update على الأجهزة المتصلة بالشبكة.

لاستخدام خادم الإدارة كخادم WSUS، قم بإنشاء مهمة إجراء مزامنة Windows Update وحدد خانة الاختيار **استخدام خادم الإدارة كخادم WSUS** في سياسة عميل الشبكة.

تعليمات للمساعدة:

- خادم الإدارة: مزامنة التحديثات من Windows Update مع خادم الإدارة، تكوين تحديثات Windows في سياسة عميل الشبكة.
- Kaspersky Security Center Web Console: إنشاء مهمة إجراء مزامنة Windows Update

7 **تشغيل مهمة تثبيت تحديث**

ابدأ مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو مهمة تثبيت تحديثات Windows Update. عندما تبدأ هذه المهام، يتم تنزيل التحديثات وتثبيتها على الأجهزة المُدارة. بعد اكتمال المهمة، تأكد من أنها بحالة مكتملة بنجاح في قائمة المهام.

8 **أنشئ التقرير حول نتائج تثبيت التحديث لبرنامج جهة خارجية (اختياري)**

لعرض إحصاءات تفصيلية حول تثبيت التحديث، قم بإنشاء **تقرير حول نتائج تثبيت تحديثات برنامج الجهة الخارجية**.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء تقرير وعرضه
- Kaspersky Security Center Web Console: إنشاء تقرير وعرضه

النتائج

إذا قمت بإنشاء وتكوين مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يتم تثبيت التحديثات على الأجهزة المُدارة تلقائيًا. عند تنزيل تحديثات جديدة إلى مستودع خادم الإدارة، يتحقق Kaspersky Security Center من أنها تستوفي المعايير المحددة في قواعد التحديث. سوف يتم تثبيت جميع التحديثات الجديدة التي تستوفي المعايير تلقائيًا عند التشغيل التالي للمهمة.

إذا قمت بإنشاء مهمة تثبيت تحديثات Windows Update، لا يتم تثبيت إلا التحديثات المحددة في خصائص مهمة تثبيت تحديثات Windows Update. في المستقبل إذا أردت تثبيت التحديثات الجديدة التي يتم تنزيلها إلى مستودع خادم الإدارة، يجب أن تضيف التحديثات المطلوبة إلى قائمة التحديثات في المهمة الموجودة أو إنشاء مهمة تثبيت تحديثات Windows Update جديدة.

عرض معلومات حول التحديثات المتوفرة لتطبيقات الطرف الثالث

لعرض قائمة بالتحديثات المتوفرة لتطبيقات الجهات الخارجية المثبتة على أجهزة العميل،

في المجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **تحديثات البرنامج**.

في مساحة عمل المجلد، يمكنك عرض قائمة بالتحديثات المتوفرة للتطبيقات المثبتة على الأجهزة.

لعرض خصائص تحديث,

في مساحة عمل المجلد **تحديثات البرنامج**، حدد **خصائص** في قائمة سياق التحديث.

تتوفر المعلومات التالية للعرض في نافذة خصائص التحديث:

- في قسم **عام** يمكنك عرض **حالة اعتماد التحديث**:
  - **غير معرّف** —التحديث متاح في قائمة التحديثات، لكن لم تتم الموافقة عليه للتثبيت.
  - **معتمد**—التحديث متاح في قائمة التحديثات والموافق عليه للتثبيت.
  - **تم رفضه** — تم رفض التحديث للتثبيت.
- في قسم **السمات** يمكنك عرض قيم حقل **تم التثبيت تلقائيًا**:
  - **تلقائيًا** يتم عرض القيمة إذا كان قم بتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية يمكن للمهمة تثبيت التحديثات للتطبيق. تقوم المهمة تلقائيًا بتثبيت التحديثات الجديدة من عنوان الويب المقدم من بائع برامج الجهة الخارجية.
  - **يدويًا** يتم عرض القيمة إذا لم يتمكن Kaspersky Security Center من تثبيت تحديثات التطبيق تلقائيًا. يمكنك تثبيت التحديثات يدويًا.

تم التثبيت تلقائيًا لا يتم عرض الحقل لتحديثات تطبيقات Windows.

- قائمة بأجهزة العملاء المنوط بها التحديث.
- قائمة مكونات النظام (المتطلبات الأساسية) التي يجب تثبيتها قبل التحديث (إن وجد).
- الثغرات الأمنية بالبرامج التي سيقوم التحديث بإصلاحها.

اعتماد ورفض تحديثات البرنامج

قد تتطلب إعدادات مهمة تثبيت تحديث الموافقة على التحديثات المراد تثبيتها. يمكنك الموافقة على التحديثات التي يجب تثبيتها ورفض التحديثات التي لا يتوجب تثبيتها.

على سبيل المثال، قد ترغب أولًا بالتحقق من تثبيت التحديثات في بيئة اختبار والتأكد من عدم تداخلها في عملية تشغيل الأجهزة، وبعد ذلك فقط تسمح بتثبيت تلك التحديثات على الأجهزة العميلة.

يعد استخدام الحالة موافق لإدارة تثبيت التحديث من جهة خارجية فعالًا لعدد صغير من التحديثات. لتثبيت عدة تحديثات من جهات خارجية، استخدم القواعد التي يمكنك تكوينها في مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. نوصي بتعيين حالة الموافقة لتلك التحديثات المحددة التي لا تفي بالمعايير المحددة في القواعد. عند الموافقة بشكل يدوي على عدد كبير من التحديثات، ينخفض أداء خادم الإدارة مما قد ينتج عنه التحميل الزائد على الخادم.

قم بما يلي للموافقة على أو رفض تحديث واحد أو عدة تحديثات:

1. في شجرة وحدة التحكم، حدد العقدة **خيارات متقدمة** ← **إدارة التطبيق** ← **تحديثات البرنامج**.

2. في مساحة عمل المجلد **تحديثات البرنامج**، انقر فوق الزر **تحديث** الموجود في الركن الأيمن العلوي. ستظهر قائمة بالتحديثات.

3. حدد التحديثات التي ترغب في الموافقة عليها أو رفضها.

   تظهر خانة المعلومات الخاصة بالكائنات المحددة في الجانب الأيمن لمساحة العمل.

4. في القائمة المنسدلة **حالة اعتماد التحديث**، حدد **معتمد** للموافقة على التحديثات المحددة أو حدد **تم رفضه** لرفض التحديثات المحددة.

   القيمة الافتراضية هي **غير معرّف**.

يتم وضع التحديثات التي تقوم بتعيين الحالة **معتمد** لها في قائمة انتظار للتثبيت.

يتم إلغاء تثبيت التحديثات التي تقوم بتعيين الحالة **تم رفضه** لها (إن أمكن) من جميع الأجهزة التي تم تثبيتها عليها سابقًا. لن يتم تثبيتها كذلك على أجهزة أخرى في المستقبل.

لا يمكن إلغاء تثبيت بعض تحديثات تطبيقات Kaspersky. إذا قمت بتعيين الحالة **تم رفضه** للتحديثات، فلن يقوم Kaspersky Security Center بإلغاء تثبيت هذه التحديثات من الأجهزة التي تم تثبيتها عليها سابقًا. ومع ذلك، لن يتم تثبيت هذه التحديثات أبدًا على أجهزة أخرى في المستقبل. إذا كان يتعذر إلغاء تثبيت أحد التحديثات لتطبيقات Kaspersky، فستظهر هذه الخاصية في نافذة خصائص التحديث: في جزء **الأقسام**، حدد **عام**، وستظهر الخاصية في مساحة العمل ضمن **متطلبات التثبيت**. إذا قمت بتعيين حالة **تم رفضه** لتحديثات برامج الجهات الخارجية، فلن يتم تثبيت هذه التحديثات على الأجهزة التي تم التخطيط لتثبيتها عليها لكنها لم تُثبَت بعد. ستظل التحديثات على الأجهزة التي تم تثبيتها عليها بالفعل. إذا كان يتعين عليك حذفها، فيمكنك حذفها يدويًا محليًا.

مزامنة التحديثات من Windows Update مع خادم الإدارة

إذا كنت قد حددت **استخدام خادم الإدارة كخادم WSUS** في نافذة **إعدادات إدارة التحديثات** الخاصة بمعالج البدء السريع، يتم إنشاء مهمة مزامنة Windows Update تلقائيًا. يمكنك تشغيل المهمة في المجلد **المهام**. تتوفر وظائف تحديث برامج Microsoft فقط بعد اكتمال مهمة **إجراء مزامنة Windows Update** بنجاح.

قد تتجاوز تحديثات برامج Microsoft حجم 10 جيجا بايت. تأكد أن قاعدة بيانات خادم الإدارة قادرة على استيعاب مثل هذه الأحجام؛ وإلا، ستفشل مهمة **إجراء مزامنة Windows Update**. لا يتم دعم قاعدة بيانات Microsoft SQL Express لمهمة **إجراء مزامنة Windows Update**.

تقوم المهمة **إجراء مزامنة Windows Update** بتنزيل البيانات الوصفية فقط من خوادم Microsoft. إذا لم تستخدم الشبكة خادم WSUS، فسيقوم كل جهاز عميل بتنزيل تحديثات Microsoft من خوادم خارجية بشكل مستقل.

لإنشاء مهمة لمزامنة تحديثات Windows مع خادم الإدارة:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **تحديثات البرنامج**.

2. انقر فوق الزر **إجراءات إضافية** وقم بتحديد **تكوين مزامنة Windows Update** في القائمة المنسدلة.

   يقوم المعالج بإنشاء المهمة **إجراء مزامنة Windows Update** التي يتم عرضها في مجلد **المهام**.

   يبدأ معالج إنشاء مهمة استرداد بيانات مركز تحديث Windows. اتبع إرشادات المعالج.

يمكنك أيضًا إنشاء مهمة إجراء مزامنة Windows Update في المجلد **المهام** عن طريق النقر فوق **إنشاء مهمة**.

تقوم Microsoft بحذف التحديثات القديمة من خوادم الشركة بشكل منتظم وبذلك يتراوح عدد التحديثات الحالية دائمًا ما بين 200 000 و300 000. لتقليل استخدام مساحة القرص وحجم قاعدة البيانات، يحذف Kaspersky Security Center التحديثات القديمة التي لم تعد موجودة على خوادم Microsoft Update.

عند تشغيل مهمة **إجراء مزامنة Windows Update**، يتلقى التطبيق قائمة بالتحديثات الحالية من خادم تحديث Microsoft. بعد ذلك، يقوم Kaspersky Security Center بتجميع قائمة بالتحديثات التي أصبحت قديمة. عند التشغيل التالي لمهمة **بحث عن الثغرات الأمنية والتحديثات المطلوبة**، يضع Kaspersky Security Center علامات على كل التحديثات القديمة ويحدد وقت حذفها. عند التشغيل التالي لمهمة **إجراء مزامنة Windows Update**، يتم حذف كل التحديثات التي تحمل علامة للحذف منذ 30 يومًا. كما يتحقق Kaspersky Security Center من التحديثات القديمة التي تم وضع علامة عليها للحذف منذ أكثر من 180 يومًا، ثم يحذف هذه التحديثات الأقدم.

عند اكتمال المهمة **إجراء مزامنة Windows Update** وحذف التحديثات القديمة، قد تظل قاعدة البيانات تحتوي على رموز تجزئة متعلقة بملفات التحديثات المحذوفة، بالإضافة إلى الملفات المقابلة في ملفات %Application\%AllUsersProfile\Data\KasperskyLab\adminkit\1093\.\working\wusfiles (إذا كان قد تم تنزيلها من قبل). يمكنك تشغيل المهمة **صيانة خادم الإدارة** لحذف هذه السجلات القديمة من قاعدة البيانات والملفات المقابلة.

الخطوة 1. تحديد ما إذا كان سيتم تقليل حركة المرور

عندما يقوم Kaspersky Security Center بمزامنة التحديثات مع خوادم Microsoft Windows Update، سيتم حفظ المعلومات حول جميع الملفات في قاعدة بيانات خادم الإدارة. يتم أيضًا تنزيل جميع الملفات اللازمة للتحديث على محرك الأقراص أثناء التفاعل مع وكيل تحديث Windows. على وجه الخصوص، يقوم Kaspersky Security Center بحفظ المعلومات حول ملفات التحديث السريع على قاعدة البيانات وتنزيلها عند اللزوم. يؤدي تنزيل ملفات التحديث السريع إلى تقليل المساحة الفارغة على محرك الأقراص.

لتجنب تقليل حجم مساحة القرص وللحد من حركة المرور، يمكنك تعطيل خيار **تنزيل ملفات التثبيت السريعة**.

إذا تم تحديد هذا الخيار، فسيتم تنزيل ملفات التحديث السريع عند تشغيل المهمة. لا يتم تحديد هذا الخيار افتراضيًا.

الخطوة 2. التطبيقات

في هذا القسم يمكنك تحديد التطبيقات التي سيتم تنزيل تحديثات لها.

إذا تم تحديد خانة الاختيار **جميع التطبيقات**، فسيتم تنزيل تحديثات لجميع التطبيقات الموجودة، ولجميع التطبيقات التي قد يتم إطلاقها في المستقبل.

يتم تحديد خانة الاختيار **جميع التطبيقات** بشكل افتراضي.

الخطوة 3. تحديث الفئات

في هذا القسم يمكنك تحديد فئات التحديثات التي سيتم تنزيلها على خادم الإدارة.

إذا تم تحديد خانة الاختيار **كافة الفئات**، فسيتم تنزيل تحديثات لجميع فئات التحديثات الموجودة، ولجميع الفئات التي قد تظهر في المستقبل.

يتم تحديد خانة الاختيار **كافة الفئات** بشكل افتراضي.

الخطوة 4. تحديثات اللغات

في هذه النافذة يمكنك تحديد لغات ترجمة التحديثات التي سيتم تنزيلها على خادم الإدارة. حدد أحد الخيارات التالية لتنزيل لغات ترجمة التحديثات:

- **تنزيل جميع اللغات بما في ذلك اللغات الجديدة**

  إذا تم تحديد هذا الخيار، فسيتم تنزيل جميع لغات ترجمة التحديثات المتوفرة على خادم الإدارة. يتم تحديد هذا الخيار افتراضيًا.

- **تنزيل اللغات المحددة**

  إذا تم تحديد هذا الخيار، فيمكنك تحديد من قائمة لغات ترجمة التحديثات اللغة التي يجب تنزيلها على خادم الإدارة.

الخطوة 5. تحديد الحساب لبدء المهمة

في النافذة **تحديد حساب لتشغيل المهمة**، يمكنك تحديد الحساب الذي تستخدمه عند تشغيل المهمة. حدد أحد الخيارات التالية:

- **الحساب الافتراضي**

  سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.

  يتم تحديد هذا الخيار افتراضيًا.

- **تحديد حساب**

  املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

  - **الحساب**

    الحساب الذي يتم تشغيل المهمة من خلاله.

  - **كلمة المرور**

    كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

الخطوة 6. تكوين جدول بدء المهمة

في صفحة المعالج **تكوين جدول المهمة**، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

  حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

  - **كل N ساعة**

    تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

    بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

  - **كل N يومًا**

    تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

    بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

  - **كل N أسبوعًا**

    تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

    بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

  - **كل N دقيقة**

    تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

    بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **مرة**

يتم تشغيل المهمة مرة واحدة، في التاريخ والوقت المحددين (افتراضيًا، في اليوم الذي تم إنشاء المهمة فيه).

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

الخطوة 7. تحديد اسم المهمة

في الصفحة **حدد اسم المهمة**، حدد اسم القاعدة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة (" * < > ? \ : |). وتكون القيمة الافتراضية هي إجراء مزامنة Windows Update.

الخطوة 8. إكمال إنشاء المهمة

في النافذة **إنهاء عملية إنشاء المهمة**، وانقر فوق زر **إنهاء** لإنهاء المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

ستظهر مهمة مزامنة Windows Update التي تم إنشاؤها حديثًا في قائمة المهام في المجلد **المهام** الخاص بشجرة وحدة التحكم.

تثبيت التحديثات على الأجهزة يدويًا

إذا قمت بتحديد **بحث عن التحديثات المطلوبة وتثبيتها** في الصفحة **إعدادات إدارة التحديثات** بمعالج البدء السريع، فسيتم إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية تلقائيًا. يمكنك تشغيل المهمة أو إيقافها في المجلد **الأجهزة المُدارة** على علامة التبويب **المهام**.

إذا قمت بتحديد **البحث عن تحديثات مطلوبة** في معالج البدء السريع، فيمكنك تثبيت تحديثات البرامج على الأجهزة العميلة من خلال المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.

يمكنك القيام بأحد الإجراءات التالية:

- إنشاء مهمة لتثبيت تحديثات.
- إضافة قاعدة لتثبيت تحديث لمهمة تثبيت تحديث حالية.
- من إعدادات مهمة تثبيت تحديث حالية، قم بتكوين اختبار تثبيت للتحديثات.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

تثبيت التحديثات عن طريق إضافة مهمة تثبيت

يمكنك القيام بأحد الإجراءات التالية:

- إنشاء مهمة لتثبيت تحديثات معينة.
- حدد تحديث وقم بإنشاء مهمة لتثبيته ولتثبيت التحديثات المماثلة.

لتثبيت تحديثات محددة:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **تحديثات البرنامج**.
2. من مساحة العمل، حدد التحديثات التي ترغب في تثبيتها.
3. قم بأحد الإجراءات التالية:
   - انقر بزر الماوس الأيمن فوق أحد التحديثات المحددة في القائمة، ثم حدد **تثبيت تحديث** ← **مهمة جديدة**.
   - انقر فوق الرابط **تثبيت تحديث (إنشاء مهمة)** في خانة معلومات التحديثات المحددة.
4. حدد اختيارك في المطالبة المعروضة حول تثبيت كافة تحديثات التطبيق السابقة. انقر فوق **نعم** إذا كنت موافق على تثبيت إصدارات التطبيق المتتالية تدريجيًا في حالة طُلب ذلك لتثبيت التحديثات المحددة. انقر فوق **لا** إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون تثبيت إصدارات متتابعة. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

   يبدأ معالج إنشاء مهمة تثبيت التحديثات وإصلاح الثغرات الأمنية. اتبع خطوات المعالج.

5. في صفحة المعالج **تحديد خيار إعادة تشغيل نظام التشغيل**، حدد الإجراء الذي سيتم اتخاذه عندما يلزم إعادة تشغيل نظام التشغيل على الأجهزة العميلة بعد عملية التشغيل:

- **لا تقم بإعادة تشغيل الجهاز**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **أعد تشغيل الجهاز**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **مطالبة المستخدم باتخاذ إجراء**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **تكرار المطالبة كل (بالدقائق)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **إعادة التشغيل بعد (دقيقة)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

6. في صفحة **تكوين جدول المهمة** للمعالج، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

7. في صفحة المعالج **حدد اسم المهمة**، حدد اسم المهمة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

8. في صفحة **إنهاء عملية إنشاء المهمة** في المعالج، انقر على زر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

بعد قيام المعالج باستكمال عملياته، تظهر **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية** في مجلد **المهام**.

يمكنك تمكين التثبيت التلقائي لمكونات النظام (المتطلبات الأساسية) قبل تثبيت تحديث في خصائص مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. عند تمكين هذا الخيار، يتم تثبيت جميع مكونات النظام المطلوبة قبل التحديث. ويمكن العثور على قائمة بالمكونات المطلوبة في خصائص التحديث.

في خصائص مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك السماح بتثبيت التحديثات التي تؤدي إلى ترقية التطبيق إلى إصدار جديد.

إذا كانت إعدادات المهمة تقدم قواعد لتثبيت تحديثات الجهات الخارجية، فسيقوم خادم الإدارة بتنزيل جميع التحديثات ذات الصلة من مواقع البائعين التابعين لتلك الجهات. ويتم حفظ التحديثات في مستودع خادم الإدارة ثم توزيعها وتثبيتها على الأجهزة حسب الاقتضاء.

إذا كانت إعدادات المهمة تقدم قواعد لتثبيت تحديثات Microsoft وكان خادم الإدارة يعمل كخادم WSUS، فسيقوم خادم الإدارة بتنزيل جميع التحديثات ذات الصلة إلى المستودع ثم توزيعها على الأجهزة المدارة. إذا لم تستخدم الشبكة خادم WSUS، فسيقوم كل جهاز عميل بتنزيل تحديثات Microsoft من خوادم خارجية بشكل مستقل.

لتثبيت تحديث محدد وتحديثات مماثلة:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **تحديثات البرنامج**.

2. من مساحة العمل، حدد التحديث الذي ترغب في تثبيته.

3. انقر على زر **تشغيل معالج تثبيت التحديث**.

يبدأ تشغيل معالج تثبيت التحديث.

> لا تتوفر ميزات معالج تثبيت التحديث إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

اتبع خطوات المعالج.

4. في الصفحة **البحث عن مهام تثبيت التحديثات الموجودة**، حدد الإعدادات التالية:

- **البحث عن مهام تثبيت هذا التحديث**

إذا تم تمكين هذا الخيار، فسيبحث معالج تثبيت التحديث عن المهام الحالية التي تقوم بتثبيت التحديث المحدد.

إذا تم تعطيل هذا الخيار أو إذا لم يسترجع البحث أي مهام سارية، فسيطالبك معالج تثبيت التحديث بإنشاء قاعدة أو مهمة لتثبيت التحديث.

يتم تمكين هذا الخيار افتراضيًا.

- **الموافقة على تثبيت التحديث**

سيتم اعتماد التحديث المحدد للتثبيت. تمكين هذا الخيار في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها فقط.

يتم تعطيل هذا الخيار افتراضيًا.

5. إذا اخترت البحث عن مهام تثبيت التحديث الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدويًا. لا يلزم اتخاذ إجراءات إضافية.

عدا ذلك، قم بالنقر فوق الزر **مهمة تثبيت التحديث الجديد**.

6. حدد نوع قاعدة التثبيت التي ستضاف إلى المهمة الجديدة، ثم انقر فوق الزر **إنهاء**.

7. حدد اختيارك في المطالبة المعروضة حول تثبيت كافة تحديثات التطبيق السابقة. انقر فوق **نعم** إذا كنت موافق على تثبيت إصدارات التطبيق المتتالية تدريجيًا في حالة طُلب ذلك لتثبيت التحديثات المحددة. انقر فوق **لا** إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون تثبيت إصدارات متتابعة. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

يبدأ معالج إنشاء مهمة تثبيت التحديثات وإصلاح الثغرات الأمنية. اتبع خطوات المعالج.

8. في صفحة المعالج **تحديد خيار إعادة تشغيل نظام التشغيل**، حدد الإجراء الذي سيتم اتخاذه عندما يلزم إعادة تشغيل نظام التشغيل على الأجهزة العميلة بعد عملية التشغيل:

- **لا تقم بإعادة تشغيل الجهاز**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **أعد تشغيل الجهاز**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **مطالبة المستخدم باتخاذ إجراء**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **تكرار المطالبة كل (بالدقائق)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **إعادة التشغيل بعد (دقيقة)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

9. في صفحة المعالج **حدد الأجهزة التي سيتم تعيين المهمة لها**، وحدد أحد الخيارات التالية:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة**

يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لمهمة تثبيت عميل الشبكة على الأجهزة غير المخصصة.

- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**

يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

- **تعيين مهمة إلى تحديد الجهاز**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

- **تعيين مهمة لمجموعة إدارة**

يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

10. في صفحة **تكوين جدول المهمة** للمعالج، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا** (يتم تحديده بصورة افتراضية)

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

11. في صفحة المعالج **حدد اسم المهمة**، حدد اسم المهمة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

12. في صفحة **إنهاء عملية إنشاء المهمة** في المعالج، انقر على زر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

عند انتهاء المعالج، يتم إنشاء المهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية** وعرضها في مجلد **المهام**.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

قد تؤدي الترقية إلى إصدار جديد للتطبيق إلى حدوث خلل في التطبيقات التابعة على أجهزة الكمبيوتر العميلة.

تثبيت تحديث من خلال إضافة قاعدة لمهمة تثبيت حالية

لتثبيت تحديث من خلال إضافة قاعدة لمهمة تثبيت حالية:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **تحديثات البرنامج**.

2. من مساحة العمل، حدد التحديث الذي ترغب في تثبيته.

3. انقر على زر **تشغيل معالج تثبيت التحديث**.

   يبدأ تشغيل معالج تثبيت التحديث.

لا تتوفر ميزات معالج تثبيت التحديث إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

   اتبع خطوات المعالج.

4. في الصفحة **البحث عن مهام تثبيت التحديثات الموجودة**، حدد الإعدادات التالية:

   - **البحث عن مهام تثبيت هذا التحديث**

     إذا تم تمكين هذا الخيار، فسيبحث معالج تثبيت التحديث عن المهام الحالية التي تقوم بتثبيت التحديث المحدد.

     إذا تم تعطيل هذا الخيار أو إذا لم يسترجع البحث أي مهام سارية، فسيطالبك معالج تثبيت التحديث بإنشاء قاعدة أو مهمة لتثبيت التحديث.

     يتم تمكين هذا الخيار افتراضيًا.

   - **الموافقة على تثبيت التحديث**

     سيتم اعتماد التحديث المحدد للتثبيت. تمكين هذا الخيار في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها فقط.

     يتم تعطيل هذا الخيار افتراضيًا.

5. إذا اخترت البحث عن مهام تثبيت التحديث الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدويًا. لا يلزم اتخاذ إجراءات إضافية.

   عدا ذلك، انقر على زر **إضافة قاعدة تثبيت تحديث**.

6. حدد المهمة التي ترغب في إضافة قاعدة لها، ثم انقر فوق الزر **إضافة قاعدة**.

   أيضًا، يمكنك عرض خصائص المهام الحالية، أو بدئهم يدويًا، أو إنشاء مهمة جديدة.

7. حدد نوع القاعدة التي ستضاف إلى المهمة المحددة، ثم انقر فوق الزر **إنهاء**.

8. حدد اختيارك في المطالبة المعروضة حول تثبيت كافة تحديثات التطبيق السابقة. انقر فوق **نعم** إذا كنت موافق على تثبيت إصدارات التطبيق المتتالية تدريجيًا في حالة طُلب ذلك لتثبيت التحديثات المحددة. انقر فوق **لا** إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون تثبيت إصدارات متتابعة. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

   تتم إضافة قاعدة جديدة لتثبيت التحديث إلى مهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية**الحالية.

تكوين اختبار تثبيت للتحديثات

لتكوين اختبار تثبيت للتحديثات:

1. في شجرة وحدة التحكم، حدد المهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية** في المجلد **الأجهزة المُدارة** على علامة التبويب **المهام**.

2. من قائمة سياق المهمة، حدد **خصائص**.

   يتم فتح نافذة خصائص مهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية**.

3. في نافذة خصائص المهمة، في القسم **تثبيت الاختبار**، حدد أحد الخيارات المتوفرة للتثبيت الاختباري:

   - **عدم الفحص**. حدد هذا الخيار إذا كنت لا ترغب في إجراء تثبيت اختباري للتحديثات.
   - **تشغيل الفحص على الأجهزة المحددة**. حدد هذا الخيار إذا كنت ترغب في اختبار تثبيت التحديثات على الأجهزة المحددة. انقر فوق الزر **إضافة** وحدد الأجهزة التي تحتاج إلى إجراء تثبيت اختباري للتحديثات عليها.
   - **تشغيل الفحص على الأجهزة في المجموعة المحددة**. حدد هذا الخيار إذا كنت ترغب في اختبار تثبيت التحديثات على مجموعة الأجهزة. في الحقل **تحديد مجموعة اختبار**، حدد مجموعة الأجهزة التي تريد إجراء تثبيت اختباري عليها.
   - **تشغيل الفحص على النسبة المئوية المحددة من الأجهزة**. حدد هذا الخيار إذا كنت ترغب في اختبار تثبيت التحديثات على بعض أجزاء الأجهزة. في الحقل **نسبة أجهزة الاختبار من كل الأجهزة الهدف**، حدد نسبة الأجهزة التي تريد إجراء تثبيت اختباري للتحديثات عليها.

4. بمجرد تحديد أي من الخيارات باستثناء **عدم الفحص**، في الحقل **مقدار الوقت اللازم لاتخاذ القرار في حال استمرار التثبيت، بالساعات**، حدد عدد الساعات التي يجب انقضائها من التثبيت الاختباري للتحديثات حتى بدء تثبيت التحديثات على جميع الأجهزة.

تكوين تحديثات Windows في سياسة عميل الشبكة

لتكوين تحديثات Windows في سياسة عميل الشبكة:

1. في شجرة وحدة التحكم، حدد **الأجهزة المُدارة**.

2. في مساحة العمل، حدد علامة التبويب **السياسات**.

3. حدد سياسة عميل الشبكة.

4. في قائمة السياق للسياسة، حدد **خصائص**.

   يتم فتح نافذة خصائص سياسة عميل الشبكة.

5. في جزء **الأقسام**، حدد **تحديثات البرنامج والثغرات الأمنية**.

6. حدد خيار **استخدام خادم الإدارة كخادم WSUS** لتنزيل تحديثات Windows إلى خادم الإدارة ثم توزيعها على الأجهزة العميلة من خلال عميل الشبكة.

   إذا لك يتم تحديد هذا الخيار، فلت يتم تنزيل تحديثات Windows في خادم الإدارة. في هذه الحالة، تتلقى الأجهزة العميلة تحديثات Windows بشكل مباشر من خوادم Microsoft.

7. حدد مجموعة التحديثات التي يمكن للمستخدمين تثبيتها يدويًا على أجهزتهم من خلال استخدام Windows Update.

في الأجهزة التي تعمل بنظام التشغيل Windows 10، إذا عثر تحديث Windows على تحديثات للجهاز، فلن يتم تطبيق الخيار الجديد الذي عثرت عليه إلا بعد تثبيت التحديثات التي تم العثور عليها **السماح للمستخدمين بإدارة تثبيت تحديثات Windows Update**.

حدد أحد العناصر في القائمة المنسدلة:

- **السماح للمستخدمين بتثبيت جميع تحديثات Windows Update القابلة للتطبيق**

يمكن للمستخدمين تثبيت كافة تحديثات Microsoft Windows Update القابلة للتطبيق على الأجهزة الخاصة بهم.

حدد هذا الخيار إذا كنت لا تريد التدخل في تثبيت التحديثات.

> عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلًا من خادم الإدارة. يمكن ذلك في حالة عدم قيام خادم الإدارة بتنزيل هذه التحديثات بعد. ينتج عن تنزيل التحديثات من خوادم Microsoft حركة مرور إضافية.

- **السماح للمستخدمين بتثبيت تحديثات Windows Update المعتمدة فقط**

يمكن للمستخدمين تثبيت كافة تحديثات Microsoft Windows Update القابلة للتطبيق على الأجهزة الخاصة بهم والمعتمدة من قبلك.

على سبيل المثال، قد ترغب أولًا بالتحقق من تثبيت التحديثات في بيئة اختبار والتأكد من عدم تداخلهم في عملية تشغيل الأجهزة، وبعد ذلك فقط تسمح بتثبيت تلك التحديثات المعتمدة على أجهزة العميل.

> عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلًا من خادم الإدارة. يمكن ذلك في حالة عدم قيام خادم الإدارة بتنزيل هذه التحديثات بعد. ينتج عن تنزيل التحديثات من خوادم Microsoft حركة مرور إضافية.

- **عدم السماح للمستخدمين بتثبيت تحديثات Windows Update**

لا يمكن للمستخدمين تثبيت تحديثات Microsoft Windows Update على الأجهزة الخاصة بهم يدويًا. تم تثبيت جميع التحديثات القابلة للتطبيق كما قمت بتكوينها.

حدد هذا الخيار إذا كنت تريد إدارة تثبيت التحديثات مركزيًا.

على سبيل المثال، قد ترغب في تحسين جدول التحديث لكي لا تصبح الشبكة محملة بشكل زائد. يمكنك جدولة التحديثات بعد ساعات العمل، بحيث لا تتعارض مع إنتاجية المستخدم.

8. حدد وضع بحث Windows Update:

- **نشط**

إذا تم تحديد هذا الخيار، فسيتم دعم خادم الإدارة من عميل الشبكة الذي يبدأ طلب من وكيل تحديث Windows على الجهاز العميل إلى مصدر تحديث: خوادم Windows Update أو WSUS. ثم يمرر عميل الشبكة المعلومات التي تم الحصول عليها من وكيل تحديث Windows إلى خادم الإدارة.

لا يصبح الخيار ساريًا إلا إذا تم تحديد الخيار **الاتصال بخادم التحديث لتحديث البيانات** لمهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة.

يتم تحديد هذا الخيار افتراضيًا.

- **سلبي**

إذا قمت بتحديد هذا الخيار، فيقوم عميل الشبكة بشكل دوري بتمرير معلومات حول التحديثات التي تم استردادها في آخر عملية مزامنة لـ Windows Update مع مصدر التحديث إلى خادم الإدارة. في حالة عدم إجراء مزامنة لوكيل تحديث Windows مع مصدر تحديث، تصبح المعلومات حول التحديثات على خادم الإدارة غير محدثة.

حدد هذا الخيار إذا كنت ترغب في الحصول على تحديثات من ذاكرة التخزين المؤقت لمصدر التحديث.

- **معطل**

إذا كان هذا الخيار مجددًا، لا يقوم خادم الإدارة بطلب أي معلومات حول التحديثات.

حدد هذا الخيار إذا كنت تريد، على سبيل المثال، اختبار التحديثات على جهازك المحلي أولاً.

9. حدد خيار **فحص الملفات التنفيذية للبحث عن الثغرات الأمنية عند تشغيلها** إذا كنت ترغب في فحص الملفات التنفيذية لاكتشاف الثغرات الأمنية عند تشغيلها.

10. تأكد من قفل التحرير لجميع الإعدادات التي قمت بتغييرها. بخلاف ذلك، لن تطبق التغييرات.

11. انقر على **تطبيق** .

إصلاح الثغرات الأمنية ببرامج الجهات الخارجية

يصف هذا القسم ميزات Kaspersky Security Center المتعلقة بإصلاح الثغرات الأمنية في البرامج المثبتة على الأجهزة المُدارة.

السيناريو: البحث عن الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها

يوفر هذا القسم سيناريو للعثور على الثغرات الأمنية وإصلاحها على الأجهزة المُدارة التي تشغل Windows. يمكنك العثور على الثغرات الأمنية بالبرامج وإصلاحها في نظام التشغيل وفي برامج الجهات الخارجية، بما في ذلك برامج Microsoft.

المتطلبات الأساسية

- يتم نشر Kaspersky Security Center في مؤسستك.
- هناك أجهزة مُدارة تشغل نظام Windows في مؤسستك.
- يلزم اتصال خادم الإدارة بالإنترنت للقيام بالمهام التالية:
  - لعمل قائمة بالإصلاحات الموصى بها بشأن الثغرات الأمنية في برنامج Microsoft. يقوم المتخصصون من Kaspersky بإنشاء القائمة وتحديثها بانتظام.
  - لإصلاح الثغرات الأمنية في برامج الطرف الثالث بدلاً من برامج Microsoft.

المراحل

يستمر البحث عن ثغرات البرامج وإصلاحها على مراحل:

1. **البحث عن الثغرات الأمنية في البرنامج المثبتة على الأجهزة المُدارة**

للعثور على الثغرات المنية الموجودة في البرامج المثبت على الأجهزة المُدارة، قم بتشغيل المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المُكتشَفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

تم إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا بواسطة معالج البدء السريع لـ Kaspersky Security Center. إذا لم تشغِّل المعالج، ابدأ تشغيله الآن أو أنشئ المهمة يدويًا.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: فحص التطبيقات بحثًا عن الثغرات الأمنية، وجدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
- Kaspersky Security Center Web Console: إنشاء بحث عن الثغرات الأمنية والتحديثات المطلوبة المهمة، والبحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة

2. **تحليل قائمة الثغرات الأمنية المكتشَفة بالبرامج**

اعرض القائمة **الثغرات الأمنية بالبرنامج** وحدد الثغرات الأمنية التي يجب إصلاحها. لعرض معلومات تفصيلية حول كل ثغرة أمنية، انقر فوق اسم الثغرة الأمنية في القائمة. لكل ثغرة أمنية في القائمة، يمكنك أيضًا عرض الإحصاءات حول الثغرة الأمنية في الأجهزة المُدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: عرض معلومات حول الثغرات الأمنية في البرامج، وعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة
- Kaspersky Security Center Web Console: عرض معلومات حول ثغرات البرامج، وعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة

3 تكوين إصلاح الثغرات الأمنية

عند اكتشاف الثغرات الأمنية بالبرامج، يمكنك إصلاح الثغرات الأمنية بالبرامج على الأجهزة المُدَارة باستخدام المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو المهمة إصلاح الثغرات الأمنية.

تُستخدَم المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية لتحديث وإصلاح الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها، بما في ذلك برامج Microsoft المثبتة على الأجهزة المُدارة. تتيح لك هذه المهمة تثبيت تحديثات متعددة وإصلاح ثغرات أمنية متعددة وفقًا لقواعد معينة. لاحظ أنه لا يمكن إنشاء هذه المهمة إلا إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات. لإصلاح الثغرات الأمنية بالبرامج تستخدم المهمةتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية تحديثات البرامج الموصى بها.

لا تتطلب مهمة إصلاح الثغرات الأمنية وجود خيار الترخيص لميزة إدارة الثغرات الأمنية والتصحيحات. لاستخدام هذه المهمة، يجب عليك تحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية المدرجة في إعدادات المهام تحديدًا يدويًا. تستخدم المهمة إصلاح الثغرات الأمنية الإصلاحات الموصى بها لبرامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية.

يمكنك بدء تشغيل معالج إصلاح الثغرات الأمنية الذي ينشئ إحدى هذه المهام تلقائيًا، أو يمكنك إنشاء واحدة من هذه المهام يدويًا.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية، إصلاح الثغرات الأمنية في التطبيقات
- Kaspersky Security Center Web Console: تحديد إصلاحات المستخدم للثغرات الأمنية في برنامج الجهة الخارجية، وإصلاح الثغرات الأمنية في برامج الجهات الخارجية، وإنشاء تثبيت التحديثات المطلوبة وإصلاح مهمة الثغرات الأمنية

4 جدولة المهام

للتأكد من أن قائمة الثغرات الأمنية مُحدَّثة دائمًا، قم بجدولة المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة لتشغيلها تلقائيًا من وقتٍ لآخر. متوسط التكرار الموصى به هو مرة واحدة في الأسبوع.

إذا كنت قد أنشأت المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، فيمكنك جدولتها لتعمل مع نفس تردد المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة أو أقل غالبًا. عند وضع جدول إصلاح الثغرات الأمنية للمهمة، لاحظ أنه يجب تحديد إصلاحات لبرامج Microsoft أو تحديد إصلاحات المستخدم لبرامج الطرف الثالث في كل مرة قبل بدء المهمة.

عند جدولة المهام، تأكد من أن مهمة إصلاح الثغرات الأمنية تبدأ بعد استكمال المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة.

5 تجاهل الثغرات الأمنية في البرامج (اختياري)

إذا كنت تريد، فيمكنك تجاهل الثغرات الأمنية بالبرامج التي يلزم إصلاحها على جميع الأجهزة المُدارة أو على الأجهزة المُدارة المحددة فحسب.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تجاهل الثغرات الأمنية بالبرامج
- Kaspersky Security Center Web Console: تجاهل الثغرات الأمنية في البرامج

6 تشغيل مهمة إصلاح الثغرات الأمنية

ابدأ المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو المهمة إصلاح الثغرات الأمنية. عند اكتمال المهمة، تأكد من وجود الحالة مكتمل بنجاح في قائمة المهام.

7 إنشاء تقرير حول نتائج إصلاح الثغرات الأمنية في البرامج (اختياري)

لعرض إحصاءات تفصيلية حول إصلاح الثغرات الأمنية، قم بإنشاء تقرير الثغرات الأمنية. يعرض التقرير معلومات حول الثغرات الأمنية بالبرامج التي لم يتم إصلاحها. وبالتالي، يمكن أن يكون لديك فكرة عن العثور على ثغرات أمنية وإصلاحها في برامج الجهات الخارجية، بما في ذلك برامج Microsoft، في مؤسستك.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء تقرير وعرضه
- Kaspersky Security Center Web Console: إنشاء تقرير وعرضه

8 **التحقق من تكوين البحث عن الثغرات الامنية وإصلاحها في برامج الجهات الخارجية**

تأكد من أنك قد قمت بما يلي:

- تم الحصول على الثغرات الأمنية بالبرامج ومراجعتها على الأجهزة المُدارة
- تجاهل الثغرات الأمنية في البرامج إذا أردت
- تم تكوين المهمة لإصلاح الثغرات الأمنية
- جدولة المهام للعثور على الثغرات الأمنية للبرامج وإصلاحها حتى تبدأ بالتتابع
- تم التحقق من تشغيل مهمة إصلاح الثغرات الأمنية في البرامج

النتائج

إذا أنشأت المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وكوَّنتها، يتم إصلاح الثغرات الأمنية على الأجهزة المُدارة تلقائيًا. عند تشغيل المهمة، فإنها تربط قائمة تحديثات البرامج المتاحة بالقواعد المحددة في إعدادات المهمة. سيتم تنزيل جميع تحديثات البرامج التي تفي بالمعايير الواردة في القواعد على مستودع خادم الإدارة وسيتم تثبيتها لإصلاح الثغرات الأمنية بالبرامج.

إذا كنت قد أنشأت المهمة إصلاح الثغرات الأمنية، فسيتم إصلاح الثغرات الأمنية في البرامج فقط في برامج Microsoft.

حول البحث عن الثغرات الأمنية بالبرامج وإصلاحها

يكتشف Kaspersky Security Center ويصلح الثغرات الأمنية على الأجهزة المُدارة التي تعمل بأنظمة تشغيل عائلات Microsoft Windows. تم الكشف عن الثغرات الأمنية في نظام التشغيل وفي برامج الجهات الخارجية، بما فيها برامج Microsoft.

وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية)، بالإضافة إلى وظيفة KSN التي قد لا تكون متاحة في البرنامج في الولايات المتحدة الأمريكية.

العثور على الثغرات الأمنية بالبرامج

للعثور على الثغرات الأمنية بالبرامج، يستخدم Kaspersky Security Center الخصائص من قاعدة بيانات الثغرات الأمنية المعروفة. يتم إنشاء قاعدة البيانات هذه بواسطة أخصائيين في Kaspersky. يحتوي على معلومات حول الثغرات الأمنية، مثل وصفها وتاريخ اكتشافها ومستوى شدتها. يمكنك العثور على تفاصيل الثغرات الأمنية بالبرامج على موقع ويب Kaspersky.

يستخدم Kaspersky Security Center المهمةبحث عن الثغرات الأمنية والتحديثات المطلوبة للعثور على الثغرات الأمنية بالبرامج.

في بعض الحالات، يمكن إصلاح الثغرات الأمنية المكتشفة في نظام التشغيل Microsoft Windows باستخدام أي من الطرق التالية:

- تثبيت تحديث لنظام التشغيل.
- ترقية نظام التشغيل إلى إصدار أحدث (على سبيل المثال، من Windows 10 إلى Windows 11).

في هذا السيناريو، يعرض Kaspersky Security Center إدخالين للثغرة الأمنية نفسها.

إصلاح الثغرات الأمنية في البرامج

لإصلاح الثغرات الأمنية بالبرامج، يستخدم Kaspersky Security Center تحديثات البرامج الصادرة عن بائعي البرامج. يتم تنزيل بيانات تعريف تحديثات البرامج إلى مستودع خادم الإدارة نتيجة تشغيل المهام التالية:

- تنزيل التحديثات إلى مستودع خادم الإدارة. تهدف هذه المهمة إلى تنزيل بيانات التعريف الخاصة بالتحديثات لـ Kaspersky وبرامج الجهات الخارجية. يتم إنشاء هذه المهمة تلقائيًا من خلال معالج البدء السريع في Kaspersky Security Center. يمكنك إنشاء تحديثات التنزيل لمهمة مستودع خادم الإدارة يدويًا.
- إجراء مزامنة Windows Update. تهدف هذه المهمة إلى تنزيل بيانات التعريف الخاصة بالتحديثات لبرامج Microsoft.

يمكن تمثيل تحديثات البرامج لإصلاح الثغرات الأمنية كحزم توزيع كاملة أو تصحيحات. تحديثات البرنامج التي تعمل على إصلاح الثغرات الأمنية بالبرامج تُسمى إصلاحات. الإصلاحات الموصى بها هي تلك الموصى بها للتثبيت بواسطة أخصائيين في Kaspersky. إصلاحات المستخدم هي التحديثات التي تُحدَّد يدويًا للتثبيت من خلال المستخدمين. لتثبيت إصلاح مستخدم، يجب عليك إنشاء حزمة تثبيت تحتوي على هذا الإصلاح.

إذا كان لديك ترخيص Kaspersky Security Center مع ميزة إدارة الثغرات الأمنية والتصحيحات، فيمكنك لإصلاح ثغرات البرامج التي يمكنك استخدام المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. تعمل هذه المهمة تلقائيًا على إصلاح ثغرات أمنية متعددة تقوم بتثبيت الإصلاحات الموصى بها. لهذه المهمة، يمكنك تكوين قواعد معينة يدويًا لإصلاح ثغرات أمنية متعددة.

إذا لم يكن لديك ترخيص Kaspersky Security Center مع ميزة إدارة الثغرات الأمنية والتصحيحات، لإصلاح الثغرات الأمنية في البرامج، فيمكنك استخدام المهمة إصلاح الثغرات الأمنية. عن طريق هذه المهمة، يمكنك إصلاح الثغرات الأمنية عن طريق تثبيت الإصلاحات الموصى بها لبرامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية.

لأسباب تتعلق بالأمان، يتم تلقائيًا فحص أي تحديثات برامج، تابعة لطرف ثالث، تقوم بتثبيتها باستخدام ميزة إدارة الثغرات الأمنية والتصحيحات بحثًا عن البرامج الضارة بواسطة تقنيات Kaspersky. تُستخدم هذه التقنيات لعمليات فحص الملفات بشكل تلقائي، وتتضمن فحص الفيروسات، وتحليلًا ثابتًا، وتحليلًا ديناميكيًا، وتحليل السلوك في بيئة وضع الحماية والتعلم الآلي.

لا يقوم خبراء Kaspersky بإجراء تحليل يدوي لتحديثات برامج الجهات الخارجية التي يمكن تثبيتها من خلال استخدام ميزة إدارة الثغرات الأمنية والتصحيحات. بالإضافة إلى ذلك، لا يبحث خبراء Kaspersky عن الثغرات الأمنية (المعروفة أو غير المعروفة) أو الميزات غير الموثقة في مثل هذه التحديثات، ولا يجرون أنواعًا أخرى من تحليل التحديثات بخلاف تلك المحددة في الفقرة أعلاه.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

لإصلاح بعض الثغرات الأمنية في البرامج، يجب عليك قبول اتفاقية ترخيص المستخدم النهائي لتثبيت البرنامج إذا كانت الموافقة على اتفاقية ترخيص المستخدم النهائي مطلوبة. إذا رفضت اتفاقية ترخيص المستخدم النهائي، فلا يتم إصلاح الثغرات الأمنية بالبرامج.

عرض معلومات حول الثغرات الأمنية بالبرنامج

لعرض قائمة بالثغرات الأمنية التي تم اكتشافها على الأجهزة العميلة,

في المجلد **خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **الثغرات الأمنية بالبرنامج**.

تعرض الصفحة قائمة بالثغرات الأمنية في التطبيقات المكتشفة على الأجهزة المُدارة.

للعثور على معلومات حول الثغرات الأمنية المحددة,

حدد **خصائص** من قائمة سياق الثغرة الأمنية.

يتم فتح نافذة خصائص الثغرات الأمنية، حيث تعرض المعلومات التالية:

- التطبيق الذي تم اكتشاف الثغرة الأمنية عليه.
- قائمة بالأجهزة التي تم اكتشاف الثغرة الأمنية عليها.
- معلومات حول ما إذا تم إصلاح الثغرات الأمنية أم لا.

لعرض تقرير حول جميع الثغرات الأمنية التي تم اكتشافها,

في المجلد **الثغرات الأمنية بالبرنامج**، انقر فوق الرابط **عرض تقرير الثغرات الأمنية**.

سيتم إنشاء تقرير الثغرات الأمنية في التطبيقات المثبتة على الأجهزة. يمكنك عرض هذا التقرير في العقدة التي تحمل اسم خادم الإدارة ذو الصلة، عن طريق فتح علامة تبويب **التقارير**.

عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة

يمكنك عرض إحصائيات لكل ثغرة أمنية في البرامج على الأجهزة المُدارة. تُمثَّل الإحصاءات في شكل مخطط. يعرض المخطط عدد الأجهزة بالحالات التالية:

- تم تجاهله على: <عدد الأجهزة>. يتم تعيين هذه الحالة إذا عيَّنت يدويًا، في خصائص الثغرة الأمنية، الخيار لتجاهل الثغرات الأمنية.
- مثبت على: <عدد الأجهزة>. يتم تعيين هذه الحالة إذا تم إكمال مهمة إصلاح الثغرات الأمنية بنجاح.
- الإصلاح مقرر في: <عدد الأجهزة> . يتم تعيين هذه الحالة إذا كنت قد أنشأت المهمة لإصلاح الثغرات الأمنية لكن لم يتم تنفيذ المهمة بعد.
- التصحيح المطبق على: <عدد الأجهزة>. يتم تعيين هذه الحالة إذا حددت تحديث برنامج يدويًا لإصلاح الثغرات الأمنية لكن تحديث البرنامج هذا لم يحل الثغرات الأمنية.
- الإصلاح مطلوب في: <عدد الأجهزة>. يتم تعيين هذه الحالة في حالة إصلاح الثغرة الأمنية على بعض الأجهزة المُدارة فقط، وكان من المطلوب إصلاح الثغرة الأمنية على المزيد من الأجهزة المُدارة.

لعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة:

1. في المجلد **خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **الثغرات الأمنية بالبرنامج**.

   تعرض الصفحة قائمة بالثغرات الأمنية في التطبيقات المكتشفة على الأجهزة المُدارة.

2. حدد ثغرة أمنية تريد عرض الإحصاءات لها.

   في الحظر للعمل مع كائن محدد، يُعرَض مخطط بحالات الثغرات الأمنية. يؤدي النقر فوق إحدى الحالات إلى فتح قائمة بالأجهزة التي تحتوي على الثغرة الأمنية للحالة المحددة.

فحص التطبيقات بحثًا عن ثغرات أمنية

إذا قمت بتكوين التطبيق من خلال معالج البدء السريع، يتم إنشاء مهمة فحص الثغرات الأمنية تلقائيًا. يمكنك عرض المهمة في المجلد **الأجهزة المُدارة**، على علامة التبويب **المهام**.

لإنشاء مهمة لفحص الثغرات الأمنية في التطبيقات المثبّتة على الأجهزة العميلة:

1. في شجرة وحدة التحكم، حدد **خيارات متقدمة** ← **إدارة التطبيق**، ثم قم بتحديد المجلد الفرعي **الثغرات الأمنية بالبرنامج**.

2. في مساحة العمل، حدد **إجراءات إضافية** ← **تكوين فحص الثغرات الأمنية**.

إذا كانت مهمة الفحص لاكتشاف الثغرات الأمنية موجودة بالفعل، تظهر علامة التبويب **المهام** الخاصة بالمجلد **الأجهزة المُدارة**، مع تحديد المهمة الموجودة. بخلاف ذلك، يبدأ تشغيل معالج البحث عن الثغرات الأمنية وإنشاء مهمة التحديثات المطلوبة. اتبع خطوات المعالج.

3. في النافذة **تحديد نوع المهمة**، حدد **البحث عن الثغرات الأمنية والتحديثات المطلوبة**.

4. في صفحة **إعدادات** المعالج، حدد إعدادات المهمة كما يلي:

- **تم إدراج البحث عن الثغرات الأمنية والتحديثات بواسطة Microsoft**

عند البحث عن الثغرات الأمنية والتحديثات، يستخدم Kaspersky Security Center المعلومات حول تحديثات Microsoft القابلة للتطبيق من مصدر تحديثات Microsoft، المتوفرة في الوقت الحالي.

على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft وتحديثات تطبيقات لجهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

لم يتم إرسال المعلومات المتعلقة بتحديثات Microsoft Windows الاختيارية إلى خادم الإدارة.

- **الاتصال بخادم التحديث لتحديث البيانات**

يتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft. يمكن أن تعمل الخوادم التالية كمصدر لتحديثات Microsoft:

- خادم إدارة Kaspersky Security Center (راجع إعدادات سياسة عميل الشبكة)
- خادم Windows مع خدمات تحديث خادم Microsoft Windows (WSUS) المنشورة في شبكة مؤسستك
- خوادم تحديثات Microsoft

إذا تم تمكين هذا الخيار، فسيتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft لتحديث المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق.

إذا تم تعطيل هذا الخيار، فسيستخدم عميل تحديث Windows على جهاز مُدار المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقتٍ سابق.

يمكن أن يكون الاتصال بمصدر تحديثات Microsoft مستهلكًا للموارد. قد ترغب في تعطيل هذا الخيار، إذا قمت بتعيين اتصال منتظم لمصدر التحديثات هذا في مهمة أخرى أو في خصائص سياسة وكلاء الشبكة في قسم **تحديثات البرنامج والثغرات الأمنية**. إذا كنت لا ترغب في تعطيل هذا الخيار، إذن لتقليل التحميل الزائد على الخادم، يمكنك تكوين جدول المهام لترتيب عملية تأخير بدء المهمة عشوائيًا في غضون 360 دقيقة.

يتم تمكين هذا الخيار افتراضيًا.

يحدد مزيج الخيارات التالية لإعدادات سياسة وكلاء الشبكة طريقة الحصول على التحديثات:

- يتصل عميل Windows Update الموجود على جهاز مُدار بخادم التحديث للحصول على التحديثات فقط في حالة تمكين الخيار **الاتصال بخادم التحديث لتحديث البيانات** في خصائص مهمة Find vulnerabilities and required updates وتم تعيين الخيار **وضع بحث تحديث Windows** على **نشط** في إعدادات سياسة عميل الشبكة.

- إذا لم تكن بحاجة إلى عميل الشبكة لبدء الاتصال بمصدر تحديث Microsoft Windows وتنزيل التحديثات عند إجراء مهمة فحص الثغرات الأمنية، يمكنك ضبط الخيار **وضع بحث تحديث Windows** على **سلبي**، بينما يجب أن يظل الخيار **الاتصال بخادم التحديث لتحديث البيانات** قيد التمكين. ويتيح لك ذلك توفير الموارد واستخدام تحديثات Windows التي تم سبق تلقيها للبحث عن الثغرات الأمنية. ويمكنك استخدام الوضع السلبي إذا كونت تلقي تحديثات Microsoft Windows بطريقة مختلفة. إذا لم يتم تكوين تلقي تحديثات Microsoft Windows بطريقة أخرى، فلا تقم بتعيين الخيار **وضع بحث تحديث Windows** على **سلبي**، لأنه في هذه الحالة، لن يتم تلقي معلومات عن التحديثات مطلقًا.

- بغض النظر عن حالة الخيار **الاتصال بخادم التحديث لتحديث البيانات** (تم تمكينه أو تم تعطيله)، ففي حالة ضبط الخيار **وضع بحث تحديث Windows** على **معطل**، لا يطلب Kaspersky Security Center أي معلومات عن التحديثات.

- **تم إدراج البحث عن الثغرات الأمنية من جهة خارجية والتحديثات بواسطة برنامج Kaspersky**

في حالة تمكين هذا الخيار، فسيبحث Kaspersky Security Center عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في سجل Windows وفي المجلدات المحددة ضمن **تحديد مسارات للبحث المتقدم للتطبيقات في نظام الملفات**. تدار القائمة الكاملة لتطبيقات الجهة الخارجية المدعومة بواسطة Kaspersky.

إذا تم تعطيل هذا الخيار، فلن يقوم Kaspersky Security Center بالبحث عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية. على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft Windows وتحديثات تطبيقات جهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

- **تحديد مسارات للبحث المتقدم للتطبيقات في نظام الملفات**

المجلدات التي يبحث فيها Kaspersky Security Center عن تطبيقات الجهة الخارجية والتي تتطلب إصلاح الثغرات الأمنية وتثبيت التحديث. يمكنك استخدام متغيرات النظام.

حدد المجلدات التي يتم تثبيت التطبيقات بها. تحتوي القائمة بشكلٍ افتراضي على مجلدات النظام التي يتم تثبيت معظم التطبيقات بها.

- **تمكين التشخيصات المتقدمة**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

5. في صفحة **تكوين جدول المهمة** للمعالج، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند تنزيل تحديثات جديدة إلى المستودع**

تعمل المهمة بعد تنزيل التحديثات إلى المستودع. على سبيل المثال، قد ترغب في استخدام هذا الجدول للبحث عن الثغرات الأمنية ومهمة التحديثات المطلوبة.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

6. في صفحة المعالج **حدد اسم المهمة**، حدد اسم المهمة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

7. في صفحة **إنهاء عملية إنشاء المهمة** في المعالج، انقر على زر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

بعد إنهاء المعالج عمليته، تظهر مهمة **البحث عن الثغرات الأمنية والتحديثات المطلوبة** في قائمة المهام في المجلد **الأجهزة المُدارة** في علامة التبويب **المهام**.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عند اكتمال مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة، يعرض خادم الإدارة قائمة بالثغرات الأمنية التي تم العثور عليها في التطبيقات المثبّتة على الجهاز؛ ويعرض أيضًا جميع تحديثات البرامج المطلوبة لإصلاح الثغرات الأمنية التي تم اكتشافها.

إذا واجهت خطأ 0x80240033 "Windows Update Agent خطأ 80240033 ("تعذر تنزيل شروط الترخيص.")"، فيمكنك حل هذه المشكلة من خلال سجل Windows.

لا يعرض خادم الإدارة قائمة بتحديثات البرامج المطلوبة عند تشغيل مهمتين بالتتابع - مهمة إجراء مزامنة Windows Update التي تم تعطيل الخيار **تنزيل ملفات التثبيت السريع** فيها، ومهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة. ولعرض قائمة بتحديثات البرامج المطلوبة، يجب عليك إعادة تشغيل مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة.

يتلقى عميل الشبكة المعلومات حول أي من تحديثات Windows المتاحة وتحديثات منتجات Microsoft الأخرى من Windows Update أو خادم الإدارة، في حالة عمل خادم الإدارة كخادم WSUS. يتم نقل المعلومات عند بدء التطبيقات (إذا كانت هذه المعلومات منصوصًا عليها بموجب السياسة) وعند كل تشغيل روتيني لمهمة البحث على الثغرات الأمنية والتحديثات المطلوبة على الأجهزة العميلة.

إصلاح الثغرات الأمنية في التطبيقات

إذا قمت بتحديد **بحث عن التحديثات المطلوبة وتثبيتها** في الصفحة **إعدادات إدارة التحديثات** بمعالج البدء السريع، فسيتم إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية تلقائيًا. يتم عرض المهمة في مساحة العمل الخاصة بالمجلد **الأجهزة المُدارة**، على علامة التبويب **المهام**.

بخلاف ذلك، يمكنك القيام بأحد الإجراءات التالية:

- إنشاء مهمة لإصلاح الثغرات الأمنية من خلال تثبيت التحديثات المتوفرة.
- إضافة قاعدة لإصلاح ثغرة أمنية لمهمة إصلاح ثغرة أمنية حالية.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

إصلاح ثغرات أمنية من خلال إنشاء مهمة إصلاح ثغرة أمنية

يمكنك القيام بأحد الإجراءات التالية:

- إنشاء مهمة لإصلاح ثغرات أمنية عديدة تستوفي قواعد معينة.
- حدد الثغرة الأمنية وقم بإنشاء مهمة لإصلاحها ولإصلاح الثغرات الأمنية المماثلة.

لإصلاح ثغرات أمنية تتوافق مع قواعد محددة:

1. في شجرة وحدة التحكم، حدد خادم الإدارة على الأجهزة التي تريد إصلاح نقاط الضعف فيها.
2. من القائمة **عرض** في نافذة التطبيق الرئيسية، حدد **تكوين الواجهة**.
3. في النافذة التي تفتح، حدد **عرض إدارة الثغرات الأمنية والتصحيح**، ثم انقر على **موافق**.
4. في النافذة التي تحتوي على رسالة التطبيق، انقر فوق **موافق**.
5. أعد تشغيل وحدة تحكم الإدارة، حتى تسري التغييرات.
6. في شجرة وحدة التحكم، افتح المجلد **الأجهزة المُدارة**.
7. في مساحة عمل المجموعة، حدد علامة تبويب **المهام**.
8. انقر فوق الزر **إنشاء مهمة** لتشغيل معالج المهمة الجديدة. اتبع خطوات المعالج.
9. في صفحة المعالج **تحديد نوع المهمة**، وحدد **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية**.

   إذا لم يتم عرض المهمة، فتحقق مما إذا كان حسابك لديه **حقوق القراءة** و **التعديل** و التنفيذ للمجال **الوظيفي**: **لإدارة الثغرات الأمنية والتصحيحات** لا يمكنك إنشاء وتكوين مهمة قم بتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية بدون حقوق الوصول هذه.

10. في صفحة **إعدادات** المعالج، حدد إعدادات المهمة كما يلي:

- **حدد قواعد لتثبيت التحديثات**

يتم تطبيق تلك القواعد على تثبيت التحديثات على الأجهزة العميلة. إذا لم يتم تحديد قواعد، فلن تقوم المهمة بتنفيذ أي شيء. للحصول على معلومات حول عمليات التشغيل من خلال القواعد، راجع قواعد لتثبيت التحديثات.

- **بدء التثبيت بعد إعادة تشغيل الجهاز أو إيقاف تشغيله**

إذا تم تمكين هذا الخيار، فسيتم تثبيت التحديثات عند إعادة تشغيل الجهاز أو إغلاقه. بخلاف ذلك، يتم تثبيت التحديثات وفقًا لجدول زمني.

استخدم هذا الخيار في حال كان تنزيل التحديثات قد يؤثر على أداء الجهاز.

يتم تعطيل هذا الخيار افتراضيًا.

- **تثبيت مكونات النظام العام المطلوبة**

إذا تم تمكين هذا الخيار، قبل تثبيت التحديث، يقوم التطبيق تلقائيًا بتثبيت كافة مكونات النظام العامة (المتطلبات الأساسية) اللازمة لتثبيت التحديث. على سبيل المثال، يمكن أن تكون تلك المتطلبات الأساسية عبارة عن تحديثات نظام التشغيل.

إذا تم تعطيل هذا الخيار، فقط يتعين عليك تثبيت المتطلبات الأساسية يدويًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **السماح بتثبيت إصدارات التطبيق الجديدة أثناء التحديثات**

إذا تم تمكين هذا الخيار، سيتم السماح بالتحديثات التي تؤدي إلى تثبيت إصدار جديد من تطبيق البرنامج.

إذا تم تعطيل هذا الخيار، فلن تتم ترقية البرنامج. بعد ذلك يمكنك تثبيت إصدارات البرنامج الجديدة يدويًا أو من خلال مهمة أخرى. على سبيل المثال، قد تستخدم هذا الخيار في حال كانت البنية الأساسية الخاصة بشركتك غير مدعومة بواسطة إصدار جديد للبرنامج أو في حال رغبت في التحقق من ترقية في اختبار البنية الأساسية.

يتم تمكين هذا الخيار افتراضيًا.

قد تؤدي ترقية التطبيق إلى حدوث خلل في التطبيقات التابعة المثبتة على أجهزة عميلة.

- **تنزيل التحديثات على الجهاز دون تثبيتها**

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بتنزيل التحديثات على الجهاز ولكن لن يقوم بتنزيلها تلقائيًا. بعد ذلك يمكنك تثبيت التحديثات التي تم تنزيلها يدويًا.

تم تنزيل تحديثات Microsoft إلى مخزن Windows في النظام. يتم تنزيل تحديثات تطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في المجلد المحدد في حقل **تنزيل التحديثات إلى**.

إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائيًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **تنزيل التحديثات إلى**

يتم استخدام هذا المجلد لتنزيل تحديثات خاصة بتطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky وMicrosoft).

- **تمكين التشخيصات المتقدمة**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

11. في صفحة المعالج **تحديد خيار إعادة تشغيل نظام التشغيل**، حدد الإجراء الذي سيتم اتخاذه عندما يلزم إعادة تشغيل نظام التشغيل على الأجهزة العميلة بعد عملية التشغيل:

- **لا تقم بإعادة تشغيل الجهاز**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **أعد تشغيل الجهاز**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **مطالبة المستخدم باتخاذ إجراء**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **تكرار المطالبة كل (بالدقائق)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **إعادة التشغيل بعد (دقيقة)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

12. في صفحة **تكوين جدول المهمة** للمعالج، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

13. في صفحة المعالج **حدد اسم المهمة**، حدد اسم المهمة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

14. في صفحة **إنهاء عملية إنشاء المهمة** في المعالج، انقر على زر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

بعد إنهاء المعالج عملياته، يتم إنشاء المهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية** وعرضها في مجلد **المهام**.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

إذا كانت نتائج المهمة تحتوي على خطأ 0x80240033 "خطأ وكيل تحديث Windows 80240033 (" تعذر تنزيل شروط الترخيص. ")"، فيمكنك حل هذه المشكلة من خلال سجل Windows.

لإصلاح ثغرة أمنية محددة وثغرات مماثلة:

1. في المجلد **خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **الثغرات الأمنية بالبرنامج**.

2. حدد الثغرة الأمنية التي ترغب في إصلاحها.

3. انقر على زر **تشغيل معالج إصلاح الثغرات الأمنية**.

يبدأ معالج إصلاح الثغرات الأمنية.

لا تتوفر ميزات معالج إصلاح الثغرات الأمنية إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

اتبع خطوات المعالج.

4. في النافذة **البحث عن المهام الموجودة لإصلاح الثغرات الأمنية**، حدد المعلمات التالية:

- **إظهار المهام التي تصلح هذه الثغرة الأمنية فقط**

إذا تم تمكين هذا الخيار، فسيبحث معالج إصلاح الثغرات الأمنية عن المهام الحالية التي تقوم بإصلاح الثغرات الأمنية المحددة.

إذا تم تعطيل هذا الخيار أو إذا لم ينتج عن البحث أي مهام سارية، فسيطالبك معالج إصلاح الثغرات الأمنية بإنشاء قاعدة أو مهمة لإصلاح الثغرات الأمنية.

يتم تمكين هذا الخيار افتراضيًا.

- **الموافقة على التحديثات التي تستهدف إصلاح هذه الثغرات الأمنية**

ستتم الموافقة على تثبيت التحديثات التي تصلح الثغرة الأمنية. تمكين هذا الخيار فقط في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها.

يتم تعطيل هذا الخيار افتراضيًا.

5. إذا اخترت البحث عن مهام إصلاح الثغرات الأمنية الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدويًا. لا يلزم اتخاذ إجراءات إضافية.

بخلاف ذلك، انقر فوق زر **مهمة إصلاح ثغرة أمنية جديدة**.

6. حدد نوع قاعدة إصلاح الثغرات الأمنية التي ستضاف إلى المهمة الجديدة، ثم انقر فوق الزر **إنهاء**.

7. حدد اختيارك في المطالبة المعروضة حول تثبيت كافة تحديثات التطبيق السابقة. انقر فوق **نعم** إذا كنت موافق على تثبيت إصدارات التطبيق المتتالية تدريجيًا في حالة طُلب ذلك لتثبيت التحديثات المحددة. انقر فوق **لا** إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون تثبيت إصدارات متتابعة. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

يبدأ معالج إنشاء مهمة تثبيت التحديثات وإصلاح الثغرات الأمنية. اتبع خطوات المعالج.

8. في صفحة المعالج **تحديد خيار إعادة تشغيل نظام التشغيل**، حدد الإجراء الذي سيتم اتخاذه عندما يلزم إعادة تشغيل نظام التشغيل على الأجهزة العميلة بعد عملية التشغيل:

- **لا تقم بإعادة تشغيل الجهاز**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **أعد تشغيل الجهاز**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **مطالبة المستخدم باتخاذ إجراء**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **تكرار المطالبة كل (بالدقائق)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **إعادة التشغيل بعد (دقيقة)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

9. في صفحة المعالج **حدد الأجهزة التي سيتم تعيين المهمة لها**، وحدد أحد الخيارات التالية:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة**

يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لمهمة تثبيت عميل الشبكة على الأجهزة غير المخصصة.

- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**

يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

- **تعيين مهمة إلى تحديد الجهاز**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

- **تعيين مهمة لمجموعة إدارة**

يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

10. في صفحة **تكوين جدول المهمة** للمعالج، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

11. في صفحة المعالج **حدد اسم المهمة**، حدد اسم المهمة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

12. في صفحة **إنهاء عملية إنشاء المهمة** في المعالج، انقر على زر **إنهاء** لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

عند انتهاء المعالج، يتم إنشاء المهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية** وعرضها في مجلد **المهام**.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

إصلاح ثغرة أمنية من خلال إضافة قاعدة لمهمة إصلاح ثغرة أمنية حالية

لإصلاح الثغرات الأمنية من خلال إضافة قاعدة لمهمة إصلاح ثغرة أمنية حالية:

1. في المجلد **خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **الثغرات الأمنية بالبرنامج**.

2. حدد الثغرة الأمنية التي ترغب في إصلاحها.

3. انقر على زر **تشغيل معالج إصلاح الثغرات الأمنية**.

يبدأ معالج إصلاح الثغرات الأمنية.

لا تتوفر ميزات معالج إصلاح الثغرات الأمنية إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

اتبع خطوات المعالج.

4. في النافذة **البحث عن المهام الموجودة لإصلاح الثغرات الأمنية**، حدد المعلمات التالية:

- **إظهار المهام التي تصلح هذه الثغرة الأمنية فقط**

إذا تم تمكين هذا الخيار، فسيبحث معالج إصلاح الثغرات الأمنية عن المهام الحالية التي تقوم بإصلاح الثغرات الأمنية المحددة.

إذا تم تعطيل هذا الخيار أو إذا لم ينتج عن البحث أي مهام سارية، فسيطالبك معالج إصلاح الثغرات الأمنية بإنشاء قاعدة أو مهمة لإصلاح الثغرات الأمنية.

يتم تمكين هذا الخيار افتراضيًا.

- **الموافقة على التحديثات التي تستهدف إصلاح هذه الثغرات الأمنية**

ستتم الموافقة على تثبيت التحديثات التي تصلح الثغرة الأمنية. تمكين هذا الخيار فقط في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها.

يتم تعطيل هذا الخيار افتراضيًا.

5. إذا اخترت البحث عن مهام إصلاح الثغرات الأمنية الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدويًا. لا يلزم اتخاذ إجراءات إضافية.

بخلاف ذلك، انقر على **إضافة قاعدة إصلاح الثغرات الأمنية لمهمة موجودة**.

6. حدد المهمة التي ترغب في إضافة قاعدة لها، ثم انقر فوق الزر **إضافة قاعدة**.

أيضًا، يمكنك عرض خصائص المهام الحالية، أو بدئهم يدويًا، أو إنشاء مهمة جديدة.

7. حدد نوع القاعدة التي ستضاف إلى المهمة المحددة، ثم انقر فوق الزر **إنهاء**.

8. حدد اختيارك في المطالبة المعروضة حول تثبيت كافة تحديثات التطبيق السابقة. انقر فوق **نعم** إذا كنت موافق على تثبيت إصدارات التطبيق المتتالية تدريجيًا في حالة طُلب ذلك لتثبيت التحديثات المحددة. انقر فوق **لا** إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون تثبيت إصدارات متتابعة. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

تتم إضافة قاعدة جديدة لإصلاح الثغرات الأمنية إلى مهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية**الحالية.

إصلاح الثغرات الأمنية في شبكة معزولة

يصف هذا القسم الخطوات التي يمكنك اتخاذها لإصلاح الثغرات الأمنية بالبرامج الناجمة عن جهات خارجية على الأجهزة المدارة المتصلة بخوادم الإدارة التي ليس لديها وصول إلى الإنترنت.

السيناريو: إصلاح الثغرات الأمنية لبرامج الجهات الخارجية في شبكة معزولة

يمكنك تثبيت التحديثات وإصلاح الثغرات الأمنية لبرامج الجهة الخارجية المثبتة على الأجهزة المُدارة في شبكة معزولة. تتضمن هذه الشبكات خوادم الإدارة والأجهزة المدارة المتصلة بها والتي ليس لها اتصال بالإنترنت. لإصلاح الثغرات الأمنية في هذا النوع من الشبكات، تحتاج إلى خادم إدارة متصل بالإنترنت. بعد ذلك، ستتمكن من تنزيل التصحيحات مع التحديثات باستخدام خادم الإدارة مع الوصول إلى الإنترنت ، ثم نقل التصحيحات إلى خوادم الإدارة المعزولة.

يمكنك تنزيل تحديثات برامج الجهات الخارجية الصادرة عن موردي البرامج، ولكن لا يمكنك تنزيل تحديثات برامج Microsoft على خوادم الإدارة المعزولة باستخدام Kaspersky Security Center.

لمعرفة كيفية عمل عملية إصلاح الثغرات الأمنية في شبكة معزولة، راجع وصف هذه العملية ومخططها.

المتطلبات الأساسية

قبل أن تبدأ، افعل ما يلي:

1. خصص جهاز واحد للاتصال بالإنترنت وتنزيل التصحيحات. سيتم اعتبار هذا الجهاز خادم الإدارة مع الوصول إلى الإنترنت.
2. قم بتثبيت Kaspersky Security Center، ليس قبل الإصدار 14، على الأجهزة التالية:
   - الجهاز المخصص، والذي سيكون بمثابة خادم الإدارة مع الوصول إلى الإنترنت
   - الأجهزة المعزولة، والتي ستكون بمثابة خوادم الإدارة المعزولة عن الإنترنت (المشار إليها فيما يلي باسم خوادم الإدارة المعزولة)
3. تأكد من أن كل خادم إدارة لديه مساحة كافية على القرص لتنزيل التحديثات والتصحيحات وتخزينها.

المراحل

يتضمن تثبيت التحديثات وإصلاح الثغرات الأمنية بالبرامج الناجمة عن جهات خارجية على الأجهزة المدارة لخوادم الإدارة المعزولة المراحل التالية:

1. **تكوين خادم الإدارة مع الوصول إلى الإنترنت**

   قم بإعداد خادم الإدارة الخاص بك مع الوصول إلى الإنترنت للتعامل مع الطلبات الخاصة بتحديثات برامج الجهات الخارجية المطلوبة وتنزيل التصحيحات.

2. **تكوين خوادم الإدارة المعزولة**

   قم بإعداد خوادم الإدارة المعزولة حتى يتمكنوا من تشكيل قوائم بالتحديثات المطلوبة بانتظام والتعامل مع التصحيحات التي تم تنزيلها بواسطة خادم الإدارة مع إمكانية الوصول إلى الإنترنت. بعد التكوين، لا تحاول خوادم الإدارة المعزولة تنزيل التصحيحات من الإنترنت بعد الآن. بدلاً من ذلك، يحصلون على التحديثات من خلال التصحيحات.

3. **إرسال التصحيحات وتثبيت التحديثات على خوادم الإدارة المعزولة**

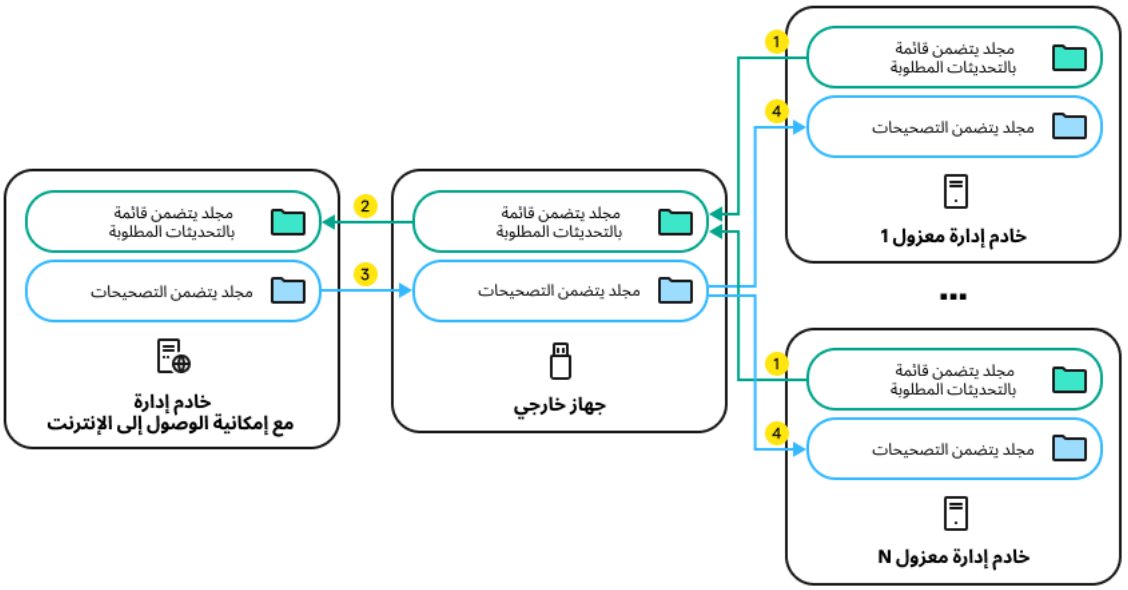
   بعد الانتهاء من تكوين خوادم الإدارة، يمكنك إرسال قوائم التحديثات والتصحيحات المطلوبة بين خادم الإدارة مع الوصول إلى الإنترنت وخوادم الإدارة المعزولة. بعد ذلك، سيتم تثبيت التحديثات من التصحيحات على الأجهزة المدارة باستخدام مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.

النتائج

وبالتالي، يتم إرسال تحديثات برامج الجهات الخارجية إلى خوادم الإدارة المعزولة وتثبيتها على الأجهزة المدارة المتصلة باستخدام Kaspersky Security Center. يكفي تكوين خوادم الإدارة مرة واحدة، وبعد ذلك يمكنك الحصول على التحديثات كلما احتجت. على سبيل المثال، مرة واحدة أو عدة مرات في اليوم.

السيناريو: إصلاح الثغرات الأمنية لبرامج الجهات الخارجية في شبكة معزولة

عملية إصلاح الثغرات الأمنية لبرامج الطرف الثالث في شبكة معزولة موضحة في الشكل وموصوفة أدناه. يمكنك تكرار هذه العملية بشكل دوري.



عملية إرسال التصحيحات وقائمة بالتحديثات المطلوبة بين خادم الإدارة مع الوصول إلى الإنترنت وخوادم الإدارة المعزولة

يُنشئ كل خادم إدارة معزول عن الإنترنت (يُشار إليه فيما يلي باسم خادم إدارة معزول) قائمة بالتحديثات المطلوبة للتثبيت على الأجهزة المُدارة المتصلة بخادم الإدارة هذا. يتم تخزين قائمة التحديثات المطلوبة في مجلد معين وتقدم مجموعة من الملفات الثنائية. كل ملف له اسم يحتوي على معرف التصحيح مع التحديث المطلوب. نتيجة لذلك، يشير كل ملف في القائمة إلى تصحيح معين.

باستخدام جهاز خارجي ، يمكنك نقل قائمة التحديثات المطلوبة من خادم الإدارة المعزول إلى خادم الإدارة المخصص مع إمكانية الوصول إلى الإنترنت. بعد ذلك، يقوم خادم الإدارة المخصص بتنزيل تصحيحات من الإنترنت ويضعها في مجلد منفصل.

عندما يتم تنزيل جميع التصحيحات ووضعها في مجلد خاص لها ، فإنك تنقل التصحيحات إلى كل خادم إدارة معزول أخذت منه قائمة بالتحديثات المطلوبة. يمكنك حفظ التصحيحات في المجلد الذي تم إنشاؤه خصيصًا لهم على خادم الإدارة المعزول. نتيجة لذلك ، تقوم مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية بتشغيل التصحيحات وتثبيت التحديثات على الأجهزة المدارة لخوادم الإدارة المعزولة.

تكوين خادم الإدارة مع الوصول إلى الإنترنت لإصلاح الثغرات الأمنية في شبكة معزولة

للتحضير من أجل إصلاح الثغرات الأمنية وإرسال التصحيحات مع التحديثات في شبكة معزولة، قم أولاً بتكوين خادم الإدارة مع الوصول إلى الإنترنت، ثم تكوين خوادم الإدارة المعزولة.

لتكوين خادم الإدارة مع الوصول إلى الإنترنت:

1. أنشئ مجلدين على القرص المثبت عليه خادم الإدارة:
   - مجلد لقائمة التحديثات المطلوبة
   - مجلد للبقع

   يمكنك تسمية هذه المجلدات بما تريد.
2. امنح حقوق الوصول المعدلة إلى مجموعة KLAdmins في المجلدات التي تم إنشاؤها، باستخدام الأدوات الإدارية القياسية لنظام التشغيل.

3. استخدم الأداة المساعدة klscflag لكتابة المسارات إلى المجلدات في خصائص خادم الإدارة.

قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Security Center\Lab.

4. أدخل الأمر التالي في موجه أوامر Windows:

- لتعيين المسار إلى مجلد التصحيحات:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<المسار إلى المجلد>"
```

- لتعيين مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:

```
klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<المسار إلى المجلد>"
```

مثال:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<مجلد التصحيحات>"
```

5. إذا لزم الأمر، استخدم الأداة المساعدة klscflag لتحديد عدد المرات التي يجب أن يتحقق فيها خادم الإدارة من طلبات التصحيح الجديدة:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <القيمة بالثواني>
```

القيمة الافتراضية هي 120 ثانية.

مثال:

```
klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150
```

6. أنشئ مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة للحصول على معلومات عن التصحيحات الخاصة بالبرامج الخارجية المثبتة على الأجهزة المدارة ، ثم قم بتعيين جدول المهام.

7. قم بإنشاء مهمة إصلاح الثغرات الأمنية لتحديد التصحيحات لبرامج الجهات الخارجية المستخدمة لإصلاح الثغرات الأمنية، ثم قم بتعيين جدول المهام.

تشغيل المهمة يدويًا إذا كنت تريد تشغيلها في وقت أبكر مما هو محدد في الجدول. الترتيب الذي تبدأ به المهام مهم. ويجب تشغيل مهمة إصلاح الثغرات الأمنية بعد الانتهاء من مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة.

8. قم بإعادة تشغيل خدمة خادم الإدارة.

أصبح الآن خادم الإدارة المزود بإمكانية الوصول إلى الإنترنت جاهزًا لتنزيل التحديثات وإرسالها إلى خوادم الإدارة المعزولة. قبل البدء في إصلاح الثغرات الأمنية، تكوين خوادم الإدارة المعزولة.

تكوين خوادم الإدارة المعزولة لإصلاح الثغرات الأمنية في شبكة معزولة

بعد الانتهاء من تكوين خادم الإدارة مع الوصول إلى الإنترنت، قم بإعداد كل خادم إدارة معزول في شبكتك، حتى تتمكن من إصلاح الثغرات الأمنية وتثبيت التحديثات على الأجهزة المدارة المتصلة بخوادم الإدارة المعزولة.

لتكوين خوادم الإدارة المعزولة، قم بتنفيذ الإجراءات التالية على كل خادم إدارة:

1. قم بتنشيط مفتاح الترخيص لميزة إدارة الثغرات الأمنية والتصحيحات (VAPM).

2. أنشئ مجلدين على القرص المثبت عليه خادم الإدارة:

- المجلد الذي ستظهر فيه قائمة التحديثات المطلوبة
- مجلد للبقع

يمكنك تسمية هذه المجلدات بما تريد.

3. امنح حقوق الوصول المعدلة إلى مجموعة KLAdmins في المجلدات التي تم إنشاؤها، باستخدام الأدوات الإدارية القياسية لنظام التشغيل.

4. استخدم الأداة المساعدة klscflag لكتابة المسارات إلى المجلدات في خصائص خادم الإدارة.

قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Security Center\Lab.

5. أدخل الأمر التالي في موجه أوامر Windows:

- لتعيين المسار إلى مجلد التصحيحات:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<المسار إلى المجلد>"
```

- لتعيين مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:

```
klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<المسار إلى المجلد>"
```

مثال:
```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<مجلد التصحيحات>"
```

6. إذا لزم الأمر، استخدم الأداة المساعدة klscflag لتحديد عدد المرات التي يجب أن يتحقق فيها خادم الإدارة المعزول من التصحيحات الجديدة:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <القيمة بالثواني>
```

القيمة الافتراضية هي 120 ثانية.

مثال:
```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150
```

7. إذا لزم الأمر، استخدم الأداة المساعدة klscflag لحساب تجزئات SHA256 للتصحيحات:

```
klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
```

إذا قمت بإدخال هذا الأمر ، يمكنك التأكد من أن التصحيحات لم يتم تعديلها أثناء نقلها إلى خادم الإدارة المعزول وأنك قد تلقيت التصحيحات الصحيحة التي تحتوي على التحديثات المطلوبة.

بشكل افتراضي، لا يحسب Kaspersky Security Center تجزئة SHA256 للتصحيحات. إذا قمت بتمكين هذا الخيار، فبعد أن يتلقى خادم الإدارة المعزول التصحيحات، يحسب Kaspersky Security Center تجزئاتها ويقارن القيم المكتسبة مع التجزئات المخزنة في قاعدة بيانات خادم الإدارة. إذا لم تتطابق التجزئة المحسوبة مع التجزئة في قاعدة البيانات، فسيحدث خطأ وسيتعين عليك استبدال التصحيحات غير الصحيحة.

8. أنشئ مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة للحصول على معلومات عن التصحيحات الخاصة بالبرامج الخارجية المثبتة على الأجهزة المدارة ، ثم قم بتعيين جدول المهام.

9. قم بإنشاء مهمة إصلاح الثغرات الأمنية لتحديد التصحيحات لبرامج الجهات الخارجية المستخدمة لإصلاح الثغرات الأمنية، ثم قم بتعيين جدول المهام.

تشغيل المهمة يدويًا إذا كنت تريد تشغيلها في وقت أبكر مما هو محدد في الجدول. الترتيب الذي تبدأ به المهام مهم. ويجب تشغيل مهمة إصلاح الثغرات الأمنية بعد الانتهاء من مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة.

10. قم بإعادة تشغيل خدمة خادم الإدارة.

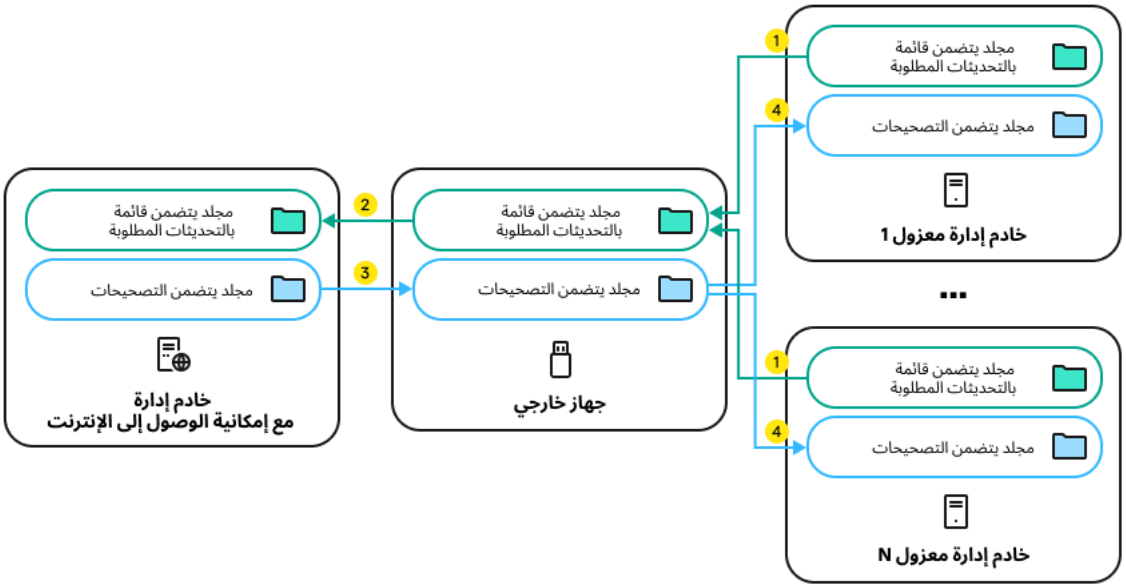
بعد تكوين جميع خوادم الإدارة، يمكنك نقل التصحيحات وقوائم التحديثات المطلوبة، وإصلاح الثغرات الأمنية بالبرامج الناجمة عن جهات خارجية على الأجهزة المدارة في الشبكة المعزولة.

جارٍ إرسال التصحيحات وتثبيت التحديثات في شبكة معزولة

بعد الانتهاء من تكوين خوادم الإدارة، يمكنك نقل التصحيحات مع التحديثات من خادم الإدارة مع الوصول إلى الإنترنت إلى خوادم الإدارة المعزولة. يمكنك إرسال التحديثات وتثبيتها كلما احتجت ذلك، على سبيل المثال، مرة واحدة أو عدة مرات في اليوم.

أنت بحاجة إلى جهاز خارجي، كمحرك أقراص خارجي لنقل التصحيحات وقائمة بالتحديثات المطلوبة بين خوادم الإدارة. لذلك، تأكد من أن الجهاز الخارجي يحتوي على مساحة ملفات كافية على القرص لتنزيل التحديثات والتصحيحات وتخزينها.

عملية إرسال التصحيحات وقائمة التحديثات المطلوبة موضحة في الشكل والموضحة أدناه:



عملية إرسال التصحيحات وقائمة بالتحديثات المطلوبة بين خادم الإدارة مع الوصول إلى الإنترنت وخوادم الإدارة المعزولة

لتثبيت التحديثات وإصلاح الثغرات الأمنية على الأجهزة المُدارة المتصلة بخوادم الإدارة المعزولة:

1. ابدأ مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية إذا لم تكن قيد التشغيل بعد.

2. قم بتوصيل جهاز خارجي بأي خادم إدارة معزول.

3. أنشئ مجلدين على الجهاز الخارجي: أحدهما لقائمة التحديثات المطلوبة والآخر للتصحيحات. يمكنك تسمية هذه المجلدات بما تريد.

   إذا قمت بإنشاء هذه المجلدات في وقت سابق، فامسحها.

4. انسخ قائمة التحديثات المطلوبة من كل خادم إدارة معزول والصق هذه القائمة في المجلد للحصول على قائمة التحديثات المطلوبة على الجهاز الخارجي.

   نتيجة لذلك ، تقوم بتوحيد جميع القوائم التي تم الحصول عليها من جميع خوادم الإدارة المعزولة في مجلد واحد. نتيجة لذلك، يجب أن يحتوي هذا المجلد على ملفات ثنائية بمعرفات التصحيحات المطلوبة لجميع خوادم الإدارة المعزولة.

5. وصّل الجهاز الخارجي بخادم الإدارة من خلال الوصول إلى الإنترنت.

6. انسخ قائمة التحديثات المطلوبة من الجهاز الخارجي والصق هذه القائمة في المجلد للحصول على قائمة التحديثات المطلوبة على خادم الإدارة مع الوصول إلى الإنترنت.

   يتم تنزيل جميع التصحيحات المطلوبة تلقائيًا من الإنترنت إلى المجلد للتصحيحات الموجودة على خادم الإدارة. قد تستغرق هذه العملية عدة ساعات.

7. تأكد من تنزيل جميع التصحيحات المطلوبة. لهذا الغرض، يمكنك إجراء ما يلي:

   - تحقق من المجلد بحثًا عن التصحيحات الموجودة على خادم الإدارة مع الوصول إلى الإنترنت. يجب تنزيل كافة التصحيحات التي تم تحديدها في قائمة التحديثات المطلوبة إلى المجلد الضروري. يكون هذا أكثر ملاءمة إذا تطلب عدد قليل من التصحيحات.

   - قم بإعداد سيناريو خاص، على سبيل المثال، سيناريو شيل. إذا حصلت على عدد كبير من التصحيحات، فسيكون من الصعب التحقق بنفسك من أنه تم تنزيل جميع التصحيحات. من الأفضل أتمتة الفحص في مثل هذه الحالات.

8. انسخ التصحيحات من خادم الإدارة مع إمكانية الوصول إلى الإنترنت والصقها في المجلد المقابل على الجهاز الخارجي.

9. انقل التصحيحات إلى كل خادم إدارة معزول. ضع التصحيحات في مجلد محدد لهم.

نتيجة لذلك، يقوم كل خادم إدارة معزول بإنشاء قائمة فعلية بالتحديثات المطلوبة للأجهزة المدارة المتصلة بخادم الإدارة الحالي. بعد أن يتلقى خادم الإدارة المتصل بالإنترنت قائمة التحديثات المطلوبة، يقوم خادم الإدارة بتنزيل التصحيحات مع التحديثات من الإنترنت. عندما تظهر هذه التصحيحات على خوادم الإدارة المعزولة ، فإن مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية تتعامل مع التصحيحات. وبالتالي، يتم تثبيت التحديثات على الأجهزة المدارة ويتم إصلاح الثغرات الأمنية بالبرامج الناجمة عن جهات خارجية.

عند تشغيل مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، لا تعيد تشغيل جهاز خادم الإدارة ولا تشغل مهمة النسخ الاحتياطي لبيانات خادم الإدارة (سيؤدي ذلك أيضًا إلى إعادة التشغيل). نتيجة لذلك، تتم مقاطعة مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، ولم يتم تثبيت التحديثات. في هذه الحالة، عليك إعادة تشغيل هذه المهمة يدويًا أو الانتظار حتى تبدأ المهمة وفقًا للجدول الذي تم تكوينه.

جارٍ تعطيل خيار إرسال التصحيحات وتثبيت التحديثات في شبكة معزولة

يمكنك تعطيل إرسال التصحيحات مع التحديثات على خوادم الإدارة المعزولة، على سبيل المثال، إذا قررت إخراج واحد أو أكثر من خوادم الإدارة من شبكة معزولة. وبالتالي، يمكنك تقليل عدد التصحيحات ووقت تنزيلها.

لتعطيل خيار إدارة التصحيحات على خوادم الإدارة المعزولة:

1. إذا كنت ترغب في إخراج جميع خوادم الإدارة من العزل، في خصائص خادم الإدارة مع الوصول إلى الإنترنت، فاحذف المسارات إلى المجلدات الخاصة بالتصحيحات وقائمة التحديثات المطلوبة. إذا كنت تريد الاحتفاظ ببعض خوادم الإدارة في شبكة معزولة، فتخط هذه الخطوة.

   قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   أدخل الأوامر التالية في موجه الأوامر:

   - لحذف المسار إلى مجلد التصحيحات:
     ```
     "" klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v
     ```
   - لحذف مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:
     ```
     "" klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v
     ```

2. أعد تشغيل خدمة خادم الإدارة إذا قمت بحذف المسارات إلى المجلدات الموجودة على خادم الإدارة هذا.

3. في خصائص كل خادم إدارة تريد إزالته من العزل، احذف المسارات إلى المجلدات من أجل التصحيحات وقائمة بالتحديثات المطلوبة.

   أدخل الأمر التالي في موجه أوامر Windows، باستخدام حقوق المسؤول:

   - لحذف المسار إلى مجلد التصحيحات:
     ```
     "" klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v
     ```
   - لحذف مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:
     ```
     "" klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v
     ```

4. أعد تشغيل خدمة كل خادم إدارة قمت بحذف المسارات إلى المجلدات عليه.

نتيجةً لذلك، إذا أعدت تكوين خادم الإدارة من خلال الوصول إلى الإنترنت، فلن تتلقى بعد الآن تصحيحات مع التحديثات من خلال Kaspersky Security Center. إذا أعدت تكوين بعض خوادم الإدارة المعزولة فقط، على سبيل المثال، مع إخراج بعضها من الشبكة المعزولة، فستحصل فقط على تصحيحات لخوادم الإدارة المعزولة المتبقية.

إذا كنت تريد البدء في إصلاح الثغرات الأمنية على خوادم الإدارة المعطلة في المستقبل، فعليك تكوين خوادم الإدارة هذه وخادم الإدارة مع الوصول إلى الإنترنت مرة أخرى.

تجاهل الثغرات الأمنية في البرامج

يمكنك تجاهل إصلاح الثغرات الأمنية بالبرامج. قد تكون أسباب تجاهل الثغرات الأمنية للبرامج، على سبيل المثال، ما يلي:

- لا تعتبر ثغرة أمنية في البرنامج مشكلة حرجة لمؤسستك.
- تدرك أن إصلاح الثغرات الأمنية بالبرامج يمكن أن يتلف البيانات المتعلقة بالبرامج التي تطلبت إصلاح الثغرات الأمنية.
- تتأكد من أن الثغرة الأمنية بالبرنامج ليست خطيرة على شبكة مؤسستك لأنك تستخدم تدابير أخرى لحماية أجهزتك المُدارة.

يمكنك تجاهل ثغرة أمنية في البرامج على جميع الأجهزة المُدارة أو على الأجهزة المدارة المحددة فقط.

لتجاهل ثغرة أمنية في البرامج على جميع الأجهزة المُدارة:

1. في المجلد **خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **الثغرات الأمنية بالبرنامج**.
تعرض مساحة عمل المجلد قائمة الثغرات الأمنية في التطبيقات التي تم اكتشافها على الأجهزة بواسطة عميل الشبكة المثبت عليها.
2. حدد الثغرة الأمنية التي ترغب في تجاهلها.
3. حدد **خصائص** من قائمة سياق الثغرة الأمنية.
ستفتح نافذة خصائص الثغرة الأمنية.
4. في القسم **عام**، حدد خيار **تجاهل الثغرات الأمنية**.
5. انقر على**موافق**.
تم إغلاق نافذة خصائص الثغرات الأمنية بالبرامج.

يتم تجاهل الثغرات الأمنية بالبرامج على جميع الأجهزة المُدارة.

لتجاهل ثغرة أمنية في البرامج على الجهاز المُدار المحدد:

1. افتح نافذة الخصائص للجهاز المُدار المحدد وحدد القسم **الثغرات الأمنية بالبرنامج**.
2. حدد ثغرة أمنية في البرامج.
3. تجاهل الثغرات الأمنية المحددة.

يتم تجاهل الثغرات الأمنية بالبرامج على الجهاز المُحدَّد.

لن يتم إصلاح الثغرات الأمنية للبرامج التي تم تجاهلها بعد الانتهاء من المهمة إصلاح الثغرات الأمنية أو المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. يمكنك استثناء الثغرات الأمنية للبرامج التي تم تجاهلها من قائمة الثغرات الأمنية باستخدام عامل تصفية.

تحديد إصلاحات المستخدم للثغرات الأمنية في برامج الجهات الخارجية

لاستخدام المهمة إصلاح الثغرات الأمنية، يجب عليك تحديد تحديثات البرامج يدويًا لإصلاح الثغرات الأمنية الموجودة في برامج الجهات الخارجية المدرجة في إعدادات المهمة. تستخدم المهمة إصلاح الثغرات الأمنية الإصلاحات الموصى بها لبرامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية الأخرى. إصلاحات المستخدم هي تحديثات للبرامج لإصلاح الثغرات الأمنية التي يحددها المسؤول يدويًا للتثبيت.

لتحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية:

1. في المجلد **خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **الثغرات الأمنية بالبرنامج**.

تعرض مساحة عمل المجلد قائمة الثغرات الأمنية في التطبيقات التي تم اكتشافها على الأجهزة بواسطة عميل الشبكة المثبت عليها.

2. حدد مشكلة الثغرة الأمنية التي تريد تحديد إصلاح مستخدم لها.

3. حدد **خصائص** من قائمة سياق الثغرة الأمنية.

ستفتح نافذة خصائص الثغرة الأمنية.

4. في**إصلاحات المستخدم وإصلاحات أخرى**، انقر على زر **إضافة**.

يتم عرض قائمة حزم التثبيت المتاحة. تتوافق قائمة حزم التثبيت المعروضة مع القائمة **التثبيت عن بُعد** ← **حزم التثبيت**. إذا لم تقم بإنشاء حزمة تثبيت تحتوي على إصلاح مستخدم لثغرة أمنية محددة، فيمكنك إنشاء الحزمة الآن عن طريق بدء معالج حزمة جديدة.

5. حدد حزمة (أو حزم) تثبيت تحتوي على إصلاح مستخدم (أو إصلاحات مستخدم) لثغرة أمنية في برنامج تابع لجهة خارجية.

6. انقر على**موافق**.

يتم تحديد حزم التثبيت التي تحتوي على إصلاحات للمستخدم للثغرات الأمنية في البرامج. عند بدء المهمة إصلاح الثغرات الأمنية، سيتم تثبيت حزمة التثبيت وإصلاح الثغرات الأمنية في البرامج.

قواعد لتثبيت التحديثات

عند إصلاح الثغرات الأمنية في التطبيقات، يجب عليك تحديد القواعد لتثبيت التحديثات. تحدد هذه القواعد التحديثات المراد تثبيتها والثغرات الأمنية المراد إصلاحها.

تعتمد نفس الإعدادات عما إذا كنت تقوم بإنشاء قاعدة لتحديثات تطبيقات Microsoft، أو تطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky وMicrosoft) أو لجميع التطبيقات. عند إنشاء قاعدة لتطبيقات Microsoft أو تطبيقات الجهات الخارجية، يمكنك تحديد تطبيقات وإصدارات تطبيق معينة ترغب في تثبيت التحديثات من أجلها. عند إنشاء قاعدة لجميع التطبيقات، يمكنك تحديد تحديثات معينة ترغب في تثبيتها وثغرات أمنية ترغب في إصلاحها عن طريق تثبيت التحديثات.

قم بما يلي لإنشاء قاعدة جديدة لتحديثات جميع التطبيقات:

1. في صفحة **إعدادات** لمعالج المهمة الجديدة، انقر فوق الزر **إضافة**.

يبدأ معالج إنشاء القاعدة. اتبع خطوات المعالج.

2. في الصفحة **نوع القاعدة**، حدد **قاعدة لجميع التحديثات**.

3. في الصفحة **معايير عامة**، قم باستخدام القوائم المنسدلة لتحديد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في الصفحة **تحديثات**، حدد التحديثات المراد تثبيتها:

- **تثبيت جميع التحديثات المناسبة**

تثبيت جميع تحديثات البرامج التي تتوافق مع المعايير المحددة في صفحة **معايير عامة** الخاصة بالمعالج. يتم تحديده بصورة افتراضية.

- **تثبيت التحديثات من القائمة فقط**

قم بتثبيت تحديثات البرامج التي تحددها يدويًا فقط من القائمة. تحتوي القائمة على جميع تحديثات البرامج المتاحة.

على سبيل المثال، قد ترغب في تحديد تحديثات معينة في الحالات التالية: للتحقق من إجراءات تثبيتها في بيئة اختبارية، أو لتحديث التطبيقات المهمة فقط، أو لتحديث التطبيقات المعينة فقط.

- **تثبيت كل تحديثات التطبيق السابقة المطلوبة لتثبيت التحديثات المحددة تلقائيًا**

استمر في تمكين هذا الخيار إذا كنت توافق على تثبيت إصدارات التطبيق مؤقتًا عندما يُطلب ذلك لتثبيت التحديثات المحددة.

إذا تم تعطيل هذا الخيار، فإنه يتم تثبيت إصدارات التطبيقات المحددة فقط. قم بتعطيل هذا الخيار إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون محاولة تثبيت إصدارات متتابعة تدريجيًا. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

على سبيل المثال، لديك الإصدار رقم 3 لتطبيق مثبت على أحد الأجهزة وتريد تحديثه إلى الإصدار رقم 5، ولكن الإصدار رقم 5 لهذا التطبيق يمكن تثبيته فوق الإصدار رقم 4 فقط. إذا تم تمكين هذا الخيار، فإن البرنامج يقوم أولاً بتثبيت الإصدار رقم 4، ومن ثم تثبيت الإصدار رقم 5. إذا تم تعطيل هذا الخيار، فإن البرنامج يفشل في تحديث التطبيق.

يتم تمكين هذا الخيار افتراضيًا.

5. في الصفحة **الثغرات الأمنية**، حدد الثغرات الأمنية التي سيتم إصلاحها عن طريق تثبيت التحديثات المحددة:

- **إصلاح جميع الثغرات الأمنية التي تطابق المعايير الأخرى**

إصلاح جميع الثغرات الأمنية التي تتوافق مع المعايير المحددة في صفحة **معايير عامة** في المعالج. يتم تحديده بصورة افتراضية.

- **إصلاح الثغرات الأمنية من القائمة فقط**

قم بإصلاح الثغرات الأمنية التي تحددها يدويًا فقط من القائمة. تحتوي هذه القائمة على جميع الثغرات الأمنية التي تم اكتشافها.

على سبيل المثال، قد ترغب في تحديد ثغرات أمنية معينة في الحالات التالية: للتحقق من إجراءات إصلاحها في بيئة اختبارية، أو لإصلاح الثغرات الأمنية في التطبيقات المهمة فقط، أو لإصلاح الثغرات الأمنية في تطبيقات معينة فقط.

6. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإنشائها. يمكنك بعد ذلك تغيير هذا الاسم في قسم **الإعدادات**من نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد أن يكمل معالج إنشاء القاعدة عملياته، يتم إنشاء القاعدة الجديدة وعرضها في الحقل **حدد قواعد لتثبيت التحديثات** الخاص بمعالج المهمة الجديدة.

قم بما يلي لإنشاء قاعدة جديدة لتحديثات تطبيقات Microsoft:

1. في صفحة **إعدادات** لمعالج المهمة الجديدة، انقر فوق الزر **إضافة**.

يبدأ معالج إنشاء القاعدة. اتبع خطوات المعالج.

2. في صفحة **نوع القاعدة**، حدد **قاعدة تحديث Windows**.

3. في صفحة **معايير عامة**، حدد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **قم بإصلاح الثغرات الأمنية ذات مستوى الخطورة MSRC الذي يساوي أو أعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Microsoft Security Response Center (MSRC) مساويًا للقيمة المحددة في القائمة أو أعلى منها (**منخفض**، أو **متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضيًا.

5. في الصفحة **فئات التحديثات**، حدد فئات التحديثات المطلوب تثبيتها. هذه الفئات هي نفس الفئات الموجودة في Microsoft Update Catalog. يتم تحديد جميع الفئات افتراضيًا.

6. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإنشائها. يمكنك بعد ذلك تغيير هذا الاسم في قسم **الإعدادات**من نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد أن يكمل معالج إنشاء القاعدة عملياته، يتم إنشاء القاعدة الجديدة وعرضها في الحقل **حدد قواعد لتثبيت التحديثات** الخاص بمعالج المهمة الجديدة.

قم بما يلي لإنشاء قاعدة جديدة لتحديثات تطبيقات الجهات الخارجية:

1. في صفحة **إعدادات** لمعالج المهمة الجديدة، انقر فوق الزر **إضافة**.

يبدأ معالج إنشاء القاعدة. اتبع خطوات المعالج.

2. في صفحة **نوع القاعدة**، حدد**قاعدة تحديثات الأطراف الخارجية**.

3. في صفحة **معايير عامة**، حدد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في الصفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضيًا.

5. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإنشائها. يمكنك بعد ذلك تغيير هذا الاسم في قسم **الإعدادات**من نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد أن يكمل معالج إنشاء القاعدة عملياته، يتم إنشاء القاعدة الجديدة وعرضها في الحقل **حدد قواعد لتثبيت التحديثات** الخاص بمعالج المهمة الجديدة.

مجموعات التطبيقات

يوضح هذا القسم كيفية إدارة مجموعات التطبيقات المثبتة على الأجهزة.

إنشاء فئات التطبيقات

يسمح لك Kaspersky Security Center بإنشاء فئات التطبيقات المثبتة على الأجهزة العميلة.

يمكن إنشاء فئات التطبيقات بإحدى الطرق التالية:

- يحدد المسؤول مجلد يتم فيه تضمين الملفات التنفيذية في الفئة المحددة.
- يحدد المسؤول جهاز يتم فيه تضمين الملفات التنفيذية في الفئة المحددة.
- يقوم المسؤول بتحديد المعايير التي سيتم استخدامها لتضمين التطبيقات في الفئة المحددة.

عند إنشاء فئة التطبيقات، يمكن للمسؤول تعيين قواعد لفئة التطبيق. تحدد القواعد سلوك التطبيقات المضمنة في الفئة المحددة. على سبيل المثال، يمكنك منع أو السماح ببدء تشغيل التطبيقات المضمنة في الفئة.

إدارة التطبيقات على الأجهزة

يتيح لك Kaspersky Security Center إدارة عملية تشغيل التطبيقات على الأجهزة الموجودة في وضع قائمة السماح. للحصول على وصف تفصيلي يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security for Windows عبر الإنترنت. أثناء الوجود في وضع قائمة السماح، يمكنك على الأجهزة المحددة تشغيل التطبيقات المضمنة في الفئات المحددة فقط. يمكن للمسؤول عرض نتائج التحليلات الإحصائية المطبقة على قواعد بدء تشغيل التطبيقات على أجهزة كل مستخدم.

مخزون البرامج المثبتة على الأجهزة

يسمح لك Kaspersky Security Center بإجراء جرد لمخزون البرامج على الأجهزة التي تعمل بنظام Windows وLinux. يستعيد عميل الشبكة معلومات عن جميع التطبيقات المثبتة على الأجهزة. يتم عرض المعلومات المستردة أثناء جرد المخزون في مساحة عمل المجلد **سجل التطبيقات**. يمكن للمسؤول عرض معلومات مفصلة حول تطبيق، بما في ذلك إصداره والشركة المصنعة له.

لا يمكن أن يتجاوز عدد الملفات التنفيذية التي تم استلامها من جهاز مفرد 150 000 ملف. بالوصول لهذا الحد، لا يمكن أن يتلقى Kaspersky Security Center أي ملفات جديدة.

إدارة مجموعة التطبيقات المرخصة

يتيح لك Kaspersky Security Center إنشاء مجموعات التطبيقات المرخصة. تشتمل مجموعات التطبيقات المرخصة على التطبيقات التي تفي بالمعايير المحددة بواسطة المسؤول. يمكن للمسؤول تحديد المعايير التالية لمجموعات التطبيقات المرخصة:

- اسم التطبيق
- إصدار التطبيق
- الشركة المصنعة
- علامة التطبيق

يتم تضمين التطبيقات التي تفي بمعيار واحد أو أكثر تلقائيًا في مجموعة. لإنشاء مجموعة تطبيقات مرخصة، يجب تعيين معيار واحد على الأقل لتضمين التطبيقات في هذه المجموعة.

لكل مجموعة تطبيقات مرخصة مفتاح ترخيص خاص بها. يحدد مفتاح الترخيص لمجموعة التطبيقات المرخصة الحد الأقصى لعدد عمليات التثبيت المسموح بها للتطبيقات المضمنة في هذه المجموعة. إذا تجاوز عدد عمليات التثبيت الحد المحدد بواسطة مفتاح الترخيص، سيتم تسجيل حدث معلوماتي على خادم الإدارة. يمكن للمسؤول تحديد تاريخ انتهاء صلاحية مفتاح الترخيص. عند الوصول إلى هذا التاريخ، يتم تسجيل حدث معلومات على خادم الإدارة.

عرض معلومات حول الملفات التنفيذية

يقوم Kaspersky Security Center باسترجاع جميع المعلومات حول الملفات التنفيذية التي يتم تشغيلها على الأجهزة العميلة منذ تثبيت نظام التشغيل عليها. يتم عرض المعلومات حول الملفات التنفيذية في نافذة التطبيق الرئيسية في مساحة عمل المجلد **الملفات التنفيذية**.

استخدام التحكم في التطبيقات لإدارة الملفات القابلة للتنفيذ

يمكنك استخدام مكون التحكم في التطبيق للسماح ببدء تشغيل الملفات القابلة للتنفيذ أو منعه على أجهزة المستخدم. ويدعم مكون التحكم في التطبيقات أنظمة التشغيل المستندة إلى Windows وLinux.

بالنسبة لأنظمة التشغيل المستندة إلى Linux، يتوفر مكون التحكم في التطبيقات بدءًا من Kaspersky Endpoint Security 11.2 لنظام Linux.
ويتوفر المكون لتطبيق Kaspersky Embedded Systems Security for Windows 3.0 أو أحدث.

المتطلبات الأساسية

- يتم نشر Kaspersky Security Center في مؤسستك.
- تم إنشاء سياسة Kaspersky Endpoint Security for Windows أو Kaspersky Endpoint Security for Linux وهي نشطة.
- تم إنشاء سياسة Kaspersky Embedded Systems Security for Windows أو Kaspersky Embedded Systems Security وهي نشطة.

المراحل

يسير سيناريو استخدام التحكم في التطبيقات في مراحل:

1. **تشكيل قائمة الملفات التنفيذية على أجهزة العميل وعرضها**

تساعدك هذه المرحلة في معرفة الملفات التنفيذية الموجودة على الأجهزة المُدارة. اعرض قائمة الملفات التنفيذية وقارنها بقوائم الملفات التنفيذية المسموح بها والمحظورة. يمكن أن تكون القيود المفروضة على استخدام الملفات التنفيذية متعلقة بسياسات أمان المعلومات في مؤسستك.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: مخزون الملفات التنفيذية
- Kaspersky Security Center Web Console: الحصول على قائمة الملفات التنفيذية المخزنة على أجهزة العميل وعرضها

2. **إنشاء فئات للملفات القابلة للتنفيذ المستخدمة في مؤسستك**

قم بتحليل قوائم الملفات التنفيذية المخزنة على الأجهزة المُدارة. استنادًا إلى التحليل، أنشئ فئات للملفات القابلة للتنفيذ. ومن الموصى به إنشاء فئة "تطبيقات العمل" التي تغطي المجموعة القياسية من الملفات القابلة للتنفيذ في مؤسستك. إذا كانت مجموعات الأمان المختلفة تستخدم مجموعاتها الخاصة من الملفات القابلة للتنفيذ في عملها، فيمكن إنشاء فئة منفصلة لكل مجموعة أمان.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا، إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة، إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد.
- Kaspersky Security Center Web Console: إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا، إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة، إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من مجلد محدد.

3. **تكوين التحكم في التطبيق في سياسة Kaspersky Endpoint Security**

قم بتكوين مكون التحكم في التطبيق في سياسة Kaspersky Endpoint Security باستخدام الفئات التي قمت بإنشائها في المرحلة السابقة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تكوين إدارة بدء تشغيل التطبيق على أجهزة العميل
- Kaspersky Security Center Web Console: تكوين التحكم في التطبيق في سياسة Kaspersky Endpoint Security for Windows

4 **تكوين التحكم في التطبيقات في سياسة تطبيق Kaspersky Embedded Systems Security**

قم بتكوين مكون التحكم في التطبيقات في سياسة Kaspersky Embedded Systems Security for Windows باستخدام الفئات التي أنشأتها. للمزيد من المعلومات عن مكون التحكم في التطبيقات، ارجع إلى تعليمات Kaspersky Embedded Systems Security for Windows أو تعليمات Kaspersky Embedded Systems Security for Linux.

إذا كنت تستخدم عددًا كبيرًا من القواعد، فقد يحدث خطأ عند تحميل السياسة. ويمكنك زيادة الحد الأقصى لحجم الطلب بالبايت باستخدام الأوامر التالية:

- لطلب JSON:

```
s KLLIM -n- "core/.independent." klscflag -fset -pv
t d- <max_request_size> LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v
```

- لطلب HTTP:

```
s KLLIM -n- "core/.independent." klscflag -fset -pv
t d- <max_request_size> LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v
```

حيث `<max_request_size>` هو الحد الأقصى لحجم الطلب بالبايت (على سبيل المثال، `200000000`).

5 **تشغيل مكون التحكم في التطبيقات في وضع الاختبار**

للتأكد من أن قواعد التحكم في التطبيقات لا تحظر الملفات القابلة للتنفيذ المطلوبة لعمل المستخدم، يوصى بتمكين اختبار قواعد التحكم في التطبيقات وتحليل عملها بعد إنشاء قواعد جديدة. وعند تمكين الاختبار، لن يحظر Kaspersky Endpoint Security for Windows أو Kaspersky Embedded Systems Security الملفات التنفيذية التي يحظر بدء تشغيلها بموجب قواعد التحكم في التطبيقات، لكنه بدلاً من ذلك سيرسل إخطارات حول بدء التشغيل إلى خادم الإدارة.

عند اختبار قواعد التحكم في التطبيقات، يُنصح باتخاذ الإجراءات التالية:

- تحديد فترة الاختبار. يمكن أن تتنوع فترة الاختبار من عدة أيام إلى شهرين.
- فحص الأحداث الناتجة عن اختبار عملية التحكم في التطبيقات.

تعليمات إرشادات Kaspersky Security Center Web Console: تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows. اتبع هذه التعليمات وقم بتفعيل خيار **وضع الاختبار** في عملية التكوين.

6 **تغيير إعدادات الفئات لمكون التحكم في التطبيقات**

أجر تغييرات في إعدادات التحكم في التطبيقات عند الضرورة. استنادًا إلى نتائج الاختبار، يمكنك إضافة ملفات قابلة للتنفيذ تتعلق بأحداث مكون التحكم في التطبيق إلى فئة مع إضافة المحتوى يدويًا.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق
- Kaspersky Security Center Web Console: إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق

7 **تطبيق قواعد التحكم في التطبيقات في وضع التشغيل**

بعد اختبار قواعد التحكم في التطبيقات واكتمال تكوين الفئات، يمكنك تطبيق قواعد التحكم في التطبيقات في وضع التشغيل.

تعليمات إرشادات Kaspersky Security Center Web Console: تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security لـ Windows. اتبع هذه التعليمات وقم بتعطيل خيار **وضع الاختبار** في عملية التكوين.

8 **التحقق من تكوين التحكم في التطبيقات**

تأكد من أنك قد قمت بما يلي:

- إنشاء فئات للملفات القابلة للتنفيذ.
- تكوين التحكم في التطبيقات باستخدام الفئات.
- قد طبقت قواعد التحكم في التطبيقات في وضع التشغيل.

النتائج

عند اكتمال السيناريو، يتم التحكم في بدء تشغيل الملفات القابلة للتنفيذ على الأجهزة المُدارة. يمكن للمستخدمين تشغيل الملفات القابلة للتنفيذ المسموح بها في مؤسستك فقط، ولا يمكنهم تشغيل الملفات القابلة للتنفيذ المحظورة في مؤسستك.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent
- تعليمات Kaspersky Embedded Systems Security for Windows
- تعليمات Kaspersky Embedded Systems Security for Linux

الحصول على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل وعرضها

يمكنك الحصول على قائمة الملفات التنفيذية المخزنة على أجهزة العميل بإحدى الطرق التالية:

- تمكين الإخطارات عن بدء التشغيل في سياسة Kaspersky Endpoint Security.
- إنشاء مهمة جرد.

تمكين الإخطارات عن بدء التشغيل في سياسة Kaspersky Endpoint Security

لتمكين الإخطارات حول بدء تشغيل التطبيقات:

1. افتح إعدادات سياسة Kaspersky Endpoint Security، وانتقل إلى **General settings** ← **Reports and Storage**.
2. في مجموعة الإعدادات **Data transfer to Administration Server**، حدد خانة الاختيار **About started applications**، واحفظ التغييرات.

عندما يحاول المستخدم بدء ملفات تنفيذية، تتم إضافة معلومات عن هذه الملفات إلى قائمة الملفات التنفيذية على جهاز عميل. ويرسل Kaspersky Endpoint Security هذه المعلومات إلى عميل الشبكة، ثم يرسلها عميل الشبكة إلى خادم الإدارة.

إنشاء مهمة جرد

ميزة جرد الملفات القابلة للتنفيذ متاحة للتطبيقات التالية:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux version 11.2 وأحدث
- Kaspersky Security for Virtualization 4.0 Light Agent والإصدارات الأحدث

يمكنك تقليل الحمل على قاعدة البيانات أثناء الحصول على معلومات عن التطبيقات المثبتة. لتوفير مساحة، قم بتشغيل مهمة جرد على الأجهزة المرجعية التي تم تثبيت مجموعة قياسية من البرامج عليها. والعدد المفضل للأجهزة هو 3-1.

نوصي بشدة بعدم تشغيل مهمة الجرد عند استخدام قواعد البيانات التالية: MySQL وPostgreSQL وSQL Server Express Edition وMariaDB (جميع الإصدارات).

لإنشاء مهمة مخزون للملفات التنفيذية على الأجهزة العميلة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. في مساحة عمل المجلد **المهام**، انقر على الزر **مهمة جديدة**.

   سيبدأ معالج المهمة الجديدة.
3. في نافذة **تحديد نوع المهمة** الخاصة بالمعالج، حدد **Kaspersky Endpoint Security** كنوع المهمة، ثم حدد **المستودع** كنوع فرعي للمهمة وانقر على **التالي**.
4. اتبع بقية تعليمات المعالج.

بعد انتهاء معالج المهمة الجديدة، يتم إنشاء مهمة **Inventory** وتكوينها. يمكنك إذا كنت ترغب أن تقوم بتغيير إعدادات المهمة التي تم إنشاؤها. يتم عرض المهمة التيتم إنشاؤها في قائمة المهام. يمكنك إذا كنت ترغب أن تقوم بتغيير إعدادات المهمة التي تم إنشاؤها.

للحصول على وصف تفصيلي لمهمة الجرد، راجع المساعدة التالية:

- تعليمات Kaspersky Endpoint Security for Windows
- دعم Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

بعد إجراء مهمة **Inventory**، يتم تشكيل قائمة الملفات التنفيذية المخزنة على الأجهزة المُدارة، ويمكنك عرض القائمة.

أثناء عملية الجرد، يمكن اكتشاف الملفات التنفيذية بالتنسيقات التالية (اعتمادًا على الخيار الذي تحدده في خصائص مهمة الجرد): MZ وCOM وPE وNE وSYS وCMD وBAT وPS1 وJS وVBS وREG وMSI وCPL وDLL وJAR وHTML.

عرض قائمة الملفات التنفيذية المخزنة على الأجهزة المُدارة

لعرض قائمة الملفات التنفيذية المخزنة على أجهزة العميل:

في شجرة وحدة التحكم، انتقل إلى **Advanced** ← **Application management** ← **Executable files**.

إذا لزم الأمر، يمكنك إرسال ملف تنفيذي من جهاز مُدار إلى الجهاز مع تثبيت وحدة تحكم الإدارة.

لإرسال ملف تنفيذي:

1. في شجرة وحدة التحكم، انتقل إلى **Advanced** ← **Application management** ← **Executable files**.
2. انقر على رابط الملف التنفيذي الذي تريد إرساله إلى الجهاز المُثبت عليه وحدة تحكم الإدارة.
3. في النافذة التي تفتح، انتقل إلى القسم **Devices**، ثم حدد خانة الاختيار الخاصة بالجهاز المُدار الذي تريد إرسال الملف القابل للتنفيذ منه.

قبل إرسال الملف التنفيذي تأكد من أن الجهاز المُدار لديه اتصال مباشر بخادم الإدارة، عن طريق تحديد خانة الاختيار **Do not disconnect from the Administration Server**.

4. انقر فوق الزر **Send** ، وحدد مجلد الوجهة، ثم انقر فوق **OK**.

يتم تنزيل الملف التنفيذي المحدد لمزيد من الإرسال إلى الجهاز المُثبت عليه وحدة تحكم الإدارة.

إنشاء فئات التطبيق من أجل سياسات Kaspersky Endpoint Security for Windows

يمكنك إنشاء فئات تطبيق لسياسات Kaspersky Endpoint Security for Windows من المجلد **فئات التطبيق** ومن النافذة **خصائص** الخاصة بسياسة Kaspersky Endpoint Security for Windows.

لإنشاء فئة تطبيق لسياسة Kaspersky Endpoint Security من المجلد **فئات التطبيق**:

1. في شجرة وحدة التحكم، حدد **خيارات متقدمة** ← **إدارة التطبيق** ← **فئات التطبيق**.
2. في مساحة عمل مجلد**فئات التطبيق**، انقر على زر **فئة جديدة**.

يبدأ تشغيل فئة المعالج الجديدة.

3. من الصفحة **نوع الفئة**، حدد نوع فئة المستخدم:

- **الفئة المضاف إليها المحتوى يدويًا**. حدد المعايير التي سيتم استخدامها لتعيين الملفات التنفيذية إلى الفئة التي يتم إنشاؤها.
- **الفئة المضاف إليها المحتوى تلقائيًا**. حدد المجلد الذي سيتم منه تعيين الملفات التنفيذية تلقائيًا إلى الفئة التي تم إنشاؤها.

عند إنشاء فئة تحتوي على محتوى تمت إضافته تلقائيًا، يقوم التطبيق بعمليات جرد لأنواع الملفات التالية: EXE وCOM وDLL وSYS وBAT وPS1 وCMD وJS وVBS وREG وMSI وMSC وCPLI وHTML وHTM وDRV وOCX وSCR.

- **الفئة التي تتضمن الملفات التنفيذية من الأجهزة المحددة**. حدد جهاز الذي يجب تعيين الملفات التنفيذية الخاصة به تلقائيًا إلى الفئة.

4. اتبع إرشادات المعالج.

بعد انتهاء المعالج، يتم إنشاء فئة تطبيق مخصصة. يمكنك عرض الفئات التي تم إنشاؤها حديثًا باستخدام قائمة الفئات الموجودة في مساحة عمل المجلد **فئات التطبيق**.

إذا كنت تريد تصدير فئة تطبيق إلى ملف KLC، فانقر بزر الماوس الأيمن فوق اسم الفئة، وحدد **تصدير** في القائمة، ثم في النافذة التي تفتح، حدد اسم الملف وانقر فوق **حفظ**.

يمكنك أيضًا إنشاء فئة تطبيق من المجلد **السياسات**.

لإنشاء فئة تطبيق من نافذة **الخصائص** الخاصة بسياسة Kaspersky Endpoint Security for Windows:

1. من شجرة وحدة التحكم، حدد مجلد **السياسات**.
2. في مساحة عمل المجلد **السياسات**، حدد سياسة Kaspersky Endpoint Security التي ترغب في إنشاء فئة لها.
3. انقر بزر الماوس الأيمن، وحدد **خصائص**.
4. في النافذة **الخصائص** التي تفتح، ومن الجزء الأيسر **الأقسام**، حدد **عناصر التحكم في الأمان** ← **التحكم في التطبيقات**.
5. في قسم **التحكم في التطبيقات**، في القوائم المنسدلة **وضع التحكم** و**الإجراء**، قم بإجراء تحديدات قائمة السماح أو قائمة الرفض ثم انقر فوق زر **إضافة**.
   يتم فتح نافذة قاعدة **التحكم في التطبيقات** التي تحتوي على قائمة من الفئات.
6. انقر فوق الزر **إنشاء جديد**.
7. أدخل اسم الفئة الجديدة وانقر فوق **نعم**.
   يبدأ تشغيل فئة المعالج الجديدة.

8. من الصفحة **نوع الفئة**، حدد نوع فئة المستخدم:

- **الفئة المضاف إليها المحتوى يدويًا**. حدد المعايير التي سيتم استخدامها لتعيين الملفات التنفيذية إلى الفئة التي يتم إنشاؤها.
- **الفئة المضاف إليها المحتوى تلقائيًا**. حدد المجلد الذي سيتم منه تعيين الملفات التنفيذية تلقائيًا إلى الفئة التي تم إنشاؤها.

عند إنشاء فئة تحتوي على محتوى تمت إضافته تلقائيًا، يقوم التطبيق بعمليات جرد لأنواع الملفات التالية: EXE وCOM وDLL وSYS وBAT وPS1 وCMD وJS وVBS وREG وMSI وMSC وCPLI وHTML وHTM وDRV وOCX وSCR.

- **الفئة التي تتضمن الملفات التنفيذية من الأجهزة المحددة**. حدد جهاز الذي يجب تعيين الملفات التنفيذية الخاصة به تلقائيًا إلى الفئة.

9. اتبع إرشادات المعالج.

بعد انتهاء المعالج، يتم إنشاء فئة تطبيق مخصصة. يمكنك عرض الفئات التي تم إنشاؤها حديثًا في قائمة الفئات.

يتم استخدام فئات التطبيق بواسطة مكون التحكم في التطبيقات الموجود في Kaspersky Endpoint Security for Windows. تتيح عملية التحكم في التطبيقات للمسؤول فرض قيود على بدء تشغيل التطبيقات على الأجهزة العميلة؛ على سبيل المثال، تقييد عمليات بدء التشغيل لتطبيقات في فئة محددة.

إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا

يمكنك تحديد مجموعة من المعايير كقالب للملفات التنفيذية التي ترغب في السماح ببدئها أو حظرها في مؤسستك. على أساس الملفات التنفيذية التي تستوفي المعايير، يمكنك إنشاء فئة تطبيق واستخدامها في تكوين مكون التحكم في التطبيقات.

لإنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا:

1. من شجرة وحدة التحكم، في المجلد **خيارات متقدمة** ← **إدارة التطبيق** حدد المجلد الفرعي **فئات التطبيق**.
2. انقر على زر **فئة جديدة**.

   يبدأ تشغيل **معالج فئة جديدة**. انتقل عبر المعالج باستخدام زر **التالي**.
3. في صفحة معالج **نوع الفئة**، حدد **الفئة المضاف إليها المحتوى يدويًا** كنوع فئة المستخدم.
4. في صفحة معالج **أدخل اسم فئة التطبيق**، أدخل اسم فئة التطبيق الجديد.
5. في صفحة **تهيئة الشروط لإدراج التطبيقات في الفئات**، انقر فوق الزر **إضافة**.
6. في القائمة المنسدلة، حدد الإعدادات ذات الصلة:

- **من قائمة الملفات التنفيذية**

إذا تم تحديد هذا الخيار، فيمكنك استخدام قائمة الملفات التنفيذية على الجهاز العميل لتحديد التطبيقات وإضافتها إلى الفئة.

- **من خصائص الملف**

إذا تم تحديد هذا الخيار، يمكنك تحديد البيانات التفصيلية للملفات التنفيذية التي ستُضاف إلى فئة تطبيقات المستخدم.

- **بيانات وصفية من الملفات في المجلد**

حدد مجلدًا في الجهاز العميل الذي يحتوي على الملفات التنفيذية. سيتم إرسال البيانات الوصفية الموجودة في الملفات التنفيذية المضمنة في المجلد المحدد إلى خادم الإدارة. ستتم إضافة الملفات التنفيذية التي تحتوي على نفس البيانات الوصفية إلى فئة تطبيقات المستخدم.

- **المجموعات الاختبارية للملفات في المجلد**

إذا تم تحديد هذا الخيار، فيمكنك تحديد أو إنشاء مجلد على الجهاز العميل. سيتم إرسال تجزئة MD5 للملفات في المجلد المحدد إلى خادم الإدارة. تتم إضافة التطبيقات التي لها نفس تجزئة الملفات الموجودة في المجلد المحدد إلى فئة تطبيقات المستخدم.

- **شهادات الملفات من المجلد**

إذا تم تحديد هذا الخيار، فيمكنك تحديد المجلد على الجهاز العميل والذي يحتوي على ملفات تنفيذية موقعة مع الشهادات. تتم قراءة شهادات الملفات التنفيذية وإضافتها إلى شروط الفئة. ستتم إضافة الملفات التنفيذية التي تم توقيعها وفقًا للشهادات المحددة إلى فئة المستخدم.

لا يمكن استخراج المعلومات عن الشهادات إلا من الملفات القابلة للتنفيذ بتنسيق PE (.exe، .dll، .sys).

- **البيانات الوصفية لملفات مُثبّت MSI**

إذا تم تحديد هذا الخيار، يمكنك تحديد ملف مثبّت MSI كشرط لإضافة تطبيقات إلى فئة المستخدم. وسيتم إرسال البيانات الوصفية لمثبِّت التطبيق إلى خادم الإدارة. تتم إضافة التطبيقات التي تشبه فيها البيانات الوصفية للمثبت مثبت MSI المحدد إلى فئة تطبيقات المستخدم.

- **المجاميع الاختبارية لملفات من مُثبِّت MSI الخاص بالتطبيق**

إذا تم تحديد هذا الخيار، يمكنك تحديد ملف مثبّت MSI كشرط لإضافة تطبيقات إلى فئة المستخدم. سيتم إرسال تجزئة ملفات مثبِّت التطبيق إلى خادم الإدارة. تتم إضافة التطبيقات التي تطابق تجزئة ملفات MSI فيها التجزئة المحددة إلى فئة تطبيق المستخدم.

- **من فئة KL**

إذا تم تحديد هذا الخيار، يمكنك تحديد فئة تطبيق Kaspersky كشرط لإضافة تطبيقات إلى فئة المستخدم. ستتم إضافة التطبيقات من فئة Kaspersky المحددة إلى فئة تطبيقات المستخدم.

- **تحديد المسار إلى تطبيق (يدعم الأقنعة)**

إذا تم تحديد هذا الخيار، فيمكنك تحديد المسار المؤدي إلى الملف أو المجلد الموجود على الجهاز العميل الذي يحتوي على الملفات التنفيذية المراد إضافتها إلى فئة تطبيقات المستخدم. يمكنك استخدام التعبيرات العادية مثل C:\path_to_exe*، على سبيل المثال: C:\Program Files\Internet\Explorer*.

- **تحديد شهادة من المستودع**

إذا تم تحديد هذا الخيار، فيمكنك تحديد الشهادات من المستودع. يتطابق شرط الفئة فقط مع الملفات التنفيذية الموقعة بواسطة الشهادة المحددة.

يتم إضافة الشهادات إلى المستودع إذا أنشأت مهمة جرد وبدأتها أو حددت خانة الاختيار **عن التطبيقات التي تم بدء تشغيلها** في سياسة Kaspersky Endpoint Security. ويمكنك تنفيذ كلا الإجراءين.

لا يمكن استخراج المعلومات عن الشهادات إلا من الملفات القابلة للتنفيذ بتنسيق PE (.exe، .dll، .sys).

- **نوع محرك الأقراص**

إذا تم تحديد هذا الخيار، يمكنك تحديد نوع الوسيط (أي جهاز أو جهاز قابل للإزالة) الذي يعمل عليه التطبيق. تتم إضافة التطبيقات التي تم تشغيلها على نوع محرك الأقراص المحدد إلى فئة تطبيقات المستخدم.

7. في صفحة معالج **إنشاء فئة التطبيق**، انقر فوق الزر **إنهاء**.

يتعامل Kaspersky Security Center فقط مع البيانات الوصفية من الملفات الموقع عليها رقميًا. لا يمكن إنشاء أي فئة بناءً على البيانات الوصفية من الملفات التي لا تحتوي على توقيع رقمي.

عند اكتمال المعالج، يتم إنشاء فئة تطبيق مستخدم، مضافًا إليها المحتوى يدويًا. يمكنك عرض الفئة التي تم إنشاؤها حديثًا باستخدام قائمة الفئات الموجودة في مساحة عمل المجلد **فئات التطبيق**.

إذا كنت تريد تصدير فئة تطبيق إلى ملف KLC، فانقر بزر الماوس الأيمن فوق اسم الفئة، وحدد **تصدير** في القائمة، ثم في النافذة التي تفتح، حدد اسم الملف وانقر فوق **حفظ**.

إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة

يمكنك استخدام الملفات التنفيذية من الأجهزة المحددة كقوالب للملفات التنفيذية التي ترغب في السماح لها أو حظرها. على أساس الملفات التنفيذية من الأجهزة المحددة، يمكنك إنشاء فئة تطبيق واستخدامها في تكوين مكون التحكم في التطبيقات.

لاسترداد قائمة الملفات التنفيذية من الأجهزة:

1. تأكد من إنشاء سياسة Kaspersky Endpoint Security for Windows أو Kaspersky Endpoint Security for Linux وأنها نشطة. قم بتمكين مكون التحكم في التطبيقات في السياسة.

2. احصل على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل.

لإنشاء فئة تطبيق تتضمن ملفات تنفيذية من أجهزة محددة:

1. من شجرة وحدة التحكم، في المجلد **خيارات متقدمة** ← **إدارة التطبيق** حدد المجلد الفرعي **فئات التطبيق**.

2. انقر على زر **فئة جديدة**.

   يبدأ تشغيل **معالج فئة جديدة**. انتقل عبر المعالج باستخدام زر **التالي**.

3. في صفحة معالج **نوع الفئة**، حدد **الفئة التي تتضمن ملفات تنفيذية من الأجهزة المحددة** كنوع فئة المستخدم.

4. في صفحة معالج **أدخل اسم فئة التطبيق**، أدخل اسم فئة التطبيق الجديد.

5. في صفحة معالج **إعدادات**، انقر فوق الزر **Add**.

6. حدد جهازًا أو أجهزة سيتم استخدام ملفاتها التنفيذية في إنشاء فئة التطبيق.

7. حدد الإعدادات التالية:

- **خوارزمية الحساب لقيمة التجزئة**

بناءً على رقم إصدار تطبيق الأمان المثبت على الأجهزة الموجودة على شبكتك، يجب عليك تحديد خوارزمية لحساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في هذه الفئة. يتم تخزين المعلومات عن قيم التجزئة المحسوبة بواسطة وظائف التجزئة في قاعدة بيانات خادم الإدارة.

SHA256 هي وظيفة تجزئة التشفير: لم يتم العثور على ثغرات أمنية في الخوارزميات الخاصة بها، فهي تعتبر وظيفة التشفير الأكثر موثوقية في الوقت الحاضر. يدعم Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث حساب SHA256. حساب وظيفة تجزئة MD5 مدعوم من جميع الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

حدد أيًا من خيارات حساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في الفئة:

- إذا كانت جميع مثيلات تطبيقات الأمان المثبتة على شبكتك هي Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows أو الإصدارات الأحدث، فحدد خانة الاختيار **SHA256** . لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA256 لملف تنفيذي للإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows. قد يتسبب ذلك في حدوث عمليات فشل في تشغيل تطبيق الأمان. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير MD5 لملفات الفئة.

- إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows على شبكتك، فحدد ملف **MD5 hash**. لا يمكنك إضافة فئة تم إنشاؤها بناءً على معيار مجموع تجزئة MD5 لملف تنفيذي لـ Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو الإصدارات الأحدث. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير SHA256 لملفات الفئة.

إذا كانت الأجهزة المختلفة الموجودة على شبكتك تستخدم كلاً من الإصدارات السابقة والإصدارات الأحدث من Kaspersky Endpoint Security 10، فحدد خانة الاختيار **SHA256** وخانة اختيار **MD5 hash**.

يتم تحديد خانة الاختيار **حساب SHA256 للملفات في هذه الفئة (المدعومة من Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو أي إصدارات أحدث)** بشكل افتراضي.

يتم إلغاء تحديد خانة الاختيار **حساب MD5 للملفات في هذه الفئة (المدعومة بواسطة الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** بشكل افتراضي.

- **Synchronize data with Administration Server repository**

حدد هذا الخيار إذا كنت ترغب في أن يقوم خادم الإدارة بالتحقق من التغييرات في المجلد المحدد (المجلدات المحددة) كل فترة.

يتم تعطيل هذا الخيار افتراضيًا.

إذا قمت بتفعيل هذا الخيار، حدد الفترة (بالساعات) للتحقق من التغييرات في المجلد المحدد (المجلدات المحددة). بشكل افتراضي، الفاصل الزمني للفحص هو 24 ساعة.

8. في صفحة معالج **عامل التصفية**، حدد الإعدادات التالية:

- **File type**

يمكنك في هذا القسم تحديد نوع الملف المستخدم في إنشاء فئة التطبيق.

All files. يتم أخذ جميع الملفات في الاعتبار عند إنشاء الفئة. يتم تحديد هذا الخيار افتراضيًا.

Only files outside the application categories. لا يتم الأخذ في الاعتبار عند إنشاء الفئة إلا الملفات خارج فئات التطبيقات.

- **Folders**

يمكنك في هذا القسم تحديد المجلدات من الجهاز المحدد (الأجهزة المحددة) التي تحتوي على ملفات مستخدمة لإنشاء فئة التطبيق.

All folders. يتم أخذ جميع المجلدات في الاعتبار لإنشاء الفئة. يتم تحديد هذا الخيار افتراضيًا.

Specified folder. لا يتم أخذ في الاعتبار لإنشاء الفئة إلا المجلد المحدد. في حالة تحديدك لهذا الخيار، يجب أن تحدد المسار الخاص بالمجلد.

9. في صفحة معالج **إنشاء فئة التطبيق**، انقر فوق الزر **إنهاء**.

عند اكتمال المعالج، يتم إنشاء فئة تطبيق مستخدم. يمكنك عرض الفئة التي تم إنشاؤها حديثًا باستخدام قائمة الفئات الموجودة في مساحة عمل المجلد **فئات التطبيق**.

إذا كنت تريد تصدير فئة تطبيق إلى ملف KLC، فانقر بزر الماوس الأيمن فوق اسم الفئة، وحدد **تصدير** في القائمة، ثم في النافذة التي تفتح، حدد اسم الملف وانقر فوق **حفظ**.

إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد

يمكنك استخدام الملفات التنفيذية من مجلد محدد كمقياس للملفات التنفيذية التي ترغب في السماح لها أو حظرها في مؤسستك. على أساس الملفات التنفيذية من المجلد المحدد، يمكنك إنشاء فئة تطبيق واستخدامها في تكوين مكون التحكم في التطبيقات.

لإنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد:

1. من شجرة وحدة التحكم، في المجلد **خيارات متقدمة** ← **إدارة التطبيق** حدد المجلد الفرعي **فئات التطبيق**.

2. انقر على زر **فئة جديدة**.

يبدأ تشغيل **معالج فئة جديدة**. انتقل عبر المعالج باستخدام زر **التالي**.

3. في صفحة معالج **نوع الفئة**، حدد **الفئة التي تتضمن ملفات تنفيذية من مجلد معين** كنوع فئة المستخدم.

4. في صفحة معالج **أدخل اسم فئة التطبيق**، أدخل اسم فئة التطبيق الجديد.

5. في صفحة معالج **مجلد المستودع**، انقر فوق الزر **استعراض**.

6. حدد المجلد الذي سيتم استخدام الملفات التنفيذية الموجودة فيه لإنشاء فئة التطبيق.

7. حدد الإعدادات التالية:

- **Include dynamic-link libraries (DLL) in this category**

تشمل فئة التطبيق مكتبات الروابط الديناميكية (ملفات بتنسيق DLL)، ويسجّل مكون التحكم في التطبيقات الإجراءات التي تقوم هذه المكتبات بتشغيلها في النظام. قد يؤدي تضمين ملفات DLL في الفئة إلى خفض أداء Kaspersky Security Center.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **Include script data in this category**

تشمل فئة التطبيق البيانات الموجودة على البرامج النصية ولا يتم حظر البرامج النصية بواسطة "الحماية من تهديدات الويب". قد يؤدي تضمين بيانات البرنامج النصي في الفئة إلى خفض أداء Kaspersky Security Center.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **خوارزمية حساب قيمة التجزئة: 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)**

بناءً على رقم إصدار تطبيق الأمان المثبت على الأجهزة الموجودة على شبكتك، يجب عليك تحديد خوارزمية لحساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في هذه الفئة. يتم تخزين المعلومات عن قيم التجزئة المحسوبة بواسطة وظائف التجزئة في قاعدة بيانات خادم الإدارة.

SHA256 هي وظيفة تجزئة التشفير: لم يتم العثور على ثغرات أمنية في الخوارزميات الخاصة بها، فهي تعتبر وظيفة التشفير الأكثر موثوقية في الوقت الحاضر. يدعم Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث حساب SHA256. حساب وظيفة تجزئة MD5 مدعوم من جميع الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

حدد أيًا من خيارات حساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في الفئة:

- إذا كانت جميع مثيلات تطبيقات الأمان المثبتة على شبكتك هي Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows أو الإصدارات الأحدث، فحدد خانة الاختيار **SHA256** . لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA256 لملف تنفيذي للإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows. قد يتسبب ذلك في حدوث عمليات فشل في تشغيل تطبيق الأمان. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير MD5 لملفات الفئة.

- إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows على شبكتك، فحدد ملف **MD5 hash**. لا يمكنك إضافة فئة تم إنشاؤها بناءً على معيار مجموع تجزئة MD5 لملف تنفيذي لـ Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو الإصدارات الأحدث. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير SHA256 لملفات الفئة.

إذا كانت الأجهزة المختلفة الموجودة على شبكتك تستخدم كلاً من الإصدارات السابقة والإصدارات الأحدث من Kaspersky Endpoint Security 10، فحدد خانة الاختيار **SHA256** وخانة اختيار **MD5 hash**.

يتم تحديد خانة الاختيار **حساب SHA256 للملفات في هذه الفئة (المدعومة من Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو أي إصدارات أحدث)** بشكل افتراضي.

يتم إلغاء تحديد خانة الاختيار **حساب MD5 للملفات في هذه الفئة (المدعومة بواسطة الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** بشكل افتراضي.

- **Force folder scan for changes**

إذا تم تمكين هذا الخيار، فسيبحث التطبيق بشكل منتظم عن مجلد إضافة محتوى الفئة لإجراء التغييرات. يمكنك تحديد تكرار الفحوصات (بالساعات) في حقل الإدخال بجوار خانة الاختيار. وبشكل افتراضي، يكون الفاصل الزمني بين الفحوصات الإجبارية هو 24 ساعة.

إذا تم تعطيل هذا الخيار، فلن يفرض التطبيق أي تحققات من المجلد. يحاول الخادم الوصول إلى الملفات إذا تم تعديلها أو إضافتها أو حذفها.

يتم تعطيل هذا الخيار افتراضيًا.

8. في صفحة معالج **إنشاء فئة التطبيق**، انقر فوق الزر **إنهاء**.

عند اكتمال المعالج، يتم إنشاء فئة تطبيق مستخدم. يمكنك عرض الفئة التي تم إنشاؤها حديثًا باستخدام قائمة الفئات الموجودة في مساحة عمل المجلد **فئات**

التطبيق.

إذا كنت تريد تصدير فئة تطبيق إلى ملف KLC، فانقر بزر الماوس الأيمن فوق اسم الفئة، وحدد **تصدير** في القائمة، ثم في النافذة التي تفتح، حدد اسم الملف وانقر فوق **حفظ**.

إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق

يمكنك إضافة الملفات التنفيذية المتعلقة بأحداث **حظر بدء تشغيل التطبيق** و **حظر بدء تشغيل التطبيق في وضع الاختبار** إلى فئة تطبيق موجودة بالفعل ذات محتوى مُضاف يدويًا أو إلى فئة تطبيق جديدة.

لإضافة ملفات تنفيذية ذات صلة بأحداث التحكم في التطبيقات إلى فئة التطبيق:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.
3. في علامة التبويب **الأحداث**، حدد الحدث المطلوب.
4. في قائمة السياق لأحد الأحداث المحددة، حدد **إضافة إلى فئة**.
5. في النافذة **الإجراء بشأن الملف التنفيذي المتعلق بالحدث** التي تفتح، حدد الإعدادات ذات الصلة:

   حدد واحدًا مما يلي:

   - **إضافة إلى فئة تطبيق جديدة**

     حدد هذا الخيار إذا كنت ترغب في إنشاء فئة تطبيق جديدة.

     انقر فوق الزر **موافق** لتشغيل معالج الفئة الجديدة. عند اكتمال المعالج، يتم إنشاء فئة بالإعدادات المحددة.

     لا يتم تحديد هذا الخيار افتراضيًا.

   - **إضافة إلى فئة تطبيق حالي**

     حدد هذا الخيار إذا كان يتعين عليك إضافة قواعد لفئة تطبيق حالية. تحديد الفئة ذي الصلة في قائمة فئات التطبيقات.

     ويتم تحديد هذا الخيار بصورة افتراضية.

   في القسم **نوع القاعدة**، حدد واحدًا من الإعدادات التالية:

   - **إضافة إلى فئة**

     حدد هذا الخيار إذا كان يتعين عليك إضافة قواعد لشروط فئة التطبيق.

     ويتم تحديد هذا الخيار بصورة افتراضية.

   - **قواعد الإضافة إلى الاستثناءات**

     حدد هذا الخيار إذا كنت ترغب في إضافة قواعد لاستثناءات فئة التطبيق.

   في القسم **نوع معلومات الملف**، حدد واحدًا من الإعدادات التالية:

   - **تفاصيل الشهادة (أو تجزئات SHA256 للملفات التي لا يوجد لديها شهادة)**

     قد يتم توقيع الملفات باستخدام شهادة. قد يتم توقيع ملفات متعددة باستخدام الشهادة ذاتها. على سبيل المثال، قد يتم توقيع الإصدارات المختلفة للتطبيق ذاته باستخدام الشهادة ذاتها أو العديد من التطبيقات المختلفة من البائع ذاته باستخدام الشهادة ذاتها. عند تحديد شهادة ما، قد تنتهي العديد من إصدارات تطبيق ما أو تطبيقات مختلفة من البائع ذاته إلى الفئة.

كل ملف لديه وظيفة تجزئة SHA256 فريدة خاصة به. عندما تحديد وظيفة تجزئة SHA256 ، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة.

حدد هذا الخيار إذا كنت ترغب بإضافة تفاصيل الشهادة الخاصة بملف تنفيذي إلى قواعد الفئة (أو وظيفة تجزئة SHA256 للملفات بدون شهادة).

يتم تحديد هذا الخيار افتراضيًا.

- **تفاصيل الشهادة (سيتم تخطي الملفات التي لا يوجد لديها شهادة)**

قد يتم توقيع الملفات باستخدام شهادة. قد يتم توقيع ملفات متعددة باستخدام الشهادة ذاتها. على سبيل المثال، قد يتم توقيع الإصدارات المختلفة للتطبيق ذاته باستخدام الشهادة ذاتها أو العديد من التطبيقات المختلفة من البائع ذاته باستخدام الشهادة ذاتها. عند تحديد شهادة ما، قد تنتهي العديد من إصدارات تطبيق ما أو تطبيقات مختلفة من البائع ذاته إلى الفئة.

حدد هذا الخيار إذا كنت ترغب بإضافة تفاصيل الشهادة الخاصة بملف تنفيذي لقواعد الفئة. إن لم يكن الملف التنفيذي يحتوي على شهادة، فسيتم تخطي هذا الملف. لم يتم إضافة معلومات حول هذا الملف إلى الفئة.

- **SHA256 فقط (سيتم تخطي الملفات التي لايوجد بها تجزئة)**

كل ملف لديه وظيفة تجزئة SHA256 فريدة خاصة به. عندما تحديد وظيفة تجزئة SHA256 ، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة.

حدد هذا الخيار إذا كنت ترغب بإضافة فقط تفاصيل وظيفة تجزئة SHA256 الخاصة بالملف التنفيذي.

- **MD5 فقط (وضع الإيقاف، فقط لإصدار Kaspersky Endpoint Security 10 Service Pack 1)**

كل ملف لديه وظيفة تجزئة MD5 فريدة خاصة به. عندما تحديد وظيفة تجزئة MD5 ، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة.

حدد هذا الخيار إذا كنت ترغب بإضافة فقط تفاصيل وظيفة تجزئة MD5 الخاصة بالملف التنفيذي. حساب وظيفة تجزئة MD5 مدعومة من Kaspersky Endpoint Security 10 Service Pack 1 for Windows وكل الإصدارات الأقدم.

6. انقر فوق **موافق**.

تكوين إدارة بدء تشغيل التطبيق على الأجهزة العميلة

يتيح لك تصنيف التطبيقات تحسين إدارة التطبيق الذي يعمل على الأجهزة. يمكنك إنشاء فئة تطبيقات وتكوين التحكم في التطبيقات للسياسة الواحدة، ليتم بدء التطبيقات من الفئة المحددة فقط على الأجهزة التي تنطبق عليها هذه السياسة. على سبيل المثال، قمت بإنشاء فئة تشتمل على تطبيقات تُسمى التطبيق_1 و التطبيق_2. بعد قيامك بإضافة هذه الفئة إلى سياسة، يسمح ببدء تطبيقين فقط على الأجهزة التي تنطبق عليها هذه السياسة: التطبيق_1 والتطبيق_2. إذا حاول المستخدم بدء تطبيق غير مشمول في هذه الفئة، على سبيل المثال، التطبيق_3، سيتم منع هذا التطبيق من البدء. سيتم إظهار إخطار للمستخدم ينص على أن التطبيق_3 تم منع بدء تشغيله وفقًا إلى قاعدة التحكم في التطبيقات. يمكنك إنشاء فئة ذات محتوى مضاف تلقائيًا بناءً على معايير مختلفة من مجلد محدد. في هذه الحالة، يتم إضافة الملفات تلقائيًا إلى الفئة من المجلد المحدد. يتم نسخ الملفات التنفيذية للتطبيقات إلى المجلد المحدد ومعالجتها تلقائيًا؛ كما يتم إضافة مقاييسها إلى الفئة.

لتكوين إدارة بدء التطبيقات على الأجهزة العميلة:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **فئات التطبيق**.

2. في مساحة عمل المجلد **فئات التطبيق**، قم بإنشاء فئة التطبيقات التي تريد إدارتها أثناء بدء تشغيلها.

3. في مجلد **الأجهزة المُدارة** وفي علامة التبويب **السياسات**، انقر فوق الزر **سياسة جديدة** لإنشاء سياسة جديدة لتطبيق Kaspersky Endpoint Security for Windows واتبع تعليمات المعالج.

في حالة وجود مثل هذه السياسة، فيمكنك تجاوز هذه الخطوة. يمكنك تكوين إدارة بدء التطبيقات في فئة محددة من خلال إعدادات هذه السياسة. يتم عرض السياسة التي تم إنشاؤها حديثًا في المجلد **الأجهزة المُدارة** على علامة التبويب **السياسات**.

4. حدد **خصائص** من قائمة سياق سياسة Kaspersky Endpoint Security for Windows.

يتم فتح نافذة خصائص سياسة Kaspersky Endpoint Security for Windows.

5. في نافذة خصائص سياسة Kaspersky Endpoint Security for Windows، في القسم **ضوابط الأمان** ← **التحكم في التطبيقات** حدد خانة الاختيار **التحكم في التطبيقات**.

6. انقر على زر **إضافة**.

يتم فتح نافذة **قاعدة التحكم في التطبيقات**.

7. في نافذة **قاعدة التحكم في التطبيقات** في القائمة المنسدلة **الفئة** حدد فئة التطبيقات التي ستغطيها قاعدة بدء التشغيل. تكوين قاعدة البدء لفئة التطبيق التي تم تحديدها.

بالنسبة إلى Kaspersky Endpoint Security 10 Service Pack 2 والإصدارات الأحدث، لا يتم عرض الفئات في حالة إنشائها وفقًا لمعيار تجزئة MD5 لملف تنفيذي.

لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA256 لملف تنفيذي للإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows. قد يؤدي هذا إلى فشل التطبيق.

تتوفر إرشادات مفصلة حول قواعد التحكم في التكوين في تعليمات Kaspersky Endpoint Security for Windows عبر الإنترنت.

8. انقر فوق **موافق**.

سيتم تشغيل التطبيقات على الأجهزة المضمَّنة في الفئة المحددة طبقًا للقاعدة التي قمت إنشائها. يتم عرض القاعدة التي تم إنشاؤها حديثًا في نافذة خصائص سياسة Kaspersky Endpoint Security for Windows، في قسم **التحكم في التطبيقات**.

عرض نتائج التحليل الإحصائي لقواعد بدء التشغيل المطبقة على الملفات التنفيذية

لعرض معلومات حول الملفات التنفيذية المحظور على المستخدمين تشغيلها:

1. في المجلد **الأجهزة المُدارة** في شجرة وحدة التحكم، حدد علامة التبويب **السياسات**.

2. حدد **خصائص** من قائمة سياق سياسة Kaspersky Endpoint Security for Windows.

يتم فتح نافذة خصائص سياسة التطبيق.

3. في الجزء **الأقسام**، حدد **عناصر التحكم في الأمان**، ثم حدد القسم الفرعي **التحكم في التطبيقات**.

4. انقر فوق زر **التحليل الإحصائي**.

تفتح نافذة **تحليل قائمة حقوق الوصول**. في الجزء الأيسر من النافذة يتم عرض قائمة بالمستخدمين استنادًا إلى بيانات Active Directory.

5. حدد مستخدمًا من القائمة.

يعرض الجزء الأيسر للنافذة فئات التطبيقات المخصصة لهذا المستخدم.

6. لعرض الملفات التنفيذية التي لا يسمح للمستخدم بتشغيلها، انقر فوق **عرض الملفات** في النافذة **تحليل قائمة حقوق الوصول**.

تفتح نافذة، عرض قائمة بالملفات التنفيذية الممنوعة.

7. لعرض قائمة الملفات التنفيذية المضمنة في فئة، حدد فئة التطبيق وانقر فوق الزر **عرض الملفات في الفئة**.

تفتح نافذة تعرض قائمة الملفات التنفيذية المضمَّنة في فئة التطبيق.

عرض سجل التطبيقات

يقوم Kaspersky Security Center بتخزين جميع البرامج المثبتة على الأجهزة المدارة.

يجمع عميل الشبكة قائمة بالتطبيقات المثبتة على جهاز يعمل بنظام التشغيل Windows أو Linux، ثم يرسل هذه القائمة إلى خادم الإدارة. بالنسبة للأجهزة العميلة المستندة إلى Windows، يتلقى عميل الشبكة معظم المعلومات حول التطبيقات المثبتة من سجل Windows. بالنسبة للأجهزة العميلة المستندة إلى Linux، يوفر مديرو الحزم معلومات حول التطبيقات المثبتة إلى عميل الشبكة.

لعرض سجل التطبيقات المثبتة على الأجهزة العميلة,

في مجلد**خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **سجل التطبيقات**.

تعرض مساحة عمل مجلد **سجل التطبيقات** قائمة بالتطبيقات المثبتة على الأجهزة العميلة وخادم الإدارة.

يمكنك عرض التفاصيل الخاصة بأي تطبيق عن طريق فتح قائمة السياق الخاصة به وتحديد **خصائص**. تعرض نافذة خصائص التطبيق تفاصيل التطبيق ومعلومات حول الملفات التنفيذية الخاصة به، بالإضافة إلى قائمة بالأجهزة المثبت عليها التطبيق.

في قائمة السياق لأي تطبيق في أي تطبيق، يمكنك:

- إضافة هذا التطبيق إلى فئة تطبيق.
- تخصيص علامة للتطبيق.
- تصدير قائمة التطبيقات إلى ملف CSV أو TXT.
- عرض خصائص التطبيق، على سبيل المثال اسم البائع أو رقم الإصدار أو قائمة الملفات التنفيذية أو قائمة الأجهزة المثبت عليها التطبيق أو قائمة تحديثات البرنامج أو قائمة الثغرات الأمنية المكتشفة في البرنامج.

لعرض التطبيقات التي تتطابق مع المعايير المحددة، يمكنك استخدام حقول التصفية في مساحة عمل مجلد **سجل التطبيقات**.

في نافذة الخصائص للجهاز المحدد، في القسم **سجل التطبيقات**، يمكنك عرض قائمة بالتطبيقات المثبتة على الجهاز.

إنشاء تقرير حول التطبيقات المثبتة

في مساحة العمل **سجل التطبيقات**، يمكنك أيضًا النقر فوق الزر **عرض تقرير حول التطبيقات المثبتة** لإنشاء تقرير يشتمل على إحصائيات تفصيلية عن التطبيقات المثبتة، بما في ذلك عدد الأجهزة المثبت عليها كل تطبيق. يشتمل هذا التقرير، الذي يفتح في صفحة **تقرير حول التطبيقات المثبتة**، على معلومات عن كل من تطبيقات Kaspersky وبرامج الجهات الأخرى. إذا أردت معلومات فقط عن تطبيقات Kaspersky المثبتة على أجهزة العملاء، حدد AO Kaspersky Lab في قائمة **الملخص**.

ويتم كذلك تخزين معلومات حول تطبيقات Kaspersky والبرامج التابعة لجهات خارجية المثبتة على الأجهزة المتصلة بخوادم إدارة ثانوية وظاهرية في سجل التطبيقات الخاص بخادم الإدارة الرئيسي. بعد إضافتك للبيانات من خوادم الإدارة الثانوية والظاهرية، انقر فوق الزر **عرض تقرير حول التطبيقات المثبتة** وعلى الصفحة **تقرير حول التطبيقات المثبتة** التي تفتح، حيث بإمكانك عرض هذه المعلومات.

لإضافة معلومات من خوادم الإدارة الثانوية والظاهرية إلى تقرير حول التطبيقات المثبتة:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .
3. في علامة التبويب **التقارير**، حدد **تقرير حول التطبيقات المثبتة**.
4. حدد **خصائص** من قائمة السياق في التقرير.

   الخصائص: تفتح نافذة **تقرير حول التطبيقات المثبتة**.
5. في قسم **التسلسل الهرمي لخوادم الإدارة**، حدد خانة الاختيار **تضمين بيانات من خوادم إدارة ثانوية وافتراضية**.
6. انقر على**موافق**.

سيتم تضمين معلومات من خوادم الإدارة الثانوية والظاهرية في **تقرير حول التطبيقات المثبتة**.

تغيير وقت بدء تخزين البرامج

يقوم Kaspersky Security Center بتسجيل مخزون جميع البرامج المثبتة على الأجهزة العميلة المُدارة التي تعمل بنظام Windows.

يقوم عميل الشبكة بإعداد قائمة بالتطبيقات المثبتة على جهاز، ثم يرسل هذه القائمة إلى خادم الإدارة. يتلقى عميل الشبكة تلقائيًا معلومات حول التطبيقات المثبتة من سجل Windows.

لحفظ موارد الجهاز، سيبدأ عميل الشبكة بشكل افتراضي في تلقي معلومات حول التطبيقات المثبتة بعد مرور 10 دقائق بعد بدء خدمة عميل الشبكة.

لتغيير وقت بدء مخزون البرنامج، الذي ينقضي بعد تشغيل خدمة عميل الشبكة على جهاز:

1. افتح سجل النظام الخاص بالجهاز المثبت عليه عميل الشبكة (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** > تشغيل).
2. انتقل إلى الخلية التالية:
   - لأنظمة 32 بت:

     NagentFlags\1.0.0.0\1103\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE
   - لأنظمة 64 بت:

     ıtFlags\1.0.0.0\1103\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE
3. للمفتاح KLINV_INV_COLLECTOR_START_DELAY_SEC، حدد القيمة المطلوبة بالثواني.

   القيمة الافتراضية هي 600 ثانية.
4. إعادة تشغيل خدمة عميل الشبكة.

تم تغيير وقت بدء مخزون البرنامج الذي ينقضي بعد تشغيل خدمة عميل الشبكة.

حول إدارة مفتاح الترخيص لتطبيقات الطرف الثالث

يسمح لك Kaspersky Security Center بتتبع استخدام مفتاح ترخيص تطبيقات الطرف الثالث المثبتة على الأجهزة المدارة. يتم أخذ قائمة التطبيقات التي يمكنك تتبع استخدام مفتاح الترخيص لها من سجل التطبيقات. لكل مفتاح ترخيص، يمكنك تحديد انتهاك القيود التالية وتعقبها:

- عدد الأجهزة التي يمكن تثبيت التطبيق الذي يستخدم مفتاح الترخيص هذا عليها
- تاريخ انتهاء صلاحية مفتاح الترخيص

لا يتحقق Kaspersky Security Center مما إذا كنت تحدد مفتاح ترخيص حقيقيًا أم لا. يمكنك فقط تتبع القيود التي تحددها. في حالة انتهاك أحد القيود التي تفرضها على مفتاح الترخيص، وخادم الإدارة مسجل كحدث إعلامي أو تحذيري أو فشل وظيفي.

ترتبط مفاتيح الترخيص بمجموعات التطبيقات. مجموعة التطبيقات هي مجموعة من تطبيقات الطرف الثالث التي تجمعها على أساس معيار واحد أو عدة معايير. يمكنك تحديد التطبيقات حسب اسم التطبيق وإصداره والبائع والعلامة. يتم إضافة طلب إلى المجموعة إذا تم استيفاء معيار واحد على الأقل. لكل مجموعة تطبيقات، يمكنك ربط عدة مفاتيح ترخيص ولكن يمكنك ربط كل مفتاح ترخيص بمجموعة تطبيقات واحدة فقط.

هناك أداة أخرى يمكنك استخدامها لتتبع استخدام مفتاح الترخيص وهي تقرير حول حالة مجموعات التطبيقات المرخصة. يوفر هذا التقرير معلومات بشأن الحالة الحالية لمجموعات التطبيقات المرخصة، بما في ذلك:

- عدد عمليات تثبيت مفاتيح الترخيص في كل مجموعة تطبيقات
- عدد مفاتيح الترخيص المستخدمة ومفاتيح الترخيص الشاغرة
- تفاصيل التطبيقات المثبتة على الأجهزة المُدارة

تقع أدوات إدارة مفتاح الترخيص لتطبيقات الطرف الثالث في المجلد الفرعي **استخدام تراخيص الجهات الخارجية (خيارات متقدمة ← إدارة التطبيق ← استخدام تراخيص الجهات الخارجية)**. في هذا المجلد الفرعي، يمكنك إنشاء مجموعات التطبيقات وإضافة مفاتيح الترخيص وإنشاء تقرير حول الحالات الموجودة في مجموعات التطبيقات المرخصة.

لا تتوفر أدوات إدارة مفتاح الترخيص لتطبيقات الجهات الخارجية إلا إذا قمت بتمكين خيار إدارة الثغرات الأمنية والتصحيحات في النافذة **Configure interface**.

إنشاء مجموعات التطبيقات المرخصة

لإنشاء مجموعة تطبيقات مرخصة:

1. في مجلد **خيارات متقدمة ← إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **استخدام تراخيص الجهات الخارجية**.
2. انقر على الزر **إضافة مجموعة تطبيقات مرخصة** لتشغيل معالج إضافة مجموعة تطبيقات مرخصة.

   يتم بدء معالج إضافة مجموعة تطبيقات مرخصة.
3. في خطوة **تفاصيل مجموعة التطبيقات المرخصة**، حدد التطبيقات التي تريد تضمينها في مجموعة التطبيقات:

   - **اسم مجموعة التطبيقات المرخصة**
   - **تتبع القيود المنتهكة**

   في حالة انتهاك أحد القيود التي تفرضها على مفتاح ترخيص مجموعة التطبيقات، يسجل خادم الإدارة حدث إعلامي أو تحذيري أو حدث فشل وظيفي:

   - سيتم تجاوز **سيتم تجاوز حد عمليات التثبيت قريبًا (تم استهلاك أكثر من 95%) لأحدى مجموعات التطبيقات المرخصة**
   - حدث تحذيري: **سيتم تجاوز حد عمليات التثبيت لإحدى مجموعات التطبيقات المرخصة قريبًا**
   - حدث الفشل الوظيفي: **تم تجاوز حد عمليات تثبيت إحدى مجموعات التطبيقات المرخصة**

   يتم تسجيل الحدث مرة واحدة فقط، عند استيفاء الشرط المذكور. في المرة القادمة، يمكن تسجيل نفس الحدث فقط عندما يتم إعادة عدد عمليات التثبيت إلى المستوى الطبيعي، ثم يتكرر الحدث مرة أخرى. لا يمكن تسجيل حدث أكثر من مرة في الساعة.

   - **معايير لإضافة التطبيقات المكتشفة إلى مجموعة التطبيقات المرخصة هذه**

   حدد معايير لتحديد التطبيقات التي تريد تضمينها في مجموعة التطبيقات. يمكنك تحديد التطبيقات حسب اسم التطبيق وإصداره والبائع والعلامة. يجب عليك تحديد معيار واحد على الأقل. يتم إضافة طلب إلى المجموعة إذا تم استيفاء معيار واحد على الأقل.

4. في خطوة **إدخال بيانات حول المفاتيح الموجودة**، حدد مفاتيح الترخيص التي تريد تتبعها. حدد خيار **التحكم إذا تم تجاوز حد الترخيص**، ثم قم بإضافة مفاتيح الترخيص:

a. انقر على زر **إضافة**.

b. حدد ملف تعريف السياسة الذي ترغب في إزالته وانقر على زر **موافق**. إذا لم يكن مفتاح الترخيص المطلوب مدرجًا، فانقر على زر **إضافة**، ثم حدد خصائص مفتاح الترخيص.

5. في خطوة **إضافة مجموعة تطبيقات مرخصة**، انقر على زر **إنهاء**.

تم إنشاء مجموعة التطبيقات المرخصة وعرضها في المجلد **استخدام تراخيص الجهات الخارجية**.

إدارة مفاتيح الترخيص لمجموعات التطبيقات المرخصة

لإنشاء مفتاح ترخيص لمجموعة تطبيقات مرخصة:

1. في مجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **استخدام تراخيص الجهات الخارجية**.

2. في مساحة العمل الخاصة بمجلد **استخدام تراخيص الجهات الخارجية**، انقر على زر **إدارة المفاتيح المتعلقة بالتطبيقات المرخصة**.
تفتح نافذة **إدارة المفتاح في التطبيقات المرخصة**.

3. في النافذة **إدارة المفتاح في التطبيقات المرخصة**، انقر فوق الزر **إضافة**.
تفتح نافذة **المفاتيح**.

4. في النافذة **المفاتيح**، حدد خصائص مفتاح الترخيص والقيود التي يفرضها مفتاح الترخيص على مجموعة التطبيقات المرخصة.

- **الاسم**. اسم مفتاح الترخيص.
- **التعليق**. ملاحظات حول مفتاح الترخيص المحدد.
- **تقييد**. عدد الأجهزة التي يمكن تثبيت التطبيق الذي يستخدم مفتاح الترخيص هذا عليها.
- **تنتهي صلاحيته في**. تاريخ انتهاء صلاحية مفتاح الترخيص.

يتم عرض مفاتيح الترخيص التي تم إنشاؤها في النافذة **إدارة المفتاح في التطبيقات المرخصة**.

لتطبيق مفتاح ترخيص على مجموعة تطبيقات مرخصة:

1. في مجلد **خيارات متقدمة** ← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **استخدام تراخيص الجهات الخارجية**.

2. في المجلد **استخدام تراخيص الجهات الخارجية**، حدد مجموعة التطبيقات المرخصة التي تريد تطبيق مفتاح ترخيص عليها.

3. حدد **خصائص** من قائمة سياق مجموعة التطبيقات المرخصة.
يؤدي هذا إلى فتح نافذة خصائص مجموعة التطبيقات المرخصة.

4. في نافذة خصائص مجموعة التطبيقات المرخصة، في قسم **المفاتيح**، حدد **التحكم إذا تم تجاوز حد الترخيص**.

5. انقر على زر **إضافة**.
تفتح النافذة **تحديد مفتاح ترخيص**.

6. في نافذة **تحديد مفتاح ترخيص** حدد مفتاح الترخيص الذي تريد تطبيقه على مجموعة التطبيقات المرخصة.

7. انقر فوق **موافق**.

ستطبق القيود المفروضة على مجموعة التطبيقات المرخصة والمحددة في مفتاح الترخيص على مجموعة التطبيقات المرخصة المحددة كذلك.

مخزون الملفات التنفيذية

يمكنك الحصول على قائمة بالملفات التنفيذية المخزنة على الأجهزة المُدارة. لجرد الملفات التنفيذية، يجب أن تقوم بإنشاء مهمة جرد.

ميزة جرد الملفات القابلة للتنفيذ متاحة للتطبيقات التالية:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent والإصدارات الأحدث

لا يمكن أن يتجاوز عدد الملفات التنفيذية التي تم استلامها من جهاز مفرد 150 000 ملف. بالوصول لهذا الحد، لا يمكن أن يتلقى Kaspersky Security Center أي ملفات جديدة.

قبل أن تبدأ، قم بتمكين الإشعارات حول بدء تشغيل التطبيقات في سياسة Kaspersky Endpoint Security وسياسة عميل الشبكة ، حتى تتمكن من نقل البيانات إلى خادم الإدارة.

لتمكين الإخطارات حول بدء تشغيل التطبيقات:

- افتح إعدادات سياسة Kaspersky Endpoint Security وقم بما يلي:

  1. انتقل إلى **الإعدادات العامة** ← **التقارير والتخزين** .

  2. في قسم **نقل البيانات إلى خادم الإدارة** ، حدد خانة الاختيار **حول التطبيقات التي** تم بدء تشغيلها.

  3. احفظ تغييراتك.

- افتح إعدادات نهج عميل الشبكة وقم بما يلي:

  1. انتقل إلى القسم **المستودعات**.

  2. حدد خانة الاختيار **تفاصيل عن التطبيقات التي تم تثبيتها** .

  3. احفظ تغييراتك.

لإنشاء مهمة مخزون للملفات التنفيذية على الأجهزة العميلة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. في مساحة عمل المجلد **المهام**، انقر على الزر **مهمة جديدة**.

سيبدأ معالج المهمة الجديدة.

3. في نافذة **تحديد نوع المهمة** الخاصة بالمعالج، حدد **Kaspersky Endpoint Security** كنوع المهمة، ثم حدد **المستودع** كنوع فرعي للمهمة وانقر على **التالي**.

4. اتبع بقية تعليمات المعالج.

بعد انتهاء المعالج، يتم إنشاء مهمة مخزون لـ Kaspersky Endpoint Security. يتم عرض المهمة التي تم إنشاؤها حديثًا في قائمة المهام في مساحة عمل المجلد **المهام**.

يتم عرض قائمة بالملفات التنفيذية التي تم اكتشافها على الأجهزة أثناء مهمة جرد المخزون، في مساحة عمل المجلد **الملفات التنفيذية**.

أثناء مهمة المخزون، يكتشف التطبيق الملفات التنفيذية ذات التنسيقات التالية: MZ وCOM وPE وNE وSYS وCMD وBAT وPS1 وJS وVBS وREG وMSI وCPL وDLL وJAR وملفات HTML.

عرض معلومات حول الملفات التنفيذية

لعرض قائمة بالملفات التنفيذية التي تم اكتشافها على الأجهزة العميلة,

في مجلد **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **الملفات التنفيذية**.

تعرض مساحة عمل المجلد **الملفات التنفيذية** قائمة بالملفات التنفيذية التي تم تشغيلها على الأجهزة منذ تثبيت نظام التشغيل، أو التي تم اكتشافها أثناء تشغيل مهمة المخزون لتطبيق Kaspersky Endpoint Security for Windows.

لعرض بيانات على الملفات التنفيذية التي تتوافق مع المعايير المحددة، يمكنك استخدام التصفية.

لعرض خصائص ملف تنفيذي,

من قائمة السياق الخاصة بالملف، حدد **خصائص**.

يتم فتح نافذة تحتوي على معلومات حول الملف التنفيذي بجانب قائمة الأجهزة التي تم اكتشاف الملف التنفيذي عليها.

المراقبة وإعداد التقارير

يبين هذا القسم إمكانيات المراقبة وإعداد التقارير في Kaspersky Security Center. تمنحك هذه الإمكانيات نظرة عامة على البنية الأساسية الخاصة بك وحالات الحماية والإحصائيات.

بعد نشر Kaspersky Security Center أو أثناء العملية، يمكنك تكوين مزايا المراقبة وإعداد التقارير لتتناسب مع احتياجاتك بشكل أفضل.

- **إشارات حركة المرور**

تتيح لك وحدة تحكم الإدارة التقييم السريع للحالة الحالية لـ Kaspersky Security Center والأجهزة المدارة عن طريق التحقق من إشارات حركة المرور.

- **الإحصائيات**

يتم عرض إحصائيات حول حالة نظام الحماية والأجهزة المدارة في أجزاء المعلومات التي يمكن تخصيصها.

- **تقارير**

تسمح لك ميزة التقارير بالحصول على معلومات رقمية تفصيلية حول أمان شبكة مؤسستك وحفظ هذه المعلومات إلى أحد الملفات وإرسالها بالبريد الإلكتروني وطباعتها.

- **أحداث**

توفر تحديدات الأحداث عرضًا على الشاشة يتضمن مجموعات الأحداث المُسمَّاة المحددة من قاعدة بيانات خادم الإدارة. يتم تجميع مجموعات الأحداث هذه وفقًا للفئات التالية:

- حسب مستوى الأهمية—**أحداث حرجة**، و**حالات الخلل الوظيفي**، و**تحذيرات**، و**معلومات عن الأحداث**
- حسب الوقت—**الأحداث الأخيرة**
- حسب النوع—**طلبات المستخدم** و**أحداث التدقيق**

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center Web Console.

السيناريو: المراقبة وإعداد التقارير

يعرض هذا القسم سيناريو لتكوين ميزة المراقبة وإعداد التقارير في Kaspersky Security Center.

المتطلبات الأساسية

بعد أن تنشر Kaspersky Security Center في شبكة مؤسسة، يمكنك بدء مراقبته وإنشاء تقارير عن عمله.

المراحل

المراقبة وإعداد التقارير في شبكة مؤسسة تسير في مراحل:

1. **تكوين تبديل حالات الجهاز**

   تعرَّف على الإعدادات التي تحدد تخصيص حالات الجهاز اعتمادًا على الظروف. يمكنك عن طريق تغيير هذه الإعدادات تغيير عدد الأحداث ذات مستويات الأهمية حرج أو تحذيري.

   عند تكوين تبديل حالات الجهاز، تأكد أن الإعدادات الجديدة لا تخالف سياسات أمان المعلومات لمؤسستك. وأنك تقدر على التفاعل مع أحداث الأمان المهمة في شبكة مؤسستك في الوقت المناسب.

2. **تكوين إخطارات الأحداث التي تحدث على أجهزة العميل:**

   قم بتكوين الإخطار (عن طريق البريد الإلكتروني أو الرسائل النصية القصيرة أو عن طريق تشغيل ملف تنفيذي) للأحداث على أجهزة العميل وفق احتياجات مؤسستك.

3. **تغيير استجابة شبكة أمانك لحدث انتشار الفيروسات.**

   لضبط استجابة الشبكة للأحداث الجديدة، يمكنك تغيير الحدود المحددة في خصائص خادم الإدارة. يمكنك كذلك إنشاء سياسة أكثر صرامة يتم تفعيلها أو إنشاء مهمة سيتم تشغيلها عند وقوع هذا الحدث.

4. **إدارة الإحصائيات**

   قم بتكوين عرض الإحصائيات وفق احتياجات مؤسستك.

5. **مراجعة حالة الأمان لشبكة مؤسستك**

لمراجعة الحالة الأمان لشبكة مؤسستك، يمكنك فعل أي مما يلي:

- في مساحة عمل عقدة **خادم الإدارة**، في تبويب **إحصائيات**، افتح تبويب (صفحة) المستوى الثاني **حالة الحماية** وراجع جزء المعلومات **حالة الحماية في الوقت الحقيقي**
- قم بإنشاء ومراجعة **تقرير عن حالة الحماية**
- قم بإنشاء ومراجعة **تقرير الأخطاء**

6 **تحديد مواقع أجهزة العميل غير المحمية**

لتحديد مواقع أجهزة العميل غير المحمية، اذهب إلى مساحة عمل عقدة **خادم الإدارة**، في تبويب **إحصائيات**، افتح تبويب (صفحة) المستوى الثاني **حالة الحماية** وراجع جزء المعلومات **محفوظات اكتشاف أجهزة جديدة متصلة بالشبكة** يمكنك كذلك إنشاء ومراجعة **تقرير نشر الحماية**.

7 **التحقق من حماية أجهزة العميل**

للتحقق من حماية أجهزة العميل، اذهب إلى مساحة عمل عقدة **خادم الإدارة**، في تبويب **إحصائيات**، افتح تبويب (صفحة) المستوى الثاني **النشر** أو **إحصائيات التهديد** وراجع لوحات المعلومات ذات الصلة. يمكنك كذلك بدء ومراجعة تحديد الحدث **أحداث حرجة**.

8 **تقييم وتقييد تحميل الحدث على قاعدة البيانات**

يتم نقل المعلومات حول الأحداث التي تحدث أثناء تشغيل التطبيقات المُدارة من جهاز عميل ويتم تسجيلها بقاعدة بيانات خادم الإدارة. لتقييد التحميل على خادم الإدارة، قم بتقييم وتقليل أقصى عدد من الأحداث التي يمكن تخزينها في قاعدة البيانات.

لتقييم حمل الحدث على قاعدة البيانات، قم بحساب مساحة قاعدة البيانات. يمكنك كذلك تقييد العدد الأقصى من الأحداث لتجنب تجاوز سعة قاعدة البيانات.

9 **مراجعة معلومات الترخيص**

لمراجعة معلومات الترخيص، اذهب إلى مساحة عمل عقدة **خادم الإدارة**، في تبويب **إحصائيات**، افتح تبويب (صفحة) المستوى الثاني **النشر** وراجع جزء المعلومات **استخدام المفتاح** يمكنك كذلك إنشاء ومراجعة **تقرير استخدام المفاتيح**.

النتائج

عند إكمال السيناريو، سيتم إعلامك بحماية شبكة مؤسستك وبالتالي يمكنك التخطيط لإجراءات للمزيد من الحماية.

مراقبة إشارات المرور والأحداث المسجلة في وحدة تحكم الإدارة

تتيح لك وحدة تحكم الإدارة التقييم السريع للحالة الحالية لـ Kaspersky Security Center والأجهزة المدارة عن طريق التحقق من إشارات حركة المرور. يتم عرض إشارات حركة المرور في مساحة العمل لعقدة **خادم الإدارة**، في علامة التبويب **المراقبة**. توفر علامة التبويب ستة لوحات معلومات مع إشارات حركة المرور والأحداث المسجلة. إشارة حركة المرور هي شريط عمودي ملون في الجزء الأيسر من اللوحة. تتوافق كل لوحة بها إشارات حركة المرور مع نطاق وظيفي محدد لـ Kaspersky Security Center (انظر الجدول أدناه).

النطاقات المغطاة بإشارات حركة المرور في وحدة تحكم الإدارة

اسم اللوحة	نطاق إشارة المرور
النشر	تثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة في شبكة مؤسسة
نظام الإدارة	بنية مجموعات الإدارة. فحص الشبكة. قواعد نقل الجهاز
إعدادات الحماية	وظائف تطبيق الأمان: حالة الحماية، فحص البرامج الضارة
تحديث	التحديثات والتصحيحات
المراقبة	حالة الحماية
خادم الإدارة	مزايا وخصائص خادم الإدارة

قد تكون كل إشارة حركة مرور أي من هذه الألوان الخمسة (انظر الجدول الموجود أدناه). يعتمد لون إشارة حركة المرور على الحالة الحالية لـ Kaspersky Security Center وعلى الأحداث التي تم الدخول إليها.

الرموز اللونية لإشارات حركة المرور

الحالة	لون إشارة حركة المرور	معنى لون إشارة حركة المرور
معلوماتي	أخضر	تدخل المسؤول غير مطلوب.
تحذير	أصفر	تدخل المسؤول مطلوب.
حرج	أحمر	تمت مصادفة مشكلات خطيرة. تدخل المسؤول مطلوب لحلها.
معلوماتي	أزرق فاتح	الأحداث التي تم الدخول إليها لا تتعلق بالتهديدات المحتملة أو الفعلية للأمان الأجهزة المدارة.
معلوماتي	رمادي	تفاصيل الأحداث غير متوفرة أو لم يتم استردادها بعد.

هدف المسؤول هو الإبقاء على إشارات حركة مرور في جميع أجزاء المعلومات على علامة التبويب **المراقبة** باللون الأخضر.

تعرض لوحات المعلومات أيضًا الأحداث المسجلة التي تؤثر على إشارات حركة المرور وحالة Kaspersky Security Center (انظر الجدول أدناه).

الاسم والوصف وألوان إشارات حرمة المرور للأحداث المسجلة

لون إشارة حركة المرور	اسم العرض لنوع الحدث	نوع الحدث	الوصف
أحمر	**انتهت صلاحية الترخيص على 1% جهاز (أجهزة)**	IDS_AK_STATUS_LIC_EXPAIRED	تقع الأحداث من هذا النوع عندما يقترب انتهاء صلاحية الترخيص التجاري. يتحقق Kaspersky Security Center مرة واحدة يوميًا مما إذا كانت صلاحية الترخيص قد انتهت على الأجهزة. عند انتهاء صلاحية الترخيص التجاري، يوفر Kaspersky Security Center الوظائف الأساسية فقط. لمتابعة استخدام Kaspersky Security Center، يرجى تجديد ترخيصك التجاري.
أحمر	**تطبيق الأمان لا يعمل على: 1% جهاز (أجهزة)**	IDS_AK_STATUS_AV_NOT_RUNNING	تقع الأحداث من هذا النوع عندما لا يكون تطبيق الأمان المُثبت على الجهاز قيد التشغيل. تأكد من تشغيل Kaspersky Endpoint Security على الجهاز.
أحمر	**الحماية مُعطَّلة على: 1% جهاز (أجهزة)**	IDS_AK_STATUS_RTP_NOT_RUNNING	تقع الأحداث من هذا النوع عندما يتم تعطيل تطبيق الأمان على الجهاز لفترة أطول من الفترة الزمنية المحددة. تحقق من الحالة الحالية للحماية في الوقت الحقيقي على الجهاز وتأكد من تمكين جميع مكونات الحماية التي تحتاجها.
أحمر	**تم اكتشاف ثغرات أمنية في البرنامج على الأجهزة**	IDS_AK_STATUS_VULNERABILITIES_FOUND	تقع الأحداث من هذا النوع عندما تكتشف مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة ثغرات أمنية بمستوى الخطورة المحدد في التطبيقات المُثبتة على الجهاز. تحقق من قائمة التحديثات المتوفرة في المجلد الفرعي **Software updates** المضمن في المجلد **Application management**. يحتوي هذا المجلد على قائمة بالتحديثات لتطبيقات Microsoft ومنتجات موردي البرامج الآخرين المستردة بواسطة خادم الإدارة، التي يمكن توزيعها إلى الأجهزة. بعد عرض معلومات عن التحديثات المتوفرة، قم بتثبيتها على الجهاز.
أحمر	**تم تسجيل الأحداث الحرجة على خادم الإدارة**	IDS_AK_STATUS_EVENTS_OCCURED	تقع الأحداث من هذا النوع عند اكتشاف أحداث حرجة لخادم الإدارة. تحقق من قائمة الأحداث المخزنة على خادم الإدارة، ثم قم بإصلاح الأحداث الحرجة واحدًا تلو الآخر.
أحمر	**تم تسجيل الأخطاء في الأحداث الموجودة على خادم الإدارة**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	تقع الأحداث من هذا النوع عند تسجيل أخطاء غير متوقعة على جانب خادم الإدارة. تحقق من قائمة الأحداث المخزنة على خادم الإدارة، ثم أصلح الأخطاء واحدًا تلو الآخر.
أحمر	**فقد الاتصال بعدد 1% جهاز (أجهزة)**	IDS_AK_STATUS_ADM_LOST_CONTROL1	تقع الأحداث من هذا النوع عند فقدان الاتصال بين خادم الإدارة والجهاز. اعرض قائمة الأجهزة غير المتصلة وحاول إعادة توصيلها.
أحمر	**لم يتصل 1% جهاز (أجهزة) بخادم الإدارة منذ وقت طويل**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	تقع الأحداث من هذا النوع عندما لا يكون الجهاز متصلاً بخادم الإدارة خلال الفترة الزمنية المحددة، بسبب إيقاف تشغيل الجهاز. تأكد من تشغيل الجهاز وتشغيل عميل الشبكة.
أحمر	**هناك جهاز (أجهزة) 1% حالته تختلف عن "موافق"**	IDS_AK_STATUS_HOST_NOT_OK	تقع الأحداث من هذا النوع عندما تتغير الحالة جيدة للجهاز المتصل بخادم الإدارة إلى حرجة" أو تحذير. يمكنك استكشاف المشكلة وإصلاحها باستخدام الأداة المساعدة للتشخيص عن بُعد في Kaspersky Security Center.

لون إشارة حركة المرور	اسم العرض لنوع الحدث	نوع الحدث	الوصف
أحمر	**قواعد البيانات قديمة على: 1% جهاز (أجهزة)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	تقع الأحداث من هذا النوع عندما لا يتم تحديث قواعد بيانات مكافحة الفيروسات على الجهاز خلال الفترة الزمنية المحددة. اتبع التعليمات لتحديث قواعد بيانات Kaspersky.
أحمر	**الجهاز (الأجهزة) التي لم يتم فحص تحديثات Windows Update عليه منذ وقت طويل: 1%**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	تقع الأحداث من هذا النوع عندما لا يتم تشغيل مهمة مزامنة Windows Update خلال الفترة الزمنية المحددة. اتبع التعليمات لمزامنة التحديثات من Windows Update مع خادم الإدارة.
أحمر	**يلزم تثبيت 1% مكون إضافي (مكونات إضافية) ل Kaspersky Security Center**	IDS_AK_STATUS_PLUGINS_REQUIRED2	تقع الأحداث من هذا النوع عندما تحتاج إلى تثبيت مكونات إضافية لتطبيقات Kaspersky. يرجى تنزيل وتثبيت المكونات الإضافية للإدارة المطلوبة لتطبيق Kaspersky من صفحة ويب الدعم الفني من Kaspersky .

التعامل مع التقارير والإحصائيات والإخطارات

يوفر لك هذا القسم معلومات حول كيفية العمل مع التقارير والإحصائيات ومجموعات الأحداث والأجهزة المحددة في Kaspersky Security Center، بالإضافة إلى كيفية تكوين إخطارات خادم الإدارة.

التعامل مع التقارير

تحتوي التقارير في Kaspersky Security Center على معلومات حول حالة الأجهزة المدارة. يتم إنشاء التقارير بناء على المعلومات المخزنة على خادم الإدارة. يمكنك إنشاء تقارير للأنواع التالية من الكائنات:

- لتحديدات الأجهزة التي تم إنشاؤها وفقًا لإعدادات محددة.
- لمجموعات الإدارة.
- لأجهزة محددة من مجموعات إدارة مختلفة.
- لكل الأجهزة على الشبكة (في تقرير النشر).

يحتوي التطبيق على مجموعة من قوالب التقارير القياسية. كذلك من الممكن إنشاء قوالب تقارير مخصصة. يتم عرض التقارير في نافذة التطبيق الرئيسية، في مجلد **خادم الإدارة** في شجرة وحدة التحكم.

إنشاء قالب تقرير

لإنشاء قالب تقرير:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .
3. انقر على زر **قالب التقارير الجديد**.

يبدأ معالج قالب التقرير الجديد. اتبع إرشادات المعالج.

بعد انتهاء المعالج من العملية، تتم إضافة قالب التقرير الذي تم إنشاؤه حديثًا إلى مجلد **خادم الإدارة** المحدد بشجرة وحدة التحكم. ويمكنك استخدام هذا القالب لإنشاء التقارير وعرضها.

عرض وتحرير خصائص قالب التقرير

يمكنك عرض وتحرير الخصائص الأساسية لقالب تقرير، على سبيل المثال، اسم قالب التقرير أو الحقول المعروضة في التقرير.

لعرض وتحرير خصائص قالب التقرير:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .

3. في قائمة قوالب التقرير، حدد قالب التقرير المطلوب.

4. من قائمة سياق قالب التقرير المحدد، حدد **خصائص**.

   كخيار بديل، يمكنك أولاً إنشاء التقرير، ثم النقر فوق إما الزر **فتح خصائص قالب التقرير** أو الزر **تكوين أعمدة التقرير**.

5. في النافذة التي تفتح، قم بتحرير خصائص قالب التقرير. قد تحتوي خصائص كل تقرير على بعض الأقسام الموضحة أدناه فقط.

- القسم **عام**:

  - اسم قالب التقرير

  - **أقصى عدد من الإدخالات المراد عرضها**

    إذا تم تمكين هذا الخيار، فإن عدد الإدخالات المعروضة في الجدول مع بيانات التقرير التفصيلية لا يزيد عن القيمة المحددة.

    يتم أولاً فرز إدخالات التقرير وفقًا للقواعد المحددة في القسم **الحقول** ← **حقول التفاصيل** في خصائص قالب التقرير، وبعد ذلك يتم الاحتفاظ فقط بالإدخالات الأولى الناتجة. يعرض عنوان الجدول المزود ببيانات تقرير مفصلة العدد المعروض من الإدخالات وإجمالي عدد الإدخالات المتاح الذي يطابق إعدادات قالب التقرير الآخر.

    إذا تم تعطيل هذا الخيار، فإن الجدول المزود ببيانات التقرير التفصيلية يعرض جميع الإدخالات المتوفرة. لا نوصيك بتعطيل هذا الخيار. إن تقليل عدد إدخالات التقرير المعروضة يقلل من الحمل على نظام إدارة قواعد البيانات (DBMS) ويقلل الوقت اللازم لإنشاء وتصدير التقرير. تحتوي بعض التقارير على عدد كبير جدًا من الإدخالات. إذا كانت هذه هي الحالة، فقد تجد صعوبة في قراءتها وتحليلها جميعًا. وقد تنفذ مساحة الذاكرة في جهازك أيضًا أثناء إنشاء مثل هذا التقرير، وبالتالي لن تتمكن من عرض التقرير.

    يتم تمكين هذا الخيار افتراضيًا. القيمة الافتراضية هي 1000.

  - **طباعة الإصدار**

    يتم تحسين التقرير الناتج من أجل طباعته: تتم إضافة أحرف المسافة بين بعض القيم لتحسين الرؤية.

    يتم تمكين هذا الخيار افتراضيًا.

- قسم **الحقول**.

  حدد الحقول التي سيتم عرضها في التقرير، وترتيب هذه الحقول، وتكوين ما إذا كان يجب فرز وتصفية المعلومات الموجودة في التقرير بحسب كل حقل من الحقول.

- قسم **الفاصل الزمني**.

  تعديل فترة التقرير. القيم المتاحة هي كما يلي:

  - بين تاريخين محددين

  - من التاريخ المحدد إلى تاريخ إنشاء التقرير

  - من تاريخ إنشاء التقرير، ناقص العدد المحدد من الأيام، إلى تاريخ إنشاء التقرير

- قسم **مجموعة**، أو **تحديد جهاز**، أو **أجهزة**.

قم بتغيير مجموعة الأجهزة العميلة التي يتم إنشاء التقرير من أجلها. قد يكون واحد فقط من هذه الأقسام موجودًا، وفقًا للإعدادات المحددة أثناء إنشاء قالب التقرير.

- قسم **الإعدادات**.

قم بتغيير إعدادات التقرير. تعتمد مجموعة الإعدادات الدقيقة على التقرير المحدد.

- قسم **الأمان**. **توريث الإعدادات من خادم الإدارة**

إذا تم تمكين هذا الخيار، فإنه يتم توريث إعدادات الأمان الخاصة بالتقرير من خادم الإدارة.

إذا تم تعطيل هذا الخيار، فبإمكانك تكوين إعدادات الأمان للتقرير. يمكنك تعيين دور لمستخدم أو مجموعة من المستخدمين أو تعيين أذونات لمستخدم أو مجموعة من المستخدمين، كما هو مطبق على التقرير.

يتم تمكين هذا الخيار افتراضيًا.

يتوفر القسم **الأمان** إذا تم تحديد خانة الاختيار **عرض أقسام إعدادات الأمان** في نافذة إعدادات الواجهة.

- قسم **التسلسل الهرمي لخوادم الإدارة**.

- **تضمين بيانات من خوادم إدارة ثانوية وافتراضية**

إذا تم تمكين هذا الخيار، فإن التقرير يقوم بتضمين معلومات من خوادم الإدارة الثانوية والظاهرية التابعة الخاضعة لخادم الإدارة الذي يتم إنشاء قالب التقرير له.

قم بتعطيل هذا الخيار إذا كنت ترغب في عرض البيانات فقط من خادم الإدارة الحالي.

يتم تمكين هذا الخيار افتراضيًا.

- **أعلى إلى مستوى التداخل**

يتضمن التقرير بيانات من خوادم الإدارة الثانوية والظاهرية الموجودة ضمن خادم الإدارة الحالي على مستوى تداخل أقل من أو يساوي القيمة المحددة.

القيمة الافتراضية هي 1. قد ترغب في تغيير هذه القيمة إذا كان عليك استعادة المعلومات من خوادم الإدارة الثانوية الموجودة في المستويات الأدنى في الشجرة.

- **فاصل انتظار البيانات (بالدقائق)**

قبل إنشاء التقرير، ينتظر خادم الإدارة الذي يتم إنشاء قالب التقرير له البيانات من خوادم الإدارة الثانوية خلال العدد المحدد من الدقائق. إذا لم يتم تلقي أي بيانات من خادم الإدارة الثانوي في نهاية هذه الفترة، فسيتم تشغيل التقرير على أي حال. بدلاً من البيانات الفعلية، يوضح التقرير البيانات المأخوذة من ذاكرة التخزين المؤقت (إذا تم تمكين الخيار **بيانات ذاكرة التخزين المؤقت من خوادم الإدارة الثانوية**)، أو **N/A** (غير متوفر) خلافًا ذلك.

القيمة الافتراضية هي 5 (ثوانٍ).

- **بيانات ذاكرة التخزين المؤقت من خوادم الإدارة الثانوية**

تقوم خوادم الإدارة الثانوية بنقل البيانات إلى خادم الإدارة الذي يتم من أجله إنشاء قالب التقرير بانتظام. وهناك يتم تخزين البيانات المنقولة في ذاكرة التخزين المؤقت.

إذا لم يتمكن خادم الإدارة الحالي من تلقي البيانات من خادم الإدارة الثانوي أثناء إنشاء التقرير، فسيعرض التقرير البيانات المأخوذة من ذاكرة التخزين المؤقت. يتم أيضًا عرض التاريخ الذي تم فيه نقل البيانات إلى ذاكرة التخزين المؤقت.

يتيح لك تمكين هذا الخيار عرض المعلومات من خوادم الإدارة الثانوية حتى إذا تعذر استرجاع البيانات الحديثة. ومع ذلك، يمكن أن تكون البيانات المعروضة قديمة.

يتم تعطيل هذا الخيار افتراضيًا.

- **تكرار تحديث التخزين المؤقت (بالساعات)**

تقوم خوادم الإدارة الثانوية بنقل البيانات إلى خادم الإدارة الذي يتم من أجله إنشاء قالب التقرير على فترات منتظمة. يمكنك تحديد هذه الفترة بالساعات. إذا حددت 0 ساعات، لا يتم نقل البيانات إلا عند إنشاء التقرير.

القيمة الافتراضية هي 0.

- **نقل معلومات تفصيلية من خوادم الإدارة الثانوية**

في التقرير الذي يتم إنشاؤه، يشتمل الجدول المزود ببيانات التقرير التفصيلية على بيانات من خوادم الإدارة الثانوية لخادم الإدارة الذي يتم من أجله إنشاء قالب التقرير.

يؤدي تمكين هذا الخيار إلى إبطاء إنشاء التقرير وزيادة حركة المرور بين خوادم الإدارة. ومع ذلك، يمكنك عرض جميع البيانات في تقرير واحد.

بدلاً من تمكين هذا الخيار، قد تحتاج إلى تحليل بيانات التقرير التفصيلية للكشف عن خادم إدارة تابع معيب، ثم إنشاء نفس التقرير فقط لخادم الإدارة المعيب هذا.

يتم تعطيل هذا الخيار افتراضيًا.

تنسيق عامل التصفية الموسع في قوالب التقرير

في Kaspersky Security Center 15.1، يمكنك تطبيق تنسيق عامل التصفية الموسع في قوالب التقرير. يوفر تنسيق عامل التصفية الموسع مزيدًا من المرونة مقارنةً بالتنسيق الافتراضي. يمكنك إنشاء شروط تصفية معقدة باستخدام مجموعة من عوامل التصفية، والتي سيتم تطبيقها على التقرير حول طريق العامل المنطقي OR (أو) أثناء إنشاء التقرير، كما هو موضح أدناه:

عامل التصفية [1] (الحقل [1] والحقل [2] ... والحقل [n]) أو عامل التصفية [2] (الحقل [1] والحقل [2]... والحقل [n]) أو ... عامل التصفية [n] (الحقل [1] والحقل [2] ... والحقل [n])

بالإضافة إلى ذلك، باستخدام تنسيق عامل التصفية الموسع، يمكنك تعيين قيمة الفاصل الزمني في تنسيق زمني نسبي (على سبيل المثال باستخدام شرط "للأيام N الأخيرة") لحقول معينة في عامل تصفية. يعتمد مدى التوفر وشروط تعيين مدة الفاصل الزمني على نوع قالب التقرير.

تحويل عامل التصفية إلى التنسيق الممتد

لا يكون تنسيق عامل التصفية الموسع لقوالب التقرير مدعومًا إلا على Kaspersky Security Center 12 والإصدارات الأحدث. بعد تحويل عامل التصفية الافتراضي إلى التنسيق الموسع، يصبح قالب التقرير غير متوافق مع خوادم الإدارة في شبكتك التي تم تثبيت الإصدارات السابقة من Kaspersky Security Center عليها. لن يتم تلقي معلومات من خوادم الإدارة هذه حول التقرير.

لتحويل عامل التصفية الافتراضي لقالب التقرير إلى التنسيق الموسع:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .
3. في قائمة قوالب التقرير، حدد قالب التقرير المطلوب.
4. من قائمة سياق قالب التقرير المحدد، حدد **خصائص**.
5. في نافذة الخصائص التي تفتح، حدد القسم **الحقول**.
6. في علامة التبويب **حقول التفاصيل** انقر فوق الرابط **تحويل عامل التصفية**.
7. في النافذة التي تفتح، انقر فوق الزر **موافق**.

لا يمكن التراجع عن التحويل إلى تنسيق عامل التصفية الموسع لقالب التقرير الذي يتم تطبيقه عليه. إذا قمت بالنقر فوق الرابط **تحويل عامل التصفية** عن طريق الخطأ، فيمكنك إلغاء التغييرات بالنقر فوق الزر **إلغاء** في النافذة خصائص قالب التقرير.

8. لتطبيق التغييرات، أغلق النافذة خصائص قالب التقرير بالنقر فوق الزر **موافق**.

عند فتح النافذة خصائص قالب التقرير مرة أخرى، يتم عرض القسم **عوامل تصفية** المتاح حديثًا. في هذا القسم، يمكنك تكوين عامل التصفية الموسع.

تكوين عامل التصفية الموسع

لتكوين عامل التصفية الموسع في خصائص قالب التقرير:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .

3. في قائمة قوالب التقرير، حدد قالب التقرير الذي تم تحويله مسبقًا إلى تنسيق عامل التصفية الموسع.

4. من قائمة سياق قالب التقرير المحدد، حدد **خصائص**.

5. في نافذة الخصائص التي تفتح، حدد قسم **عوامل تصفية** الفرعي.

   لا يتم عرض القسم **عوامل تصفية** إذا لم يتم تحويل قالب التقرير من قبل إلى تنسيق عامل تصفية موسع.

   في القسم **عوامل تصفية** الخاص بالنافذة خصائص قالب التقرير، يمكنك مراجعة وتعديل قائمة عوامل التصفية المطبقة على التقرير. يكون لكل عامل تصفية في القائمة اسمًا فريدًا وهو يمثل مجموعة من عوامل التصفية للحقول المقابلة في التقرير.

6. افتح نافذة إعدادات عامل التصفية بإحدى الطرق التالية:

   - لإنشاء عامل تصفية جديد، انقر فوق الزر **إضافة**.
   - لتعديل عامل التصفية الحالي، حدد عامل التصفية المطلوب وانقر فوق الزر **تعديل**.

7. في النافذة التي تفتح، اختر قيم الحقول المطلوبة لعامل التصفية وحددها.

8. انقر فوق الزر **موافق** لحفظ التغييرات وإغلاق النافذة.

   إذا كنت تقوم بإنشاء عامل تصفية جديد، فيجب تحديد اسم عامل التصفية في الحقل **اسم عامل التصفية** قبل النقر فوق الزر **موافق**.

9. أغلق النافذة خصائص قالب التقرير بالنقر فوق الزر **موافق**.

   يتم تكوين عامل التصفية الموسع في قالب التقرير. يمكنك الآن إنشاء تقارير باستخدام قالب التقرير هذا.

إنشاء تقرير وعرضه

لإنشاء تقرير وعرضه:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .

3. في قائمة قوالب التقارير، انقر نقرًا مزدوجًا فوق قالب التقرير الذي تحتاجه.

   يتم عرض تقرير للقالب المحدد.

ويعرض التقرير البيانات التالية:

- اسم ونوع التقرير، ووصف مختصر له، وفترة التقرير بالإضافة إلى معلومات حول مجموعة الأجهزة التي تم إنشاء التقرير لها.
- مخطط رسم بياني يوضح بيانات التقرير الأكثر تمثيلًا.
- جدول موحد يحتوي على مؤشرات التقرير المعدودة.
- جدول يحتوي على بيانات التقرير التفصيلية.

حفظ تقرير

لحفظ تقرير تم إنشاؤه:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .
3. في قائمة قوالب التقرير، حدد قالب التقرير الذي تحتاجه.
4. من قائمة سياق قالب التقرير المحدد، حدد **حفظ**.

   يبدأ تشغيل معالج حفظ التقرير. اتبع إرشادات المعالج.

بعد انتهاء المعالج، يفتح المجلد الذي حفظت فيه ملف التقرير.

عند حفظ تقرير كملف XLS، يتم حفظ جميع الصور ذات الصلة، مثل الشعار ومخطط البيانات، كملفات منفصلة.

إنشاء مهمة تسليم تقرير

يمكن إرسال التقارير عبر البريد الإلكتروني. تسليم التقارير يتم تنفيذه في Kaspersky Security Center باستخدام مهمة تسليم التقرير.

لإنشاء مهمة تسليم لتقرير منفرد:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .
3. في قائمة قوالب التقرير، حدد قالب التقرير الذي تحتاجه.
4. من قائمة سياق قالب التقرير المحدد، حدد **تسليم التقارير**.

   يبدأ معالج إنشاء مهمة تسليم التقرير. اتبع إرشادات المعالج.

لإنشاء مهمة تسليم للعديد من التقارير:

1. في شجرة وحدة التحكم، ضمن العقدة التي تحمل اسم خادم الإدارة المطلوب، حدد المجلد **المهام**.
2. في مساحة عمل المجلد **المهام**، انقر على زر **إنشاء مهمة**.

   سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

   يتم عرض المهمة تسليم التقرير التي تم إنشاؤها حديثًا في المجلد **المهام** في شجرة وحدة التحكم.

يتم إنشاء مهمة تسليم التقارير تلقائيًا إذا تم تحديد إعدادات البريد الإلكتروني أثناء تثبيت Kaspersky Security Center.

الخطوة 1. تحديد نوع المهمة

في النافذة **تحديد نوع المهمة**، في قائمة المهام حدد **تسليم التقارير** كنوع المهمة.

انقر فوق **التالي** للمتابعة إلى الخطوة التالية.

الخطوة 2. تحديد نوع التقرير

في النافذة **حدد نوع التقرير**، في قائمة قوالب إنشاء المهام، حدد نوع التقرير.

انقر فوق **التالي** للمتابعة إلى الخطوة التالية.

الخطوة 3. إجراءات على التقرير

في نافذة **الإجراء الذي يتخذ على التقارير**، حدد الإعدادات التالية:

- **إرسال التقارير عبر البريد الإلكتروني**

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بإرسال التقارير التي تم إنشاؤها عبر البريد الإلكتروني.

يمكنك تكوين التقرير الذي يتم إرساله بالبريد الإلكتروني بالنقر فوق الارتباط **إعدادات إخطار البريد الإلكتروني**. يتوفر الرابط في حال تمكين هذا الخيار.

إذا تم تعطيل هذا الخيار، فسيقوم التطبيق بحفظ التقارير في المجلد المحدد لكي يتم تخزينها.

يتم تعطيل هذا الخيار افتراضيًا.

- **حفظ التقارير إلى مجلد مشترك**

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بحفظ التقارير في المجلد المحدد في الحقل أسفل خانة الاختيار. لحفظ التقارير على مجلد مشترك، حدد مسار UNC إلى المجلد. في هذه الحالة، يتعين عليك تحديد حساب المستخدم وكلمة المرور للوصول إلى هذا المجلد في النافذة **تحديد حساب لتشغيل المهمة**.

إذا تم تعطيل هذا الخيار، فلن يقوم التطبيق بحفظ التقارير في المجلد وبدلاً من ذلك سيقوم بإرسالها عبر البريد الإلكتروني.

يتم تعطيل هذا الخيار افتراضيًا.

- **استبدال التقارير القديمة من النوع الواحد**

إذا تم تمكين هذا الخيار، فسيقوم كل ملف تقرير جديد عند بدء تشغيل كل مهمة بالكتابة فوق الملف الذي تم حفظه في مجلد التقارير عند بدء تشغيل المهمة السابقة.

إذا تم تعطيل هذا الخيار، فلن تتم الكتابة فوق ملفات التقرير. يتم تخزين ملف تقرير جديد في مجلد التقارير عند تشغيل كل مهمة.

تتوفر خانة الاختيار، إذا تم تحديد **حفظ التقرير إلى مجلد**.

يتم تعطيل هذا الخيار افتراضيًا.

- **تحديد حساب للوصول إلى مجلد مشترك**

إذا تم تمكين هذا الخيار، فيمكنك تحديد الحساب الذي سيتم حفظ التقرير بموجبه في المجلد. إذا تم تحديد مسار UNC لأى مجلد مشترك كإعداد **حفظ التقرير في مجلد** في نافذة **الإجراء الذي سيتم تطبيقه على التقرير**، فيتعين عليك تحديد حساب المستخدم وكلمة المرور للوصول لهذا المجلد.

إذا تم تعطيل هذا الخيار، فسيتم حفظ التقرير في المجلد بموجب حساب خادم الإدارة.

تتوفر خانة الاختيار، إذا تم تحديد **حفظ التقرير إلى مجلد**.

يتم تعطيل هذا الخيار افتراضيًا.

عند حفظ أو إرسال تقرير كملف XLS، يتم حفظ جميع الصور ذات الصلة، مثل الشعار ومخطط البيانات، كملفات منفصلة.

انقر فوق **التالي** للمتابعة إلى الخطوة التالية.

الخطوة 4. تحديد الحساب لبدء المهمة

في النافذة **تحديد حساب لتشغيل المهمة**، يمكنك تحديد الحساب الذي تستخدمه عند تشغيل المهمة. حدد أحد الخيارات التالية:

- **الحساب الافتراضي**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.

يتم تحديد هذا الخيار افتراضيًا.

- **تحديد حساب**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **الحساب**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **كلمة المرور**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

انقر فوق **التالي** للمتابعة إلى الخطوة التالية.

الخطوة 5. تكوين جدول مهمة

في صفحة المعالج **تكوين جدول المهمة**، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N أسبوعًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

الخطوة 6. تحديد اسم المهمة

في الصفحة **حدد اسم المهمة**، حدد اسم القاعدة التي تقوم بإنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة (" * < > ? \ : |).

انقر فوق **التالي** للمتابعة إلى الخطوة التالية.

الخطوة 7. إكمال إنشاء المهمة

في النافذة **إنهاء عملية إنشاء المهمة**، وانقر فوق زر **إنهاء** لإنهاء المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة اختيار **تشغيل المهمة بعد انتهاء المعالج**.

إدارة الإحصائيات

يتم عرض إحصائيات حول حالة نظام الحماية والأجهزة المدارة في أجزاء المعلومات التي يمكن تخصيصها. يتم عرض الإحصائيات في مساحة عمل العقدة **خادم الإدارة** في علامة التبويب **إحصائيات**. تحتوي علامة التبويب على بعض علامات تبويب من المستوى الثاني (صفحات). تعرض كل صفحة مبوبة أجزاء المعلومات التي تحتوي على إحصائيات، بالإضافة إلى روابط تختص بأخبار الشركة ومواد أخرى من Kaspersky. يتم عرض المعلومات الإحصائية في أجزاء المعلومات على شكل جدول أو مخطط (دائري أو شريطي). يتم تحديث البيانات المضمنة في أجزاء المعلومات أثناء تشغيل التطبيق وتعكس الحالة الحالية لتطبيق الحماية.

يمكنك تعديل مجموعة علامات التبويب من المستوى الثاني في علامة التبويب **إحصائيات**، وعدد أجزاء المعلومات في كل صفحة مبوبة ووضع عرض البيانات في أجزاء المعلومات.

لإضافة علامة تبويب جديدة من المستوى الثاني بأجزاء معلومات على علامة التبويب **إحصائيات**:

1. انقر فوق الزر **تخصيص العرض** الموجود في الركن الأيمن العلوي من علامة التبويب **إحصائيات**.

تفتح نافذة خصائص الإحصائيات. تحتوي هذه النافذة على قائمة بالصفحات المبوبة التي يتم عرضها في الوقت الحالي على علامة التبويب **إحصائيات**. في هذه النافذة، يمكنك تغيير ترتيب عرض الصفحات على علامة التبويب، وإضافة صفحات وإزالتها، وتكوين خصائص الصفحة عبر النقر فوق الزر **خصائص**.

2. انقر على الزر **إضافة**.

يؤدي هذا إلى فتح نافذة خصائص صفحة جديدة.

3. تكوين الصفحة الجديدة:

- في القسم **عام**، حدد اسم الصفحة.
- في القسم **جزء المعلومات**، انقر فوق الزر **إضافة** لإضافة أجزاء المعلومات التي يجب عرضها على الصفحة.

انقر فوق الزر **جزء المعلومات** في القسم **خصائص** لإعداد خصائص أجزاء المعلومات التي قمت بإضافتها: الاسم والنوع وطريقة ظهور المخطط في الجزء، بالإضافة إلى البيانات المطلوبة لرسم المخطط.

4. انقر على**موافق**.

تظهر الصفحة المبوبة التي تحتوي على أجزاء المعلومات التي قمت بإضافتها على علامة التبويب **إحصائيات**. انقر فوق الرمز (⚙) للإعدادات للانتقال على الفور إلى تكوين الصفحة أو إلى جزء المعلومات المحدد في هذه الصفحة.

تكوين إخطار الحدث

يتيح لك Kaspersky Security Center تحديد طريقة لإخطار المسؤول بالأحداث التي تحدث على الأجهزة العميلة وكذلك تكوين الإخطار:

- البريد الإلكتروني. عند وقوع حدث ما، يقوم التطبيق بإرسال إخطار لعناوين البريد الإلكتروني المحددة. يمكنك تحرير نص الإخطار.
- SMS عند وقوع حدث ما، يقوم التطبيق بإرسال إخطار لأرقام الهاتف المحددة. يمكنك تكوين إخطارات SMS ليتم إرسالها عبر بوابة البريد.
- الملف التنفيذي عند وقوع حدث ما على جهاز، يتم بدء الملف التنفيذي على محطة عمل المسؤول. باستخدام الملف التنفيذي، يمكن للمسؤول تلقي معلمات أي حدث وقع.

لتكوين إخطار بالأحداث التي تحدث على أجهزة الكمبيوتر العميلة:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.

3. انقر فوق الرابط **تكوين الإخطارات وتصدير الأحداث** وحدد القيمة **تكوين الإخطارات** في القائمة المنسدلة.

يؤدي ذلك لفتح النافذة **خصائص: الأحداث**.

4. في القسم **إخطار**، حدد طريقة الإخطار (عبر البريد الإلكتروني، أو عبر SMS أو عبر تشغيل ملف تنفيذي) وحدد إعدادات الإخطار:

- **البريد الإلكتروني**

تتيح لك علامة التبويب **البريد الإلكتروني** تكوين إشعارات الأحداث عبر البريد الإلكتروني.

في حقل **المستلمون (عناوين البريد الإلكتروني)**، حدد عناوين البريد الإلكتروني التي سيرسل التطبيق الإخطارات إليها. يمكنك تحديد عدة عناوين في هذا الحقل بالفصل بينهم بفواصل منقوطة.

في حقل **SMTP خوادم**، حدد عناوين خادم البريد، مع الفصل بينهم بفواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

في حقل **منفذ خادم SMTP**، حدد رقم منفذ اتصال خادم SMTP. رقم المنفذ الافتراضي هو 25.

إذا قمت بتمكين خيار **استخدم بحث DNS MX**، فيمكنك استخدام عدة سجلات من MX لعناوين IP الخاصة بنفس اسم منطقة DNS في خادم SMTP. قد يكون لاسم DNS نفسه عدة سجلات من MX بقيم مختلفة لتلقي رسائل البريد الإلكتروني ذو الأولوية. يحاول خادم الإدارة إرسال إشعارات البريد الإلكتروني إلى خادم SMTP بترتيب تصاعدي لسجلات MX ذات الأولوية. يتم تعطيل هذا الخيار افتراضيًا.

> إذا قمت بتمكين خيار **استخدم بحث DNS MX**، ولم تقم بتمكين استخدام إعدادات TLS، فإننا نوصي باستخدام إعدادات DNSSEC على جهاز الخادم الخاص بك كإجراء إضافي للحماية لإرسال إعلامات البريد الإلكتروني.

انقر على رابط **الإعدادات** لتحديد إعدادات الإشعارات الإضافية:انقر على رابط الإعدادات لتحديد إعدادات الإشعارات الإضافية:

- اسم الموضوع (اسم موضوع رسالة البريد الإلكتروني)
- عنوان البريد الإلكتروني للمرسل
- إعدادات مصادقة ESMTP

يجب عليك تحديد حساب للمصادقة على خادم SMTP، إذا تم تمكين خيار مصادقة ESMTP لخادم SMTP.

- إعدادات TLS لخادم SMTP:
  - **لا تستخدم TLS**

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

  - **استخدم TLS إذا كان يدعمه خادم SMTP**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام اتصال TLS مع خادم SMTP. إذا كان خادم SMTP لا يدعم TLS، فإن خادم الإدارة يتصل بخادم SMTP بدون استخدام TLS.

  - **استخدام TLS دومًا، وتحقق من شهادة الخادم للتحقق من الصلاحية**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام إعدادات مصادقة TLS. إذا كان خادم SMTP لا يدعم TLS، فلن يتمكن خادم الإدارة من توصيل خادم SMTP.

> نوصي باستخدام هذا الخيار لتوفير حماية أفضل للاتصال بخادم SMTP. إذا قمت بتحديد هذا الخيار، فيمكنك تعيين إعدادات المصادقة لاتصال TLS.

إذا اخترت قيمة **استخدام TLS دومًا والتحقق من شهادة الخادم للتحقق من الصلاحية**، فيمكنك تحديد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال من خلال أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. يمكنك أيضًا تحديد شهادة لمصادقة العميل على خادم SMTP.

يمكنك تحديد إعدادات TLS لخادم SMTP:

- تصفح للوصول إلى ملف شهادة خادم SMTP:

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

- تصفح للوصول إلى ملف شهادة العميل:

يمكنك استخدام شهادة استلمتها من أي مصدر، على سبيل المثال، من أي جهة إصدار موثوقة. يجب تحديد الشهادة ومفتاحها الخاص باستخدام أحد أنواع الشهادات التالية:

- شهادة X-509:

يجب تحديد ملف مع الشهادة وملف مع المفتاح الخاص. كلا الملفين لا يعتمدان على بعضهما البعض وترتيب تحميل الملفات ليس مهمًا. عند تحميل كلا الملفين، يجب تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- الحاوية pkcs12:

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك بعد ذلك تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

يحتوي الحقل **رسالة إخطار** على نص قياسي يحتوي على معلومات حول الحدث الذي يرسله التطبيق عند وقوع حدث. يتضمن هذا النص معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة من خلال إضافة معلمات بديلة أخرى مع تفاصيل ذات صلة أكثر بالحدث. تتوفر قائمة بالمعلمات البديلة عبر النقر فوق الزر على يمين الحقل.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

انقر فوق رابط **تكوين حد الإخطارات الرقمي** لتحديد الحد الأقصى لعدد الإشعارات التي يمكن للتطبيق إرسالها خلال الفترة الزمنية المحددة.

انقر فوق زر **إرسال رسالة اختبار** للتحقق مما إذا كنت قد قمت بتكوين الإشعارات بشكل صحيح. يجب أن يرسل التطبيق إشعار الاختبار إلى عناوين البريد الإلكتروني التي حددتها.

- **رسالة SMS**

تتيح لك علامة التبويب **رسالة SMS** تكوين إرسال إخطارات بمختلف الأحداث عبر رسالة SMS إلى هاتف محمول. يتم إرسال الرسائل النصية القصيرة عبر بوابة بريد.

في الحقل **المستلمين (عناوين البريد الإلكتروني)**، حدد عناوين البريد الإلكتروني التي سيرسل التطبيق الإخطارات إليها. يمكنك تحديد عدة عناوين في هذا الحقل بالفصل بينهم بفواصل منقوطة. سيتم إرسال الإخطارات إلى أرقام الهواتف المرتبطة بعناوين البريد الإلكتروني المحددة.

في الحقل **خوادم SMTP**، حدد عناوين خادم البريد، مع الفصل بينهم بفواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

في الحقل **منفذ خادم SMTP**، حدد رقم منفذ اتصال خادم SMTP. رقم المنفذ الافتراضي هو 25.

انقر على رابط **الإعدادات** لتحديد إعدادات الإشعارات الإضافية:انقر على رابط الإعدادات لتحديد إعدادات الإشعارات الإضافية:

- اسم الموضوع (اسم موضوع رسالة البريد الإلكتروني)
- عنوان البريد الإلكتروني للمرسل
- إعدادات مصادقة ESMTP

إذا لزم الأمر، يمكنك تحديد حساب للمصادقة على خادم SMTP إذا تم تمكين خيار مصادقة ESMTP لخادم SMTP.

- إعدادات TLS لخادم SMTP

يمكنك تعطيل استخدام TLS، استخدام TLS إذا كان خادم SMTP يدعم هذا البروتوكول أو يمكنك فرض استخدام TLS فقط. إذا اخترت استخدام TLS فقط، فيمكنك تحديد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال عبر أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. إذا اخترت أيضًا استخدام TLS فقط، فيمكنك تحديد شهادة لمصادقة العميل على خادم SMTP.

- تصفح للبحث عن ملف شهادة خادم SMTP

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى Kaspersky Security Center. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك بعد ذلك تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم ترميز المفتاح الخاص. يحتوي حقل **رسالة الإشعار** على نص قياسي به معلومات عن الحدث الذي يرسله التطبيق عند وقوع حدث ما. يتضمن هذا النص معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة من خلال إضافة معلمات بديلة أخرى مع تفاصيل ذات صلة أكثر بالحدث. تتوفر قائمة بالمعلمات البديلة عبر النقر فوق الزر على يمين الحقل.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

انقر فوق رابط **تكوين حد الإشعارات الرقمي** لتحديد الحد الأقصى لعدد الإشعارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

انقر فوق زر **إرسال رسالة اختبار** للتحقق مما إذا كنت قد قمت بتكوين الإشعارات بشكل صحيح. يجب أن يرسل التطبيق إشعار اختبار إلى المستلم الذي حددته.

- **الملف التنفيذي المراد تشغيله**

إذا تم تحديد أسلوب الإخطار هذا، ففي حقل الإدخال يمكنك تحديد التطبيق الذي سيتم بدء تشغيله عند وقوع حدث ما.

يتيح لك النقر فوق الرابط **تكوين حد الإخطارات الرقمي** تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

يتيح لك النقر فوق الزر **إرسال رسالة اختبار** التحقق مما إذا قمت بتكوين الإخطارات بطريقة صحيحة: يرسل التطبيق إخطار اختبار إلى عناوين البريد الإلكتروني التي حددتها.

5. في الحقل **رسالة إخطار**، أدخل النص الذي سيرسله التطبيق عند وقوع حدث.

يمكنك استخدام القائمة المنسدلة الموجودة على يسار حقل النص لإضافة إعدادات الاستبدال مع تفاصيل الحدث (على سبيل المثال، وصف الحدث أو قت وقوع الحدث).

إذا كان نص الإخطار يحتوي على نسبة (%)، فيجب عليك تحديده مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

6. انقر فوق الزر **إرسال رسالة اختبار** للتحقق مما إذا تم تكوين الإخطار بشكل صحيح أم لا.

يرسل التطبيق رسالة اختبار إلى المستخدم المحدد.

7. انقر فوق **موافق** لحفظ التغييرات.

يتم تطبيق إعدادات الإخطارات المعاد ضبطها على كل الأحداث التي تحدث على الأجهزة العميلة.

يمكنك تجاوز إعدادات الإخطار لبعض الأحداث من القسم **تكوين الحدث** لإعدادات خادم الإدارة، أو لإعدادات السياسة، أو إعدادات التطبيق.

إنشاء شهادة لخادم STMP

لإنشاء شهادة لخادم SMTP:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.

3. انقر فوق الرابط **تكوين الإخطارات وتصدير الأحداث** وحدد القيمة **تكوين الإخطارات** في القائمة المنسدلة.

تفتح نافذة خصائص الحدث.

4. في علامة التبويب **البريد الإلكتروني**، انقر فوق الرابط **إعدادات** لفتح النافذة **إعدادات**.

5. في النافذة **إعدادات** انقر فوق الرابط **تحديد شهادة** لفتح النافذة **شهادة التوقيع**.

6. في نافذة**شهادة التوقيع**، انقر على زر **استعراض**.
تفتح نافذة **الشهادة**.

7. في القائمة المنسدلة **نوع الشهادة**، حدد نوع الشهادة العامة أو الخاصة:

- إذا تم تحديد نوع الشهادة الخاصة (**الحاوية PKCS#12**)، فقم بتحديد ملف الشهادة وكلمة المرور.
- إذا تم تحديد نوع الشهادة العامة (**الشهادة X.509**):

a. حدد ملف المفتاح الخاص (الملف ذو الامتداد *.prk أو *.pem).

b. حدد كلمة مرور المفتاح الخاص.

c. حدد ملف المفتاح العام (الملف ذو الامتداد *.cer).

8. انقر على**موافق**.

يتم إصدار شهادة لخادم SMTP.

مجموعات الأحداث المحددة

يتم حفظ المعلومات حول الأحداث في تشغيل Kaspersky Security Center والتطبيقات المُدارة في كل من قاعدة بيانات خادم الإدارة وفي سجل نظام Microsoft Windows. يمكنك عرض معلومات من قاعدة بيانات خادم الإدارة في مساحة عمل العقدة **خادم الإدارة**، في علامة التبويب **الأحداث**.

يتم تقديم المعلومات في علامة التبويب **الأحداث** على شكل قائمة مجموعات الأحداث المحددة. تتضمن كل مجموعة نوع محدد من الأحداث فقط. على سبيل المثال، تحتوي المجموعة "حالة الجهاز حرجة" فقط على سجلات حول تغييرات حالات الجهاز إلى "حرجة". بعد تثبيت التطبيق، تحتوي علامة التبويب **الأحداث** على بعض أحداث التحديدات القياسية. يمكنك إنشاء اختيارات (مخصصة) حدث إضافية أو تصدير معلومات الحدث إلى ملف.

عرض تحديد حدث

لعرض اختيار الحدث:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.

3. في القائمة المنسدلة **تحديدات الأحداث**، حدد تحديد الحدث ذي الصلة.
إذا أردت عرض الأحداث من هذه المجموعة باستمرار في مساحة العمل، انقر على أيقونة النجمة (☆) بجانب المجموعة.

ستعرض مساحة العمل قائمة بالأحداث، مخزنة على خادم الإدارة، للنوع المحدد.

يمكنك ترتيب المعلومات في قائمة الأحداث بترتيب تصاعدي أو تنازلي في أي عمود.

تخصيص تحديد حدث

لتخصيص تحديد حدث:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.
3. افتح تحديد الحدث ذي الصلة في علامة التبويب **الأحداث**.
4. انقر على زر **خصائص التحديد**.

   في نافذة خصائص المجموعة المحددة التي تفتح، يمكنك تكوين اختيار الحدث.

إنشاء تحديد حدث

لإنشاء تحديد حدث:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.
3. انقر على زر **إنشاء مجموعة محددة**.
4. في نافذة **تحديد حدث جديد** التي تفتح، أدخل اسم التحديد الجديد وانقر فوق **موافق**.

   يتم إنشاء تحديد يحمل الاسم الذي قمت بتحديده في القائمة المنسدلة **تحديدات الأحداث**.

بشكل افتراضي، يحتوي اختيار الحدث الذي تم إنشاؤه على جميع الأحداث المُخزّنة على خادم الإدارة. لجعل الاختيار يعرض الأحداث التي تريدها فقط، يجب عليك تخصيص الاختيار.

تصدير تحديد حدث إلى ملف نصي

لتصدير تحديد حدث إلى ملف نصي:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.
3. انقر على زر **استيراد/تصدير**.
4. في القائمة المنسدلة، حدد **تصدير الأحداث إلى ملف**.

   يبدأ معالج تصدير الأحداث. اتبع إرشادات المعالج.

حذف أحداث من الاختيار

لحذف أحداث من الاختيار:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة ذي الصلة.
2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.
3. حدد الأحداث التي ترغب في حذفها باستخدام الماوس أو مفتاح **Shift** أو **Ctrl**.
4. احذف الأحداث المحددة بإحدى الطرق التالية:
   - عن طريق تحديد **حذف** في قائمة السياق الخاصة بأي من الأحداث المحددة.

     إذا حددت العنصر **حذف الكل** من قائمة السياق، فسيتم حذف جميع الأحداث المعروضة من التحديد، بصرف النظر عن اختيارك للأحداث المراد حذفها.
   - عن طريق النقر فوق الرابط **حذف حدث** (في حالة تحديد حدث واحد) أو الرابط **حذف الأحداث** (في حالة تحديد عدة أحداث) في خانة المعلومات لهذه الأحداث.

   تم حذف الأحداث المحددة.

إضافة تطبيقات لاستثناءات بواسطة طلبات المستخدم

عندما تتلقى طلبات المستخدمين لإلغاء حظر التطبيقات التي تم حظرها عن طريق الخطأ، يمكنك إنشاء استثناء من قواعد الأمان التكيفية لهذه التطبيقات. وبالتالي، لن يتم حظر التطبيقات على أجهزة المستخدمين بعد الآن. يمكنك تعقب عدد من طلبات المستخدم في علامة التبويب **المراقبة** الخاصة بخادم الإدارة.

لإضافة تطبيقات تم حظرها بواسطة برنامج Kaspersky Endpoint Security للاستثناءات بواسطة طلبات المستخدم:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في مساحة عمل العقدة، حدد علامة التبويب **الأحداث**.
3. في القائمة المنسدلة **تحديدات الأحداث**، حدد **طلبات المستخدم**.
4. انقر بزر الماوس الأيمن فوق طلب المستخدم (أو عدة طلبات للمستخدم) التي تريد إضافتها إلى الاستثناءات، ثم حدد **إضافة استثناء**.

   هذا يبدأ في معالج إضافة الاستثناء. اتبع تعليماته.

سيتم استثناء التطبيقات المحددة من القائمة **يتم تشغيل القاعدة في حالة التدريب الذكي** (ضمن **المستودعات** في شجرة وحدة التحكم) بعد عملية المزامنة التالية للجهاز العميل المزود بخادم الإدارة ولن تظهر في القائمة بعد الآن.

تحديدات الأجهزة

يتم عرض المعلومات حول حالة الأجهزة في المجلد **تحديدات الأجهزة** في شجرة وحدة التحكم.

يتم عرض المعلومات في المجلد **تحديدات الأجهزة** كقائمة بتحديدات الأجهزة. يحتوي كل تحديد على أجهزة تفي بشروط محددة. على سبيل المثال، لا يحتوي التحديد **الأجهزة ذات الحالة حرج** سوى على الأجهزة ذات الحالة حرج. بعد تثبيت التطبيق، يحتوي المجلد **تحديدات الأجهزة** على بعض التحديدات القياسية. ويمكنك إنشاء تحديدات أجهزة إضافية (مخصصة)، أو تصدير إعدادات التحديد إلى ملف، أو إنشاء اختيارات باستخدام إعدادات مستوردة من ملف آخر.

عرض تحديد جهاز

لعرض تحديد جهاز:

1. في شجرة وحدة التحكم، حدد مجلد**تحديدات الأجهزة**.
2. في مساحة عمل المجلد، داخل القائمة المنسدلة **الأجهزة في هذا التحديد**، حدد مجموعة الأجهزة المعنية بالتحديد.
3. انقر على زر **تشغيل التحديد**.
4. انقر على تبويب **نتائج التحديد**.

ستعرض مساحة العمل قائمة بالأجهزة التي تتوافق مع معايير الاختيار.

يمكنك ترتيب المعلومات في قائمة الأجهزة بترتيب تصاعدي أو تنازلي في أي عمود.

تكوين تحديد جهاز

لتكوين تحديد جهاز:

1. في شجرة وحدة التحكم، حدد مجلد**تحديدات الأجهزة**.
2. في مساحة العمل، انقر فوق علامة التبويب **تحديد**، ثم انقر فوق تحديد الجهاز ذي الصلة من قائمة تحديدات المستخدم.
3. انقر على زر **خصائص التحديد**.
4. في نافذة خصائص التي تفتح، حدد الإعدادات التالية:
   - الخصائص العامة للتحديد.
   - الشروط التي يجب تحقيقها لتضمين الأجهزة في هذا التحديد. يمكنك تكوين الشروط بعد تحديد اسم الشرط والنقر فوق الزر **خصائص**.
   - إعدادات الأمان.
5. انقر على**موافق**.

   يتم تطبيق الإعدادات وحفظها.

فيما يلي أوصاف شروط تعيين الأجهزة في تحديد. يتم تجميع الشروط باستخدام المعامل المنطقي OR: سيحتوي التحديد على أجهزة تتوافق على الأقل مع شرط واحد من الشروط الواردة.

عام

في القسم **عام**، يمكنك تغيير اسم شرط التحديد وتحديد ما إذا كان يجب عكس هذا الشرط أم لا:

عكس حالة التحديد

يتم تعطيل هذا الخيار افتراضيًا.

إذا قمت بتمكين هذا الخيار، فسيتم عكس حالة التحديد المحددة. سيتضمن التحديد جميع الأجهزة التي لا تتوافق مع الحالة.

يوضح المثال التالي منطق عمل الانعكاس:

- **الشرط** : يوجد على جهازك نظام تشغيل من نوع Linux ورقم الإصدار 00.0.000.
- **الحالة المعكوسة** : يوجد على جهازك نظام تشغيل ليس (من النوع Linux ورقم الإصدار 00.0.000)، وهو ما يعادل ما يلي:
  يوجد نظام تشغيل من نوع ليس Linux أو رقم الإصدار ليس 00.0.000.

وبالتالي، ستتضمن المجموعة المحددة الأجهزة التي تحتوي على نظام تشغيل، على سبيل المثال، من نوع Windows ورقم الإصدار 00.0.000، أو نوع Linux وأي رقم إصدار آخر بخلاف 00.0.000.

الشبكة

في القسم **الشبكة**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لبيانات الشبكة الخاصة بهم:

- **اسم الجهاز أو عنوان IP**

  اسم شبكة Windows (اسم NetBIOS) للجهاز، أو عنوان IPv4 أو IPv6.

- **مجال Windows**

  عرض كل الأجهزة المضمنة في مجال Windows® المحدد.

- **مجموعة الإدارة**

  عرض الأجهزة المضمنة في مجموعة الإدارة المحددة.

- **الوصف**

  نص في نافذة خصائص الجهاز: في الحقل **الوصف** بالقسم **عام**.

  لوصف النص في الحقل **الوصف**، يمكنك استخدام الرموز التالية:

  - وسط الكلمة:
    - *. تحل محل أية سلسلة بها أي عدد من الحروف.

    مثال:

    لوصف كلمات مثل **الخادم** أو **خاص بالخادم**، يمكنك إدخال **خادم***.

    - ؟. تحل محل أي حرف مفرد.

    مثال:

    لوصف كلمات مثل **نافذة** أو **نوافذ**، يمكنك إدخال **نافذة؟**.

    لا يمكن استخدام نجمة (*) أو علامة استفهام (؟) كأول حرف في الاستعلام.

  - للبحث عن كلمات متعددة:
    - مسافة. تعرض جميع الأجهزة التي يحتوي وصفها على أي كلمة من الكلمات المدرجة.

    مثال:

    للبحث عن عبارة تحتوي على كلمة **تابع** أو **ظاهري**، يمكنك إدخال **تابع ظاهري** في الاستعلام.

    - +. عندما تأتي علامة الزائد قبل كلمة، ستحتوي جميع نتائج البحث على هذه الكلمة.

    مثال:

للبحث عن عبارة تحتوي على الكلمتين **تابع** و**ظاهري**، أدخل الاستعلام **+تابع+ظاهري**.

- **-**. عندما تأتي علامة الناقص قبل كلمة، لن تحتوي نتائج البحث على هذه الكلمة.

مثال:

للبحث عن عبارة تحتوي على كلمة **تابع** ولا تحتوي على كلمة **ظاهري**، أدخل الاستعلام **+تابع-ظاهري**.

- **"<some text>"**. النص الموضوع بين علامتي الاقتباس يجب أن يكون موجودًا في النص.

مثال:

للبحث عن عبارة تحتوي على الكلمة المركّبة **الخادم التابع**، أدخل **"الخادم التابع"** في الاستعلام.

- **نطاق IP**

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.

يتم تعطيل هذا الخيار افتراضيًا.

العلامات

في القسم **العلامات**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على الكلمات المفتاحية (العلامات) التي تمت إضافتها سابقًا إلى أوصاف الأجهزة المدارة:

- **تطبيق في حالة مطابقة علامة محددة واحدة على الأقل**

إذا تم تمكين هذا الخيار، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على علامة واحدة من العلامات على الأقل.

إذا تم تعطيل هذا الخيار، فستعرض نتائج البحث فقط الأجهزة التي تحتوي أوصافها على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

- **يجب تضمين العلامة**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

يتم تحديد هذا الخيار افتراضيًا.

- **يجب استثناء العلامة**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي لا تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

Active Directory

في القسم **Active Directory**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناء على بيانات Active Directory الخاصة بها:

- **الجهاز في وحدة Active Directory التنظيمية**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من وحدة Active Directory المؤسسية المحددة في حقل الإدخال.

يتم تعطيل هذا الخيار افتراضيًا.

- **تضمين وحدات تنظيمية تابعة**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من الوحدات المؤسسية التابعة لوحدات Active Directory المؤسسية.

يتم تعطيل هذا الخيار افتراضيًا.

- **هذا الجهاز عضو في مجموعة Active Directory**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من مجموعة Active Directory المحددة في حقل الإدخال.

يتم تعطيل هذا الخيار افتراضيًا.

نشاط الشبكة

في القسم **نشاط الشبكة** يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لنشاط الشبكة الخاص بهم:

- **هذا الجهاز هوعبارة عن نقطة توزيع**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. سوف يتضمن التحديد أجهزة الكمبيوتر التي تعمل كنقاط توزيع.
- **لا**. لن يتم تضمين الأجهزة التي تعمل كنقاط توزيع في التحديد.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **عدم قطع الاتصال عن خادم الإدارة**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **مُمكّن**. سيتضمن التحديد الأجهزة التي تم تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
- **معطل**. سيتضمن التحديد الأجهزة التي تم إلغاء تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تم تبديل ملف تعريف الاتصال**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. سوف يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
- **لا**. لن يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تاريخ آخر اتصال بخادم الإدارة**

يمكنك استخدام خانة الاختيار هذه لتعيين معيار للبحث عن الأجهزة إلى وقت آخر اتصال بخادم الإدارة.

إذا تم تحديد خانة الاختيار هذه، فيمكنك في حقول الإدخال تحديد الفاصل الزمني (التاريخ والوقت) الذي تم خلاله إنشاء آخر اتصال بين عميل الشبكة المثبت على الجهاز العميل وخادم الإدارة. سوف يتضمن الاختيار الأجهزة التي تقع ضمن الفاصل الزمني المحدد.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **تم اكتشاف أجهزة جديدة بواسطة استقصاء الشبكة**

عمليات البحث عن أجهزة جديدة تم اكتشافها بواسطة استقصاء الشبكة على مدار الأيام القليلة الماضية.

إذا تم تمكين هذا الخيار، فسيتضمن التحديد فقط الأجهزة الجديدة التي تم اكتشافها بواسطة خاصية اكتشاف الأجهزة على مدار عدد الأيام المحددة في حقل **فترة الكشف (بالأيام)**.

إذا تم تعطيل هذا الخيار، فسيتضمن التحديد جميع الأجهزة التي تم اكتشافها بواسطة خاصية اكتشاف الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- **الجهاز مرئي**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المرئية في الوقت الحالي على الشبكة.
- **لا**. يشمل التطبيق في التحديد الأجهزة غير المرئية في الوقت الحالي على الشبكة.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

التطبيق

في القسم **التطبيق**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على التطبيق المدار المحدد:

- **اسم التطبيق**

في القائمة المنسدلة، يمكنك إعداد معيار لتضمين الأجهزة في تحديد عند إجراء بحث باسم تطبيق Kaspersky.

توفر القائمة أسماء التطبيقات مع الأدوات الإضافية للإدارة فقط والمثبتة على محطة عمل المسؤول.

إذا لم يتم تحديد تطبيق، لن يتم تطبيق المعيار.

- **إصدار التطبيق**

في حقل الإدخال، يمكنك تحديد معيار لتضمين الأجهزة في تحديد عند إجراء بحث برقم إصدار تطبيق Kaspersky.

إذا لم يتم تحديد رقم إصدار، لن يتم تطبيق المعيار.

- **اسم التحديث الحرج**

في حقل الإدخال، يمكنك تحديد معيار للأجهزة المشمولة في التحديد عند إجراء بحث باسم التطبيق أو برقم حزمة التحديث.

إذا تم ترك الحقل فارغًا، لن يتم تطبيق المعيار.

- **آخر تحديث للوحدات**

يمكنك استخدام هذا الخيار لتعيين معيار للبحث في الأجهزة على وقت آخر تحديث للوحدات النمطية الخاصة بالتطبيقات المثبتة على تلك الأجهزة.

إذا تم تحديد خانة الاختيار هذه، يمكنك تحديد في حقل الإدخال الفاصل الزمني (الوقت والتاريخ) الذي تم خلاله إجراء التحديث الأخير للوحدات النمطية المثبتة على تلك الأجهزة.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **الجهاز مُدار بواسطة Kaspersky Security Center**

في هذه القائمة المنسدلة، يمكنك تضمين الأجهزة المدارة بواسطة Kaspersky Security Center في التحديد:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المدارة بواسطة Kaspersky Security Center في الاختيار.
- **لا**. يشمل التطبيق الأجهزة الموجودة في التحديد ما لم تكن مدارة من خلال Kaspersky Security Center.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تم تثبيت تطبيق الأمان**

في هذه القائمة المنسدلة، يمكنك تضمين جميع الأجهزة المدارة المثبت عليها تطبيق الأمان في التحديد:

- **نعم**. يشمل التطبيق في الاختيار جميع الأجهزة المدارة بواسطة تطبيق الأمان الذي تم تثبيته:
- **لا**. يشمل التطبيق في الاختيار جميع الأجهزة غير المثبت عليها تطبيق الأمان.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

نظام التشغيل

في القسم **نظام التشغيل**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لنوع نظام التشغيل الخاص بهم.

- **إصدار نظام التشغيل**

إذا تم تحديد خانة الاختيار، فيمكنك تحديد نظام تشغيل من القائمة. يتم تضمين الأجهزة المثبت عليها أنظمة التشغيل المحددة في نتائج البحث.

- **حجم نظام التشغيل بالبت**

في القائمة المنسدلة، يمكنك تحديد بنية نظام التشغيل والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز (**غير معروف**, **x86, AMD64**, أو **IA64**). وبشكل افتراضي، لا يتم تحديد أي خيار في القائمة ومن ثم لا يتم تحديد بنية نظام التشغيل.

- **إصدار حزمة خدمة نظام التشغيل**

في هذا الحقل، يمكنك تحديد إصدار حزمة نظام التشغيل (بتنسيق X.Y)، والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز. وبشكل افتراضي، لا يتم تحديد أي قيمة إصدار.

- **نظام التشغيل بناء**

> لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

رقم نسخة نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم نسخة مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.

- **معرف تحرير نظام التشغيل**

> لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

معرف إصدار (ID) نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك معرف إصدار مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام معرف الإصدار باستثناء الرقم المحدد.

حالة الجهاز

في القسم **حالة الجهاز**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على وصف حالة الأجهزة من التطبيق المدار:

- **حالة الجهاز**

القائمة المنسدلة التي يمكنك فيها تحديد إحدى حالات الجهاز: موافق، أو حرج، أو تحذير.

- **وصف حالة الجهاز**

يمكنك في هذا الحقل، تحديد خانات الاختيار بجانب الشروط التي تحدد، إن تم استيفائها، إحدى الحالات التالية لجهاز الكمبيوتر: موافق أو حرج أو تحذير.

- **حالة الجهاز المحددة بواسطة التطبيق**

يمكنك في القائمة المنسدلة تحديد حالة الحماية في الوقت الحقيقي. يتم تضمين الأجهزة مع حالة الحماية في الوقت الحقيقي في التحديد.

مكونات الحماية

في القسم **مكونات الحماية**، يمكنك إعداد معايير لتضمين الأجهزة في تحديد بناءً على حالة الحماية الخاصة بها:

- **تم إصدار قاعدة البيانات**

إذا تم تحديد هذا الخيار، يمكنك البحث عن أجهزة العميل حسب تاريخ إصدار قاعدة بيانات تطبيق مكافحة الفيروسات. في حقول الإدخال، يمكنك تعيين الفاصل الزمني الذي يتم إجراء البحث بناءً عليه.

يتم تعطيل هذا الخيار افتراضيًا.

- **عملية الفحص الأخيرة**

إذا تم تمكين هذا الخيار، فيمكنك البحث عن أجهزة العميل حسب وقت آخر فحص للبرامج الضارة. في حقول الإدخال، يمكنك تحديد الفترة الزمنية التي تم فيها آخر فحص للبرامج الضارة.

يتم تعطيل هذا الخيار افتراضيًا.

- **إجمالي عدد التهديدات المكتشفة**

إذا تم تمكين هذا الخيار، يمكنك البحث عن أجهزة العميل حسب عدد الفيروسات التي تم العثور عليها. في حقول الإدخال، يمكنك تعيين قيم الحد الأدنى والأعلى لعدد الفيروسات التي تم العثور عليها.

يتم تعطيل هذا الخيار افتراضيًا.

سجل التطبيقات

في القسم **سجل التطبيقات**، يمكنك إعداد معايير البحث عن الأجهزة وفقًا للتطبيقات المثبتة عليها:

- **اسم التطبيق**

القائمة المنسدلة التي يمكنك فيها تحديد أي تطبيق. يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **إصدار التطبيق**

يمكنك في حقل الإدخال تحديد إصدار التطبيق المحدد.

- **المورّد**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة لأي تطبيق مثبت على الجهاز.

- **حالة التطبيق**

يمكنك في القائمة المنسدلة تحديد حالة أي تطبيق (مثبت، غير مثبت). سيتم تضمين الأجهزة التي تم تثبيت التطبيق المحدد أو لم يتم تثبيته عليها، بناءً على الحالة المحددة، في التحديد.

- **بحث حسب التحديث**

إذا تم تمكين هذا الخيار، فسيتم إجراء البحث باستخدام تفاصيل تحديثات التطبيقات المثبتة على الأجهزة ذات الصلة. بعد تحديد خانة الاختيار، تتغير الحقول **اسم التطبيق** و**إصدار التطبيق** و**حالة التطبيق** إلى **اسم التحديث** و**إصدار التحديث** و**الحالة** على التوالي.

يتم تعطيل هذا الخيار افتراضيًا.

- **اسم تطبيق الأمان غير المتوافق**

القائمة المنسدلة التي يمكنك فيها تحديد تطبيقات الحماية الخاصة بالجهة الخارجية. خلال البحث، يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **علامة التطبيق**

يمكنك في القائمة المنسدلة تحديد علامة التطبيق. يتم تضمين جميع الأجهزة المثبت عليها تطبيقات مشتملة على العلامة المحددة في الوصف، في تحديد الجهاز.

- **التطبيق على الأجهزة بدون العلامات المحددة**

إذا تم تمكين هذا الخيار، فسيتضمن التحديد أجهزة أوصافها لا تحتوي على أي من العلامات المحددة.

إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار.
يتم تعطيل هذا الخيار افتراضيًا.

سجل الأجهزة

في القسم **سجل الأجهزة**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناء على الأجهزة المثبتة:

- **الجهاز**

يمكنك في القائمة المنسدلة تحديد نوع الوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.
يدعم الحقل البحث بالنص الكامل.

- **المورّد**

يمكنك في القائمة المنسدلة تحديد اسم الشركة المصنعة للوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.
يدعم الحقل البحث بالنص الكامل.

- **اسم الجهاز**

اسم الجهاز الموجود في شبكة Windows. سيتم تضمين الجهاز ذي الاسم المحدد في التحديد.

- **الوصف**

وصف الجهاز أو وحدة الجهاز. سيتم تضمين الأجهزة ذات الوصف المحدد في هذا الحقل في التحديد.
يمكن إدخال وصف الجهاز بأي تنسيق في نافذة خصائص هذا الجهاز. يدعم الحقل البحث بالنص الكامل.

- **بائع الجهاز**

اسم الشركة المصنعة للجهاز. سيتم تضمين الأجهزة التي تنتجها الشركة المصنعة المحددة في هذا الحقل في التحديد.
يمكنك إدخال اسم الشركة المصنعة في نافذة خصائص جهاز.

- **الرقم التسلسلي**

سيتم تضمين جميع وحدات الأجهزة ذات الرقم التسلسلي المحددة في هذا الحقل في التحديد.

- **رقم المخزون**

سيتم تضمين الأجهزة ذات رقم المخزون والمحدد في هذا الحقل في التحديد.

- **المستخدم**

سيتم تضمين جميع وحدات أجهزة المستخدم المحدد في هذا الحقل في التحديد.

- **الموقع**

موقع جهاز أو وحدة أجهزة (على سبيل المثال، في المقر الرئيسي أو مكتب فرعي). سيتم تضمين أجهزة الكمبيوتر أو الأجهزة الأخرى التي تم نشرها في الموقع المحدد في هذا الحقل في التحديد.

يمكنك وصف موقع جهاز بأي تنسيق في نافذة خصائص هذا الجهاز.

- **سرعة وحدة المعالجة المركزية (CPU) (بالميجاهرتز)**

نطاق تردد وحدة المعالجة المركزية. سيتم تضمين الأجهزة ذات وحدة المعالجة المركزية التي تتطابق مع نطاق التردد في حقوق الإدخال هذه (شامل) في التحديد.

- **مراكز CPU الظاهرية**

نطاق عدد النوى الظاهري في وحدة معالجة مركزية. سيتم تضمين أجهزة الكمبيوتر ذات وحدات المعالجة المركزية والتي تتطابق مع النطاق في حقوق الإدخال هذه (شامل) في التحديد.

- **حجم القرص الثابت بالجيجابايت**

نطاق القيم لحجم محرك القرص الثابت على الجهاز. سيتم تضمين الأجهزة ذات محركات الأقراص الثابتة والتي تطابق مع النطاق في حقوق الإدخال هذه (شامل) في التحديد.

- **حجم ذاكرة الوصول العشوائي RAM، بالميجابايت**

نطاق القيم لحجم ذاكرة الوصول العشوائي للجهاز. سيتم تضمين الأجهزة التي تحتوي على ذاكرة الوصول العشوائي، والتي تطابق النطاق في حقول الإدخال هذه (ضمناً) في التحديد.

الأجهزة الظاهرية

في القسم **الأجهزة الظاهرية**، يمكنك إعداد المعايير لتضمين الأجهزة في التحديد بناءً على ما إذا كانت تعد أجهزة ظاهرية أو جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI):

- **هذا جهاز ظاهري**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

  - **ليس هامًا**.
  - **لا**. البحث عن الأجهزة التي لا تعد أجهزة افتراضية.
  - **نعم**. البحث عن الأجهزة التي تعد أجهزة ظاهرية.

- **نوع الجهاز الظاهري**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة للجهاز الظاهري.

هذه القائمة المنسدلة متاحة إذا تم تحديد القيمة **نعم** أو **ليس هامًا** تم تحديد القيمة **هذا جهاز ظاهري** في القائمة المنسدلة.

- **جزء من البنية الأساسية لسطح المكتب الافتراضي**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

  - **ليس هامًا**.
  - **لا**. البحث عن الأجهزة التي لا تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي.
  - **نعم**. البحث عن الأجهزة التي تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI).

الثغرات الأمنية والتحديثات

في القسم **الثغرات الأمنية والتحديثات**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لمصدر Windows Update الخاص بها:

تم تبديل WUA إلى خادم الإدارة

يمكنك تحديد خيار من خيارات البحث التالية من القائمة المنسدلة:

- **نعم**. إذا تم تحديد هذا الخيار، فستشتمل نتائج البحث على الأجهزة التي تتلقى تحديثات من خلال Windows Update من خادم الإدارة.
- **لا**. إذا تم تحديد هذا الخيار، ستشتمل النتائج الأجهزة التي تتلقى تحديثات من خلال Windows Update من مصادر أخرى.

المستخدمون

في القسم **المستخدمون**، يمكنك إعداد المعايير لتضمين الأجهزة في التحديد بحسب حسابات المستخدمين الذين قاموا بتسجيل الدخول إلى نظام التشغيل.

- **آخر مستخدم سجّل الدخول إلى النظام**

إذا تم تمكين هذا الخيار، فانقر فوق زر **استعراض** لتحديد حساب مستخدم. تشتمل نتائج البحث على الأجهزة التي قام مستخدم محدد بإجراء آخر تسجيل دخول عليها إلى النظام.

- **مستخدم قام بتسجيل الدخول إلى النظام مرة واحدة على الأقل**

إذا تم تمكين هذا الخيار، فانقر فوق زر **استعراض** لتحديد حساب مستخدم. ستتضمن نتائج البحث الأجهزة التي قام مستخدم محدد بتسجيل الدخول عليها مرة واحدة على الأقل.

مشاكل تؤثر على الحالة في التطبيقات المُدارة

في القسم **مشاكل تؤثر على الحالة في التطبيقات المُدارة**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لقائمة المشكلات المحتملة التي يتم اكتشافها بواسطة التطبيق المُدار. إذا كانت مشكلة واحدة على الأقل من المشكلات التي حددتها موجودة على جهاز، فسيتم تضمين الجهاز في القسم. في حالة اختيار مشكلة مدرجة للعديد من التطبيقات، فلديك الخيار لتحديد هذه المشكلة في جميع القوائم تلقائيًا.

وصف حالة الجهاز

يمكنك تحديد خانات الاختيار الخاصة بأوصاف الحالات من تطبيق مدار؛ وفور استلام هذه الحالات، سيتم تضمين الأجهزة في التحديد. في حالة اختيار حالة مدرجة للعديد من التطبيقات، فلديك الخيار لتحديد هذه الحالة في جميع القوائم تلقائيًا.

حالات المكونات في التطبيقات المُدارة

في القسم **حالات المكونات في التطبيقات المُدارة**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على حالات المكونات في التطبيقات المُدارة:

- **حالة منع تسريب البيانات**

البحث عن الأجهزة حسب حالة منع تسرب البيانات (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **حالة الحماية الخاصة بتعاون الخوادم**

البحث عن الأجهزة حسب حالة حماية تعاون الخادم (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **حالة الحماية ضد الفيروسات الخاصة بخوادم البريد**

البحث عن الأجهزة حسب حالة حماية خادم البريد (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **حالة أداة استشعار نقطة النهاية**

البحث عن الأجهزة حسب حالة المكون أداة استشعار نقطة النهاية (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

التشفير

خوارزمية التشفير

مقياس التشفير المتقدم (AES) خوارزمية التشفير الكتلي المتناظر. في القائمة المنسدلة، يمكنك تحديد حجم مفتاح التشفير (56 بت أو 128 بت أو 192 بت أو 256 بت).

القيم المتوفرة: AES56وAES128وAES192وAES256.

قطاعات السحابة

في القسم **قطاعات السحابة**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد وفقًا لقطاعات السحابة الخاصة بها:

- **الجهاز موجود ضمن قطاع السحابة**

إذا تم تمكين هذا الخيار، فيمكنك النقر فوق زر **استعراض** لتحديد قطاع البحث.

إذا تم أيضًا تمكين خيار **تضمين كائنات فرعية**، فسيتم تشغيل البحث في جميع الكائنات التابعة للقطاع المحدد.

البحث عن النتائج التي تشتمل فقط على أجهزة من القطاع المحدد.

- **تم اكتشاف الجهاز باستخدام واجهة برمجة التطبيقات**

يمكنك تحديد ما إذا كان تم اكتشاف الجهاز بواسطة أدوات API في القائمة المنسدلة:

- **AWS**. يتم اكتشاف الجهاز باستخدام AWS API، أي أن الجهاز يوجد بالفعل في بيئة سحابة AWS.
- **Azure**. يتم اكتشاف الجهاز باستخدام Azure API، أي أن الجهاز يوجد بالفعل في بيئة سحابة Azure.
- **Google Cloud**. يتم اكتشاف الجهاز باستخدام Google API، أي أن الجهاز موجود بالفعل في بيئة Google cloud.
- **لا**. لا يمكن اكتشاف الجهاز باستخدام AWS أو Azure أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة لكن لا يمكن اكتشافه باستخدام واجهة برمجة التطبيق (API).
- **لا توجد قيمة**. هذا الشرط لا ينطبق.

مكونات التطبيق

يحتوي هذا القسم على قائمة المكونات لهذه التطبيقات التي لديها مكونات إدارة إضافية مطابقة مُثبتة في وحدة تحكم الإدارة.

في القسم **مكونات التطبيق**، يمكنك تحديد معايير لتضمين الأجهزة في تحديد وفقًا للحالات ولأرقام الإصدار المكونات التي تشير للتطبيق الذي حددته:

- **الحالة**

البحث عن الأجهزة وفقًا لحالة المكون المُرسلة بواسطة تطبيق إلى خادم الإدارة. يمكنك تحديد أحد الحالات التالية: لا بيانات من الجهاز، أو متوقف، أو بدء التشغيل، أو تم الإيقاف مؤقتًا، أو قيد التشغيل، أو اختلال تشغيل أو غير مثبت. إذا كان للمكون المحدد للتطبيق المُثبت على جهاز مُدار حالة محددة، فإنه يتم تضمين الجهاز في تحديد الجهاز.

الحالات المرسلة بواسطة التطبيقات:

- بدء تشغيل—يكون المكون في عملية التهيئة في الوقت الحالي.
- قيد التشغيل—يكون المكون ممكنًا ويعمل على النحو الصحيح.
- تم الإيقاف مؤقتًا—تم تعليق المكون، على سبيل المثال، بعد إيقاف المستخدم للحماية مؤقتًا في التطبيق المُدار.
- اختلال التشغيل—حدث خطأ أثناء تشغيل المكون.

- متوقف—تم تعطيل المكون وهو لا يعمل في الوقت الحالي.
- غير مثبت—لم يقم المستخدم بتحديد المكون للتثبيت عند تكوين التثبيت المخصص للتطبيق.

بخلاف التطبيقات الأخرى، فإن الحالة لا بيانات من الجهاز لا تُرسل بواسطة التطبيقات. يُظهر هذا الخيار عدم امتلاك التطبيقات لمعلومات حول حالة المكون المحدد. على سبيل المثال، قد يحدث هذا عندما يكون المكون المحدد لا ينتمي لأي من التطبيقات المثبتة على الجهاز، أو عند إيقاف تشغيل الجهاز.

- **الإصدار**

البحث عن الأجهزة وفقًا لرقم الإصدار للمكون الذي حددته في القائمة. يمكنك كتابة رقم الإصدار، على سبيل المثال `3.4.1.0`، ثم تحديد ما إذا كان المكون المحدد يجب أن يمتلك إصدارًا مماثلاً أو إصدارًا سابقًا أو إصدارًا أحدث. يمكنك أيضًا تكوين البحث عن جميع الإصدارات عدا الإصدار المحدد.

تصدير إعدادات تحديد جهاز إلى ملف

لتصدير إعدادات تحديد جهاز إلى ملف نصي:

1. في شجرة وحدة التحكم، حدد مجلد**تحديدات الأجهزة**.
2. في مساحة العمل، انقر فوق علامة التبويب **تحديد**، ثم انقر فوق تحديد الجهاز ذي الصلة من قائمة تحديدات المستخدم.

> يمكن تصدير الإعدادات فقط من تحديدات الجهاز التي أنشأها المستخدم.

3. انقر على زر **تشغيل التحديد**.
4. في علامة التبويب **نتائج التحديد**، انقر فوق الزر **إعدادات التصدير**.
5. في نافذة **حفظ باسم** التي تفتح, حدد اسمًا لملف تصدير إعدادات التحديد، وحدد مجلدًا لحفظه فيه، وانقر فوق الزر **حفظ**.

وسوف يتم حفظ إعدادات تحديد الجهاز على الملف المحدد.

إنشاء تحديد جهاز

لإنشاء تحديد جهاز:

1. في شجرة وحدة التحكم، حدد مجلد**تحديدات الأجهزة**.
2. في مساحة عمل المجلد، انقر فوق **خيارات متقدمة** وحدد **إنشاء مجموعة محددة** في القائمة المنسدلة.
3. في نافذة **تحديد جهاز جديد** التي تفتح، أدخل اسم التحديد الجديد وانقر على **موافق**.

سيظهر مجلد جديد بالاسم الذي أدخلته في شجرة وحدة التحكم في المجلد **تحديدات الأجهزة**. بشكل افتراضي، يحتوي تحديد الأجهزة الجديد على جميع الأجهزة المضمنة في مجموعات الإدارة الخاصة بخادم الإدارة الذي تم إنشاء التحديد عليه. لجعل التحديد يعرض الأجهزة التي تريدها فقط، قم بتكوين التحديد عن طريق النقر فوق الزر **خصائص التحديد**.

إنشاء تحديد جهاز وفقًا لإعدادات مستوردة

لإنشاء تحديد جهاز وفقًا لإعدادات مستوردة:

1. في شجرة وحدة التحكم، حدد مجلد**تحديدات الأجهزة**.
2. في مساحة عمل المجلد، انقر فوق الزر **خيارات متقدمة** وحدد **استيراد مجموعة محددة من ملف** في القائمة المنسدلة.
3. في النافذة التي تفتح، حدد المسار إلى الملف الذي تريد استيراد الإعدادات المحددة منه. انقر فوق الزر **فتح**.

يتم إنشاء الإدخال **تحديد جديد** في المجلد **تحديدات الأجهزة**. تم استيراد إعدادات التحديد الجديد من الملف الذي قمت بتحديده.

إذا كان التحديد الذي يحمل اسم **تحديد جديد** موجودًا بالفعل في المجلد **تحديدات الأجهزة**، فسيتم إضافة فهرس بتنسيق **(<رقم التسلسل التالي>)** إلى اسم التحديد الذي تم إنشاؤه، على سبيل المثال: **(1)**، **(2)**.

إزالة أجهزة من مجموعات الإدارة في تحديد

عند العمل مع تحديد جهاز، يمكنك إزالة الأجهزة من مجموعات الإدارة في هذا التحديد، دون التبديل إلى مجموعات الإدارة التي يجب إزالة هذه الأجهزة منها.

لإزالة الأجهزة من مجموعات إدارة:

1. من شجرة وحدة التحكم، حدد المجلد **تحديدات الأجهزة**.
2. حدد الأجهزة التي تريد إزالتها باستخدام مفاتيح **Shift** أو **Ctrl**.
3. قم بإزالة الأجهزة المحددة من مجموعات الإدارة بإحدى الطرق التالية:
   - حدد **حذف** في قائمة السياق الخاصة بأي من الأجهزة المحددة.
   - انقر على زر **تنفيذ الإجراء** وتحديد **إزالة من المجموعة** في القائمة المنسدلة.

يتم إزالة الأجهزة المحددة من مجموعات الإدارة الخاصة بها.

مراقبة تثبيت التطبيقات وإلغاء تثبيتها

يمكنك مراقبة تثبيت تطبيقات محددة أو زالة تثبيتها على الأجهزة المُدارة، (على سبيل المثال، مستعرض مُعيَّن). لاستخدام هذه الوظيفة، يمكنك إضافة تطبيقات من سجل التطبيقات إلى قائمة التطبيقات المُراقَبة. عند تثبيت تطبيق مُراقَب أو إزالة تثبيته، ينشر عميل الشبكة الأحداث المعنية: **تم تثبيت التطبيق المراقب** أو **تم إلغاء تثبيت التطبيق المراقب**. يمكنك مراقبة هذه الأحداث باستخدام، على سبيل المثال، تحديدات الأحداث أو التقارير.

لا يمكنك مراقبة هذه الأحداث إلا إذا تم تخزينها في قاعدة بيانات خادم الإدارة.

لإضافة تطبيق لقائمة النطاقات المُراقَبة:

1. في مجلد**خيارات متقدمة**← **إدارة التطبيق** بشجرة وحدة التحكم، حدد المجلد الفرعي **سجل التطبيقات**.

2. فوق قائمة التطبيق، التي يتم عرضها، انقر فوق الزر **عرض نافذة خصائص سجل التطبيقات**.

3. في النافذة **التطبيقات المراقبة** المعروضة انقر فوق الزر **إضافة** .

4. في النافذة **تحديد اسم التطبيق** المعروضة حدد التطبيقات من سجل التطبيقات الذي تريد مراقبة تثبيته أو إلغاء تثبيته.

5. في النافذة **تحديد اسم التطبيق**، انقر فوق الزر **موافق**.

بعد تكوين قائمة التطبيقات المُراقبة وتثبيت التطبيق المُراقَب أو إلغاء تثبيته على الأجهزة المُدارة في مؤسستك، يمكنك مراقبة الأحداث المعنية، على سبيل المثال باستخدام تحديد الحدث الأحداث الأخيرة.

أحداث مكونات Kaspersky Security Center

يحتوي كل مكون من مكونات Kaspersky Security Center على مجموعة من أنواع الأحداث خاصة به. يقوم هذا القسم بإدراج أنواع الأحداث التي تقع في خادم إدارة Kaspersky Security Center، وفي عميل الشبكة، وخادم iOS MDM. أنواع الأحداث التي تظهر في تطبيقات Kaspersky غير مدرجة في هذا القسم.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

بنية البيانات لوصف نوع الحدث

بالنسبة لكل أنواع الأحداث، يتوفر اسم العرض والمعرف (ID) والرمز بالحروف الأبجدية والوصف ومدة التخزين الافتراضية.

- **اسم العرض لنوع الحدث**. يتم عرض هذا النص في Kaspersky Security Center عند قيامك بتكوين الأحداث وعند حدوثها.
- **مُعرّف نوع الحدث**. يتم استخدام هذا الرمز الرقمي عند قيامك بمعالجة الأحداث باستخدام أدوات تابعة لجهات خارجية لتحليل الأحداث.
- **نوع الحدث** (رمز بالحروف الأبجدية). يتم استخدام هذا الرمز عند قيامك باستعراض ومعالجة الأحداث باستخدام طرق العرض العامة المتوفرة في قاعدة بيانات Kaspersky Security Center وعندما يتم تصدير الأحداث إلى نظام SIEM.
- **الوصف**. يحتوي هذا النص على المواقف التي يحدث فيها الحدث وما يمكنك القيام به في مثل هذه الحالة.
- **مدة التخزين الافتراضية**. هذا هو عدد الأيام التي يتم خلالها تخزين الحدث في قاعدة بيانات خادم الإدارة ويتم عرضه في قائمة الأحداث على خادم الإدارة. بعد انقضاء هذه الفترة، يتم حذف الحدث. إذا كانت قيمة وقت تخزين الحدث هي عدم التخزين، فإنه يتم اكتشاف هذه الأحداث ولكن لا يتم عرضها في قائمة الأحداث على خادم الإدارة. إذا قمت بتكوين الإعدادات الخاصة بك لحفظ مثل هذه الأحداث في سجل أحداث نظام التشغيل، فيمكنك العثور عليها هناك.

  يمكنك تغيير مدّة التخزين للأحداث:

  - وحدة تحكم الإدارة: تعيين مدة التخزين لحدث
  - Kaspersky Security Center Web Console: تعيين مدة تخزين حدث

قد تتضمن البيانات الأخرى الحقول التالية:

- **event_id**: رقم فريد للحدث في قاعدة البيانات يتم إنشاؤه وتخصيصه تلقائيًا؛ لا يجب الخلط بينه وبين **معرف نوع الحدث**.
- **task_id**: معرّف المهمة التي تسببت في الحدث (إن وجد)
- **الخطورة**: أحد مستويات الخطورة التالية (بترتيب تصاعدي للخطورة):
  0) مستوى خطورة غير صالح
  1) معلومات
  2) تحذير
  3) خطأ
  4) خطير

أحداث خادم الإدارة

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بخادم الإدارة.

الأحداث الحرجة لخادم الإدارة

يوضح الجدول أدناه أنواع أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **حرج**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

إذا حددت المنفذ في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة، فإن **Kaspersky Security Center ينشر مقاييسه** والأحداث المهمة التي سيحصل عليها نظام Prometheus، وهو نظام للمراقبة والتنبيه. ويحصل نظام Prometheus على المقاييس والأحداث الحرجة، ثم ينشئ تنبيهات لكل حدث.

// Kaspersky Security Center common counters—KL.KSC.Common

"klserver errors" ,"counter" ,"xdr_klserver_errors"

"klserver api calls time" ,"counter" ,"xdr_klserver_api_calls_time"

// Transport counters set—KL.KSC.Transport

"number of all connections" ,"counter" ,"ksc_Transport__Number_of_all_connections"

"number of all Network Agent connection" ,"counter" ,"ksc_Transport__Number_of_all_nagent_connection"

number of controlled Network Agent" ,"counter" ,"ksc_Transport__Number_of_controlled_nagent_connections" "connections

"total active devices count" ,"gauge" ,"ksc_Transport__Total_active_hosts_count"

"number of pings processed" ,"counter" ,"ksc_Transport__Number_of_pings_processed"

"number of pings rejected" ,"counter" ,"ksc_Transport__Number_of_pings_rejected"

"number of ping processing errors" ,"counter" ,"ksc_Transport__Number_of_ping_processing_errors"

"number of TCP connections accepted" ,"counter" ,"ksc_Transport__Number_of_TCP_connections_accepted"

"number of failed TCP connections" ,"counter" ,"ksc_Transport__Number_of_failed_TCP_connections"

"bytes sent by TCP" ,"counter" ,"ksc_Transport__Bytes_sent_by_TCP"

"bytes received by TCP" ,"counter" ,"ksc_Transport__Bytes_received_by_TCP"

"number of GetNextFileChunk requests" ,"counter" ,"ksc_Transport__Number_of_GetNextFileChunk_requests"

"number of GetNextFileChunk rejected" ,"counter" ,"ksc_Transport__Number_of_GetNextFileChunk_rejected"

bytes transmitted through" ,"counter" ,"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk" "GetNextFileChunk

Events delivery counters set—KL.KSC.Events //

"number of event bulks processed" ,"counter" ,"ksc_Events__Number_of_event_bulks_processed"

"number of event bulks rejected" ,"counter" ,"ksc_Events__Number_of_event_bulks_rejected"

"number of event bulks processing errors" ,"counter" ,"ksc_Events__Number_of_event_bulks_processing_errors"

number of event bulks processing just" ,"gauge" ,"ksc_Events__Number_of_event_bulks_processing_just_now" "now

"number of events processed" ,"counter" ,"ksc_Events__Number_of_events_processed"

"number of events rejected" ,"counter" ,"ksc_Events__Number_of_events_rejected"

"number of events processing errors" ,"counter" ,"ksc_Events__Number_of_events_processing_errors"

"number of events processing just now" ,"gauge" ,"ksc_Events__Number_of_events_processing_just_now"

Kaspersky Security Center resources usage—KL.KSC.Resources //

"CPU time in user mode" ,"counter" ,"ksc_Resources__CPU_time_in_user_mode"

"CPU time in kernel mode" ,"counter" ,"ksc_Resources__CPU_time_in_kernel_mode"

"process ID of klserver" ,"gauge" ,"ksc_Resources__PID_of_klserver_process"

"process ID of klnagent" ,"gauge" ,"ksc_Resources__PID_of_klnagent_process"

"available disk user quota for server data" ,"gauge" ,"ksc_Resources__Available_disk_user_quota_for_server_data"

"available disk user quota for packages" ,"gauge" ,"ksc_Resources__Available_disk_user_quota_for_packages"

"current OpenAPI threads count" ,"counter" ,"ksc_Resources__Current_OpenAPI_threads_count"

"maximum OpenAPI threads count" ,"counter" ,"ksc_Resources__Maximum_OpenAPI_threads_count"

KL.KSC.NLST //

List of server transactions—KL.KSC.NLST.Trans.Common //

"current transactions count" ,"gauge" ,"ksc_NLST__Common__Current_transactions_count"

"transactions queue full" ,"gauge" ,"ksc_NLST__Common__Transactions_queue_ful"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Common__Transactions_queue_near_to_ful"

Application Control link—KL.KSC.NLST.InvAppCtrlLink //

"items changed" ,"gauge" ,"ksc_NLST__Application_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Application_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Application_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Application_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_in_queue"

Software Inventory—KL.KSC.NLST.InvSoft //

"items changed" ,"gauge" ,"ksc_NLST__Software_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Software_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Software_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Software_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Software_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Software_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Software_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Software_inventory__transactions_in_queue"

Hardware Inventory—KL.KSC.NLST.InvHard //

"items changed" ,"gauge" ,"ksc_NLST__Hardware_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Hardware_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Hardware_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Hardware_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Hardware_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Hardware_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Hardware_inventory__transactions_in_queue"

Device Control—KL.KSC.NLST.DevCtrl //

"items changed" ,"gauge" ,"ksc_NLST__Device_control__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Device_control__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Device_control__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Device_control__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Device_control__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Device_control__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Device_control__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Device_control__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Device_control__transactions_in_queue"

Mobile Device Management—KL.KSC.NLST.MDM //

"items changed" ,"gauge" ,"ksc_NLST__Mobile_device_management__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Mobile_device_management__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Mobile_device_management__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Mobile_device_management__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Mobile_device_management__transactions_queue_full"

transactions queue near" ,"gauge" ,"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full" "to full

"list is pending" ,"gauge" ,"ksc_NLST__Mobile_device_management__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Mobile_device_management__transactions_in_queue"

Device management emails—KL.KSC.NLST.MDMmails //

"items changed" ,"gauge" ,"ksc_NLST__Device_management_emails__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Device_management_emails__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Device_management_emails__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Device_management_emails__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Device_management_emails__transactions_queue_full"

transactions queue near" ,"gauge" ,"ksc_NLST__Device_management_emails__transactions_queue_near_to_full" "to full

"list is pending" ,"gauge" ,"ksc_NLST__Device_management_emails__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Device_management_emails__transactions_in_queue"

Application Control—KL.KSC.NLST.AppCtrl //

"items changed" ,"gauge" ,"ksc_NLST__Application_control__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Application_control__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Application_control__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Application_control__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Application_control__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Application_control__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Application_control__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Application_control__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Application_control__transactions_in_queue"

"items changed" ,"gauge" ,"ksc_NLST__Application_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Application_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Application_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Application_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_in_queue"

Data protection errors—KL.KSC.NLST.DPEErrors //

"items changed" ,"gauge" ,"ksc_NLST__Data_protection_errors__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Data_protection_errors__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Data_protection_errors__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Data_protection_errors__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Data_protection_errors__transactions_queue_full"

transactions queue near to" ,"gauge" ,"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full" "full

"list is pending" ,"gauge" ,"ksc_NLST__Data_protection_errors__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Data_protection_errors__transactions_in_queue"

iOS Mobile Device Management—KL.KSC.NLST.iOsMDM //

"items changed" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__change_item_operations"

list is disabled due" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize" "to oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__transactions_queue_full"

transactions queue" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full" "near to full

"list is pending" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__transactions_in_queue"

Vulnerability assessment and patch management—KL.KSC.NLST.Vapm //

"items changed" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items"

change" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations" "item operations

list" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize" "is disabled due to oversize

,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full" "transactions queue full"

,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full" "transactions queue near to full"

"list is pending" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending"

transactions" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue" "in queue

Vulnerability assessment—KL.KSC.NLST.Va //

"items changed" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__transactions_queue_full"

transactions queue near to" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full" "full

"list is pending" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__transactions_in_queue"

Virtual machines—KL.KSC.NLST.VM //

"items changed" ,"gauge" ,"ksc_NLST__Virtual_machines__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Virtual_machines__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Virtual_machines__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Virtual_machines__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Virtual_machines__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Virtual_machines__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Virtual_machines__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Virtual_machines__transactions_in_queue"

Windows Update—KL.KSC.NLST.WUS //

"items changed" ,"gauge" ,"ksc_NLST__Windows_update__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Windows_update__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Windows_update__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Windows_update__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Windows_update__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Windows_update__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Windows_update__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Windows_update__transactions_in_queue"

CIP PLC—KL.KSC.NLST.CIP_PLC //

"items changed" ,"gauge" ,"ksc_NLST__CIP_PLC__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__CIP_PLC__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__CIP_PLC__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__CIP_PLC__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__CIP_PLC__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__CIP_PLC__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__CIP_PLC__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__CIP_PLC__transactions_in_queue"

Network Agent Network Scan—KL.KSC.NLST.NagentNetScan //

"items changed" ,"gauge" ,"ksc_NLST__Network_scan__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Network_scan__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Network_scan__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Network_scan__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Network_scan__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Network_scan__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Network_scan__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Network_scan__transactions_in_queue"

Adaptive Security—KL.KSC.NLST.AS //

"items changed" ,"gauge" ,"ksc_NLST__Adaptive_security__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Adaptive_security__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Adaptive_security__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Adaptive_security__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Adaptive_security__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Adaptive_security__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Adaptive_security__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Adaptive_security__transactions_in_queue"

Adaptive Security State—KL.KSC.NLST.ASS //

"items changed" ,"gauge" ,"ksc_NLST__Adaptive_security_state__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Adaptive_security_state__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Adaptive_security_state__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Adaptive_security_state__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Adaptive_security_state__transactions_queue_full"

transactions queue near to" ,"gauge" ,"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full" "full

"list is pending" ,"gauge" ,"ksc_NLST__Adaptive_security_state__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Adaptive_security_state__transactions_in_queue"

Kill Chain—KL.KSC.NLST.KillChain //

"items changed" ,"gauge" ,"ksc_NLST__Kill_chain__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Kill_chain__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Kill_chain__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Kill_chain__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Kill_chain__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Kill_chain__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Kill_chain__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Kill_chain__transactions_in_queue"

الأحداث الحرجة لخادم الإدارة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تم تجاوز حد الترخيص	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	يتحقق Kaspersky Security Center مرة واحدة يوميًا من تجاوز حد الترخيص. تحدث الأحداث من هذا النوع عند اكتشاف خادم الإدارة حدوث تجاوز لبعض قيود الترخيص بواسطة تطبيقات Kaspersky المثبتة على الأجهزة العميلة وكذلك في حال تجاوز عدد وحدات الترخيص المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد لنسبة 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص. حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). يحدد Kaspersky Security Center القواعد المُستخدمة لإنشاء أحداث عند تجاوز حد الترخيص.	180 يومًا
انتشار الفيروسات	26 (للحماية من تهديدات الملفات)	GNRL_EV_VIRUS_OUTBREAK	تقع الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة قصيرة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة اليتي سيتم تشغيلها عند وقوع هذا الحدث.	180 يومًا
انتشار الفيروسات	27 (للحماية من تهديدات البريد)	GNRL_EV_VIRUS_OUTBREAK	تقع الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة قصيرة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة اليتي سيتم تشغيلها عند وقوع هذا الحدث.	180 يومًا
انتشار الفيروسات	28 (لجدار الحماية)	GNRL_EV_VIRUS_OUTBREAK	تقع الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة قصيرة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة اليتي سيتم تشغيلها عند وقوع هذا الحدث.	180 يومًا
أصبح الجهاز غير مُدار	4111	KLSRV_HOST_OUT_CONTROL	تقع الأحداث من هذا النوع في حالة وجود أي جهاز مُدار مرئيًا على الشبكة، ولكنه غير متصل بخادم الإدارة لفترة محددة. تعرف على ما يمنع التشغيل السليم لعميل الشبكة على الجهاز. تتضمن الأسباب المحتملة حدوث مشكلات في الشبكة وإزالة عميل الشبكة من الجهاز.	180 يومًا
حالة الجهاز حرج	4113	KLSRV_HOST_STATUS_CRITICAL	تحدث الأحداث من هذا النوع عندما يتم تعيين أي جهاز مُدار للحالة حرج. يمكنك تكوين الشروط التي يتم من خلالها تغيير حالة الجهاز إلى حرجة.	180 يومًا
تمت إضافة ملف المفتاح إلى قائمة الرفض	4124	KLSRV_LICENSE_BLACKLISTED	تقع الأحداث من هذا النوع عندما يضيف برنامج Kaspersky رمز التفعيل أو ملف المفتاح الذي تستخدمه في قائمة الرفض. تواصل مع الدعم الفني للحصول على المزيد من التفاصيل.	180 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
وضع الوظائف المحدودة	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	تحدث الأحداث من هذا النوع عند قيام Kaspersky Security Center ببدء التشغيل باستخدام الوظائف الأساسية، دون إدارة الثغرات الأمنية والتصحيحات وكذلك دون مزايا إدارة الجهاز المحمول. في ما يلي أسباب وقوع الحدث والاستجابات المناسبة له: • لقد انتهت فترة الترخيص. يقدم ترخيص لاستخدام وضع الوظائف الكاملة لـ Kaspersky Security Center (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). • يقوم خادم الإدارة بإدارة عدد أجهزة أكبر من المحدد من قبل حد الترخيص. قم بنقل الأجهزة من مجموعات الإدارة الخاصة بخادم الإدارة إلى تلك الخاصة بخادم إدارة آخر (إذا سمح حد الترخيص الخاص بخادم الإدارة الأخر).	180 يومًا
ستنتهي فترة صلاحية الترخيص قريبًا	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	تحدث أحداث من هذا النوع عندما يقترب تاريخ انتهاء صلاحية الترخيص التجاري. يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز تاريخ انتهاء صلاحية الترخيص أم لا بمعدل مرة يوميًا. يتم نشر أحداث من هذا النوع قبل 30 يوم و15يوم و 5 أيام ويوم واحد من تاريخ انتهاء صلاحية الترخيص. لا يمكنك تغيير عدد الأيام. إذا تم إيقاف تشغيل خادم الإدارة في اليوم المحدد قبل تاريخ انتهاء صلاحية الترخيص، فلن يتم نشر الحدث حتى اليوم التالي. عند انتهاء صلاحية الترخيص التجاري، يوفر Kaspersky Security Center الوظائف الأساسية فقط. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تأكد من إضافة مفتاح ترخيص احتياطي إلى خادم الإدارة. • إذا كنت تستخدم اشتراكًا، فتأكد من تجديده. يتم تجديد الاشتراك غير المحدود تلقائيًا في حالة الدفع المسبق لموفر الخدمة في المواعيد المحددة.	180 يومًا
انتهت صلاحية الشهادة	4132	KLSRV_CERTIFICATE_EXPIRED	تقع الأحداث من هذا النوع عند انتهاء صلاحية شهادة العميل على الأجهزة المحمولة.	180 يومًا
انتهت صلاحية شهادة خادم الإدارة.	6129	ServerCertificateExpired	تقع الأحداث من هذا النوع عند انتهاء صلاحية شهادات خادم الإدارة للأجهزة المحمولة وأجهزة UEFI. تحتاج إلى تحديث الشهادة منتهية الصلاحية.	180 يومًا
تم إبطال تحديثات الوحدات النمطية لتطبيق Kaspersky	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	تحدث الأحداث من هذا النوع في حالة إبطال التحديثات المستمرة (يتم عرض حالة الإبطال لتلك التحديثات) بواسطة متخصصين فنيين في Kaspersky؛ لأنه على سبيل المثال يلزم تحديثها إلى إصدار أحدث. يتعلق الحدث بتصحيحات Kaspersky Security Center ولا يتعلق بالوحدات النمطية الخاصة بتطبيقات Kaspersky المُدارة. يقدم الحدث السبب الذي يؤدي إلى عدم تثبيت التحديثات المستمرة.	180 يومًا
Audit: Export to SIEM failed	5130	KLAUD_EV_SIEM_EXPORT_ERROR	تحدث أحداث من هذا النوع عند فشل تصدير الأحداث إلى نظام SIEM بسبب خطأ في الاتصال بنظام SIEM.	180 يومًا

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

يوضح الجدول أدناه أنواع أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **خلل وظيفي**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
حدث خطأ وقت التشغيل	4125	KLSRV_RUNTIME_ERROR	تحدث الأحداث من هذا النوع بسبب حدوث مشكلات غير معروفة. وفي الغالب ما تكون عبارة عن مشكلات DBMS، ومشكلات في الشبكة، ومشكلات أخرى في البرامج والأجهزة. يمكن العثور على تفاصيل الحدث في وصف الحدث.	180 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تم تجاوز حد عمليات تثبيت إحدى مجموعات التطبيقات المرخصة	4126	KLSRV_INVLICPROD_EXCEDED	ينشئ خادم الإدارة أحداث من هذا النوع بشكل دوري (كل ساعة). تحدث الأحداث من هذا النوع في حالة قيامك بإدارة مفاتيح الترخيص لتطبيقات تابعة لجهات خارجية في Kaspersky Security Center وكذلك إذا تجاوز عدد عمليات التثبيت الحد الذي تم تعيينه بواسطة مفتاح الترخيص التابع لجهة خارجية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. قم بحذف التطبيق التابع لجهة خارجية من الأجهزة التي لا يستخدم عليها التطبيق. • قم باستخدام ترخيص تابع لجهة خارجية لعدد أجهزة أكثر. يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة. تشتمل مجموعة التطبيقات المرخصة على التطبيقات التي تفي بالمعايير المحددة بواسطتك.	180 يومًا
فشل استقصاء قطاع السحابة	4143	KLSRV_KLCLOUD_SCAN_ERROR	تحدث الأحداث من هذا النوع عندما يفشل خادم الإدارة في استقصاء مقطع شبكة في بيئة سحابية . اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقًا لذلك.	غير مخزنة
فشل نسخ التحديثات إلى المجلد المحدد	4123	KLSRV_UPD_REPL_FAIL	تحدث الأحداث من هذا النوع عند القيام بنسخ تحديثات البرنامج إلى مجلد (مجلدات) إضافية مشتركة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا كان يحتوي حساب المستخدم المخصص للحصول على إمكانية الوصول إلى المجلد (المجلدات) على أذن كتابي أم لا. • تحقق مما إذا تم تغيير اسم المستخدم و / أو كلمة المرور الخاصة بالمجلد أم لا. • تحقق من الاتصال بالإنترنت لأنه قد يكون السبب في حدوث هذا الحدث. اتبع التعليمات للقيام بتحديث قواعد البيانات والوحدات النمطية للبرامج.	180 يومًا
لا توجد مساحة فارغة على القرص	4107	KLSRV_DISK_FULL	تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة. قم بتحرير مساحة القرص على الجهاز.	180 يومًا
المجلد المشترك غير متاح	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	تحدث الأحداث من هذا النوع في حال عدم توافر المجلد المشترك لخادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا تم تشغيل خادم الإدارة وتوافره (حيث يوجد المجلد المشترك) أم لا. • تحقق مما إذا تم تغيير اسم المستخدم و / أو كلمة المرور الخاصة بالمجلد أم لا. • تحقق من الاتصال بالشبكة.	180 يومًا
قاعدة بيانات خادم الإدارة غير متوفرة	4109	KLSRV_DATABASE_UNAVAILABLE	تحدث الأحداث من هذا النوع في حال أصبحت قاعدة بيانات خادم الإدارة غير متاحة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا كان الخادم البعيد الذي يحتوي على خادم SQL المثبت متاحًا أم لا. • اعرض سجلات DBMS لمعرفة سبب عدم توافر قاعدة بيانات خادم الإدارة. على سبيل المثال، بسبب الصيانة الوقائية قد يكون الخادم البعيد الذي يحتوي على خادم SQL غير متاح.	180 يومًا
لا توجد مساحة فارغة في قاعدة بيانات خادم الإدارة	4110	KLSRV_DATABASE_FULL	تحدث الأحداث من هذا النوع في حالة عدم توافر مساحة فارغة في قاعدة بيانات خادم الإدارة. لا يقوم خادم الإدارة بإداء وظيفته عند وصول قاعدة البيانات الخاصة به إلى سعته وكذلك عند استحالة إجراء المزيد من التسجيلات في قاعدة البيانات. فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـDBMS التي تستخدمها، والاستجابات المناسبة للحدث: • إنك تستخدم خادم SQL Server Express Edition DBMS: في وثيقة SQL Server Express، قم بفحص حد حجم قاعدة البيانات للإصدار الذي تستخدمه. من المحتمل أنه قد تجاوزت قاعدة بيانات خادم الإدارة الخاصة بك حد حجم قاعدة البيانات. يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. في قاعدة بيانات خادم الإدارة، توجد أحداث تجاوز عددها الحد الأقصى أرسلها مكون التحكم في التطبيقات. يمكنك تغيير إعدادات سياسة Kaspersky Endpoint Security for Windows المتعلقة بتخزين حدث التحكم في التطبيقات في قاعدة بيانات خادم الإدارة. • إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition: لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. استعرض المعلومات عند تحديد DBMS.	180 يومًا

أحداث التحذير لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **تحذير**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث التحذير لخادم الإدارة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تم اكتشاف حدث متكرر		KLSRV_EVENT_SPAM_EVENTS_DETECTED	تقع الأحداث من هذا النوع عندما يكتشف خادم الإدارة حدثًا متكررًا على جهاز مُدار. راجع القسم التالي للحصول على التفاصيل: منع الأحداث المتكررة.	90 يومًا
تم تجاوز حد الترخيص	4098	KLSRV_EV_LICENSE_CHECK_100_110	يتحقق Kaspersky Security Center مرة واحدة يوميًا من تجاوز حد الترخيص. تحدث الأحداث من هذا النوع عند اكتشاف خادم الإدارة حدوث تجاوز لبعض قيود الترخيص بواسطة تطبيقات Kaspersky المثبتة على الأجهزة العميلة وكذلك في حال كان عدد وحدات الترخيص المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد يشكل من 100% إلى 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص. حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). يحدد Kaspersky Security Center القواعد المُستخدمة لإنشاء أحداث عند تجاوز حد الترخيص.	90 يومًا
ظل الجهاز غير نشط على الشبكة لوقت طويل	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	تحدث الأحداث من هذا النوع عندما يظهر الجهاز المُدار عدم النشاط لبعض الوقت. يحدث هذا غالبًا عند إيقاف تشغيل الجهاز المُدار. يمكنك الاستجابة للحدث من خلال الطرق التالية: • إزالة الجهاز من قائمة الأجهزة المدارة تلقائيًا. • حدد الفاصل الزمني الذي يتم بعده إنشاء الحدث **ظل الجهاز غير نشط على الشبكة لوقت طويل** باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center Web Console. • حدد الفاصل الزمني الذي يتم بعده إزالة الجهاز تلقائيًا من المجموعة باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center Web Console.	90 يومًا
تعارض في أسماء الجهاز	4102	KLSRV_EVENT_HOSTS_CONFLICT	تحدث الأحداث من هذا النوع عندما يعتبر خادم الإدارة جهازين مُدارين أو أكثر كجهاز واحد. يحدث هذا غالبًا عند استخدام محرك أقراص ثابت مستنسخ لنشر البرامج على الأجهزة المُدارة وبدون تحويل عميل الشبكة إلى وضع استنساخ القرص المخصص على جهاز مرجعي. لتجنب هذه المشكلة، قم بتبديل عميل الشبكة إلى وضع استنساخ القرص على جهاز مرجعي قبل استنساخ محرك الأقراص الثابتة لهذا الجهاز.	90 يومًا
حالة الجهاز 'تحذير'	4114	KLSRV_HOST_STATUS_WARNING	تحدث الأحداث من هذا النوع عندما يتم تعيين الحالة تحذير للجهاز المُدار. يمكنك تكوين الشروط التي يتم من خلالها تغيير حالة الجهاز إلى تحذير.	90 يومًا
سيتم تجاوز حد عمليات التثبيت لإحدى مجموعات التطبيقات المرخصة قريبًا	4127	KLSRV_INVLICPROD_FILLED	تحدث الأحداث من هذا النوع عندما يصل عدد عمليات التثبيت لتطبيقات الطرف الثالث المضمنة في مجموعة التطبيقات المرخصة إلى 90% من الحد الأقصى للقيمة المسموح بها المحددة في خصائص مفتاح الترخيص. يمكنك الاستجابة للحدث من خلال الطرق التالية: • إذا لم يكن تطبيق الطرف الثالث قيد الاستخدام على بعض الأجهزة المدارة، فاحذف التطبيق من هذه الأجهزة. • إذا كنت تتوقع أن يتجاوز عدد عمليات التثبيت لتطبيق الطرف الثالث الحد الأقصى المسموح به في المستقبل القريب، ففكر في الحصول على ترخيص جهة خارجية لعدد أكبر من الأجهزة مقدمًا. يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة.	90 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تم طلب شهادة	4133	KLSRV_CERTIFICATE_REQUESTED	تحدث الأحداث من هذا النوع عندما تفشل إعادة إصدار شهادة إدارة الأجهزة المحمولة تلقائيًا. قد تكون الأسباب والردود المناسبة على الحدث فيما يلي: • تم بدء إعادة الإصدار التلقائي للشهادة التي تم تعطيل خيار **إعادة إصدار الشهادة تلقائيًا إن أمكن**. قد يكون هذا بسبب حدوث خطأ أثناء إنشاء الشهادة. قد يلزم إعادة إصدار الشهادة يدويًا. • إذا كنت تستخدم تكاملاً مع بنية تحتية للمفتاح العام، فقد يكون السبب هو عدم وجود سمة SAM-Account-Name للحساب المستخدم للتكامل مع PKI ولإصدار الشهادة. راجع خصائص الحساب.	90 يومًا
تمت إزالة الشهادة	4134	KLSRV_CERTIFICATE_REMOVED	تحدث الأحداث من هذا النوع عندما يزيل المسؤول أي نوع من الشهادات (عامة، بريد، VPN) لإدارة جهاز المحمول. بعد إزالة الشهادة، ستفشل الأجهزة المحمولة المتصلة عبر هذه الشهادة في الاتصال بخادم الإدارة. قد يكون هذا الحدث مفيدًا عند التحقيق في الأعطال المرتبطة بإدارة الأجهزة المحمولة.	90 يومًا
تنتهي صلاحية الشهادة	6128	ServerCertificateExpiresSoon	تقع الأحداث من هذا النوع عند انتهاء صلاحية شهادات خادم الإدارة للأجهزة المحمولة وأجهزة UEFI. تحتاج إلى تحديث الشهادة منتهية الصلاحية.	90 يومًا
انتهت صلاحية شهادة أسماء نقاط الوصول	4135	KLSRV_APN_CERTIFICATE_EXPIRED	تحدث الأحداث من هذا النوع عند انتهاء صلاحية شهادة APN. تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.	غير مخزنة
ستنتهي صلاحية شهادة أسماء نقاط الوصول قريبًا	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	تحدث الأحداث من هذا النوع عندما يتبقى أقل من 14 يومًا قبل انتهاء صلاحية شهادة APN. عند انتهاء صلاحية شهادة APN، تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. نوصيك بجدولة تجديد شهادة أسماء نقاط الوصول (APNs) قبل تاريخ انتهاء الصلاحية.	غير مخزنة
فشل إرسال رسالة FCM إلى الجهاز المحمول	4138	KLSRV_GCM_DEVICE_ERROR	تقع الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Firebase Cloud Messaging (FMC) للاتصال بأجهزة الجوال المدارة بنظام تشغيل Android ويفشل خادم FMC في التعامل مع بعض الطلبات الواردة من خادم الإدارة. هذا يعني أن بعض الأجهزة المحمولة المدارة لن تتلقى إشعارًا فوريًا. اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقًا لذلك. لمزيد من المعلومات حول رموز HTTP المستلمة من خادم FMC والأخطاء ذات الصلة، يُرجى الرجوع إلى وثائق خدمة Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات").	90 يومًا
حدث خطأ في HTTP أثناء إرسال رسالة FCM إلى خادم FCM	4139	KLSRV_GCM_HTTP_ERROR	تقع الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Firebase Cloud Messaging (FMC) لتوصيل الأجهزة المحمولة المدارة بنظام التشغيل Android ويعود خادم FMC إلى طلب خادم الإدارة برمز HTTP غير 200 (موافق). قد تكون الأسباب والردود المناسبة على الحدث فيما يلي: • مشكلات من جانب خادم FMC. اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقًا لذلك. لمزيد من المعلومات حول رموز HTTP المستلمة من خادم FMC والأخطاء ذات الصلة، يُرجى الرجوع إلى وثائق خدمة Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات"). • مشاكل من جانب الخادم الوكيل (إذا كنت تستخدم خادمًا وكيلاً). اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقًا لذلك.	90 يومًا
فشل إرسال رسالة FCM إلى خادم FCM	4140	KLSRV_GCM_GENERAL_ERROR	تحدث الأحداث من هذا النوع بسبب أخطاء غير متوقعة من جانب خادم الإدارة عند العمل مع بروتوكول Firebase Cloud Messaging HTTP. اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقًا لذلك. إذا لم تتمكن من إيجاد حل لمشكلة ما بنفسك، فنوصيك بالاتصال بالدعم الفني لـ Kaspersky.	90 يومًا
توجد مساحة فارغة قليلة على القرص الصلب	4105	KLSRV_NO_SPACE_ON_VOLUMES	تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة. قم بتحرير مساحة القرص على الجهاز.	90 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
توجد مساحة فارغة قليلة في قاعدة بيانات خادم الإدارة	4106	KLSRV_NO_SPACE_IN_DATABASE	تحدث الأحداث من هذا النوع في حال أصبحت مساحة قاعدة بيانات خادم الإدارة محدودة للغاية. إذا لم يتم إصلاح الوضع، فستصل قاعدة بيانات خادم الإدارة إلى سعتها ولن يقوم خادم الإدارة بأداء وظيفته قريبًا. فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـ DBMS التي تستخدمها، والاستجابات المناسبة للحدث. إنك تستخدم خادم SQL Server Express Edition DBMS: • في وثيقة SQL Server Express، قم بفحص حد حجم قاعدة البيانات للإصدار الذي تستخدمه. من المحتمل أن قاعدة بيانات خادم الإدارة الخاصة بك على وشك الوصول إلى حد حجم قاعدة البيانات. • يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • في قاعدة بيانات خادم الإدارة، توجد أحداث تجاوز عددها الحد الأقصى أرسلها مكون التحكم في التطبيقات. يمكنك تغيير إعدادات سياسة Kaspersky Endpoint Security for Windows المتعلقة بتخزين حدث التحكم في التطبيقات في قاعدة بيانات خادم الإدارة. إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition: • لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. استعرض المعلومات عند تحديد DBMS.	90 يومًا
تمت مقاطعة الاتصال بخادم الإدارة الثانوي	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي. اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الثانوي واستجب وفقًا لذلك.	90 يومًا
تم قطع الاتصال بخادم الإدارة الأساسي	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي. اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الرئيسي واستجب وفقًا لذلك.	90 يومًا
تم تسجيل تحديثات جديدة للوحدات النمطية لتطبيق Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	تحدث أحداث من هذا النوع عندما يسجل خادم الإدارة تحديثات جديدة لبرنامج Kaspersky المثبت على الأجهزة المدارة التي تتطلب الموافقة ليتم تثبيتها. وافق على التحديثات أو ارفضها باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center Web Console.	90 يومًا
تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وبدأت عملية حذف الأحداث	4145	KLSRV_EVP_DB_TRUNCATING	تحدث الأحداث من هذا النوع عند بدء حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد الوصول إلى سعة قاعدة بيانات خادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.	غير مخزنة
تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وتم حذف الأحداث	4146	KLSRV_EVP_DB_TRUNCATED	تحدث الأحداث من هذا النوع عند حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد الوصول إلى سعة قاعدة بيانات خادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • قم بتغيير الحد الأقصى المسموح به لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.	غير مخزنة
التدقيق (فشل اختبار الاتصال بخادم SIEM)	5120	KLAUD_EV_SIEM_TEST_FAILED	تحدث الأحداث من هذا النوع عند فشل اتصال اختبار خادم SIEM.	30 يومًا
فشل إصدار الشهادة تلقائيا		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	يحدث هذا الحدث في حالة حدوث خطأ أثناء إنشاء شهادة عميل لجهاز محمول (جهاز يعمل بموجب بروتوكول محمول).	90 يومًا

الأحداث المعلوماتية لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **معلومات**.

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.	ملاحظات
تم استنفاد أكثر من 90% من هذا المفتاح	4097	KLSRV_EV_LICENSE_CHECK_90	30 يومًا	
تم اكتشاف جهاز جديد	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 يومًا	
تمت إضافة جهاز إلى المجموعة تلقائيًا	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 يومًا	
تم نقل الجهاز تلقائيًا وفقًا لقاعدة	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 يومًا	
تمت إزالة الجهاز من المجموعة: غير نشط على الشبكة لمدة طويلة	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 يومًا	
سيتم تجاوز حد عمليات التثبيت قريبًا (تم استهلاك أكثر من 95%) لأحدى مجموعات التطبيقات المرخصة	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 يومًا	
تم العثور على ملفات ستُترسل إلى Kaspersky للتحليل	4131	KLSRV_APS_FILE_APPEARED	30 يومًا	
تم تغيير معرف مثيل FCM على هذا الجهاز المحمول	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 يومًا	
تم نسخ التحديثات بنجاح إلى المجلد المحدد	4122	KLSRV_UPD_REPL_OK	30 يومًا	
تم إنشاء الاتصال بخادم الإدارة الثانوي	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 يومًا	
تم إنشاء الاتصال بخادم الإدارة الأساسي	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 يومًا	
تم تحديث قواعد البيانات	4144	KLSRV_UPD_BASES_UPDATED	30 يومًا	
تدقيق: تم إنشاء اتصال بخادم الإدارة	4147	KLAUD_EV_SERVERCONNECT	30 يومًا	
تدقيق: تم تعديل الكائن	4148	KLAUD_EV_OBJECTMODIFY	30 يومًا	يتتبع هذا الحدث التغييرات في العناصر التالية: • مجموعة الإدارة • مجموعة الأمان • المستخدم • الحزمة • المهمة • سياسة • الخادم • الخادم الافتراضي
تدقيق: تم تغيير حالة الكائن	4150	KLAUD_EV_TASK_STATE_CHANGED	30 يومًا	على سبيل المثال، يقع هذا الحدث عندما تفشل مهمة مع وجود خطأ.
تدقيق: تم تعديل إعدادات المجموعة	4149	KLAUD_EV_ADMGROUP_CHANGED	30 يومًا	
التدقيق: تم إنهاء الاتصال بخادم الإدارة	4151	KLAUD_EV_SERVERDISCONNECT	30 يومًا	
التدقيق: تم تعديل خصائص الكائن	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 يومًا	يتتبع هذا الحدث التغييرات في الخصائص التالية: • المستخدم • الترخيص • الخادم • الخادم الافتراضي
التدقيق: تم تعديل أذونات المستخدم	4153	KLAUD_EV_OBJECTACLMODIFIED	30 يومًا	
تدقيق: تم استيراد مفاتيح التشفير أو تصديرها من خادم الإدارة	5100	KLAUD_EV_DPEKEYSEXPORT	30 يومًا	
التدقيق (نجح اختبار الاتصال بخادم SIEM)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 يومًا	يحدث هذا الحدث عندما ينجح اتصال اختبار خادم SIEM.

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.	ملاحظات
تم إنشاء الشهادة الاحتياطية		ServerReserveCertificateCreated	30 يومًا	يقع هذا الحدث عندما يتم إنشاء شهادة خادم الإدارة.
تجديد الشهادة		ServerCertificateRenewed	30 يومًا	يقع هذا الحدث عند تجديد شهادة خادم الإدارة.
تم إصدار الشهادة تلقائيًا بنجاح		KLSRV_CERTIFICATE_AUTO_ISSUED	30 يومًا	يحدث هذا الحدث عندما يتم إنشاء شهادة لجهاز محمول (جهاز يعمل بموجب بروتوكول محمول) بنجاح.

يتم نشر أحداث **تم إنشاء الشهادة الاحتياطية وتجديد الشهادة وتم إصدار الشهادة تلقائيًا بنجاح** تلقائيًا بواسطة خادم الإدارة ويتم عرضها في وحدة تحكم الإدارة فقط عند تنفيذ العمليات المقابلة لهذه الأحداث لشهادات خادم الإدارة للأجهزة المحمولة وأجهزة UEFI.

أحداث عميل الشبكة

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بعميل الشبكة.

أحداث الخلل الوظيفي لعميل الشبكة

يوضح الجدول أدناه أنواع حدث عميل شبكة Kaspersky Security Center التي تندرج ضمن مستوى خطورة **خلل وظيفي**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث الخلل الوظيفي لعميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
خطأ في تثبيت التحديث	7702	KLNAG_EV_PATCH_INSTALL_ERROR	تحديث الأحداث من هذا النوع في حالة عدم نجاح التحديث والتصحيح التلقائي لمكونات Kaspersky Security Center. لا يتعلق الحدث بعمليات تحديث تطبيقات Kaspersky المُدارة. اقرأ وصف الحدث. قد يرجع ظهور هذا الحدث إلى حدوث مشكلة في Windows على خادم الإدارة. إذا ذكر الوصف أي مشكلة تتعلق بتكوين Windows، فقم بحل هذه المشكلة.	30 يومًا
فشل تثبيت تحديث برامج الجهة الخارجية	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	تحدث الأحداث من هذا النوع في حالة استخدام مزايا إدارة الثغرات الأمنية والتصحيحات وإدارة جهاز المحمول وإذا لم ينجح تحديث البرامج التابعة لجهة خارجية. تحقق من صحة الرابط الخاص بالبرامج التابعة لجهة خارجية. اقرأ وصف الحدث.	30 يومًا
فشل تثبيت تحديثات Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	تحدث الأحداث من هذا النوع في حالة عدم نجاح تحديثات Windows. يمكنك تكوين تحديثات Windows في سياسة عميل الشبكة. اقرأ وصف الحدث. ابحث عن الخطأ في قاعدة معارف Microsoft. واتصل بالدعم الفني لـ Microsoft إذا تعذر عليك حل المشكلة بنفسك.	30 يومًا
User management: errors	7723	KLNAG_EV_USR_MNG_ERR	حدث تحذير عام.	30 يومًا
Failed to restore sudoers file to reference value	7726	KLNAG_EV_SUDOER_RESTORED_ERR	يحتوي الحدث على وصف لخطأ استبدال ملف sudoers.	30 يومًا
Failed to install root certificates	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	يحتوي الحدث على وصف خطأ تثبيت الشهادات.	30 يومًا
Failed to remove root certificates	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	يحتوي الحدث على وصف لخطأ إزالة الشهادات.	30 يومًا

أحداث تحذير عميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تندرج ضمن مستوى خطورة **تحذير**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث تحذير عميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
ظهر تحذير أثناء تثبيت تحديث الوحدة النمطية للبرامج	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 يومًا
اكتمل تثبيت تحديث برامج الجهة الخارجية مع وجود تحذير	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 يومًا
تم تأجيل تثبيت تحديث برامج الجهة الخارجية	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 يومًا
حدثت مشكلة أمنية	549	GNRL_EV_APP_INCIDENT_OCCURED	30 يومًا
بدأ وكيل KSN. فشل فحص مدى توفر KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 يومًا
User management: warnings	7722	KLNAG_EV_USR_MNG_WRN	30 يومًا
Sudoers file found doesn't match reference value	7724	KLNAG_EV_SUDOER_DIFFERENT	30 يومًا

الأحداث المعلوماتية لعميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تندرج ضمن مستوى خطورة **معلومات**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

الأحداث المعلوماتية لعميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم تثبيت تحديث الوحدات النمطية للبرامج بنجاح	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 يومًا
بدأ تثبيت تحديث الوحدة النمطية للبرامج	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 يومًا
تم تثبيت التطبيق	7703	KLNAG_EV_INV_APP_INSTALLED	30 يومًا
تم إلغاء تثبيت التطبيق	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 يومًا
تم تثبيت التطبيق المراقب	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 يومًا
تم إلغاء تثبيت التطبيق المراقب	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 يومًا
تم تثبيت التطبيق التابع لجهة خارجية	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 يومًا
تمت إضافة جهاز جديد	7708	KLNAG_EV_DEVICE_ARRIVAL	30 يومًا
تمت إزالة الجهاز	7709	KLNAG_EV_DEVICE_REMOVE	30 يومًا
تم اكتشاف جهاز جديد	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 يومًا
تم اعتماد الجهاز	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 يومًا
مشاركة سطح المكتب لـ Windows: تمت قراءة الملف	7712	KLUSRLOG_EV_FILE_READ	30 يومًا
مشاركة سطح المكتب لـ Windows: تم تعديل الملف	7713	KLUSRLOG_EV_FILE_MODIFIED	30 يومًا
مشاركة سطح المكتب لـ Windows: تم بدء التطبيق	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 يومًا
مشاركة سطح المكتب لـ Windows: تم البدء	7715	KLUSRLOG_EV_WDS_BEGIN	30 يومًا
مشاركة سطح المكتب لـ Windows: تم الإيقاف	7716	KLUSRLOG_EV_WDS_END	30 يومًا
تم تثبيت تحديث برامج الجهات الخارجية بنجاح	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 يومًا
تم بدء تثبيت تحديث برامج الجهة الخارجية	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
بدأ وكيل KSN. اكتمل فحص مدى توفر KSN بنجاح	7719	KSNPROXY_STARTED_CON_CHK_OK	30 يومًا
توقف وكيل شبكة KSN	7720	KSNPROXY_STOPPED	30 يومًا

أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لـ Kaspersky Security Center التي تندرج ضمن مستوى الخطورة **خلل وظيفي**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
فشل في طلب قائمة ملفات التعريف	PROFILELIST_COMMAND_FAILED	30 يومًا
فشل في تثبيت ملف التعريف	INSTALLPROFILE_COMMAND_FAILED	30 يومًا
فشل في إزالة ملف التعريف	REMOVEPROFILE_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة ملفات تعريف التزويد	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 يومًا
فشل في تثبيت ملف تعريف التزويد	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 يومًا
فشل في إزالة ملف تعريف التزويد	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة الشهادات الرقمية	CERTIFICATELIST_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة التطبيقات المثبتة	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 يومًا
فشل في طلب المعلومات العامة بشأن الجهاز المحمول	DEVICEINFORMATION_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة معلومات الأمان	SECURITYINFO_COMMAND_FAILED	30 يومًا
فشل في قفل الجهاز المحمول	DEVICELOCK_COMMAND_FAILED	30 يومًا
فشل في إعادة تعيين كلمة المرور	CLEARPASSCODE_COMMAND_FAILED	30 يومًا
فشل في مسح البيانات من الجهاز المحمول	ERASEDEVICE_COMMAND_FAILED	30 يومًا
فشل في تثبيت التطبيق	INSTALLAPPLICATION_COMMAND_FAILED	30 يومًا
فشل في تعيين رمز الاسترداد للتطبيق	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة التطبيقات المُدارة	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 يومًا
فشل في إزالة التطبيق المُدار	REMOVEAPPLICATION_COMMAND_FAILED	30 يومًا
تم رفض إعدادات التجوال	SETROAMINGSETTINGS_COMMAND_FAILED	30 يومًا
حدث خطأ في تشغيل التطبيق	PRODUCT_FAILURE	30 يومًا
تحتوي نتيجة الأمر على بيانات غير صالحة	MALFORMED_COMMAND	30 يومًا
فشل في إرسال إشعار الدفع	SEND_PUSH_NOTIFICATION_FAILED	30 يومًا
فشل في إرسال الأمر	SEND_COMMAND_FAILED	30 يومًا
لم يتم العثور على الجهاز	DEVICE_NOT_FOUND	30 يومًا

أحداث التحذير لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لـ Kaspersky Security Center التي تندرج ضمن مستوى خطورة **تحذير**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث التحذير لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم اكتشاف محاولة توصيل جهاز محمول مقفل	INACTICE_DEVICE_TRY_CONNECTED	30 يومًا
تم إزالة ملف التعريف	MDM_PROFILE_WAS_REMOVED	30 يومًا
تم اكتشاف محاولة إعادة استخدام شهادة عميل.	CLIENT_CERT_ALREADY_IN_USE	30 يومًا
تم اكتشاف جهاز غير مفعل.	FOUND_INACTIVE_DEVICE	30 يومًا
رمز الاسترداد مطلوب.	NEED_REDEMPTION_CODE	30 يومًا
تم تضمين ملف التعريف في سياسة تمت إزالتها من الجهاز.	UMDM_PROFILE_WAS_REMOVED	30 يومًا

الأحداث المعلوماتية لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لـ Kaspersky Security Center التي تندرج ضمن مستوى خطورة **معلومات**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

الأحداث المعلوماتية لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم توصيل جهاز محمول جديد.	NEW_DEVICE_CONNECTED	30 يومًا
تم طلب قائمة بملفات التعريف بنجاح.	PROFILELIST_COMMAND_SUCCESSFULL	30 يومًا
تم تثبيت ملف التعريف بنجاح.	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تمت إزالة ملف التعريف بنجاح.	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة بملفات تعريف التزويد بنجاح.	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 يومًا
تم تثبيت ملف تعريف التزويد بنجاح.	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تم إزالة ملف تعريف التزويد بنجاح.	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة بالشهادات الرقمية بنجاح.	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة بالتطبيقات المثبتة بنجاح.	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 يومًا
تم طلب المعلومات العامة بشأن الجهاز المحمول بنجاح.	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 يومًا
تم طلب معلومات الأمان بنجاح.	SECURITYINFO_COMMAND_SUCCESSFULL	30 يومًا
تم قفل الجهاز المحمول بنجاح.	DEVICELOCK_COMMAND_SUCCESSFULL	30 يومًا
تمت إعادة تعيين كلمة المرور بنجاح.	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 يومًا
تم مسح البيانات من الجهاز المحمول.	ERASEDEVICE_COMMAND_SUCCESSFULL	30 يومًا
تم تثبيت التطبيق بنجاح.	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 يومًا
تم تعيين رمز الاسترداد الخاص بالتطبيق بنجاح.	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة التطبيقات المُدارة بنجاح.	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 يومًا

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تمت إزالة التطبيق المدار بنجاح.	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 يومًا
تم تطبيق إعدادات التجوال بنجاح.	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 يومًا

حظر الأحداث المتكررة

يوفر هذا القسم معلومات حول إدارة حظر الأحداث المتكررة، وحول إزالة حظر الأحداث المتكررة، وحول تصدير قائمة الأحداث المتكررة إلى ملف.

حول حظر الأحداث المتكررة

التطبيق المُدار، على سبيل المثال، Kaspersky Endpoint Security for Windows، المثبت على جهاز مدار واحد أو عدة أجهزة مُدارة يمكنه إرسال الكثير من الأحداث من نفس النوع إلى خادم الإدارة. تلقي أحداث متكررة قد يؤدي إلى زيادة التحميل على قاعدة بيانات خادم الإدارة والكتابة فوق أحداث أخرى. يبدأ خادم الإدارة في حظر الأحداث الجماعية عندما يتجاوز مقدار كل الأحداث المستلمة الحد المحدد لقاعدة البيانات.

يحظر خادم الإدارة الأحداث المتكررة من الاستلام تلقائيًا. لا يمكنك حظر الأحداث المتكررة بنفسك، أو اختر الأحداث التي ترغب في حظرها.

إذا كنت ترغب في معرفة ما إذا تم حظر حدث أم لا، يمكنك التحقق مما إذا كان هذا الحدث موجودًا في قسم **حظر الأحداث المتكررة** في خصائص خادم الإدارة. في النافذة، يمكنك إجراء ما يلي:

- إذا كنت ترغب في منع الكتابة فوق قاعدة البيانات، يمكنك ذلك الاستمرار في حظر استلام مثل هذا النوع من الأحداث.
- إذا كنت ترغب، على سبيل المثال، في معرفة سبب إرسال الأحداث المتكررة إلى خادم الإدارة، يمكنك رفع الحظر عن الأحداث المتكررة والاستمرار في استقبال أحداث من هذا النوع على أي حال.
- إذا كنت ترغب في الاستمرار في تلقي الأحداث المتكررة حتى يتم حظرها مرة أخرى، يمكنك رفع الحظر عن الأحداث المتكررة.

إدارة حظر الأحداث المتكررة

يقوم خادم الإدارة تلقائيًا بحظر تلقي الأحداث المتكررة، ولكن يمكنك إيقاف الحظر والاستمرار في تلقي الأحداث المتكررة. يمكنك كذلك حظر تلقي الأحداث المتكررة التي قمت بإلغاء حظرها من قبل.

لإدارة منع الأحداث المتكررة:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.
2. في نافذة خصائص خادم الإدارة، انتقل إلى لوحة **الأقسام** وبعدها حدد **حظر الأحداث المتكررة**.
3. في قسم **حظر الأحداث المتكررة**:
   - حدد خيارات **نوع الحدث** للأحداث التي ترغب في حظر استلامها.
   - الغ تحديد خيارات **نوع الحدث** للأحداث التي ترغب في الاستمرار في استلامها.
4. انقر على زر **تطبيق**.
5. انقر على زر **موافق**.

خادم الإدارة يستلم الأحداث المتكررة التي قمت بإلغاء تحديد خيار **نوع الحدث** لها ويحظر استلام الأحداث المتكررة التي حددت خيار **نوع الحدث** لها.

إزالة حظر الأحداث المتكررة

يمكنك إزالة حظر الأحداث المتكررة والبدء في استلامها حتى يقوم خادم الإدارة بحظر هذا النوع من الأحداث المتكررة مرة أخرى.

لإزالة حظر الأحداث المتكررة:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.
2. في نافذة خصائص خادم الإدارة، انتقل إلى لوحة **الأقسام** وبعدها حدد **حظر الأحداث المتكررة**.
3. في قسم **حظر الأحداث المتكررة**، انقر على صف الحدث المتكرر الذي ترغب في إزالة الحظر عنه.
4. انقر على زر **حذف**.

بهذا تم حذف الحدث المتكرر من قائمة الأحداث المتكررة. سيستلم خادم الإدارة أحداثًا من هذا النوع.

تصدير قائمة بالأحداث المتكررة إلى ملف

لتصدير قائمة بالأحداث المتكررة إلى ملف:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.
2. في نافذة خصائص خادم الإدارة، انتقل إلى لوحة **الأقسام** وبعدها حدد **حظر الأحداث المتكررة**.
3. انقر على زر **تصدير إلى الملف**.
4. في **نافذة** حفظ باسم التي تفتح، حدد المسار إلى الملف الذي تريد استيراد المهمة منه.
5. انقر على زر **حفظ**.

يتم تصدير جميع السجلات الموجودة في قائمة الأحداث المتكررة إلى ملف.

التحكم في التغييرات في حالة الأجهزة الظاهرية

يقوم خادم الإدارة بتخزين معلومات حول حالة الأجهزة المُدارة، مثل سجل الأجهزة وقائمة التطبيقات المثبتة أو إعدادات التطبيقات والمهام والسياسات المدارة. إذا كان جهاز ظاهري يعمل كجهاز مُدار، فيمكن للمستخدم استعادة حالته في أي وقت باستخدام لقطة الجهاز الظاهري التي تم إنشائها مسبقًا. يمكن أن تصبح المعلومات حول حالة الجهاز الظاهري على خادم الإدارة قديمة.

على سبيل المثال، قام المسؤول بإنشاء سياسة حماية على خادم الإدارة في الساعة 00:12 مساءً، والتي ستبدأ على الجهاز الافتراضي VM_1 في تمام الساعة 01:12 مساءً. وفي تمام الساعة 30:12 مساءً، قام مستخدم الجهاز الافتراضي VM_1 بتغيير حالته باستعادتها من لقطة تم إجراؤها في تمام الساعة 00:11 صباحًا. وتتوقف سياسة الحماية عن العمل على الجهاز الافتراضي. ومع ذلك، تنص المعلومات القديمة المخزنة على خادم الإدارة على أن سياسة الحماية على الجهاز الظاهري VM_1 لا تزال قيد المتابعة.

يتيح لك Kaspersky Security Center مراقبة جميع التغييرات في حالة الأجهزة الافتراضية.

وبعد كل مزامنة مع جهاز، يقوم خادم الإدارة بإنشاء معرف فريد، والذي يتم تخزينه على الجهاز وخادم الإدارة. قبل بدء المزامنة التالية، يقوم خادم الإدارة بمزامنة قيم هذه المعرفات على الجانبين. في حالة عدم تطابق قيم المعرفات، يتعرف خادم الإدارة على الجهاز الظاهري على أنه تمت استعادته من لقطة. يقوم خادم الإدارة بإعادة تعيين جميع إعدادات السياسات والمهام المفعلة للجهاز الظاهري وإرساله السياسات الحديثة وقائمة مهام المجموعة.

مراقبة حالة الحماية ضد الفيروسات باستخدام معلومات من سجل النظام

لمراقبة حالة الحماية ضد الفيروسات على جهاز عميل باستخدام المعلومات المسجلة بواسطة عميل الشبكة، بناءً على نظام التشغيل للجهاز:

- على الأجهزة التي تعمل بنظام Windows:

1. افتح سجل النظام الخاص بالجهاز العميل (على سبيل المثال، محليًا، باستخدام الأمر regedit من القائمة **بدء** > **تشغيل**).

2. انتقل إلى الخلية التالية:

- لأنظمة 32 بت:

AVState\Statistics\1.0.0.0\1103\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE

- لأنظمة 64 بت:

:ics\1.0.0.0\1103\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE

يعرض سجل النظام معلومات حول حالة الحماية ضد الفيروسات الخاصة بالجهاز العميل.

- على الأجهزة التي تعمل بنظام Linux:

- يتم تضمين المعلومات في ملفات نصية منفصلة، واحد لكل نوع من البيانات، وتقع في / ./var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState

- على الأجهزة التي تعمل بنظام macOS:

- يتم تضمين المعلومات في ملفات نصية منفصلة، واحد لكل نوع من البيانات، وتقع في /Library/Application Support/Kaspersky ./Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState

تتطابق حالة الحماية ضد الفيروسات مع قيم المفاتيح الموصوفة في الجدول التالي.

مفاتيح التسجيل وقيمها المحتملة

المفتاح (نوع البيانات)	القيمة	الوصف
(REG_SZ) Protection_LastConnected	DD-MM-YYYY HH-MM-SS	التاريخ والوقت (بتنسيق UTC) لآخر اتصال بخادم الإدارة
(REG_SZ) Protection_AdmServer	IP أو اسم DNS أو اسم NetBIOS	اسم خادم الإدارة الذي يُدير الجهاز
(REG_SZ) Protection_NagentVersion	a.b.c.d	بناء رقم عميل الشبكة المثبت على الجهاز
Protection_NagentFullVersion (REG_SZ)	a.b.c.d (patch1؛ patch2؛ ...؛ patchN)	العدد الكامل لإصدار عميل الشبكة (مع تصحيحات) المثبتة على الجهاز
(REG_SZ) Protection_HostId	مُعرِّف الجهاز	معرف الجهاز
(REG_DWORD) Protection_DynamicVM	0 - لا 1 - نعم	يتم تثبيت عميل الشبكة في الوضع الديناميكي للبنية الأساسية لسطح المكتب الافتراضي (VDI)
(REG_DWORD) Protection_AvInstalled	0 - لا 1 - نعم	يوجد تطبيق أمن مثبت على الجهاز
(REG_DWORD) Protection_AvRunning	0 - لا 1 - نعم	تم تمكين الحماية في الوقت الحقيقي على الجهاز
(REG_DWORD) Protection_HasRtp	0 - لا 1 - نعم	يتم تثبيت مكون الحماية في الوقت الحقيقي

المفتاح (نوع البيانات)	القيمة	الوصف
(REG_DWORD) Protection_RtpState	حالة الحماية في الوقت الحقيقي:	
	0	غير معروف
	1	معطل
	2	متوقف مؤقتًا
	3	يجري البدء
	4	مُمكّن
	5	ممكّن مع مستوى مرتفع من الحماية (حماية القصوى)
	6	ممكّن مع انخفاض مستوى الحماية (السرعة القصوى)
	7	ممكّن مع الإعدادات الافتراضية (مستحسن)
	8	ممكّن مع الإعدادات المخصصة
	9	فشلت العملية
(REG_SZ) Protection_LastFscan	DD-MM-YYYY HH-MM-SS	التاريخ والوقت (بتنسيق UTC) لآخر فحص كامل
(REG_SZ) Protection_BasesDate	DD-MM-YYYY HH-MM-SS	التاريخ والوقت (تنسيق UTC) لإصدار قواعد بيانات التطبيق

عرض وتكوين الإجراءات عندما تكون حالة الأجهزة غير نشطة

إذا كانت الأجهزة العميلة ضمن مجموعة ما غير نشطة، فبإمكانك الحصول على إشعارات عنها. يمكنك أيضًا حذف مثل هذه الأجهزة تلقائيًا.

لعرض أو تكوين الإجراءات عندما تكون حالة الأجهزة في المجموعة غير نشطة:

1. في شجرة وحدة التحكم، انقر بزر الماوس الأيمن فوق اسم مجموعة الإدارة المطلوبة.
2. في قائمة السياق، حدد **خصائص**.

   يفتح ذلك نافذة خصائص مجموعة الإدارة.
3. في نافذة **الخصائص**، انتقل إلى القسم **الأجهزة**.
4. إذا لزم الأمر، قم بتمكين أو تعطيل الخيارات التالية:

- **إخطار المسؤول إذا ظل الجهاز غير نشط لمدة تزيد عن (بالأيام)**

إذا تم تمكين هذا الخيار، فسوف يتلقى المسؤول إشعارات حول الأجهزة غير المفعلة. يمكنك تحديد الفاصل الزمني الذي يتم بعد حلوله إنشاء حدث **استمر الجهاز في حالة عدم النشاط على الشبكة منذ فترة طويلة**. الفاصل الزمني الافتراضي هو 7 أيام.

يتم تمكين هذا الخيار افتراضيًا.

- **إزالة الجهاز من المجموعة إذا ظل غير نشط لمدة تزيد عن (بالأيام)**

إذا تم تمكين هذا الخيار، فيمكنك تحديد الفترة الزمنية التي يتم بعدها إزالة الجهاز تلقائيًا من المجموعة. الفاصل الزمني الافتراضي هو 60 أيام.

يتم تمكين هذا الخيار افتراضيًا.

- **توريث من المجموعة الأصلية**

سيتم توريث الإعدادات الموجودة في هذا القسم من المجموعة الرئيسية التي تم تضمين الجهاز العميل بها. إذا تم تمكين هذا الخيار، فسيتم قفل الإعدادات الموجودة ضمن **نشاط الجهاز على الشبكة** من إحداث أي تغييرات.

يكون هذا الخيار متاحًا فقط إذا كانت مجموعة الإدارة لديها مجموعة رئيسية.

يتم تمكين هذا الخيار افتراضيًا.

- **فرض التوريث في المجموعات الفرعية**

سيتم توزيع قيم الإعداد إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم قفل هذه الإعدادات.

يتم تعطيل هذا الخيار افتراضيًا.

5. انقر على**موافق**.

تم حفظ وتطبيق التغييرات الخاصة بك.

تعطيل أخبار Kaspersky

في Kaspersky Security Center Web Console، قسم أخبار Kaspersky (**Monitoring & reporting** ← **أخبار Kaspersky**)يبقيك على اطلاع من خلال توفير المعلومات المتعلقة بإصدار Kaspersky Security Center لديك والتطبيقات المدارة المثبتة على الأجهزة المدارة. إذا كنت لا ترغب في تلقي أخبار Kaspersky، يمكنك تعطيل هذه الميزة.

أخبار Kaspersky تشمل نوعين من المعلومات: الأخبار المتعلقة بالأمان والأخبار التسويقية. يمكنك تعطيل الأخبار من كل نوع على حدة.

لتعطيل الأخبار المتعلقة بالأمان:

1. في شجرة وحدة التحكم، حدد خادم الإدارة الذي ترغب في تعطيل الأخبار المتعلقة بالأمان له.
2. انقر بزر الماوس الأيمن، وحدد **خصائص** في قائمة السياق التي تظهر.
3. في نافذة خصائص خادم الإدارة التي تفتح، في قسم **إعلامات Kaspersky**، قم بتعطيل خيار **تمكين عرض أخبار Kaspersky في Kaspersky Security Center Web Console**.
4. انقر فوق **موافق**.

بهذا تم تعطيل أخبار Kaspersky.

يتم تعطيل الأخبار التسويقية افتراضيًا. أنت لا تتلقى أخبار تسويقية إلا إذا قمت بتمكين Kaspersky Security Network (KSN). يمكنك تعطيل هذا النوع من الأخبار عن طريق تعطيل KSN.

تعديل نقاط التوزيع وبوابات الاتصال

تُجري بنية مجموعات الإدارة في Kaspersky Security Center الوظائف التالية:

- تعيين نطاق السياسات.

توجد طريقة بديلة لتطبيق مجموعات الإعدادات ذات الصلة على الأجهزة، عن طريق استخدام ملفات تعريف السياسة. في هذه الحالة، يمكنك تعيين نطاق السياسات باستخدام العلامات أو مواقع الجهاز في الوحدات التنظيمية لـ Active Directory والعضوية في مجموعات الأمان الخاصة بـ Active Directory.

- تعيين نطاق المهام الجماعية

يوجد نهج لتحديد نطاق المهام الجماعية غير المستندة إلى التسلسل الهرمي لمجموعات الإدارة: استخدام المهام لتحديدات الأجهزة والمهام لأجهزة محددة.

- تعيين حقوق الوصول إلى الأجهزة وخوادم الإدارة الافتراضية وخوادم الإدارة الثانوية.
- تعيين نقاط التوزيع

عند بناء بنية مجموعات الإدارة، يجب عليك الأخذ في الاعتبار مخطط شبكة المؤسسة للتعيين الأمثل لنقاط التوزيع. يتيح التوزيع المثالي لنقاط التوزيع توفير الحركة على شبكة المؤسسة.

بناءً على المخطط المؤسسي ومخطط الشبكة، يمكن تطبيق التكوينات القياسية التالية على بنية مجموعات الإدارة:

- مكتب واحد
- مكاتب صغيرة متعددة بعيدة

يجب أن تكون الأجهزة التي تعمل كنقاط توزيع محمية، بما في ذلك الحماية الفعلية، وضد أي وصول غير مصرح به.

التكوين القياسي لنقاط التوزيع: مكتب واحد

في التكوين القياسي "مكتب واحد"، تكون كل الأجهزة داخل شبكة المؤسسة ويمكنها "رؤية" بعضها البعض. قد تتكون شبكة المؤسسة من عدد قليل من أجزاء منفصلة (الشبكات أو قطاعات الشبكة) التي ترتبط من خلال قنوات ضيقة.

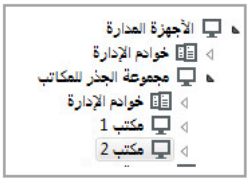
يمكن أن تتوفر الطرق التالية لبناء بنية مجموعات الإدارة:

- بناء بنية مجموعات الإدارة مع الأخذ في الاعتبار مخطط الشبكة. قد لا تعكس بنية مجموعات الإدارة مخطط الشبكة بالدقة المطلقة. قد يكون التطابق بين الأجزاء المنفصلة للشبكة ومجموعات الإدارة المحددة كافيًا. يمكنك استخدام التعيين التلقائي لنقاط التوزيع أو تعيينها يدويًا.
- بناء بنية مجموعات الإدارة دون أخذ مخطط الشبكة في الاعتبار. في هذه الحالة، يجب عليك تعطيل التعيين التلقائي لنقاط التوزيع ثم تعيين جهاز واحد أو عدة أجهزة للعمل كنقاط توزيع لمجموعة إدارة الجذر في كل جزء من الأجزاء المنفصلة للشبكة، على سبيل المثال، لمجموعة **الأجهزة المُدارة**. ستكون جميع نقاط التوزيع عند نفس المستوى وستتميز بنفس النطاق لتغطي جميع الأجهزة في شبكة المؤسسة. في هذه الحالة، سيتصل كل من عميل الشبكة بنقطة التوزيع التي تحتوي على أقصر مسار. يمكن تتبع المسار إلى نقطة توزيع عن طريق الأداة المساعدة tracert.

التكوين القياسي لنقاط التوزيع: مكاتب صغيرة متعددة بعيدة

يقدم هذا التكوين القياسي عدد من المكاتب الصغيرة البعيدة، والتي قد تتصل بالمكتب الرئيسي عبر الإنترنت. كل مكتب بعيد موجود وراء NAT، بمعنى أن الاتصال من مكتب بعيد إلى مكتب آخر غير ممكن لأن الأجهزة معزولة عن بعضها.

يجب أن ينعكس هذا التكوين في بنية مجموعات الإدارة: يجب إنشاء مجموعة إدارة منفصلة لكل مكتب بعيد (المجموعات **المكتب 1** و**المكتب 2** في الشكل الموجود أدناه).



يتم تضمين المكاتب البعيدة في بنية مجموعة الإدارة

يجب تعيين نقطة توزيع واحدة أو عدة نقاط توزيع لكل مجموعة إدارة مقابلة لمكتب ما. يجب أن تكون نقاط التوزيع أجهزة موجودة في المكتب البعيد تحتوي على مساحة قرص خالية كافية. ستتمكن الأجهزة التي تم نشرها في المجموعة **المكتب 1** على سبيل المثال، من الوصول إلى نقاط التوزيع المعينة لمجموعة الإدارة **المكتب 1**.

إذا كان بعض المستخدمين يتنقلون فعليًا بين المكاتب مع أجهزة الكمبيوتر المحمولة الخاصة بهم، فيجب عليك تحديد جهازين أو أكثر (بالإضافة إلى نقاط التوزيع الحاليين) في كل مكتب بعيد وتعيينهم للعمل كنقاط توزيع لمجموعة إدارة من المستوى الأعلى (**المجموعة الجذر للمكاتب** في الشكل الموجود أعلاه).

مثال: جهاز كمبيوتر محمول تم نشره في مجموعة الإدارة **المكتب 1** ثم انتقل فعليًا إلى مكتب مقابل لمجموعة الإدارة **المكتب 2**. بعد انتقال جهاز الكمبيوتر المحمول، يحاول عميل الشبكة الوصول إلى نقاط التوزيع المعينة إلى المجموعة **المكتب 1**، إلا إن هذه النقاط تكون غير متاحة. آنذاك، يحاول عميل الشبكة الوصول إلى نقاط التوزيع التي تم تعيينها إلى **المجموعة الجذر للمكاتب**. ولأن المكاتب البعيدة معزولة عن بعضها، فإن محاولات الوصول إلى نقاط التوزيع المعينة إلى مجموعة الإدارة **المجموعة الجذر للمكاتب** لن تكون ناجحة إلا عند محاولة عميل الشبكة الوصول إلى نقاط التوزيع في مجموعة **المكتب 2**. بمعنى أن جهاز الكمبيوتر المحمول سيظل في مجموعة الإدارة المقابلة للمكتب الأولي، ولكن جهاز الكمبيوتر المحمول سيستخدم نقطة التوزيع الخاصة بالمكتب الذي يوجد فيه فعليًا في الوقت الحالي.

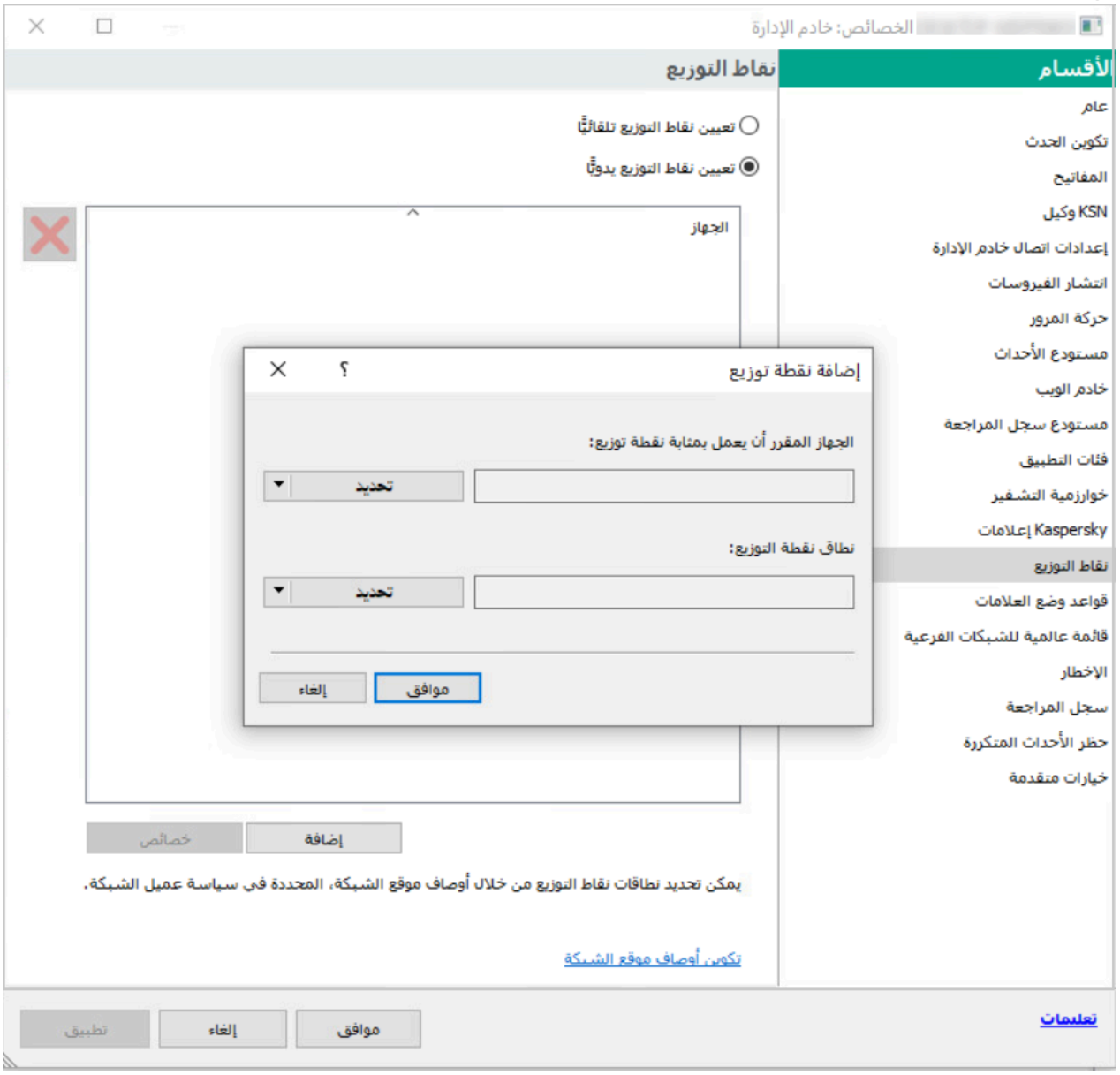
تعيين جهاز مُدار يعمل كنقطة توزيع

يمكنك تعيين جهاز بشكل يدوي للعمل كنقطة توزيع في مجموعة الإدارة، وتكوينه للعمل كبوابة اتصال في وحدة تحكم الإدارة.

لتعيين جهاز كنقطة توزيع لمجموعة إدارة:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.
2. في قائمة السياق بخادم الإدارة، حدد **خصائص**.
3. في نافذة خصائص خادم الإدارة، حدد القسم **نقاط التوزيع**.
4. في الجزء الأيمن من النافذة، حدد خيار **تعيين نقاط التوزيع يدويًا**.

5. انقر على الزر **إضافة**.



تعيين نقطة توزيع يدويًا

يؤدي ذلك إلى فتح النافذة **إضافة نقطة توزيع**.

6. في النافذة **إضافة نقطة توزيع**، قم بتنفيذ الإجراءات التالية:

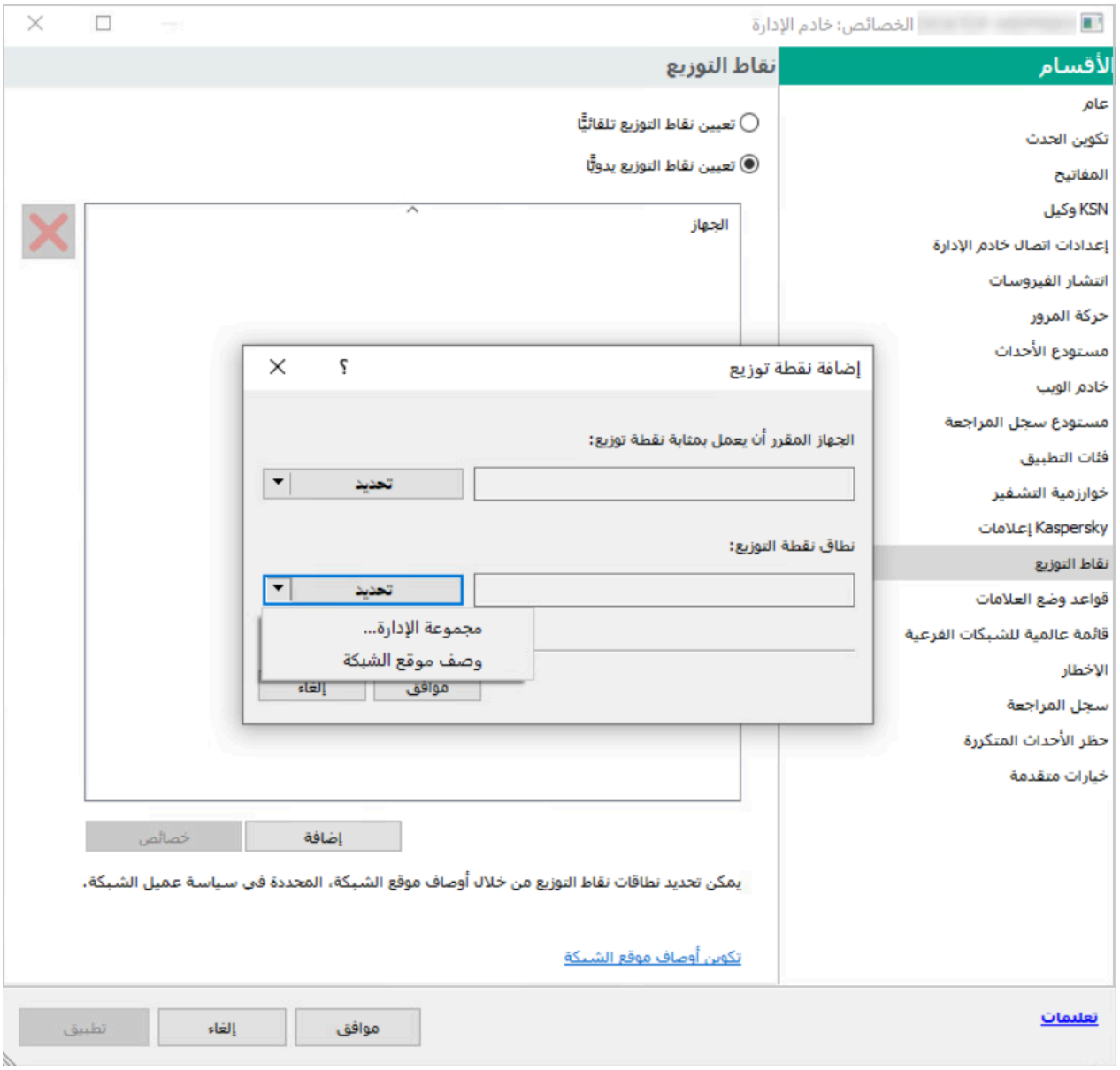
a. ضمن **الجهاز للعمل كنقطة توزيع**، انقر على السهم لأسفل على الزر المنقسم **تحديد** وحدد خيار **إضافة جهاز من مجموعة**.

b. في نافذة **تحديد الأجهزة** التي تفتح، حدد الجهاز ليعمل كنقطة توزيع.

c. ضمن **نطاق نقطة التوزيع**، انقر على السهم لأسفل على الزر المنقسم **تحديد**.

d. حدد الأجهزة المحددة التي ستقوم نقطة التوزيع بتوزيع التحديثات إليها. يمكنك تحديد مجموعة إدارة أو وصف موقع الشبكة.

e. انقر على **موافق** لإغلاق نافذة **إضافة نقطة توزيع**.



تحديد نطاق نقطة التوزيع

سيتم عرض نقطة التوزيع التي أضفتها في قائمة نقاط التوزيع، في القسم **نقاط التوزيع**.

سيتم تعيين الجهاز الأول المثبت عليه عميل الشبكة والذي يتصل بخادم الإدارة الافتراضي تلقائيًا للعمل كنقطة توزيع وتكوينه كبوابة اتصال.

توصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصولة مباشرة بالإنترنت

لتوصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ):

1. يقوم المسؤول بتثبيت عميل الشبكة على الجهاز العميل.

2. قم بتشغيل البرنامج النصي بعد التثبيت واتبع المعالج من أجل إعداد تكوين البيئة المحلية. من موجّه الأوامر، قم بتشغيل الأمر التالي:

```
sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl $
```

3. في الخطوة التي يتم فيها طلب وضع عميل الشبكة، اختر خيار **الاستخدام كبوابة اتصال**.

4. في وحدة تحكم الإدارة المعتمدة على MMC, في قائمة السياق لخادم الإدارة، اختر **خصائص**.

5. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **نقاط التوزيع**.

6. في نافذة **نقاط التوزيع** التي تفتح، في الجزء الأيمن من النافذة:

   a. حدد خيار **تعيين نقاط التوزيع يدويًا**.

   b. انقر على الزر **إضافة**.

   يؤدي ذلك إلى فتح النافذة **إضافة نقطة توزيع**.

7. في النافذة **إضافة نقطة توزيع**، قم بتنفيذ الإجراءات التالية:

   a. تحت **Device to act as distribution point**، انقر على السهم لأسفل (▾) في الزر المنقسم **Select**، وحدد الخيار **Add connection gateway in DMZ by address**.

   b. ضمن **نطاق نقطة التوزيع**، انقر على السهم لأسفل ▾ على الزر المنقسم **تحديد**.

   c. حدد الأجهزة المحددة التي ستقوم نقطة التوزيع بتوزيع التحديثات إليها. يمكنك تحديد أحد مجموعات الإدارة.

   d. انقر على **موافق** لإغلاق نافذة **إضافة نقطة توزيع**.

8. سيتم عرض نقطة التوزيع التي أضفتها في قائمة نقاط التوزيع، في القسم **نقاط التوزيع**.

9. قم بتشغيل klnagchk للتحقق مما إذا كان الاتصال بـ Kaspersky Security Center قد تم تكوينه بنجاح. في موجه الأوامر، قم بتشغيل:
```
sudo /opt/kaspersky/klnagent64/bin/klnagchk $
```

10. في القائمة الرئيسية، انتقل إلى Kaspersky Security Center واكتشف الجهاز.

11. في النافذة التي تفتح، انقر فوق <اسم الجهاز>.

12. في القائمة المنسدلة، اختر **الانتقال إلى رابط المجموعة**.

13. في نافذة **تحديد المجموعة** التي تفتح، انقر على رابط **نقاط التوزيع**.

14. انقر فوق **موافق**.

15. أعد تشغيل خدمة عميل الشبكة على عميل Linux عن طريق تنفيذ الأمر التالي في موجه الأوامر:
```
sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart $
```

اكتمل توصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

بعد ذلك، يمكنك توصيل جهاز Linux بخادم الإدارة من خلال بوابة الاتصال التي تم تكوينها. ولا تتبع هذه الإجراءات إلا بعد إكمال سيناريو التثبيت الرئيسي.

اتصال جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال

تسمح لك بوابة اتصال بتوصيل أجهزة العميل من منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ) بخادم الإدارة. ومن الممكن أن تعمل الأجهزة التي تعمل بنظام Windows وLinux كبوابة اتصال. وبعد توصيل بوابة الاتصال وتكوينها، يمكنك استخدام هذه البوابة لتوصيل جهاز Linux بخادم الإدارة. ولا تتبع الإجراء أدناه إلا بعد إكمال سيناريو التثبيت الرئيسي.

لتوصيل جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال، قم بتنفيذ الإجراءات التالية على هذا الجهاز:

1. يقوم المسؤول بتثبيت عميل الشبكة على الجهاز العميل.

2. قم بتشغيل البرنامج النصي بعد تثبيت عميل الشبكة عن طريق تنفيذ الأمر التالي في موجه الأوامر:
```
sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl $
```

3. في الخطوة التي يتم فيها طلب تشغيل وضع عميل الشبكة، اختر خيار **الاتصال بالخادم من خلال بوابة الاتصال** وأدخل عنوان بوابة الاتصال.

4. تحقق من الاتصال ببرنامج Kaspersky Security Center وبوابة الاتصال، باستخدام الأمر التالي من موجّه الأوامر:
```
sudo /opt/kaspersky/klnagent64/bin/klnagchk $
```
يتم عرض عنوان بوابة الاتصال في الإخراج.

اكتمل اتصال جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال. يمكنك استخدام هذا الجهاز لتحديث التوزيع وتثبيت التطبيقات عن بُعد واسترداد معلومات حول الأجهزة المتصلة بالشبكة.

إضافة بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت للعمل كنقطة توزيع

تنتظر بوابة الاتصال توفر الاتصالات من خادم الإدارة بدلاً من إنشاء اتصالات بخادم الإدارة. هذا يعني أنه بعد تثبيت بوابة الاتصال مباشرة بجهاز في منطقة الأجهزة الموصلة مباشرة بالإنترنت، لا يقوم خادم الإدارة بإدراج الجهاز ضمن الأجهزة المدارة. لذلك، تحتاج إلى القيام بإجراء خاص للتأكد من أن خادم الإدارة ينشأ اتصالاً ببوابة الاتصال.

لإضافة جهاز به بوابة اتصال كنقطة توزيع:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

2. في قائمة السياق بخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة، حدد القسم **نقاط التوزيع**.

4. في الجزء الأيمن من النافذة، حدد خيار **تعيين نقاط التوزيع يدويًا**.

5. انقر على الزر **إضافة**.
يؤدي ذلك إلى فتح النافذة **إضافة نقطة توزيع**.

6. في النافذة **إضافة نقطة توزيع**، قم بتنفيذ الإجراءات التالية:

a. تحت **Device to act as distribution point**، انقر على السهم لأسفل (▾) في الزر المنقسم **Select**، وحدد الخيار **إضافة بوابة اتصال في DMZ حسب العنوان**.

b. في نافذة **إدخال عنوان بوابة الاتصال** التي تفتح، أدخل عنوان IP لبوابة الاتصال (أو أدخل الاسم إذا كان يمكن الوصول إلى بوابة الاتصال بالاسم).

c. ضمن **نطاق نقطة التوزيع**، انقر على السهم لأسفل ▾ على الزر المنقسم **تحديد**.

d. حدد الأجهزة المحددة التي ستقوم نقطة التوزيع بتوزيع التحديثات إليها. يمكنك تحديد مجموعة إدارة أو وصف موقع الشبكة.
نوصي بأن يكون لديك مجموعة منفصلة للأجهزة الخارجية المُدارة.

بعد القيام بهذه الإجراءات، تحتوي قائمة نقاط التوزيع على إدخال جديد يسمى **الإدخال المؤقت لبوابة الاتصال**.

يحاول خادم الإدارة الاتصال ببوابة الاتصال حسب العنوان الذي حددته على الفور. إذا نجحت في ذلك، يتغير اسم الإدخال إلى اسم جهاز بوابة الاتصال. تستغرق هذه العملية حوالي خمس دقائق.

أثناء تحويل الإدخال المؤقت لبوابة الاتصال إلى إدخال مسمى، تظهر بوابة الاتصال أيضًا في مجموعة **الأجهزة غير المعينة**.

لإضافة بوابة اتصال إلى شبكة تم تكوينها مسبقًا، أعد تثبيت عميل الشبكة على الأجهزة التي تريد توصيلها ببوابة الاتصال المضافة حديثًا.

تعيين نقاط التوزيع تلقائيًا

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. حينئذ، سيحدد Kaspersky Security Center بنفسه الأجهزة التي يجب تعيين نقاط التوزيع لها.

لتعيين نقاط التوزيع تلقائيًا:

1. افتح نافذة التطبيق الرئيسية.
2. في شجرة وحدة التحكم، حدد الجزء الذي يحمل اسم خادم الإدارة الذي تريد تعيين نقاط التوزيع له.
3. في قائمة السياق لخادم الإدارة، انقر على **خصائص**.
4. من النافذة خصائص خادم الإدارة، في الجزء **الأقسام**، حدد **نقاط التوزيع**.
5. في الجزء الأيمن من النافذة، حدد خيار **تعيين نقاط التوزيع تلقائيًا**.

في حالة تمكين التعيين التلقائي للأجهزة كنقاط توزيع، سيتعذر عليك تكوين نقاط التوزيع يدويًا أو تحرير قائمة نقاط التوزيع.

6. انقر فوق **موافق**.

يقوم خادم الإدارة بتعيين نقاط التوزيع وتكوينهم تلقائيًا.

حول التثبيت المحلي لعميل الشبكة على جهاز مُحدد للعمل كنقطة توزيع

للسماح للجهاز المحدد كنقطة توزيع للاتصال المباشر بخادم الإدارة الافتراضي للعمل كبوابة اتصال، يجب تثبيت Network Agent محليًا على هذا الجهاز.

تتطابق إجراءات التثبيت المحلي لعميل الشبكة على الجهاز المحدد للعمل كنقطة توزيع مع التثبيت المحلي لعميل الشبكة على أي جهاز بالشبكة.

يجب استيفاء الشروط التالية في الجهاز المحدد كنقطة توزيع:

- أثناء تثبيت عميل الشبكة، حدد عنوان خادم الإدارة الافتراضي الذي يدير الجهاز في الحقل **عنوان الخادم** في نافذة **خادم الإدارة** لمعالج الإعداد. يمكنك استخدام عنوان IP أو اسم الجهاز في شبكة Windows.

  يتم استخدام الصيغة التالية لعنوان خادم الإدارة الافتراضي: <العنوان الفعلي الكامل لخادم الإدارة الذي يتبع له الخادم الافتراضي>/<اسم خادم الإدارة الافتراضي>.

- ولذلك يمكنه العمل كبوابة اتصال وفتح جميع منافذ اللازم للاتصال بخادم الإدارة.

بعد أن يتم تثبيت عميل الشبكة مع الإعدادات المحددة على الجهاز، يقوم Kaspersky Security Center بتنفيذ الإجراءات التالية بشكل تلقائي:

- تضمين هذا الجهاز في مجموعة **الأجهزة المُدارة** الخاصة بخادم الإدارة الافتراضي.
- تعيين هذا الجهاز للعمل كنقطة توزيع لمجموعة **الأجهزة المُدارة** الخاصة بخادم الإدارة الافتراضي.

من الضروري أن يتم التثبيت المحلي لـ Network Agent على الجهاز المعين كنقطة توزيع لمجموعة **الأجهزة المُدارة** على شبكة المؤسسة. يمكنك تثبيت عميل الشبكة عن بُعد على الأجهزة التي تعمل كنقطة توزيع في مجموعات الإدارة المتداخلة. لتنفيذ هذا الأمر، استخدم نقطة التوزيع الخاصة بمجموعة **الأجهزة المُدارة** كبوابة اتصال.

حول استخدام نقطة توزيع كبوابة اتصال

إذا كان خادم الإدارة خارج منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، فيتعذر على عميل الشبكة من هذه المنطقة الاتصال بخادم الإدارة.

عند توصيل خادم الإدارة مع عملاء الشبكة، يمكنك استخدام نقطة التوزيع كبوابة اتصال. تفتح نقطة التوزيع منفذ إلى خادم الإدارة لإنشاء الاتصال. عند بدء خادم الإدارة، فإنه يتصل بنقطة التوزيع هذه ويحافظ على هذا الاتصال خلال الجلسة بأكملها.

لدى تلقي إشارة من خادم الإدارة، تقوم نقطة التوزيع بإرسال إشارة UDP إلى عملاء الشبكة من أجل السماح بالاتصال بخادم الإدارة. عندما يتلقى عملاء الشبكة هذه الإشارة، فإنهم يتصلون بنقطة التوزيع، التي تنقل المعلومات بين وكلاء الشبكة وخادم الإدارة. يمكن أن يحدث تبادل المعلومات عبر شبكة IPv4 أو IPv6.

نوصي باستخدام جهاز معيّن خصيصًا كبوابة اتصال، وتغطية 10 000 جهاز عميل (بما في ذلك الأجهزة المحمولة) كحد أقصى باستخدام بوابة الاتصال هذه.

لإضافة بوابة اتصال إلى شبكة تم تكوينها مسبقًا:

1. قم بتثبيت عميل الشبكة في وضع بوابة الاتصال.
2. أعد تثبيت عميل الشبكة على الأجهزة التي تريد توصيلها ببوابة الاتصال المضافة حديثًا.

إضافة نطاقات IP إلى قائمة النطاقات التي تم استقصاؤها بواسطة نقطة توزيع

يمكنك إضافة نطاق IP إلى قائمة النطاقات التي تم استقصاؤها بواسطة نقطة توزيع.

لإضافة نطاق IP لقائمة النطاقات التي تم استقصاؤها:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.
2. في قائمة السياق الخاصة بالعقدة، حدد **خصائص**.
3. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **نقاط التوزيع**.
4. في القائمة، حدد نقطة التوزيع اللازمة، وانقر فوق **خصائص**.
5. في نافذة خصائص نقطة التوزيع التي تفتح في الجزء الأيسر، **الأقسام** حدد **اكتشاف الأجهزة** ← **نطاقات IP**.
6. حدد مربع الاختيار **تمكين استقصاء النطاق**.
7. انقر على الزر **إضافة**.

لا يكون الزر **إضافة** نشطًا إلا في حالة تحديدك لخانة الاختيار **تمكين استقصاء النطاق**.

تفتح نافذة خصائص **نطاق IP**.

8. في النافذة **نطاق IP**، أدخل اسم نطاق IP الجديد (يكون النطاق الجديد هو الاسم الافتراضي).

9. انقر على الزر **إضافة**.

10. قم بأحد الإجراءات التالية:

- حدد نطاق IP باستخدام عناوين IP للبداية والنهاية.
- حدد نطاق IP باستخدام العنوان وقناع الشبكة الفرعية.
- انقر فوق **استعراض** وقم بإضافة شبكة فرعية من القائمة العمومية للشبكات الفرعية.

11. انقر على**موافق**.

12. انقر فوق **موافق** لإضافة النطاق الجديد ذي الاسم المحدد.

سيظهر النطاق الجديد في قائمة النطاقات التي تم استقصاؤها.

استخدام نقطة توزيع كخادم إرسال

في Kaspersky Security Center، يمكن أن تعمل نقطة التوزيع كخادم دفع للأجهزة المدارة من خلال بروتوكول الهاتف المحمول وللأجهزة التي يديرها عميل الشبكة. على سبيل المثال، يجب تمكين خادم الإرسال إذا كنت تريد أن تكون قادرًا على فرض المزامنة لأجهزة KasperskyOS المزودة بخادم الإدارة. خادم الإرسال لديه نفس نطاق الأجهزة المدارة التي تعمل كنقطة التوزيع حيث يتم فيها تمكين خادم الإرسال. إذا كان لديك العديد من نقاط التوزيع المخصصة لمجموعة الإدارة نفسها، فيمكنك تمكين خادم الإرسال في كل نقطة من نقاط التوزيع. في هذه الحالة، يوازن خادم الإدارة التحميل بين نقاط التوزيع.

يدعم خادم الدفع تحميل ما يصل إلى 50 000 اتصال متزامن.

قد ترغب في استخدام نقاط التوزيع كخوادم دفع للتأكد من وجود اتصال مستمر بين الجهاز المُدار وخادم الإدارة. يلزم الاتصال المستمر لبعض العمليات، مثل تشغيل المهام المحلية وإيقافها، أو تلقي إحصائيات لتطبيق مُدار، أو إنشاء نفق. إذا كنت تستخدم نقطة توزيع كخادم دفع، فلن تضطر إلى استخدام خيار **عدم قطع الاتصال عن خادم الإدارة** على الأجهزة المدارة أو إرسال الحزم إلى منفذ UDP الخاص بعميل الشبكة.

لاستخدام نقطة توزيع كخادم إرسال:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

2. في قائمة السياق الخاصة بالعقدة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **نقاط التوزيع**.

4. في القائمة، حدد نقطة التوزيع اللازمة، وانقر فوق **خصائص**.

5. في نافذة خصائص نقطة التوزيع التي تفتح، في القسم **عام** في الجزء الأيمن **الأقسام**، حدد خيار **استخدم نقطة التوزيع هذه كخادم إرسال**.

6. حدد رقم منفذ خادم الإرسال، أي المنفذ الموجود على نقطة التوزيع التي ستستخدمها الأجهزة العميلة للاتصال.

يتم استخدام المنفذ 13295 بشكل افتراضي.

7. انقر فوق زر **موافق** لإغلاق نافذة خصائص خادم الإدارة.

8. افتح نافذة إعدادات سياسة عميل الشبكة.

9. في القسم **الاتصال**، انتقل إلى القسم الفرعي **الشبكة**.

10. في القسم الفرعي **الشبكة**، حدد الخيار **استخدم نقطة التوزيع لفرض الاتصال بخادم الإدارة**.

11. انقر فوق زر **موافق** للخروج من النافذة.

تبدأ نقطة التوزيع بالعمل كخادم إرسال. يمكنه الآن إرسال إشعارات الإرسال إلى أجهزة العميل.

إذا كنت تدير أجهزة مثبت عليها KasperskyOS، أو تخطط للقيام بذلك، فيجب عليك استخدام نقطة توزيع كخادم إرسال. يمكنك أيضًا استخدام نقطة توزيع كخادم إرسال، إذا كنت ترغب في إرسال إشعارات إلى أجهزة العميل.

عمل روتيني آخر

يوفر هذا القسم توصيات حول العمل الروتيني باستخدام Kaspersky Security Center.

إدارة خوادم الإدارة

يقدم هذا القسم معلومات حول كيفية التعامل مع خوادم الإدارة وطريقة تكوينها.

إنشاء تسلسل هرمي من خوادم الإدارة: إضافة خادم إدارة تابع

يمكنك إضافة خادم إدارة كخادم إدارة تابع والذي يقوم بإنشاء تسلسل هرمي "رئيسي/تابع". يمكن إضافة خادم إدارة تابع بغض النظر عما إذا كان خادم الإدارة الذي تنوي استخدامه كخادم تابع متوفر للاتصال عبر وحدة تحكم الإدارة أم لا.

عند الجمع بين خادمي إدارة في تسلسل هرمي، تأكد من أنه يمكن الوصول إلى المنفذ 13291 على خادمي الإدارة كليهما. المنفذ 13291 مطلوب لتلقي الاتصالات من وحدة تحكم الإدارة إلى خادم الإدارة.

توصيل خادم إدارة كخادم تابع بالرجوع إلى خادم الإدارة الرئيسي

يمكنك إضافة خادم إدارة كخادم تابع عن طريق توصيله بخادم الإدارة الرئيسي عبر المنفذ 13000. ستحتاج لجهاز مثبّت عليه وحدة تحكم إدارة والتي من خلالها يمكن الوصول إلى منافذ TCP رقم 13291 على كلٍ من خادمي الإدارة: خادم الإدارة الرئيسي المفترض وخادم الإدارة الثانوي المفترض.

لإضافة خادم إدارة متوفر للاتصال عبر وحدة تحكم الإدارة كخادم تابع:

1. تأكد أن المنفذ 13000 الخاص بخادم الإدارة الرئيسي المزعوم متوفر لتلقي الاتصالات من خوادم الإدارة الثانوية.

2. استخدم وحدة تحكم الإدارة للاتصال بخادم الإدارة الرئيسي المفترض.

3. حدد مجموعة الإدارة التي تنوي إضافة خادم الإدارة الثانوي لها.

4. في مساحة عمل عقدة **خوادم الإدارة** الخاصة بالمجموعة المحددة، انقر على رابط **إضافة خادم إدارة ثانوي**.

يبدأ تشغيل معالج إضافة خادم إدارة ثانوي.

5. في الخطوة الأولى من المعالج (إدخال عنوان خادم الإدارة الذي تتم إضافته إلى المجموعة)، أدخل اسم الشبكة الخاصة بخادم الإدارة الثانوي المفترض.

6. اتبع إرشادات المعالج.

يتم بناء التسلسل الهرمي "رئيسي / تابع". سيتلقى خادم الإدارة الثانوي اتصال من خادم الإدارة الرئيسي.

إن لم يكن لديك جهازًا مثبّتًا عليه وحدة تحكم الإدارة والذي يمكن من خلاله الوصول إلى منافذ TCP 13291 على كلٍ من خادمي الإدارة (إذا كان، على سبيل المثال، خادم الإدارة الثانوي المفترض موجود في مكتب بعيد وكان مسؤول النظام الخاص بالمكتب لا يمكنه فتح الوصول إلى الإنترنت إلى المنفذ 13291 لأسباب تتعلق بالأمان)، ما زال بإمكانك إضافة خادم إدارة تابع.

لإضافة خادم إدارة ليس متوفر للاتصال عبر وحدة تحكم الإدارة كخادم تابع:

1. تأكد أن المنفذ 13000 الخاص بخادم الإدارة الرئيسي المزعوم متوفر للاتصال من خوادم الإدارة الثانوية.

2. اكتب ملف الشهادة لخادم الإدارة الرئيسي المفترض على جهاز خارجي، مثل محرك فلاش، أو قم بإرساله إلى مسؤول نظام المكتب البعيد حيث يوجد خادم الإدارة.

   ملف الشهادة الخاص بخادم الإدارة على خادم الإدارة نفسه، في %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. اكتب ملف الشهادة لخادم الإدارة الثانوي المفترض على جهاز خارجي، مثل محرك فلاش. إذا كان خادم الإدارة الثانوي المفترض موجود في مكتب بعيد، اتصل بمسؤول النظام لهذا المكتب لمطالبته بإرسال الشهادة إليك.

   ملف الشهادة الخاص بخادم الإدارة على خادم الإدارة نفسه، في %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. استخدم وحدة تحكم الإدارة للاتصال بخادم الإدارة الرئيسي المفترض.

5. حدد مجموعة الإدارة التي تنوي إضافة خادم الإدارة الثانوي لها.

6. في مساحة عمل عقدة **خوادم الإدارة**، انقر على رابط **إضافة خادم إدارة ثانوي**.

   يبدأ تشغيل معالج إضافة خادم إدارة ثانوي.

7. في الخطوة الأولى من المعالج (إدخال العنوان)، اترك حقل **عنوان خادم الإدارة الثانوي (اختياري)** فارغًا.

8. في النافذة **ملف شهادة خادم الإدارة الثانوي**، انقر فوق الزر **استعراض** وحدد ملف الشهادة الخاص بخادم الإدارة الثانوي الذي حفظته.

9. عند اكتمال المعالج، استخدم مثيلاً مختلفًا لوحدة تحكم الإدارة للاتصال بخادم الإدارة الثانوي المفترض. إذا كان خادم الإدارة موجود في مكتب بعيد، اتصل بمسؤول النظام الخاص بهذا المكتب لمطالبته بالاتصال بخادم الإدارة الثانوي المفترض وإجراء الخطوات اللاحقة المستحقة.

10. في قائمة السياق الخاصة بعقدة **خادم الإدارة**، حدد **خصائص**.

11. في خصائص خادم الإدارة، انتقل إلى القسم **خيارات متقدمة** ثم إلى القسم الفرعي **التسلسل الهرمي لخوادم الإدارة**.

12. حدد مربع الاختيار **خادم الإدارة هذا ثانوي في التسلسل الهرمي**.

    تصبح حقول الإدخال متوفرة لإدخال البيانات وتحريرها.

13. في حقل **عنوان خادم الإدارة الأساسي**، أدخل اسم شبكة خادم الإدارة الرئيسي المزعوم.

14. حدد الملف الذي تم حفظه سابقًا والذي يحتوي على شهادة خادم الإدارة الرئيسي المفترض عن طريق النقر فوق الزر **استعراض**.

15. انقر على**موافق**.

يتم بناء التسلسل الهرمي "رئيسي / تابع". يمكنك الاتصال بخادم الإدارة الثانوي عبر وحدة تحكم الإدارة. سيتلقى خادم الإدارة الثانوي اتصال من خادم الإدارة الرئيسي.

توصيل خادم الإدارة الرئيسي بخادم الإدارة الثانوي

يمكنك إضافة خادم إدارة جديد كخادم تابع وبذلك يمكن لخادم الإدارة الرئيسي الاتصال بخادم الإدارة الثانوي عبر المنفذ 13000. يُنصح بذلك إذا، على سبيل المثال، قمت بوضع خادم إدارة تابع في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

ستحتاج لجهاز مثبّت عليه وحدة تحكم إدارة والتي من خلالها يمكن الوصول إلى منافذ TCP رقم 13291 على كلٍ من خادمي الإدارة: خادم الإدارة الرئيسي المفترض وخادم الإدارة الثانوي المفترض.

لإضافة خادم إدارة جديد كخادم تابع وتوصيله بخادم الإدارة الرئيسي عبر المنفذ 13000.

1. تأكد من توفر المنفذ 13000 الخاص بخادم الإدارة الثانوي لتلقي الاتصالات من خادم الإدارة الرئيسي.

2. استخدم وحدة تحكم الإدارة للاتصال بخادم الإدارة الرئيسي المفترض.

3. حدد مجموعة الإدارة التي تنوي إضافة خادم الإدارة الثانوي لها.

4. في مساحة عمل عقدة **خوادم الإدارة** الخاصة بمجموعة الإدارة ذات الصلة، انقر على رابط **إضافة خادم إدارة ثانوي**.

   يبدأ تشغيل معالج إضافة خادم إدارة ثانوي.

5. في الخطوة الأولى من المعالج (إدخال عنوان خادم الإدارة الذي تتم إضافته إلى المجموعة)، أدخل اسم الشبكة الخاصة بخادم الإدارة الثانوي المفترض وحدد خانة الاختيار **توصيل خادم الإدارة الأساسي بخادم الإدارة الثانوي في DMZ**.

6. إذا قمت بالاتصال بخادم الإدارة الثانوي باستخدام خادم وكيل، ففي الخطوة الأولى من المعالج، حدد خانة الاختيار **استخدام الخادم الوكيل** وحدد إعدادات الاتصال.

7. اتبع إرشادات المعالج.

يتم إنشاء التسلسل الهرمي لخوادم الإدارة. سيتلقى خادم الإدارة الثانوي اتصال من خادم الإدارة الرئيسي.

الاتصال بخادم الإدارة والتبديل بين خوادم الإدارة

بعد بدء تشغيل Kaspersky Security Center، يحاول الاتصال بخادم إدارة. إذا توفرت عدة خوادم إدارة على الشبكة، يطلب التطبيق الخادم الذي كان متصلاً به أثناء الجلسة السابقة لـ Kaspersky Security Center.

عند بدء تشغيل التطبيق لأول مرة بعد التثبيت، يحاول الاتصال بخادم الإدارة المحدد أثناء تثبيت Kaspersky Security Center.

بعد إنشاء اتصال بخادم إدارة، يتم عرض شجرة المجلدات لهذا الخادم في شجرة وحدة التحكم.

إذا تمت إضافة عدة خوادم إدارة إلى شجرة وحدة التحكم، يمكنك التبديل بينها.

وحدة تحكم الإدارة مطلوبة للعمل مع كل خادم إدارة. قبل الاتصال الأول بخادم إدارة جديد، تأكد من أن المنفذ 13291، الذي يتلقى الاتصالات من وحدة تحكم الإدارة، مفتوح، بالإضافة إلى كل المنافذ المتبقية المطلوبة للتواصل بين خادم الإدارة ومكونات Kaspersky Security Center الأخرى.

للتبديل إلى خادم إدارة آخر:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في قائمة السياق الخاصة بالعقدة، حدد **الاتصال بخادم الإدارة**.

3. في النافذة **إعدادات الاتصال** التي تفتح، في الحقل **عنوان خادم الإدارة** حدد اسم خادم الإدارة الذي تريد الاتصال به. يمكنك تحديد عنوان IP أو اسم جهاز على شبكة Windows كاسم لخادم الإدارة. يمكنك النقر فوق الزر **خيارات متقدمة** لتكوين الاتصال بخادم الإدارة (راجع الشكل أدناه).

للاتصال بخادم الإدارة عبر منفذ غير المنفذ الافتراضي، أدخل قيمة في الحقل **عنوان خادم الإدارة** بالتنسيق <اسم خادم الإدارة>:<المنفذ>.

للاتصال بخادم إدارة افتراضي، أدخل قيمة في الحقل **عنوان خادم الإدارة** بتنسيق <Administration Server address>/<virtual server name>.

سيتم رفض وصول المستخدمين الذين ليس لديهم حقوق **القراءة** إلى خادم الإدارة.

الاتصال بخادم الإدارة

4. انقر فوق **موافق** لإكمال التبديل بين الخوادم.

بعد توصيل خادم الإدارة، يتم تحديث شجرة مجلدات العقدة المقابلة في شجرة وحدة التحكم.

حقوق الوصول إلى خادم الإدارة وكائناته

يتم إنشاء المجموعات **KLAdmins** و**KLOperators** تلقائيًا أثناء تثبيت Kaspersky Security Center. وتُمنح إلى هاتين المجموعتين أذونات الاتصال بخادم الإدارة ومعالجة كائناته.

واعتمادًا على نوع الحساب المستخدم لتثبيت Kaspersky Security Center، يتم إنشاء المجموعتين **KLAdmins** و**KLOperators** كما يلي:

- إذا تم تثبيت التطبيق بواسطة حساب مستخدم مضمن في مجال، فيتم إنشاء المجموعات على خادم الإدارة وفي المجال الذي يتضمن خادم الإدارة.
- وإذا تم تثبيت التطبيق بواسطة حساب النظام، يتم إنشاء المجموعتين على خادم الإدارة فقط.

يمكنك عرض مجموعات **KLAdmins** و**KLOperators** وتعديل امتيازات الوصول الخاصة بالمستخدمين المنتمين إلى مجموعات **KLAdmins** و**KLOperators** باستخدام أدوات الإدارة القياسية لنظام التشغيل.

تتمتع المجموعة **KLAdmins** بجميع حقوق الوصول، بينما تتمتع المجموعة **KLOperators** بحقي القراءة والتنفيذ فقط. يتم تأمين الحقوق الممنوحة إلى مجموعة **KLAdmins** .

المستخدمون المنتمون إلى المجموعة **KLAdmins** يُطلق عليهم مسؤولو Kaspersky Security Center؛ أما المستخدمون المنتمون إلى المجموعة **KLOperators** فيُطلق عليهم مشغلو Kaspersky Security Center.

وبالإضافة إلى المستخدمين المضمنين في المجموعة **KLAdmins**، تُمنح حقوق مسؤول Kaspersky Security Center إلى المسؤولين المحليين للأجهزة المثبت عليها خادم الإدارة.

ويمكنك استثناء المسؤولين المحليين من قائمة المستخدمين الذين يتمتعون بحقوق مسؤول Kaspersky Security Center.

جميع العمليات التي يبدأها مسؤولو Kaspersky Security Center سوف تتم باستخدام حقوق حساب خادم الإدارة.

يمكن إنشاء مجموعة **KLAdmins** فردية لكل خادم إدارة من الشبكة؛ ستمتلك المجموعة الحقوق الضرورية لخادم الإدارة هذا فقط.

إذا كانت الأجهزة التي تنتمي إلى نفس المجال مضمنة في مجموعات إدارة تخص خوادم إدارة مختلفة، فيكون مسؤول المجال هو مسؤول Kaspersky Security Center لكل المجموعات. وتظل مجموعة **KLAdmins** هي ذاتها لكل مجموعات الإدارة؛ ويتم إنشاؤها أثناء تثبيت خادم الإدارة الأول. جميع العمليات التي يبدأها مسؤول Kaspersky Security Center تتم باستخدام حقوق حساب خادم الإدارة الذي بدأت لأجله هذه العمليات.

بعد تثبيت التطبيق، يمكن لمسؤول Kaspersky Security Center القيام بما يلي:

- تعديل الحقوق الممنوحة إلى مجموعات **KLOperators**.
- منح حقوق الوصول إلى وظائف Kaspersky Security Center إلى مجموعات الأمان الأخرى والمستخدمين الفرديين المُسجلين في محطة عمل المسؤول.
- تعيين حقوق وصول المستخدم داخل كل مجموعة إدارة.

يمكن لمسؤول Kaspersky Security Center تعيين حقوق الوصول إلى كل مجموعة إدارة أو إلى الكائنات الأخرى لخادم الإدارة في القسم **الأمان** بنافذة خصائص الكائن المحدد.

ويمكنك تتبع نشاط المستخدم باستخدام سجلات الأحداث في تشغيل خادم الإدارة. يتم عرض سجلات الحدث في العقدة **خادم الإدارة** في علامة التبويب **الأحداث**. وتتمتع هذه الأحداث بمستوى الأهمية **معلومات عن الأحداث** وتبدأ أنواع الحدث بـ "**التدقيق**".

شروط الاتصال بخادم إدارة عبر الإنترنت

إذا كان خادم الإدارة موجودًا في مكان بعيد خارج شبكة الشركة، فيمكن أن تتصل الأجهزة العميلة به عبر الإنترنت.

بالنسبة للأجهزة العميلة التي تتصل بخادم الإدارة عبر الإنترنت، يجب الوفاء بالشروط التالية:

- يجب أن يحتوي خادم الإدارة على عنوان IP خارجي ويجب أن يظل المنفذ الوارد 13000 مفتوحًا (للاتصال بعملاء الشبكة). ننصحك بفتح منفذ UDP 13000 (لاستقبال إشعارات إيقاف تشغيل الجهاز).
- يجب تثبيت عملاء الشبكة على الأجهزة.
- عند تثبيت عميل الشبكة على الأجهزة، يجب أن تحدد عنوان IP الخارجي لخادم الإدارة عن بُعد. في حالة استخدام حزمة تثبيت من أجل القيام بالتثبيت، يجب تحديد عنوان IP الخارجي يدويًا في خصائص حزمة التثبيت في القسم **إعدادات**.
- لاستخدام خادم الإدارة عن بُعد لإدارة التطبيقات والمهام الخاصة بأحد الأجهزة، من نافذة خصائص الجهاز في القسم **عام**، قم بتحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة**. بعد تحديد خانة الاختيار، انتظر حتى تتم مزامنة خادم الإدارة مع الجهاز البعيد. لا يمكن أن يتجاوز عدد الأجهزة العميلة التي تبقى على اتصال مستمر مع خادم الإدارة عن 300.

لتحسين أداء المهام التي يتم بدؤها بواسطة خادم الإدارة عن بُعد، يمكنك فتح المنفذ 15000 على الجهاز. في هذه الحالة، لتشغيل مهمة، يرسل خادم الإدارة حزمة خاصة إلى عميل الشبكة من خلال المنفذ 15000 بدون الانتظار حتى تكتمل المزامنة مع الجهاز.

اتصال مشفر بخادم إدارة

يمكن تنفيذ تبادل البيانات بين الأجهزة العميلة وخادم الإدارة، فضلاً عن أنه يمكن توصيل وحدة تحكم الإدارة بخادم الإدارة باستخدام بروتوكول طبقة مقابس التوصيل الآمنة (TLS). ويمكن لبروتوكول TLS تحديد الأطراف المتفاعلة، وتشفير البيانات التي يتم نقلها، وحمايتها من التعديل أثناء النقل. يستخدم بروتوكول TLS مفاتيح عامة لمصادقة الأطراف المتفاعلة وتشفير البيانات.

مصادقة خادم الإدارة عند اتصال جهاز

عند اتصال جهاز عميل بخادم الإدارة لأول مرة، يقوم عميل الشبكة على الجهاز بتنزيل نسخة من شهادة خادم الإدارة وتخزينها عليه محليًا.

وإذا قمت بتثبيت عميل الشبكة على جهاز محليًا، فيمكنك تحديد شهادة خادم الإدارة يدويًا.

تُستخدم النسخة المُنزَّلة من الشهادة في التحقق من حقوق خادم الإدارة وأذونه أثناء الاتصالات اللاحقة.

وفي الجلسات التالية، يطلب عميل الشبكة شهادة خادم الإدارة عند كل عملية اتصال للجهاز بخادم الإدارة ويقوم بمقارنتها بالنسخة المحلية. فإذا لم تكن النسختان متطابقتين، فلا يُسمح للجهاز بالوصول إلى خادم الإدارة.

مصادقة خادم الإدارة أثناء توصيل وحدة تحكم الإدارة

عند الاتصال بخادم الإدارة لأول مرة، تطلب وحدة تحكم الإدارة شهادة خادم الإدارة وتقوم بحفظها محليًا في محطة عمل المسؤول. وبعدها، في كل مرة تحاول فيها وحدة تحكم الإدارة الاتصال بخادم الإدارة، يتم تحديد الخادم بناءً على نسخة الشهادة.

فإذا كانت شهادة خادم الإدارة غير مطابقة للنسخة المُخزّنة على محطة عمل المسؤول، فسوف تطالبك وحدة تحكم الإدارة بتأكيد الاتصال بخادم الإدارة الذي يتكون من الاسم المحدد وتنزيل شهادة جديدة. وبعد إنشاء الاتصال، تقوم وحدة تحكم الإدارة بحفظ نسخة من شهادة خادم الإدارة الجديدة، تُستخدم هذه النسخة في تحديد خادم الإدارة في المستقبل.

تكوين قائمة السماح بعناوين IP للاتصال بخادم الإدارة

بشكل افتراضي، يمكن للمستخدمين تسجيل الدخول إلى Kaspersky Security Center عبر أي جهاز حيث يمكنهم فتح Kaspersky Security Center Web Console (المشار إليها فيما يلي باسم Web Console) أو حيث يتم تثبيت وحدة تحكم الإدارة المستندة إلى MMC. ومع ذلك، يمكنك تكوين خادم الإدارة بحيث يمكن للمستخدمين الاتصال به فقط من الأجهزة ذات عناوين IP المسموح بها. في هذه الحالة، حتى إذا سرق متطفل حساب Kaspersky Security Center، فلن يتمكن من تسجيل الدخول إلى Kaspersky Security Center لأن عنوان IP الخاص بجهاز الدخيل ليس في قائمة السماح.

يتم التحقق من عنوان IP عندما يقوم المستخدم بتسجيل الدخول إلى Kaspersky Security Center أو تشغيل تطبيق يتفاعل مع خادم الإدارة عبر Kaspersky Security Center OpenAPI. يحاول جهاز المستخدم إنشاء اتصال بخادم الإدارة في هذه اللحظة. إذا لم يكن عنوان IP للجهاز مدرجًا في قائمة السماح، فسيحدث خطأ في المصادقة ويعلمك حدث KLAUD_EV_SERVERCONNECT أنه لم يتم إنشاء اتصال بخادم الإدارة.

متطلبات قائمة السماح لعناوين IP

يتم التحقق من عناوين IP فقط عندما تحاول التطبيقات التالية الاتصال بخادم الإدارة:

- Web Console Server

إذا قمت بتسجيل الدخول إلى Web Console على جهاز واحد وتم تثبيت Web Console Server على جهاز آخر ، يمكنك تكوين جدار حماية على الجهاز حيث تم تثبيت Web Console Server باستخدام الوسائل القياسية لنظام التشغيل. بعد ذلك، إذا حاول شخص ما تسجيل الدخول إلى Web Console، فإن جدار الحماية يساعد على منع المتطفلين من التدخل.

- وحدة تحكم الإدارة
- تتفاعل التطبيقات مع خادم الإدارة عبر كائنات أتمتة klakaut
- التطبيقات التي تتفاعل مع خادم الإدارة عبر OpenAPI، مثل Kaspersky Anti Targeted Attack Platform أو Kaspersky Security for Virtualization

لذلك، حدد عناوين الأجهزة التي تم تثبيت التطبيقات المذكورة أعلاه عليها.

يمكنك تعيين عناوين IPv4 وIPv6. لا يمكنك تحديد نطاقات عناوين IP.

كيفية إنشاء قائمة السماح بعناوين IP

إذا لم تقم بتعيين قائمة السماح مسبقًا، فاتبع الإرشادات أدناه.

لإنشاء قائمة السماح بعناوين IP لتسجيل الدخول إلى Kaspersky Security Center:

1. على جهاز خادم الإدارة، قم بتشغيل موجه الأوامر ضمن حساب له حقوق المسؤول.
2. قم بتغيير دليلك الحالي إلى مجلد تثبيت Kaspersky Security Center (عادةً، Kaspersky\(x86) Program Files\:<Disk>\Kaspersky Security Center\Lab).
3. أدخل الأمر التالي، باستخدام حقوق المسؤول:

```
"<عناوين IP>" klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -vt s-
```

حدد عناوين IP التي تفي بالمتطلبات المذكورة أعلاه. يجب فصل عدة عناوين IP بفاصلة منقوطة.

مثال على كيفية السماح لجهاز واحد فقط بالاتصال بخادم الإدارة:

```
"192.0.2.0" klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -vt s-
```

مثال على كيفية السماح لأجهزة متعددة بالاتصال بخادم الإدارة:

```
;192.0.2.0" klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -vt s- "203.0.113.0 ;198.51.100.0
```

4. قم بإعادة تشغيل خدمة خادم الإدارة.

يمكنك معرفة ما إذا كنت قد نجحت في تكوين قائمة السماح بعناوين IP في Kaspersky Event Log على خادم الإدارة.

كيفية تغيير قائمة السماح بعناوين IP

يمكنك تغيير قائمة السماح تمامًا كما فعلت عند إنشائها لأول مرة. لهذا الغرض، قم بتشغيل نفس الأمر وحدد قائمة سماح جديدة:

```
"<عناوين IP>" klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -vt s-
```

إذا كنت تريد حذف بعض عناوين IP من قائمة السماح، فأعد كتابتها. على سبيل المثال ، تتضمن قائمة السماح الخاصة بك عناوين IP التالية: 192.0.2.0؛ 198.51.100.0؛ 203.0.113.0. تريد حذف عنوان IP 198.51.100.0. للقيام بذلك، أدخل الأمر التالي في موجه الأوامر:

```
;192.0.2.0" klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -vt s- "203.0.113.0
```

لا تنس إعادة تشغيل خدمة خادم الإدارة.

كيفية إعادة تعيين قائمة السماح المكونة لعناوين IP

لإعادة تعيين قائمة السماح المكونة بالفعل لعناوين IP:

1. أدخل الأمر التالي في موجه الأوامر، باستخدام حقوق المسؤول:

```
t s- "" klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v
```

2. قم بإعادة تشغيل خدمة خادم الإدارة.

بعد ذلك، لم يتم التحقق من عناوين IP بعد الآن.

استخدام الأداة المساعدة klscflag لإغلاق المنفذ 13291

يتم استخدام المنفذ 13291 على خادم الإدارة لتلقي الاتصالات من وحدات تحكم الإدارة. هذا المنفذ مفتوح بشكل افتراضي. إذا كنت لا تريد استخدام وحدة تحكم الإدارة المستندة إلى MMC أو الأداة المساعدة klakaut، فيمكنك إغلاق هذا المنفذ باستخدام الأداة المساعدة klscflag. تعمل هذه الأداة على تغيير قيمة المعلمة KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

لإغلاق المنفذ 13291:

1. قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky\Kaspersky Security Center\Lab.

2. قم بتنفيذ الأمر التالي في سطر الأوامر:

```
klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -
";"\SS_SETTINGS"\ = ss_type|" svt BOOL_T -ss
```

3. أعد تشغيل خدمة خادم إدارة Kaspersky Security Center.

المنفذ 13291 مغلق.

للتحقق مما إذا كان المنفذ 13291 قد تم إغلاقه بنجاح:

قم بتنفيذ الأمر التالي في سطر الأوامر:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -
";"\SS_SETTINGS"\ = ss_type|" ss
```

يُرجع هذا الأمر النتيجة التالية:

```
(PARAMS_T) ---+
false(BOOL_T) = KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN---+
```

تعني القيمة `false` أن المنفذ مغلق. خلاف ذلك، يتم عرض القيمة `true`.

قطع الاتصال من خادم إدارة

لقطع الاتصال من خادم إدارة:

1. حدد من شجرة وحدة التحكم العقدة التي تقابل خادم الإدارة الذي تريد قطع الاتصال عنه.

2. في قائمة سياق العقدة، حدد **قطع الاتصال عن خادم الإدارة**.

إضافة خادم إدارة إلى شجرة وحدة التحكم

لإضافة خادم إدارة إلى شجرة وحدة التحكم:

1. في النافذة الرئيسية لـ Kaspersky Security Center، حدد عقدة **Kaspersky Security Center** في شجرة وحدة التحكم.

2. في قائمة سياق العقدة، حدد **جديد** ← **خادم الإدارة**.

سيتم إنشاء عقدة تسمى **خادم إدارة - <اسم الجهاز> (غير متصل)** في شجرة وحدة التحكم التي سيمكنك منها الاتصال بأي من خوادم الإدارة المثبتة على الشبكة.

إزالة خادم إدارة من شجرة وحدة التحكم

لإزالة خادم إدارة من شجرة وحدة التحكم:

1. حدد من شجرة وحدة التحكم العقدة التي تقابل خادم الإدارة الذي تريد إزالته.

2. في قائمة سياق العقدة، حدد **إزالة**.

إضافة خادم إدارة افتراضي إلى شجرة وحدة التحكم

لإضافة خادم إدارة افتراضي إلى شجرة وحدة التحكم:

1. في شجرة وحدة التحكم، حدد العقدة التي تحتوي على اسم خادم الإدارة الذي تحتاج إلى إنشاء خادم إدارة افتراضي له.

2. في العقدة خادم الإدارة، حدد المجلد **خوادم الإدارة**.

3. في مساحة عمل المجلد **خوادم الإدارة**، انقر فوق الرابط **إضافة خادم الإدارة الافتراضي**.

   بدء تشغيل معالج خادم إدارة افتراضي جديد.

4. في النافذة **اسم خادم الإدارة الافتراضي**، حدد اسم خادم الإدارة الافتراضي الذي سيتم إنشاؤه.

   لا يمكن أن يكون طول اسم خادم الإدارة الافتراضي أكبر من 255 حرفًا ولا يمكن أن يتضمن أي رموز خاصة (مثل "*<>?\:|).

5. في النافذة **إدخال العنوان لتوصيل الجهاز بخادم الإدارة الافتراضي**، حدد عنوان اتصال الجهاز

   عنوان اتصال خادم الإدارة الافتراضي هو عنوان الشبكة الذي ستتصل من خلاله الأجهزة بخادم الإدارة. يشتمل عنوان الاتصال على جزأين: عنوان شبكة خادم إدارة فعلي واسم خادم إدارة افتراضي، يفصل بينهما شرطة مائلة. سيتم استبدال اسم خادم الإدارة الافتراضي تلقائيًا. سيتم استخدام العنوان المحدد على خادم الإدارة الافتراضي كعنوان افتراضي في حزم تثبيت عميل الشبكة.

6. في النافذة **إنشاء حساب مسؤول خادم الإدارة الافتراضي**، حدد أحد المستخدمين من القائمة للعمل كمسؤول خادم إدارة افتراضي، أو أضِف حساب مسؤول جديد عن طريق النقر فوق الزر **إنشاء**.

يمكنك تحديد حسابات متعددة.

يتم إنشاء عقدة باسم **خادم الإدارة <اسم خادم الإدارة الافتراضي>** في شجرة وحدة التحكم.

تغيير حساب خدمة خادم الإدارة. الأداة المساعدة klsrvswch

إذا كنت بحاجة إلى تغيير حساب خدمة خادم الإدارة الذي تم إعداده عند تثبيت Kaspersky Security Center، يمكنك استخدام أداة مساعدة تسمى klsrvswch والتي تم تصميمها لتغيير حساب خادم الإدارة.

عند تثبيت Kaspersky Security Center، يتم نسخ الأداة المساعدة تلقائيًا في مجلد تثبيت التطبيق.

عدد مرات تشغيل الأداة المساعدة غير محدود أساسيًا.

يجب تشغيل الأداة المساعدة klsrvswch على جهاز خادم الإدارة تحت الحساب الذي يتمتع بحقوق المسؤول الذي تم استخدامه لتثبيت خادم الإدارة.

تسمح لك الأداة المساعدة klsrvswch بتغيير نوع الحساب. على سبيل المثال، إذا كنت تستخدم حساب محلي، يمكنك تغييره إلى حساب مجال أو إلى حساب خدمة مُدار (والعكس صحيح). لا تسمح لك الأداة المساعدة klsrvswch بتغيير نوع الحساب إلى حساب الخدمة المُدارة للمجموعة (gMSA).

لا يسمح Windows Vista والإصدارات الأحدث من Windows باستخدام حساب النظام المحلي لخادم الإدارة. في هذه الإصدارات لـ Windows، يكون خيار **حساب النظام المحلي** غير نشط.

لتغيير حساب خدمة خادم الإدارة إلى حساب مجال:

1. قم بتشغيل الأداة المساعدة klsrvswch من مجلد تثبيت Kaspersky Security Center. مسار التثبيت الافتراضي: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

يؤدي هذا الإجراء أيضًا إلى تشغيل معالج تعديل حساب خدمة خادم الإدارة. اتبع إرشادات المعالج.

2. في النافذة **حساب خدمة خادم الإدارة**، حدد **حساب النظام المحلي**.

بعد اكتمال المعالج، يتم تغيير حساب خادم الإدارة. ستبدأ خدمة خادم الإدارة ضمن حساب النظام المحلي وباستخدام بيانات اعتماده.

يتطلب التشغيل الصحيح لـ Kaspersky Security Center أن يشتمل الحساب المستخدم لبدء خدمة خادم الإدارة على حقوق المسؤول للمورد الذي تستضيفه قاعدة بيانات خادم الإدارة.

لتغيير حساب خدمة خادم الإدارة إلى حساب مستخدم أو حساب خدمة مُدار:

1. قم بتشغيل الأداة المساعدة klsrvswch من مجلد تثبيت Kaspersky Security Center. مسار التثبيت الافتراضي: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

يؤدي هذا الإجراء أيضًا إلى تشغيل معالج تعديل حساب خدمة خادم الإدارة. اتبع إرشادات المعالج.

2. في النافذة **حساب خدمة خادم الإدارة**، حدد **حساب مخصص**.

3. انقر على زر **البحث الآن**.

تفتح النافذة **تحديد المستخدم**.

4. في النافذة **تحديد المستخدم**، انقر فوق الزر **أنواع الكائنات**.

5. في قائمة أنواع الكائنات، حدد **المستخدمين** (إذا كنت تريد حساب المستخدم) أو **حسابات الخدمة** (إذا كنت تريد حساب الخدمة المُدار) وانقر فوق **موافق**.

6. في حقل اسم الكائن، أدخل اسم الحساب، أو جزء من الاسم وانقر فوق **التحقق من الأسماء**.

7. في قائمة الأسماء المتطابقة، حدد الاسم اللازم، ثم انقر فوق **موافق**.

8. إذا قمت بتحديد **حسابات الخدمة**، في النافذة **كلمة مرور الحساب**، اترك حقل **كلمة المرور** و**تأكيد كلمة المرور** فارغًا. إذا قمت بتحديد **المستخدمين**، أدخل كلمة مرور جديدة للمستخدم وقم بتأكيدها.

سيتم تغيير حساب خدمة خادم إدارة إلى الحساب الذي قمت بتحديده.

عند استخدام خادم Microsoft SQL Server في وضع يفترض مسبقًا مصادقة حسابات المستخدمين باستخدام أدوات Microsoft Windows، يجب منح حق الوصول إلى قاعدة البيانات. يجب أن يمتلك حساب المستخدم حالة مالك قاعدة بيانات Kaspersky Security Center. يتم استخدام نظام dbo بشكل افتراضي.

تغيير بيانات اعتماد DBMS

قد تحتاج إلى تغيير بيانات اعتماد DBMS، على سبيل المثال من أجل إجراء تدوير لبيانات الاعتماد لأغراض أمنية.

لتغيير بيانات اعتماد DBMS في بيئة نظام Windows باستخدام klsrvswch.exe:

1. قم بتشغيل الأداة المساعدة klsrvswch الموجودة في مجلد تثبيت Kaspersky Security Center. مسار التثبيت الافتراضي: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

يجب تشغيل الأداة المساعدة klsrvswch على جهاز خادم الإدارة تحت الحساب الذي يتمتع بحقوق المسؤول الذي تم استخدامه لتثبيت خادم الإدارة.

2. انقر على زر **التالي** في المعالج حتى تصل إلى خطوة **تغيير بيانات اعتماد الوصول إلى DBMS**.

3. في خطوة **تغيير بيانات اعتماد الوصول إلى DBMS** في المعالج، عليك بالقيام بما يلي:

سيتم تخطي خطوة **تغيير بيانات اعتماد الوصول إلى DBMS** في المعالج إذا تم استخدام مصادقة Windows.

- حدد خيار **تطبيق بيانات اعتماد جديدة**.
- حدد اسم حساب جديد في حقل **الحساب**.
- حدد كلمة سر جديدة لحساب في حقل **كلمة السر**.
- حدد كلمة السر الجديدة في حقل **تأكيد كلمة السر**.

يجب أن تحدد بيانات اعتماد حساب يوجد في DBMS.

4. انقر فوق زر **التالي**.

بعد انتهاء المعالج، يتم تغيير بيانات اعتماد DBMS.

لا يمكن استخدام الأداة المساعدة klsrvswch إلا لتغيير كلمة مرور الحساب لمصادقة SQL. لا يتم دعم تغيير طريقة الترخيص. ولتغيير طريقة الترخيص، أعد تثبيت خادم الإدارة وحدد الإعدادات المطلوبة.

تغيير المجلد المشترك لخادم الإدارة

يتم تحديد المجلد المشترك لخادم الإدارة أثناء تثبيت خادم الإدارة. ويمكنك تغيير موقع المجلد المشترك في خصائص خادم الإدارة.

لتغيير المجلد المشترك:

1. أنشئ مجلد مشاركة على شبكة اتصال وكوّن أذونات للمشاركة ولبنية المجلد للسماح بحقوق التحكم الكاملة للمجموعة الفرعية **الكل**.
2. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وحدد **خصائص**.
3. في النافذة خصائص خادم الإدارة، في الجزء **الأقسام**، حدد **خيارات متقدمة** ثم **Administration Server shared folder**.
4. في القسم **Administration Server shared folder**، انقر فوق الزر **تغيير**.
5. حدد المجلد الذي تريد استخدامه كمجلد مشترك.
6. انقر فوق الزر **موافق** لإغلاق النافذة خصائص خادم الإدارة.
7. قم بتعيين حقوق القراءة للمجموعة الفرعية **Everyone** للمجلد الذي حددته كمشترك.

إيجاد الحلول لمشكلات عقد خادم الإدارة

تحتوي شجرة وحدة التحكم في الجزء الأيسر لوحدة تحكم الإدارة على عقد خوادم الإدارة. يمكنك إضافة أكبر عدد من خوادم الإدارة التي تحتاجها إلى شجرة وحدة التحكم.

يتم تخزين قائمة عقد خادم الإدارة في شجرة وحدة التحكم في نسخة مطابقة من ملف msc. عن طريق Microsoft Management Console. توجد النسخة المطابقة لهذا الملف في المجلد %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ على الجهاز حيث تم تثبيت وحدة تحكم الإدارة. لكل عقدة من عقد خادم الإدارة، يحتوي الملف على المعلومات التالية:

- عنوان خادم الإدارة
- رقم المنفذ
- سواء كان TLS مُستخدمًا أم لا

  تعتمد هذه المعلمات على رقم المنفذ المستخدم لتوصيل وحدة تحكم الإدارة بخادم الإدارة.
- اسم المستخدم
- شهادة خادم الإدارة

استكشاف الأخطاء وحلها

عندما تتصل وحدة تحكم الإدارة بخادم الإدارة، تتم مقارنة الشهادة المخزنة محليًا بشهادة خادم الإدارة. إذا لم تتطابق الشهادات، فستُظهر وحدة تحكم الإدارة حدوث خطأ. على سبيل المثال، قد يحدث عدم تطابق شهادة عند قيامك باستبدال شهادة خادم الإدارة. في هذه الحالة، قم بإعادة إنشاء عقدة خادم الإدارة في وحدة التحكم.

لإعادة إنشاء عقدة خادم الإدارة:

1. إغلاق نافذة وحدة تحكم إدارة Kaspersky Security Center.

2. احذف ملف Kaspersky Security Center 15.1 في %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.

3. قم بتشغيل وحدة تحكم إدارة Kaspersky Security Center.

   ستتم مطالبتك بالاتصال بخادم الإدارة وقبول شهادته الموجودة.

4. قم بأحد الإجراءات التالية:

   - أقبل الشهادة الموجودة من خلال النقر فوق الزر **نعم**.
   - لتحديد الشهادة الخاصة بك، انقر فوق الزر **لا**، ثم قم بالاستعراض للوصول لملف الشهادة الذي سيتم استخدامه لمصادقة خادم الإدارة.

   يتم حل مشكلة الشهادة. يمكنك استخدام وحدة تحكم الإدارة للاتصال بخادم الإدارة.

عرض وتعديل إعدادات خادم إدارة

يمكنك ضبط إعدادات خادم إدارة في نافذة خصائص هذا الخادم.

لفتح نافذة خصائص: خادم الإدارة,

حدد **خصائص** في قائمة سياق عقدة خادم الإدارة في شجرة وحدة التحكم.

ضبط الإعدادات العامة لخادم الإدارة

يمكنك ضبط الإعدادات العامة لخادم الإدارة في الأقسام **عام** و**إعدادات اتصال خادم الإدارة** و**مستودع الأحداث** و**الأمان** بنافذة خصائص خادم الإدارة.

لا يتم عرض القسم **الأمان** في نافذة خصائص خادم الإدارة إذا تم تعطيل العرض في واجهة وحدة تحكم الإدارة.

لتمكين عرض القسم **الأمان** في وحدة تحكم الإدارة:

1. حدد من شجرة وحدة التحكم خادم الإدارة الذي تريده.

2. من القائمة **عرض** في نافذة التطبيق الرئيسية، حدد **تكوين الواجهة**.

3. في نافذة **تكوين الواجهة** التي تفتح، حدد خانة الاختيار **عرض أقسام إعدادات الأمان** وانقر فوق **موافق**.

4. في النافذة التي تحتوي على رسالة التطبيق، انقر فوق **موافق**.

   سيتم عرض القسم **الأمان** في نافذة خصائص خادم الإدارة.

إعدادات واجهة وحدة تحكم الإدارة

يمكنك ضبط إعدادات واجهة وحدة تحكم الإدارة لعرض أو إخفاء أدوات التحكم في واجهة المستخدم المتعلقة بالميزات التالية:

- إدارة الثغرات الأمنية والتصحيحات
- تشفير البيانات وحمايتها
- إعدادات التحكم في نقطة النهاية
- إدارة الأجهزة المحمولة
- خوادم الإدارة الثانوية
- أقسام إعدادات الأمان

لتكوين إعدادات واجهة وحدة تحكم الإدارة:

1. حدد من شجرة وحدة التحكم خادم الإدارة الذي تريده.
2. من القائمة **عرض** في نافذة التطبيق الرئيسية، حدد **تكوين الواجهة**.
3. في النافذة **تكوين الواجهة** التي تفتح، حدد خانات الاختيار بجانب الميزات التي تريد عرضها وانقر فوق **موافق**.
4. في النافذة التي تحتوي على رسالة التطبيق، انقر فوق **موافق**.

سيتم عرض الميزات المحددة في واجهة وحدة تحكم الإدارة.

معالجة الحدث وتخزينه على خادم الإدارة

يتم حفظ المعلومات عن الأحداث التي تحدث أثناء تشغيل التطبيق والأجهزة المدارة في قاعدة بيانات خادم الإدارة. ينتسب كل حدث إلى نوع ومستوى خطورة محدد (حدث حرج، أو خلل وظيفي، أو تحذير، أو معلومات). وبناءً على الظروف التي وقع فيها الحدث، يمكن للتطبيق تعيين مستويات خطورة مختلفة للأحداث من نفس النوع.

يمكنك عرض أنواع ومستويات الخطورة التي تم تعيينها للأحداث في القسم **تكوين الحدث** من نافذة خصائص خادم الإدارة. في القسم **تكوين الحدث** يمكنك أيضًا تكوين معالجة كل حدث بواسطة خادم الإدارة:

- تسجيل الأحداث على خادم الإدارة وفي سجل أحداث نظام التشغيل على أحد الأجهزة وعلى خادم الإدارة.
- الطريقة المستخدمة لإخطار المسؤول بحدث ما (على سبيل المثال، رسالة SMS أو رسالة بريد إلكتروني).

من القسم **Events repository** في النافذة خصائص خادم الإدارة، يمكنك تحرير إعدادات تخزين الأحداث في قاعدة بيانات خادم الإدارة من خلال تقييد عدد سجلات الأحداث أو مدة تخزين السجل. عندما تحدد الحد الأقصى لعدد الأحداث، يقوم التطبيق بحساب مقدار تقريبي لمساحة التخزين المطلوبة للرقم المحدد. يمكنك استخدام هذا الحساب التقريبي لتقييم ما إذا كانت لديك مساحة خالية كافية على القرص لتجنب تجاوز سعة قاعدة البيانات. السعة الافتراضية لقاعدة بيانات خادم الإدارة هي 400 000 حدث. أقصى سعة موصى بها لقاعدة البيانات هي 45 مليون حدث.

يتحقق التطبيق من قاعدة البيانات كل 10 دقائق. وإذا وصل عدد الأحداث إلى القيمة القصوى المحددة بالإضافة إلى 10 000، فسوف يحذف التطبيق الأحداث الأقدم بحيث يبقى الحد الأقصى لعدد الأحداث المحدد فقط.

عند قيام خادم الإدارة بحذف الأحداث القديمة، فلا يمكن حفظ الأحداث الجديدة في قاعدة البيانات. وأثناء هذه الفترة الزمنية، تتم كتابة معلومات حول الأحداث المرفوضة في سجل أحداث Kaspersky. يتم وضع الأحداث الجديدة في قائمة الانتظار ثم حفظها في قاعدة البيانات بعد اكتمال عملية الحذف.

يمكنك تغيير إعدادات أي مهمة لحفظ الأحداث المتعلقة بتقدم المهمة، أو حفظ نتائج تنفيذ المهمة فقط. عند فعل ذلك، ستقلل من عدد الأحداث الموجودة في قاعدة البيانات، وتزيد من سرعة تنفيذ السيناريوهات المرتبطة بتحليل جدول الأحداث في قاعدة البيانات وخفض خطر الكتابة فوق الأحداث الحرجة بواسطة عدد كبير من الأحداث.

عرض سجل الاتصالات بخادم الإدارة

يمكن حفظ محفوظات الاتصالات ومحاولات الاتصال بخادم الإدارة أثناء تشغيله إلى ملف سجل. تسمح لك المعلومات الموجودة في الملف بتعقب ليس فقط الاتصالات ضمن البنية الأساسية لشبكتك، ولكن أيضًا المحاولات غير المصرح بها للوصول إلى الخادم.

لتسجيل أحداث الاتصال بخادم الإدارة:

1. في شجرة وحدة التحكم، حدد خادم الإدارة الذي ترغب في أن تقوم بتمكين تسجيل أحداث الاتصال له.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة الخصائص التي تفتح، في قسم **إعدادات اتصال خادم الإدارة**، وحدد القسم الفرعي **منافذ الاتصال**.
4. تمكين الخيار **تسجيل أحداث الاتصال بخادم الإدارة**.
5. انقر فوق الزر **موافق** لإغلاق النافذة خصائص خادم الإدارة.

سيتم حفظ جميع الأحداث الأخرى للاتصالات الواردة إلى خادم الإدارة، ونتائج المصادقة، وأخطاء SSL في ملف %ProgramData%\KasperskyLab\adminkit\logs\syslog.sc.

التحكم في انتشار الفيروسات

يتيح لك Kaspersky Security Center الاستجابة بسرعة لتهديدات انتشار الفيروسات. يتم تقييم مخاطر انتشار الفيروسات عن طريق مراقبة نشاط الفيروس على الأجهزة.

يمكنك تكوين قواعد تقييم تهديدات انتشار الفيروسات والإجراءات التي سيتم اتخاذها في حالة ظهورها؛ للقيام بذلك استخدم القسم **انتشار الفيروسات** الخاص بنافذة خصائص خادم الإدارة.

يمكنك تحديد إجراء الإخطار للحدث انتشار الفيروسات في القسم **تكوين الحدث** في نافذة خصائص خادم الإدارة، في النافذة خصائص حدث انتشار الفيروسات.

يتم إنشاء حدث انتشار الفيروسات فور اكتشاف أحداث تم اكتشاف كائنات ضارة أثناء تشغيل تطبيقات الأمن. ولذلك، ينبغي حفظ المعلومات حول جميع أحداث تم اكتشاف كائنات ضارة على خادم الإدارة من أجل التعرف على انتشار الفيروسات.

يمكنك تحديد إعدادات حفظ معلومات حول أي حدث كائن ضار تم اكتشافه في سياسات تطبيقات الأمن.

عند عدّ أحداث تم اكتشاف كائنات ضارة لا يتم مراعاة سوى المعلومات الواردة من الأجهزة لخادم الإدارة الرئيسي. ولا يتم أخذ المعلومات الواردة من خوادم الإدارة الثانوية بعين الاعتبار. يتم تكوين الحدث انتشار الفيروسات لكل خادم تابع على حدة.

تقييد حركة المرور

لخفض أحجام حركة المرور داخل شبكة، يوفر التطبيق خيار تقييد سرعة نقل البيانات إلى خادم إدارة من نطاقات IP والشبكات الفرعية IP المحددة.

يمكنك إنشاء وتكوين قواعد تقييد حركة المرور في القسم **حركة المرور** بنافذة خصائص خادم الإدارة.

لإنشاء قاعدة تقييد حركة المرور:

1. في شجرة وحدة التحكم، حدد العقدة التي تحتوي على اسم خادم الإدارة التي تحتاج إلى إنشاء قاعدة تقييد حركة المرور لها.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة، حدد قسم **حركة المرور**.

4. انقر على الزر **إضافة**.

5. في نافذة **قاعدة جديدة**، حدد الإعدادات التالية:

في القسم **نطاق IP لحد حركة المرور**، حدد الطريقة التي سيتم استخدامها لتحديد الشبكة الفرعية أو نطاق تقييد معدل نقل البيانات، وأدخل القيم الخاصة بالإعدادات الخاصة بالطريقة المحددة. حدد إحدى الطرق التالية:

- **حدد النطاق باستخدام العنوان وقناع الشبكة**

يتم تقييد حركة المرور بناءً على إعدادات الشبكة الفرعية. حدد عنوان الشبكة الفرعية وقناع الشبكة الفرعية لتحديد النطاق الذي سيتم تقييد حركة المرور فيه.

يمكنك أيضًا النقر فوق **استعراض** لإضافة شبكات فرعية من القائمة العمومية للشبكات الفرعية.

- **حدد النطاق باستخدام عناوين البداية والنهاية**

يتم تقييد حركة المرور بناءً على نطاق عناوين IP. حدد نطاق عناوين IP في حقول إدخال **البداية** و**النهاية**.

ويتم تحديد هذا الخيار بصورة افتراضية.

في القسم **تقييد حركة المرور**، يمكنك ضبط إعدادات التقييد التالية لمعدل نقل البيانات:

- **الفاصل الزمني**

الفاصل الزمني التي يتم خلاله فرض تقييد حركة المرور. يمكنك تحديد حدود الفاصل الزمني في حقول الإدخال.

- **الحد (كيلوبايت/ثانية)**

الحد الأقصى لسرعة نقل البيانات الواردة والصادرة من خادم الإدارة. لن يكون تقييد حركة المرور فعالًا إلى من خلال الفاصل الزمني المحدد في الحقل **الفاصل الزمني**.

- **الحد على حركة المرور في الأوقات المتبقية (كيلوبايت/ثانية)**

لن يتم تقييد حركة المرور فقط أثناء الفاصل الزمني المحدد في الحقل **الفاصل الزمني** ولكن أيضًا في أوقات أخرى.

تكون خانة الاختيار غير محددة بشكل افتراضي. قد لا تتطابق قيمة هذا الحقل مع قيمة الحقل **الحد (كيلوبايت/ثانية)**.

بصورة أساسية، تؤثر قواعد تقييد حركة المرور على نقل الملفات. لا يتم تطبيق تلك القواعد على حركة المرور الناجمة عن المزامنة بين خادم الإدارة وعميل الشبكة، أو بين خوادم الإدارة الثانوية والأساسية.

تكوين خادم الويب

تم تصميم خادم الويب لنشر حزم التثبيت المستقلة وملفات تعريف iOS MDM وملفات من المجلد المشترك.

يمكنك تحديد إعدادات اتصال خادم الويب بخادم الإدارة وتعيين شهادة خادم ويب في القسم **خادم الويب** بنافذة خصائص خادم الإدارة.

التعامل مع المستخدمين الداخليين

تُستخدم حسابات المستخدمين الداخليين للعمل مع خوادم الإدارة الافتراضية. يمنح Kaspersky Security Center حقوق المستخدمين الفعليين للمستخدمين الداخليين للتطبيق.

يتم إنشاء واستخدام حسابات المستخدمين الداخليين فقط ضمن Kaspersky Security Center. لا يتم نقل أي بيانات عن المستخدمين الداخليين إلى نظام التشغيل. Kaspersky Security Center يصادق المستخدمين الداخليين.

يمكنك تكوين حسابات المستخدمين الداخليين في المجلد **حسابات المستخدمين** من شجرة وحدة التحكم.

النسخ الاحتياطي والاستعادة لإعدادات خادم الإدارة

النسخ الاحتياطي لإعدادات خادم الإدارة وقاعدة البيانات الخاصة به عبر مهمة النسخ الاحتياطي والأداة المساعدة klbackup. تتضمن النسخة الاحتياطية جميع الإعدادات والكائنات الرئيسية المتعلقة بخادم الإدارة، مثل الشهادات، والمفاتيح الأساسية لتشفير محركات الأقراص على الأجهزة المُدارة، ومفاتيح التراخيص المختلفة، وهيكل مجموعات الإدارة بكل محتوياتها، ومهامها، وسياساتها، إلخ. . باستخدام نسخة احتياطية، يمكنك استعادة تشغيل خادم الإدارة في أسرع وقت ممكن، حيث تستغرق من اثنتي عشرة دقيقة إلى بضع ساعات في ذلك.

في حالة عدم توفر نسخة احتياطية، قد يؤدي العطل إلى خسارة نهائية للشهادات وكل إعدادات خادم الإدارة. وسيستلزم هذا إعادة تكوين Kaspersky Security Center من البداية، وإجراء النشر الأولي لعميل الشبكة على شبكة الشركة مرة أخرى. كما ستفقد أيضًا كل المفاتيح الرئيسية لتشفير محركات الأقراص الموجودة على الأجهزة المدارة، مما يعرضك لمجازفة الفقد النهائي لكل البيانات المشفرة الموجودة على الأجهزة المثبت عليها Kaspersky Endpoint Security. وبالتالي، لا تغفل عن عمليات النسخ الاحتياطي لخادم الإدارة باستخدام مهمة النسخ الاحتياطي القياسية.

ينشئ معالج البدء السريع مهمة النسخ الاحتياطي لإعدادات خادم الإدارة ويضبطها كي تعمل يوميًا الساعة 00:4 صباحًا. يتم حفظ النسخ الاحتياطية افتراضيًا في المجلد %ALLUSERSPROFILE%\Application Data\KasperskySC.

في حالة تثبيت مثيل لخادم Microsoft SQL Server على جهاز آخر يُستخدم كنظام إدارة قواعد البيانات، فيجب عليك تعديل مهمة النسخ الاحتياطي عن طريق تحديد مسار UNC، المتوفر للكتابة بواسطة كلاً من خدمة خادم الإدارة وخدمة خادم SQL Server، كمجلد لتخزين النسخ الاحتياطية. هذا المتطلب مشتق من ميزة خاصة للنسخ الاحتياطي في نظام إدارة قواعد البيانات الخاص بخادم Microsoft SQL Server.

في حالة استخدام مثيل محلي لخادم Microsoft SQL Server كنظام إدارة قواعد بيانات، ننصح كذلك بحفظ النسخ الاحتياطية على وسيط مخصص لتأمينها ضد التلف بالإضافة إلى خادم الإدارة.

لأن النسخة الاحتياطية تحتوي على بيانات مهمة، فإن مهمة النسخ الاحتياطي والأداة المساعدة klbackup يعملان على حماية النسخ احتياطية باستخدام كلمة مرور. بشكل افتراضي، يتم إنشاء مهمة النسخ الاحتياطي بكلمة مرور فارغة. يجب عليك تعيين كلمة مرور في خصائص مهمة النسخ الاحتياطي. يتسبب تجاهل هذا الطلب في أن تظل كل مفاتيح شهادات خادم الإدارة ومفاتيح التراخيص والمفاتيح الرئيسية لتشفير كل محركات الأقراص الموجودة على الأجهزة المدارة غير مشفرة.

بالإضافة إلى إجراء النسخ الاحتياطي بانتظام، يجب عليك أيضًا إنشاء نسخة احتياطية قبل كل تغيير مهم، بما في ذلك تثبيت خادم الإدارة وترقياته وتصحيحاته.

إذا كنت تستخدم Microsoft SQL Server باعتباره DBMS، فيمكنك تصغير حجم النسخ الاحتياطية. للقيام بذلك، قم بتمكين **ضغط النسخ الاحتياطي** الخيار في إعدادات خادم SQL.

تتم الاستعادة من نسخة احتياطية باستخدام الأداة المساعدة klbackup على مثيل قابل للتشغيل لخادم الإدارة الذي تم تثبيته للتو وله نفس الإصدار (أو أحدث) الذي تم إنشاء النسخة الاحتياطية له.

يجب أن يقوم مثيل خادم الإدارة الذي ستتم عملية الاستعادة عليه باستخدام نظام إدارة قواعد بيانات من النوع نفسه (على سبيل المثال، SQL Server أو MariaDB نفسه) والإصدار نفسه أو إصدار أحدث. يمكن أن يكون إصدار خادم الإدارة هو نفسه (بتصحيح مشابه أو أحدث) أو إصدار أحدث.

يوضح هذا القسم السيناريوهات القياسية لإعدادات الاستعادة وكائنات خادم الإدارة.

استخدام لقطة نظام الملفات لتقليل مدة النسخ الاحتياطي

في Kaspersky Security Center 15.1، تم تقليل وقت خمول خادم الإدارة خلال عملية النسخ الاحتياطي بالمقارنة بالإصدارات الأقدم. وعلاوةً على ذلك، تمت إضافة ميزة **استخدام لقطة نظام الملفات للنسخ الاحتياطي للبيانات** إلى إعدادات المهام. وتقدّم هذه الميزة خفضًا إضافيًا لوقت الخمول عن طريق استخدام الأداة المساعدة klbackup، والتي تنشئ نسخة مطابقة للقرص خلال عملية النسخ الاحتياطي (يستغرق هذا الأمر ثواني قليلة)، كما تقوم بنسخ قاعدة البيانات بنفس الوقت (يستغرق هذا الأمر دقائق معدودة على أقصى تقدير). عندما تقوم الأداة المساعدة klbackup بإنشاء نسخة مطابقة للقرص ونسخة من قاعدة البيانات، تمكّن الأداة من إمكانية الاتصال بخادم الإدارة مرة أخرى.

يمكنك استخدام ميزة التقاط لقطة للنظام فقط في حالة استيفاء الشرطين التاليين:

- وجود مجلد خادم الإدارة المشترك و%ALLUSERSPROFILE%\KasperskyLab على القرص المنطقي ذاته وأن يكونا محليين بالرجوع إلى خادم الإدارة.
- أن لا يحتوي المجلد %ALLUSERSPROFILE%\KasperskyLab على أي روابط رمزية تمت إنشاؤها يدويًا.

لا تستخدم الميزة في حالة عدم استيفاء شرط من هذين الشرطين. في هذه الحالة، قد يُرجع التطبيق رسالة خطأ كاستجابة لأي محاولة لإنشاء لقطة لنظام الملفات.

لاستخدام الميزة، يجب أن يكون لديك حساب تم منحه الإذن لإنشاء لقطات للقرص المنطقي الذي يخزّن مجلد %ALLUSERSPROFILE%. لاحظ أن حساب خدمة خادم الإدارة ليس لديها مثل هذا الإذن.

لاستخدام ميزة التقاط لقطة لنظام الملفات لتقليل مدة النسخ الاحتياطي:

1. في القسم **مهام**، حدد مهمة النسخ الاحتياطي.
2. في قائمة السياق، حدد **خصائص**.
3. في نافذة خصائص المهمة التي تفتح، حدد القسم **الإعدادات**.
4. حدد خانة الاختيار **استخدام لقطة نظام الملفات للنسخ الاحتياطي للبيانات**.
5. في الحقلين **اسم المستخدم** و**كلمة المرور**، قم بإدخال اسم وكلمة مرور حساب لديه إذن إنشاء لقطات للقرص المنطقي الذي يخزّن مجلد %ALLUSERSPROFILE%.
6. انقر فوق **تطبيق**.

عند أي عملية بدء تشغيل لاحقة لمهمة النسخ الاحتياطي، ستقوم الأداة المساعدة klbackup بإنشاء لقطات لنظام الملفات والتي تقلل من وقت خمول خادم الإدارة خلال عمل المهمة.

تعذر تشغيل جهاز يحتوي على خادم الإدارة

في حالة تعذر تشغيل جهاز يحتوي على خادم الإدارة نتيجة لعطل ما، فمن المستحسن أن تقوم بالإجراءات التالية:

- يجب تعيين خادم الإدارة الجديد إلى العنوان نفسه: اسم NetBIOS أو FQDN أو IP ثابت (بناءً على ما تم تعيينه منهم عند نشر عملاء الشبكة).
- تثبيت خادم إدارة من الإصدار نفسه (أو أحدث) باستخدام نظام إدارة قواعد بيانات من نفس النوع. يمكنك تثبيت الإصدار نفسه من الخادم بالتصحيح نفسه (أو أحدث) أو إصدار أحدث من الخادم. بعد التثبيت، لا تقم بإعداد أولي من خلال المعالج.
- من قائمة **ابدأ** قم بتشغيل الأداة المساعدة klbackup وتنفيذ الاستعادة.

إعدادات خادم الإدارة أو قاعدة البيانات تالفة

إذا تعذر تشغيل خادم الإدارة نتيجة لتلف الإعدادات أو قاعدة البيانات (على سبيل المثال، بعد حدوث تغير مفاجئ في الطاقة)، فمن المستحسن أن تستخدم سيناريو الاستعادة التالي:

1. فحص نظام الملفات الموجود على الجهاز التالف.
2. إلغاء تثبيت الإصدار غير القابل للتشغيل من خادم الإدارة.
3. إعادة تثبيت خادم الإدارة، باستخدام نظام إدارة قواعد بيانات من النوع نفسه ومن الإصدار نفسه (أو أحدث). يمكنك تثبيت الإصدار نفسه من الخادم بالتصحيح نفسه (أو أحدث) أو إصدار أحدث من الخادم. بعد التثبيت، لا تقم بإعداد أولي من خلال المعالج.
4. من القائمة **بدء**، قم بتشغيل الأداة المساعدة klbackup وإجراء الاستعادة.

يُحظر استعادة خادم الإدارة بأي طريقة إلا من خلال الأداة المساعدة klbackup.

أية محاولات لاستعادة خادم الإدارة من خلال برنامج تابع لجهة خارجية ستؤدي حتمًا إلى عدم مزامنة البيانات على عُقَد تطبيق Kaspersky Security Center الموزّع، وبالتالي عمل التطبيق بطريقة غير صحيحة.

النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة

النسخ الاحتياطي للبيانات يسمح بنقل خادم الإدارة من جهاز إلى آخر دون فقان للبيانات. من خلال النسخ الاحتياطي، يمكنك استعادة البيانات عند نقل قاعدة بيانات خادم الإدارة إلى جهاز آخر، أو عند الترقية إلى إصدار أحدث من Kaspersky Security Center. ويمكنك كذلك استخدام النسخ الاحتياطي للبيانات لنقل بيانات خادم الإدارة من Kaspersky Security Center Windows تحت إدارة Kaspersky Security Center Linux (لا يتم دعم نقل البيانات من Kaspersky Security Center Linux إلى Kaspersky Security Center Windows).

لا يتم نسخ المكونات الإضافية للإدارة المثبتة احتياطيًا. بعد استعادة بيانات خادم الإدارة من نسخة احتياطية، تحتاج إلى تنزيل وإعادة تثبيت المكونات الإضافية للتطبيقات المدارة.

قبل إجراء نسخ احتياطي لبيانات خادم الإدارة، تحقق من إضافة خادم إدارة افتراضي إلى مجموعة الإدارة. وفي حالة إضافة خادم إدارة افتراضي، تأكد من تعيين مسؤول إلى خادم الإدارة الافتراضي هذا قبل إجراء النسخ الاحتياطي. ولا يمكنك منح حقوق وصول المسؤول إلى خادم الإدارة الافتراضي بعد النسخ الاحتياطي. ولاحظ أنه في حالة فقدان بيانات اعتماد حساب المسؤول، فلن تتمكن من تعيين مسؤول جديد لخادم المسؤول الافتراضي.

لإجراء نسخ احتياطي لمجموعة التجاوز الفشل من Kaspersky Security Center أو استعادتها، يجب إيقاف المجموعة بأكملها للصيانة ثم إعادة تشغيلها عند اكتمال النسخ الاحتياطي أو الاستعادة.

يمكنك إنشاء نسخة احتياطية من بيانات خادم الإدارة بإحدى الطرق التالية:

- من خلال إنشاء مهمة نسخ احتياطي للبيانات وتشغيلها عبر وحدة تحكم الإدارة.
- من خلال تشغيل أداة klbackup المساعدة على الجهاز المثبت عليه خادم الإدارة. يتم تضمين الأداة المساعدة هذه في مجموعة توزيع Kaspersky Security Center. بعد تثبيت خادم الإدارة، ستكون الأداة المساعدة موجودة في جذر المجلد الوجهة المحدد عند تثبيت التطبيق.

يتم حفظ البيانات التالية في النسخة الاحتياطية لخادم الإدارة:

- قاعدة بيانات خادم الإدارة (السياسات والمهام وإعدادات التطبيق والأحداث المحفوظة في خادم الإدارة).
- تفاصيل التكوين الخاصة ببنية مجموعات الإدارة والأجهزة العميلة.
- تخزين حزم توزيع التطبيقات للتثبيت عن بُعد.
- شهادة خادم الإدارة.
- محتويات مجلد التحديثات.

  بشكل افتراضي، يكون مسار المجلد هو C:\ProgramData\KasperskyLab\adminkit\1093.working\share\Updates\

ولا يمكن استعادة بيانات خادم الإدارة إلا باستخدام أداة klbackup المساعدة. ويجب أن تنفذ الاستعادة على مثيل قابل للتشغيل لخادم الإدارة الذي تم تثبيته للتو وله نفس الإصدار (أو أحدث) الذي تم إنشاء النسخة الاحتياطية له.

مهمة النسخ الاحتياطي لبيانات خادم الإدارة

إنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة

مهمة النسخ الاحتياطي هي مهمة لخادم الإدارة؛ ويتم إنشاؤها من خلال معالج البدء السريع. إذا تم حذف مهمة منشأة بواسطة "معالج البدء السريع"، يمكنك إنشاء مهمة يدويًا.

لإنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. بدء إنشاء المهمة بإحدى الطرق التالية:
   - عن طريق تحديد **جديد** ← **مهمة** في قائمة سياق مجلد **المهام** في شجرة وحدة التحكم.
   - بالنقر فوق الزر **إنشاء مهمة** في مساحة العمل.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج. في نافذة **تحديد نوع المهمة** بالمعالج، حدد نوع المهمة الذي يحمل الاسم **النسخ الاحتياطي لبيانات خادم الإدارة**.

يمكن إنشاء مهمة **النسخ الاحتياطي لبيانات خادم الإدارة** في نسخة مفردة فقط. في حالة إنشاء مهمة النسخ الاحتياطي لبيانات خادم الإدارة بالفعل لخادم الإدارة، لا يتم عرضها في نافذة تحديد نوع المهمة لمعالج إنشاء مهمة النسخ الاحتياطي لخادم الإدارة.

تكوين مهمة النسخ الاحتياطي لبيانات خادم الإدارة

بعد إنشاء مهمة نسخ احتياطي، يمكنك تكوين إعدادات المهمة.

لتكوين مهمة النسخ الاحتياطي لبيانات خادم الإدارة:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. في قائمة السياق لمهمة **Backup of Administration Server data**، حدد **خصائص**.

تفتح نافذة خصائص مهمة النسخ الاحتياطي لبيانات خادم الإدارة. تتوفر الخصائص التالية:

- **General**

في القسم **General**، يمكنك تحديد اسم المهمة وعرض تاريخ إنشاء المهمة وتاريخ الأمر الأخير وحالات بدء المهمة ونتائجها.

- **الإخطار**

في القسم **الإخطار**، يمكنك تحديد إعدادات تخزين الأحداث المتعلقة بنتائج تنفيذ المهمة، بالإضافة إلى تكوين الإخطارات الخاصة بنتائج تنفيذ المهمة.

- **الجدول**

في القسم **الجدول**، يمكنك تحديد جدول لبدء المهمة.

- **الوجهة**

في القسم **الوجهة**، يمكنك تحديد مسار المجلد الذي سيخزن النسخ الاحتياطية لبيانات خادم الإدارة.

- **إعدادات**

في القسم **إعدادات**، يمكنك تعيين كلمة مرور حماية النسخ الاحتياطي وعدد النُسخ الاحتياطية إذا لزم الأمر.

يمكنك أيضًا إنشاء نسخة احتياطية من القرص المنطقي يخزن المجلد %ALLUSERSPROFILE% ونسخ قاعدة بيانات خادم الإدارة. ولفعل ذلك، يجب تمكين الخيار **Use a file system snapshot for data backup**، ثم تحديد اسم وكلمة مرور حساب يمتلك الإذن لإنشاء لقطات.

- **الأمان**

في القسم **الأمان**، يمكنك منح المستخدمين والمجموعات أذونات لإجراء العمليات على خادم الإدارة. إذا تم تمكين الخيار **توريث الإعدادات من خادم الإدارة**، يتم توريث إعدادات الأمان للمهمة من خادم الإدارة.

إذا تم تعطيل هذا الخيار، فبإمكانك تكوين إعدادات الأمان للمهمة. يمكنك تعيين دور لمستخدم أو مجموعة من المستخدمين أو تعيين أذونات لمستخدم أو مجموعة من المستخدمين، كما هو مطبق على المهمة.

بشكل افتراضي ، يتم تمكين الخيار **توريث الإعدادات من خادم الإدارة**.

- **سجل المراجعة**

في القسم **سجل المراجعة**، يمكنك تتبع تعديل المهمة . وفي كل مرة تحفظ فيها التغييرات التي أُجريت على المهمة، يتم إنشاء مراجعة.

الأداة المساعدة لنسخ البيانات احتياطيًا واستعادتها (klbackup)

يمكنك نسخ بيانات خادم الإدارة للنسخ الاحتياطي واسترجاعها في المستقبل باستخدام أداة klbackup المساعدة التي تعد جزءًا من حزمة توزيع Kaspersky Security Center.

ويمكن تشغيل أداة klbackup المساعدة في وضع من الوضعين التاليين:

- التفاعلي
- صامت

النسخ الاحتياطي للبيانات واستعادتها في الوضع التفاعلي

قد تحدث أخطاء أثناء استعادة بيانات خادم الإدارة من نسخة احتياطية تم إنشاؤها باستخدام الأداة المساعدة klbackup في الوضع التفاعلي. إذا قمت بتثبيت التصحيح 15.1.0.20748-pf2 لخادم الإدارة، ثم أنشأت نسخة احتياطية باستخدام الأداة المساعدة klbackup مع تعطيل خيار **ترحيل قاعدة البيانات**، فسيحدث خطأ عند استعادة هذه النسخة (لكل أنظمة إدارة قواعد البيانات باستثناء MySQL وMariaDB). إذا كان التصحيح 15.1.0.20748-pf2 لخادم الإدارة مُثبتًا لديك وترغب في إنشاء نسخة احتياطية دون الترحيل إلى نظام إدارة قواعد بيانات (DBMS) آخر، فاستخدم مهمة النسخ الاحتياطي للبيانات أو قم بتشغيل الأداة المساعدة klbackup من سطر الأوامر.

لإنشاء نسخة احتياطية من بيانات خادم الإدارة في الوضع التفاعلي:

1. قم بتشغيل الأداة المساعدة klbackup الموجودة في مجلد تثبيت Kaspersky Security Center.

   يبدأ معالج النسخ الاحتياطي والاستعادة.

2. في النافذة الأولى من المعالج حدد **إجراء النسخ الاحتياطي لبيانات خادم الإدارة**.

   إذا قمت بتحديد خيار **استعادة شهادة خادم الإدارة أو نسخها احتياطيًا فقط**، سيتم حفظ نسخة احتياطية من شهادة خادم الإدارة والمفتاح الخاص فقط. قد يكون النسخ الاحتياطي لشهادة خادم الإدارة والمفتاح الخاص مفيدًا عند إجراء الترحيل من خادم إدارة Kaspersky Security Center Windows إلى خادم إدارة Kaspersky Security Center Linux. يمكنك أيضًا ترحيل الأجهزة المدارة بين خوادم الإدارة في Kaspersky Security Center Linux، وكذلك بين خوادم إدارة Kaspersky Security Center Windows. وللمزيد من المعلومات، انظر استخدام الأداة المساعدة klbackup لتبديل الأجهزة المدارة تحت إدارة خادم إدارة آخر.

   انقر فوق **التالي**.

3. في النافذة التالية من المعالج، حدد الخيارات التالية:

   - **المجلد الوجهة للنسخ الاحتياطي**
   - **ترحيل قاعدة البيانات**

   قم بتمكين هذا الخيار إذا كنت تخزن حاليًا بيانات خادم الإدارة في قاعدة بيانات Microsoft SQL Server وتحتاج إلى ترحيلها إلى إحدى قواعد البيانات التالية: MySQL أو MariaDB أو PostgreSQL أو Postgres Pro أو Azure SQL. يتم تعطيل هذا الخيار افتراضيًا.

   - **الانتقال إلى تنسيق MySQL / MariaDB**

   قم بتمكين هذا الخيار إذا كنت تستخدم خادم SQL حاليًا باعتباره DBMS لخادم الإدارة وتريد ترحيل البيانات من خادم SQL إلى MySQL أو MariaDB DBMS. سينشئ Kaspersky Security Center نسخة احتياطية متوافقة مع MySQL وMariaDB. بعد ذلك، يمكنك استعادة البيانات من النسخة الاحتياطية إلى MySQL أو MariaDB.

   - **الترحيل إلى Postgres**

   قم بتمكين هذا الخيار إذا كنت تستخدم خادم SQL حاليًا باعتباره نظام إدارة قواعد البيانات لخادم الإدارة وتريد ترحيل البيانات من خادم SQL إلى PostgreSQL أو Postgres Pro DBMS. سينشئ Kaspersky Security Center نسخة احتياطية متوافقة مع PostgreSQL وPostgres Pro. بعد ذلك، يمكنك استعادة البيانات من النسخة الاحتياطية إلى PostgreSQL وPostgres Pro.

   يصبح هذا الخيار متاحًا إذا طلبت من الدعم الفني في Kaspersky وقمت بتثبيت التصحيح 15.1.0.20748-pf2 لخادم الإدارة أو التحديث إلى الإصدار 15.1.0.22239 من Kaspersky Security Center.

   - **الترحيل إلى تنسيق Azure**

   قم بتمكين هذا الخيار إذا كنت تستخدم خادم SQL حاليًا باعتباره DBMS لخادم الإدارة وتريد ترحيل البيانات من خادم SQL إلى Azure SQL DBMS. سيقوم Kaspersky Security Center بإنشاء نسخة احتياطية متوافقة مع Azure SQL. بعد ذلك، يمكنك استعادة البيانات من النسخة الاحتياطية إلى Azure SQL.

- **قم بتضمين التاريخ والوقت الحاليين في اسم مجلد وجهة النسخ الاحتياطي**
- **كلمة مرور النسخ الاحتياطي**

4. انقر فوق زر **التالي** لبدء النسخ الاحتياطي.

5. إذا كنت تتعامل مع قاعدة بيانات في بيئة سحابة مثل Amazon Web Services (AWS) أو Microsoft Azure، فقم بملء الحقول التالية في النافذة **تسجيل الدخول إلى التخزين عبر الإنترنت**:

- بالنسبة لـ AWS:

- **اسم مستودع S3**

اسم مستودع S3 الذي قمت بإنشائه للنسخ الاحتياطي.

- **معرف مفتاح الوصول**

لقد تلقيت معرف المفتاح (عبارة عن تسلسل من الحروف الأبجدية الرقمية) عند إنشائك حساب مستخدم IAM للتعامل مع مثيل تخزين مستودع S3.

يكون الحقل متاحًا في حالة تحديد قاعدة بيانات RDS على مستودع S3.

- **المفتاح السري**

المفتاح السري الذي تلقيته مع معرف مفتاح الوصول عند إنشائك حساب مستخدم IAM.

تظهر حروف المفتاح السري في صورة علامة النجمة. بعد أن تبدأ في إدخال المفتاح السري، سيظهر الزر **إظهار** . انقر مع الاستمرار فوق هذا الزر لتحديد الفترة الزمنية اللازمة لإظهار الحروف التي أدخلتها.

هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

- بالنسبة لـ Microsoft Azure:

- **اسم حساب تخزين Azure**

لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

- **معرف اشتراك Azure**

لقد قمت بإنشاء الاشتراك على مدخل Azure.

- **كلمة مرور Azure**

لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

- **معرف تطبيق Azure**

لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

- **اسم خادم Azure SQL Server**

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

- **مجموعة مورد خادم Azure SQL Server**

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

- **مفتاح وصول تخزين Azure**

يكون متاحًا في خصائص حساب التخزين الخاص بك، في قسم مفاتيح الوصول. يمكنك استخدام أي من المفاتيح (المفتاح1 أو المفتاح2).

لاستعادة بيانات خادم الإدارة في الوضع التفاعلي:

1. قم بتشغيل الأداة المساعدة klbackup الموجودة في مجلد تثبيت Kaspersky Security Center. يجب بدء الأداة المساعدة تحت نفس الحساب الذي استخدمته لتثبيت خادم الإدارة. نوصي بتشغيل الأداة المساعدة على خادم إدارة تم تثبيته حديثًا.

   يبدأ معالج النسخ الاحتياطي والاستعادة.

2. في النافذة الأولى من المعالج، حدد **استعادة بيانات خادم الإدارة**، ثم انقر فوق **التالي**.

   إذا قمت بتحديد الخيار **استعادة شهادة خادم الإدارة أو نسخها احتياطيًا فقط**، سيتم استعادة شهادة خادم الإدارة والمفتاح الخاص فقط.

   عند تشغيل الأداة المساعدة klbackup على عقدة نظام مجموعة تجاوز الفشل غير النشطة، ستتم مطالبتك بتحديد أحد الخيارات: تحديد شهادة خادم الإدارة أو استرداد البيانات تلقائيًا من خادم الإدارة.

3. في النافذة **استعادة الإعدادات** الخاصة بالمعالج:

   - حدد المجلد الذي يحتوي على نسخة احتياطية من بيانات خادم الإدارة.

     إذا كنت تستخدم بيئة سحابة كـ AWS، أو Azure، حدد عنوان المخزن. أيضًا، يجب عليك التأكد أن الملف باسم backup.zip.

   - حدد كلمة المرور التي تم إدخالها أثناء النسخ الاحتياطي للبيانات.

     عند استعادة البيانات، يجب عليك تحديد نفس كلمة المرور التي تم إدخالها أثناء النسخ الاحتياطي. إذا تم تغيير مسار المجلد المشترك بعد النسخ الاحتياطي، فقم بالتحقق من تشغيل المهام التي تستخدم البيانات التي تمت استعادتها (مهام الاستعادة ومهام التثبيت عن بُعد). إذا لزم الأمر، قم بتحرير إعدادات هذه المهام. بينما تتم استعادة البيانات من ملف النسخ الاحتياطي، فلا يجوز لأحد الوصول للمجلد المشترك لخادم الإدارة. يجب أن يكون للحساب الذي تعمل بموجبه أداة النسخ الاحتياطي وصول كامل للمجلد المشترك.

4. انقر فوق زر **التالي** لاستعادة البيانات.

النسخ الاحتياطي للبيانات واستعادتها في الوضع الصامت

لإنشاء نسخة احتياطية من بيانات خادم الإدارة أو استعادتها في الوضع الصامت:

قم بتشغيل الأداة klbackup التي تحتوي على مجموعة المفاتيح المطلوبة من سطر الأوامر بالجهاز المثبت عليه خادم الإدارة.

> لا تتم استعادة علامات عميل الشبكة عند استخدام الأداة المساعدة klbackup. ويتعين عليك تكوين علامات عميل الشبكة يدويًا.

يجب أن يستخدم مثيل خادم الإدارة الذي سيتم إجراء الاستعادة عليه نظام إدارة قواعد البيانات (DBMS) من النوع نفسه. يمكن أن يكون إصدار خادم الإدارة هو نفسه (بتصحيح مشابه أو أحدث) أو إصدار أحدث.

بناء جملة سطر الأوامر للأداة المساعدة:

```
klbackup -path <backup path> [-linux_path <مسار النسخ الاحتياطي لخادم SQL Server>]-
node_cert <مسار الشهادة> [-logfile <ملف السجل> [-use_ts]|[-restore] [-password
<كلمة المرور>] [-cert_only] [-online] [-migrate postgres]
```

> إذا لم يتم تحديد كلمة مرور في سطر الأوامر بأداة klbackup المساعدة، فستطالبك الأداة بإدخال كلمة مرور بشكل تفاعلي.

مواصفات المفاتيح:

- `-path <backup path>` - احفظ المعلومات في مجلد النسخ الاحتياطي المحدد، أو استخدم البيانات من مجلد النسخ الاحتياطي للاسترداد (المعلمة الإلزامية)

  يجب منح حساب خادم قاعدة البيانات وأداة klbackup المساعدة الأذون الخاصة بتغيير البيانات في مجلد النسخ الاحتياطي

- `-linux_path <SQL Server backup path>` - المسار المحلي للمجلد الذي يحتوي على بيانات النسخ الاحتياطي لخادم SQL Server على Linux.

  يجب منح حساب خادم قاعدة البيانات وأداة klbackup المساعدة الأذون الخاصة بتغيير البيانات في مجلد النسخ الاحتياطي لنظام SQL Server

- `-node_cert <certificate path>` - ملف شهادة الخادم لتكوين عقدة نظام مجموعة تجاوز الفشل غير النشطة بعد الاسترداد. إذا لم يتم تعيينها، فسيتم استردادها تلقائيًا من الخادم.

  عند تشغيل الأداة المساعدة klbackup على عقدة نظام مجموعة تجاوز الفشل غير النشطة، استخدم هذا المفتاح لتحديد المسار إلى شهادة الخادم.

- `-logfile <log file>` - حفظ تقرير عن النسخ الاحتياطي لبيانات خادم الإدارة واستعادتها.

- `-use_ts` - عند حفظ البيانات، انسخ المعلومات إلى مجلد النسخ الاحتياطي، وإلى المجلد الفرعي الذي يحمل اسم klbackup بتنسيق `YYYY-MM-DD # HH-MM-SS`، والذي يتضمن التاريخ الحالي ووقت التشغيل بالتوقيت العالمي المنسق. إذا لم يتم تحديد مفتاح، يتم حفظ المعلومات في جذر مجلد النسخ الاحتياطي.

  أثناء محاولة حفظ المعلومات في مجلد مُخزّن به نسخة احتياطية بالفعل، تظهر رسالة خطأ. ولن يتم تحديث أية معلومات.

  يتيح توفر المفتاح `-use_ts` الحفاظ على بأرشيف بيانات خادم الإدارة. على سبيل المثال، إذا كان مفتاح `-path` يشير إلى المجلد `C:\KLBackups`، المجلد `klbackup 2022/6/19 # 11-30-18` معلومات عن حالة خادم الإدارة اعتبارًا من 19 يونيو 2022 في تمام الساعة 18:30:11 ص.

- `-restore`—استعادة بيانات خادم الإدارة. يتم إجراء استعادة البيانات بناءً على المعلومات الموجودة في مجلد النسخ الاحتياطي. وفي حالة عدم توفر مفتاح، يتم نسخ البيانات احتياطيًا في مجلد النسخ الاحتياطي.

- `-password <password>` - كلمة مرور لحماية البيانات الحساسة.

> لا يمكن استعادة كلمة مرور منسية. لا توجد متطلبات لكلمة المرور. طول كلمة المرور غير محدود والطول الصفري (أي دون استخدام كلمة مرور) ممكن أيضًا.

عند استعادة البيانات، يجب عليك تحديد نفس كلمة المرور التي تم إدخالها أثناء النسخ الاحتياطي. إذا تم تغيير مسار المجلد المشترك بعد النسخ الاحتياطي، فقم بالتحقق من تشغيل المهام التي تستخدم البيانات التي تمت استعادتها (مهام الاستعادة ومهام التثبيت عن بُعد). إذا لزم الأمر، قم بتحرير إعدادات هذه المهام. بينما تتم استعادة البيانات من ملف النسخ الاحتياطي، فلا يجوز لأحد الوصول للمجلد المشترك لخادم الإدارة. يجب أن يكون للحساب الذي تعمل بموجبه أداة النسخ الاحتياطي وصول كامل للمجلد المشترك. نوصي بتشغيل الأداة المساعدة على خادم إدارة تم تثبيته حديثًا.

- `-cert_only` - حفظ أو استرداد الشهادة والمفتاح الخاص لخادم الإدارة فقط.

  يمكن أن تكون هذه العلامة مفيدة عند إجراء التحويل من خادم إدارة Kaspersky Security Center Windows إلى خادم إدارة Kaspersky Security Center Linux. يمكنك أيضًا ترحيل الأجهزة المدارة بين خوادم الإدارة في Kaspersky Security Center Linux، وكذلك بين خوادم إدارة Kaspersky Security Center Windows.

- `-online` - بيانات خادم الإدارة عن طريق إنشاء لقطة وحدة التخزين لتقليل الوقت غير المتصل لخادم الإدارة. عند استخدام الأداة المساعدة لاستعادة البيانات، يتم تجاهل هذا الخيار. لا تستخدم هذه العلامة عند إنشاء نسخة احتياطية للترحيل إلى نظام إدارة قواعد بيانات (DBMS) مختلف.

- - - الاحتفاظ ببيانات الخادم كملفات عادية. بشكل افتراضي (`-archive 1`)، يتم تخزين بيانات الخادم في ملف أرشيف.

- `-migrate mysql` - إنشاء نسخة احتياطية لبيانات خادم الإدارة المخزنة في قاعدة بيانات SQL Server تكون متوافقة مع MySQL (بما في ذلك MariaDB). ويمكنك استعادة البيانات من النسخة الاحتياطية إلى MySQL.

- `migrate postgres-`—إنشاء نسخة احتياطية لبيانات خادم الإدارة المخزنة في قواعد بيانات SQL Server المتوافقة مع PostgreSQL وPostgres Pro. ويمكنك استعادة البيانات من النسخة الاحتياطية إلى PostgreSQL أو Postgres Pro. استخدم هذه العلامة عند إجراء الترحيل إلى Kaspersky Security Center Linux باستخدام نسخة احتياطية لبيانات خادم الإدارة.

  يصبح هذا الخيار متاحًا إذا طلبت من الدعم الفني في Kaspersky وقمت بتثبيت التصحيح 15.1.0.20748-pf2 لخادم الإدارة أو التحديث إلى الإصدار 15.1.0.22239 من Kaspersky Security Center.

استخدام الأداة المساعدة klbackup لتبديل الأجهزة المدارة تحت إدارة خادم إدارة آخر

تسمح لك الأداة المساعدة klbackup بتبديل الأجهزة المدارة تحت إدارة خادم إدارة آخر. ويمكنك تغيير خادم إدارة Kaspersky Security Center Windows إلى خادم إدارة Kaspersky Security Center Linux باستخدام الأداة المساعدة klbackup عند إجراء الترحيل. يمكنك أيضًا ترحيل الأجهزة المدارة بين خوادم الإدارة في Kaspersky Security Center Linux، وكذلك بين خوادم إدارة Kaspersky Security Center Windows.

لتبديل الأجهزة المدارة تحت إدارة خادم إدارة آخر باستخدام الأداة المساعدة klbackup:

1. على الجهاز السابق، أنشئ نسخة احتياطية من شهادة خادم الإدارة والمفتاح الخاص.

   يمكنك إنشاء نسخة احتياطية بإحدى الطرق التالية:

   - باستخدام واجهة الأداة المساعدة klbackup (لخادم إدارة Kaspersky Security Center Windows فقط)

     قم بتشغيل الأداة المساعدة klbackup الموجودة في مجلد تثبيت Kaspersky Security Center، ثم أنشئ نسخة احتياطية باستخدام الخيار **استعادة شهادة خادم الإدارة أو نسخها احتياطيًا فقط**.

   - باستخدام موجه الأوامر (للإصدار 15.1 أو أحدث من Kaspersky Security Center Windows وخوادم الإدارة من Kaspersky Security Center Linux)

     قم بتشغيل الأداة المساعدة klbackup باستخدام المفتاح `cert_only-` من سطر الأوامر، لإنشاء نسخة احتياطية من شهادة خادم الإدارة والمفتاح الخاص:

     ```
     klbackup -path <المسار إلى النسخة الاحتياطية لشهادة خادم الإدارة> -cert_only
     ```

2. على الجهاز السابق، اقطع اتصال خادم الإدارة عن الشبكة.

3. قم بتعيين العنوان نفسه للجهاز من خلال خادم إدارة آخر.

   يمكن تعيين اسم NetBIOS وFQDN وعنوان IP الثابت لخادم الإدارة الجديد. ويعتمد ذلك على عنوان خادم الإدارة الذي تم تعيينه في حزمة تثبيت عميل الشبكة عند نشر عملاء الشبكة. وبدلاً من ذلك، يمكنك استخدام عنوان الاتصال الذي يحدد خادم الإدارة الذي يتصل به عميل الشبكة (يمكنك الحصول على هذا العنوان على الأجهزة المُدارة باستخدام الأداة المساعدة klnagchk).

4. على جهاز به خادم إدارة آخر، قم باستعادة شهادة خادم الإدارة والمفتاح الخاص من النسخة الاحتياطية.

   يمكنك استعادة نسخة احتياطية بإحدى الطرق التالية:

   - باستخدام واجهة الأداة المساعدة klbackup (لخادم إدارة Kaspersky Security Center Windows فقط)

     قم بتشغيل الأداة المساعدة klbackup، ثم قم باستعادة نسخة احتياطية باستخدام الخيار **استعادة شهادة خادم الإدارة أو نسخها احتياطيًا فقط**.

   - باستخدام موجه الأوامر (للإصدار 15.1 أو أحدث من Kaspersky Security Center Windows وخوادم الإدارة من Kaspersky Security Center Linux)

     قم بتشغيل الأداة المساعدة `cert_only-` باستخدام المفتاح cert_only- من سطر الأوامر، لاستعادة نسخة احتياطية من شهادة خادم الإدارة والمفتاح الخاص:

     ```
     klbackup -path <path to the backup copy of Administration Server certificate> -cert_only- restore
     ```

يتم وضع الأجهزة المدارة تحت إدارة خادم إدارة آخر. ويمكنك الانتقال إلى خادم الإدارة هذا والتأكد من أن الأجهزة المُدارة مرئية في الشبكة، ومن تثبيت عميل الشبكة وتشغيله عليها (القيمة نعم في الأعمدة **Visible** و**Network Agent is installed** و**Network Agent is running**).

النسخ الاحتياطي واستعادة بيانات خادم الإدارة عند استخدام MySQL أو MariaDB

يمكنك استخدام نسخة احتياطية للبيانات لترحيل بيانات خادم الإدارة من Kaspersky Security Center Windows تحت إدارة Kaspersky Security Center Linux. يتم دعم الترحيل باستخدام النسخ الاحتياطي للبيانات في خادم الإدارة فقط للترحيل إلى Kaspersky Security Center Linux 15.2 أو أحدث من أي إصدار مدعوم من Kaspersky Security Center Windows.

إذا كنت تستخدم MySQL أو MariaDB كنظام لإدارة قواعد البيانات لتطبيق Kaspersky Security Center Windows وKaspersky Security Center Linux، فيجب أن تتطابق معلمة `lower_case_table_names` مع نظامي إدارة قواعد البيانات الحالي والجديد. وإلا، فسيتم ترحيل بيانات خادم الإدارة بشكل غير صحيح.

قبل إجراء نسخ احتياطي لبيانات خادم الإدارة على Kaspersky Security Center Windows، تحقق من قيمة معلمة `lower_case_table_names`. إذا لم تحدد هذه المعلمة أثناء تثبيت المُثبت لنظام إدارة قاعدة البيانات في وقت سابق، فسيتم استخدام قيمة المعلمة الافتراضية. القيمة الافتراضية لمعلمة `lower_case_table_names` لنظام التشغيل Windows هي 1.

عند تثبيت MySQL أو MariaDB لتطبيق Kaspersky Security Center Linux، اضبط معلمة `lower_case_table_names` على القيمة نفسها المحددة لهذه المعلمة لنظام Windows باستخدام التعليمات من موقع ويب MySQL. إذا لم تحدد هذه المعلمة، فسيتم استخدام قيمة المعلمة الافتراضية. وبالنسبة لأنظمة التشغيل المستندة إلى Linux، تختلف القيمة الافتراضية لمعلمة `lower_case_table_names` عن القيمة الافتراضية لنظام Windows.

إذا كنت تريد تثبيت MySQL 8.0، فقد لا يعمل تحديد معلمة `lower_case_table_names` وفقًا لهذه التعليمات. وفي هذه الحالة، يجب عليك أولاً تثبيت MySQL 5.7 باستخدام المُثبت، وتحديد معلمة `lower_case_table_names` باستخدام التعليمات، ثم قم بترقية MySQL 5.7 إلى MySQL 8.0. وإذا لم تتطابق معلمة `lower_case_table_names` مع أنظمة إدارة قواعد البيانات الحالية والجديدة، فسيتم استعادة بيانات خادم الإدارة بشكل غير صحيح.

تحسين النسخ الاحتياطي واستعادة بيانات خادم الإدارة

لتحسين النسخ الاحتياطي واستعادة بيانات خادم الإدارة لتقليل وقت تعطل خادم الإدارة، نفذ أحد الخيارات التالية:

- قم بتمكين الخيار **استخدام لقطة نظام الملفات للنسخ الاحتياطي للبيانات**.

  راجع المقالة التالية للحصول على التفاصيل: استخدام لقطة نظام الملفات لتقليل مدة النسخ الاحتياطي.

- قم بتكوين العلامات التالية:

  قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Security Center\Lab.

- `KLSRV_BKP_FILES` – تقسيم ملف قاعدة البيانات إلى ملفات متعددة أصغر، من 2 إلى 32. ويمكن أن يؤدي هذا إلى تسريع عملية النسخ الاحتياطي والاستعادة إذا كان أداء نظام إدارة قاعدة البيانات مقيدًا بواسطة وحدة المعالجة المركزية.

  مثال:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
  ```

- `KLSRV_BKP_BACKUP_EXTRA_PARS` – يحدد معلمتي `COMPRESSION` و `MAXTRANSFERSIZE`. ويمكن أن يؤدي ذلك إلى تسريع النسخ الاحتياطي إذا كان أداء نظام إدارة قاعدة البيانات مقيدًا بإدخال/إخراج الملف.

  مثال:

  ```
  klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION, MAXTRANSFERSIZE = 4194304"
  ```

- `KLSRV_BKP_RESTORE_EXTRA_PARS` – يحدد معلمة `MAXTRANSFERSIZE`. ويمكن أن يؤدي ذلك إلى تسريع الاستعادة إذا كان أداء نظام إدارة قاعدة البيانات مقيدًا بإدخال/إخراج الملف.

مثال:

```
MAXTRANSFERSIZE" klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v
"4194304 =
```

- KLSRV_BKP_ONLINE_DB_BACKUP - يزيل وقت تعطل خادم الإدارة أثناء النسخ الاحتياطي. متاح فقط لأنظمة إدارة قواعد البيانات التالية:
  - PostgreSQL وPostgres Pro
  - SQL Server مع نموذج الاسترداد الكامل. يرجى الرجوع إلى وثائق SQL Server للحصول على التفاصيل. وعند تمكين علامة KLSRV_BKP_ONLINE_DB_BACKUP، يتم تحويل SQL Server DBMS تلقائيًا إلى نموذج الاسترداد الكامل.

مثال:

```
klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
```

نقل خادم إدارة إلى جهاز آخر

إذا كنت بحاجة إلى استخدام خادم الإدارة على جهاز جديد، فيمكنك نقله بإحدى الطرق التالية:

- انقل خادم الإدارة وخادم قاعدة البيانات إلى جهاز جديد (يمكن تثبيت خادم قاعدة البيانات على الجهاز الجديد مع خادم الإدارة، أو على جهاز آخر).
- احتفظ بخادم قاعدة البيانات على الجهاز السابق وانقل خادم الإدارة فقط إلى جهاز جديد.

لنقل خادم الإدارة إلى جهاز جديد:

1. على الجهاز السابق، أنشئ نسخة احتياطية من بيانات خادم الإدارة.

لفعل ذلك، يمكنك تشغيل مهمة النسخ الاحتياطي للبيانات من خلال وحدة تحكم الإدارة أو تشغيل الأداة المساعدة klbackup.

إذا كنت تستخدم SQL Server كنظام لإدارة قاعدة البيانات لخادم الإدارة، يمكنك ترحيل البيانات من SQL Server إلى MySQL أو MariaDB DBMS. للقيام بذلك، قم بتشغيل الأداة المساعدة klbackup في الوضع التفاعلي لإنشاء نسخة احتياطية للبيانات. قم بتمكين ملف **الانتقال إلى تنسيق MySQL / MariaDB** الخيار في **إعدادات النسخ الاحتياطي** نافذة معالج النسخ الاحتياطي والاستعادة. سينشئ Kaspersky Security Center نسخة احتياطية متوافقة مع MySQL وMariaDB. بعد ذلك، يمكنك استعادة البيانات من النسخة الاحتياطية إلى MySQL أو MariaDB.

يمكنك أيضًا تمكين **الترحيل إلى تنسيق Azure** الخيار إذا كنت تريد ترحيل البيانات من SQL Server إلى Azure SQL DBMS.

2. على الجهاز السابق، اقطع اتصال خادم الإدارة عن الشبكة.
3. حدد جهازًا جديدًا لتثبيت خادم الإدارة عليه. تأكد أن الأجهزة والبرامج الموجودة على الجهاز المحدد تفي بمتطلبات خادم الإدارة ووحدة تحكم الإدارة وعميل الشبكة. تحقق أيضًا من توفر المنافذ المستخدمة في خادم الإدارة.
4. تعيين العنوان نفسه للجهاز الجديد.

يمكن تعيين اسم NetBIOS وFQDN وعنوان IP الثابت لخادم الإدارة الجديد. ويعتمد ذلك على عنوان خادم الإدارة الذي تم تعيينه في حزمة تثبيت عميل الشبكة عند نشر عملاء الشبكة. وبدلاً من ذلك، يمكنك استخدام عنوان الاتصال الذي يحدد خادم الإدارة الذي يتصل به عميل الشبكة (يمكنك الحصول على هذا العنوان على الأجهزة المُدارة باستخدام الأداة المساعدة klnagchk).

5. إذا لزم الأمر، على جهاز آخر، قم بتثبيت نظام إدارة قاعدة البيانات (DBMS) الذي سيستخدمه خادم الإدارة.

يمكن تثبيت قاعدة البيانات على الجهاز الجديد مع خادم الإدارة، أو على جهاز آخر. تأكد أن هذا الجهاز يلبي متطلبات الأجهزة والبرامج. عند تحديد DBMS، ضع في اعتبارك عدد الأجهزة التي يغطيها خادم الإدارة.

6. قم بتشغيل تثبيت خادم الإدارة على الجهاز الجديد.

7. أثناء تثبيت خادم الإدارة، قم بتكوين إعدادات اتصال خادم قاعدة البيانات.

مثال على نافذة إعدادات الاتصال لـ Microsoft SQL Server

بناءً على المكان الذي تريد تحديد موقع خادم قاعدة البيانات فيه، قم بأحد الإجراءات التالية:

- **احتفظ بخادم قاعدة البيانات على الجهاز السابق**

1. انقر على **استعراض** بجانب **اسم مثيل خادم SQL Server**، ثم حدد اسم الجهاز السابق في القائمة التي تظهر.

   لاحظ أن الجهاز السابق يجب أن يكون متاحًا للاتصال بخادم الإدارة الجديد.

2. أدخل اسم قاعدة البيانات السابقة في ملف **اسم قاعدة البيانات** مجال.

- **انقل خادم قاعدة البيانات إلى جهاز آخر**

1. انقر على **استعراض** بجانب **اسم مثيل خادم SQL Server**، ثم حدد اسم الجهاز في القائمة التي تظهر.

2. أدخل اسم قاعدة البيانات الجديدة في ملف **اسم قاعدة البيانات** مجال.

لاحظ أن اسم قاعدة البيانات الجديدة يجب أن يتطابق مع اسم قاعدة البيانات من الجهاز السابق. يجب أن تكون أسماء قواعد البيانات متطابقة، بحيث يمكنك استخدام النسخة الاحتياطية لخادم الإدارة. اسم قاعدة البيانات الافتراضي هو KAV.

8. بعد اكتمال التثبيت، قم باستعادة بيانات خادم الإدارة على الجهاز الجديد باستخدام الأداة المساعدة klbackup.

إذا كنت تستخدم SQL Server كنظام DBMS على الأجهزة السابقة والجديدة، فلاحظ أن إصدار SQL Server المثبت على الجهاز الجديد يجب أن يكون هو نفسه أو أحدث من إصدار SQL Server المثبت على الجهاز السابق. خلاف ذلك، لا يمكنك استعادة بيانات خادم الإدارة على الجهاز الجديد.

9. فتح وحدة تحكم الإدارة والاتصال بخادم الإدارة.

10. تحقق من أن جميع الأجهزة المُدارة متصلة بخادم الإدارة.

11. قم بإلغاء تثبيت خادم الإدارة وخادم قاعدة البيانات من الجهاز السابق.

يمكنك أيضا استخدام Kaspersky Security Center Web Console لنقل خادم الإدارة وخادم قاعدة البيانات إلى جهاز آخر.

تجنب التعارض بين العديد من خوادم الإدارة

إذا كان لديك أكثر من خادم إدارة واحد على شبكتك، فإنه يمكن لهذه الخوادم رؤية نفس الأجهزة العميلة. وقد ينتج عن ذلك، على سبيل المثال، تثبيت خادم الإدارة لتطبيق تم تثبيته بالفعل بواسطة خادم إدارة آخر، وتعارضات أخرى. ولمنع تثبيت تطبيق على جهاز مُدار بواسطة خادم إدارة آخر، يجب عليك تمكين خيار **يتم التثبيت فقط على الأجهزة المُدارة من خلال خادم الإدارة هذا** في خصائص مهمة Install application remotely.

إذا قمت بتمكين الخيار **يتم التثبيت فقط على الأجهزة المُدارة من خلال خادم الإدارة هذا**، وقمت بتشغيل مهمة Install application remotely، يتم إجراء فحص لتحديد ما إذا كانت إدارة الأجهزة تتم بواسطة خادم إدارة آخر. وبالنسبة للأجهزة المدارة بواسطة خادم إدارة آخر، سيتم تعيين قيمة السمة **تتم إدارته بواسطة خادم إدارة مختلف** على `true`. ولن يتم تطبيق مهمة Install application remotely على هذه الأجهزة.

يتم عرض قيم سمة **تتم إدارته بواسطة خادم إدارة مختلف** في عمود **تتم إدارته بواسطة خادم إدارة مختلف** في قائمة الأجهزة المُدارة وقائمة الأجهزة غير المخصصة.

يمكنك كذلك استخدام الخاصية **تتم إدارته بواسطة خادم إدارة مختلف** كمعيار للأغراض التالية:

- البحث عن الأجهزة
- تحديدات الأجهزة
- قواعد نقل الجهاز
- قواعد وضع العلامات تلقائيًا

لإعادة تعيين سمة تتم إدارته بواسطة خادم إدارة مختلف:

1. في القائمة الرئيسية لبرنامج Kaspersky Security Center Web Console، انتقل إلى **Discovery & deployment** ← **Unassigned devices**.
2. حدد الجهاز المطلوب، ثم انقر فوق الزر **Remove the Managed by a different Administration Server attribute**.

تتم إعادة تعيين سمة **تتم إدارته بواسطة خادم إدارة مختلف**.

إدارة مجموعات الإدارة

يوفر هذا القسم معلومات عن كيفية إدارة مجموعات الإدارة.

يمكنك تنفيذ الإجراءات التالية على مجموعات الإدارة:

- إضافة أي عدد من المجموعات المتداخلة عند أي مستوى تسلسل هيكلي إلى مجموعات الإدارة.
- إضافة أجهزة إلى مجموعات الإدارة.
- تغيير التسلسل الهيكلي لمجموعات الإدارة من خلال نقل الأجهزة الفردية والمجموعات ككل إلى مجموعات أخرى.
- إزالة المجموعات المتداخلة والأجهزة من مجموعات الإدارة.
- إضافة خوادم إدارة ثانوية وظاهرية إلى مجموعات الإدارة.
- نقل الأجهزة من مجموعات الإدارة لخادم إدارة إلى مجموعات الإدارة الخاصة بخادم آخر.
- تحديد تطبيقات Kaspersky التي سيتم تثبيتها تلقائيًا على الأجهزة المضمنة في مجموعة.

لا يمكنك القيام بهذه الإجراءات إلا في حالة امتلاكك إذن التعديلفي نطاق **إدارة مجموعات الإدارة** لمجموعات الإدارة التي ترغب في إدارتها (أو لخادم الإدارة الذي تنتمي له هذه المجموعات).

إنشاء مجموعات إدارة

يتم إنشاء التسلسل الهرمي لمجموعات الإدارة في نافذة التطبيق الرئيسية في Kaspersky Security Center، وذلك بمجلد **الأجهزة المدارة**. يتم عرض مجموعات الإدارة كمجلدات في شجرة وحدة التحكم (انظر الشكل أدناه).

على الفور بعد تثبيت Kaspersky Security Center، يحتوي المجلد **الأجهزة المُدارة** فقط على مجلد **خوادم إدارة** فارغ.

تحدد إعدادات واجهة المستخدم ما إذا كان مجلد **خوادم الإدارة** سيظهر في شجرة وحدة التحكم. لعرض هذا المجلد، على شريط القائمة حدد **عرض** > **واجهة التكوين**، وفي نافذة **واجهة التكوين** التي تفتح، حدد خانة الاختيار **عرض خوادم الإدارة الثانوية**.

عند إنشاء ترتيب هرمي لمجموعات الإدارة، يمكنك إضافة الأجهزة والأجهزة الظاهرية إلى المجلد **الأجهزة المُدارة** وكذلك إضافة المجموعات المتداخلة. يمكنك إضافة خوادم الإدارة الافتراضية إلى مجلد **خوادم الإدارة**.

وتمامًا مثل المجلد **الأجهزة المُدارة**، تحتوي كل مجموعة تم إنشاؤها في بادئ الأمر على مجلد **خوادم الإدارة** فارغ بغرض التعامل مع خوادم الإدارة الافتراضية الخاصة بهذه المجموعة. يتم عرض معلومات عن السياسات والمهام للمجموعة ومعلومات عن الأجهزة الموجودة في هذه المجموعة في علامات التبويب ذات الأسماء المقابلة في مساحة عمل هذه المجموعة.

عرض الترتيب الهرمي لمجموعات الإدارة

لإنشاء مجموعة إدارة:

1. في شجرة وحدة التحكم، قم بتوسيع المجلد **الأجهزة المُدارة**.

2. إذا كنت تريد إنشاء مجموعة فرعية من مجموعة إدارة حالية، في المجلد **الأجهزة المُدارة** حدد مجلدًا فرعيًا يتطابق مع المجموعة التي ستتضمن مجموعة الإدارة الجديدة.

   إذا قمت بإنشاء مجموعة إدارة جديدة بالمستوى الأعلى، يمكنك تجاوز هذه الخطوة.

3. يمكنك بدء إنشاء مجموعة الإدارة بإحدى الطرق التالية:

   - من خلال استخدام الأمر **جديد** ← **مجموعة**مجموعة في قائمة السياق.
   - بالنقر فوق الزر **مجموعة جديدة** الموجود في مساحة عمل نافذة التطبيق الرئيسية، في علامة التبويب **الأجهزة**.

4. في نافذة **اسم المجموعة** التي تفتح، أدخل اسم المجموعة، ثم انقر فوق **موافق**.

   يظهر مجلد مجموعة الإدارة الجديد ذو الاسم المحدد في شجرة وحدة التحكم.

يتيح التطبيق إنشاء تسلسل هرمي لمجموعات الإدارة بناءً على هيكل Active Directory أو هيكل شبكة المجال. وكذلك، يمكنك إنشاء هيكل من المجموعات من ملف نصي.

لإنشاء هيكل لمجموعات الإدارة:

1. في شجرة وحدة التحكم، افتح المجلد **الأجهزة المُدارة**.

2. في قائمة السياق الخاصة بالمجلد **الأجهزة المُدارة**، حدد **جميع المهام** ← **بنية مجموعة جديدة**.

يبدأ معالج بنية مجموعة الإدارة الجديدة. اتبع إرشادات المعالج.

نقل مجموعات الإدارة

يمكنك نقل مجموعات الإدارة المتداخلة داخل التسلسل الهيكلي للمجموعات.

يتم نقل مجموعة الإدارة مع كل المجموعات المتداخلة وخوادم الإدارة الثانوية والأجهزة وسياسات المجموعة والمهام. سيطبق النظام على المجموعة كل الإعدادات التي تقابل موقعه الجديد في التسلسل الهيكلي لمجموعات الإدارة.

يجب أن يكون اسم المجموعة فريدًا في نطاق مستوى واحد للتسلسل الهرمي. إذا كانت توجد مجموعة لها نفس الاسم بالفعل في المجلد الذي تنقل إليه مجموعة الإدارة، فينبغي عليك تغيير اسم المجموعة التي يتم نقلها. إذا لم تقم بتغيير اسم المجموعة المنقولة، فستتم إضافة فهرس بتنسيق **<رقم التسلسل التالي>** تلقائيًا إلى اسمها عند نقلها، على سبيل المثال: **(1)**، **(2)**.

لا يمكنك إعادة تسمية المجموعة **الأجهزة المدارة** لأنه عنصر مضمن بوحدة تحكم الإدارة.

لنقل مجموعة إلى مجلد آخر في شجرة وحدة التحكم:

1. حدد مجموعة للنقل في شجرة وحدة التحكم.

2. قم بأحد الإجراءات التالية:

- نقل المجموعة باستخدام قائمة السياق:

  1. حدد **قص** من قائمة سياق المجموعة.

  2. حدد **لصق** من قائمة سياق مجموعة الإدارة التي ترغب في نقل المجموعة المحددة إليها.

- نقل المجموعة باستخدام قائمة التطبيق الرئيسية:

  a. من القائمة الرئيسية، حدد **الإجراء** ← **قص**.

  b. حدد مجموعة الإدارة التي يجب نقل المجموعة المحددة إليها، في شجرة وحدة التحكم.

  c. من القائمة الرئيسية، حدد **الإجراء** > **لصق**.

- انقل المجموعة إلى مجموعة أخرى في شجرة وحدة التحكم باستخدام الماوس.

حذف مجموعات الإدارة

يمكنك حذف مجموعة إدارة إذا كانت لا تحتوي على خوادم إدارة ثانوية أو مجموعات متداخلة أو أجهزة عميلة وفي حالة عدم إنشاء مهام مجموعة أو سياسات لها.

قبل حذف مجموعة إدارة، يجب عليك حذف كل خوادم الإدارة الثانوية والمجموعات المتداخلة والأجهزة العميلة من هذه المجموعة.

لحذف مجموعة:

1. حدد مجموعة إدارة في شجرة وحدة التحكم.

2. قم بأحد الإجراءات التالية:

- حدد **حذف** من قائمة سياق المجموعة.
- من قائمة التطبيق الرئيسية، حدد **إجراء** > **حذف**.
- اضغط على المفتاح **DELETE**.

الإنشاء التلقائي لبنية مجموعات الإدارة

يتيح Kaspersky Security Center إمكانية إنشاء بنية مجموعات الإدارة باستخدام معالج إنشاء هيكل المجموعات.

يتم من خلال المعالِج إنشاء بنية مجموعات الإدارة بناءً على البيانات التالية:

- هياكل مجالات Windows ومجموعات العمل
- هياكل مجموعات Active Directory؛
- محتويات ملف النص الذي تم إنشاؤه يدويًا بواسطة المسؤول

عندما يتم إنشاء ملف النص، يجب استيفاء المتطلبات التالية:

- يجب أن يبدأ اسم كل مجموعة جديدة بسطر جديد؛ ويجب أن يبدأ المحدِد بفاصل أسطر. يتم تجاهل الأسطر الفارغة.

  مثال:

  المكتب 1

  المكتب 2

  المكتب 3

  سيتم إنشاء ثلاث مجموعات من المستوى الأول للتسلسل الهرمي في المجموعة الهدف.

- يجب إدخال اسم المجموعة المتداخلة مع علامة الشرطة المائلة (/).

  مثال:

  المكتب 1/الفرع 1/القسم 1/المجموعة 1

  سيتم إنشاء أربع مجموعات فرعية متداخلة مع بعضها البعض في المجموعة الهدف.

- لإنشاء مجموعات متداخلة متعددة من نفس مستوى التسلسل الهرمي، يجب تحديد "المسار الكامل للمجموعة".

  مثال:

  المكتب 1/الفرع 1/القسم 1

  المكتب 2/الفرع 1/القسم 1

  المكتب 1/الفرع 3/القسم 1

  المكتب 1/الفرع 4/القسم 1

  سيتم إنشاء مجموعة واحدة من مستوى الترتيب الهرمي المكتب 1 في المجموعة الهدف؛ ستشمل هذه المجموعة أربع مجموعات متداخلة من نفس مستوى الترتيب الهرمي: "الفرع 1" و"الفرع 2" و"الفرع 3" و"الفرع 4". ستتضمن كل مجموعة من هذه المجموعات مجموعة "القسم 1".

إنشاء التسلسل الهرمي للمجموعات الإدارية من خلال المعالج لا يوثر على تكامل الشبكة: بدلاً من خروج المجموعات التي يتم استبدالها، سيتم إضافة مجموعات جديدة. لا يمكن تضمين جهاز عميل في مجموعة إدارة للمرة الثانية حيث أن الجهاز قد تمت إزالته من المجموعة **الأجهزة غير المخصصة** عند نقله إلى مجموعة الإدارة.

أثناء إنشاء بنية مجموعة الإدارة، إذا لم يكن الجهاز مضمنًا في المجموعة **الأجهزة غير المخصصة** لأي سبب كان (تم إيقاف تشغيله أو قطع اتصاله بالشبكة)، فلن يتم نقل الجهاز تلقائيًا إلى مجموعة الإدارة. يمكنك إضافة أجهزة إلى مجموعات الإدارة يدويًا بعد اكتمال المعالج.

لتشغيل الإنشاء التلقائي لبنية مجموعات الإدارة:

1. حدد المجلد **الأجهزة المُدارة** في شجرة وحدة التحكم.

2. في قائمة السياق الخاصة بالمجلد **الأجهزة المُدارة**، حدد **جميع المهام** > **بنية مجموعة جديدة**.

   يبدأ معالج بنية مجموعة الإدارة الجديدة. اتبع إرشادات المعالج.

التثبيت التلقائي للتطبيقات على الأجهزة الموجودة في مجموعة إدارة

يمكنك تحديد حزم التثبيت التي يجب استخدامها للتثبيت التلقائي عن بُعد لتطبيقات Kaspersky على الأجهزة العميلة في مجموعة إدارة.

لتكوين تثبيت تلقائي للتطبيقات على الأجهزة في مجموعة إدارة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة المطلوبة.

2. افتح نافذة الخصائص الخاصة بمجموعة الإدارة هذه.

3. من الجزء **الأقسام**، حدد **التثبيت التلقائي**، ومن مساحة العمل حدد حزم تثبيت التطبيقات التي سيتم تثبيتها على الأجهزة.

4. انقر على**موافق**.

يتم إنشاء مهام جماعية. سيتم تشغيل المهام على الأجهزة العميلة مباشرة بعد إضافتها إلى مجموعة الإدارة.

في حالة تحديد بعض حزم التثبيت الخاصة بتطبيق واحد للتثبيت التلقائي، فسيتم إنشاء مهمة التثبيت لإصدار التطبيق الأحدث فقط.

إدارة الأجهزة العميلة

يحتوي هذا القسم على معلومات حول العمل مع الأجهزة العميلة.

توصيل الأجهزة العميلة بخادم الإدارة

يتم إنشاء اتصال الجهاز العميل بخادم الإدارة من خلال عميل الشبكة المثبت على الجهاز العميل.

وعند توصيل جهاز عميل بخادم الإدارة، يتم تنفيذ العمليات التالية:

- المزامنة التلقائية للبيانات:
  - مزامنة قائمة التطبيقات المثبتة على الجهاز العميل.
  - مزامنة السياسات وإعدادات التطبيق والمهام وإعدادات المهمة.
- استعادة معلومات محدّثة حول حالة التطبيقات وتنفيذ المهام وإحصاءات تشغيل التطبيقات من قبل خادم الإدارة.
- تسليم معلومات الحدث إلى خادم الإدارة لمعالجتها.

تتم المزامنة التلقائية للبيانات بصورة منتظمة وفقًا لإعدادات عميل الشبكة (كل 15 دقيقة على سبيل المثال). ويمكنك تحديد الفاصل الزمني للاتصال يدويًا.

يتم تسليم معلومات حول الحدث إلى خادم الإدارة حال حدوثها.

إذا كان خادم الإدارة موجودًا في مكان بعيد خارج شبكة الشركة، فيمكن أن تتصل الأجهزة العميلة به عبر الإنترنت.

بالنسبة للأجهزة العميلة التي تتصل بخادم الإدارة عبر الإنترنت، يجب الوفاء بالشروط التالية:

- يجب أن يحتوي خادم الإدارة على عنوان IP خارجي ويجب أن يظل المنفذ الوارد 13000 مفتوحًا (للاتصال بعملاء الشبكة). ننصحك بفتح منفذ UDP 13000 (لاستقبال إشعارات إيقاف تشغيل الجهاز).
- يجب تثبيت عملاء الشبكة على الأجهزة.
- عند تثبيت عميل الشبكة على الأجهزة، يجب أن تحدد عنوان IP الخارجي لخادم الإدارة عن بُعد. في حالة استخدام حزمة تثبيت من أجل القيام بالتثبيت، يجب تحديد عنوان IP الخارجي يدويًا في خصائص حزمة التثبيت في القسم **إعدادات**.
- لاستخدام خادم الإدارة عن بُعد لإدارة التطبيقات والمهام الخاصة بأحد الأجهزة، من نافذة خصائص الجهاز في القسم **عام**، قم بتحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة**. بعد تحديد خانة الاختيار، انتظر حتى تتم مزامنة خادم الإدارة مع الجهاز البعيد. لا يمكن أن يتجاوز عدد الأجهزة العميلة التي تبقى على اتصال مستمر مع خادم الإدارة عن 300.

لتحسين أداء المهام التي يتم بدؤها بواسطة خادم الإدارة عن بُعد، يمكنك فتح المنفذ 15000 على الجهاز. في هذه الحالة، لتشغيل مهمة، يرسل خادم الإدارة حزمة خاصة إلى عميل الشبكة من خلال المنفذ 15000 بدون الانتظار حتى تكتمل المزامنة مع الجهاز.

يتيح لك Kaspersky Security Center تكوين الاتصال بين جهاز عميل وخادم الإدارة بحيث يظل الاتصال نشطًا بعد اكتمال جميع العمليات. الاتصال غير المنقطع ضروري إذا كانت مراقبة الوقت الحقيقي لحالة التطبيق مطلوبة وخادم الإدارة لا يمكنه إنشاء اتصال بالعميل لأحد الأسباب (الاتصال محمي بجدار حماية، لا يُسمح بفتح منافذ على الجهاز العميل، عنوان IP للجهاز العميل غير معروف). يمكنك إنشاء اتصال مستمر بين جهاز عميل وخادم الإدارة في النافذة خصائص الجهاز، وذلك في القسم **عام**.

نوصيك بإنشاء اتصال دون انقطاع مع الأجهزة الأكثر أهمية. يقتصر إجمالي عدد الاتصالات التي يتم الحفاظ عليها في وقت واحد بواسطة خادم الإدارة على 300.

عند إجراء المزامنة يدويًا، يستخدم النظام طريقة اتصال بديلة، تسمح ببدء الاتصال بواسطة خادم الإدارة. قبل إنشاء اتصال على جهاز عميل، يجب عليك فتح منفذ UDP. إذ يُرسل خادم الإدارة طلب اتصال إلى منفذ UDP على الجهاز العميل. وفي المقابل، يتم التحقق من شهادة خادم الإدارة. فإذا كانت شهادة خادم الإدارة مطابقة لنسخة الشهادة المخزنة على الجهاز العميل، يتم إنشاء الاتصال.

كما يُستخدم البدء اليدوي للمزامنة للحصول على معلومات محدثة عن حالة التطبيقات وتنفيذ المهام وإحصاءات تشغيل التطبيقات.

اتصال جهاز عميل بخادم الإدارة يدويًا. الأداة المساعدة Klmover

إذا كان يتعين عليك توصيل جهاز عميل بخادم الإدارة، فيمكنك استخدام الأداة المساعدة klmover على الجهاز العميل.

عندما يتم تثبيت عميل الشبكة على جهاز عميل، يتم نسخ الأداة المساعدة تلقائيًا إلى مجلد تثبيت عميل الشبكة.

لتوصيل جهاز عميل بخادم الإدارة يدويًا باستخدام الأداة المساعدة klmover:

على الجهاز، ابدأ تشغيل الأداة المساعدة klmover من سطر الأوامر.

يمكن للأداة المساعدة klmover عند بدء تشغيلها من سطر الأوامر القيام بالإجراءات التالية (بناءً على المفاتيح المستخدمة):

- توصيل عميل الشبكة بخادم إدارة بإعدادات معينة؛
- تسجيل نتائج العملية في ملف سجل الأحداث أو عرضها على الشاشة.

لا يمكنك استخدام الأداة المساعدة KLMover لأجهزة العميل المتصلة بخادم الإدارة من خلال بوابات الاتصال. وبالنسبة لهذه الأجهزة، يتعين عليك إما إعادة تكوين عميل الشبكة أو إعادة تثبيت عميل الشبكة وتحديد بوابة الاتصال.

بناء جملة سطر الأوامر للأداة المساعدة:

```
klmover [-logfile < اسم الملف>] [-address < عنوان الخادم>] [-pn < رقم المنفذ>] [-ps
< رقم منفذ SSL>] [-nossl] [-cert < المسار إلى ملف الشهادة>] [-silent] [-dupfix] [-
cloningmode] [-virtserv]
```

حقوق المسؤول مطلوبة لتشغيل الأداة.

مواصفات المفاتيح:

- `-logfile` < اسم الملف> – تسجيل نتائج تشغيل الأداة المساعدة في ملف سجل.

  يتم حفظ المعلومات افتراضيًا في دفق الإخراج القياسي (stdout). إذا لم يكن المفتاح مستخدمًا، فسيتم عرض النتائج ورسائل الخطأ على الشاشة.

- -address < عنوان الخادم > - عنوان خادم الإدارة للاتصال.

  يمكنك تحديد عنوان IP أو اسم NetBIOS أو اسم DNS الخاص بالجهاز كعنوانه.

- -pn < رقم المنفذ > - رقم المنفذ الذي سيتم إنشاء اتصال غير مشفر بخادم الإدارة عن طريقه.

  رقم المنفذ الافتراضي هو 14000.

- -ps < رقم منفذ SSL > - رقم منفذ SSL الذي سيتم إنشاء اتصال مشفر بخادم الإدارة عن طريقه باستخدام SSL.

  رقم المنفذ الافتراضي هو 13000.

- -nossl—استخدام اتصال غير مشفر بخادم الإدارة.

  إذا لم يكن المفتاح مستخدمًا، فسيتم توصيل عميل الشبكة بخادم الإدارة عن طريق استخدام بروتوكول SSL المشفر.

- -cert < المسار إلى ملف الشهادة > - استخدام ملف الشهادة المحدد لمصادقة الوصول إلى خادم الإدارة.

  إذا لم يكن المفتاح مستخدمًا، فسيتلقى عميل الشبكة شهادة في الاتصال الأول بخادم الإدارة.

- -silent—تشغيل الأداة المساعدة في وضع السكون.

  ربما يكون استخدام المفتاح مفيدًا، إذا تم بدء تشغيل الأداة المساعدة مثلاً من برنامج تسجيل الدخول عند تسجيل المستخدم.

- -dupfix— المفتاح مستخدَم إذا تم تثبيت عميل الشبكة باستخدام طريقة تختلف عن الطريقة المعتادة (مع حزمة التوزيع) - مثل استعادته من صورة قرص ISO.

- -virtserv—اسم خادم الإدارة الافتراضي

- -cloningmode - وضع استنساخ قرص عميل الشبكة

  استخدم إحدى المعلمات التالية لتكوين وضع استنساخ القرص:

  - -cloningmode—طلب حالة وضع استنساخ القرص.
  - -cloningmode 1 —تمكين وضع استنساخ القرص.
  - -cloningmode 0 —تعطيل وضع استنساخ القرص.

- -nauninstpwd < كلمة المرور > - يتم استخدام المفتاح لتحديد كلمة مرور إلغاء تثبيت عميل الشبكة.

  المفتاح ليس إلزاميًا.

على سبيل المثال، لتوصيل عميل الشبكة بخادم الإدارة، قم بتشغيل الأمر التالي:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

نفق اتصال أحد الأجهزة العميلة بخادم الإدارة

يتيح Kaspersky Security Center باتصالات TCP عبر الأنفاق من وحدة تحكم الإدارة عبر خادم الإدارة ثم عبر عميل الشبكة إلى منفذ محدد على جهاز مُدار. الأنفاق مصممة لتوصيل تطبيق عميل على جهاز مثبّت عليه وحدة تحكم الإدارة إلى منفذ TCP على جهاز مُدار—في حالة عدم إمكانية الاتصال المباشر بين وحدة تحكم الإدارة والجهاز المستهدف.

على سبيل المثال، تُستخدم الأنفاق لإجراء اتصالات بسطح مكتب بعيد، لكل من الاتصال بجلسة موجودة بالفعل، أو لإنشاء جلسة بعيدة جديدة.

يمكن أيضًا تمكين الأنفاق عن طريق استخدام أدوات خارجية. على سبيل المثال، يمكن للمسؤول تشغيل الأداة المساعدة putty وعميل VNC والأدوات الأخرى بهذه الطريقة.

نفق اتصال بين جهاز عميل بعيد وخادم الإدارة مطلوب في حالة عدم توفر المنفذ المستخدم لاتصال خادم الإدارة على الجهاز. قد لا يتوفر المنفذ الموجود على الجهاز في الحالات التالية:

- اتصال الجهاز البعيد بشبكة محلية تستخدم آلية NAT.
- الجهاز البعيد يعتبر جزء من الشبكة المحلية الخاصة بخادم الإدارة، لكن تم غلق منفذه بواسطة جدار الحماية.

للتحقق من اتصال أحد الأجهزة العميلة بخادم الإدارة:

1. من شجرة وحدة التحكم، حدد مجموعة الإدارة التي تتضمن الجهاز العميل.
2. في علامة التبويب **الأجهزة**، حدد الجهاز.
3. في قائمة السياق الخاصة بالجهاز، حدد **جميع& المهام** ← **نفق الاتصال**.
4. قم بإنشاء نفق في نافذة **نفق الاتصال** التي تفتح.

الاتصال البعيد بسطح مكتب جهاز عميل

يمكن للمسؤول الحصول على وصول عن بُعد لسطح مكتب جهاز عميل من خلال عميل الشبكة المثبت على الجهاز.

ومن الممكن أيضًا الاتصال عن بُعد بجهاز من خلال عميل الشبكة في حالة إغلاق منافذ TCP وUDP بالجهاز العميل. عند إنشاء اتصال مع الجهاز، يكون للمسؤول حق الوصول الكامل للمعلومات المُخزنة على هذا الجهاز ليتمكن من إدارة التطبيقات المثبتة عليه.

يصف هذا القسم كيفية إنشاء اتصال بملف جهاز عميل Windows و جهاز عميل macOS من خلال عميل الشبكة.

الاتصال بنظام التشغيل Windows الأجهزة العميلة

يمكن إنشاء الاتصال عن بُعد بجهاز عميل Windows بإحدى الطرق التالية:

- عن طريق استخدام مكون Microsoft Windows القياسي المُسمى Remote Desktop Connection.
  يتم إنشاء اتصال سطح المكتب عن بُعد عبر أداة Windows القياسية mstsc.exe وفقًا لإعدادات الأداة.
- عن طريق استخدام تقنية مشاركة سطح المكتب لـ Windows.

الاتصال بجهاز عميل Windows باستخدام الاتصال بسطح المكتب البعيد

تم إنشاء اتصال بجلسة سطح المكتب البعيد الحالية للمستخدم دون علم المستخدم. بمجرد اتصال المسؤول بالجلسة، يتم قطع اتصال مستخدم الجهاز من الجلسة دون إخطار مسبق.

للاتصال بسطح مكتب جهاز عميل عبر مكون Remote Desktop Connection:

1. في شجرة وحدة تحكم الإدارة، حدد الجهاز الذي تحتاج الوصول إليه.
2. في قائمة السياق الخاصة بالجهاز، حدد **جميع& المهام** > **الاتصال بالجهاز** >**جلسة RDP جديدة**.
   تبدأ أداة Windows المساعدة القياسية mstsc.exe التي تساعد على الاتصال بسطح المكتب البعيد.
3. اتبع الإرشادات التي تظهر في مربعات الحوار الخاصة بالأداة المساعدة.

عند إجراء الاتصال بالجهاز، يُتاح سطح المكتب في نافذة الاتصال عن بُعد لـ Microsoft Windows.

الاتصال بجهاز عميل Windows باستخدام Windows Desktop Sharing

عند الاتصال بجلسة موجودة لسطح مكتب بعيد، يتلقى مستخدم الجلسة على الجهاز طلبًا للاتصال من المسؤول. لن توجد أي معلومات بشأن نشاط عن بُعد على الجهاز وسوف يتم حفظ نتائجه في التقارير التي تم إنشاؤها بواسطة Kaspersky Security Center.

يمكن للمسؤول الاتصال بالجلسة الموجودة على جهاز عميل بدون فصل اتصال المستخدم في هذه الجلسة. وفي هذه الحالة، سيشارك المسؤول ومستخدم الجلسة على الجهاز الوصول إلى سطح المكتب.

يمكن للمسؤول تكوين مراجعة لنشاط المستخدم على جهاز عميل بعيد. أثناء المراجعة، يحفظ التطبيق معلومات بشأن ملفات على الجهاز العميل تم فتحها و/أو تعديلها من خلال المسؤول.

للاتصال بسطح مكتب الجهاز العميل عبر مشاركة سطح المكتب لـ Windows، ينبغي عليك تلبية الشروط التالية:

- يلزم تثبيت Microsoft Windows Vista أو إصدار نظام تشغيل أحدث على محطة عمل المسؤول. لا يفرض نوع نظام التشغيل المستخدم على الجهاز الذي يستضيف خادم الإدارة قيودًا على الاتصال عبر مشاركة سطح المكتب لـ Windows.

  للتحقق مما إذا كانت ميزة Windows Desktop Sharing مضمنة في إصدار Windows، تأكد من وجود مفتاح CLSID \\ {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} في سجل Windows.

- يتم تثبيت Microsoft Windows Vista أو إصدار أحدث على الجهاز العميل.
- يستخدم Kaspersky Security Center ترخيصًا لإدارة الثغرات الأمنية والتصحيحات.

للاتصال بسطح مكتب جهاز عميل من خلال مشاركة سطح المكتب لـ Windows:

1. في شجرة وحدة تحكم الإدارة، حدد الجهاز الذي تحتاج الوصول إليه.
2. في قائمة السياق الخاصة بالجهاز، حدد **جميع& المهام** ← **الاتصال بالجهاز** ← **مشاركة سطح المكتب لـ Windows**.
3. في النافذة **تحديد جلسة سطح المكتب البعيد** التي تفتح، حدد الجلسة على الجهاز الذي تحتاج إلى الاتصال به.

   إذا تم إنشاء الاتصال بالجهاز بنجاح، فسيتوفر سطح مكتب الجهاز في النافذة **عارض جلسة سطح المكتب الجديد من Kaspersky**.
4. لبدء التفاعل مع الجهاز، في القائمة الرئيسية للنافذة **عارض جلسة سطح المكتب الجديد من Kaspersky**، حدد **الإجراءات** ← **الوضع التفاعلي**.

تتطلب الأداة المساعدة **عارض جلسة سطح المكتب الجديد من Kaspersky** ترخيصًا تجاريًا.

الاتصال بنظام macOS الأجهزة العميلة

يمكن للمسؤول استخدام نظام حوسبة الشبكة الافتراضية (VNC) للاتصال بأجهزة macOS.

يتم إنشاء الاتصال بسطح مكتب بعيد من خلال عميل VNC مثبت على جهاز خادم الإدارة. يقوم عميل VNC بتحويل لوحة المفاتيح والتحكم في الماوس من جهاز العميل إلى المسؤول.

عندما يتصل المسؤول بسطح المكتب البعيد، لا يتلقى المستخدم إعلامات أو طلبات اتصال من المسؤول. يتصل المسؤول بجلسة حالية على جهاز العميل، بدون قطع اتصال المستخدم بهذه الجلسة.

للاتصال بسطح المكتب لجهاز عميل macOS من خلال عميل VNC، يجب استيفاء الشروط التالية:

- يتم تثبيت عميل VNC على جهاز خادم الإدارة.
- يُسمح بتسجيل الدخول عن بُعد والإدارة عن بُعد على جهاز العميل.
- سمح المستخدم للمسؤول بالوصول إلى جهاز العميل في **مشاركة** إعدادات نظام التشغيل macOS.

للاتصال بسطح مكتب جهاز عميل من خلال نظام حوسبة الشبكة الافتراضية:

1. في شجرة وحدة تحكم الإدارة، حدد الجهاز الذي تحتاج الوصول إليه.

2. في قائمة السياق الخاصة بالجهاز، حدد **جميع& المهام** ← **نفق الاتصال**.

3. في النافذة **نفق الاتصال** التي تفتح، نفذ ما يلي:

   a. في قسم **1. منفذ الشبكة** ، حدد رقم منفذ الشبكة للجهاز الذي تريد الاتصال به.
   يتم استخدام المنفذ 5900 بشكل افتراضي.

   b. في قسم **2. النفق**، انقر فوق زر **إنشاء قناة اتصال**.

   c. في قسم **3. إعدادات الشبكة**، انقر فوق الزر **نسخ**.

4. افتح عميل VNC والصق سمات الشبكة المنسوخة في حقل النص. اضغط على **دخول**.

5. في النافذة التي تفتح، اعرض تفاصيل الشهادة. إذا كنت توافق على استخدام الشهادة، فانقر فوق **نعم** زر.

6. في نافذة **المصادقة**، حدد بيانات اعتماد جهاز العميل، ثم انقر على **موافق**.

الاتصال بالأجهزة من خلال مشاركة سطح المكتب لـ Windows

للاتصال بجهاز من خلال مشاركة سطح المكتب لـ Windows:

1. في شجرة وحدة التحكم، على علامة التبويب **الأجهزة**، حدد المجلد **الأجهزة المُدارة**.
   تعرض مساحة عمل هذا المجلد قائمة الأجهزة.

2. في قائمة سياق الجهاز الذي ترغب في الاتصال به، حدد **الاتصال بالجهاز** ← **مشاركة سطح المكتب لـ Windows**.
   تفتح النافذة **تحديد جلسة سطح المكتب البعيد**.

3. في النافذة **تحديد جلسة سطح المكتب البعيد**، حدد جلسة سطح مكتب للاتصال بالجهاز.

4. انقر فوق **موافق**.

   الجهاز متصل.

تكوين إعادة تشغيل الجهاز العميل

عند استخدام Kaspersky Security Center أو تثبيته أو إزالته، قد تحتاج إلى إعادة تشغيل الجهاز. يمكنك تحديد إعدادات إعادة التشغيل للأجهزة التي تعمل بنظام Windows فقط.

لتكوين إعادة تشغيل جهاز عميل:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي يجب تكوين إعادة التشغيل لها.

2. في مساحة العمل الخاصة بالمجموعة، حدد علامة التبويب **السياسات**.

3. في مساحة العمل، حدد سياسة عميل شبكة Kaspersky Security Center في قائمة السياسات، ثم حدد **خصائص** في قائمة سياق السياسة.

4. في نافذة خصائص السياسة، حدد قسم **إدارة إعادة التشغيل**.

5. حدد الإجراء الذي يجب تنفيذه في حالة طلب إعادة تشغيل الجهاز العميل:

- تحديد **عدم إعادة تشغيل نظام التشغيل** لمنع إعادة التشغيل التلقائي.
- تحديد **إعادة تشغيل نظام التشغيل تلقائيًا عند الحاجة** للسماح بإعادة التشغيل التلقائي.
- حدد **مطالبة المستخدم باتخاذ إجراء** لتمكين مطالبة المستخدم بالسماح بإعادة التشغيل.

يمكنك تحديد معدل تكرار طلبات إعادة التشغيل، وتمكين فرض إعادة التشغيل وفرض الإغلاق للتطبيقات في الجلسات الممنوعة على الجهاز، عن طريق تحديد خانات الاختيار المقابلة وإعدادات الوقت في مربعات الزيادة والنقصان.

6. انقر فوق **موافق** لحفظ التغييرات وغلق نافذة خصائص السياسة.

سيتم الآن تكوين إعادة تشغيل الجهاز.

مراجعة الإجراءات على جهاز عميل

يتيح التطبيق إجراء مراجعة إجراءات المسؤول على الأجهزة العميلة البعيدة التي تعمل بنظام Windows. أثناء المراجعة، يحفظ التطبيق، على الجهاز، معلومات حول الملفات التي تم فتحها و / أو تعديلها من خلال المسؤول. تتوفر مراجعة إجراءات المسؤول عند تلبية الشروط التالية:

- ترخيص إدارة الثغرات الأمنية والتصحيحات قيد الاستخدام.
- يكون للمسؤول الحق في تشغيل الوصول المشترك لسطح مكتب الجهاز البعيد.

لتمكين مراجعة الإجراءات على جهاز عميل بعيد:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي يُفترض تكوين مراجعة إجراءات المسؤول لها.
2. في مساحة العمل الخاصة بالمجموعة، حدد علامة التبويب **السياسات**.
3. حدد سياسة عميل شبكة Kaspersky Security Center، ثم حدد **خصائص** في قائمة سياق السياسة.
4. في نافذة خصائص السياسة ، حدد قسم **مشاركة سطح المكتب لـ Windows** .
5. حدد خيار **تمكين التدقيق**.
6. في القوائم **أقنعة الملفات التي ينبغي مراقبتها عند قراءتها** و**أقنعة الملفات التي ينبغي مراقبتها عند تعديلها**، قم بإضافة أقنعة الملفات التي يتعين على التطبيق مراقبة الإجراءات أثناء التدقيق من خلالها.

   يقوم التطبيق بمراقبة الإجراءات على الملفات ذات الامتدادات txt و rtf و doc و xls و docx و xlsx و odt و pdf افتراضيًا.
7. انقر فوق **موافق** لحفظ التغييرات وغلق نافذة خصائص السياسة.

ونتيجة لذلك، يتم تكوين مراجعة إجراءات المسؤول على جهاز المستخدم البعيد مع الوصول المشترك لسطح المكتب.

يتم تسجيل إجراءات المسؤول على الجهاز البعيد:

- في سجل الأحداث على الجهاز البعيد.
- في ملف بامتداد syslog موجود في مجلد عميل الشبكة على الجهاز البعيد (مثال C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- في قاعدة بيانات الأحداث لـ Kaspersky Security Center.

التحقق من اتصال جهاز عميل بخادم الإدارة

يتيح لك Kaspersky Security Center إمكانية التحقق من الاتصالات بين جهاز عميل وخادم الإدارة تلقائيًا أو يدويًا.

يتم إجراء تحقق تلقائي من الاتصال على خادم الإدارة. يتم إجراء التحقق اليدوي من الاتصال على الجهاز.

التحقق من اتصال جهاز عميل بخادم الإدارة تلقائيًا

لبدء التحقق التلقائي من اتصال جهاز عميل بخادم الإدارة:

1. من شجرة وحدة التحكم، حدد مجموعة الإدارة التي تتضمن الجهاز.
2. من مساحة العمل الخاصة بمجموعة الإدارة، في علامة التبويب **الأجهزة**، حدد الجهاز.
3. في قائمة السياق الخاصة بالجهاز، حدد **التحقق من إمكانية الوصول إلى الجهاز**.

تفتح النافذة التي تحتوي على معلومات حول إمكانية الوصول إلى الجهاز.

التحقق يدويًا من اتصال جهاز عميل بخادم الإدارة الأداة المساعدة Klnagchk

يمكنك التحقق من الاتصال والحصول على معلومات تفصيلية عن إعدادات الاتصال بين جهاز عميل وخادم الإدارة باستخدام الأداة المساعدة klnagchk. توجد الأداة المساعدة klnagchk في مجلد تثبيت عميل الشبكة.

يمكن للأداة المساعدة klnagchk عند بدء تشغيلها من سطر الأوامر القيام بالإجراءات التالية (بناء على المفاتيح المستخدمة):

- عرض قيم الإعدادات المستخدمة لاتصال عميل الشبكة المثبت على الجهاز بخادم الإدارة على على الشاشة أو تسجيلها.
- تسجيل إحصائيات عميل الشبكة في ملف سجل الأحداث (منذ آخر مرة بدأ تشغيلها) ونتائج تشغيل الأداة المساعدة، أو عرض المعلومات على الشاشة.
- محاولة إنشاء اتصال بين عميل الشبكة وخادم الإدارة.
  إذا فشلت محاولة الاتصال، فسترسل الأداة المساعدة حزمة ICMP للتحقق من حالة الجهاز المثبت عليه خادم الإدارة.

للتحقق من الاتصال بين جهاز عميل وخادم الإدارة باستخدام الأداة المساعدة klnagchk،

على الجهاز المثبت عليه عميل الشبكة، قم بتشغيل الأداة المساعدة klnagchk من سطر الأوامر تحت حساب مسؤول محلي.

بناء جملة سطر الأوامر للأداة المساعدة:

```
-] [< path to certificate file > savecert-] [sp-] [< file name > logfile-] klnagchk
[sendhb-][restart
```

مواصفات المفاتيح:

- `-logfile < file name >` - يسجل في ملف سجل قيم إعدادات الاتصال بين عميل الشبكة وخادم الإدارة ونتائج تشغيل الأداة المساعدة.
  يتم حفظ المعلومات افتراضيًا في دفق الإخراج القياسي (stdout). إذا لم يكن المفتاح مستخدمًا، فسيتم عرض الإعدادات والنتائج ورسائل الخطأ على الشاشة.
- `-sp` — إظهار كلمة مرور مصادقة المستخدم على خادم الوكيل.
  يكون المفتاح قيد الاستخدام في حالة إنشاء اتصال بخادم الإدارة من خلال خادم وكيل.

- `-savecert < file name >` - يحفظ الشهادة المستخدمة للوصول إلى خادم الإدارة في ملف محدد.
- `-restart` —إعادة تشغيل عميل الشبكة بعد اكتمال الأداة المساعدة.
- `-sendhb` — بدء مزامنة عميل الشبكة مع خادم الإدارة.

بعد بدء التشغيل، تصل الأداة المساعدة klnagchk إلى ملفات تكوين عميل الشبكة وتعرض معلمات الاتصال. ويتم تحديد هذه المعلمات أثناء تثبيت عميل الشبكة وفي إعدادات سياسة عميل الشبكة:

- `Current device`—اسم مجال Windows للجهاز العميل.
- `Network Agent version`—العدد الكامل لإصدار عميل الشبكة (مع التصحيحات) المثبتة على الجهاز.
- `Administration Server address`—عنوان خادم الإدارة.
- `Use SSL`—المعلمة التي تشير إلى ما إذا كان سيتم استخدام اتصال آمن عند الاتصال بخادم الإدارة.
  القيم الممكنة:
  - 0—لا يتم استخدام الاتصال الآمن.
  - 1—يتم استخدام الاتصال الآمن.
- `Compress traffic` — المعلمة التي تشير إلى ما إذا كانت حركة المرور بين جهاز العميل وخادم الإدارة مضغوطة أم لا.
- `Numbers of the Administration Server SSL ports`—عدد المنافذ الصالحة للاتصال بخادم الإدارة عند استخدام اتصال آمن.
- `Numbers of the Administration Server ports`—عدد المنافذ الصالحة للاتصال بخادم الإدارة عند استخدام اتصال عادي.
- `Use proxy server`—المعلمة التي تشير إلى ما إذا كان سيتم استخدام خادم وكيل أم لا.
  القيم الممكنة:
  - 0—لا يتم استخدام خادم وكيل.
  - 1—يتم استخدام خادم وكيل.
- `Address`—عنوان ومنفذ الخادم الوكيل مفصول بنقطتين. ويتم عرض هذه المعلمة فقط في حالة استخدام خادم وكيل.
- `User name`—اسم المستخدم للوصول إلى الخادم الوكيل. ويتم عرض هذه المعلمة فقط في حالة استخدام خادم وكيل.
- `Password`—كلمة المرور للوصول إلى الخادم الوكيل. ويتم عرض هذه المعلمة فقط في حالة استخدام خادم وكيل. لإظهار كلمة مرور الخادم الوكيل، تحتاج إلى استخدام المفتاح `sp` في الأمر.
- `Administration Server certificate`—المعلمة التي تشير إلى ما إذا كان الجهاز العميل لديه شهادة خادم إدارة. وقد لا توجد شهادة، على سبيل المثال، إذا لم يتصل عميل الشبكة بخادم الإدارة بنجاح.
  القيم الممكنة:
  - `not installed`—جهاز العميل ليست لديه شهادة خادم إدارة
  - `available`—جهاز العميل لديه شهادة خادم إدارة
- `Open UDP port`—المعلمة التي تشير إلى ما إذا كان عميل الشبكة يستخدم منفذ UDP لتلقي طلبات المزامنة من خادم الإدارة.

القيم الممكنة:

- 0—منفذ UDP مغلق لاستلام طلبات المزامنة من خادم الإدارة.
- 1—منفذ UDP مفتوح لتلقي طلبات المزامنة من خادم الإدارة.

- `Numbers of UDP ports` عدد منافذ UDP التي يمكن استخدامها بواسطة عميل الشبكة.
- `Location name`—موقع الشبكة للجهاز.
- `State of network location`—المعلمة التي تشير إلى ما إذا كان يمكن تبديل جهاز العميل من ملف تعريف اتصال خادم إدارة إلى آخر.
القيم الممكنة:
  - `Enabled`—يمكن تبديل ملف تعريف اتصال خادم الإدارة لجهاز العميل.
  - `Disabled`—لا يمكن تبديل ملف تعريف اتصال وحدة خدمة الإدارة لجهاز العميل.
- `Profile to use`—ملف تعريف الاتصال لخادم الإدارة.
- `Condition`—عنوان IP وقناع الشبكة الفرعية للشبكة التي يتصل بها جهاز العميل.
- `Synchronization interval (min)`—الفاصل الزمني القياسي بين عمليات المزامنة.
- `Connection timeout (in seconds)` مهلة الاتصال.
- `Send / receive timeout (in seconds)`—مهلة الاتصال لعمليات القراءة والكتابة.
- `Device ID`—معرف الجهاز في الشبكة. يعتبر `Device ID` فريدًا بين الأجهزة العميلة التي تتم إدارتها بواسطة خادم إدارة معين.
- `Locations of connection gateways`—معلمات لتوصيل الجهاز العميل بخادم الإدارة من خلال بوابة الاتصال.
- `Location of distribution points`—معلمات لتوصيل الجهاز العميل بخادم الإدارة من خلال نقطة التوزيع.
- `Connection with server`—المعلمة التي تشير إلى ما إذا كانت بوابة الاتصال لديها اتصال مستمر بخادم الإدارة. وتعرض المعلمة فقط ما إذا كان الجهاز العميل يعمل كبوابة اتصال.
القيم الممكنة:
  - `active`—تحتوي بوابة الاتصال على اتصال مستمر بخادم الإدارة.
  - `inactive`—لا تمتك بوابة الاتصال اتصالاً مستمرًا بخادم الإدارة.
- `Connection with server through connection gateway`—المعامل الذي يشير إلى ما إذا كان الاتصال بخادم الإدارة قد تم إنشاؤه بشكل صحيح أم لا. وتعرض المعلمة فقط ما إذا كان الجهاز العميل يعمل كبوابة اتصال.
القيم الممكنة:
  - `active`—تم تأسيس الاتصال بخادم الإدارة من خلال بوابة اتصال بشكل صحيح
  - `inactive`—لم يتم إنشاء الاتصال بخادم الإدارة من خلال بوابة اتصال بشكل صحيح.

أيضًا، يمكن أن يحتوي إخراج الأداة المساعدة klnagchk على أحد الأسطر التالية:

- `Administration Server is installed on this device`—يتم تشغيل الأداة المساعدة klnagchk على جهاز خادم الإدارة.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` - يتم تشغيل الأداة المساعدة klnagchk على الجهاز الذي تم تثبيت عميل الشبكة عليه، في وضع بوابة الاتصال. وتنتظر بوابة الاتصال التي تم تكوينها اتصالاً من خادم الإدارة، لكن خادم الإدارة لا يسرد الجهاز بين الأجهزة المدارة. وتحتاج إلى التأكد من أن خادم الإدارة يبدأ الاتصال ببوابة الاتصال.
- `This device is a connection gateway` - يتم تشغيل الأداة المساعدة klnagchk على الجهاز الذي يعمل كبوابة اتصال.
- `Acts as a distribution point` - يتم تشغيل الأداة المساعدة klnagchk على الجهاز الذي يعمل كنقطة توزيع.

تتحقق الأداة المساعدة klnagchk من حالة خدمة عميل الشبكة. إذا لم تكن الخدمة قيد التشغيل، تتوقف الأداة المساعدة. وإذا كانت الخدمة قيد التشغيل، فستعرض الأداة المساعدة إحصائيات الاتصال التالية:

- `Total number of synchronization requests`—عدد محاولات توصيل الجهاز العميل بخادم الإدارة.
- `The number of successful synchronization request`—عدد المحاولات الناجحة لتوصيل جهاز العميل بخادم الإدارة.
- `Total number of synchronizations`—عدد المحاولات لمزامنة إعدادات الجهاز العميل مع إعدادات خادم الإدارة.
- `The number of successful synchronizations`—عدد المحاولات الناجحة لمزامنة إعدادات الجهاز العميل مع خادم الإدارة.
- `Date/time of the last request for synchronization`—تاريخ ووقت آخر اتصال.

تحتاج إلى استخدام `Total number of synchronization requests` و `The number of successful synchronization request` عند تحليل الاتصال بين خادم الإدارة وعميل الشبكة. وتتم مزامنة إعدادات جهاز العميل مع إعدادات خادم الإدارة فقط في حالة تغيير إعدادات خادم الإدارة (على سبيل المثال، في حالة إضافة مهام جديدة أو تعديل إعدادات السياسة). وبخلاف ذلك، يظل `Total number of synchronizations` وعدد قيم `The number of successful synchronizations` دون تغيير.

للمزيد من المعلومات عن كيفية استكشاف المشكلات المتعلقة بتوصيل عميل الشبكة بخادم الإدارة وإصلاحها، راجع الأسئلة الشائعة عن Kaspersky Security Center.

حول التحقق من وقت الاتصال بين جهاز ما وخادم الإدارة

عند إيقاف تشغيل جهاز ما، يقوم عميل الشبكة بإخطار خادم الإدارة بهذا الحدث. في وحدة تحكم الإدارة، يتم عرض هذا الجهاز كمتوقف التشغيل. ولكن، لا يمكن لعميل الشبكة إخطار خادم الإدارة بكل مثل هذه الأحداث. لذلك يقوم خادم الإدارة بشكل دوري بتحليل سمة **تم الاتصال بخادم الإدارة** (تُعرض قيمة هذه السمة في وحدة تحكم الإدارة، في خصائص الجهاز، في القسم **عام**) لكل جهاز ويقارنها مقابل الفاصل الزمني للمزامنة من الإعدادات الحالية لعميل الشبكة. في حالة عدم استجابة جهاز على مدى أكثر ثلاثة فواصل زمنية متتابعة للمزامنة، يتم تمييز هذا الجهاز كمتوقف التشغيل.

تحديد الأجهزة العميلة على خادم الإدارة

يتم تحديد الأجهزة العميلة بناءً على أسمائها. ويكون اسم الجهاز فريدًا بين جميع أسماء الأجهزة المتصلة بخادم الإدارة.

ويتم نقل اسم الجهاز إلى خادم الإدارة عند استقصاء شبكة Windows واكتشاف جهاز جديد بها أو عند أول اتصال لعميل الشبكة المثبت على الجهاز بخادم الإدارة. افتراضيًا، يكون الاسم مطابقًا لاسم الجهاز في شبكة Windows (اسم NetBIOS). وإذا كان الجهاز الذي يحمل هذا الاسم مُسجلاً بالفعل على خادم الإدارة، تتم إضافة مؤشر دلالي برقم التسلسل التالي إلى اسم الجهاز الجديد، مثل: **<الاسم>-1**, **<الاسم>-2** بموجب هذا الاسم، يتم إضافة الجهاز إلى مجموعة الإدارة.

نقل أجهزة إلى مجموعة إدارة

لا يمكنك نقل الأجهزة من أحد مجموعات الإدارة إلى مجموعة أخرى إلا في حالة امتلاكك إذن **Modify** في منطقة **إدارة مجموعات الإدارة** لكل من مصدر وهدف مجموعات الإدارة (أو لخادم الإدارة الذي تنتمي له هذه المجموعات).

لتضمين جهاز أو أكثر في مجموعة إدارة محددة:

1. في شجرة وحدة التحكم، قم بتوسيع المجلد **الأجهزة المُدارة**.

2. في المجلد **الأجهزة المُدارة**، حدد المجلد الفرعي المقابل للمجموعة التي سيتم تضمين الأجهزة العميلة فيها.

   إذا كنت تريد تضمين الأجهزة في المجموعة **الأجهزة المُدارة**، يمكنك تخطي هذه الخطوة.

3. في مساحة عمل مجموعة الإدارة المحددة، على علامة التبويب **الأجهزة**، قم بتشغيل عملية تضمين الأجهزة في المجموعة بإحدى الطرق التالية:

   - عن طريق إضافة الأجهزة إلى المجموعة من خلال النقر فوق الزر **نقل الأجهزة إلى المجموعة** في خانة معلومات قائمة الأجهزة
   - عن طريق تحديد **إنشاء** > **الجهاز** في قائمة السياق الخاصة بقائمة الأجهزة

يبدأ تشغيل معالج نقل الأجهزة. بإتباع التعليمات الخاصة به، حدد طريقة لنقل الأجهزة إلى المجموعة ثم قم بإنشاء قائمة بالأجهزة لتضمينها في المجموعة.

إذا قمت بإنشاء قائمة الأجهزة يدويًا، يمكنك استخدام عنوان IP (أو نطاق IP) أو اسم NetBIOS أو اسم DNS كعنوان الجهاز. يمكنك النقل إلى القائمة بشكل يدوي فقط للأجهزة التي تمت إضافة معلومات حولها بالفعل إلى قاعدة بيانات خادم الإدارة وذلك عند اتصال الجهاز أو بعد اكتشاف الأجهزة.

لاستيراد قائمة أجهزة من ملف، حدد ملف txt الذي يحتوي على قائمة عناوين الأجهزة التي سيتم إضافتها. يجب تحديد كل عنوان في سطر منفصل.

بعد أن يقوم المعالج بالإكمال، يتم تضمين الأجهزة المحددة في مجموعة الإدارة وتُعرَض في قائمة الأجهزة بأسماء أنشأها خادم الإدارة.

يمكنك نقل جهاز إلى مجموعة الإدارة المحددة عن طريق سحبه من المجلد **الأجهزة غير المخصصة** إلى مجلد مجموعة الإدارة هذه.

تغيير خادم الإدارة للأجهزة العميلة

يمكنك تغيير خادم الإدارة الذي يدير الأجهزة العميلة إلى خادم مختلف باستخدام مهمة تغيير خادم الإدارة.

لتغيير خادم الإدارة الذي يدير الأجهزة العميلة بخادم آخر:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.

2. في مساحة عمل هذا المجلد، انقر على الزر **مهمة جديدة**.

   سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

3. في الخطوة **تحديد نوع المهمة** من المعالج، حدد عقدة **Kaspersky Security Center Administration Server**، وقم بتوسيع المجلد **خيارات متقدمة**، ثم حدد المهمة **تغيير خادم الإدارة**.

4. في النافذة التي تفتح، انقر فوق الزر **موافق** لتأكيد موافقتك على شروط تغيير خادم الإدارة لأجهزة العميل.

5. في خطوة **إعدادات** من المعالج، حدد خادم الإدارة الذي تريد استخدامه لإدارة الأجهزة المحددة:

- **التغيير إلى خادم إدارة أساسي آخر**

لنقل أجهزة العميل إلى خادم إدارة أساسي آخر، حدد إعدادات اتصال خادم الإدارة التالية:

1. في الحقل **خادم الإدارة**، حدد عنوان خادم الإدارة الأساسي الجديد.

2. في الحقل **المنفذ**، حدد رقم المنفذ الذي تريد الاتصال عن طريقه بخادم الإدارة.
رقم المنفذ الافتراضي هو 14000.

3. في الحقل **منفذ SSL**، حدد رقم منفذ SSL على خادم الإدارة الرئيسي.
رقم المنفذ الافتراضي هو 13000.

4. إذا لزم الأمر، حدد مربع الاختيار **Use proxy server**.
إذا لم يتم مسح خانة الاختيار هذه، فسيتم استخدام الاتصال المباشر لتوصيل الجهاز بخادم الإدارة.
في حالة تحديد خانة الاختيار هذه، حدد معلمات الخادم الوكيل:

- **عنوان الخادم الوكيل**

- **منفذ الخادم الوكيل**

إذا كان الخادم الوكيل يتطلب المصادقة، حدد **اسم المستخدم** و**كلمة المرور** للحساب الذي تم إنشاء اتصال بالخادم الوكيل باستخدامه. ونوصي بتحديد بيانات اعتماد حساب لديه الحد الأدنى من الامتيازات المطلوبة فقط لمصادقة الخادم الوكيل.

5. إذا لزم الأمر، قم بتحميل شهادة خادم الإدارة الجديدة.

- **التغيير إلى خادم افتراضي آخر على هذا الخادم الأساسي**

حدد هذا الخيار لنقل أجهزة العميل إلى خادم الإدارة الافتراضي على خادم الإدارة الأساسي الحالي. ولفعل ذلك، في الحقل **اسم خادم الإدارة الافتراضي**، حدد اسم خادم الإدارة الافتراضي المطلوب.

إذا لزم الأمر، حدد وقت الانتظار قبل إعادة تشغيل عميل الشبكة.

6. في هذه الخطوة من المعالج، قم بإجراء تحديدات الأجهزة التي سيتم تعيين المهمة لها:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة** . في هذه الحالة، يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.

- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**. يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

- **تعيين مهمة إلى تحديد الجهاز** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في المجموعة المحددة التي تم إنشائها في وقت سابق. يمكنك تحديد المجموعة المحددة مسبقًا أو المجموعة المخصصة التي أنشأتها.

- **تعيين مهمة لمجموعة إدارة** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في مجموعة الإدارة التي تم إنشائها في وقت سابق.

7. في الخطوة **تحديد حساب لتشغيل المهمة** في المعالج، حدد إعدادات الحساب:

- **الحساب الافتراضي**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.
يتم تحديد هذا الخيار افتراضيًا.

- **تحديد حساب**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **الحساب**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **كلمة المرور**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

8. في خطوة **تكوين جدول المهمة** من المعالج، أنشئ جدولاً لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. وهو ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **مرة**

يتم تشغيل المهمة مرة واحدة، في التاريخ والوقت المحددين (افتراضيًا، في اليوم الذي تم إنشاء المهمة فيه).

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **فورًا**

يتم تشغيل المهمة مباشرة بعد أن يصبح الجهاز مرئيًا على الشبكة أو مباشرة بعد تضمين الجهاز في نطاق المهمة.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا ومرة وفورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

9. في هذه الخطوة من المعالج، حدد اسم المهمة التي تقوم بإنشائها.

10. في خطوة **إنهاء عملية إنشاء المهمة** من المعالج انقر فوق الزر **إنهاء** لإنهاء المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج**.

بعد اكتمال المهمة، يتم وضع الأجهزة العميلة التي تم إنشاء المهمة من أجلها تحت إدارة خادم الإدارة المحدد في إعدادات المهمة.

إذا كان خادم الإدارة يدعم التشفير وحماية البيانات وأنت تقوم بإنشاء مهمة تغيير خادم الإدارة، فسيتم عرض تحذير. ينص التحذير على أنه إذا تم تخزين أي بيانات مشفرة على الأجهزة، بعد بدء الخادم الجديد في إدارة الأجهزة، سيتمكن المستخدمين من الوصول إلى البيانات المشفرة فقط التي عملوا عليها مسبقًا. وفي الحالات الأخرى، لن يُمنح الوصول إلى البيانات المشفرة. للوصول إلى أوصاف تفصيلية للسيناريوهات التي لا يتم فيها الوصول إلى البيانات المشفرة، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security for Windows.

نقل الأجهزة المتصلة بخادم الإدارة عبر بوابات الاتصال إلى خادم إدارة آخر

يمكنك نقل الأجهزة المتصلة بخادم الإدارة عبر بوابات الاتصال إلى خادم إدارة آخر. على سبيل المثال، قد يكون هذا مطلوبًا إذا قمت بتثبيت إصدار آخر من خادم الإدارة ولا تريد إعادة تثبيت عميل الشبكة على الأجهزة لأنه قد يستغرق وقتًا طويلاً.

يجب تشغيل الأوامر الموضحة في التعليمات على الأجهزة العميلة ضمن حساب يمتلك حقوق المسؤول.

لنقل جهاز متصل عبر بوابة الاتصال إلى خادم إدارة آخر:

1. قم بتشغيل الأداة المساعدة klmover باستخدام المعلمة `-address < server address >`، للتبديل إلى خادم الإدارة الجديد.

2. قم بتشغيل الأمر `klnagchk -nagwait -tl 4`.

3. قم بتشغيل الأوامر التالية لتعيين بوابة اتصال جديدة:

- `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt ";"\SS_SETTINGS"\ = ss_type|" BOOL_T -ss`
- `gateway ip or >" klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv ";"\SS_SETTINGS"\ = ss_type|" svt STRING_T -ss- "< name`

  هنا، يمثل `< gateway ip or name >` عنوان بوابة الاتصال التي يمكن الوصول إليها من الإنترنت.
- `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt ";"\SS_SETTINGS"\ = ss_type|" INT_T -ss`

  `13000` هو رقم منفذ TCP الذي تستمع إليه بوابة الاتصال.

4. قم بتشغيل الأمر `klnagchk -restart -tl 4` لبدء تشغيل خدمة عميل شبكة الاتصال.

يتم نقل الجهاز إلى خادم الإدارة الجديد وتوصيله من خلال البوابة المتصلة الجديدة.

مصفوفات المجموعات والخوادم

يدعم Kaspersky Security Center تقنية نظام المجموعة. إذا قام عميل الشبكة بإرسال معلومات لخادم الإدارة لتأكيد أن التطبيق المثبت على جهاز عميل أصبح جزءًا من مصفوفة خادم، فيصبح هذا الجهاز العميل عقدة نظام المجموعة. سيتم إضافة المجموعة بوصفها كائن فردي في المجلد **الأجهزة المُدارة** الخاص بشجرة وحدة التحكم مع أيقونة الخوادم ( ).

يمكن تمييز بعض الميزات النموذجية لنظام المجموعة:

- يكون نظام الإدارة والعقد الخاصة به دائمًا في نفس مجموعة الإدارة.
- في حالة محاول المسؤول نقل عقدة نظام مجموعة، تعود العقدة إلى مكانها الأصلي.
- إذا حاول المسؤول نقل نظام مجموعة إلى مجموعة مختلفة، فيتم نقل جميع عقده معه.

تشغيل الأجهزة العميلة وإيقاف تشغيلها وإعادة تشغيلها عن بُعد

يسمح لك Kaspersky Security Center بإدارة الأجهزة العميلة عن بُعد عن طريق تشغيلها أو إيقافها أو إعادة تشغيلها.

لإدارة الأجهزة العميلة عن بُعد:

1. اتصل بخادم الإدارة الذي يتولى إدارة الأجهزة.
2. يمكنك إنشاء مهمة إدارة الجهاز باستخدام إحدى الطرق التالية:

- إذا أردت تشغيل أو إيقاف تشغيل أو إعادة تشغيل الأجهزة المضمنة في مجموعة الإدارة المحددة، فقم بإنشاء مهمة للمجموعة المحددة.
- إذا كان عليك تشغيل أو إيقاف تشغيل أو إعادة تشغيل الأجهزة المضمنة في مجموعات إدارة مختلفة أو التي لا تنتمي إلى أي مجموعة منها، فقم بإنشاء مهمة لأجهزة محددة.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج. في النافذة **تحديد نوع المهمة** الخاصة بمعالج مهمة جديدة، حدد العقدة **Kaspersky Security Center** وافتح المجلد **خيارات متقدمة** وحدد المهمة **إدارة الأجهزة**.

3. قم بتشغيل المهمة التي تم إنشاؤها.

بعد انتهاء المهمة، سيتم تنفيذ الأمر (تشغيل أو إيقاف تشغيل أو إعادة تشغيل) على الأجهزة المحددة.

حول استخدام الاتصال المستمر بين جهاز مُدار وخادم الإدارة

بشكل افتراضي، لا يقدم Kaspersky Security Center الاتصال المستمر بين الأجهزة المدارة وخادم الإدارة. يؤسس عملاء الشبكة على الأجهزة المدارة بشكل دوري اتصالات ومزامنة مع خادم الإدارة. يتم تحديد الفاصل الزمني بين جلسات المزامنة هذه في سياسة عميل الشبكة وهو 15 دقيقة افتراضيًا. إذا كانت المزامنة المبكرة مطلوبة (على سبيل المثال، لفرض تطبيق نهج ما)، فيرسل خادم الإدارة حزمة شبكة موقعة إلى عميل الشبكة على المنفذ 15000 UDP. (يمكن لخادم الإدارة إرسال هذه الحزمة عبر شبكة IPv4 أو IPv6). إذا لم يكن هناك اتصال ممكن عبر UDP بين خادم الإدارة وجهاز مُدار لأي سبب من الأسباب، فسيتم تشغيل المزامنة عند الاتصال الروتيني التالي بين عميل الشبكة وخادم الإدارة أثناء فترة المزامنة.

ومع ذلك، لا يمكن إجراء بعض العمليات بدون اتصال مبكر بين عميل الشبكة وخادم الإدارة. تتضمن هذه العملية تشغيل وإيقاف المهام المحلية، وتلقي إحصائيات لتطبيق مُدار، وإنشاء نفق. لجعل هذه العمليات ممكنة، يجب عليك تمكين **عدم قطع الاتصال عن خادم الإدارة** اختيار على الجهاز المُدار.

حول المزامنة المفروضة

على الرغم من قيام Kaspersky Security Center بمزامنة الحالة والإعدادات والمهام والسياسات الخاصة بالأجهزة المدارة تلقائيًا، في بعض الحالات يحتاج المسؤول لمعرفة بالضبط ما إذا قد تم إجراء المزامنة بالفعل أم لا لجهاز محدد في الوقت الحالي.

في قائمة السياق الخاصة بالأجهزة المُدارة في وحدة تحكم الإدارة، يحتوي عنصر القائمة **جميع& المهام** على الأمر**فرض المزامنة**. عندما ينفذ Kaspersky Security Center 15.1 هذا الأمر، يحاول خادم الإدارة الاتصال بالجهاز. إذا نجحت هذه المحاولة، فسيتم تنفيذ المزامنة المفروضة. وإلا، فسيتم فرض المزامنة فقط بعد إجراء الاتصال المجدول التالي بين عميل الشبكة وخادم الإدارة.

حول جدول الاتصال

في نافذة خصائص عميل الشبكة، في القسم **الاتصال** وفي القسم الفرعي **جدول الاتصال**، يمكنك تحديد الفواصل الزمنية التي سيقوم خلالها عميل الشبكة بإرسال البيانات إلى خادم الإدارة.

الاتصال عند الحاجة. إذا حددت هذا الخيار، يتم إنشاء الاتصال عندما يتعين على عميل الشبكة إرسال بيانات إلى خادم الإدارة.

الاتصال في فواصل زمنية محددة. إذا حددت هذا الخيار، يقوم عميل الشبكة بالاتصال بخادم الإدارة في فترات محددة. ويمكنك إضافة فترات زمنية متعددة للاتصال.

إرسال رسائل إلى مستخدمي الجهاز

لإرسال رسالة إلى مستخدمي الأجهزة:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. يمكنك إنشاء مهمة إرسال رسالة لمستخدمي الجهاز بإحدى الطرق التالية:

- إذا كنت ترغب في إرسال رسالة إلى مستخدمي الأجهزة التي تنتمي إلى مجموعة الإدارة المحددة، فقم بإنشاء مهمة لمجموعة محددة.

- إذا أردت إرسال رسالة إلى مستخدمي الأجهزة التي تنتمي إلى مجموعات إدارة مختلفة أو التي لا تنتمي إلى أية مجموعات إدارة، فقم بإنشاء مهمة للأجهزة المحددة.

سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

3. في نافذة نوع المهمة في معالج مهمة جديدة، حدد عقدة **خادم الإدارة لـ Kaspersky Security Center** وافتح المجلد **خيارات متقدمة** وحدد مهمة **إرسال رسالة إلى مستخدم**. لا تتوافر مهمة إرسال رسائل إلى مستخدم إلا للأجهزة التي تعمل بنظام Windows. يمكنك أيضًا إرسال رسائل في قائمة سياق المستخدم في مجلد **حسابات المستخدمين**.

4. قم بتشغيل المهمة التي تم إنشاؤها.

بعد اكتمال المهمة، سيتم إرسال الرسالة التي تم إنشاؤها إلى مستخدمي الأجهزة المحددة. لا تتوافر مهمة إرسال رسائل إلى مستخدم إلا للأجهزة التي تعمل بنظام Windows. يمكنك أيضًا إرسال رسائل في قائمة سياق المستخدم في مجلد **حسابات المستخدمين**.

إدارة Kaspersky Security for Virtualization

يدعم Kaspersky Security Center خيار اتصال الأجهزة الظاهرية بخادم الإدارة. تتم حماية الأجهزة الظاهرية بواسطة Kaspersky Security for Virtualization. للمزيد من التفاصيل، يُرجى الرجوع إلى مستندات هذا التطبيق.

تكوين تبديل حالات الجهاز

يمكنك تغيير الشروط لتعيين الحالة حرجة أو تحذير لجهازٍ ما.

لتمكين تغيير حالة الجهاز إلى حرجة:

1. افتح نافذة الخصائص من خلال إحدى الطرق التالية:

- في المجلد **السياسات**، في قائمة السياق الخاصة بسياسة خادم إدارة، حدد **خصائص**.

- حدد **خصائص** في قائمة سياق مجموعة الإدارة.

2. في نافذة **خصائص**التي تفتح في جزء **الأقسام**، حدد **حالة الجهاز**.

3. في الجزء الأيمن، في القسم **تعيين الحالة إلى حرجة إذا** ، حدد خانة الاختيار المجاورة للحالة الموجودة في القائمة.

لا يمكنك تغيير سوى الإعدادات غير المقفلة في السياسة الأصلية.

4. انقر نقرًا مزدوجًا فوق اسم الشرط المحدد، ثم في النافذة التي تفتح، قم بتعيين القيمة المطلوبة للشرط.

لا يمكنك تعيين قيم للشروط التالية conditions: تطبيق الأمان غير مثبت، تم تثبيت تطبيقات غير متوافقة، تم اكتشاف ثغرات أمنية بالبرنامج، لا تتوافق إعدادات الجهاز المحمول مع السياسة، تم اكتشاف مشكلات أمان لم تتم معالجتها، حالة الجهاز المحددة بواسطة التطبيق، أصبح الجهاز غير مُدار، تطبيق الأمان ليس قيد التشغيل، انتهت صلاحية الترخيص.

بالنسبة لشرط **إعادة التشغيل مطلوبة**، يمكنك تحديد أسباب إعادة التشغيل. ونوصيك بتحديد خانات الاختيار الموجودة بجوار جميع الأسباب الموجودة في القائمة.

5. انقر على **موافق**.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار عى حرج .

لتمكين تغيير حالة الجهاز إلى تحذير:

1. افتح نافذة الخصائص من خلال إحدى الطرق التالية:

- في المجلد **السياسات**، في قائمة السياق الخاصة بسياسة خادم الإدارة، حدد **خصائص**.
- حدد **خصائص** في قائمة سياق مجموعة الإدارة.

2. في نافذة **خصائص**التي تفتح في جزء **الأقسام**، حدد **حالة الجهاز**.

3. في الجزء الأيمن، في قسم **تعيين الحالة إلى تحذير إذا**، حدد خانة الاختيار المجاورة للحالة الموجودة في القائمة.

لا يمكنك تغيير سوى الإعدادات غير المقفلة في السياسة الأصلية.

4. انقر نقرًا مزدوجًا فوق اسم الشرط المحدد، ثم في النافذة التي تفتح، قم بتعيين القيمة المطلوبة للشرط.

لا يمكنك تعيين قيم للشروط التالية conditions: تطبيق الأمان غير مثبت، تم تثبيت تطبيقات غير متوافقة، تم اكتشاف ثغرات أمنية بالبرنامج، لا تتوافق إعدادات الجهاز المحمول مع السياسة، تم اكتشاف مشكلات أمان لم تتم معالجتها، حالة الجهاز المحددة بواسطة التطبيق، أصبح الجهاز غير مُدار، تطبيق الأمان ليس قيد التشغيل، انتهت صلاحية الترخيص.

بالنسبة لشرط **إعادة التشغيل مطلوبة**، يمكنك تحديد أسباب إعادة التشغيل. ونوصيك بتحديد خانات الاختيار الموجودة بجوار جميع الأسباب الموجودة في القائمة.

5. انقر على **موافق**.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار عى تحذير .

وضع العلامات على الأجهزة وعرض العلامات المعينة

يتيح Kaspersky Security Center وضع العلامات الأجهزة. العلامة هي معرف جهاز التي يمكن استخدامها لتجميع الأجهزة أو وصفها أو العثور عليها. يمكن استخدام العلامات المخصصة للأجهزة لإنشاء التحديدات، للعثور على الأجهزة وتوزيعها بين مجموعات الإدارة.

يمكنك وضع علامة على الأجهزة يدويًا أو تلقائيًا. قم بوضع علامة على الجهاز يدويًا في خصائص الجهاز؛ قد يمكنك استخدام وضع العلامات يدويًا عندما يجب وضع علامة على جهاز فردي. يتم إجراء وضع العلامات التلقائي بواسطة خادم الإدارة وفقًا لقواعد وضع العلامات المحددة.

في خصائص خادم الإدارة، يمكنك إعداد وضع العلامات التلقائي للأجهزة التي يتم إدارتها بواسطة خادم الإدارة هذا. يتم وضع العلامات على الأجهزة تلقائيًا عند استيفاء قواعد محددة. تتطابق كل قاعدة فردية مع كل علامة. تنطبق القواعد على خصائص شبكة الجهاز ونظام التشغيل والتطبيقات المثبتة على الجهاز وخصائص الجهاز الأخرى. على سبيل المثال، يمكنك إعداد قاعدة التي ستقوم بتعيين علامة Win على جميع الأجهزة التي تعمل بنظام تشغيل Windows. ثم يمكنك استخدام هذه العلامة عند إنشاء تحديد جهاز، سيساعدك هذا على ترتيب جميع الأجهزة التي تعمل بنظام تشغيل Windows، وتعيين مهمة لهم.

يمكنك أيضًا استخدام العلامات كشروط لتفعيل ملف تعريف السياسة على جهاز مدار وذلك من أجل تطبيق ملفات تعريف سياسة محددة فقط على الأجهزة التي توجد عليها علامات محددة. على سبيل المثال، إذا ظهر جهاز يحمل علامة ساعٍ في مجموعة إدارة المستخدمين وإذا تم تمكين تفعيل ملف تعريف السياسة المقابلة بواسطة علامة ساعٍ، لذلك لن يتم تطبيق السياسة التي تم إنشاؤها لمجموعة المستخدمين على هذا الجهاز—لكن سيتم تطبيق ملف التعريف الخاص بملف تعريف السياسة. يمكن أن يتيح ملف تعريف السياسة لهذا الجهاز بدء بعض التطبيقات التي تم منعها من التشغيل بواسطة السياسة.

يمكن إنشاء العديد من قواعد وضع العلامات. يمكن تعيين جهاز فردي بالعديد من العلامات إذا قمت بإنشاء العديد من قواعد وضع العلامات وإذا تم استيفاء الشروط الخاصة بهذه القواعد في وقت واحد. يمكنك عرض قائمة بجميع العلامات التي تم تعيينها في خصائص الجهاز. يمكن تمكين كل قاعدة وضع علامات أو تعطيلها. إذا تم تمكين قاعدة، يتم تطبيقها على الأجهزة التي تمت إدارتها بواسطة خادم الإدارة. إذا لم تكن تستخدم قاعدة في الوقت الحالي ولكن قد تحتاجها في المستقبل، فليس عليك أن تقوم بإزالتها؛ يمكنك أن تقوم ببساطة بإلغاء تحديد خانة الاختيار **تمكين القاعدة** بدلًا من ذلك. في هذه الحالة، يتم تعطيل القاعدة؛ ولن يتم تنفيذها إلا في حالة تحديد خانة الاختيار **تمكين القاعدة** مرة أخرى. قد تحتاج إلى تعطيل قاعدة دون أن تقوم بإزالتها إذا كان يجب عليك استبعاد القاعدة من قائمة قواعد وضع العلامات بشكل مؤقت ومن ثم تضمينها مرة أخرى.

وضع علامات على الجهاز تلقائيًا

يمكنك إنشاء قواعد وضع العلامات تلقائيًا وتحريرها في نافذة خصائص الخادم.

لوضع علامات على الأجهزة تلقائيًا:

1. في شجرة وحدة التحكم، حدد العقدة التي تشتمل على اسم خادم الإدارة الذي يتعين عليك تحديد قواعد وضع العلامات له.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة خصائص خادم الإدارة، حدد قسم **قواعد وضع العلامات**.
4. في القسم **قواعد وضع العلامات**، انقر على الزر **إضافة**.
   يتم فتح النافذة **قاعدة جديدة**.
5. في النافذة **قاعدة جديدة**، قم بتكوين الخصائص العامة للقاعدة:
   - حدد اسم القاعدة.
     لا يمكن أن يحتوي اسم القاعدة على أكثر من 255 حرف ولا يمكن أن يتضمن أي رموز خاصة (مثل "*<>?\:|).
   - قم بتمكين أو تعطيل القاعدة باستخدام خانة الاختيار **تمكين القاعدة**.
     يتم تحديد خيار **تمكين القاعدة** بشكل افتراضي.
   - في حقل **علامة**، أدخل اسم العلامة.
     لا يمكن أن يحتوي اسم العلامة على أكثر من 255 حرف ولا يمكن أن يتضمن أي رموز خاصة (مثل "*<>?\:|).
6. في القسم **الشروط**، انقر على زر **إضافة** لإضافة شرط جديد، أو انقر على زر **خصائص** لتحرير شرط موجود.
   ستفتح نافذة معالج شرط قاعدة وضع العلامة تلقائيًا الجديد.
7. في النافذة **شرط تعيين العلامة**، حدد خانات الاختيار الخاصة بالشروط التي يجب أن تؤثر على وضع العلامات. يمكنك تحديد العديد من الشروط.
8. بناءً على شروط وضع العلامات التي حددتها، يعرض المعالج نوافذ إعداد الشروط المطابقة. إعداد بدء تشغيل القاعدة بحسب الشروط التالية:

- **استخدام الجهاز أو الاقتران مع شبكة محددة**—خصائص شبكة الجهاز، مثل اسم الجهاز في شبكة Windows، وتضمين الجهاز في مجال أو شبكة IP فرعية.

> إذا تم تعيين ترتيب حساس لحالة الأحرف لقاعدة البيانات التي تستخدمها في Kaspersky Security Center، احتفظ بالحالة عند تحديد اسم DNS للجهاز. وبخلاف ذلك، لن تعمل قاعدة وضع العلامات التلقائي.

- **استخدام Active Directory**—وجود الجهاز في الوحدة التنظيمية لـ Active Directory، وعضوية الجهاز في مجموعة Active Directory.
- **تطبيقات محددة**— وجود عميل الشبكة على الجهاز ونوع نظام التشغيل والإصدار والبنية.

- **الأجهزة الظاهرية**—تضمين الجهاز في نوع محدد من الأجهزة الظاهرية.
- **تم تثبيت تطبيق من سجل التطبيقات**—وجود تطبيقات لبائعين مختلفين على الجهاز.

9. بعد إعداد الشرط، أدخل اسمًا له، ثم أغلِق المعالج.

يمكنك إعداد العديد من الشروط لقاعدة واحدة إن لزم الأمر. في هذه الحالة، سيتم تعيين العلامة إلى الجهاز عند استيفائه لشرط واحد على الأقل. سيتم عرض الشروط التي قمت بإضافتها في نافذة خصائص القاعدة.

10. انقر فوق **موافق** في النافذة **قاعدة جديدة**، ثم انقر فوق **موافق** في نافذة خصائص خادم الإدارة.

يتم فرض تطبيق القواعد التي تم إنشائها حديثًا على الأجهزة المدارة بواسطة خادم الإدارة المحدد. إذا كانت إعدادات الجهاز مستوفية لشروط القاعدة، يتم تعيين العلامة إلى الجهاز.

عرض العلامات المعينة إلى جهاز وتكوينها

يمكنك عرض قائمة جميع العلامات التي تم تعيينها إلى الجهاز، وكذلك المتابعة لإعداد قواعد وضع العلامات تلقائيًا في نافذة خصائص الجهاز.

لعرض قائمة لجميع العلامات التي تم تعيينها إلى الجهاز وإعدادها:

1. في شجرة وحدة التحكم، افتح المجلد **الأجهزة المُدارة**.
2. في مساحة عمل المجلد **الأجهزة المُدارة**، حدد الجهاز الذي تود عرض العلامات المعينة له.
3. من قائمة سياق الجهاز المحمول، حدد **خصائص**.
4. في نافذة خصائص الجهاز، حدد القسم **علامات**.

سيتم عرض قائمة بالعلامات التي تم تعيينها للجهاز المحدد، وكذلك الطريقة التي تم بها تعيين كل علامة: يدويًا أو عن طريق قاعدة.

5. قم بتنفيذ أحد الإجراءات التالية، عند اللزوم:
   - لمتابعة إلى إعداد قواعد وضع العلامات، انقر فوق رابط **إعداد قواعد وضع العلامات تلقائيًا** (فقط مع نظام Windows).
   - لإعادة تسمية علامة، حدد علامة وانقر فوق الزر **إعادة تسمية**.
   - لإزالة علامة، حدد علامة انقر فوق الزر **إزالة**.
   - لإضافة علامة يدويًا، أدخل علامة في الحقل الموجود في الجزء السفلي من قسم **العلامات** وانقر فوق الزر **إضافة**.
6. انقر فوق الزر **تطبيق**، إذا قمت بإجراء تغييرات على قسم **العلامات**، لكي تسري التغييرات التي أجريتها.
7. انقر فوق **موافق**.

إذا قمت بإزالة علامة أو إعادة تسميتها في خصائص الجهاز، فلن يؤثر هذا التغيير على قواعد وضع العلامات التي تم إعدادها في خصائص خادم الإدارة. سيسري التغيير فقط على الجهاز الذي تم إعداد خصائصه.

التشخيصات عن بُعد للأجهزة العميلة. أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center

أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center (المشار إليها فيما بعد باسم أداة التشخيصات المساعدة عن بُعد) مصممة لتنفيذ العمليات التالية عن بُعد على الأجهزة العميلة:

- تمكين وتعطيل التتبع، تغيير مستوى التتبع، تنزيل ملف التتبع.
- تنزيل معلومات النظام وإعدادات التطبيق.
- تنزيل سجلات الأحداث.
- إنشاء ملف تفريغ لتطبيق.
- بدء التشخيصات وتنزيل تقاريرها.
- تشغيل التطبيقات وإيقاف تشغيلها.

يمكنك استخدام سجلات الأحداث وتقارير التشخيصات التي تم تنزيلها من جهاز عميل لاستكشاف المشكلات وإصلاحها بنفسك. قد يطالبك أيضًا أخصائي الدعم الفني لـ Kaspersky بتنزيل ملفات التتبع وملفات التفريغ وسجلات الأحداث وتقارير التشخيصات من جهاز عميل لإجراء المزيد من التحليلات في Kaspersky.

يتم تثبيت أداة التشخيص المساعدة عن بُعد تلقائيًا على الجهاز مع وحدة تحكم الإدارة.

توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل

توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل:

1. حدد أي مجموعة إدارة في شجرة وحدة التحكم.
2. في مساحة العمل، من علامة التبويب **الأجهزة**، في قائمة سياق أي جهاز، حدد **أدوات مخصصة** ← **تشخيصات عن بعد**.
   تفتح النافذة الرئيسية لأداة التشخيصات المساعدة عن بُعد.
3. حدد في الحقل الأول من النافذة الرئيسية للأداة المساعدة للتشخيصات عن بُعد الأدوات التي تنوي استخدامها للاتصال بالجهاز.
   - **الوصول باستخدام شبكة Microsoft Windows**.
   - **الوصول باستخدام خادم الإدارة**.
4. إذا قمت بتحديد **الوصول باستخدام شبكة Microsoft Windows** في الحقل الأول من النافذة الرئيسية للأداة المساعدة، فقم بتنفيذ الإجراءات التالية:
   - في الحقل **الجهاز**، حدد عنوان الجهاز الذي تريد الاتصال به
     يمكنك استخدام عنوان IP أو اسم NetBIOS أو اسم DNS كعنوان للجهاز.
     القيمة الافتراضية هي عنوان الجهاز الذي تم تشغيل الأداة المساعدة من قائمة السياق الخاصة به.

- تعيين حساب للاتصال بالجهاز:
  - **الاتصال كمستخدم حالي** (يتم تحديده بصورة افتراضية). اتصل بحساب المستخدم الحالي:
  - **استخدام اسم المستخدم وكلمة المرور المتوفرين للاتصال**. اتصل باستخدام حساب مستخدم متوفر: حدد **اسم المستخدم** و**كلمة المرور** الحساب المطلوب.

يمكن الاتصال بجهاز فقط بحساب المدير المحلي للجهاز.

5. إذا قمت بتحديد **الوصول باستخدام خادم الإدارة** في الحقل الأول من النافذة الرئيسية للأداة المساعدة، فقم بتنفيذ الإجراءات التالية:

- في الحقل **خادم الإدارة**، حدد عنوان خادم الإدارة الذي تنوي توصيل الجهاز به.

  يمكنك استخدام عنوان IP أو اسم NetBIOS أو اسم DNS كعنوان للخادم.

  القيمة الافتراضية هي عنوان خادم الإدارة الذي يتم منه تشغيل الأداة المساعدة.

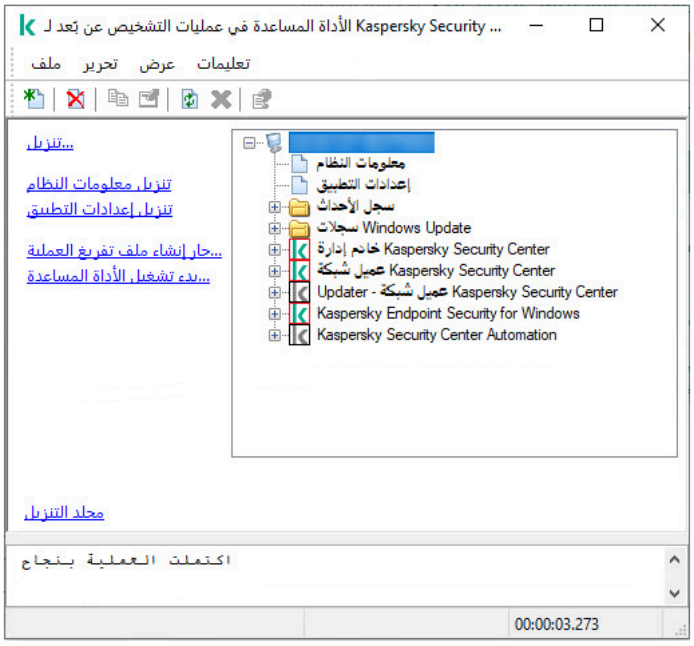
- إذا لزم الأمر، حدد خانات الاختيار **استخدام SSL**، و**ضغط حركة المرور**، و**ينتمي الجهاز إلى خادم إدارة ثانوي**.

  إذا تم تحديد خانة الاختيار **ينتمي الجهاز إلى خادم إدارة ثانوي**، يمكنك ملء الحقل **ينتمي الجهاز إلى خادم إدارة ثانوي** باسم خادم الإدارة الثانوي الذي يدير الجهاز عن طريق النقر فوق الزر **استعراض**.

6. للاتصال بالجهاز، انقر فوق الزر **تسجيل الدخول**.

يجب عليك أخذ التصريح باستخدام التحقق بخطوتين إذا تم تمكين التحقق بخطوتين في حسابك.

يفتح هذا النافذة المخصصة للتشخيصات عن بُعد للجهاز (انظر الشكل أدناه). يحتوي الجزء الأيسر من النافذة على ارتباطات لتشغيل تشخيصات الأجهزة. يحتوي الجزء الأيمن من النافذة على شجرة كائنات الجهاز الذي يمكن للأداة المساعدة التعامل معه. يعرض الجزء السفلي من النافذة تقدم عمليات الأداة المساعدة.



أداة التشخيصات المساعدة عن بُعد. نافذة تشخيصات الجهاز البعيد

تحفظ أداة التشخيصات المساعدة عن بُعد الملفات التي يتم تنزيلها من الأجهزة على سطح مكتب الجهاز الذي يتم منه تشغيل الأداة.

إنشاء ملف تفريغ لتطبيق.

يتيح لك ملف تفريغ التطبيق عرض معلمات التطبيق الذي يتم تشغيله على جهاز عميل في وقت معين. ويحتوي هذا الملف أيضًا على معلومات عن الوحدات النمطية التي تم تحميلها لأحد التطبيقات.

لا يتم دعم الحصول على عمليات تفريغ من الأجهزة المستندة إلى Linux.

للحصول على عمليات التفريغ من خلال التشخيص عن بعد، يتم استخدام الأداة المساعدة klldumper. وتم تصميم هذه الأداة للحصول على تفريغات عمليات تطبيقات Kaspersky بناءً على طلب متخصصي الدعم الفني. تتوفر معلومات تفصيلية عن متطلبات استخدام الأداة المساعدة klldumper في قاعدة معارف Kaspersky Security Center.

لإنشاء ملف تفريغ لتطبيق:

1. في مساحة عمل مجلد **الأجهزة المُدارة**، في علامة التبويب **الأجهزة**، افتح قائمة السياق للجهاز المطلوب، ثم حدد **أدوات مخصصة** ← **تشخيصات عن بعد**.
   تفتح النافذة **الأداة المساعدة في عمليات التشخيص عن بُعد لـ Kaspersky Security Center**.
2. توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل.
   يفتح هذا النافذة المخصصة للتشخيصات عن بُعد للجهاز.
3. في الجزء الأيسر من النافذة، انقر فوق الرابط **جارٍ إنشاء ملف تفريغ العملية**
4. في القسم **جارٍ إنشاء ملف تفريغ العملية**، حدد الملف التنفيذي الذي تريد إنشاء ملف تفريغ له.
5. انقر على زر **موافق**.

يتم تنزيل أرشيف يحتوي على ملف التفريغ للتطبيق المحدد.

إذا كان التطبيق المحدد لا يعمل على الجهاز العميل، فسيكون مجلد "النتيجة" الموجود في الأرشيف الذي تم تنزيله فارغًا.

إذا كان التطبيق المحدد قيد التشغيل، ولكن فشل التنزيل بسبب خطأ أو كان مجلد "النتيجة" الموجود في الأرشيف الذي تم تنزيله فارغًا، فارجع إلى قاعدة معارف Kaspersky Security Center.

تمكين وتعطيل التتبع، تنزيل ملف التتبع

لتمكين التتبع على جهاز بعيد:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد ثم قم بالاتصال بالجهاز المطلوب.
2. في شجرة كائنات الجهاز، حدد التطبيق الذي تحتاج إلى تمكين التتبع له.

يمكن تمكين التتبع وتعطيله للتطبيقات التي بها حماية ذاتية فقط إذا كان الجهاز متصلاً باستخدام أدوات خادم الإدارة.

إذا كنت ترغب في تمكين التتبع لعميل الشبكة، يمكنك أيضًا القيام بذلك أثناء إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. في هذه الحالة، سيقوم عميل الشبكة بكتابة معلومات التتبع وذلك حتى في حالة تعطيل التتبع لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد.

3. لتمكين التتبع:

a. في الجزء الأيسر من نافذة أداة التشخيصات المساعدة عن بُعد، انقر فوق **تمكين التتبع**.

b. في النافذة **تحديد مستوى التتبع** التي تفتح، نوصي بإبقاء القيم الافتراضية للإعدادات. عند الضرورة، سيقوم أخصائي الدعم الفني بإرشادك خلال عملية التكوين. تتوفر الإعدادات التالية:

- **مستوى التتبع**

يحدد مستوى التتبع مقدار التفاصيل التي يحتويها ملف التتبع.

- **التتبع القائم على التدوير** (غير متوفر سوى لـ Kaspersky Endpoint Security)

يقوم التطبيق باستبدال معلومات التتبع لمنع الزيادة المفرطة في حجم ملف التتبع. حدد العدد الأقصى للملفات التي سيتم استخدامها لتخزين معلومات التتبع، وأقصى حجم لكل ملف. في حالة كتابة العدد الأقصى لملفات التتبع ذات الحد الأقصى للحجم، يتم حذف ملف التتبع القديم حتى يتسنى كتابة ملف التتبع الجديد.

c. انقر فوق **موافق**.

4. في حالة For Kaspersky Endpoint Security، قد يطالبك أخصائي الدعم الفني بتمكين تتبع Xperf للحصول على معلومات حول أداء النظام.
لتمكين تتبع Xperf:

a. في الجزء الأيسر من نافذة أداة التشخيصات المساعدة عن بُعد، انقر فوق **تمكين تتبع Xperf**.

b. في النافذة **تحديد مستوى التتبع** التي تفتح، واستنادًا إلى طلب أخصائي الدعم الفني، قم بتحديد واحد من مستويات التتبع التالية:

- **مستوى سطحي**

يحتوي ملف التتبع من هذا النوع على الحد الأدنى لمقدار المعلومات حول النظام.

يتم تحديد هذا الخيار افتراضيًا.

- **مستوى عميق**

يحتوي ملف التتبع من هذا النوع على معلومات مفصلة مقارنة بملفات التتبع من النوع البسيط، وقد يطالبك أخصائي الدعم الفني بتحديده عندما لا يكون ملف التتبع من النوع البسيط كافيًا لتقييم الأداء. يحتوي ملف التتبع العميق على معلومات تقنية حول النظام والتي تشتمل على معلومات حول الجهاز ونظام التشغيل وقائمة بالتطبيقات والعمليات التي تم بدؤها وإنهاؤها والأحداث المستخدمة في تقييم الأداء والأحداث من أداة تقييم نظام Windows.

c. حدد أحد أنواع التتبع التالية:

- **النوع الرئيسي**

يتم استقبال معلومات التتبع أثناء تشغيل تطبيق Kaspersky Endpoint Security.

يتم تحديد هذا الخيار افتراضيًا.

- **النوع القائم على إعادة التشغيل**

يتم استقبال معلومات التتبع عند بدء تشغيل نظام التشغيل على الجهاز المُدار. يكون نوع التتبع هذا فعالًا عند حدوث المشكلة التي تؤثر على أداء النظام بعد تشغيل الجهاز وقبل بدء تشغيل Kaspersky Endpoint Security.

d. قد تتم مطالبتك أيضًا بتمكين الخيار **التتبع القائم على التدوير** لمنع الزيادة المفرطة في حجم ملف التتبع. ثم حدد الحد الأقصى لحجم ملف التتبع. عند وصول الملف للحد الأقصى للحجم، يتم استبدال معلومات التتبع القديمة بالمعلومات الجديدة.

e. انقر فوق **موافق**.

في بعض الحالات، يجب إعادة تشغيل تطبيق الأمان والمهمة التابعة له ليتم تمكين التتبع.

تقوم أداة التشخيصات المساعدة عن بُعد بتمكين التتبع للتطبيق المحدد.

لتنزيل ملف التتبع لتطبيق:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد وقم بالاتصال بالجهاز المطلوب، كما هو موصوف في "توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل".

2. من عقدة التطبيق، في المجلد **ملفات التتبع**، حدد الملف المطلوب.

3. في الجزء الأيسر من نافذة أداة التشخيصات المساعدة عن بُعد، انقر فوق **تنزيل ملف بالكامل**.

   بالنسبة إلى الملفات الكبيرة، يمكن تنزيل أحدث أجزاء التتبع.

   يمكنك حذف ملف التتبع المحدد. يمكن حذف الملف بعد تعطيل التتبع.

يتم تنزيل الملف المحدد في الموقع المحدد في الجزء السفلي من النافذة.

لتعطيل التتبع على جهاز بعيد:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد وقم بالاتصال بالجهاز المطلوب، كما هو موصوف في "توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل".

2. في شجرة كائن الجهاز، حدد التطبيق الذي ترغب في تعطيل التتبع له.

> يمكن تمكين التتبع وتعطيله للتطبيقات التي بها حماية ذاتية فقط إذا كان الجهاز متصلاً باستخدام أدوات خادم الإدارة.

3. في الجزء الأيسر من نافذة أداة التشخيصات المساعدة عن بُعد، انقر فوق **تعطيل التتبع**.

تقوم أداة التشخيصات المساعدة عن بُعد بتعطيل التتبع للتطبيق المحدد.

تنزيل إعدادات التطبيق

لتنزيل إعدادات التطبيق من جهاز بعيد:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد وقم بالاتصال بالجهاز المطلوب، كما هو موصوف في "توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل".

2. في شجرة الكائنات الخاصة بنافذة أداة التشخيصات المساعدة عن بُعد، حدد العقدة العليا باسم الجهاز.

3. في الجزء الأيسر من نافذة أداة التشخيصات المساعدة عن بُعد، حدد الإجراء الذي تحتاجه من الخيارات التالية:

   - **تنزيل معلومات النظام**
   - **تنزيل إعدادات التطبيق**
   - **جارٍ إنشاء ملف تفريغ العملية**

     في النافذة التي تفتح بعد أن تنقر فوق هذا الرابط، حدد الملف التنفيذي للتطبيق الذي تريد إنشاء ملف تفريغ له.
   - **بدء تشغيل الأداة المساعدة**

     في النافذة التي تفتح بعد أن تنقر فوق هذا الرابط، حدد الملف التنفيذي للأداة المساعدة التي ترغب في تشغيلها وإعدادات تشغيلها.

يتم تنزيل الأداة المساعدة المحددة وتشغيلها على الجهاز.

تنزيل سجلات الأحداث

لتنزيل سجل الأحداث من جهاز بعيد:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد وقم بالاتصال بالجهاز المطلوب، كما هو موصوف في "توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل".

2. في المجلد **سجلات أحداث النظام** الخاص بشجرة كائن الجهاز، حدد السجل ذي الصلة.

3. قم بتنزيل السجل المحدد من خلال النقر فوق الرابط **تنزيل سجل الحدث <Event log name>** في الجزء الأيسر لنافذة أداة التشخيصات المساعدة عن بُعد.

يتم تنزيل سجل الحدث المحدد في الموقع المحدد في الجزء السفلي.

تنزيل عناصر معلومات التشخيص المتعددة

تتيح لك الأداة المساعدة للتشخيص عن بُعد من Kaspersky Security Center تنزيل عناصر متعددة من المعلومات التشخيصية بما في ذلك سجلات الأحداث، ومعلومات النظام، وملفات التتبع، وملفات التفريغ.

قم بما يلي لتنزيل معلومات تشخيصية من جهاز بعيد:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد وقم بالاتصال بالجهاز المطلوب، كما هو موصوف في "توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل".

2. في الجزء الأيسر من نافذة أداة التشخيصات المساعدة عن بُعد، انقر فوق **تنزيل**.

3. حدد خانات الاختيار الموجودة بجوار العناصر التي تريد تنزيلها.

4. انقر على **بدء**

يتم تنزيل كل عنصر محدد في الموقع المحدد في الجزء السفلي.

بدء التشخيصات وتنزيل النتائج

لبدء التشخيصات لأحد التطبيقات على جهاز بعيد وتنزيل نتائجها:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد وقم بالاتصال بالجهاز المطلوب، كما هو موصوف في "توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل".

2. في شجرة كائنات الجهاز، حدد التطبيق المطلوب.

3. قم ببدء تشغيل التشخيصات من خلال النقر فوق الرابط **تشغيل التشخيصات** الموجود في الجزء الأيسر من نافذة أداة التشخيصات المساعدة عن بُعد.

يظهر تقرير التشخيص في عقدة التطبيق المحدد في شجرة الكائن.

4. حدد تقرير التشخيصات المنشأ حديثًا في شجرة الكائنات وقم بتنزيله عن طريق النقر فوق الرابط **مجلد التنزيل**.

يتم تنزيل التقرير المحدد في الموقع المحدد في الجزء السفلي.

تشغيل التطبيقات وإيقافها وإعادة تشغيلها

يمكنك تشغيل التطبيقات وإيقافها وإعادة تشغيلها فقط إذا كنت متصلاً بالجهاز باستخدام أدوات خادم الإدارة.

لتشغيل أحد التطبيقات وإيقافه وإعادة تشغيله:

1. قم بتشغيل أداة التشخيصات المساعدة عن بُعد وقم بالاتصال بالجهاز المطلوب، كما هو موصوف في "توصيل أداة التشخيصات المساعدة عن بُعد بجهاز عميل".
2. في شجرة كائنات الجهاز، حدد التطبيق المطلوب.
3. حدد أحد الإجراءات من الجزء الأيسر لنافذة أداة التشخيصات المساعدة عن بُعد:
   - **إيقاف التطبيق**
   - **إعادة تشغيل التطبيق**
   - **بدء تشغيل التطبيق**

   بناءً على الإجراء الذي حددته، يتم تشغيل التطبيق أو إيقافه أو إعادة تشغيله.

أجهزة الحماية UEFI

جهاز حماية UEFI هو جهاز مثبت عليه حل أو تطبيق Kaspersky لواجهة البرامج الثابتة الموحدة القابلة للتوسيع (UEFI) المتكاملة على مستوى BIOS. تضمن الحماية المتكاملة أمن الجهاز من الوقت الذي يبدأ فيه تشغيل النظام، ولكن تبدأ الحماية على الأجهزة دون البرامج المتكاملة في العمل بعد بدء تطبيق الأمن فقط. يدعم Kaspersky Security Center إدارة هذه الأجهزة

لتعديل إعدادات اتصال أجهزة حماية UEFI:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة خصائص خادم الإدارة، حدد **إعدادات الاتصال بالخادم** > **المنافذ الإضافية**.
4. في القسم **منافذ إضافية**، قم بتعديل الإعدادات ذات الصلة:
   - **فتح منفذ لأجهزة حماية جهاز UEFI وأجهزة KasperskyOS**

     يمكن لأجهزة حماية UEFI الاتصال بخادم الإدارة.
   - **منفذ لأجهزة حماية UEFI وأجهزة KasperskyOS**

     يمكنك تغيير رقم المنفذ إذا تم تمكين الخيار **فتح منفذ لأجهزة حماية جهاز UEFI وأجهزة KasperskyOS**. رقم المنفذ الافتراضي هو 13294.
5. انقر على**موافق**.

إعدادات جهاز مدار

لعرض إعدادات جهاز مُدار:

1. في شجرة وحدة التحكم، افتح المجلد **الأجهزة المُدارة**.
2. في مساحة عمل المجلد، حدد جهازًا.
3. في قائمة السياق الخاصة بالجهاز، حدد **خصائص**.

يتم فتح نافذة الخصائص للجهاز المحدد، مع تحديد القسم **عام**.

عام

يعرض القسم **عام** معلومات عامة عن الجهاز العميل. يتم تقديم المعلومات بناءً على البيانات المستلمة أثناء المزامنة الأخيرة للجهاز العميل مع خادم الإدارة:

- **الاسم**

  في هذا الحقل، يمكنك عرض اسم كمبيوتر الجهاز وتعديله في مجموعة الإدارة.

- **الوصف**

  في هذا الحقل، يمكنك إدخال وصف إضافي للجهاز العميل.

- **مجال Windows**

  مجال Windows أو مجموعة العمل، التي تحتوي على الجهاز.

- **اسم NetBIOS**

  اسم مجال Windows للجهاز العميل.

- **اسم DNS**

  اسم مجال DNS للجهاز العميل.

- **عنوان IP**

  عنوان IP الخاص بالجهاز.

- **المجموعة**

  مجموعة الإدارة التي تتضمن الجهاز العميل.

- **تاريخ آخر تحديث**

  تاريخ آخر تحديث لقواعد بيانات مكافحة الفيروسات أو التطبيقات على الجهاز.

- **آخر وقت مرئي**

  التاريخ والوقت اللذين كان فيهما الجهاز مرئيًا على الشبكة.

- **تم الاتصال بخادم الإدارة**

تاريخ ووقت تثبيت عميل الشبكة على آخر جهاز عميل تم توصيله بخادم الإدارة.

- **عدم قطع الاتصال عن خادم الإدارة**

إذا تم تمكين هذا الخيار، فسيتم الحفاظ على الاتصال المستمر بين الجهاز المُدار وخادم الإدارة. قد ترغب في استخدام هذا الخيار إذا لم تكن تستخدم خوادم الإرسال، التي توفر مثل هذا الاتصال.

إذا تم تعطيل هذا الخيار، فسيتصل جهاز العميل فقط بخادم الإدارة لمزامنة البيانات أو نقل المعلومات فقط.

الحد الأقصى لعدد الأجهزة التي تم تحديد خيار **عدم قطع الاتصال عن خادم الإدارة** هو 300.

يتم تعطيل هذا الخيار افتراضيًا على الأجهزة المُدارة. يتم تمكين هذا الخيار افتراضيًا على الجهاز حيث تم تثبيت خادم الإدارة ويظل ممكّنًا حتى إذا حاولت تعطيله.

الحماية

يقدم القسم **الحماية** معلومات حول الحالة الحالية للحماية ضد الفيروسات على الجهاز العميل:

- **حالة الجهاز**

يتم تعيين حالة الجهاز بناء على المعايير التي حددها المسؤول عن حالة الحماية ضد الفيروسات على الجهاز وعن نشاط الجهاز على الشبكة.

- **كل المشكلات**

يحتوي هذا الجدول على قائمة كاملة من المشكلات التي تم اكتشافها من خلال التطبيقات المُدارة المثبتة على الجهاز العميل. كل مشكلة تقترن بها حالة ما، والتي يقترحها التطبيق عليك لتعيينها إلى الجهاز المعني بهذه المشكلة.

- **الحماية في الوقت الحقيقي**

يوضح هذا الحقل الحالة الحالية للحماية في الوقت الفعلي على الجهاز العميل.

عندما تتغير الحالة على الجهاز، يتم عرض الحالة الجديدة في نافذة خصائص الجهاز فقط بعد أن تتم مزامنة الجهاز العميل مع خادم الإدارة.

- **آخر فحص عند الطلب**

تاريخ ووقت آخر فحص للبرمجيات الضارة تم إجراءه على الجهاز العميل.

- **إجمالي عدد التهديدات المكتشفة**

العدد الإجمالي للتهديدات المكتشفة على الجهاز العميل منذ تثبيت تطبيق الأمان (الفحص الأول) أو منذ آخر إعادة تعيين لعداد الفيروسات.

- **تهديدات نشطة**

عدد الملفات التي لم تتم معالجتها على الجهاز العميل.

يتجاهل هذا الحقل عدد الملفات التي لم تتم معالجتها على الأجهزة المحمولة.

- **حالة تشفير القرص**

الحالة الحالية لتشفير الملفات على محركات أقراص الجهاز المحلية. للحصول على وصف للحالات، انظر تعليمات Kaspersky Endpoint Security for Windows.

التطبيقات

يدرج قسم **التطبيقات** جميع تطبيقات Kaspersky المثبتة على الجهاز العميل: يحتوي هذا القسم على زر البدء ( ) وزر الإيقاف ( ) الذي يسمح لك ببدء تشغيل تطبيق Kaspersky المحدد وإيقافه (باستثناء عميل الشبكة). ويتم تمكين هذه الأزرار في حالة توفر المنفذ 15000 UDP على الجهاز المُدار لاستلام الإخطارات الفورية من خادم الإدارة. إذا كان الجهاز المُدار غير متاح للإخطارات الفورية، لكن تم تمكين وضع الاتصال المستمر بخادم الإدارة (يتم تمكين خيار **عدم قطع الاتصال عن خادم الإدارة** في القسم **عام**)، فإن زري البدء والإيقاف يكونا متاحين أيضًا. ويحتوي القسم **التطبيقات** أيضًا على الأزرار التالية:

- **الأحداث**

انقر على زر لعرض قائمة بالأحداث التي وقعت على الأجهزة العميلة عندما تم تشغيل التطبيق، ولعرض نتائج المهمة لهذا التطبيق.

- **إحصائيات**

انقر فوق هذا الزر لعرض المعلومات الإحصائية الحالية حول التطبيق.

- **خصائص**

انقر على الزر لتلقي معلومات حول التطبيق وكذلك لتكوين التطبيق.

المهام

في علامة التبويب **المهام**، يمكنك إدارة المهام الخاصة بأجهزة العميل: عرض قائمة المهام الحالية وإنشاء مهام جديدة وإزالتها وبدء المهام وإيقافها وتعديل إعداداتها وعرض نتائج التنفيذ. تتوفر قائمة المهام بناءً على البيانات المستلمة أثناء آخر جلسة لمزامنة الكمبيوتر العميل مع خادم الإدارة. يطلب خادم الإدارة تفاصيل حالة المهمة من الجهاز العميل.

البدء ( ) والإيقاف ( ) والإزالة ( ) يتم تمكين الأزرار في حالة توفر المنفذ 15000 UDP على الجهاز المُدار لاستلام الإخطارات الفورية من خادم الإدارة. إذا كان الجهاز المُدار غير متاح للإخطارات الفورية، لكن تم تمكين وضع الاتصال المستمر بخادم الإدارة (يتم تمكين خيار **عدم قطع الاتصال عن خادم الإدارة** في القسم **عام**)، فإن أزرار البدء والإيقاف والإزالة تكون متاحة أيضًا.

إذا لم يتم إنشاء الاتصال، فلن يتم عرض حالة المهمة ويتم تعطيل الأزرار.

أحداث

علامة التبويب **الأحداث** تعرض الأحداث المسجلة على خادم الإدارة للجهاز العميل المحدد.

يمكنك تصدير ونسخ وحذف أحداث الجهاز.

العلامات

في علامة التبويب **العلامات**، يمكنك إدارة قائمة الكلمات الأساسية المستخدمة للعثور على أجهزة العميل: قم بعرض قائمة بالعلامات الحالية وتعيين علامات من القائمة وتكوين قواعد وضع العلامات تلقائيًا وإضافة علامات جديدة وإعادة تسمية العلامات القديمة وإزالة العلامات.

معلومات النظام

يوفر القسم **معلومات عامة عن النظام** معلومات حول التطبيق المثبت على الجهاز العميل.

سجل التطبيقات

في القسم **سجل التطبيقات**، يمكنك عرض سجل التطبيقات المثبتة على الجهاز العميل والتحديثات الخاصة بها؛ بالإضافة إلى إعداد عرض سجل التطبيقات.

يتم توفير معلومات حول التطبيقات المثبتة في حالة تثبيت عميل الشبكة على الجهاز العميل الذي يقوم بإرسال المعلومات المطلوبة إلى خادم الإدارة. يمكنك تكوين إرسال المعلومات إلى خادم الإدارة في نافذة خصائص عميل الشبكة أو سياستها في القسم **المستودعات**.

- **عرض تطبيقات الأمان غير المتوافقة فقط**

  في حال تمكين هذا الخيار، فلن تحتوي قائمة التطبيقات إلا على تطبيقات الأمان غير المتوافقة مع تطبيقات Kaspersky.

  يتم تعطيل هذا الخيار افتراضيًا.

- **عرض التحديثات**

  في حال تمكين هذا الخيار، ستحتوي قائمة التطبيقات على التطبيقات وحزم التحديثات المثبتة لها.

  لإظهار قائمة التحديثات، هناك حاجة إلى 100 كيلوبايت من حركة البيانات. إذا أغلقت القائمة وأعدت فتحها، فسيتعين عليك إنفاق 100 كيلوبايت من حركة البيانات مرة أخرى.

  يتم تعطيل هذا الخيار افتراضيًا.

- **تصدير إلى الملف**

  انقر على هذا الزر لتصدير قائمة التطبيقات المثبتة على الجهاز إلى ملف CSV أو TXT.

- **محفوظات**

  انقر على هذا الزر لعرض الأحداث المتعلقة بتثبيت التطبيقات على الجهاز. يتم عرض المعلومات التالية:

  - تاريخ ووقت تثبيت التطبيق على الجهاز
  - اسم التطبيق
  - إصدار التطبيق

- **خصائص**

  انقر على هذا الزر لعرض خصائص التطبيق المحدد في قائمة التطبيقات المثبتة على الجهاز. يتم عرض المعلومات التالية:

  - اسم التطبيق
  - إصدار التطبيق
  - بائع التطبيق

الملفات التنفيذية

يعرض القسم **الملفات التنفيذية** الملفات التنفيذية التي تم العثور عليها على الجهاز العميل.

سجل الأجهزة

في القسم **سجل الأجهزة**، يمكنك عرض معلومات عن الأجهزة المثبتة على الجهاز العميل. يمكنك عرض هذه المعلومات لأجهزة Windows وأجهزة Linux.

تأكد من تثبيت الأداة المساعدة lshw على أجهزة Linux التي تريد جلب تفاصيل الأجهزة منها. قد تكون تفاصيل الأجهزة التي يتم جلبها من الأجهزة الافتراضية غير مكتملة بناءً على برنامج مراقب الأجهزة الافتراضية المستخدم.

في حالة تثبيت عميل الشبكة على جهاز يعمل بنظام Windows، فإنه يرسل إلى خادم الإدارة المعلومات التالية عن أجهزة الجهاز:

- الذاكرة العشوائية
- أجهزة تخزين كبيرة السعة
- اللوحة الأم
- CPU
- محولات الشبكة
- الشاشات
- محول الفيديو
- بطاقة الصوت

في حالة تثبيت عميل الشبكة على جهاز يعمل بنظام Linux أو macOS، فإنه يرسل إلى خادم الإدارة المعلومات التالية فقط عن مكونات الجهاز، إذا وفر نظام التشغيل هذه المعلومات:

- إجمالي حجم RAM
- الحجم الإجمالي لأجهزة التخزين عالية السعة
- اللوحة الأم
- CPU
- محولات الشبكة

الجلسات

يعرض القسم **الجلسات** فقط لأجهزة Windows ويحتوي على معلومات عن مالك الجهاز العميل، بالإضافة إلى حسابات المستخدمين الذين عملوا على جهاز العميل المحدد.

يتم إنشاء المعلومات بشأن مستخدمي المجال اعتمادًا على بيانات Active Directory. تتوفر تفاصيل المستخدمين المحليين بواسطة Windows Security Account Manager المثبت على الجهاز العميل.

- **مالك الجهاز**

  يعرض الحقل **مالك الجهاز** اسم المستخدم الذي يمكن للمسؤول الاتصال به عند الحاجة إلى إجراء عمليات محددة على الجهاز العميل.

  استخدام الأزرار **تعيين** و**خصائص** لتحديد مالك الجهاز وعرض معلومات حول المستخدم الذي تم تعيينه كمالك للجهاز.

  استخدام الزر الذي يحتوي على رمز صليب أحمر لحذف مالك الجهاز الحالي.

تعرض القائمة حسابات المستخدمين الذين يعملون على الجهاز العميل.

- **الاسم**

  اسم الجهاز الموجود في شبكة Windows.

- **اسم المشارك**

  اسم (اسم المجال أو الاسم المحلي) المستخدم الذي قام بتسجيل الدخول إلى النظام على هذا الجهاز.

- **الحساب**

  حساب المستخدم الذي قام بتسجيل الدخول إلى هذا الجهاز.

- **البريد الإلكتروني**

  عنوان البريد الإلكتروني للمستخدم.

- **الهاتف**

  رقم هاتف المستخدم.

مشاكل الأمان

في علامة التبويب **مشاكل الأمان**، يمكنك عرض مشاكل الأمان وتحريرها وإنشاؤها للجهاز العميل. يمكن إنشاء مشاكل الأمان إما تلقائيًا من خلال تطبيقات Kaspersky المُدارة المثبتة على الجهاز العميل أو يدويًا من قبل المسؤول. على سبيل المثال، إذا قام بعض المستخدمين بنقل برامج ضارة من محركات الأقراص القابلة للإزالة الخاصة بهم إلى الأجهزة بانتظام، فيمكن للمسؤول إنشاء مشكلة أمان. يمكن للمسؤول توفير وصف مختصر للحالة والإجراءات الموصى بها (مثل الإجراءات التأديبية التي سيتم اتخاذها ضد المستخدم) في نص مشكلة الأمان، ويمكنه إضافة رابط للمستخدم أو المستخدمين.

يُطلق على مشكلة أمان تم اتخاذ جميع الإجراءات المطلوبة بشأنها تمت المعالجة. قد يتم اختيار وجود مشاكل أمان غير معالجة كشرط لتغيير حالة الجهاز إلى حرج أو تحذير.

يحتوي هذا القسم على قائمة بمشاكل الأمان التي تم إنشاؤها للجهاز. يتم تصنيف مشاكل الأمان بحسب مستوى الخطورة وبحسب النوع. يتم تحديد نوع مشكلة أمان بواسطة تطبيق Kaspersky، الذي يقوم بإنشاء مشكلة الأمان. يمكنك تمييز مشاكل الأمان التي تمت معالجتها في القائمة عن طريق تحديد خانة الاختيار الموجودة في العمود **تمت المعالجة**.

الثغرات الأمنية بالبرامج

يوفر القسم **الثغرات الأمنية بالبرنامج** معلومات حول الثغرات الأمنية في تطبيقات الجهة الخارجية المثبتة على أجهزة العميل. يمكنك استخدام حقل البحث الموجود فوق القائمة للبحث عن الثغرات الأمنية بحسب أسمائها.

- **تصدير إلى الملف**

انقر على زر **تصدير إلى ملف** لحفظ قائمة بالثغرات الأمنية في ملف. يقوم التطبيق بتصدير قائمة الثغرات الأمنية إلى ملف CSV تلقائيًا.

- **إظهار الثغرات الأمنية التي يمكن إصلاحها فقط**

إذا تم تمكين هذا الخيار، فسيعرض القسم الثغرات الأمنية التي يمكن إصلاحها عن طريق استخدام تصحيح.

إذا تم تعطيل هذا الخيار، فسيعرض القسم كل من الثغرات الأمنية التي يمكن إصلاحها باستخدام تصحيح، والثغرات الأمنية التي لم يتم إصدار تصحيح لها.

يتم تمكين هذا الخيار افتراضيًا.

- **خصائص**

حدد ثغرة أمنية في البرامج في القائمة وانقر على الزر **خصائص** لعرض خصائص الثغرات الأمنية في البرامج المُحدَّد في نافذة منفصلة. في النافذة، يمكنك إجراء ما يلي:

- تجاهل الثغرات الأمنية في البرامج على هذا الجهاز الذي تتم إدارته(في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console).
- عرض قائمة الإصلاحات الموصى بها للثغرة الأمنية.
- حدد تحديثات البرامج يدويًا لإصلاح الثغرات الأمنية (في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console).
- عرض مثيلات الثغرات الأمنية.
- عرض قائمة المهام الحالية لإصلاح الثغرات الأمنية وإنشاء مهام جديدة لإصلاح الثغرات الأمنية.

التحديثات المتوفرة

يعرض هذا القسم تحديثات البرامج التي تم العثور عليها على هذا الجهاز والتي لم يتم تثبيتها بعد. لم يتم إرسال المعلومات المتعلقة بتحديثات Microsoft Windows الاختيارية إلى خادم الإدارة.

- **عرض التحديثات المثبتة**

إذا تم تمكين هذا الخيار، فستعرض القائمة كلاً من التحديثات غير المثبتة والتحديثات المثبتة بالفعل على الجهاز العميل.

يتم تعطيل هذا الخيار افتراضيًا.

سياسات نشطة

يعرض هذا القسم قائمة بسياسات تطبيق Kaspersky المعينة حاليًا على هذا الجهاز.

- **تصدير إلى الملف**

يمكنك النقر على زر **تصدير إلى ملف** لحفظ قائمة السياسات المفعلة في ملف. بشكل افتراضي، يقوم التطبيق بتصدير قائمة السياسات إلى ملف CSV.

ملفات تعريف السياسة النشطة

- **ملفات تعريف السياسة النشطة**

تتيح لك القائمة عرض معلومات حول ملفات تعريف السياسة الموجودة، والتي تكون نشطة على الأجهزة العميلة. يمكنك استخدام شريط البحث الموجود فوق القائمة للعثور على ملفات تعريف السياسة المفعلة على القائمة عبر إدخال اسم السياسة أو اسم ملف تعريف السياسة.

- **تصدير إلى الملف**

يمكنك النقر فوق زر **تصدير إلى ملف** لحفظ قائمة ملفات تعريف السياسة المفعلة في ملف. بشكل افتراضي يقوم التطبيق بتصدير قائمة ملفات تعريف السياسة إلى ملف CSV.

نقاط توزيع

يوفر هذا القسم قائمة بنقاط التوزيع التي يتفاعل معها الجهاز.

- **تصدير إلى الملف**

انقر على زر **تصدير إلى ملف** لحفظ قائمة نقاط التوزيع صالتي يتفاعل معها الجهاز إلى ملف. بشكل افتراضي يقوم التطبيق بتصدير قائمة الأجهزة إلى ملف CSV.

- **خصائص**

انقر على زر **خصائص** لعرض نقطة التوزيع التي يتفاعل معها الجهاز وتكوينها.

إعدادات السياسة العامة

عام

في القسم **عام**، يمكنك تعديل حالة السياسة وتحديد إعدادات سياسة التوريث:

- في الكتلة **حالة السياسة**، يمكنك تحديد أحد أوضاع السياسة:
  - **سياسة نشطة**

    إذا تم تحديد هذا الخيار، تصبح السياسة نشطة.

    يتم تحديد هذا الخيار افتراضيًا.

  - **سياسة الوجود خارج المكتب**

    إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.

  - **سياسة غير نشطة**

    إذا تم تحديد هذا الخيار، تصبح السياسة غير نشطة، ولكنها تظل مخزنة في مجلد **السياسات**. إذا لزم الأمر، يمكن تنشيط السياسة.

- في مجموعة الإعدادات **توريث الإعدادات**، يمكنك تكوين توريث السياسة:

- **توريث الإعدادات من السياسة الأصلية**

إذا تم تمكين هذا الخيار، يتم توريث قيم إعدادات السياسة من سياسة المجموعة ذات المستوى الأعلى؛ ولهذا يتم إلغاء تأمينها.

يتم تمكين هذا الخيار افتراضيًا.

- **فرض توريث الإعدادات في السياسات الفرعية**

إذا تم تمكين هذا الخيار، يتم تنفيذ الإجراءات التالية بعد تطبيق تغييرات السياسة:

- سيتم توزيع قيم إعدادات السياسة إلى سياسات المجموعات الفرعية للإدارة، أي إلى السياسات الفرعية.

- في كتلة **توريث الإعدادات** الخاصة بالقسم **عام** في نافذة الخصائص لكل سياسة فرعية، سيتم تمكين الخيار **توريث الإعدادات من السياسة الأصلية** تلقائيًا.

إذا تم تمكين هذا الخيار، فسيتم تأمين إعدادات السياسة الفرعية.

يتم تعطيل هذا الخيار افتراضيًا.

تكوين الحدث

يتيح لك القسم **تكوين الحدث** تكوين تسجيل الحدث وإخطارات الحدث. يتم توزيع الأحداث حسب مستوى الأهمية على علامات التبويب التالية:

- **حرج**

لا يتم عرض علامة التبويب **حرج** في خصائص سياسة عميل الشبكة.

- **خلل وظيفي**

- **تحذير**

- **معلومات**

على كل علامة تبويب، تعرض القائمة أنواع الأحداث ومدّة تخزين الحدث الافتراضي على خادم الإدارة (بالأيام). يتيح لك النقر فوق الزر **خصائص** تحديد إعدادات تسجيل الحدث والإخطارات حول الأحداث المحددة في القائمة. بشكل افتراضي، يتم استخدام إعدادات الإخطار العام المحددة لخادم الإدارة الكامل لجميع أنواع الأحداث. إلا أنه يمكنك تغيير إعدادات محددة لأنواع الأحداث المطلوبة.

على سبيل المثال، في علامة التبويب **تحذير**، يمكنك تكوين نوع حدث **حدثت مشكلة أمنية**. قد تحدث مثل هذه الأحداث، على سبيل المثال ، عندما تكون مساحة القرص الحرة لنقطة التوزيع أقل من 2 جيجابايت (يلزم توفر 4 جيجابايت على الأقل لتثبيت التطبيقات وتنزيل التحديثات عن بُعد). لتكوين حدث **حدثت مشكلة أمنية**، حدده وانقر على زر **خصائص** . بعد ذلك، يمكنك تحديد مكان تخزين الأحداث التي وقعت وكيفية الإبلاغ عنها.

إذا اكتشف عميل الشبكة مشكلة أمان، فيمكنك إدارة هذه المشكلة باستخدام إعدادات جهاز مُدار.

لتحديد أنواع متعددة للحدث، استخدم مفتاح **Shift** أو **Ctrl**؛ لتحديد كل الأنواع، استخدم زر **تحديد الكل**.

إعدادات سياسة عميل الشبكة

لتكوين سياسة عميل الشبكة:

1. من شجرة وحدة التحكم، حدد مجلد **السياسات**.
2. في مساحة عمل المجلد، حدد سياسة عميل الشبكة.
3. في قائمة السياق للسياسة، حدد **خصائص**.

تفتح نافذة الخصائص لسياسة عميل الشبكة.

انظر جدول المقارنة الذي يوضح بالتفصيل كيفية تطبيق الإعدادات أدناه اعتمادًا على نوع نظام التشغيل المستخدم.

عام

في القسم **عام**، يمكنك تعديل حالة السياسة وتحديد إعدادات سياسة التوريث:

- في الكتلة **حالة السياسة**، يمكنك تحديد أحد أوضاع السياسة:
  - **سياسة نشطة**

    إذا تم تحديد هذا الخيار، تصبح السياسة نشطة.
    يتم تحديد هذا الخيار افتراضيًا.
  - **سياسة الوجود خارج المكتب**

    إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.
  - **سياسة غير نشطة**

    إذا تم تحديد هذا الخيار، تصبح السياسة غير نشطة، ولكنها تظل مخزنة في مجلد **السياسات**. إذا لزم الأمر، يمكن تنشيط السياسة.
- في مجموعة الإعدادات **توريث الإعدادات**، يمكنك تكوين توريث السياسة:
  - **توريث الإعدادات من السياسة الأصلية**

    إذا تم تمكين هذا الخيار، يتم توريث قيم إعدادات السياسة من سياسة المجموعة ذات المستوى الأعلى؛ ولهذا يتم إلغاء تأمينها.
    يتم تمكين هذا الخيار افتراضيًا.
  - **فرض توريث الإعدادات في السياسات الفرعية**

    إذا تم تمكين هذا الخيار، يتم تنفيذ الإجراءات التالية بعد تطبيق تغييرات السياسة:
    - سيتم توزيع قيم إعدادات السياسة إلى سياسات المجموعات الفرعية للإدارة، أي إلى السياسات الفرعية.
    - في كتلة **توريث الإعدادات** الخاصة بالقسم **عام** في نافذة الخصائص لكل سياسة فرعية، سيتم تمكين الخيار **توريث الإعدادات من السياسة الأصلية** تلقائيًا.

    إذا تم تمكين هذا الخيار، فسيتم تأمين إعدادات السياسة الفرعية.

يتم تعطيل هذا الخيار افتراضيًا.

تكوين الحدث

يتيح لك القسم **تكوين الحدث** تكوين تسجيل الحدث وإخطارات الحدث. يتم توزيع الأحداث حسب مستوى الأهمية على علامات التبويب التالية:

- **حرج**

  لا يتم عرض علامة التبويب **حرج** في خصائص سياسة عميل الشبكة.

- **خلل وظيفي**
- **تحذير**
- **معلومات**

على كل علامة تبويب، تعرض القائمة أنواع الأحداث ومدّة تخزين الحدث الافتراضي على خادم الإدارة (بالأيام). يتيح لك النقر فوق الزر **خصائص** تحديد إعدادات تسجيل الحدث والإخطارات حول الأحداث المحددة في القائمة. بشكل افتراضي، يتم استخدام إعدادات الإخطار العام المحددة لخادم الإدارة الكامل لجميع أنواع الأحداث. إلا أنه يمكنك تغيير إعدادات محددة لأنواع الأحداث المطلوبة.

على سبيل المثال، في علامة التبويب **تحذير**، يمكنك تكوين نوع حدث **حدثت مشكلة أمنية**. قد تحدث مثل هذه الأحداث، على سبيل المثال ، عندما تكون مساحة القرص الحرة لنقطة التوزيع أقل من 2 جيجابايت (يلزم توفر 4 جيجابايت على الأقل لتثبيت التطبيقات وتنزيل التحديثات عن بُعد). لتكوين حدث **حدثت مشكلة أمنية**، حدده وانقر على زر **خصائص** . بعد ذلك، يمكنك تحديد مكان تخزين الأحداث التي وقعت وكيفية الإبلاغ عنها.

إذا اكتشف عميل الشبكة مشكلة أمان، فيمكنك إدارة هذه المشكلة باستخدام إعدادات جهاز مُدار.

لتحديد أنواع متعددة للحدث، استخدم مفتاح **Shift** أو **Ctrl**؛ لتحديد كل الأنواع، استخدم زر **تحديد الكل**.

الإعدادات

في نافذة **الإعدادات**، يمكنك تكوين سياسة عميل الشبكة.

- **توزيع الملفات عبر نقاط التوزيع فقط**

  إذا تم تمكين هذا الخيار، فإن عملاء الشبكة على الأجهزة المدارة يستردون التحديثات من نقاط التوزيع فقط.

  إذا تم تعطيل هذا الخيار، فسيسترد عملاء الشبكة على الأجهزة المُدارة التحديثات من نقاط التوزيع أو من خادم الإدارة.

> لاحظ أن تطبيقات الأمان على الأجهزة المدارة تسترد التحديثات من مجموعة المصدر الموجودة في مهمة تحديث كل تطبيق أمان. إذا قمت بتمكين **توزيع الملفات عبر نقاط التوزيع فقط**، فتأكد من تعيين Kaspersky Security Center كمصدر تحديث في مهام التحديث.

يتم تعطيل هذا الخيار افتراضيًا.

- **الحجم الأقصى لقائمة انتظار الحدث، بالميجابايت**

  في هذا الحقل، يمكنك تحديد أقصى مساحة يمكن أن تشغلها قائمة انتظار الحدث على محرك الأقراص.

  القيمة الافتراضية هي 2 ميجابايت.

- **يُسمح للتطبيق باسترداد بيانات السياسة الموسعة على الجهاز**

يقوم عملاء الشبكة المثبت على جهاز تتم إدارته، بنقل معلومات حول سياسة تطبيق الأمان المطبقة على تطبيق الأمان (على سبيل المثال، Kaspersky Endpoint Security for Windows). يمكنك عرض المعلومات المنقولة في واجهة تطبيق الأمان.

يقوم عملاء الشبكة بنقل المعلومات التالية:

- وقت تسليم السياسة إلى الجهاز المُدار.
- اسم السياسة النشطة في لحظة تسليم السياسة إلى الجهاز المُدار.
- اسم سياسة "خارج المكتب" في لحظة تسليم السياسة إلى الجهاز المُدار (غير متوفر لعميل الشبكة لنظام Linux).
- الاسم والمسار الكامل لمجموعة الإدارة التي كانت تحتوي على الجهاز المُدار في لحظة تسليم السياسة إلى الجهاز المُدار.
- قائمة بملفات تعريف السياسة النشطة مع أسمائها وأولوياتها في لحظة تسليم السياسة إلى الجهاز المُدار.

يمكنك استخدام المعلومات لضمان تطبيق السياسة الصحيحة على الجهاز ولأغراض استكشاف الأخطاء وإصلاحها. يتم تعطيل هذا الخيار افتراضيًا.

- **حماية خدمة عميل الشبكة من عمليات الإزالة أو الإنهاء غير المُصرَّح بها، ومنع إجراء تغييرات في الإعدادات**

عند تمكين هذا الخيار، بعد تثبيت عميل الشبكة على جهاز مُدار، يتعذر إزالة المكون أو إعادة تكوينه دون الامتيازات المطلوبة. يتعذر إيقاف خدمة عميل الشبكة. هذا الخيار ليس له أي تأثير على وحدات التحكم في المجال.

قم بتمكين هذا الخيار لحماية عميل الشبكة في محطات العمل التي تعمل بحقوق المسؤول المحلي.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدام كلمة مرور إلغاء التثبيت**

إذا تم تمكين هذا الخيار، يمكنك تحديد كلمة المرور لإلغاء تثبيت أداة klmover وعميل الشبكة عن بُعد بالنقر فوق الزر **تعديل**.

يتم تعطيل هذا الخيار افتراضيًا.

المستودعات

في القسم **المستودعات**، يمكنك تحديد أنواع الكائنات التي سيتم إرسال تفاصيلها من عميل الشبكة إلى خادم الإدارة:

- **تفاصيل تحديثات Windows Update**

إذا تم تمكين هذا الخيار، فسيتم إرسال معلومات تحديثات Microsoft Windows التي يجب تثبيتها على أجهزة العميل إلى خادم الإدارة.

في بعض الأحيان، حتى في حال تعطيل هذا الخيار، يتم عرض التحديثات في خصائص الجهاز في قسم **التحديثات المتوفرة**. قد يحدث هذا الأمر إذا كانت أجهزة المؤسسة، على سبيل المثال، بها ثغرات أمنية يمكن إصلاحها بواسطة هذه التحديثات.

يتم تمكين هذا الخيار افتراضيًا. إنه متاح فقط لنظام التشغيل Windows.

لم يتم إرسال المعلومات المتعلقة بتحديثات Microsoft Windows الاختيارية إلى خادم الإدارة.

- **تفاصيل الثغرات الأمنية بالبرنامج والتحديثات المطابقة لها**

في حالة تمكين هذا الخيار، يتم إرسال معلومات حول الثغرات الأمنية في برامج الجهات الخارجية (بما في ذلك برامج Microsoft)، والتي تم الكشف عنها على الأجهزة المُدارة، وحول تحديثات البرامج لإصلاح الثغرات الأمنية الخارجية (لا يتضمن ذلك برامج Microsoft) إلى خادم الإدارة.

يعمل تحديد هذا الخيار (**تفاصيل الثغرات الأمنية بالبرنامج والتحديثات المطابقة لها**) على زيادة تحميل الشبكة، وتحميل قرص إدارة الخادم، واستهلاك موارد عميل الشبكة.

يتم تمكين هذا الخيار افتراضيًا. إنه متاح فقط لنظام التشغيل Windows.

لإدارة تحديثات البرامج لبرامج Microsoft، استخدم خيار **تفاصيل تحديثات Windows Update**.

- **تفاصيل سجلات الأجهزة**

يقوم عميل الشبكة المثبت على جهاز بإرسال معلومات حول مكونات الجهاز إلى خادم الإدارة. يمكنك عرض تفاصيل المكونات في خصائص الجهاز.

تأكد من تثبيت الأداة المساعدة lshw على أجهزة Linux التي تريد جلب تفاصيل الأجهزة منها. قد تكون تفاصيل الأجهزة التي يتم جلبها من الأجهزة الافتراضية غير مكتملة بناءً على برنامج مراقب الأجهزة الافتراضية المستخدم.

- **تفاصيل عن التطبيقات التي تم تثبيتها**

إذا تم تمكين هذا الخيار، فسيتم إرسال معلومات التطبيقات المثبتة على أجهزة العميل إلى خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **تضمين معلومات حول التصحيحات**

يتم إرسال معلومات حول تصحيحات التطبيقات المثبتة على الأجهزة العميلة إلى خادم الإدارة. قد يؤدي تمكين هذا الخيار إلى زيادة الحمل على خادم الإدارة ونظام إدارة قواعد البيانات (DBMS)، فضلاً عن زيادة حجم قاعدة البيانات.

يتم تمكين هذا الخيار افتراضيًا. إنه متاح فقط لنظام التشغيل Windows.

إذا كان تعديل بعض الإعدادات في هذا القسم ممنوعًا في سياسة عميل الشبكة، فلا يمكنك تعديلها.

تحديثات البرنامج والثغرات الأمنية

في القسم **تحديثات البرنامج والثغرات الأمنية**، يمكنك تكوين البحث عن تحديثات Windows وتوزيعها، وكذلك تمكين فحص الملفات التنفيذية لاكتشاف الثغرات الأمنية:

- **استخدام خادم الإدارة كخادم WSUS**

إذا تم تمكين هذا الخيار، فسيتم تنزيل تحديثات Windows في خادم الإدارة. يوفر خادم الإدارة تحديثات يمكن تنزيلها لخدمات Windows Update على الأجهزة العميلة في الوضع المركزي عن طريق عملاء الشبكة.

إذا تم تعطيل هذا الخيار، فلن يتم استخدام خادم الإدارة لتنزيل تحديثات Windows. في هذه الحالة، تتلقى الأجهزة العميلة تحديثات Windows بشكل مستقل.

يتم تعطيل هذا الخيار افتراضيًا.

- ضمن **السماح للمستخدمين بإدارة تثبيت تحديثات Windows Update**، يمكنك تقييد تحديثات Windows التي يمكن للمستخدمين تثبيتها يدويًا على أجهزتهم من خلال استخدام Windows Update.

> في الأجهزة التي تعمل بنظام التشغيل Windows 10، إذا عثر تحديث Windows على تحديثات للجهاز، فلن يتم تطبيق الخيار الجديد الذي عثرت عليه إلا بعد تثبيت التحديثات التي تم العثور عليها **السماح للمستخدمين بإدارة تثبيت تحديثات Windows Update**.

حدد أحد العناصر في القائمة المنسدلة:

- **السماح للمستخدمين بتثبيت جميع تحديثات Windows Update القابلة للتطبيق**

يمكن للمستخدمين تثبيت كافة تحديثات Microsoft Windows Update القابلة للتطبيق على الأجهزة الخاصة بهم.

حدد هذا الخيار إذا كنت لا تريد التدخل في تثبيت التحديثات.

> عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلًا من خادم الإدارة. يمكن ذلك في حالة عدم قيام خادم الإدارة بتنزيل هذه التحديثات بعد. ينتج عن تنزيل التحديثات من خوادم Microsoft حركة مرور إضافية.

- **السماح للمستخدمين بتثبيت تحديثات Windows Update المعتمدة فقط**

يمكن للمستخدمين تثبيت كافة تحديثات Microsoft Windows Update القابلة للتطبيق على الأجهزة الخاصة بهم والمعتمدة من قبلك.

على سبيل المثال، قد ترغب أولًا بالتحقق من تثبيت التحديثات في بيئة اختبار والتأكد من عدم تداخلهم في عملية تشغيل الأجهزة، وبعد ذلك فقط تسمح بتثبيت تلك التحديثات المعتمدة على أجهزة العميل.

عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلًا من خادم الإدارة. يمكن ذلك في حالة عدم قيام خادم الإدارة بتنزيل هذه التحديثات بعد. ينتج عن تنزيل التحديثات من خوادم Microsoft حركة مرور إضافية.

- **عدم السماح للمستخدمين بتثبيت تحديثات Windows Update**

لا يمكن للمستخدمين تثبيت تحديثات Microsoft Windows Update على الأجهزة الخاصة بهم يدويًا. تم تثبيت جميع التحديثات القابلة للتطبيق كما قمت بتكوينها.

حدد هذا الخيار إذا كنت تريد إدارة تثبيت التحديثات مركزيًا.

على سبيل المثال، قد ترغب في تحسين جدول التحديث لكي لا تصبح الشبكة محملة بشكل زائد. يمكنك جدولة التحديثات بعد ساعات العمل، بحيث لا تتعارض مع إنتاجية المستخدم.

- في مجموعة الإعدادات **وضع بحث تحديث Windows**، يمكنك تحديد وضع البحث عن التحديثات:

- **نشط**

إذا تم تحديد هذا الخيار، فسيتم دعم خادم الإدارة من عميل الشبكة الذي يبدأ طلب من وكيل تحديث Windows على الجهاز العميل إلى مصدر تحديث: خوادم Windows Update أو WSUS. ثم يمرر عميل الشبكة المعلومات التي تم الحصول عليها من وكيل تحديث Windows إلى خادم الإدارة.

لا يصبح الخيار ساريًا إلا إذا تم تحديد الخيار **الاتصال بخادم التحديث لتحديث البيانات** لمهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة.

يتم تحديد هذا الخيار افتراضيًا.

- **سلبي**

إذا قمت بتحديد هذا الخيار، فيقوم عميل الشبكة بشكل دوري بتمرير معلومات حول التحديثات التي تم استردادها في آخر عملية مزامنة لـ Windows Update مع مصدر التحديث إلى خادم الإدارة. في حالة عدم إجراء مزامنة لوكيل تحديث Windows مع مصدر تحديث، تصبح المعلومات حول التحديثات على خادم الإدارة غير محدثة.

حدد هذا الخيار إذا كنت ترغب في الحصول على تحديثات من ذاكرة التخزين المؤقت لمصدر التحديث.

- **معطل**

إذا كان هذا الخيار مجددًا، لا يقوم خادم الإدارة بطلب أي معلومات حول التحديثات.

حدد هذا الخيار إذا كنت تريد، على سبيل المثال، اختبار التحديثات على جهازك المحلي أولاً.

- **فحص الملفات التنفيذية للبحث عن الثغرات الأمنية عند تشغيلها**

إذا تم تمكين هذا الخيار، فيستم مسح الملفات التنفيذية ضوئيا للعثور على الثغرات الأمنية عند تشغيلها.

يتم تمكين هذا الخيار افتراضيًا.

إدارة إعادة التشغيل

في القسم **إدارة إعادة التشغيل**، يمكنك تحديد الإجراء المراد تنفيذه إذا كان يتعين إعادة تشغيل نظام التشغيل للجهاز المدار لاستخدام أحد التطبيقات بشكل صحيح أو تثبيته أو إلغاء تثبيته:

- **عدم إعادة تشغيل نظام التشغيل**

لن يتم إعادة تشغيل نظام التشغيل

- **إعادة تشغيل نظام التشغيل تلقائيًا عند الحاجة**

إذا لزم الأمر، يتم إعادة تشغيل نظام التشغيل تلقائيًا.

- **مطالبة المستخدم باتخاذ إجراء**

يقوم التطبيق بمطالبة المستخدم بالسماح بإعادة تشغيل نظام التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **تكرار المطالبة كل (بالدقائق)**

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بمطالبة المستخدم بالسماح بإعادة تشغيل نظام التشغيل بمعدل تكرار محدد في الحقل المجاور لخانة الاختيار. التردد المطلوب هو 5 دقائق بشكل افتراضي.

إذا تم تعطيل هذا الخيار، فلن يطالب التطبيق المستخدم بإعادة التشغيل بشكل متكرر.

يتم تمكين هذا الخيار افتراضيًا.

- **فرض إعادة التشغيل بعد (دقيقة)**

إذا تم تمكين هذا الخيار، بعد مطالبة المستخدم، فسيقوم التطبيق بفرض إعادة تشغيل نظام التشغيل عند انتهاء الفترة الزمنية المحددة في الحقل المجاور لخانة الاختيار.

إذا تم تعطيل هذا الخيار، فلن يفرض التطبيق إعادة التشغيل.

يتم تمكين هذا الخيار افتراضيًا.

- **فترة الانتظار قبل فرض إغلاق التطبيقات في الجلسات المحجوبة (بالدقائق)**

يتم غلق التطبيقات إجباريًا عند قفل جهاز المستخدم (تلقائيًا عقب فترة زمنية محددة من عدم النشاط، أو يدويًا)

إذا تم تمكين هذا الخيار، فسيتم فرض غلق التطبيقات على الجهاز المقفل عند انتهاء الفترة الزمنية المحددة في حقل الإدخال.

إذا تم تعطيل هذا الخيار، فلن يتم غلق التطبيقات على الجهاز المقفل.

يتم تعطيل هذا الخيار افتراضيًا.

مشاركة سطح المكتب لـ Windows

في القسم **مشاركة سطح المكتب لـ Windows**، يمكنك تمكين وتكوين مراجعة إجراءات المسؤول التي تم إجراؤها على جهاز عن بُعد عند مشاركة الوصول إلى سطح المكتب:

- **تمكين التدقيق**

إذا تم تحديد هذا الاختيار، فسيتم تمكين التدقيق في إجراءات المسؤول التي تمت في الجهاز البعيد. يتم تسجيل إجراءات المسؤول على الجهاز البعيد:

- في سجل الحدث على الجهاز البعيد
- في ملف مزود بامتداد syslog الموجود في مجلد تثبيت عميل الشبكة على الجهاز البعيد
- في قاعدة بيانات الحدث في برنامج Kaspersky Security Center

تتوفر مراجعة إجراءات المسؤول عند تلبية الشروط التالية:

- استخدام ترخيص إدارة الثغرات الأمنية والتصحيحات بالفعل
- تمتع المسؤول بالحق في تشغيل الوصول المشترك لسطح مكتب الجهاز البعيد

إذا تم تعطيل هذا الاختيار، فسيتم تعطيل مراجعة إجراءات المسؤول على الجهاز البعيد.

يتم تعطيل هذا الخيار افتراضيًا.

- **أقنعة الملفات التي ينبغي مراقبتها عند قراءتها**

تحتوي القائمة على أقنعة الملف. عند تمكين المراجعة، يقوم التطبيق بمراقبة ملفات قراءة المسؤول التي تتطابق مع الأقنعة ثم يقوم بحفظ معلومات بشأن الملفات التي تمت قراءتها. تتوفر القائمة إذا تم تحديد خانة الاختيار **تمكين المراجعة**. يمكنك تحرير أقنعة الملف وإضافة أقنعة جديدة إلى القائمة. ينبغي تحديد كل قناع ملف جديد في القائمة على سطر جديد.

يتم تحديد أقنعة الملف التالية افتراضيًا:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **أقنعة الملفات التي ينبغي مراقبتها عند تعديلها**

تضم القائمة أقنعة الملفات الموجودة على الجهاز البعيد. عند تمكين المراجعة، يقوم التطبيق بمراقبة التغييرات التي تم إجراؤها بواسطة المسؤول في الملفات التي تتطابق مع الأقنعة، ثم يقوم بحفظ معلومات بشأن تلك التعديلات. تتوفر القائمة إذا تم تحديد خانة الاختيار **تمكين المراجعة**. يمكنك تحرير أقنعة الملف وإضافة أقنعة جديدة إلى القائمة. ينبغي تحديد كل قناع ملف جديد في القائمة على سطر جديد.

يتم تحديد أقنعة الملف التالية افتراضيًا:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

إدارة التصحيحات والتحديثات

في القسم **إدارة التصحيحات والتحديثات**، يمكنك تكوين تنزيل التحديثات وتوزيعها، وكذلك تثبيت التصحيحات على الأجهزة المدارة:

- **التثبيت التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة**

إذا تم تمكين هذا الخيار، فإنه يتم تثبيت تصحيحات Kaspersky ذات حالة الموافقة غير محدد تلقائيًا على الأجهزة المُدارة على الفور بعد تنزيلها من خوادم التحديث.

إذا تم تعطيل هذا الخيار، فسوف يتم تثبيت تصحيحات Kaspersky التي تم تنزيلها وتعيين الحالة غير محددة لها فقط بعد أن تقوم بتغيير حالتها إلى معتمدة.

يتم تمكين هذا الخيار افتراضيًا.

- **تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة مقدمًا (مستحسن)**

إذا تم تمكين هذا الخيار، فإنه يتم استخدام الوضع "غير متصل بالإنترنت" الخاص بتنزيل التحديثات. عند تلقي خادم الإدارة للتحديثات، يقوم بإخطار عميل الشبكة (على الأجهزة المثبت عليها) بالتحديثات المطلوبة للتطبيقات المُدارة. وعندما يتلقى عميل الشبكة معلومات حول هذه التحديثات، يقوم بتنزيل الملفات ذات الصلة من خادم الإدارة بشكلٍ مسبق. وعند أول اتصال مع عميل الشبكة، يبدأ خادم الإدارة بتنزيل التحديث. بعد أن يقوم عميل الشبكة بتنزيل جميع التحديثات إلى جهاز عميل، تصبح التحديثات متاحة للتطبيقات على هذا الجهاز.

عندما يحاول تطبيق مُدار على جهاز عميل الوصول إلى عميل الشبكة للحصول على تحديثات، يقوم عميل الشبكة بالتحقق مما إذا كانت جميع التحديثات المطلوبة متوفرة. إذا تم تلقي التحديثات من خادم الإدارة قبل فترة لا تزيد عن 25 ساعة من طلبها بواسطة تطبيق مُدار، فلن يتصل عميل الشبكة بخادم الإدارة ولكنه سيوفر بدلًا من ذلك تحديثات للتطبيق المُدار من خلال ذاكرة التخزين المؤقت المحلية. وقد يتعذر إنشاء اتصال بخادم الإدارة عند توفير عميل الشبكة لتحديثات للتطبيقات الموجودة على الأجهزة العميلة، إلا إن الاتصال غير مطلوب للتحديث.

إذا تم تعطيل هذا الخيار، فإنه لا يتم استخدام الوضع "غير متصل بالإنترنت" الخاص بتنزيل التحديثات. يتم توزيع التحديثات وفقًا لجدول مهمة تنزيل التحديث.

يتم تمكين هذا الخيار افتراضيًا.

الاتصال

يتضمن القسم **الاتصال** ثلاثة أقسام فرعية متداخلة:

- **الشبكة**
- **ملفات تعريف الاتصال** (لنظام التشغيل Windows وmacOS فقط)
- **جدول الاتصال**

في القسم الفرعي **الشبكة**، يمكنك تكوين الاتصال بخادم الإدارة وتمكين استخدام منفذ UDP وتحديد رقمه. تتوفر الميزات التالية:

- في مجموعة الإعدادات **الاتصال بخادم الإدارة**، يمكنك تكوين الاتصال بخادم الإدارة، وتحديد الفترة الزمنية للمزامنة بين أجهزة العميل وخادم الإدارة:

- **ضغط حركة مرور الشبكة**

إذا تم تمكين هذا الخيار، فستتم زيادة سرعة نقل البيانات بواسطة عميل الشبكة عن طريق تقليل مقدار المعلومات الجاري نقلها والتحميل المنخفض الناتج على خادم الإدارة.

قد يزيد التحميل على وحدة المعالجة المركزية الخاصة بالكمبيوتر العميل.

يتم تمكين خانة الاختيار هذه بشكل افتراضي.

- **فتح منافذ عميل الشبكة في جدار حماية Microsoft Windows**

إذا تم تمكين هذا الخيار، فستتم إضافة المنافذ اللازمة لعمل عميل الشبكة، إلى قائمة استثناء جدار حماية Microsoft Windows.

يتم تمكين هذا الخيار افتراضيًا.

- **استخدام SSL**

في حال تمكين هذا الخيار، يتم إجراء الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL.

يتم تمكين هذا الخيار افتراضيًا.

- **استخدم بوابة الاتصال على نقطة التوزيع (إن كانت متاحة) ضمن إعدادات الاتصال الافتراضية**

إذا تم تمكين هذا الخيار، فسيتم استخدام بوابة الاتصال في نقطة التوزيع بموجب الإعدادات المحددة في خصائص مجموعة الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **استخدام منفذ UDP**

إذا كنت بحاجة إلى عميل الشبكة للاتصال بخادم الإدارة من خلال منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد **رقم منفذ UDP**. يتم تمكين هذا الخيار افتراضيًا. ويكون منفذ UDP الافتراضي للاتصال بخادم الإدارة هو 15000.

- **رقم منفذ UDP**

يمكنك في هذا الحقل إدخال اسم منفذ UDP. رقم المنفذ الافتراضي هو 15000.

تم استخدام النظام العشري للسجلات.

إذا كان الجهاز العميل يعمل بنظام التشغيل Windows XP Service Pack 2، فسوف يقوم جدار الحماية المدمج بمنع منفذ UDP 15000. يجب أن يتم فتح هذا المنفذ يدويًا.

- **استخدم نقطة التوزيع لفرض الاتصال بخادم الإدارة**

حدد هذا الخيار إذا كنت قد حددت خيار **استخدم نقطة التوزيع هذه كخادم إرسال** في نافذة إعدادات نقطة التوزيع. بخلاف ذلك، لن تعمل نقطة التوزيع كخادم إرسال.

في القسم الفرعي **ملفات تعريف الاتصال**، يمكنك تحديد إعدادات موقع الشبكة وتكوين ملفات تعريف الاتصال لخادم الإدارة وتمكين وضع الوجود خارج المكتب عندما لا يكون خادم الإدارة متاحًا.

- **إعدادات موقع الشبكة**

تحدد إعدادات موقع الشبكة سمات الشبكة المتصل بها الجهاز العميل وتحدد قواعد تبديل عميل الشبكة من ملف تعريف اتصال خادم الإدارة إلى آخر عند تغيير سمات الشبكة هذه.

- **ملفات تعريف اتصال خادم الإدارة**

في هذا القسم يمكنك عرض ملفات التعريف وإضافتها لاتصال عميل الشبكة بخادم الإدارة. في هذا القسم، يمكنك أيضًا إنشاء قواعد لتحويل عميل الشبكة إلى خادم إدارة مختلف عند وقوع الأحداث التالية:

  - عند اتصال الجهاز العميل بشبكة محلية مختلفة
  - عندما يفقد الجهاز الاتصال بالشبكة المحلية للمؤسسة
  - عندما يتم تغيير عنوان بوابة الاتصال أو تعديل عنوان خادم DNS

إن ملفات تعريف الاتصال مدعومة فقط للأجهزة التي تعمل بنظام Windows و macOS.

- **تمكين وضع الوجود خارج المكتب عندما يكون خادم الإدارة غير متاح**

في حال تمكين هذا الخيار، وفي حال وجود اتصال عبر ملف التعريف ذلك، ستقوم التطبيقات المثبتة على الجهاز العميل باستخدام ملفات تعريف السياسة للأجهزة التي في وضع الوجود خارج المكتب، بالإضافة إلى سياسات الوجود خارج المكتب. في حالة عدم تحديد سياسة الوجود خارج المكتب للتطبيق، سيتم استخدام السياسة المفعلة.

في حال تعطيل هذا الخيار، ستستخدم التطبيقات السياسات المفعلة.

يتم تعطيل هذا الخيار افتراضيًا.

في القسم الفرعي **جدول الاتصال**، يمكنك تحديد الفواصل الزمنية التي يرسل خلالها عميل الشبكة بيانات إلى خادم الإدارة:

- **الاتصال عند الحاجة**

إذا حددت هذا الخيار، يتم إنشاء الاتصال عندما يتعين على عميل الشبكة إرسال بيانات إلى خادم الإدارة.

يتم تحديد هذا الخيار افتراضيًا.

- **الاتصال في فواصل زمنية محددة**

إذا حددت هذا الخيار، يقوم عميل الشبكة بالاتصال بخادم الإدارة في فترات محددة. ويمكنك إضافة فترات زمنية متعددة للاتصال.

نقاط توزيع

يتضمن القسم **نقاط التوزيع** أربعة أقسام فرعية متداخلة:

- **استقصاء الشبكة**
- **إعدادات الاتصال بالإنترنت**
- **وكيل KSN**
- **تحديثات**

في القسم الفرعي **استقصاء الشبكة**، يمكنك تكوين الاستقصاء التلقائي للشبكة. يمكنك تمكين ثلاثة أنواع من الاستقصاء، أي استقصاء الشبكة، واستقصاء نطاق IP، واستقصاء Active Directory:

- **تمكين استقصاء الشبكة**

إذا تم تمكين الخيار، فإن خادم الإدارة يجري استقصاء الشبكة تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الروابط **تعيين جدول استقصاء سريع** و**تعيين جدول استقصاء كامل**.

إذا تم تعطيل هذا الخيار، يستطلع خادم الإدارة الشبكة مع الفاصل الزمني المحدد في الحقل **معدل استقصاءات الشبكة (بالدقائق)**.

يمكن تكوين الفاصل الزمني لاكتشاف الجهاز لإصدارات عميل الشبكة التي تسبق الإصدار 10.2 في الحقلين **معدل الاستقصاءات من مجالات Windows (دقيقة)** (لاستطلاع سريع لشبكة Windows) و**معدل استقصاءات الشبكة (بالدقائق)** (لاستطلاع كامل لشبكة Windows).

يتم تعطيل هذا الخيار افتراضيًا.

- **تمكين استقصاء نطاق IP**

إذا تم تمكين الخيار، فإن نقطة التوزيع تجري استقصاء نطاقات IP تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الزر **تعيين جدول الاستقصاء**.

إذا تم تعطيل هذا الخيار، فلن تجري نقطة التوزيع استقصاء نطاقات IP.

يمكن تكوين تردد استقصاء نطاق IP لإصدارات عميل الشبكة السابقة لـ 10.2 في الحقل **الفاصل الزمني للاستقصاء (دقيقة)**. يتوفر الحقل إذا تم تمكين الخيار.

يتم تعطيل هذا الخيار افتراضيًا.

- **سيتم تجاهل استخدم استقصاء شبكة لا تتطلب تكوينًا (على النظام الاساسي Linux فقط); نطاقات IP المحددة يدويًا**

إذا تم تمكين هذا الخيار، فستقوم نقطة التوزيع تلقائيًا باستقصاء الشبكة باستخدام أجهزة IPv6 عن طريق شبكات التكوين الصفري (كما يشار إلى شبكة لا تتطلب تكوينًا). في هذه الحالة، يتم تجاهل استقصاء نطاق IP الذي تم تمكينه، لأن نقطة التوزيع تستقصي الشبكة بالكامل.

لبدء استخدام شبكة لا تتطلب تكوينًا، يجب استيفاء الشروط التالية:

- يجب أن تعمل نقطة التوزيع على نظام Linux.
- يجب عليك تثبيت أداة استعراض avahi على نقطة التوزيع.

إذا تم تعطيل هذا الخيار، فإن نقطة التوزيع لا تستقصي الشبكات مع أجهزة IPv6.

يتم تعطيل هذا الخيار افتراضيًا.

- **تمكين استقصاء ActiveDirectory**

إذا تم تمكين الخيار، فإن نقطة التوزيع تجري استقصاء Active Directory تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الرابط **تعيين جدول الاستقصاء**.

إذا تم تعطيل هذا الخيار، فلن يجري خادم الإدارة استقصاء Active Directory.

يمكن تكوين تردد استقصاء Active Directory لإصدارات عميل الشبكة السابقة لـ 10.2 في الحقل **الفاصل الزمني للاستقصاء (دقيقة)**. يكون الحقل متاحًا إذا تم تمكين هذا الخيار.

يتم تعطيل هذا الخيار افتراضيًا.

إذا كانت نقاط التوزيع الخاصة بك تستخدم خادمًا وكيلاً عند الاتصال بالإنترنت، ففي القسم الفرعي **إعدادات الاتصال بالإنترنت**، يمكنك تحديد الإعدادات التالية:

- **استخدام الخادم الوكيل**

في حالة تحديد خانة الاختيار هذه، سيتم استخدام خادم وكيل للإنترنت لتوصيل نقاط التوزيع بخوادم التحديث لدى Kaspersky. وفي حقول الإدخال، يمكنك تكوين اتصال الخادم الوكيل.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **عنوان الخادم الوكيل**

عنوان الخادم الوكيل.

- **رقم المنفذ**

رقم المنفذ المستخدم في الاتصال.

- **تجاوز الخادم الوكيل للعناوين المحلية**

إذا تم تمكين هذا الخيار، فلن يتم استخدام خادم الوكيل للاتصال بالأجهزة على الشبكة المحلية.

يتم تعطيل هذا الخيار افتراضيًا.

- **مصادقة الخادم الوكيل**

إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **اسم المستخدم**

حساب المستخدم الذي من خلاله تم إنشاء اتصال بخادم الوكيل.

- **كلمة المرور**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

في القسم الفرعي **وكيل KSN**، يمكنك تكوين التطبيق لاستخدام نقطة التوزيع لإعادة توجيه طلبات KSN من الأجهزة المُدارة:

- **تمكين وكيل KSN على جانب نقطة التوزيع**

تعمل خدمة وكيل KSN على الجهاز المستخدم كنقطة توزيع. استخدم هذه الميزة لإعادة توزيع حركة مرور البيانات في الشبكة وتحسينها.

ترسل نقطة التوزيع إحصاءات KSN المُدرجة في بيان Kaspersky Security Network إلى Kaspersky.

يتم تعطيل هذا الخيار افتراضيًا. يسري تمكين هذا الخيار فقط في حالة تمكين الخيارين **Use Administration Server as a proxy server** و **I agree to use Kaspersky Security Network** في نافذة خصائص خادم الإدارة.

يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل خادم KSN على هذه العقدة.

- **توجيه طلبات KSN إلى خادم الإدارة**

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المدارة إلى خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **الوصول إلى KSN Cloud/KPSN مباشرة عبر الإنترنت**

تعيد نقطة التوزيع توجيه طلبات KSN من الأجهزة المُدارة إلى KSN Cloud أو KPSN. يتم أيضًا إرسال طلبات KSN – التي تم إنشاؤها على نقطة التوزيع نفسها – مباشرةً إلى KSN Cloud أو PKSN.

لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى KPSN مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KPSN، فقم بتمكين خيار **توجيه طلبات KSN إلى خادم الإدارة** لكل نقطة توزيع.

لا يمكن لنقاط التوزيع التي لديها الإصدار 12 المثبت من Network Agent (أو إصدار أقدم)، الوصول إلى KPSN مباشرةً.

- **منفذ TCP**

رقم منفذ TCP الذي ستستخدمه الأجهزة المُدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

- **استخدام منفذ UDP**

إذا كنت بحاجة إلى عميل الشبكة للاتصال بخادم الإدارة من خلال منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد **رقم منفذ UDP**. يتم تمكين هذا الخيار افتراضيًا. ويكون منفذ UDP الافتراضي للاتصال بخادم الإدارة هو 15000.

في القسم الفرعي **تحديثات**، يمكنك تحديد ما إذا كان يجب على عميل الشبكة تنزيل ملفات مختلفة من خلال تمكين خيار**تنزيل ملفات تفاضلية** أو تعطيله (يتم تمكين هذا الخيار افتراضيًا).

محفوظات المراجعة

في علامة التبويب **سجل المراجعة**، يمكنك عرض محفوظات مراجعات سياسة عميل الشبكة. يمكنك مقارنة المراجعات، وعرض المراجعات، وتنفيذ العمليات المتقدمة، مثل حفظ المراجعات في ملف، والعودة إلى مراجعة ما، وإضافة وتحرير أوصاف للمراجعة.

إدارة حسابات المستخدمين

يوفر هذا القسم معلومات حول حسابات المستخدمين والأدوار التي يتم دعمها بواسطة التطبيق. يحتوي هذا القسم على تعليمات حول كيفية إنشاء حسابات وأدوار لمستخدمي Kaspersky Security Center.

يتيح Kaspersky Security Center إدارة حسابات المستخدمين ومجموعات الحسابات. يدعم التطبيق ثلاثة أنواع من الحسابات:

- حسابات موظفي المؤسسة. يسترد خادم الإدارة بيانات حسابات مستخدمي هذه النطاقات عند استقصاء وحدة تحكم نطاق المؤسسة.
- حسابات المستخدمين المحليين. الحسابات المحلية على الأجهزة المدارة، بالإضافة إلى الحسابات المحلية على الجهاز الذي تم تثبيت خادم الإدارة عليه.
- حسابات المستخدمين الداخليين لتطبيق Kaspersky Security Center. يمكنك إنشاء حسابات للمستخدمين الداخليين. يتم استخدام هذه الحسابات فقط داخل Kaspersky Security Center.

العمل باستخدام حسابات المستخدمين

يتيح Kaspersky Security Center إدارة حسابات المستخدمين ومجموعات الحسابات. يدعم التطبيق نوعين من الحسابات:

- حسابات موظفي المؤسسة. يقوم خادم الإدارة باسترداد بيانات حسابات هؤلاء المستخدمون عند استقصاء شبكة المؤسسة.
- حسابات مستخدمين داخليين. يتم تطبيق تلك الحسابات عند استخدام خوادم إدارة افتراضية. يتم إنشاء واستخدام حسابات المستخدمين الداخليين فقط ضمن Kaspersky Security Center.

يمكنك عرض قائمة حسابات المستخدمين بإحدى الطرق التالية:

- في شجرة وحدة التحكم، انتقل إلى **خيارات متقدمة** ← **حسابات المستخدمين**.
- في شجرة وحدة التحكم، انتقل إلى **الأجهزة المُدارة** ← علامة التبويب **الأجهزة** ← رابط <device name> ← قسم **الجلسات**.
  يعرض القسم **الجلسات** حسابات المستخدمين ذات الجلسات النشطة على الأجهزة التي تعمل بنظام Windows.

يتم عرض قائمة حسابات المستخدم بشكل صحيح إذا تم استيفاء المتطلبات التالية:

- استخدم عميل الشبكة من إصدار خادم الإدارة نفسه أو إصدار أحدث.
- يتم تمكين استقصاء Active Directory لعرض حسابات مستخدمي المجال.
- على الأجهزة المدارة التي تعمل بنظام Windows، تعمل خدمة **الخادم (LanmanServer)**.

يمكنك إجراء الإجراءات التالية على حسابات المستخدمين ومجموعات الحسابات:

- قم بتكوين حقوق المستخدم للوصول إلى ميزات التطبيق باستخدام الأدوار.
- إرسال رسائل إلى المستخدمين بواسطة البريد الإلكتروني والرسائل القصيرة.
- عرض قائمة من الأجهزة المحمولة الخاصة بالمستخدم.
- إصدار الشهادات على الأجهزة المحمولة للمستخدم وتثبيتها.
- عرض قائمة من الشهادات التي تم إصدارها للمستخدم.
- تعطيل المصادقة الثنائية لحساب مستخدم.

إضافة حساب خاص بمستخدم داخلي

لإضافة حساب مستخدم داخلي جديد إلى Kaspersky Security Center:

1. في شجرة وحدة التحكم، افتح مجلد **حسابات المستخدمين**.
   مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.
2. في مساحة العمل، انقر على زر **إضافة مستخدم**.
3. في النافذة **مستخدم جديد** التي تفتح، حدد الإعدادات الخاصة بحساب المستخدم الجديد:

- اسم مستخدم ( )

الرجاء توخي الحذر عند إدخال اسم المستخدم. لن تتمكن من تغييرها بعد حفظ التغييرات.

- **الوصف**
- **الاسم بالكامل**
- **البريد الإلكتروني الرئيسي**
- **الهاتف الرئيسي**

- **كلمة المرور** لاتصال المستخدم بـ Kaspersky Security Center

يجب أن تتوافق كلمة المرور مع القواعد التالية:

- يجب أن يتراوح طول كلمة المرور من 8 إلى 256 حرفًا.
- يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
  - الأحرف الكبيرة (A-Z)
  - الأحرف الصغيرة (a-z)
  - الأعداد (0-9)
  - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار**.

عدد محاولات إدخال كلمة المرور محدود. افتراضيًا، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد المحاولات المسموح به لإدخال كلمة مرور، كما هو موضح في "تغيير عدد محاولات إدخال كلمة المرور المسموح به".

إذا أدخل المستخدم كلمة مرور غير صالحة لعدد المرات المحدد، فسيتم منع الوصول إلى حساب المستخدم لمدة ساعة واحدة. في قائمة حسابات المستخدمين، تكون أيقونة المستخدم ( ) الخاصة بحساب محظور خافتة (غير متاحة). يمكنك إلغاء قفل حساب المستخدم فقط عن طريق تغيير كلمة المرور.

- إذا لزم الأمر، حدد خانة الاختيار **تعطيل الحساب** لمنع المستخدم من الاتصال بالتطبيق. يمكنك تعطيل حساب، على سبيل المثال، إذا رغبت في إنشائه مقدمًا ولكن تريد تفعيله في وقت لاحق.
- حدد خيار **اطلب كلمة المرور عند تعديل إعدادات الحساب** إذا كنت ترغب في تفعيل خانة اختيار إضافية لحماية حساب مستخدم من التعديل غير المصرح به. في حال تمكين هذا الخيار، فإن تعديل إعدادات حساب المستخدم يتطلب تفويضًا للمستخدم مع حق تعديل قوائم التحكم في الوصول للكائن للمجال الوظيفي **الميزات العامة: أذونات المستخدم**.

4. انقر على**موافق**.

يتم عرض حساب المستخدم الذي تم إنشاؤه حديثًا في مساحة عمل المجلد **حسابات المستخدمين**.

تحرير حساب خاص بمستخدم داخلي

قم بما يلي لتحرير حساب مستخدم داخلي في Kaspersky Security Center:

1. في شجرة وحدة التحكم، افتح مجلد **حسابات المستخدمين**.

مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.

2. في مساحة العمل، انقر نقرًا مزدوجًا فوق حساب المستخدم الداخلي الذي تريد تحريره.

3. في نافذة **الخصائص: <user name>** التي تفتح، قم بتغيير إعدادات حساب المستخدم:

- **الوصف**
- **الاسم بالكامل**
- **البريد الإلكتروني الرئيسي**
- **الهاتف الرئيسي**
- **كلمة المرور** لاتصال المستخدم بـ Kaspersky Security Center
  يجب أن تتوافق كلمة المرور مع القواعد التالية:
  - يجب أن يتراوح طول كلمة المرور من 8 إلى 256 حرفًا.
  - يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
    - الأحرف الكبيرة (A-Z)
    - الأحرف الصغيرة (a-z)
    - الأعداد (0-9)
    - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار**.

عدد محاولات إدخال كلمة المرور محدود. افتراضيًا، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد المحاولات المسموح به لإدخال كلمة مرور، كما هو موضح في "تغيير عدد محاولات إدخال كلمة المرور المسموح به".

إذا أدخل المستخدم كلمة مرور غير صالحة لعدد المرات المحدد، فسيتم منع الوصول إلى حساب المستخدم لمدة ساعة واحدة. في قائمة حسابات المستخدمين، تكون أيقونة المستخدم ( ) الخاصة بحساب محظور خافتة (غير متاحة). يمكنك إلغاء قفل حساب المستخدم فقط عن طريق تغيير كلمة المرور.

- إذا لزم الأمر، حدد خانة الاختيار **تعطيل الحساب** لمنع المستخدم من الاتصال بالتطبيق. يمكنك تعطيل حساب، مثلاً بعد ترك الموظف للشركة.
- حدد خيار **اطلب كلمة المرور عند تعديل إعدادات الحساب** إذا كنت ترغب في تفعيل خيار إضافي لحماية حساب مستخدم من التعديل غير المصرح به. في حال تمكين هذا الخيار، فإن تعديل إعدادات حساب المستخدم يتطلب تفويضًا للمستخدم مع حق تعديل قوائم التحكم في الوصول للكائن للمجال الوظيفي **الميزات العامة: أذونات المستخدم**.

4. انقر على**موافق**.

يتم عرض حساب المستخدم الذي تم تحريره في مساحة عمل المجلد **حسابات المستخدمين**.

تغيير عدد محاولات إدخال كلمة المرور المسموح بها

يمكن لمستخدم Kaspersky Security Center إدخال كلمة مرور غير صالحة لعدد محدود من المرات. بعد الوصول إلى الحد الأقصى، يتم حظر حساب المستخدم لمدة ساعة واحدة.

افتراضيًا، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد المحاولات المسموح به لإدخال كلمة مرور، كما هو موضح في هذا القسم.

قم بما يلي لتغيير عدد محاولات إدخال كلمة المرور المسموح بها:

1. افتح سجل النظام الخاص بالجهاز المثبت عليه خادم الإدارة (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** ← **تشغيل**).

2. انتقل إلى المفتاح التالي:

- لأنظمة 32 بت:

ServerFlags\1.0.0.0\1093\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE

- لأنظمة 64 بت:

rFlags\1.0.0.0\1093\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE

3. إذا لم تكن قيمة SrvSplPpcLogonAttempts موجودة، فقم بإنشائها. نوع القيمة هو DWORD.

افتراضيًا، لا يتم إنشاء هذه القيمة بعد تثبيت Kaspersky Security Center.

4. حدد العدد المطلوب من المحاولات في القيمة SrvSplPpcLogonAttempts.

5. انقر فوق **موافق** لحفظ التغييرات.

6. قم بإعادة تشغيل خدمة خادم الإدارة.

تم تغيير الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به.

تكوين التحقق من تميز اسم أحد المستخدمين الداخليين

يمكنك تكوين التحقق من تميز اسم أحد مستخدمي Kaspersky Security Center الداخليين عند إضافة هذا الاسم إلى التطبيق. يمكن تنفيذ التحقق من تميز اسم أحد المستخدمين الداخليين فقط على خادم إدارة افتراضي أو على خادم الإدارة الرئيسي الذي سيتم إنشاء حساب المستخدم لأجله، أو على جميع خوادم الإدارة الافتراضية وعلى خادم الإدارة الرئيسي. بشكل افتراضي، يتم التحقق من تميز اسم أحد المستخدمين الداخليين على جميع خوادم الإدارة الافتراضية وعلى خادم الإدارة الرئيسي.

لتمكين التحقق من تميز اسم أحد المستخدمين الداخليين على خادم إدارة افتراضي أو على خادم الإدارة الرئيسي:

1. افتح سجل النظام الخاص بالجهاز المثبت عليه خادم الإدارة (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** ← **تشغيل**).

2. انتقل إلى الخلية التالية:

- لأنظمة 32 بت:

KLLIM\independent.\core.\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE

- لأنظمة 64 بت:

ndependent.\core.\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE

3. للمفتاح LP_InterUserUniqVsScope (DWORD)، قم بتعيين القيمة 00000001.

0 هو القيمة الافتراضية المحددة لهذا المفتاح.

4. قم بإعادة تشغيل خدمة خادم الإدارة.

سيتم التحقق فقط من تميز الاسم على خادم الإدارة الافتراضي الذي تم إنشاء المستخدم الداخلي عليه، أو على خادم الإدارة الرئيسي إذا تم إنشاء المستخدم الداخلي على خادم الإدارة الرئيسي.

لتمكين التحقق من اسم أحد المستخدمين الداخليين على كل خوادم الإدارة الافتراضية وعلى خادم الإدارة الرئيسي:

1. افتح سجل النظام الخاص بالجهاز المثبت عليه خادم الإدارة (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** ← **تشغيل**).

2. انتقل إلى الخلية التالية:

- لأنظمة 64 بت:

ndependent.\core.\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE

- لأنظمة 32 بت:

KLLIM\independent.\core.\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE

3. للمفتاح LP_InterUserUniqVsScope (DWORD)، قم بتعيين القيمة 00000000.

0 هو القيمة الافتراضية المحددة لهذا المفتاح.

4. قم بإعادة تشغيل خدمة خادم الإدارة.

سيتم تنفيذ عملية التحقق من تميز الاسم على جميع خوادم الإدارة الافتراضية وعلى خادم الإدارة الرئيسي.

إضافة مجموعة أمان

يمكنك إضافة مجموعات أمان (مجموعات مستخدمين)، وإجراء تكوين مرن لوصول المجموعات ومجموعة الأمان إلى ميزات التطبيق المختلفة. يمكن تعيين أسماء لمجموعات الأمان التي تتوافق مع أغراض كل منها. على سبيل المثال، يمكن أو يتوافق الاسم مع مكان تواجد المستخدمين في المكتب أو مع اسم الوحدة التنظيمية للشركة التي ينتمي إليها المستخدمين.

قد ينتمي مستخدم واحد إلى العديد من مجموعات الأمان. من الممكن أن ينتمي حساب مستخدم مُدار بواسطة خادم إدارة افتراضي فقط إلى مجموعات الأمان الخاصة بخادم الإدارة الافتراضي هذا ويكون له حقوق الوصول إلى الخادم الافتراضي فقط.

لإضافة مجموعة أمان:

1. في شجرة وحدة التحكم، حدد المجلد **حسابات المستخدمين**.

مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.

2. انقر على زر **إضافة مجموعة أمان**.

ستفتح نافذة **إضافة مجموعة أمان**.

3. في النافذة **إضافة مجموعة أمان**، في القسم **عام**، حدد اسم المجموعة.

يتعذر أن يزيد اسم المجموعة عن 255 حرف وأن يحتوي على رموز محددة مثل *, <, >, ?, \, :, |. يجب أن يكون اسم المجموعة فريدًا.

يمكنك إدخال وصف المجموعة في حقل الإدخال **الوصف**. ملء الحقل **الوصف** اختياري.

4. انقر على**موافق**.

تظهر مجموعة الأمان التي قمت بإضافتها في المجلد **حسابات المستخدمين** في شجرة وحدة التحكم. يمكنك إضافة مستخدمين للمجموعة التي تم إنشاؤها حديثًا.

إضافة مستخدم إلى مجموعة

لإضافة مستخدم إلى مجموعة:

1. من شجرة وحدة التحكم، حدد المجلد **حسابات المستخدمين**.
   مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.
2. في قائمة مجموعات وحسابات المستخدمين، حدد المجموعة التي تريد إضافة مستخدم لها.
3. في نافذة خصائص المجموعة، حدد القسم **مستخدمو المجموعة** وانقر فوق الزر **إضافة**.
   يتم فتح نافذة تحتوي على قائمة بالمستخدمين.
4. من القائمة، حدد المستخدم الذي ترغب في تضمنه في المجموعة.
5. انقر فوق **موافق**.

يتم إضافة المستخدم إلى المجموعة ويتم عرضه في قائمة مستخدمي المجموعة.

تكوين حقوق الوصول إلى ميزات التطبيق. التحكم في الوصول على أساس الدور

يوفر Kaspersky Security Center تسهيلات للوصول إلى ميزات Kaspersky Security Center أو تطبيقات Kaspersky المُدارة.

يمكنك تكوين حقوق الوصول إلى ميزات التطبيق لمستخدمي Kaspersky Security Center بإحدى الطرق التالية:

- عن طريق تكوين الحقوق لكل مستخدم أو مجموعة من المستخدمين بشكل فردي.
- عن طريق إنشاء أدوار المستخدم القياسية مع مجموعة محددة مسبقًا من الحقوق وتعيين هذه الأدوار للمستخدمين اعتمادًا على مدى نطاق واجباتهم.

دور المستخدم (يُشار إليه أيضًا بالدور) هو مجموعة محددة مسبقًا من حقوق الوصول إلى ميزات Kaspersky Security Center أو تطبيقات Kaspersky المُدارة. يمكن تعيين دور لمستخدم أو مجموعة من المستخدمين.

يهدف تطبيق أدوار المستخدم إلى تبسيط وتقصير الإجراءات الروتينية لتكوين حقوق وصول المستخدمين إلى ميزات التطبيق. يتم تكوين حقوق الوصول ضمن دور ما وفقًا للمهام القياسية ونطاق واجبات المستخدمين.

يمكن تعيين أسماء لأدوار المستخدمين وفقًا لأغراض كل منها. يمكنك إنشاء عدد غير محدود من الأدوار في التطبيق.

يمكنك استخدام أدوار المستخدم المحددة مسبقًا مع مجموعة الحقوق المكونة بالفعل، أو إنشاء أدوار جديدةوتكوين الحقوق المطلوبة بنفسك.

حقوق الوصول إلى ميزات التطبيق

يوضح الجدول أدناه ميزات Kaspersky Security Center مع حقوق الوصول لإدارة المهام والتقارير والإعدادات المرتبطة بها وتنفيذ إجراءات المستخدم المرتبطة.

لتنفيذ إجراءات المستخدم المدرجة في الجدول، يجب أن يكون لدى المستخدم الحق المحدد بجوار الإجراء.

تنطبق حقوق **Read** و**Write** و**Execute** على أي مهمة أو تقرير أو إعداد. بالإضافة إلى هذه الحقوق، يجب أن يكون لدى المستخدم حق **Perform operations on device selections** لإدارة المهام أو التقارير أو الإعدادات في تحديدات الجهاز.

تنتمي جميع المهام والتقارير والإعدادات وحزم التثبيت المفقودة في الجدول إلى المنطقة الوظيفية **General features: Basic functionality**.

حقوق الوصول إلى ميزات التطبيق

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
General features: Management of administration groups	**Write**	• إضافة جهاز إلى مجموعة الإدارة: **Write** • حذف الجهاز من مجموعة الإدارة: **Write** • أضف مجموعة إدارة إلى مجموعة إدارة أخرى: **Write** • حذف مجموعة إدارة من مجموعة إدارة أخرى: **Write**	لا شيء	لا شيء	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
General features: Access objects regardless of their ACLs	Read	الحصول على وصول Read لجميع الكائنات: **Read**	لا شيء	لا شيء	لا شيء
General features: Basic functionality	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• قواعد نقل الجهاز (إنشاء أو تعديل أو حذف) للخادم الافتراضي: **Write, Perform operations on device selections** • احصل على شهادة مخصصة لبروتوكول Mobile (LWNGT): **Read** • تعيين شهادة بروتوكول Mobile (LWNGT) المخصصة: **Write** • احصل على قائمة الشبكة المعرفة من قبل NLA: **Read** • إضافة أو تعديل أو حذف قائمة الشبكة المعرفة من قبل NLA: **Write** • اعرض قائمة مجموعات التحكم في الوصول: **Read** • اعرض سجل أحداث Kaspersky: **Read** • اعرض مفتاح الاسترداد لاستعادة الوصول إلى قرص ثابت تم تشفيره بواسطة BitLocker: **Execute**	• "تنزيل التحديثات إلى مستودع خادم الإدارة" • "تسليم التقارير" • "توزيع حزم التثبيت" • "تثبيت التطبيق عن بُعد على خوادم الإدارة الثانوية"	• "تقرير حالة الحماية" • "تقرير التهديدات" • "تقرير حول الأجهزة الأكثر إصابة" • "تقرير حول حالة قواعد بيانات مكافحة الفيروسات" • "تقرير الأخطاء" • "الإبلاغ عن هجمات الشبكة" • "تقرير موجز عن تطبيقات حماية نظام البريد المثبتة" • "تقرير موجز عن تطبيقات الدفاع المحيطي المثبتة" • "تقرير موجز عن التطبيقات المثبتة" • "تقرير حول مستخدمي الأجهزة المصابة" • "تقرير حول الحوادث" • "تقرير حول الأحداث" • "تقرير حول نشاط نقاط التوزيع" • "تقرير حول خوادم الإدارة الثانوية" • "تقرير حول أحداث التحكم في الجهاز" • "تقرير الثغرات الأمنية" • "تقرير حول التطبيقات المحظورة" • "تقرير حول التحكم في الويب" • "تقرير حول حالة تشفير الأجهزة المُدارة" • "تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة" • "تقرير حول أخطاء تشفير الملف" • "تقرير حول حجب الوصول إلى الملفات المشفرة" • "تقرير حول حقوق الوصول إلى الأجهزة المشفرة" • "تقرير حول أذونات المستخدم الفعالة" • "تقرير حول الحقوق"	لا شيء
General features: Deleted objects	• **Read** • **Write**	• اعرض الكائنات المحذوفة في سلة المحذوفات: **Read** • حذف كائنات من سلة المحذوفات: **Write**	لا شيء	لا شيء	لا شيء
General features: Event processing	• **Delete events** • **Edit event notification settings** • **Edit event logging settings** • **Write**	• تغيير إعدادات تسجيل الأحداث: **Edit event logging settings** • تغيير إعدادات إشعار الأحداث: **Edit event notification settings** • حذف الأحداث: **Delete events**	لا شيء	لا شيء	الإعدادات: • إعدادات تفشي الفيروسات: عدد عمليات كشف الفيروسات المطلوبة لإنشاء حدث اندلاع فيروسات • إعدادات تفشي الفيروسات: فترة

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
					زمنية لتقييم عمليات كشف الفيروسات • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة البيانات • فترة زمنية لتخزين الأحداث من الأجهزة المحذوفة
General features: Operations on Administration Server	• Read • Write • Execute • Modify object ACLs • Perform operations on device selections	• حدد منافذ خادم الإدارة لاتصال عميل الشبكة: **Write** • حدد منافذ وكيل التنشيط الذي تم تشغيله على خادم الإدارة: **Write** • حدد منافذ وكيل التفعيل للجوال التي تم تشغيلها على خادم الإدارة: **Write** • حدد منافذ خادم الويب لتوزيع الحزم المستقلة: **Write** • حدد منافذ خادم الويب لتوزيع ملفات تعريف MDM: **Write** • حدد منافذ SSL لخادم الإدارة للاتصال عبر Kaspersky Security Center Web Console: **Write** • حدد منافذ خادم الإدارة لاتصال الهاتف المحمول: **Write** • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة: **Write** • حدد الحد الأقصى لعدد الأحداث التي يمكن أن يرسلها خادم الإدارة: **Write** • حدد الفترة الزمنية التي يمكن خلالها إرسال الأحداث بواسطة خادم الإدارة: **Write**	• "النسخ الاحتياطي لبيانات خادم الإدارة" • "صيانة قاعدة البيانات"	لا شيء	لا شيء
General features: Kaspersky application deployment	• Manage Kaspersky patches • Read • Write • Execute • Perform operations on device selections	اقبل تثبيت التصحيح أو ارفضه: **Manage Kaspersky patches**	لا شيء	• "تقرير حول استخدام مفتاح الترخيص بواسطة خادم الإدارة الافتراضي" • "تقرير حول إصدارات برامج Kaspersky" • "تقرير التطبيقات غير المتوافقة" • "تقرير حول إصدارات تحديثات وحدة برامج Kaspersky" • "تقرير نشر الحماية"	حزمة التثبيت: "Kaspersky"
General features: License key management	• Export key file • Write	• تصدير ملف مفتاح: **Export key file** • تعديل إعدادات مفتاح ترخيص خادم الإدارة: **Write**	لا شيء	لا شيء	لا شيء
General features: Enforced report management	• Read • Write	• إنشاء التقارير بغض النظر عن قوائم ACL الخاصة بهم: **Write** • تنفيذ التقارير بغض النظر عن قوائم ACL الخاصة بهم: **Read**	لا شيء	لا شيء	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
General features: Hierarchy of Administration Servers	Configure hierarchy of Administration Servers	تسجيل خوادم الإدارة الثانوية أو تحديثها أو حذفها: **Configure hierarchy of Administration Servers**	لا شيء	لا شيء	لا شيء
General features: User permissions	Modify object ACLs	• تغيير خصائص "الأمان" لأي كائن: **Modify object ACLs** • إدارة أدوار المستخدم: **Modify object ACLs** • إدارة المستخدمين الداخليين: **Modify object ACLs** • إدارة مجموعات الأمان: **Modify object ACLs** • إدارة الأسماء المستعارة: **Modify object ACLs**	لا شيء	لا شيء	لا شيء
General features: Virtual Administration Servers	• Manage virtual Administration Servers • Read • Write • Execute • Perform operations on device selections	• الحصول على قائمة خوادم الإدارة الافتراضية: **Read** • الحصول على معلومات حول خادم الإدارة الافتراضي: **Read** • إنشاء خادم إدارة افتراضي أو تحديثه أو حذفه: **Manage virtual Administration Servers** • نقل خادم الإدارة الافتراضي إلى مجموعة أخرى: **Manage virtual Administration Servers** • تعيين أذونات خادم الإدارة الافتراضي: **Manage virtual Administration Servers**	لا شيء	"تقرير حول نتائج تثبيت تحديثات برامج الجهات الخارجية"	لا شيء
General features : Encryption Key Management	• Read • Write	• تصدير مفاتيح التشفير: **Read** • استيراد مفاتيح التشفير: **Write**	لا شيء	لا شيء	لا شيء
Mobile Device Management: General	• Connect new devices • Send only information commands to mobile devices • Send commands to mobile devices • Manage certificates • Read • Write	• الحصول على بيانات استعادة خدمة إدارة المفاتيح: **Read** • حذف شهادات المستخدم: **Manage certificates** • الحصول على الجزء العام لشهادة المستخدم: **Read** • تحقق مما إذا تم تمكين البنية الأساسية للمفتاح العام: **Read** • تحقق من حساب البنية التحتية للمفتاح العام: **Read** • احصل على قوالب البنية التحتية للمفتاح العام: **Read** • احصل على قوالب البنية التحتية للمفتاح العام عن طريق شهادة استخدام المفتاح الموسع: **Read** • تحقق مما إذا تم إبطال شهادة البنية التحتية للمفتاح العام: **Read** • تحديث إعدادات إصدار شهادة المستخدم: **Manage certificates** • الحصول على إعدادات إصدار شهادة المستخدم: **Read** • احصل على الحزم حسب اسم المنتج والإصدار: **Read** • تعيين أو إلغاء شهادة المستخدم: **Manage certificates** • تجديد شهادة المستخدم: **Manage certificates** • تعيين علامة شهادة المستخدم: **Manage certificates** • تشغيل إنشاء حزمة تثبيت MDM؛ إلغاء إنشاء حزمة تثبيت MDM: **Connect new devices**	لا شيء	لا شيء	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
System management: Connectivity	• Start RDP sessions • Connect to existing RDP sessions • Initiate tunneling • Save files from devices to the administrator's workstation • Read • Write • Execute • Perform operations on device selections	• إنشاء جلسة مشاركة سطح المكتب: **Start RDP sessions** • إنشاء جلسة RDP: **Connect to existing RDP sessions** • إنشاء نفق: **Initiate tunneling** • حفظ قائمة شبكة المحتوى: **Save files from devices to the administrator's workstation**	لا شيء	"تقرير حول مستخدمي الأجهزة"	لا شيء
System management: Hardware inventory	• Read • Write • Execute • Perform operations on device selections	• الحصول على كائن مخزون الأجهزة أو تصديره: **Read** • إضافة جرد الأجهزة أو تعيينه أو حذفه: **Write**	لا شيء	• "تقرير حول سجل الأجهزة" • "تقرير حول تغييرات التكوين" • "تقرير حول الأجهزة"	لا شيء
System management: Network Access Control	• Read • Write	• عرض إعدادات CISCO: **Read** • تغيير إعدادات CISCO: **Write**	لا شيء	لا شيء	لا شيء
System management: Operating system deployment	• Deploy PXE servers • Read • Write • Execute • Perform operations on device selections	• نشر خادم PXE: **Deploy PXE servers** • عرض قائمة بخوادم PXE: **Read** • بدأ عملية التثبيت على عملاء PXE أو أوقفها: **Execute** • إدارة برامج التشغيل لـ WinPE وصور نظام التشغيل: **Write**	"إنشاء حزمة التثبيت على مرجع صورة نظام التشغيل للجهاز"	لا شيء	حزمة التثبيت: "صورة نظام التشغيل"
System management: Vulnerability and patch management	• Read • Write • Execute • Perform operations on device selections	• عرض خصائص تصحيح الطرف الثالث: **Read** • تغيير خصائص تصحيح الطرف الثالث: **Write**	• "مزامنة Windows Update" • "تثبيت تحديثات Windows Update" • "إصلاح الثغرات الأمنية" • "قم بتثبيت التحديثات المطلوبة وضبط إعدادات مهمة إصلاح الثغرات الأمنية"	"تقرير تحديثات البرامج"	لا شيء
System management: Remote installation	• Read • Write • Execute • Perform operations on device selections	• عرض خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: **Read** • تغيير خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: **Write**	لا شيء	لا شيء	حزم التثبيت: • "تطبيق مخصص " • "حزمة VAPM"
System management: Software inventory	• Read • Write • Execute • Perform operations on device selections	لا شيء	لا شيء	• "تقرير حول التطبيقات المثبتة" • "تاريخ تقرير سجل التطبيقات" • "تقرير حول حالة مجموعات التطبيقات المرخصة" • "تقرير حول مفاتيح ترخيص برامج الجهات الخارجية"	لا شيء

أدوار المستخدم المحددة مسبقًا

توفر أدوار المستخدم المعينة لمستخدمي Kaspersky Security Center مجموعات من حقوق الوصول إلى ميزات التطبيق.

لا يمكن تعيين دور للمستخدمين الذين تم إنشاؤهم على خادم افتراضي على خادم الإدارة.

يمكنك استخدام أدوار المستخدم المحددة مسبقًا المصحوبة بمجموعة من الحقوق المكونة بالفعل، أو إنشاء أدوار جديدة. عند إنشاء دور جديد، يجب عليك تعيين نطاق الدور وتعيين حقوق الوصول إلى ميزات Kaspersky Security Center بنفسك. يمكن ربط بعض أدوار المستخدم المحددة مسبقًا والمتوفرة في Kaspersky Security Center بمناصب وظيفية محددة، على سبيل المثال، **المدقق**، **مسؤول الأمن**، **المشرف** (هذه الأدوار موجودة في Kaspersky Security Center بدءًا من الإصدار 11). تم تكوين حقوق الوصول لهذه الأدوار مسبقًا وفقًا للمهام القياسية ونطاق واجبات الوظائف المرتبطة. يوضح الجدول أدناه كيف يمكن ربط الأدوار يمكن ربط الأدوار بمناصب وظيفية محددة.

أمثلة على أدوار المناصب الوظيفية المحددة

الدور	التعليق
مدقق الحسابات	للسماح بجميع عمليات العرض وتنفيذ أي مهام تم إنشاؤها على مجموعة مختارة من الأجهزة المتصلة بخادم الإدارة عبر وكيل الشبكة مع حقوق المسؤول المحلي (الجذر لنظام Linux). ونوصي بتعيين هذا الدور بعناية لمجموعة محدودة من المستخدمين الذين يحتاجون إليه لأداء واجباتهم الرسمية.
المشرف	يسمح بتنفيذ جميع عمليات العرض، لا يسمح بتنفيذ عمليات أخرى. يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمان تكنولوجيا المعلومات في مؤسستك.
مسؤول الأمن	يسمح بتنفيذ جميع عمليات العرض ويسمح بإدارة التقارير ويمنح أذونات محدودة في **إدارة النظام**: نطاق **الاتصال**. يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمان تكنولوجيا المعلومات في مؤسستك.

يوضح الجدول أدناه حقوق الوصول المعينة لكل دور مستخدم محدد مسبقًا.

حقوق الوصول لأدوار المستخدم المحددة مسبقًا

الدور	الوصف
مسؤول خادم الإدارة	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **معالجة الحدث** • **التسلسل الهرمي لخوادم الإدارة** • **خوادم الإدارة الافتراضية** • **إدارة النظام**: • **الاتصال** • **مخزون الأجهزة** • **مخزون البرنامج** تمنح حقوق **قراءة وكتابة** في منطقة الوظائف **الميزات العامة: إدارة مفتاح التشفير**.

الدور	الوصف
مشغّل خادم الإدارة	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **خوادم الإدارة الافتراضية** • **إدارة النظام**: • **الاتصال** • **مخزون الأجهزة** • **مخزون البرنامج**
مدقق الحسابات	للسماح بجميع العمليات في المجالات الوظيفية ، في **الميزات العامة** : • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **الكائنات المحذوفة** • **إدارة التقارير المفروضة** يمكنك تعيين هذا الدور لشخص يقوم بإجراء تدقيق لمؤسستك.
مسؤول التثبيت	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **نشر برنامج Kaspersky** • **إدارة مفتاح الترخيص** • **إدارة النظام**: • **نشر نظام التشغيل** • **إدارة الثغرات الأمنية والتصحيحات** • **التثبيت عن بُعد** • **مخزون البرنامج** منح حقوق **القراءة والتنفيذ** في **الميزات العامة: المجالات الوظيفية لخوادم الإدارة الافتراضية**.
مشغّل التثبيت	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **نشر برنامج Kaspersky** (يمنح أيضًا **تصحيحات إدارة Kaspersky** مباشرةً في هذه المنطقة) • **خوادم الإدارة الافتراضية** • **إدارة النظام**: • **نشر نظام التشغيل** • **إدارة الثغرات الأمنية والتصحيحات** • **التثبيت عن بُعد** • **مخزون البرنامج**
مسؤول Kaspersky Endpoint Security	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات تمنح حقوق **قراءة وكتابة** في منطقة الوظائف **الميزات العامة: إدارة مفتاح التشفير**.
مشغّل Kaspersky Endpoint Security	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات

الدور	الوصف
المسؤول الرئيسي	يسمح بجميع العمليات في المجالات الوظيفية، باستثناء المجالات التالية، في **الميزات العامة**: • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **إدارة التقارير المفروضة** تمنح حقوق **قراءة وكتابة** في منطقة الوظائف **الميزات العامة: إدارة مفتاح التشفير**.
المشغل الرئيسي	يمنح حقوق **القراءة والتنفيذ** (إن أمكن) في جميع المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **الكائنات المحذوفة** • **العمليات على خادم الإدارة** • **نشر تطبيق Kaspersky** • **خوادم الإدارة الافتراضية** • **إدارة جهاز المحمول: عام** • **إدارة النظام**، بما في ذلك جميع الميزات • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات
إدارة جهاز المحمول	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • **إدارة جهاز المحمول: عام**
مشّغل إدارة جهاز المحمول	يمنح حقوق **القراءة** و**التنفيذ** في **الميزات العامة**: المجالات الوظيفية**للوظائف الأساسية**. يمنح **قراءة** و**إرسال أوامر المعلومات فقط إلى الأجهزة المحمولة** في المجال الوظيفي **إدارة جهاز المحمول: عام**.
مسؤول الأمن	يسمح بجميع العمليات في المجالات الوظيفية التالية، في **الميزات العامة**: • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **إدارة التقارير المفروضة** تمنح **قراءة** و**كتابة** و**تنفيذ** و**حفظ الملفات من الأجهزة على محطة عمل المسؤول** و**تنفيذ العمليات على حقوق تحديدات الأجهزة** في منطقة الوظائف **إدارة النظام: الاتصال**. يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمان تكنولوجيا المعلومات في مؤسستك.
مستخدم Self Service Portal	يسمح بجميع العمليات في **إدارة جهاز المحمول: المجالات الوظيفية لـ Self Service Portal**. هذه الميزة غير مدعومة في Kaspersky Security Center 11 والإصدار الأحدث.
المشرف	يمنح حق **القراءة** في **الميزات العامة**: **الوصول إلى الكائنات، بغض النظر عن قوائم التحكم في الوصول ACLs** و**الميزات العامة**: المجالات الوظيفية **لإدارة التقارير المفروضة**. يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمان تكنولوجيا المعلومات في مؤسستك.
مسؤول إدارة الثغرات الأمنية والتصحيحات	يسمح بجميع العمليات في **الميزات العامة**: المجالات الوظيفية **للوظائف الأساسية** و**إدارة النظام** (بما في ذلك جميع الميزات).
مشغّل إدارة الثغرات الأمنية والتصحيحات	يمنح حقوق **القراءة** و**التنفيذ** (إن أمكن) في **الميزات العامة**: المجالات الوظيفية **للوظائف الأساسية** و**إدارة النظام** (بما في ذلك جميع الميزات).

إضافة دور للمستخدم

إضافة دور المستخدم

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة خصائص خادم الإدارة، في الجزء **الأقسام**، حدد **أدوار المستخدم** وانقر فوق الزر **إضافة**.

يكون القسم **أدوار المستخدم** متاحًا إذا تم تمكين الخيار **عرض أقسام إعدادات الأمان**.

4. من نافذة الخصائص **دور جديد**، قم بتكوين الدور:

- من **الأقسام**، حدد **عام** وقم بتعيين اسم الدور.

  يتعذر أن يكون اسم الدور أكثر من 100 حرف.

- حدد القسم **الحقوق**، وقم بتكوين مجموعة الحقوق من خلال تحديد خانات الاختيار **سماح** و**رفض** المجاورة لميزات التطبيق.

إذا كنت تعمل على خادم الإدارة الرئيسي، يمكنك تفعيل خيار **ترحيل قائمة الأدوار إلى خوادم الإدارة الثانوية**.

5. انقر على**موافق**.

تمت إضافة الدور.

يتم عرض أدوار المستخدم التي تم إنشاؤها لخادم الإدارة في نافذة خصائص خادم الإدارة في القسم **أدوار المستخدم**. يمكنك تعديل أدوار المستخدم وحذفها، وكذلك تعيين أدوار لمجموعات الأمان أو المستخدمين المحددين.

تعيين دور لمستخدم أو لمجموعة أمان

لتعيين دور لمستخدم أو مجموعة من المستخدمين:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة، حدد القسم **الأمن**.

يتوفر القسم **الأمان** إذا تم تحديد خانة الاختيار **عرض أقسام إعدادات الأمان** في نافذة إعدادات الواجهة.

4. في الحقل **أسماء المجموعات أو المستخدمين**، حدد مستخدمًا أو مجموعة من المستخدمين ترغب في تعيين دور لهم.

   إذا لم يكن المستخدم أو المجموعة موجود في الحقل، يمكنك أضافة المستخدم أو المجموعة بواسطة النقر على الزر **إضافة**.

   عند قيامك بإضافة مستخدم عن طريق النقر على الزر **إضافة**، يمكنك تحديد نوع مصادقة المستخدم (Microsoft Windows أو Kaspersky Security Center). يتم استخدام مصادقة Kaspersky Security Center لتحديد حسابات المستخدمين الداخليين التي تستخدم للعمل مع خوادم الإدارة الافتراضية.

5. حدد علامة التبويب **الأدوار** وانقر فوق الزر **إضافة**.

   ستفتح نافذة **أدوار المستخدم**. تُعرض هذه النافذة أدوار المستخدم التي تم إنشاؤها.

6. في نافذة **أدوار المستخدم**، حدد دور لمجموعة الأمان.

7. انقر فوق **موافق**.

سيتم تعيين دور مع مجموعة من الحقوق للعمل مع خادم الإدارة لمستخدم أو مجموعة الأمان. يتم عرض الأدوار التي تم تعيينها في علامة التبويب **الأدوار** في القسم **الأمان** من نافذة خصائص خادم الإدارة.

تعيين أذونات للمستخدمين والمجموعات

يمكنك منح المستخدمين والمجموعات أذونات لاستخدام ميزات مختلفة لخادم الإدارة، ولبرامج Kaspersky التي تتوفر لديك مكونات إضافية للإدارة من أجلها، على سبيل المثال، Kaspersky Endpoint Security for Windows.

قم بما يلي لتعيين الأذونات لمستخدم أو مجموعة من المستخدمين:

1. في شجرة وحدة التحكم، قم بأحد الإجراءات التالية:

- قم بتمديد عقدة **خادم الإدارة** وحدد المجلد الفرعي الذي يحمل اسم خادم الإدارة المطلوب.
- حدد مجموعة الإدارة.

2. في قائمة السياق لخادم الإدارة أو مجموعة الإدارة، حدد **خصائص**.

3. في النافذة خصائص خادم الإدارة (أو النافذة خصائص مجموعة الإدارة) التي تفتح، من الجزء الأيسر **الأقسام**، حدد **الأمن**.

يتوفر القسم **الأمان** إذا تم تحديد خانة الاختيار **عرض أقسام إعدادات الأمان** في نافذة إعدادات الواجهة.

4. في القسم **الأمان**، وفي القائمة **أسماء المجموعات أو المستخدمين**، حدد مستخدم أو مجموعة ما.

5. في قائمة الأذونات في الجزء السفلي من مساحة العمل، على علامة التبويب **الحقوق**، قم بتكوين مجموعة من الحقوق للمستخدم أو المجموعة:

a. انقر فوق علامات الجمع (+) لتوسيع العقد في القائمة والحصول على إمكانية الوصول إلى الأذونات.

b. حدد خانات الاختيار **سماح** و**رفض** الموجودة بجوار الأذونات التي تريدها.

مثال 1: قم بتمديد العقدة **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACL) الخاصة بها** أو العقدة **الكائنات المحذوفة**، وحدد **قراءة**.

مثال 2: قم بتمديد العقدة **الوظائف الأساسية**، وحدد **كتابة**.

6. عند قيامك بتكوين مجموعة الحقوق، انقر فوق **تطبيق**.

سيتم تكوين مجموعة الحقوق للمستخدم أو مجموعة المستخدمين.

يتم تقسيم أذونات خادم الإدارة (أو مجموعة الإدارة) إلى المناطق التالية:

- الميزات العامة:
  - إدارة مجموعات الإدارة
  - الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم
  - الوظائف الأساسية
  - الكائنات المحذوفة
  - معالجة الحدث
  - عمليات يتم إجراؤها لخادم الإدارة (فقط في نافذة خصائص خادم الإدارة)
  - نشر تطبيقات Kaspersky
  - إدارة مفتاح الترخيص
  - إدارة التقارير المفروضة
  - التسلسل الهرمي للخوادم

- حقوق المستخدم
- خوادم الإدارة الافتراضية
- إدارة جهاز المحمول:
  - عام
- إدارة النظام:
  - الاتصال
  - مخزن المكونات المادية
  - التحكم في الوصول إلى الشبكة
  - نشر نظام التشغيل
  - إدارة الثغرات الأمنية والتصحيحات
  - التثبيت عن بُعد
  - مخزون البرنامج

إذا لم يتم اختيار **سماح** ولا **رفض** للإذن، فحينئذ يُعتبر الإذن غير محدد: يتم رفضه إلى حين رفضه صراحة أو السماح به للمستخدم.

تمثل حقوق المستخدم مجموع ما يلي:

- حقوق المستخدم الخاصة به
- حقوق جميع الأدوار التي تم تعيينها لهذا المستخدم
- حقوق جميع عناصر مجموعة الأمان التي ينتمي إليها المستخدم
- حقوق جميع الأدوار التي تم تعيينها لمجموعات الأمان التي ينتمي إليها المستخدم

إذا كان لدى أحد هذه الحقوق على الأقل حالة **رفض** للحصول على الإذن، فعندئذ يتم رفض منح المستخدم هذا الإذن، حتى إذا سمحت به المجموعات الأخرى أو تركته غير محدد.

نشر أدوار المستخدم على خوادم الإدارة الثانوية

بشكلٍ افتراضي، تكون قوائم أدوار المستخدم الخاصة بخوادم الإدارة الأساسية والتابعة مستقلة. يمكنك تكوين التطبيق ليقوم تلقائيًا بنشر أدوار المستخدم التي تم إنشاؤها على خادم الإدارة الرئيسي لجميع خوادم الإدارة الثانوية. يمكن أيضًا نشر أدوار المستخدم من خادم إدارة تابع إلى خوادم الإدارة الثانوية الخاصة به.

قم بما يلي لنشر أدوار المستخدم من خادم الإدارة الرئيسي إلى خوادم الإدارة الثانوية:

1. افتح نافذة التطبيق الرئيسية.
2. قم بأحد الإجراءات التالية:
   - في شجرة وحدة التحكم، انقر بزر الماوس الأيمن فوق اسم خادم الإدارة وحدد **خصائص** في قائمة السياق.
   - إذا كانت لديك سياسة خادم إدارة نشطة، في مساحة العمل للمجلد **السياسات**، انقر بزر الماوس الأيمن فوق هذه السياسة وحدد **خصائص** في قائمة السياق.

3. في النافذة خصائص خادم الإدارة، أو في النافذة إعدادات السياسة، في الجزء **الأقسام**، حدد **أدوار المستخدم**.

> يكون القسم **أدوار المستخدم** متاحًا إذا تم تمكين الخيار **عرض أقسام إعدادات الأمان**.

4. قم بتمكين الخيار **ترحيل قائمة الأدوار إلى خوادم الإدارة الثانوية**.

5. انقر فوق **موافق**.

يقوم التطبيق بنسخ أدوار المستخدم لخادم الإدارة الرئيسي إلى خوادم الإدارة الثانوية.

عندما يتم تمكين الخيار **ترحيل قائمة الأدوار إلى خوادم الإدارة الثانوية** ويتم نشر أدوار المستخدم، لا يمكن تحريرها أو حذفها على خوادم الإدارة الثانوية. عند قيامك بإنشاء دور جديد أو تحرير دور موجود بالفعل على خادم الإدارة الرئيسي، يتم نسخ التغييرات تلقائيًا إلى خوادم الإدارة الثانوية. عند قيامك بحذف دور مستخدم على خادم الإدارة الرئيسي، يظل هذا الدور على خوادم الإدارة الثانوية بعد ذلك، ولكن يمكن تحريره أو حذفه.

يتم عرض الأدوار التي يتم نشرها إلى خادم الإدارة الثانوي من الخادم الرئيسي مع ظهور أيقونة "القفل" (🔒). لا يمكنك تحرير هذه الأدوار على خادم الإدارة الثانوي.

إذا قمت بإنشاء دور على خادم الإدارة الرئيسي، وهناك دور بنفس الاسم على خادم الإدارة الثانوي له، فإنه يتم نسخ الدور الجديد إلى خادم الإدارة الثانوي مع إضافة الفهرس إلى اسمه، على سبيل المثال، ~~1، ~~2 (يمكن أن يكون المؤشر عشوائيًا).

إذا قمت بتعطيل خيار **ترحيل قائمة الأدوار إلى خوادم الإدارة الثانوية**، فإن جميع أدوار المستخدم الأخرى تظل موجودة على خوادم الإدارة الثانوية، ولكنها تصبح مستقلة عن تلك الأدوار الموجودة على خادم الإدارة الرئيسي. بعد أن تصبح أدوار المستخدم مستقلة، يمكن تحرير أو حذف أدوار المستخدم الموجودة على خوادم الإدارة الثانوية.

تعيين المستخدم كمالك للجهاز

يمكنك تحديد المستخدم كمالك للجهاز لتخصيص جهاز لهذا المستخدم. إذا كان يجب تنفيذ بعض الإجراءات على الجهاز (على سبيل المثال، ترقية الأجهزة)، فيمكن للمسؤول إخطار مالك الجهاز للسماح بتلك الإجراءات.

لتحديد مستخدم كمالك للجهاز:

1. في شجرة وحدة التحكم، افتح المجلد **الأجهزة المُدارة**.

2. في مساحة عمل المجلد، في علامة التبويب **الأجهزة**، حدد الجهاز الذي يلزم تحديد مالك له.

3. في قائمة السياق الخاصة بالجهاز، حدد **خصائص**.

4. في نافذة خصائص السياسة، حدد **معلومات النظام** ← **الجلسات**.

5. انقر فوق الزر **تعيين** بجوار الحقل **مالك الجهاز**.

6. في النافذة **تحديد المستخدم**، حدد المستخدم لتعيينه كمالك للجهاز وانقر فوق **موافق**.

7. انقر على**موافق**.

تم تعيين مالك الجهاز. افتراضيًا، يتم ملء الحقل **مالك الجهاز** بقيمة من Active Directory ويتم تحديثه مع كل استقصاء Active Directory. يمكنك عرض قائمة بملاك الجهاز في **تقرير حول مالكي الجهاز**. يمكنك إنشاء تقرير باستخدام معالج نموذج تقرير جديد.

تسليم الرسائل للمستخدمين

لإرسال رسالة إلى مستخدم بواسطة البريد الإلكتروني:

1. في شجرة وحدة التحكم، في المجلد **حسابات المستخدمين**، حدد أحد المستخدمين.
   مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.
2. في قائمة سياق المستخدم، حدد **إخطار عبر البريد الإلكتروني**.
3. قم بملأ الحقول ذات الصلة في النافذة **إرسال رسالة إلى المستخدم** وانقر فوق الزر **موافق**.

   سيتم إرسال الرسالة إلى عنوان البريد الإلكتروني المحدد في خصائص المستخدم.

لإرسال رسالة SMS إلى مستخدم:

1. في شجرة وحدة التحكم، في المجلد **حسابات المستخدمين**، حدد أحد المستخدمين.
2. في قائمة سياق المستخدم ، حدد **إرسال رسالة نصية قصيرة**.
3. قم بملأ الحقول ذات الصلة في نافذة **نص رسالة SMS** وانقر فوق الزر **موافق**.

   سيتم إرسال الرسالة إلى رقم الجهاز المحمول المحدد في خصائص المستخدم.

عرض قائمة الأجهزة المحمولة للمستخدم

لعرض قائمة بالأجهزة المحمولة للمستخدم

1. في شجرة وحدة التحكم، في المجلد **حسابات المستخدمين**، حدد أحد المستخدمين.
   مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.
2. في قائمة سياق حساب المستخدم، حدد **خصائص**.
3. في نافذة خصائص حساب المستخدم، حدد القسم **الأجهزة المحمولة**.

في القسم **الأجهزة المحمولة**، يمكنك عرض قائمة بالأجهزة المحمولة للمستخدم ومعلومات حول كل منهم. انقر على زر **تصدير إلى ملف** لحفظ قائمة الأجهزة المحمولة في ملف.

تثبيت شهادة لمستخدم

يمكنك تثبيت ثلاثة أنواع من الشهادات لمستخدم:

- شهادة مشتركة، والتي تُطلب لتحديد جهاز محمول المستخدم.
- شهادة البريد، والتي تُطلب لإعداد البريد الخاص بالشركة على جهاز محمول المستخدم.
- شهادة VPN، والتي تُطلب لإعداد الشبكة الخاصة الظاهرية على جهاز محمول المستخدم.

لإصدار شهادة لمستخدم ثم تثبيتها:

1. في شجرة وحدة التحكم، افتح المجلد **حسابات المستخدمين**، وحدد حساب مستخدم.
مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.

2. في قائمة سياق حساب المستخدم، حدد **استيراد شهادة**.

يبدأ معالج تثبيت الشهادة. اتبع إرشادات المعالج.

عقب انتهاء معالج تثبيت الشهادة، سيتم إنشاء الشهادة للمستخدم وتثبيتها. يمكنك عرض قائمة شهادات المستخدم المثبتة وتصديرها إلى ملف.

عرض قائمة الشهادات التي تم إصدارها لمستخدم

لعرض قائمة بجميع الشهادات التي تم إصدارها لمستخدم:

1. في شجرة وحدة التحكم، في المجلد **حسابات المستخدمين**، حدد أحد المستخدمين.
مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.

2. في قائمة سياق حساب المستخدم، حدد **خصائص**.

3. في نافذة خصائص حساب المستخدم، حدد قسم **الشهادات**.

في القسم **الشهادات**، يمكنك عرض قائمة بشهادات المستخدم ومعلومات حول كل منهم. يمكنك النقر فوق الزر **تصدير إلى الملف** لحفظ قائمة الشهادات في ملف.

حول مسؤول خادم الإدارة الافتراضي

يبدأ مسؤول شبكة المؤسسة التي تتم إدارتها عبر خادم إدارة افتراضي بتشغيل Kaspersky Security Center Web Console لعرض تفاصيل الحماية ضد الفيروسات ضمن حساب المستخدم المحدد في هذه النافذة.

إذا لزم الأمر، يمكن إنشاء حسابات مسؤولين متعددة على الخادم الافتراضي.

لا يمكن تعيين دور للمستخدمين الذين تم إنشاؤهم على خادم افتراضي على خادم الإدارة.

مسؤول خادم الإدارة الافتراضي هو مستخدم داخلي لتطبيق Kaspersky Security Center. لا يتم نقل أي بيانات عن المستخدمين الداخليين إلى نظام التشغيل. Kaspersky Security Center يصادق المستخدمين الداخليين.

التثبيت عن بُعد لنظم التشغيل والتطبيقات

يتيح لك Kaspersky Security Center إنشاء صور نظام التشغيل ونشرها على الأجهزة العميلة عبر الشبكة، وجراء تثبيت عن بُعد للتطبيقات بواسطة Kaspersky أو البائعين الآخرين.

لإنشاء صور لأنظمة التشغيل، قم بتثبيت أدوات نشر Windows ADK والوظيفة الإضافية لبيئة Windows PE لأدوات Windows ADK على خادم الإدارة. يمكنك إنشاء صورة لأي إصدار من نظام تشغيل Windows يتوافق مع متطلبات Kaspersky Security Center.

لا يدعم Kaspersky Security Center إصدارات 64 بت من Windows ADK وWindows PE.

التقاط صور لأنظمة التشغيل

يستطيع Kaspersky Security Center التقاط صور نظام التشغيل من الأجهزة ونقل هذه الصور إلى خادم الإدارة. يتم تخزين صور أنظمة التشغيل على خادم الإدارة في مجلد مخصص. يمكن التقاط صورة نظام تشغيل جهاز مرجعي وإنشاؤها عن طريق مهمة إنشاء حزمة التثبيت.

تحتوي وظائف التقاط صور نظام التشغيل على الميزات التالية:

- لا يمكن التقاط صورة نظام التشغيل على جهاز تم تثبيت خادم الإدارة عليه.
- أثناء التقاط صورة نظام التشغيل، تقوم أداة sysprep.exe المساعدة بإعادة تعيين إعدادات الجهاز المرجعي. إذا كنت ترغب في استعادة إعدادات الجهاز المرجعي، حدد خانة الاختيار **إنشاء نسخة احتياطية لحالة الجهاز** في معالج إنشاء مهمة صورة نظام التشغيل.
- تتوفر عملية التقاط الصورة لإعادة تشغيل الجهاز المرجعي.

نشر صور أنظمة التشغيل على الأجهزة الجديدة

يمكنك استخدام الصور التي تم استلامها لنشرها على الأجهزة الجديدة المتصلة بالشبكة التي لم يتم تثبيت نظام تشغيل عليها بعد. يتم استخدام تقنية Preboot eXecution Environment (PXE) في هذه الحالة. لقد حددت جهاز متصل بالشبكة كخادم PXE. يجب أن يفي الجهاز بالمتطلبات التالية:

- يجب تثبيت عميل الشبكة على الجهاز.
- يتعذر تفعيل خادم No DHCP على الجهاز، لأن خادم PXE يستخدم نفس المنافذ التي يستخدمها خادم DHCP.
- يجب ألا يحتوي جزء الشبكة الذي يشتمل على الجهاز على أي خوادم PXE أخرى.

يجب استيفاء الشروط التالية لنشر نظام تشغيل:

- يجب تركيب بطاقة شبكة على الجهاز.
- يجب أن يكون الجهاز متصلاً بالشبكة.
- يجب تحديد خيار تمهيد الشبكة في BIOS عند تمهيد الجهاز.

يتم إجراء نشر نظام التشغيل كما يلي:

1. ينشئ الجهاز العميل اتصالاً بخادم PXE أثناء عملية التمهيد.
2. يبدأ الجهاز العميل التشغيل في بيئة التثبيت المسبق لنظام Windows (WinPE).

> قد يتطلب إضافة الجهاز العميل إلى WinPE تكوين مجموعة برامج التشغيل لـ WinPE.

3. يتم تسجيل الجهاز العميل على خادم الإدارة.

4. يقوم المسؤول بتعيين حزمة تثبيت للجهاز العميل مع صورة نظام التشغيل.

يمكن للمسؤول إضافة برامج تشغيل إلى حزمة التثبيت باستخدام صورة نظام التشغيل. يمكن للمسؤول أيضًا تحديد ملف تكوين يحتوي على إعدادات نظام التشغيل (ملف الإجابة) التي يجب تطبيقها أثناء التثبيت.

5. يتم نشر نظام التشغيل على الجهاز العميل.

يمكن للمسؤول تحديد عناوين MAC للأجهزة العميلة التي لم يتم اتصالها بعد يدويًا، وتعيين حزمة التثبيت التي تحتوي على صورة نظام التشغيل لها. عند اتصال الأجهزة العميلة المحددة بخادم PXE، يتم تثبيت نظام التشغيل على الأجهزة هذه.

نشر صور أنظمة التشغيل على الأجهزة التي تم تثبيت نظام تشغيل آخر عليها بالفعل

يتم إجراء نشر صور أنظمة التشغيل على الأجهزة العميلة التي تم تثبيت نظام تشغيل آخر عليها بالفعل من خلال مهمة التثبيت عن بُعد للأجهزة المحددة.

لاحظ أنه يتم إجراء تثبيت نظيف لنظام التشغيل. وسيتم حذف جميع البيانات.

تثبيت التطبيقات بواسطة Kaspersky والبائعين الآخرين

يمكن للمسؤول إنشاء حزم تثبيت لأي تطبيقات، بما في ذلك التطبيقات المحددة بواسطة المستخدم وتثبيت هذه التطبيقات على الأجهزة العميلة من خلال مهمة التثبيت عن بُعد.

إنشاء صور لأنظمة التشغيل

يتم إنشاء صور أنظمة التشغيل باستخدام مهمة إزالة صورة نظام التشغيل للجهاز المرجعي.

لإنشاء مهمة صناعة صورة نظام التشغيل:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.
2. انقر فوق الزر **إنشاء حزمة التثبيت** لتشغيل معالج الحزمة الجديدة.
3. في نافذة المعالج **تحديد نوع حزمة التثبيت**، انقر فوق الزر **إنشاء حزمة تثبيت مع صورة نظام التشغيل**.
4. اتبع إرشادات المعالج.

عند انتهاء المعالج، يتم إنشاء مهمة خادم إدارة تُسمّى **إنشاء حزمة تثبيت وفقًا لصورة نظام التشغيل للجهاز المرجعي**. يمكنك عرض المهمة في المجلد **المهام**.

عند انتهاء مهمة **إنشاء حزمة تثبيت وفقًا لصورة نظام تشغيل الجهاز المرجعي**، يتم إنشاء حزمة تثبيت التي يمكن استخدامها لنشر نظام التشغيل على الأجهزة العميلة من خلال خادم PXE أو مهمة التثبيت عن بُعد. يمكنك عرض حزمة التثبيت في المجلد **حزم التثبيت**.

تثبيت صور أنظمة التشغيل

يتيح Kaspersky Security Center لك نشر صور WIM الخاصة بسطح المكتب وأنظمة تشغيل ®Windows التي تستند إلى خادم على أجهزة توجد ضمن شبكة مؤسسة ما.

يمكن استخدام الطرق التالية لاسترداد صورة نظام التشغيل التي ينبغي أن تكون قابلة للنشر باستخدام أدوات Kaspersky Security Center:

- الاستيراد من ملف install.wim المُضمن في حزمة توزيع Windows
- التقاط صورة من جهاز مرجعي

يوجد سيناريوهان مدعومان لنشر صورة نظام التشغيل:

- النشر على جهاز "خالي" والذي لا يحتوي على أي نظام تشغيل مثبّت
- النشر على جهاز به نظام تشغيل Windows قيد التشغيل

استخدم بيئة التثبيت المسبق لنظام Windows (Windows PE) لالتقاط صور نظام التشغيل ونشرها. يجب إضافة كل برامج التشغيل المطلوبة لعمل كل الأجهزة المستهدفة بشكل صحيح إلى WinPE. وبشكل عام، يجب إضافة برامج تشغيل محول الشبكة ووحدة التحكم في التخزين.

يجب تحقيق المتطلبات التالية لتطبيق سيناريوهات نشر الصورة والتقاطها:

- يجب تثبيت مجموعة أدوات التثبيت التلقائي لنظام Windows (WAIK) الإصدار 2.0 أو أحدث أو Windows ADK باستخدام الوظيفة الإضافية لبيئة التثبيت المسبق لنظام Windows لنظام Windows ADK على خادم الإدارة. إذا كان السيناريو يسمح بتثبيت صور لـ Windows XP أو التقاطها، فيجب تثبيت WAIK.
- يجب أن يتوفر خادم DHCP على الشبكة حيث يوجد الجهاز المستهدف.
- يجب أن يكون المجلد المشترك الخاص بخادم الإدارة مفتوحًا للقراءة من الشبكة حيث يوجد الجهاز المستهدف. في حالة وجود المجلد المشترك على خادم الإدارة، يتم طلب الوصول لحساب KlPxeUser (يتم إنشاء هذا الحساب تلقائيًا أثناء تشغيل مثبّت خادم الإدارة). في حالة وجود المجلد المشترك خارج خادم الإدارة، يجب منح إمكانية الوصول للجميع.

عند تحديد صورة نظام التشغيل المراد تثبيتها، يجب على المسؤول ضمنيًا تحديد بنية وحدة المعالجة المركزية للجهاز الهدف: x86 أو x86-64.

تكوين عنوان الخادم الوكيل لشبكة KSN

بشكل افتراضي، يتطابق اسم الاتصال أو عنوان IP الخاص بخادم الإدارة مع عنوان خادم وكيل KSN. إذا قمت بتغيير اسم الاتصال أو عنوان IP خادم الإدارة، فيجب عليك تحديد عنوان خادم وكيل KSN الصحيح لتجنب فقدان الاتصال بين الأجهزة المضيفة وKSN.

لتكوين عنوان خادم وكيل KSN:

1. في شجرة وحدة التحكم، انتقل إلى **خيارات متقدمة** ← **التثبيت عن بُعد** ← **حزم التثبيت**.
2. من قائمة سياق **حزم التثبيت**، حدد **خصائص**.
3. في النافذة التي تفتح، حدد عنوان خادم وكيل KSN الجديد في علامة التبويب **عام** .
4. انقر على زر **تطبيق**.

من الآن فصاعدًا، يتم استخدام العنوان المحدد كعنوان خادم وكيل KSN. نوصي بتمكين خيار **استخدام خادم وكيل KSN** لتحسين حركة البيانات على الشبكة.

إضافة برامج تشغيل بيئة التثبيت المسبق من Windows (WinPE)

لإضافة برامج تشغيل بيئة التثبيت المسبق من Windows (WinPE):

1. في المجلد **التثبيت عن بُعد** بشجرة وحدة التحكم، حدد المجلد الفرعي **نشر صور الجهاز**.

2. في مساحة العمل الخاصة بمجلد **نشر صور الجهاز**، انقر على زر **إجراءات إضافية** وحدد **تكوين مجموعة برنامج التشغيل لبيئة التثبيت المسبق لـ Windows (WinPE)** في القائمة المنسدلة.

   ستفتح نافذة **برامج تشغيل بيئة التثبيت المسبق من Windows**.

3. في النافذة **برامج تشغيل بيئة التثبيت المسبق من Windows**، انقر فوق الزر **إضافة**.

   ستفتح نافذة **تحديد برنامج تشغيل**.

4. في النافذة **تحديد برنامج تشغيل**، حدد برنامج تشغيل من القائمة.

   في حالة فقدان برنامج التشغيل الضروري من القائمة، انقر فوق الزر **إضافة** وحدد اسم برنامج التشغيل ومجلد حزمة توزيع برنامج التشغيل في النافذة **إضافة برنامج تشغيل** التي تفتح.

   يمكنك تحديد مجلد عن طريق النقر فوق الزر **استعراض**.

   في النافذة **إضافة برنامج تشغيل**، انقر فوق **موافق**.

5. في نافذة **تحديد برنامج تشغيل**، انقر على**موافق**.

   سيتم إضافة برنامج التشغيل إلى مستودع خادم الإدارة. عند إضافة برنامج التشغيل إلى المستودع، يتم عرضه في النافذة **تحديد برنامج تشغيل**.

6. في نافذة **برامج تشغيل بيئة التثبيت المسبق من Windows**، انقر على زر **موافق**.

   سيتم إضافة برنامج التشغيل إلى بيئة التثبيت المسبق لـ Windows (WinPE).

إضافة برامج تشغيل إلى حزمة تثبيت مع صورة نظام تشغيل

لإضافة برامج تشغيل إلى حزمة تثبيت مع صورة نظام تشغيل:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.

2. من قائمة السياق لحزمة التثبيت ذات صورة نظام التشغيل، حدد **خصائص**.

   يتم فتح نافذة خصائص حزمة التثبيت.

3. في نافذة خصائص حزمة التثبيت، حدد القسم **برامج تشغيل إضافية**.

4. انقر فوق الزر **إضافة** في القسم **برامج تشغيل إضافية**.

   ستفتح نافذة **تحديد برنامج تشغيل**.

5. في النافذة **تحديد برنامج تشغيل** حدد برامج التشغيل التي تريد إضافتها إلى حزمة التثبيت ذات صورة نظام التشغيل.

   يمكنك إضافة برامج تشغيل جديدة إلى مستودع خادم الإدارة عن طريق النقر فوق الزر **إضافة** في النافذة **تحديد برنامج تشغيل**.

6. انقر على**موافق**.

   يتم عرض برامج التشغيل المضافة في القسم **برامج تشغيل إضافية** لنافذة خصائص حزمة التثبيت ذات صورة نظام التشغيل.

تكوين الأداة المساعدة sysprep.exe

تهدف الأداة المساعدة sysrep.exe إلى تجهيز الجهاز لإنشاء صورة نظام التشغيل.

لتكوين الأداة المساعدة sysprep.exe:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.
2. من قائمة السياق لحزمة التثبيت ذات صورة نظام التشغيل، حدد **خصائص**.
   يتم فتح نافذة خصائص حزمة التثبيت.
3. في نافذة خصائص حزمة التثبيت، حدد قسم **إعدادات sysprep.exe**.
4. في القسم **إعدادات sysprep.exe** حدد ملف تكوين سيتم استخدامه أثناء نشر نظام التشغيل على الجهاز العميل:
   - **استخدام ملف التكوين الافتراضي**. حدد هذا الخيار لاستخدام ملف الإجابة الذي تم إنشاؤه بشكل افتراضي أثناء التقاط صورة نظام التشغيل.
   - **تحديد قيم مخصصة للإعدادات الرئيسية**. حدد هذا الخيار لتحديد قيم الإعدادات من خلال واجهة المستخدم.
   - **تحديد ملف تكوين**. حدد هذا الخيار لاستخدام ملف إجابة مخصص.
5. لتطبيق التغييرات التي تم إجراؤها، انقر فوق الزر **تطبيق**.

نشر أنظمة التشغيل على الأجهزة الجديدة المتصلة بالشبكة

لنشر نظام تشغيل على أجهزة جديدة لم تمتلك بعد أي نظام تشغيل مثبت:

1. في المجلد **التثبيت عن بُعد** بشجرة وحدة التحكم، حدد المجلد الفرعي **نشر صور الجهاز**.
   تأكد من تمكين الخيار **عرض إدارة الثغرات الأمنية والتصحيح في النافذة تكوين الواجهة**. وإلا ، فلن يتم عرض مجلد **التثبيت عن بُعد**.
2. انقر على زر **إجراءات إضافية** وحددإدارة **قائمة بخوادم PXE على الشبكة** في القائمة المنسدلة.
   تفتح النافذة **خصائص: نشر صور الجهاز** في القسم **خوادم PXE**.
3. في القسم **خوادم PXE**، انقر فوق الزر **إضافة**، وفي النافذة **خوادم PXE** التي ستفتح، حدد الجهاز الذي سيتم استخدامه كخادم PXE.
   سيتم عرض الجهاز المضاف في قسم خوادم PXE. يتم نقل ملفات WinPE التي تم إنشاؤها إلى الجهاز من خادم الإدارة. وتستغرق عملية نقل الملفات عادةً 10 دقائق. بمجرد اكتمال النقل، تتغير قيمة **الحالة** المعروضة من **جارٍ البدء** إلى **جاهز**.
4. في القسم **خوادم PXE** حدد خادم PXE وانقر فوق الزر **خصائص**.
5. في نافذة خصائص خادم PXE المحدد، على علامة التبويب **إعدادات اتصال خادم PXE**، قم بتكوين اتصال بين خادم الإدارة وخادم PXE.
6. قم بتمهيد الجهاز العميل الذي تريد نشر نظام التشغيل عليه.
7. في BIOS بالجهاز العميل، حدد خيار تثبيت تمهيد الشبكة.
   يتصل الجهاز العميل بخادم PXE ثم يتم عرضه في مساحة عمل المجلد **نشر صور الجهاز**.
8. في قسم **الإجراءات** انقر فوق الرابط **تعيين حزم التثبيت** لتحديد حزمة التثبيت التي سيتم استخدامها لتثبيت نظام التشغيل على الجهاز المحدد.
   استخدم أداة DiskPart على الجهاز المحدد للتحقق من الأقراص المتاحة. وفي موجه أوامر Windows PE، اكتب `diskpart` لفتح أداة DiskPart. اكتب `list disk` لسرد الأقراص.

بعد إضافة الجهاز وتعيين حزمة تثبيت له، يبدأ نشر نظام التشغيل تلقائيًا على هذا الجهاز.

9. لإلغاء نشر نظام تشغيل على الجهاز العميل، انقر فوق الرابط **إلغاء تثبيت صورة نظام التشغيل** في القسم **الإجراءات**.

لإضافة أجهزة بواسطة عناوين MAC,

- في المجلد **نشر صور الجهاز**، انقر فوق **إضافة عنوان MAC للجهاز** لفتح النافذة **جهاز جديد**، وحدد عنوان MAC للجهاز الذي تود إضافته.
- في المجلد **نشر صور الجهاز**، انقر فوق **استيراد عناوين MAC للأجهزة من ملف** لتحديد الملف الذي يحتوي على قائمة بعناوين MAC لجميع الأجهزة التي تريد نشر نظام التشغيل عليها.

نشر أنظمة التشغيل على الأجهزة العميلة

لنشر نظام تشغيل على الأجهزة العميلة المثبت عليها نظام تشغيل آخر بالفعل:

1. في شجرة وحدة التحكم، افتح مجلد **التثبيت عن بُعد** وانقر فوق رابط **نشر حزمة التثبيت على الأجهزة المُدارة (محطات العمل)** لتشغيل معالج نشر الحماية.
2. في نافذة المعالج **تحديد حزمة التثبيت**، حدد حزمة التثبيت بصورة للنظام التشغيل.
3. اتبع إرشادات المعالج.

بعد إنهاء المعالج عملياته، يتم إنشاء مهمة التثبيت عن بُعد لتثبيت نظام التشغيل على الأجهزة العميلة. يمكن بدء المهمة أو إيقافها في المجلد **المهام**.

إنشاء حزم تثبيت التطبيقات

لإنشاء حزمة تثبيت تطبيق:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.
2. انقر فوق الزر **إنشاء حزمة التثبيت** لتشغيل معالج الحزمة الجديدة.
3. في نافذة المعالج **تحديد نوع حزمة التثبيت**، انقر فوق أحد الأزرار التالية:

- **إنشاء حزمة تثبيت لتطبيق Kaspersky**. حدد هذا الخيار إذا كنت ترغب في إنشاء حزمة تثبيت لتطبيق Kaspersky.
- **إنشاء حزمة تثبيت للملف التنفيذي المحدد**. حدد هذا الخيار إذا كنت ترغب في إنشاء حزمة تثبيت لتطبيق جهة خارجية باستخدام ملف تنفيذي. عادةً، يكون الملف التنفيذي ملف إعداد للتطبيق.

- **نسخ المجلد بالكامل إلى حزمة التثبيت**

حدد هذا الخيار إذا كان الملف التنفيذي مصحوبًا بملفات إضافية مطلوبة لتثبيت التطبيق. قبل تمكين هذا الخيار، يُرجى التأكد من أن كل الملفات المطلوبة مخزّنة في المجلد نفسه. وفي حالة تمكين هذا الخيار، يُضيف التطبيق محتويات المجلد بالكامل، بما في ذلك الملف التنفيذي المحدد إلى حزمة التثبيت.

- **حدد معلمات التثبيت**

لضمان نجاح عملية التثبيت عن بُعد، تتطلب معظم التطبيقات إجراء التثبيت في الوضع الصامت. وإذا كان الأمر كذلك، يلزم تحديد المعلمة للتثبيت الصامت.

تكوين إعدادات التثبيت:

- **سطر أوامر الملف التنفيذي**

إذا كان التطبيق يتطلب معلمات إضافية للتثبيت الصامت، فيرجى تحديدها في هذا الحقل. راجع وثائق البائع للاطلاع على التفاصيل.

يمكنك أيضًا إدخال معلمات أخرى.

- **تحويل الإعدادات إلى القيم الموصى بها للتطبيقات التي تم التعرف عليها من قبل Kaspersky Security Center**

  سيتم تثبيت التطبيق من خلال الإعدادات الموصى بها، إذا كانت المعلومات عن التطبيق المحدد مشتملة على قاعدة بيانات Kaspersky.

  إذا أدخلتَ المعلمات في الحقل **سطر أوامر الملف التنفيذي**، تتم إعادة كتابتها باستخدام الإعدادات الموصى بها.

  يتم تمكين هذا الخيار افتراضيًا.

  قام محللو Kaspersky بإنشاء قاعدة بيانات Kaspersky وصيانتها. يحدد محللو Kaspersky إعدادات التثبيت المثلى لكل تطبيق تتم إضافته إلى قاعدة البيانات. يتم تحديد الإعدادات لضمان نجاح عملية التثبيت عن بُعد لتطبيق على الجهاز العميل. يتم تحديث قاعدة البيانات على خادم الإدارة تلقائيًا عند تنفيذ تنزيل التحديثات إلى مستودع مهمة خادم الإدارة.

- **تحديد تطبيق من قاعدة بيانات Kaspersky لإنشاء حزمة تثبيت**. حدد هذا الخيار إذا كنت ترغب في تحديد تطبيق الجهة الخارجية المطلوب من قاعدة بيانات Kaspersky لإنشاء حزمة تثبيت. يتم إنشاء قاعدة البيانات تلقائيًا عند تنفيذ تنزيل التحديثات إلى مستودع مهمة خادم الإدارة، ويتم عرض التطبيقات في القائمة.

- **إنشاء حزمة التثبيت المشتملة على صورة نظام تشغيل**. حدد هذا الخيار إذا كان يجب إنشاء حزمة تثبيت باستخدام صورة نظام تشغيل لجهاز مرجعي.

  عند انتهاء المعالج، يتم إنشاء مهمة خادم إدارة تُسمّى **إنشاء حزمة تثبيت وفقًا لصورة نظام تشغيل الجهاز المرجعي**. عند انتهاء هذه المهمة، يتم إنشاء حزمة تثبيت يمكنك استخدامها لنشر صورة نظام التشغيل من خلال خادم PXE أو مهمة التثبيت عن بُعد.

4. اتبع إرشادات المعالج.

بعد اكتمال إجراءات المعالج، يتم إنشاء حزمة تثبيت يمكن استخدامها لتثبيت التطبيق على الأجهزة العميلة. يمكنك عرض حزمة التثبيت من خلال تحديد **حزم التثبيت** في شجرة وحدة التحكم.

إصدار شهادة لحزم تثبيت التطبيقات

لإصدار شهادة لحزمة تثبيت تطبيق:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.

   إن المجلد **التثبيت عن بُعد** هو مجلد فرعي من المجلد **خيارات متقدمة** بشكل افتراضي.

2. في قائمة السياق للمجلد **حزم التثبيت**، حدد **خيارات متقدمة**.

   يؤدي هذا إلى فتح نافذة خصائص مجلد **حزم التثبيت**.

3. في نافذة خصائص المجلد **حزم التثبيت**، حدد القسم **توقيع الحزم المستقلة**.

4. في القسم **توقيع الحزم المستقلة**، انقر فوق الزر **تحديد**.

   النافذة **الشهادة**.

5. في الحقل **نوع الشهادة**، حدد نوع الشهادة العامة أو الخاصة:

- إذا تم تحديد القيمة **الحاوية PKCS#12**، فحدد ملف الشهادة وكلمة المرور.
- إذا تم تحديد القيمة **الشهادة X.509**:

a. حدد ملف المفتاح الخاص (الملف ذو الامتداد *.prk أو *.pem).

b. حدد كلمة مرور المفتاح الخاص.

c. حدد ملف المفتاح العام (الملف ذو الامتداد *.cer).

6. انقر على**موافق**.

تم إصدار شهادة لحزمة تثبيت التطبيق.

تثبيت التطبيقات على الأجهزة العميلة

لتثبيت تطبيق على الأجهزة العميلة:

1. في شجرة وحدة التحكم، افتح مجلد **التثبيت عن بُعد** وانقر فوق **نشر حزمة التثبيت على الأجهزة المُدارة (محطات العمل)** لتشغيل معالج نشر الحماية.
2. في نافذة المعالج **تحديد حزمة التثبيت**، حدد حزمة تثبيت التطبيق التي تريد تثبيتها.
3. اتبع إرشادات المعالج.

عند اكتمال إجراءات المعالج، يتم إنشاء مهمة التثبيت عن بُعد لتثبيت التطبيق على الأجهزة العميلة. يمكن بدء المهمة أو إيقافها في المجلد **المهام**.

باستخدام معالج نشر الحماية، يمكنك تثبيت عميل الشبكة على الأجهزة العميلة التي تعمل بأنظمة تشغيل Windows وLinux وMacOS.

لإدارة تطبيقات الأمان 64-بت باستخدام Kaspersky Security Center على الأجهزة التي تعمل بأنظمة تشغيل Linux، يجب عليك استخدام عميل شبكة نظام Linux 64-بت. يمكنك تنزيل الإصدار الضروري لعميل الشبكة من موقع الدعم الفني على الويب.

قبل التثبيت عن بُعد لعميل الشبكة على أي جهاز يعمل بنظام Linux، ينبغي عليك إعداد الجهاز.

إدارة مراجعات الكائن

يحتوي هذا القسم على معلومات حول إدارة مراجعات الكائنات. يتيح لك Kaspersky Security Center تتبع تعديل الكائن. في كل مرة تحفظ فيها التغييرات التي أُجريت على الكائن، يتم إنشاء مراجعة. لكل مراجعة رقم.

تشتمل كائنات التطبيق التي تدعم إدارة المراجعة على:

- خصائص خادم الإدارة
- السياسات

- المهام
- مجموعات الإدارة
- حسابات المستخدمين
- حزم التثبيت

يمكنك تنفيذ الإجراءات التالية على مراجعات الكائنات:

- المقارنة بين مراجعة محددة والمراجعة الحالية
- المقارنة بين المراجعات المحددة
- مقارنة كائن بمراجعة محددة لكائن آخر من نفس النوع
- عرض المراجعة المحددة
- التراجع عن التغييرات التي أُجريت على كائن في مراجعة محددة
- حفظ المراجعات في ملف بتنسيق txt.

في نافذة خصائص أي كائن يدعم إدارة المراجعة، يعرض القسم **سجل المراجعة** قائمة مراجعات الكائنات تتضمن التفاصيل التالية:

- رقم مراجعة الكائن
- تاريخ ووقت تعديل الكائن
- اسم المستخدم الذي قام بتعديل الكائن
- الإجراء الذي تم تنفيذه على الكائن
- وصف المراجعة ذات الصلة بالتغيير الذي أُتم إجراؤه على إعدادات الكائن

حول مراجعات الكائن

يمكنك تنفيذ الإجراءات التالية على مراجعات الكائنات:

- المقارنة بين مراجعة محددة والمراجعة الحالية
- المقارنة بين المراجعات المحددة
- مقارنة كائن بمراجعة محددة لكائن آخر من نفس النوع
- عرض المراجعة المحددة
- التراجع عن التغييرات التي أُجريت على كائن في مراجعة محددة
- حفظ المراجعات في ملف بتنسيق txt.

في نافذة خصائص أي كائن يدعم إدارة المراجعة، يعرض القسم **سجل المراجعة** قائمة مراجعات الكائنات تتضمن التفاصيل التالية:

- رقم مراجعة الكائن
- تاريخ ووقت تعديل الكائن
- اسم المستخدم الذي قام بتعديل الكائن
- الإجراء الذي تم تنفيذه على الكائن
- وصف المراجعة ذات الصلة بالتغيير الذي أُتم إجراؤه على إعدادات الكائن

عرض قسم محفوظات المراجعة

يمكنك مقارنة مراجعات كائن بالمراجعة الحالية، أو مقارنة مراجعات مختلفة محددة في القائمة، أو مقارنة كائن بمراجعة كائن آخر من نفس النوع.

لعرض القسم **سجل المراجعة** الخاص بكائن:

1. في شجرة وحدة التحكم، حدد أحد الكائنات التالية:
   - عقدة **خادم الإدارة**
   - **السياسات** المجلد
   - ملف **المهام**
   - مجلد مجموعة إدارة
   - ملف **حسابات المستخدمين**
   - ملف **الكائنات المحذوفة**
   - **حزم التثبيت** المجلد الفرعي، الذي يتداخل في المجلد **التثبيت عن بُعد**
2. بناءً على موقع الكائن ذو الصلة، قم بأحد الإجراءات التالية:
   - إذا كان الكائن في عقدة **خادم الإدارة** أو في عقدة مجموعة الإدارة، انقر بزر الماوس الأيمن فوق العقدة، ومن قائمة السياق حدد **خصائص**.
   - إذا كان الكائن في المجلد **السياسات** أو **المهام** أو **حسابات المستخدمين** أو **الكائنات المحذوفة** أو **حزم التثبيت**، فقم بتحديد المجلد، وحدد الكائن في مساحة العمل المقابلة.

   تفتح نافذة خصائص الكائن.
3. في الجزء الأيسر **الأقسام**، حدد **سجل المراجعة**.

   يتم عرض محفوظات المراجعة في مساحة العمل.

مقارنة مراجعات الكائن

يمكنك مقارنة المراجعات السابقة لكائن بالمراجعة الحالية، أو مقارنة المراجعات المختلفة المحددة في القائمة، أو مقارنة مراجعة كائن بمراجعة كائن آخر من نفس النوع.

لمقارنة مراجعات كائن:

1. حدد كائنًا وانتقل إلى نافذة الخصائص للكائن.

2. في نافذة الخصائص، انتقل إلى القسم **سجل المراجعة**.

3. في مساحة العمل، في قائمة مراجعات الكائنات، حدد المراجعة للمقارنة.
لتحديد أكثر من مراجعة واحدة للكائن، استخدم مفتاحي **Shift** و**Ctrl**.

4. قم بأحد الإجراءات التالية:

- انقر فوق الزر المنقسم **مقارنة** وحدد إحدى القيم الموجودة في القائمة المنسدلة:

  - **مقارنة بالإصدار الحالي**

    حدد هذا الخيار لمقارنة المراجعة المحددة بالمراجعة الحالية.

  - **مقارنة المراجعات المحددة**

    حدد هذا الخيار لمقارنة مراجعتين محددتين.

  - **مقارنة بمهمة أخرى**

    إذا كنت تتعامل مع مراجعات المهام، حدد **مقارنة بمهمة أخرى** لمقارنة المراجعة المحددة بمراجعة مهمة أخرى.
    إذا كنت تتعامل مع مراجعات السياسات، حدد **مقارنة بسياسة أخرى** لمقارنة المراجعة المحددة بمراجعة سياسة أخرى.

- انقر فوق اسم المراجعة نقرًا مزدوجًا، وانقر فوق أحد الأزرار التالية في نافذة خصائص المراجعة التي تفتح:

  - **مقارنة بالحالي&**

    انقر فوق هذا الزر لمقارنة المراجعة المحددة بالمراجعة الحالية.

  - **مقارنة بالسابق&**

    انقر فوق هذا الزر لمقارنة المراجعة المحددة بالمراجعة السابقة.

يتم عرض تقرير بتنسيق HTML عن مقارنة المراجعات في المستعرض الافتراضي.

في هذا التقرير، يمكنك تصغير بعض الأقسام التي تشتمل على إعدادات المراجعات. لتصغير قسم يحتوي على إعدادات مراجعة الكائن، انقر فوق أيقونة السهم (▲) بجوار اسم القسم.

تشتمل مراجعات خادم الإدارة على جميع تفاصيل التغييرات التي أُجريت، باستثناء التفاصيل من النطاقات التالية:

- قسم **حركة المرور**
- قسم **قواعد وضع العلامات**
- قسم **الإخطار**
- قسم **نقاط التوزيع**
- قسم **انتشار الفيروسات**

  لا يتم تسجيل أي معلومات من القسم **انتشار الفيروسات**، حول تكوين تفعيل السياسة والتي تحدث عند تشغيل حدث انتشار الفيروسات.

يمكنك مقارنة مراجعات الكائن المحذوف مع مراجعة الكائن الموجود، وليس العكس: لا يمكنك مقارنة مراجعات الكائن الموجود بمراجعة الكائن المحذوف.

إعداد فترة التخزين لمراجعات الكائن وللمعلومات حول الكائن المحذوف

تكون فترة التخزين لمراجعات الكائن وللمعلومات حول الكائنات المحذوفة نفس المدة. فترة التخزين الافتراضية هي 90 يومًا. هذه الفترة هي فترة كافية للمراجعة المنتظمة للبرنامج.

لا يتمكن إلا المستخدمون الذين يمتلكون الإذن **تعديل** في النطاق **الكائنات المحذوفة** من تغيير فترة التخزين.

لتغيير فترة التخزين لمراجعات الكائن وللمعلومات حول الكائنات المحذوفة:

1. في شجرة وحدة التحكم، حدد خادم الإدارة الذي ترغب في تغيير فترة التخزين له.
2. انقر بزر الماوس الأيمن، وحدد **خصائص** من قائمة السياق.
3. في النافذة خصائص خادم الإدارة التي تفتح، في القسم **مستودع سجل المراجعة**، أدخل فترة التخزين المرغوبة (عدد الأيام).
4. انقر فوق **موافق**.

سيتم تخزين مراجعات الكائن والمعلومات حول الكائنات المحذوفة لعدد الأيام الذي قمت بإدخاله.

عرض مراجعة كائن

إذا كنت بحاجة إلى معرفة التعديلات التي أُجريت على كائن على مدار فترة زمنية معينة، يمكنك عرض مراجعات هذا الكائن.

لعرض مراجعات كائن:

1. تابع إلى القسم **سجل المراجعة** الخاص بالكائن.
2. في قائمة مراجعات الكائن، حدد المراجعة التي تريد عرض إعداداتها.
3. قم بأحد الإجراءات التالية:
   - انقر على زر **عرض المراجعة**.
   - افتح نافذة خصائص المراجعة من خلال النقر المزدوج فوق اسم المراجعة ثم النقر فوق الزر **عرض المراجعة**.

يتم عرض تقرير بتنسيق HTML يحتوي على إعدادات مراجعة الكائن المحدد. في هذا التقرير، يمكنك تصغير بعض الأقسام المشتملة على إعدادات مراجعة الكائن. لتصغير قسم يحتوي على إعدادات مراجعة الكائن، انقر فوق أيقونة السهم (▲) بجوار اسم القسم.

حفظ مراجعة كائن في ملف

يمكنك حفظ مراجعة كائن في ملف نصي، على سبيل المثال، لإرساله عبر البريد الإلكتروني.

لحفظ مراجعة كائن في ملف:

1. تابع إلى القسم **سجل المراجعة** الخاص بالكائن.

2. في قائمة مراجعات الكائن، حدد المراجعة التي يتعين حفظ إعداداتها.

3. انقر على زر **خيارات متقدمة** وحدد قيمة **حفظ في ملف** في القائمة المنسدلة.

يتم حفظ المراجعة الآن في ملف بتنسيق txt.

التراجع عن التغييرات

وإذا لزم الأمر، يمكنك التراجع عن التغييرات التي تم إجراؤها على الكائن. على سبيل المثال، قد يلزمك إعادة إعدادات سياسة إلى حالتها في تاريخ محدد.

للتراجع عن التغييرات التي تم إجراؤها على أحد الكائنات:

1. تابع إلى القسم **سجل المراجعة** الخاص بالكائن.

2. في قائمة مراجعات الكائنات، حدد رقم المراجعة التي تريد التراجع عن التغييرات لها.

3. انقر فوق الزر **خيارات متقدمة** وحدد القيمة **التراجع** في القائمة المنسدلة.

تمت إعادة الكائن حاليًا إلى المراجعة المحددة. تعرض قائمة مراجعات الكائنات سجلًا بالإجراء الذي تم تنفيذه. يعرض وصف المراجعة معلومات حول رقم المراجعة التي قمت بإعادة الكائن إليها.

إضافة وصف للمراجعة

يمكنك إضافة وصف للمراجعة لتبسيط البحث عن المراجعات في القائمة.

لإضافة وصف لمراجعة:

1. تابع إلى القسم **سجل المراجعة** الخاص بالكائن.

2. في قائمة مراجعات الكائنات، حدد المراجعة التي تحتاج إلى إضافة وصف لها.

3. انقر على زر **الوصف**.

4. في النافذة **وصف مراجعة الكائن**، أدخل نصاً لوصف المراجعة.
تكون خانة وصف مراجعة الكائن فارغة بشكل افتراضي.

5. انقر على**موافق**.

حذف الكائنات

يوفر هذا القسم معلومات عن حذف الكائنات.

يمكنك حذف الكائنات، بما يشمل الكائنات التالية:

- السياسات
- المهام
- حزم التثبيت
- خوادم الإدارة الافتراضية
- المستخدمين
- مجموعات الأمان
- مجموعات الإدارة

لحذف كائن:

1. افتح القسم المطلوب من Kaspersky Security Center Web Console، ثم حدد الكائن.
2. في شريط الأدوات، انقر فوق الزر **Delete**.
3. في النافذة التي تفتح انقر على زر **OK** لتأكيد اختيارك.

سيتم حذف الكائن المحدد.

عند قيامك بحذف كائن ما، تظل المعلومات حول هذا الكائن في قاعدة البيانات. تكون فترة تخزين المعلومات حول الكائنات المحذوفة هي نفس فترة التخزين لمراجعات الكائن (الفترة الموصى بها هي 90 يومًا). لا يمكنك تغيير مدّة التخزين إلا في حالة حصولك على إذن **التعديل** في نطاق حقوق **الكائنات المحذوفة**.

حول حذف أجهزة العميل

عندما تحذف جهازًا مُدارًا من مجموعة إدارة، ينقل التطبيق الجهاز إلى مجموعة الأجهزة غير المخصصة. بعد حذف الجهاز، تظل تطبيقات Kaspersky المُثبتة - عميل الشبكة وأي تطبيق أمان، مثل Kaspersky Endpoint Security - على الجهاز.

يتعامل Kaspersky Security Center مع الأجهزة الموجودة في مجموعة الأجهزة غير المخصصة وفقًا للقواعد التالية:

- إذا كونت قواعد نقل الجهاز ولبى الجهاز معايير قاعدة النقل، سيتم نقل الجهاز تلقائيًا إلى مجموعة إدارة وفقًا للقاعدة.
- يتم تخزين الجهاز في مجموعة الأجهزة غير المخصصة وإزالته تلقائيًا من المجموعة وفقًا لقواعد الاحتفاظ بالجهاز .

لا تؤثر قواعد الاحتفاظ بالجهاز على الأجهزة التي تحتوي على محرك أقراص واحد أو أكثر مشفر باستخدام تشفير القرص بالكامل. لا يتم حذف هذه الأجهزة تلقائيًا، يمكنك حذفها يدويًا فقط. إذا كنت بحاجة إلى حذف جهاز يحتوي محرك أقراص مشفر، فقم أولاً بفك تشفير محرك الأقراص، ثم احذف الجهاز.

وعند حذف جهاز يحتوي على محرك أقراص مشفر، يتم أيضًا حذف البيانات المطلوبة لفك تشفير محرك الأقراص. إذا حددت خانة الاختيار **أفهم المخاطر وأريد حذف الجهاز المحدد (الأجهزة المحددة)** في نافذة التأكيد التي تفتح عند حذف هذه الأجهزة (إما من مجموعة **Unassigned devices** أو **Managed Devices**)، فهذا يعني أنك على دراية بحذف البيانات اللاحق.

لفك تشفير محرك الأقراص، يجب استيفاء الشروط التالية:

- تمت إعادة توصيل الجهاز بخادم الإدارة لاستعادة البيانات المطلوبة لفك تشفير محرك الأقراص.
- يتذكر مستخدم الجهاز كلمة مرور فك التشفير.
- لا يزال تطبيق الأمان الذي تم استخدامه لتشفير محرك الأقراص، مثل Kaspersky Endpoint Security for Windows، مُثبتًا على الجهاز.

وفي حالة تشفير محرك الأقراص بواسطة تقنية تشفير القرص من Kaspersky، يمكنك أيضًا محاولة استعادة البيانات باستخدام FDERT Restore Utility.

في VDI، إذا كان لديك جهاز يحتوي على محركات أقراص مشفرة، يتم حذف المعلومات الموجودة على محرك الأقراص المشفر بعد حذف الجهاز.

عندما تحذف جهازًا من مجموعة الأجهزة غير المخصصة يدويًا، يزيل التطبيق الجهاز من القائمة. بعد حذف الجهاز، تظل تطبيقات Kaspersky المُثبتة على الجهاز (إن وجدت). بعد ذلك، إذا كان الجهاز لا يزال مرئيًا لخادم الإدارة وكونت استقصاء شبكة منتظم، يكتشف Kaspersky Security Center الجهاز أثناء استقصاء الشبكة ويضيفه مرة أخرى إلى مجموعة الأجهزة غير المخصصة. لذلك، من المعقول حذف الجهاز يدويًا فقط إذا كان الجهاز غير مرئي لخادم الإدارة.

حذف كائن

يمكنك حذف الكائنات مثل السياسات والمهام وحزم التثبيت والمستخدمين الداخليين ومجموعات الأمان الداخلية إذا كان لديك الإذن تعديل الموجود في فئة حقوق الوظائف الأساسية (ارجع إلى مقالة تعيين أذونات للمستخدمين والمجموعات للحصول على المزيد من المعلومات).

لا يمكنك حذف حزم التثبيت المستخدمة في مهام التثبيت عن بُعد. يجب عليك إيقاف المهام المقابلة أولاً. للمزيد من المعلومات عن مهام التثبيت التلقائي في مجموعة إدارة، راجع المقالة بعنوان التثبيت التلقائي للتطبيقات على الأجهزة الموجودة في مجموعة إدارة.

لحذف كائن:

1. في شجرة وحدة التحكم، في مساحة العمل للمجلد المطلوب وحدد الكائن.
2. قم بأحد الإجراءات التالية:
   - انقر بزر الماوس الأيمن فوق وحدد **حذف**.
   - اضغط على المفتاح **DELETE**.

سيتم حذف الكائن، وتخزين المعلومات حوله في قاعدة البيانات.

عرض معلومات حول الكائنات المحذوفة

يتم حفظ المعلومات حول الكائنات المحذوفة في مجلد الكائنات المحذوفة لنفس المقدار من الوقت لمراجعات الكائن (الفترة الموصي بها 90 يومًا).

يستطيع فقط المستخدمون الذين يمتلكون إذن **قراءة** في نطاق الحقوق **الكائنات المحذوفة** عرض قائمة الكائنات المحذوفة (انظر تعيين أذونات للمستخدمين والمجموعات للحصول على المزيد من المعلومات).

لعرض قائمة الكائنات المحذوفة،

في شجرة وحدة التحكم، حدد **الكائنات المحذوفة** (بشكلٍ افتراضي، تصبح **الكائنات المحذوفة** مجلدًا فرعيًا للمجلد **خيارات متقدمة**).

إذا لم يكن لديك إذن قراءة في نطاق الحقوق **الكائنات المحذوفة**، فسيتم عرض قائمة فارغة في المجلد **الكائنات المحذوفة**.

تحتوي مساحة عمل المجلد **الكائنات المحذوفة** على المعلومات التالية حول الكائنات المحذوفة:

- **الاسم**. اسم الكائن.
- **النوع**. نوع الكائن كالسياسة أو المهمة أو حزمة التثبيت.
- **الوقت**. الوقت عندما تم حذف الكائن.
- **المستخدم** اسم الحساب للمستخدم الذي قام بحذف الكائن.

لعرض المزيد من المعلومات حول الكائن:

1. في شجرة وحدة التحكم، حدد **الكائنات المحذوفة** (بشكلٍ افتراضي، تصبح **الكائنات المحذوفة** مجلدًا فرعيًا للمجلد **خيارات متقدمة**).
2. من مساحة العمل **الكائنات المحذوفة**، حدد الكائن الذي تريده.
   تظهر خانة التعامل مع الكائن المحدد في الجانب الأيمن لمساحة العمل.
3. قم بأحد الإجراءات التالية:
   - انقر فوق الرابط **خصائص** في الخانة.
   - انقر بزر الماوس الأيمن فوق الكائن الذي قمت بتحديده في مساحة العمل، وحدد **خصائص** في قائمة السياق.

   يتم فتح نافذة خصائص الكائن، حيث تعرض علامات التبويب التالية:
   - **عام**
   - **سجل المراجعة**

حذف الكائنات بصورة دائمة من قائمة الكائنات المحذوفة

يستطيع فقط المستخدمون الذين يمتلكون إذن **تعديل** في نطاق الحقوق **الكائنات المحذوفة** حذف الكائنات بصورة دائمة من قائمة الكائنات المحذوفة (انظر تعيين أذونات للمستخدمين والمجموعات للحصول على المزيد من المعلومات).

لحذف كائن من قائمة الكائنات المحذوفة:

1. في شجرة وحدة التحكم، حدد عقدة خادم الإدارة المطلوب ثم حدد المجلد **الكائنات المحذوفة**.
2. من مساحة العمل، حدد الكائن (الكائنات) التي تريد حذفها.
3. قم بأحد الإجراءات التالية:
   - اضغط على المفتاح **DELETE**.
   - من قائمة السياق الخاصة بالكائن (الكائنات) الذي حددته، حدد **حذف**.
4. في مربع الحوار تأكيد، انقر فوق **نعم**.

يتم حذف الكائن بصورة دائمة من قائمة الكائنات المحذوفة. تتم إزالة جميع المعلومات حول هذا الكائن (بما يشمل جميع مراجعاته) بصورة دائمة من قاعدة البيانات. لا يمكنك استعادة هذه المعلومات.

إدارة الأجهزة المحمولة

يتم تنفيذ إدارة حماية الجهاز المحمول من خلال Kaspersky Security Center باستخدام ميزة إدارة الجهاز المحمول، التي تتطلب ترخيصًا مخصصًا. إذا كنت تنوي إدارة الأجهزة المحمولة التي يملكها الموظفون في مؤسستك، فيجب عليك تمكين إدارة جهاز المحمول.

يقدم هذا القسم تعليمات لتمكين إدارة جهاز المحمول وتعطيله وتكوينه. يوضح هذا القسم أيضًا كيفية إدارة الأجهزة المحمولة المتصلة بخادم الإدارة.

للحصول على تفاصيل حول Kaspersky Security for Mobile، راجع تعليمات Kaspersky Security for Mobile.

السيناريو: نشر إدارة الجهاز المحمول

يعرض هذا القسم سيناريو لتكوين ميزة إدارة الأجهزة المحمولة في Kaspersky Security Center.

المتطلبات الأساسية

تأكد من أنك تتمتع بترخيص يمنح الوصول إلى ميزة إدارة جهاز المحمول.

المراحل

يتم تنفيذ عملية نشر ميزة إدارة الأجهزة المحمولة على المراحل التالية:

1. **إعداد المنافذ**

   تأكد من أن المنفذ 13292 متوفر على خادم الإدارة. ويلزم توفير هذا المنفذ للاتصال بالأجهزة المحمولة. كذلك، قد تحتاج إلى التأكد من توفر المنفذ 17100. لا تحتاج إلى هذا المنفذ إلا لخادم وكيل التفعيل الخاص بالأجهزة المحمولة المُدارة، فإذا كانت الأجهزة المحمولة المُدارة تملك صلاحية الوصول إلى الإنترنت، لن تحتاج إلى توفير هذا المنفذ.

2. **تمكين إدارة الجهاز المحمول**

   يمكنك تمكين إدارة الأجهزة المحمولة عند تشغيل معالج البدء السريع لخادم الإدارة أو إصدار أحدث.

3. **تحديد العنوان الخارجي لخادم الإدارة**

   يمكنك تحديد العنوان الخارجي عند تشغيل معالج البدء السريع لخادم الإدارة أو الإصدار الأحدث. وإذا لم تحدد إدارة الجهاز المحمول للتثبيت ولم تحدد العنوان في معالج التثبيت، فحدد العنوان الخارجي في خصائص حزمة التثبيت.

4. **إضافة الأجهزة المحمولة إلى مجموعة الأجهزة المُدارة**

   أضف الأجهزة المحمولة إلى مجموعة الأجهزة المُدارة بحيث يمكنك إدارة هذه الأجهزة من خلال السياسات. ويمكنك إنشاء قاعدة نقل في إحدى خطوات معالج البدء السريع لخادم الإدارة. كما يمكنك إنشاء قاعدة النقل لاحقًا. وإذا لم تحدد هذه القاعدة، يمكنك إضافة الأجهزة المحمولة إلى مجموعة الأجهزة المُدارة يدويًا.

   يمكنك إضافة الأجهزة المحمولة إلى مجموعة الأجهزة المُدارة مباشرة أو يمكنك إنشاء مجموعة فرعية (أو مجموعات فرعية متعددة) لهذه الأجهزة.

   ويمكنك لاحقًا توصيل أي جهاز محمول جديد بخادم الإدارة باستخدام معالج اتصال الجهاز المحمول الجديد.

5. **إنشاء سياسة للأجهزة المحمولة**

   للإدارة الأجهزة المحمولة، أنشئ سياسة (أو سياسات متعددة) لها في المجموعة التي تنتمي لها تلك الأجهزة. ويمكنك تغيير إعدادات هذه السياسة لاحقًا.

النتائج

بعد إكمال السيناريو، يمكنك إدارة الأجهزة التي تعمل بنظام تشغيل Android وiOS باستخدام Kaspersky Security Center. يمكنك العمل مع شهادات الأجهزة المحمولة وإرسال الأوامر إلى الأجهزة المحمولة.

حول سياسة المجموعة لإدارة أجهزة iOS MDM

لإدارة أجهزة iOS MDM، يمكنك استخدام مكون لإدارة الإضافي لـ Kaspersky Device Management for iOS، والمضمن في مجموعة توزيع Kaspersky Security Center. يتيح لك Kaspersky Device Management for iOS إنشاء سياسات المجموعة لتحديد إعدادات تكوين أجهزة iOS MDM دون استخدام أداة تكوين ®iPhone المساعدة.

توفر سياسة مجموعة لإدارة أجهزة iOS MDM الخيارات التالية للمسؤول:

- تكوين إعدادات أمن كلمة مرور الجهاز.
- تكوين قيود على استخدام ميزات الأجهزة للجهاز والقيود على تثبيت وإزالة التطبيقات المحمولة.
- تكوين قيود على استخدام التطبيقات المحمولة المثبتة سابقًا، مثل ™YouTube ®iTunes Store وSafari.
- تكوين قيود على محتوى الوسائط (مثل الأفلام والعروض التليفزيونية) التي تم عرضها حسب المنطقة التي يوجد بها الجهاز.
- تكوين اتصال الجهاز بالإنترنت عبر الخادم الوكيل (وكيل HTTP العام).
- تكوين الحساب الذي يستطيع المستخدم استخدامه للوصول إلى تطبيقات وخدمات الشركة (تقنية تسجيل الدخول الأحادي (SSO)).
- مراقبة استخدام الإنترنت (الزيارات إلى مواقع الويب) على الأجهزة المحمولة.
- تكوين الشبكات اللاسلكية (Wi-Fi)، ونقاط الوصول (APN)، والشبكات الظاهرية الخاصة (VPN) التي تستخدم آليات مصادقة وبروتوكولات شبكة مختلفة.
- تكوين إعدادات الاتصال بأجهزة ®AirPlay لبث الصور والموسيقى والفيديو.
- تكوين إعدادات الاتصال بطابعات ™AirPrint للطباعة اللاسلكية للمستندات من الجهاز.
- تكوين المزامنة مع خادم Microsoft Exchange وحسابات المستخدمين لاستخدام البريد الإلكتروني للشركة على الأجهزة.
- تكوين بيانات اعتماد المستخدم للمزامنة مع خدمة دليل LDAP.
- تكوين بيانات اعتماد المستخدم للاتصال بخدمات CalDAV وCardDAV التي تمكن المستخدمين من الوصول إلى التقويمات وقوائم الاتصال الخاصة بالشركة.
- تكوين إعدادات واجهة iOS، مثل الخطوط أو الرموز لمواقع الويب المفضلة، على جهاز المستخدم.
- إضافة شهادات أمن جديدة على الأجهزة.
- تكوين Simple Certificate Enrollment Protocol (SCEP) لاستعادة الشهادات تلقائيًا بواسطة الجهاز من هيئة إصدار الشهادات.
- إضافة إعدادات مخصصة للعمل باستخدام التطبيقات المحمولة.

تعتبر سياسة إدارة أجهزة iOS MDM خاصة حيث يتم تعيينها لمجموعة إدارة تتضمن خادم iOS MDM (يُشار إليه باسم "خادم الجهاز المحمول"). ويتم تطبيق جميع الإعدادات المحددة في هذه السياسة أولًا على خوادم الأجهزة المحمولة ثم إلى الأجهزة المحمولة المدارة بواسطة تلك الخوادم. في حالة وجود بنية هرمية لمجموعات الإدارة، فإن خوادم الجهاز المحمول التابعة تتلقى إعدادات السياسة من خوادم الأجهزة المحمولة الرئيسية وتقوم بتوزيعها على الأجهزة المحمولة.

للحصول على مزيد من التفاصيل عن كيفية استخدام سياسة المجموعة لإدارة أجهزة iOS MDM في وحدة تحكم إدارة Kaspersky Security Center، يرجى الرجوع إلى مستندات Kaspersky Security for Mobile.

تمكين إدارة الجهاز المحمول

لإدارة الأجهزة المحمولة، يجب عليك تمكين إدارة الجهاز المحمول. إذا لم تقم بتمكين هذه الميزة في معالج البدء السريع، يمكنك تمكينها لاحقًا. تتطلب إدارة الجهاز المحمول وجود رخصة.

يكون تمكين إدارة جهاز المحمول متوفرًا فقط على خادم الإدارة الرئيسي.

لتمكين إدارة جهاز المحمول:

1. في شجرة وحدة التحكم، حدد مجلد **إدارة الجهاز المحمول**.
2. في مساحة عمل المجلد، انقر فوق الزر **تمكين إدارة الجهاز المحمول**. يكون هذا المفتاح متاحًا فقط إذا لم تقم بتمكين **إدارة الجهاز المحمول** من قبل.
   سيتم عرض صفحة **مكونات إضافية** الخاصة بمعالج البدء السريع لخادم الإدارة.
3. حدد **تمكين إدارة الجهاز المحمول** من أجل إدارة الأجهزة المحمولة.
4. في الصفحة **تحديد طريقة تفعيل التطبيقحدد طريقة تفعيل التطبيق**، قم بتفعيل التطبيق باستخدام ملف مفتاح أو رمز التنشيط.
   لن تكون إدارة الأجهزة المحمولة ممكنة ما لم تقوم بتفعيل ميزة إدارة جهاز المحمول.
5. في الصفحة **إعدادات الخادم الوكيل للوصول إلى الإنترنت**، حدد خانة الاختيار **استخدام الخادم الوكيل** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. عند تحديد خانة الاختيار هذه، فستتوفر الحقول لإدخال الإعدادات. حدد إعدادات اتصال الخادم الوكيل.
6. في الصفحة **التحقق من صحة التحديثات للمكونات الإضافية وحزم التثبيت**، حدد أحد الخيارات التالية:

- **التحقق من تحديث المكونات الإضافية وحزم التثبيت**

  بدء تشغيل التحقق من حالة التحديث. إذا اكتشفت عملية التحقق إصدارات قديمة لبعض المكونات الإضافية أو حزم التثبيت، فسيطالبك المعالج بتنزيل الإصدارات لاستبدال الإصدارات القديمة بالحديثة.

- **تخطي التحقق**

  العمل المستمر بدون التحقق من تحديث المكونات الإضافية وحزم التثبيت. يمكنك تحديد هذا الاختيار، على سبيل المثال، إذا لم يتوفر لديك اتصال بالإنترنت أو إذا كنت ترغب في المتابعة بإصدار قديم من التطبيق لسبب من الأسباب.

قد يؤدي تخطي التحقق من تحديثات المكونات الإضافية إلى عدم عمل التطبيق بشكل صحيح.

7. في الصفحة **أحدث إصدارات المكون الإضافي المتوفرة**، قم بتنزيل آخر إصدارات المكونات الإضافية وتثبيتها باللغة التي يطلبها إصدار تطبيقك. لا يتطلب تحديث المكونات الإضافية وجود رخصة.

بعد تثبيتك للمكونات الإضافية وحزم التثبيت، يتحقق التطبيق من تثبيت جميع المكونات الإضافية المطلوبة لتشغيل الأجهزة المحمولة بشكل صحيح. في حالة اكتشاف إصدارات قديمة لبعض المكونات الإضافية، سيطالبك المعالج بتنزيل الإصدارات الحديثة واستبدالها بالقديمة.

8. في الصفحة **إعدادات اتصال الجهاز المحمول**، قم بإعداد منافذ خادم الإدارة.

عند اكتمال المعالج، سيتم إجراء التغييرات التالية:

- سيتم إنشاء سياسة Kaspersky Endpoint Security for Android.
- سيتم إنشاء سياسة Kaspersky Device Management for iOS.
- ستكون المنافذ مفتوحة للأجهزة المحمولة على خادم الإدارة.

تعديل إعدادات إدارة جهاز المحمول

لتمكين دعم الأجهزة المحمولة:

1. في شجرة وحدة التحكم، حدد مجلد **إدارة الجهاز المحمول**.
2. في مساحة عمل المجلد، انقر فوق الرابط **منافذ الاتصال للأجهزة المحمولة**.

سيتم عرض القسم **منافذ إضافية** لنافذة خصائص خادم الإدارة.

3. في القسم **منافذ إضافية**، قم بتعديل الإعدادات ذات الصلة:

- منفذ SSL لخادم وكيل التفعيل
- **فتح منفذ للأجهزة المحمولة**

يفتح منفذ لاتصال الأجهزة المحمولة بخادم الترخيص. يمكنك تحديد رقم المنفذ والإعدادات الأخرى في الحقول الموضحة أدناه.

يتم تمكين هذا الخيار افتراضيًا.

- **منفذ لمزامنة الجهاز المحمول**

رقم المنفذ الذي ستتصل من خلاله الأجهزة المحمولة بخادم الإدارة وستتبادل معه البيانات. رقم المنفذ الافتراضي هو 13292.

يمكنك تخصيص منفذ مختلف إذا تم استخدام المنفذ 13292 لأغراض أخرى.

- **المنفذ الخاص بتفعيل جهاز المحمول**

منفذ اتصال Kaspersky Endpoint Security for Android بخوادم تنشيط Kaspersky.

رقم المنفذ الافتراضي هو 17100.

4. انقر على**موافق**.

تعطيل إدارة جهاز المحمول

يكون تعطيل إدارة جهاز المحمول متوفرًا فقط على خادم الإدارة الرئيسي.

لتعطيل إدارة جهاز المحمول

1. في شجرة وحدة التحكم، حدد مجلد **إدارة الجهاز المحمول**.

2. في مساحة عمل هذا المجلد، انقر فوق الرابط **تكوين مكونات إضافية**.

   سيتم عرض صفحة **مكونات إضافية** الخاصة بمعالج البدء السريع لخادم الإدارة.

3. حدد **عدم تمكين إدارة جهاز المحمول** إذا لم تعد ترغب في إدارة الأجهزة المحمولة بعد الآن.

4. انقر على**موافق**.

سيتعذر على الأجهزة المحمولة المتصلة فيما سبق الاتصال بخادم الإدارة. سيتم إغلاق منفذ اتصال الجهاز المحمول ومنفذ تفعيل الجهاز المحمول تلقائيًا.

لا يتم حذف السياسات التي تم إنشاؤها لـ Kaspersky Endpoint Security for Android و Kaspersky Device Management for iOS. لن يتم تعديل قواعد إصدار الشهادة. لن تتم إزالة المكونات الإضافية التي تم تثبيتها. لن يتم حذف قاعدة نقل الأجهزة المحمولة.

بعد إعادة تمكين إدارة جهاز المحمول على الأجهزة المحمولة المُدارة، قد يتعين عليك إعادة تثبيت التطبيقات المحمولة المطلوبة لإدارة جهاز المحمول.

العمل مع الأوامر للأجهزة المحمولة

يحتوي هذا القسم على معلومات عن الأوامر الخاصة بإدارة الأجهزة المحمولة المدعومة من Kaspersky Security Center. يوفر القسم تعليمات حول كيفية إرسال أوامر إلى الأجهزة المحمولة، وكذلك كيفية عرض الحالات التنفيذية للأوامر في سجل الأوامر.

الأوامر لإدارة الجهاز المحمول

يدعم Kaspersky Security Center أوامر إدارة جهاز المحمول.

تستخدم هذه الأوامر لإدارة جهاز المحمول عن بُعد. على سبيل المثال، في حالة فقدان جهازك المحمول، يمكنك حذف بيانات الشركة من الجهاز عن طريق استخدام أحد الأوامر.

يمكنك استخدام الأوامر لأنواع الأجهزة المحمولة المدارة التالية:

- أجهزة iOS MDM
- أجهزة Kaspersky Endpoint Security (KES)

يدعم نوع كل جهاز مجموعة مخصصة من الأوامر.

اعتبارات خاصة لبعض الأوامر

- لجميع أنواع الأجهزة، إذا تم تنفيذ الأمر **إعادة التعيين إلى إعدادات المصنع** بنجاح، فسيتم حذف جميع البيانات من الجهاز، وسيتم إرجاع إعدادات الجهاز إلى قيم المصنع.
- عقب التنفيذ الناجح للأمر **مسح بيانات الشركة** على جهاز iOS MDM، سيتم إزالة من الجهاز جميع ملفات تعريف التكوين المثبتة وملفات تعريف التزويد وملفات تعريف iOS MDM والتطبيقات التي تم تحديد خانة الاختيار **إزالة مع ملف تعريف iOS MDM** لها.

- إذا تم تنفيذ الأمر **مسح بيانات الشركة** بنجاح على جهاز KES، فسيتم حذف من الجهاز جميع بيانات الشركة والإدخالات في جهات الاتصال ومحفوظات SMS وسجل المكالمات والتقويم وإعدادات الاتصال بالإنترنت وحسابات المستخدمين، باستثناء حساب Google™. بالنسبة لجهاز KES، فسيتم أيضًا حذف جميع البيانات من بطاقة الذاكرة.

- قبل إرسال الأمر **تحديد الموقع** إلى جهاز KES، عليك التأكد من أنك تستخدم هذا الأمر لبحث مصرح به لجهاز مفقود ينتمي إلى مؤسستك أو أحد الموظفون الذين يعملون لديك. جهاز محمول يتلقى أمر **تحديد الموقع** غير مقفل.

قائمة الأوامر للأجهزة المحمولة

الجدول التالي يعرض مجموعة من الأوامر لأجهزة iOS MDM.

الأوامر المدعومة لإدارة الأجهزة المحمولة: أجهزة iOS MDM

الأوامر	نتائج تنفيذ الأمر
قفل	تم قفل الجهاز المحمول.
فتح	تم تعطيل قفل الجهاز المحمول باستخدام PIN. تم إعادة تعيين PIN المحدد سابقًا.
إعادة التعيين إلى إعدادات المصنع	تم حذف جميع البيانات من الجهاز المحمول، وتم استرجاع الإعدادات إلى القيم الافتراضية الخاصة بها.
مسح بيانات الشركة	سيتم إزالة جميع ملفات تعريف التكوين المثبتة وملفات تعريف التزويد وملفات تعريف iOS MDM والتطبيقات التي تم تحديد خانة الاختيار **إزالة مع ملف تعريف iOS MDM** لها من الجهاز.
مزامنة الجهاز	تتم مزامنة بيانات الجهاز المحمول مع خادم الإدارة.
تثبيت ملف التعريف	تم تثبيت ملف تعريف التكوين على الجهاز المحمول.
إزالة ملف التعريف	تم حذف ملف تعريف التكوين من الجهاز المحمول.
تثبيت ملف تعريف التزويد	تم تثبيت ملف تعريف التزويد على الجهاز المحمول.
إزالة ملف تعريف التزويد	تم حذف ملف تعريف التزويد من الجهاز المحمول.
تثبيت التطبيق	تم تثبيت التطبيق على الجهاز المحمول.
إزالة التطبيق	تمت إزالة التطبيق من الجهاز المحمول.
إدخال رمز الاسترداد	رمز الاسترداد الذي تم إدخاله لتطبيق مدفوع.
تكوين التجوال	تم تمكين أو تعطيل تجوال البيانات والتجوال الصوتي.

يعرض الجدول التالي مجموعة من الأوامر لأجهزة KES.

الأوامر المدعومة لإدارة الأجهزة المحمولة: أجهزة KES

الأمر	نتائج تنفيذ الأمر
قفل	تم قفل الجهاز المحمول.
فتح	تم تعطيل قفل الجهاز المحمول باستخدام PIN. تم إعادة تعيين PIN المحدد سابقًا.
إعادة التعيين إلى إعدادات المصنع	تم حذف جميع البيانات من الجهاز المحمول، وتم استرجاع الإعدادات إلى القيم الافتراضية الخاصة بها.
مسح بيانات الشركة	تم حذف بيانات الشركة والإدخالات في جهات الاتصال ومحفوظات SMS وسجل المكالمات والتقويم وإعدادات الاتصال بالإنترنت وحسابات المستخدمين (باستثناء حساب Google). تم مسح بيانات بطاقة الذاكرة.
مزامنة الجهاز	تتم مزامنة بيانات الجهاز المحمول مع خادم الإدارة.
تحديد موقع الجهاز	تم تحديد موقع الجهاز وإظهاره على Google Maps™. يتحمل حامل الجهاز المحمول تكلفة إرسال رسائل SMS وتوفير الاتصال بالإنترنت.
لقطة للوجه	تم قفل الجهاز المحمول. تم التقاط الصورة بواسطة الكاميرا الأمامية للجهاز وحفظها على خادم الإدارة. يمكن عرض الصور في سجل الأمر. يتحمل حامل الجهاز المحمول تكلفة إرسال رسائل SMS وتوفير الاتصال بالإنترنت.
إنذار	يصدر الجهاز المحمول صوت إنذار.

استخدام مراسلة Firebase Cloud

لضمان تسليم الأوامر إلى أجهزة KES التي تتم إدارتها بواسطة نظام تشغيل Android في الوقت المناسب، يستخدم Kaspersky Security Center آلية إرسال الإخطارات. يتم تبادل الإخطارات الفورية بين أجهزة KES وخادم الإدارة من خلال Firebase Cloud Messaging (المشار إليه فيما يلي باسم FCM). في وحدة تحكم إدارة Kaspersky Security Center، يمكنك تحديد إعدادات Firebase Cloud Messaging لتوصيل أجهزة KES بالخدمة.

لاستعادة إعدادات مراسلة Google Firebase Cloud، يجب أن تمتلك حساب.

لتمكين استخدام مراسلة FCM:

1. في وحدة تحكم الإدارة، حدد العقدة **إدارة الجهاز المحمول**، والمجلد **الأجهزة المحمولة**.
2. من قائمة سياق المجلد **الأجهزة المحمولة**، حدد **خصائص**.
3. في خصائص المجلد، حدد القسم **إعدادات Firebase Cloud Messaging**.
4. في الحقل **رقم مشروع Firebase**، حدد معرف مرسل FCM.
5. في الحقل **ملف المفتاح الخاص (بتنسيق JSON)**، حدد ملف المفتاح الخاص.

في المزامنة التالية مع خادم الإدارة، ستتصل أجهزة KES التي تمت إدارتها بواسطة أنظمة التشغيل Android بمراسلة Firebase Cloud.

يمكنك تحرير إعدادات Firebase Cloud Messaging من خلال النقر فوق الزر **إعادة تعيين الإعدادات**.

إرسال أوامر

لإرسال أمر لجهاز محمول المستخدم:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.
2. حدد جهاز محمول المستخدم الذي تحتاج إلى إرسال الأمر إليه.
3. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.
4. في النافذة **أوامر إدارة جهاز المحمول**، انتقل إلى القسم الذي يحمل اسم الأمر الذي تحتاج إلى إرساله إلى الجهاز المحمول، ثم انقر فوق الزر **إرسال أمر**.

   بناءً على الأمر الذي حددته، قد يؤدي النقر فوق الزر **إرسال أمر** إلى فتح نافذة الإعدادات المتقدمة للتطبيق. على سبيل المثال، عندما تقوم بإرسال أمر لحذف ملف تعريف تزويد من جهاز محمول، يطالبك التطبيق بتحديد ملف تعريف التزويد الذي ينبغي حذفه من الجهاز. حدد الإعدادات المتقدمة للأمر في تلك النافذة ثم قم بتأكيد اختيارك. وبعد ذلك، سيتم إرسال الأمر إلى الجهاز المحمول.

   يمكنك النقر فوق الزر **إعادة إرسال** لإرسال الأمر إلى جهاز محمول المستخدم مرة أخرى.

   يمكنك النقر فوق الزر **إزالة من قائمة الانتظار** لإلغاء تنفيذ أمر تم إرساله إذا لم يتم تنفيذ الأمر بعد.

   يعرض القسم **سجل الأمر** الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق **تحديث** لتحديث قائمة الأوامر.
5. انقر فوق **موافق** لإغلاق النافذة **أوامر إدارة جهاز المحمول**.

عرض حالات الأوامر في سجل الأمر.

يقوم التطبيق بحفظ معلومات حول جميع الأوامر التي تم إرسالها إلى الأجهزة المحمولة إلى سجل الأمر. يحتوي سجل الأمر على معلومات حول وقت وتاريخ كل أمر تم إرساله إلى الجهاز المحمول، والحالات الخاصة بهم، والأوصاف التفصيلية لنتائج تنفيذ الأمر. على سبيل المثال، في حالة عدم نجاح تنفيذ أمر، يعرض السجل سبب الخطأ. يتم تخزين السجلات في سجل الأمر لمدة 30 يومًا بحد أقصى.

يمكن أن يكون للأوامر التي تم إرسالها إلى الأجهزة المحمولة الحالات التالية:

- قيد التنفيذ—تم إرسال الأمر إلى الجهاز المحمول.
- اكتمل—تم اكتمال تنفيذ الأمر بنجاح.
- اكتمل مع إرجاع خطأ—فشل تنفيذ الأمر.
- جار الحذف – يتم إزالة الأمر من قائمة انتظار الأوامر التي تم إرسالها إلى الجهاز المحمول.
- تم الحذف – تم إزالة الأمر من قائمة انتظار الأوامر التي تم إرسالها إلى الجهاز المحمول بنجاح.
- خطأ في الحذف – يتعذر إزالة الأمر من قائمة انتظار الأوامر التي تم إرسالها إلى الجهاز المحمول؛

يحتفظ التطبيق بسجل أمر لكل جهاز محمول.

لعرض سجل الأوامر التي تم إرسالها إلى جهاز محمول:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.
   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.
2. في قائمة الأجهزة المحمولة، حدد الجهاز الذي تريد عرض سجل الأمر له.
3. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.
   يتم فتح نافذة **أوامر إدارة جهاز المحمول**. تتوافق الأقسام الخاصة بنافذة **أوامر إدارة جهاز المحمول** مع الأوامر التي يمكن إرسالها إلى الجهاز المحمول.
4. حدد الأقسام التي تحتوي على الأوامر المهمة وقم بعرض معلومات حول كيفية إرسال الأوامر وتنفيذها في القسم **سجل الأمر**.

في القسم **سجل الأمر**، يمكنك عرض قائمة بالأوامر التي تم إرسالها إلى الجهاز المحمول وتفاصيل حول تلك الأوامر. يتيح لك عامل التصفية **إظهار الأوامر** عرض الأوامر بالحالة المحددة فقط في القائمة.

جارٍ العمل بشهادات الأجهزة المحمولة

يحتوي هذا القسم على معلومات حول كيفية العمل مع شهادات الأجهزة المحمولة.

مدة صلاحية شهادة الجذر للأجهزة المحمولة هي 700 يوم بعد إنشائها. ويتم إنشاء الشهادة الاحتياطية قبل 60 يومًا من تاريخ انتهاء الصلاحية. ويمكنك تعديل الفترة الزمنية لإنشاء شهادة احتياطية باستخدام الأمر التالي:

```
timeout > klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v
< in seconds
```

يجب أن تكون الفترة الزمنية لإنشاء شهادة احتياطية طويلة بما يكفي لكي تتم مزامنة جميع الأجهزة المحمولة المدارة مع خادم الإدارة واسترداد الشهادة.

توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Security Center\Lab.

لا يتم دعم التجديد اليدوي لشهادة الجذر للأجهزة المحمولة.

بدء معالج تثبيت الشهادة

يمكنك تثبيت أنواع الشهادات التالية على جهاز محمول المستخدم:

- الشهادات المشتركة لتحديد الجهاز المحمول
- شهادة البريد لتكوين بريد الشركة على الجهاز المحمول
- شهادة VPN لتكوين الوصول إلى شبكة ظاهرية خاصة على الجهاز المحمول

لتثبيت شهادة على جهاز محمول المستخدم:

1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد المجلد الفرعي **الشهادات**.
2. في مساحة عمل مجلد **الشهادات**، انقر فوق رابط **إضافة شهادة** لتشغيل معالج تثبيت الشهادة.

   اتبع إرشادات المعالج.

بعد انتهاء المعالج، سيتم إنشاء شهادة وإضافتها إلى قائمة شهادات المستخدم؛ بالإضافة إلى ذلك، سيتم إرسال إخطار إلى المستخدم لتزويده برابط لتنزيل الشهادة على الجهاز المحمول وتثبيتها. يمكنك عرض قائمة بجميع الشهادات وتصديرها إلى ملف. يمكنك حذف وإعادة إصدار الشهادات، وكذلك عرض الخصائص الخاصة بها.

الخطوة 1. تحديد نوع الشهادة

حدد نوع الشهادة التي يجب تثبيتها على الجهاز المحمول للمستخدم:

- **شهادة المحمول**—لتحديد الجهاز المحمول
- **شهادة البريد**—لتكوين بريد الشركة على الجهاز المحمول
- **شهادة VPN**—لتكوين الوصول إلى شبكة افتراضية خاصة على الجهاز المحمول

الخطوة 2. تحديد نوع الجهاز المحمول

لا تظهر هذه النافذة إلا في حالة قيامك بتحديد **شهادة البريد** أو **شهادة VPN** كنوع الشهادة.

حدد نوع نظام التشغيل الموجود على الجهاز:

- **جهاز iOS MDM**. حدد هذا الخيار إذا كنت مضطرًا لتثبيت شهادة على جهاز محمول متصل بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM باستخدام بروتوكول iOS MDM.
- **جهاز KES مُدار بواسطة Kaspersky Security for Mobile**. حدد هذا الخيار إذا كنت مضطرًا لتثبيت شهادة على جهاز KES. في هذه الحالة، سيتم استخدام الشهادة لتحديد المستخدم عند كل اتصال بخادم الإدارة.
- **جهاز KES متصل بخادم الإدارة بدون مصادقة شهادة المستخدم**. حدد هذا الخيار إذا كنت مضطرًا لتثبيت شهادة على جهاز KES بدون استخدام مصادقة شهادة. في هذه الحالة، في المرحلة الأخيرة من المعالج، في نافذة **طريقة إخطار المستخدم**، يجب على المسؤول تحديد نوع مصادقة المستخدم عند كل اتصال له بخادم الإدارة.

الخطوة 3. تحديد مستخدم

في القائمة، حدد المستخدمين أو مجموعة الأمان أو مجموعة أمان Active Directory التي تحتاج لتثبيت الشهادة لها.

في النافذة **تحديد المستخدم**، يمكنك البحث عن المستخدمين الداخليين لـ Kaspersky Security Center. يمكنك النقر فوق **إضافة** لإضافة مستخدم داخلي.

الخطوة 4. تحديد مصدر الشهادة

في هذه النافذة، يمكنك تحديد مصدر الشهادة الذي سيستخدمه خادم الإدارة لتعريف الجهاز المحمول. يمكنك تحديد شهادة باستخدام إحدى الطرق التالية:

- إنشاء شهادة بشكل تلقائي، بواسطة أدوات خادم الإدارة، ثم تسليم الشهادة إلى الجهاز.
- تحديد ملف شهادة تم إنشاؤه مسبقًا. لا تتوفر هذه الطريقة إذا تم تحديد العديد من المستخدمين في الخطوة السابقة.

حدد خانة الاختيار **نشر شهادة** إذا ما كان ينبغي عليك إرسال إخطار لمستخدم ما حول إنشاء شهادة لجهازه المحمول.

إذا تم تخويل الجهاز المحمول الخاص بالمستخدم في وقت سابق باستخدام شهادة، بحيث لا توجد حاجة للقيام بتحديد اسم حساب وكلمة مرور لاستلام شهادة جديدة، فقم بإلغاء تحديد خانة الاختيار **نشر شهادة**. في هذه الحالة، لن يتم عرض النافذة **طريقة إخطار المستخدم**.

الخطوة 5. تخصيص علامة للشهادة

يتم عرض النافذة **علامة الشهادة** إذا تم تحديد **جهاز iOS MDM** في **نوع الجهاز**.

في القائمة المنسدلة، يمكنك تعيين علامة للشهادة الخاصة بجهاز iOS MDM الخاص بالمستخدم. قد تحتوي الشهادة المعيّن لها علامة على مجموعة معلمات خاصة لهذه العلامة في خصائص سياسة Kaspersky Device Management for iOS.

تطلب منك القائمة المنسدلة تحديد علامة قالب الشهادة 1 أو قالب الشهادة 2 أو قالب الشهادة 3. يمكنك تكوين العلامات في الأقسام التالية:

- في حالة تحديد **شهادة البريد** في النافذة **نوع الشهادة**، فيمكن تكوين علامتها في خصائص حساب Exchange ActiveSync للأجهزة المحمولة (**الأجهزة المُدارة** ← **السياسات**> خصائص سياسة Kaspersky Device Management for iOS← قسم **Exchange ActiveSync** ← **إضافة** ← **متقدم**).
- في حالة تحديد **شهادة VPN** في النافذة **نوع الشهادة**، فيمكن تكوين علامتها في خصائص VPN للأجهزة المحمولة (**الأجهزة المُدارة** ← **السياسات** ← خصائص سياسة Kaspersky Device Management for iOS← قسم **VPN** ← **إضافة** ← **متقدم**). لا يمكنك تكوين العلامات المُستخدمة لشهادات VPN في حالة تحديد نوع الاتصال L2TP أو PPTP أو IPSec (Cisco™) لشبكة VPN الخاصة بك.

الخطوة 6. تحديد إعدادات نشر الشهادة

يمكنك في هذه النافذة تحديد إعدادات نشر الشهادة التالية:

- **لا تقم بإخطار المستخدم بالشهادة الجديدة**

قم بتمكين هذا الخيار إذا كنت لا تريد إرسال إشعار إلى المستخدم حول إنشاء شهادة لجهاز المستخدم المحمول. في هذه الحالة، لن يتم عرض نافذة **طريقة إخطار المستخدم**.

ينطبق هذا الخيار فقط على الأجهزة المثبت عليها Kaspersky Endpoint Security for Android.

ربما ترغب في تمكين هذا الخيار، على سبيل المثال، إذا تم تخويل الجهاز المحمول الخاص بالمستخدم في وقت سابق بالفعل باستخدام شهادة، فليست هناك حاجة لتحديد اسم حساب وكلمة مرور لاستلام شهادة جديدة.

- **السماح للجهاز بامتلاك إيصالات متعددة لشهادة واحدة (فقط للأجهزة المثبّت عليها Kaspersky Endpoint Security for Android)**

قم بتمكين هذا الخيار إذا كنت تريد من Kaspersky Security Center إعادة إرسال الشهادة تلقائيًا في كل مرة توشك فيها أن تنتهي صلاحيتها أو عندما لا يتم العثور عليها على الجهاز المستهدف.

تتم إعادة إرسال الشهادة تلقائيًا قبل عدة أيام من تاريخ انتهاء صلاحية الشهادة. يمكنك تعيين عدد الأيام في النافذة قواعد إصدار الشهادة.

في بعض الحالات، لا يمكن العثور على الشهادة على الجهاز. على سبيل المثال، يمكن أن يحدث هذا عندما يقوم المستخدم بإعادة تثبيت تطبيق أمان Kaspersky على الجهاز أو يعيد تعيين إعدادات الجهاز والبيانات إلى إعدادات المصنع الافتراضية. في هذه الحالة، يتحقق Kaspersky Security Center من معرف الجهاز في المحاولة التالية للجهاز للاتصال بخادم الإدارة. إذا كان للجهاز نفس المعرف الذي كان عليه عند إصدار الشهادة، فإن التطبيق يعيد إرسال الشهادة إلى الجهاز.

الخطوة 7. تحديد طريقة إخطار المستخدم

لا يتم عرض هذه النافذة إذا قمت بتحديد **جهاز iOS MDM** كنوع الجهاز أو إذا قمت بتحديد الخيار **لا تقم بإخطار المستخدم بالشهادة الجديدة**.

في النافذة **طريقة إخطار المستخدم**، يمكنك تكوين إخطار المستخدم حول تثبيت الشهادة على الجهاز المحمول.

في الحقل **وسيلة المصادقة**، حدد نوع مصادقة المستخدم:

- **بيانات الاعتماد (المجال أو الاسم المستعار)**

في هذه الحالة، يستخدم المستخدم كلمة مرور المجال أو كلمة مرور المستخدم الداخلي لـ Kaspersky Security Center لاستلام شهادة جديدة.

- **كلمة مرور لمرة واحدة**

في هذه الحالة، يستلم المستخدم كلمة مرور لمرة واحدة ويتم إرسالها عبر البريد الإلكتروني أو بواسطة رسالة SMS. يجب إدخال كلمة المرور هذه لاستلام شهادة جديدة.

يتغير هذا الخيار إلى **كلمة المرور**، إذا قمت بتمكين (تحديد) خيار **السماح للجهاز بإجراء عدة حالات استقبال لشهادة واحدة (فقط للأجهزة المثبت عليها تطبيقات الأمان من Kaspersky المخصصة للأجهزة المحمولة)** في نافذة **إعدادات نشر الشهادة**.

- **كلمة المرور**

في هذه الحالة، تُستخدم كلمة المرور في كل مرة يتم فيها إرسال الشهادة إلى المستخدم.

يتغير هذا الخيار إلى **كلمة مرور تصلح لمرة واحدة**، إذا قمت بتعطيل (مسح) خيار **السماح للجهاز بإجراء عدة حالات استقبال لشهادة واحدة (فقط للأجهزة المثبت عليها تطبيقات الأمان من Kaspersky المخصصة للأجهزة المحمولة)** في نافذة **إعدادات نشر الشهادة**.

يتم عرض هذا الحقل إذا حددت **شهادة المحمول** في النافذة **نوع الشهادة** أو إذا حددت **جهاز KES متصل بخادم الإدارة بدون مصادقة شهادة المستخدم** كنوع الجهاز.

حدد خيار إخطار المستخدم:

- **عرض كلمة مرور المصادقة عند اكتمال المعالج**

إذا قمت بتحديد هذا الخيار، فسيتم عرض اسم المستخدم، واسم المستخدم في مدير حساب الأمان (SAM)، وكلمة مرور لاسترداد الشهادة لكل مستخدم من المستخدمين المحددين في الخطوة الأخيرة من معالج تثبيت الشهادة. لن يكون تكوين إخطار المستخدم بشهادة تم تثبيتها متاحًا.

عند قيامك بإضافة شهادات لعدة مستخدمين، يمكنك حفظ بيانات الاعتماد المقدمة في ملف عن طريق النقر فوق زر **تصدير** في الخطوة الأخيرة لمعالج تثبيت الشهادة.

هذا الخيار غير متاح في حال قيامك بتحديد **بيانات الاعتماد (المجال أو الاسم المستعار)** في خطوة **طريقة إخطار المستخدم** لمعالج تثبيت الشهادة.

- **إخطار المستخدم بالشهادة الجديدة**

إذا قمت بتحديد هذا الخيار، يمكنك تكوين إخطار المستخدم بشهادة جديدة.

- **بواسطة البريد الإلكتروني**

في هذه مجموعة من الإعدادات، يمكنك تكوين إخطار المستخدم بشأن تثبيت شهادة جديدة على جهازه المحمول باستخدام رسائل البريد الإلكتروني. لا تتوفر طريقة الإخطار هذه إلا في حالة تمكين خادم SMTP.

انقر فوق الرابط **تحرير رسالة** لعرض وتحرير رسالة الإخطار، إذا لزم الأمر.

- **عبر رسالة SMS**

في هذه مجموعة من الإعدادات، يمكنك تكوين إخطار المستخدم بشأن استخدام الرسائل النصية القصيرة لتثبيت شهادة على أجهزة محمولة. لا تتوفر طريقة الإخطار هذه إلا في حالة تمكين إخطارات رسائل SMS.

انقر فوق الرابط **تحرير رسالة** لعرض وتحرير رسالة الإخطار، إذا لزم الأمر.

الخطوة 8. إنشاء الشهادة

في هذه الخطوة، يتم إنشاء الشهادة.

ويمكنك النقر فوق **إنهاء** للخروج من المعالج.

يتم إنشاء الشهادة وعرضها في قائمة الشهادات الموجودة في مساحة عمل المجلد **الشهادات**.

تكوين قواعد إصدار الشهادة

يتم استخدام الشهادات لمصادقة الجهاز على خادم الإدارة. يجب أن تكون جميع أجهزة المحمول المُدارة حاصلة على شهادات. يمكنك تكوين كيفية إصدار الشهادات.

لتكوين قواعد إصدار الشهادة:

1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد المجلد الفرعي **الشهادات**.

2. في مساحة عمل المجلد **الشهادات**، انقر فوق الزر **تكوين قواعد إصدار الشهادات** لفتح النافذة **قواعد إصدار الشهادات**.

3. انتقل إلى القسم الذي يحمل اسم نوع الشهادة:

إصدار شهادات المحمول—لتكوين إصدار شهادات الأجهزة المحمولة.

إصدار شهادات البريد—لتكوين إصدار شهادات البريد.

إصدار شهادات VPN—لتكوين إصدار شهادات VPN.

4. في القسم **إعدادات الإصدار**، قم بتكوين إصدار الشهادة:

- حدد مدة الشهادة بالأيام.

تكون شهادات الأجهزة المحمولة مقيدة بتاريخ انتهاء صلاحية الشهادة الجذر. إذا حددت مدة الشهادة أطول من تاريخ انتهاء صلاحية شهادة الجذر، فسيتم ضبط مدة الشهادة تلقائيًا عند الإنشاء.

- حدد مصدر شهادة (**خادم الإدارة** أو **يتم تحديد الشهادات يدويًا**).

يتم اختيار خادم الإدارة كمصدر الشهادات الافتراضي.

- حدد قالب شهادة (**القالب الافتراضي، قالب آخر**).

يتوافر تكوين القوالب إذا كانت ميزات التكامل مع البنية الأساسية للمفتاح العام في القسم **التكامل مع PKI** ممكنة.

5. في القسم **إعدادات التحديثات التلقائية**، قم بتكوين التحديثات التلقائية للشهادة:

- في الحقل **التجديد عند انتهاء صلاحية الشهادة خلال (أيام)**، حدد عدد الأيام التي يجب تجديد الشهادة خلالها قبل موعد انتهاء صلاحيتها.
- لتمكين التحديثات التلقائية للشهادات، حدد خانة الاختيار **إعادة إصدار الشهادة تلقائيًا إن أمكن**.

6. في القسم **حماية بكلمة مرور** قم بتمكين وتكوين استخدام كلمة المرور عند فك تشفير الشهادات.

تتوفر الحماية بكلمة مرور لشهادات الجهاز المحمول فقط.

a. حدد خيار **المطالبة بكلمة مرور أثناء تثبيت الشهادة**.

b. استخدم شريط التمرير لتحديد الحد الأقصى لعدد الرموز في كلمة المرور للتشفير.

7. انقر على**موافق**.

التكامل مع البنية الأساسية للمفاتيح العامة

يتطلب دمج التطبيق مع البنية الأساسية للمفتاح العام (PKI) لتبسيط إصدار شهادات المجال للمستخدمين. في أعقاب الدمج، يتم إصدار الشهادات تلقائيًا.

الحد الأدنى لإصدار خادم PKI المدعوم هو Windows Server 2008.

يجب عليك تكوين الحساب للدمج مع PKI. يجب أن يفي الحساب بالمتطلبات التالية:

- أن يكون أحد مستخدمي المجال والمسؤول على جهاز مثبت عليه خادم الإدارة.
- أن يتم منحه امتياز SeServiceLogonRight على الجهاز الذي المثبت عليه خادم الإدارة.

لإنشاء ملف تعريف مستخدم دائم، قم بتسجيل الدخول مرة واحدة على الأقل بموجب حساب المستخدم الموجود على الجهاز المثبت عليه خادم الإدارة. في مستودع شهادة المستخدم هذا على جهاز خادم الإدارة، قم بتثبيت شهادة وكيل التسجيل المقدمة من مسؤولي المجال.

لتكوين الدمج مع البنية الأساسية للمفاتيح العامة:

1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد المجلد الفرعي **الشهادات**.

2. في مساحة العمل، انقر فوق الزر **التكامل مع البنية الأساسية للمفتاح العام** لفتح القسم **التكامل مع PKI** للنافذة **قواعد إصدار الشهادات**.
يفتح القسم **التكامل مع PKI** للنافذة **قواعد إصدار الشهادات**.

3. حدد خيار **دمج إصدار الشهادات مع PKI**.

4. في الحقل **الحساب**، حدد اسم حساب المستخدم الذي سيتم استخدامه للدمج مع البنية الأساسية للمفتاح العام.

5. في الحقل **كلمة المرور**، أدخل كلمة مرور المجال للحساب.

6. في القائمة **اسم قالب الشهادة في نظام PKI**، حدد قالب الشهادة الذي سيتم استخدامه لإصدار الشهادات لمستخدمي المجال.
تم تشغيل خدمة مخصصة في Kaspersky Security Center بموجب حساب المستخدم المحدد. هذه الخدمة مسؤولة عن إصدار شهادات المجال الخاصة بالمستخدمين. يتم تشغيل الخدمة عند تحميل قائمة بقوالب الشهادة عن طريق النقر فوق الزر **تحديث القائمة** أو عند إنشاء شهادة.

7. انقر فوق **موافق** لحفظ الإعدادات.

في أعقاب الدمج، يتم إصدار الشهادات تلقائيًا.

تمكين دعم تفويض Kerberos المقيد

يدعم التطبيق استخدام تفويض Kerberos المقيد.

لتمكين دعم تفويض Kerberos المقيد:

1. في شجرة وحدة التحكم، افتح مجلد **إدارة الجهاز المحمول**.

2. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم ، حدد المجلد الفرعي **خوادم الأجهزة المحمولة**.

3. في مساحة عمل المجلد **خوادم الأجهزة المحمولة**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

4. في قائمة السياق لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد **خصائص**.

5. في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM حدد القسم **الإعدادات**.

6. في القسم **الإعدادات**، حدد خانة الاختيار **ضمان التوافق مع تفويض Kerberos المقيد**.

7. انقر على**موافق**.

إضافة أجهزة محمولة iOS إلى قائمة الأجهزة المُدارة

لإضافة جهاز محمول iOS إلى قائمة الأجهزة المُدارة، يجب أن يتم تسليم شهادة مشتركة وتثبيتها على الجهاز. يتم استخدام الشهادات المشتركة بواسطة خادم الإدارة لتحديد الأجهزة المحمولة. يتم تسليم شهادة مشتركة لجهاز iOS المحمول ضمن ملف تعريف iOS MDM. بعد تسليم شهادة مشتركة وتثبيتها على جهاز محمول، يظهر الجهاز في قائمة الأجهزة المُدارة.

لم يعد Kaspersky يدعم Kaspersky Safe Browser بعد الآن.

يمكنك إضافة الأجهزة المحمولة للمستخدمين إلى قائمة الأجهزة المُدارة عن طريق معالج اتصال الجهاز المحمول الجديد.

لتوصيل جهاز iOS بخادم الإدارة باستخدام شهادة مشتركة:

1. بدء تشغيل معالج اتصال الجهاز المحمول الجديد بأحد الطرق التالية:

- استخدم قائمة السياق في المجلد **حسابات المستخدمين**:

  1. في شجرة وحدة التحكم ، قم بتوسيع مجلد **خيارات متقدمة** وحدد مجلد **حسابات المستخدمين** الفرعي .

  2. في مساحة عمل المجلد **حسابات المستخدمين**، حدد المستخدمين أو مجموعات المستخدمين أو مجموعات مستخدمي Active Directory الذين ترغب في إضافة الأجهزة المحمولة الخاصة بهم إلى قائمة الأجهزة المُدارة.

  3. انقر بزر الماوس الأيمن وفي قائمة سياق حساب المستخدم، حدد **إضافة جهاز محمول**.

     يبدأ تشغيل معالج اتصال الجهاز المحمول الجديد.

- في مساحة عمل المجلد **الأجهزة المحمولة**، انقر فوق الزر **إضافة جهاز محمول**:

  1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد مجلد **الأجهزة المحمولة** الفرعي .

  2. في مساحة عمل المجلد الفرعي **الأجهزة المحمولة**، انقر فوق الزر **إضافة جهاز محمول**.

     يبدأ تشغيل معالج اتصال الجهاز المحمول الجديد.

2. في صفحة **نظام التشغيل** للمعالج، حدد **iOS** كنوع نظام تشغيل الجهاز المحمول.

3. في الصفحة **تحديد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

4. في الصفحة **حدد المستخدمين الذين ترغب في إدارة أجهزتهم المحمولة** حدد المستخدمين أو مجموعات الأمان أو مجموعات أمان Active Directory التي ترغب في إضافة الأجهزة المحمولة الخاصة بها إلى قائمة الأجهزة المُدارة.

> يتم تخطي هذه الخطوة إذا بدأت المعالج بتحديد **إضافة جهاز محمول** في قائمة السياق لمجلد **حسابات المستخدمين**.

إذا كنت ترغب في إضافة حساب مستخدم جديد إلى القائمة، انقر فوق الزر **إضافة** وأدخل خصائص حساب المستخدم في النافذة التي تفتح. إذا كنت ترغب في تعديل أو مراجعة خصائص حساب المستخدم، فحدد حساب المستخدم من القائمة وانقر فوق الزر **خصائص**.

5. في صفحة **مصدر الشهادة** الخاصة بالمعالج، حدد طريقة إنشاء الشهادة المشتركة التي سيستخدمها خادم الإدارة لتحديد الجهاز المحمول. يمكنك تحديد شهادة مشتركة باستخدام إحدى الطرق التالية:

- **إصدار الشهادة من خلال أدوات خادم الإدارة**

  حدد هذا الخيار لإنشاء شهادة جديدة عن طريق أدوات خادم الإدارة إذا لم تقم بإنشائها مسبقًا.

  إذا تم تحديد هذا الخيار، فسيتم توقيع ملف تعريف iOS MDM تلقائيًا بشهادة تم إنشاؤها بواسطة خادم الإدارة.

  ويتم تحديد هذا الخيار بصورة افتراضية.

- **تحديد ملف شهادة**

  حدد هذا الخيار لتحديد ملف شهادة تم إنشاؤه مسبقًا.

  لا تتوفر هذه الطريقة إذا تم تحديد العديد من المستخدمين في الخطوة السابقة.

6. في صفحة **طريقة إخطار المستخدم** في المعالج، حدد الإعدادات الخاصة بإخطار مستخدم الجهاز المحمول عن طريق الرسائل القصيرة أو البريد الإلكتروني حول إنشاء الشهادة:

- **إظهار رمز الاستجابة السريعة في المعالج**

إذا حددت هذا الخيار، سيتم عرض رابط لحزمة التثبيت في الخطوة الأخيرة من معالج اتصال جهاز المحمول جديد.

لا يتوفر هذا الخيار إذا تم تحديد العديد من المستخدمين لاتصال الجهاز.

- **إرسال رمز الاستجابة السريعة إلى المستخدم**

يتيح لك تحديد هذا الخيار تكوين إخطار المستخدم باتصال جهاز محمول جديد.

يمكنك تحديد نوع عنوان البريد الإلكتروني، وتحديد عنوان بريد إلكتروني إضافي، وتحرير نص الرسالة. كذلك يمكنك تحديد نوع هاتف المستخدم الذي سيتم إرسال رسالة SMS إليه، وتحديد رقم هاتف إضافي، وتحرير نص رسالة SMS.

إذا لم يتم تكوين خادم SMTP بعد، فلا يمكن إرسال أي رسائل بريد إلكتروني إلى المستخدمين. إذا لم يتم تكوين إخطارات SMS بعد، فلا يمكن إرسال أي رسائل SMS إلى المستخدمين.

7. في صفحة **النتيجة**، انقر فوق **إنهاء** لإغلاق المعالج.

يتم نشر ملف تعريف iOS MDM على Kaspersky Security Center Web Server. يتلقى مستخدم الجهاز المحمول إخطارًا برابط لتنزيل ملف تعريف iOS MDM من خادم الويب. يقوم المستخدم بالنقر فوق الرابط. بعد ذلك، سيطالب نظام التشغيل على الجهاز المستخدم بقبول تثبيت ملف تعريف iOS MDM. يجب أن يوافق المستخدم على تثبيت ملف تعريف iOS MDM قبل إمكانية تنزيل ملف تعريف iOS MDM على الجهاز المحمول. بعد تنزيل ملف تعريف iOS MDM ومزامنة الجهاز المحمول مع خادم الإدارة، يتم عرض الجهاز في المجلد **الأجهزة المحمولة** وهو المجلد الفرعي للمجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم.

لمتابعة المستخدم إلى Kaspersky Security Center Web Server باستخدام الرابط، يجب توفير اتصال مع خادم الإدارة عبر المنفذ 8061 على الجهاز المحمول.

إضافة أجهزة محمولة تعمل بنظام Android إلى قائمة الأجهزة المُدارة

لإضافة جهاز محمول يعمل بنظام Android إلى قائمة الأجهزة المُدارة، يجب تسليم Kaspersky Endpoint Security for Android وشهادة مشتركة وتثبيتها على الجهاز المحمول. يتم استخدام الشهادات المشتركة بواسطة خادم الإدارة لتحديد الأجهزة المحمولة. بعد تسليم شهادة مشتركة وتثبيتها على جهاز محمول، يظهر الجهاز في قائمة الأجهزة المُدارة.

يمكنك إضافة الأجهزة المحمولة للمستخدمين إلى قائمة الأجهزة المُدارة عن طريق معالج اتصال الجهاز المحمول الجديد. يوفر المعالج خيارين لتسليم وتثبيت شهادة مشتركة وKaspersky Endpoint Security for Android:

- باستخدام رابط Google Play
- باستخدام رابط من Kaspersky Security Center Web Server

يتم استخدام حزمة تثبيت Kaspersky Endpoint Security for Android المخزنة للتوزيع على خادم الإدارة للتثبيت

بدء معالج اتصال الجهاز المحمول الجديد

لبدء تشغيل معالج اتصال الجهاز المحمول الجديد، قم بأحد الإجراءات التالية:

- استخدم قائمة السياق في المجلد **حسابات المستخدمين**:

1. في شجرة وحدة التحكم ، قم بتوسيع مجلد **خيارات متقدمة** وحدد مجلد **حسابات المستخدمين** الفرعي .

2. في مساحة عمل المجلد **حسابات المستخدمين**، حدد المستخدمين أو مجموعات المستخدمين أو مجموعات مستخدمي Active Directory الذين ترغب في إضافة الأجهزة المحمولة الخاصة بهم إلى قائمة الأجهزة المُدارة.

3. انقر بزر الماوس الأيمن وفي قائمة سياق حساب المستخدم، حدد **إضافة جهاز محمول**.

   يبدأ تشغيل معالج اتصال الجهاز المحمول الجديد.

- في مساحة عمل المجلد **الأجهزة المحمولة**، انقر فوق الزر **إضافة جهاز محمول**:

1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد مجلد **الأجهزة المحمولة** الفرعي .

2. في مساحة عمل المجلد الفرعي **الأجهزة المحمولة**، انقر فوق الزر **إضافة جهاز محمول**.

   يبدأ تشغيل معالج اتصال الجهاز المحمول الجديد.

إضافة جهاز محمول يعمل بنظام Android باستخدام رابط Google Play

لتثبيت Kaspersky Endpoint Security for Android وشهادة مشتركة على جهاز محمول باستخدام رابط Google Play:

1. ابدأ معالج اتصال الجهاز المحمول الجديد.

2. في صفحة **نظام التشغيل** في المعالج، حدد **Android** كنوع نظام التشغيل للجهاز المحمول.

3. في صفحة **طريقة لتثبيت Kaspersky Endpoint Security for Android على الأجهزة** من المعالج، حدد **تنزيل التطبيق من Google Play**.

4. في صفحة **حدد المستخدمين الذين ترغب في إدارة أجهزتهم المحمولة** في المعالج، حدد المستخدمين أو مجموعات الأمان أو مجموعات أمان Active Directory الذين ترغب في إضافة الأجهزة المحمولة الخاصة بهم إلى قائمة الأجهزة المُدارة.

> يتم تخطي هذه الخطوة إذا بدأ المعالج بتحديد **إضافة جهاز محمول** في قائمة السياق للمجلد **حسابات المستخدمين**.

إذا كنت ترغب في إضافة حساب مستخدم جديد إلى القائمة، انقر فوق الزر **إضافة** وأدخل خصائص حساب المستخدم في النافذة التي تفتح. إذا كنت ترغب في تعديل أو مراجعة خصائص حساب المستخدم، فحدد حساب المستخدم من القائمة وانقر فوق الزر **خصائص**.

5. في صفحة **مصدر الشهادة** الخاصة بالمعالج، حدد طريقة إنشاء الشهادة المشتركة التي سيستخدمها خادم الإدارة لتحديد الجهاز المحمول. يمكنك تحديد شهادة مشتركة باستخدام إحدى الطرق التالية:

- **إصدار الشهادة من خلال أدوات خادم الإدارة**

  حدد هذا الخيار لإنشاء شهادة جديدة عن طريق أدوات خادم الإدارة إذا لم تقم بإنشائها مسبقًا.

  في حالة تحديد هذا الخيار، يتم إصدار الشهادة تلقائيًا باستخدام أدوات خادم الإدارة.

  ويتم تحديد هذا الخيار بصورة افتراضية.

- **تحديد ملف شهادة**

حدد هذا الخيار لتحديد ملف شهادة تم إنشاؤه مسبقًا.

لا تتوفر هذه الطريقة إذا تم تحديد العديد من المستخدمين في الخطوة السابقة.

6. في صفحة **طريقة إخطار المستخدم** في المعالج، حدد الإعدادات الخاصة بإخطار مستخدم الجهاز المحمول عن طريق الرسائل القصيرة أو البريد الإلكتروني حول إنشاء الشهادة:

- **إظهار رمز الاستجابة السريعة في المعالج**

إذا حددت هذا الخيار، سيتم عرض رابط لحزمة التثبيت في الخطوة الأخيرة من معالج اتصال جهاز المحمول جديد.

لا يتوفر هذا الخيار إذا تم تحديد العديد من المستخدمين لاتصال الجهاز.

- **إرسال رمز الاستجابة السريعة إلى المستخدم**

يتيح لك تحديد هذا الخيار تكوين إخطار المستخدم باتصال جهاز محمول جديد.

يمكنك تحديد نوع عنوان البريد الإلكتروني، وتحديد عنوان بريد إلكتروني إضافي، وتحرير نص الرسالة. كذلك يمكنك تحديد نوع هاتف المستخدم الذي سيتم إرسال رسالة SMS إليه، وتحديد رقم هاتف إضافي، وتحرير نص رسالة SMS.

إذا لم يتم تكوين خادم SMTP بعد، فلا يمكن إرسال أي رسائل بريد إلكتروني إلى المستخدمين. إذا لم يتم تكوين إخطارات SMS بعد، فلا يمكن إرسال أي رسائل SMS إلى المستخدمين.

7. في صفحة **النتيجة**، انقر فوق **إنهاء** لإغلاق المعالج.

بعد انتهاء المعالج، سيتم إرسال رابط ورمز QR إلى الجهاز المحمول للمستخدم، مما يسمح بتنزيل Kaspersky Endpoint Security for Android. يقوم المستخدم بالنقر فوق الرابط أو مسح رمز QR. بعد ذلك، يطالب نظام تشغيل الجهاز المحمول المستخدم بقبول تثبيت Kaspersky Endpoint Security for Android. بعد تنزيل Kaspersky Endpoint Security for Android وتثبيته، يتصل الجهاز المحمول بخادم الإدارة ويقوم بتنزيل الشهادة المشتركة. بعد تثبيت الشهادة على الجهاز المحمول، يتم عرض الجهاز في مجلد **الأجهزة المحمولة**، وهو المجلد الفرعي لمجلد **إدارة الجهاز المحمول** الموجود بشجرة وحدة التحكم.

إضافة جهاز محمول بنظام Android باستخدام رابط من Kaspersky Security Center Web Server

يتم استخدام حزمة تثبيت Kaspersky Endpoint Security for Android الموجودة على خادم الإدارة لإجراء التثبيت.

لتثبيت Kaspersky Endpoint Security for Android وشهادة مشتركة على جهاز محمول باستخدام رابط من Web Server:

1. ابدأ معالج اتصال الجهاز المحمول الجديد.

2. في صفحة **نظام التشغيل** في المعالج، حدد **Android** كنوع نظام التشغيل للجهاز المحمول.

3. في صفحة **طريقة لتثبيت Kaspersky Endpoint Security for Android على الأجهزة** في المعالج، حدد **تنزيل حزمة تثبيت التطبيق من Kaspersky Security Center**.

في الحقل الذي يظهر أدناه، حدد حزمة تثبيت أو قم بإنشاء حزمة جديدة بالنقر فوق **جديد**.

4. في صفحة **حدد المستخدمين الذين ترغب في إدارة أجهزتهم المحمولة** في المعالج، حدد المستخدمين أو مجموعات الأمان أو مجموعات أمان Active Directory الذين ترغب في إضافة الأجهزة المحمولة الخاصة بهم إلى قائمة الأجهزة المُدارة.

يتم تخطي هذه الخطوة إذا بدأ المعالج بتحديد **إضافة جهاز محمول** في قائمة السياق للمجلد **حسابات المستخدمين**.

إذا كنت ترغب في إضافة حساب مستخدم جديد إلى القائمة، انقر فوق الزر **إضافة** وأدخل خصائص حساب المستخدم في النافذة التي تفتح. إذا كنت ترغب في تعديل أو مراجعة خصائص حساب المستخدم، فحدد حساب المستخدم من القائمة وانقر فوق الزر **خصائص**.

5. في صفحة **مصدر الشهادة** الخاصة بالمعالج، حدد طريقة إنشاء الشهادة المشتركة التي سيستخدمها خادم الإدارة لتحديد الجهاز المحمول. يمكنك تحديد شهادة مشتركة باستخدام إحدى الطرق التالية:

- **إصدار الشهادة من خلال أدوات خادم الإدارة**

  حدد هذا الخيار لإنشاء شهادة جديدة عن طريق أدوات خادم الإدارة إذا لم تقم بإنشائها مسبقًا.

  في حالة تحديد هذا الخيار، يتم إصدار الشهادة تلقائيًا باستخدام أدوات خادم الإدارة.

  ويتم تحديد هذا الخيار بصورة افتراضية.

- **تحديد ملف شهادة**

  حدد هذا الخيار لتحديد ملف شهادة تم إنشاؤه مسبقًا.

  لا تتوفر هذه الطريقة إذا تم تحديد العديد من المستخدمين في الخطوة السابقة.

6. في صفحة **طريقة إخطار المستخدم** في المعالج، حدد الإعدادات الخاصة بإخطار مستخدم الجهاز المحمول عن طريق الرسائل القصيرة أو البريد الإلكتروني حول إنشاء الشهادة:

- **إظهار رمز الاستجابة السريعة في المعالج**

  إذا حددت هذا الخيار، سيتم عرض رابط لحزمة التثبيت في الخطوة الأخيرة من معالج اتصال جهاز المحمول جديد.

  لا يتوفر هذا الخيار إذا تم تحديد العديد من المستخدمين لاتصال الجهاز.

- **إرسال رمز الاستجابة السريعة إلى المستخدم**

  يتيح لك تحديد هذا الخيار تكوين إخطار المستخدم باتصال جهاز محمول جديد.

  يمكنك تحديد نوع عنوان البريد الإلكتروني، وتحديد عنوان بريد إلكتروني إضافي، وتحرير نص الرسالة. كذلك يمكنك تحديد نوع هاتف المستخدم الذي سيتم إرسال رسالة SMS إليه، وتحديد رقم هاتف إضافي، وتحرير نص رسالة SMS.

  إذا لم يتم تكوين خادم SMTP بعد، فلا يمكن إرسال أي رسائل بريد إلكتروني إلى المستخدمين. إذا لم يتم تكوين إخطارات SMS بعد، فلا يمكن إرسال أي رسائل SMS إلى المستخدمين.

7. في صفحة **النتيجة**، انقر فوق **إنهاء** لإغلاق المعالج.

يتم نشر حزمة تطبيق الجهاز المحمول لـ Kaspersky Endpoint Security for Android بشكل تلقائي على Kaspersky Security Center Web Server Web Server. تحتوي حزمة تطبيق الجهاز المحمول على التطبيق، وإعدادات لاتصال الجهاز المحمول بخادم الإدارة، وشهادة. سيتلقى مستخدم الجهاز المحمول إخطار يحتوي على رابط لتنزيل الحزمة من خادم الويب. يقوم المستخدم بالنقر فوق الرابط. سيطالب نظام تشغيل الجهاز المستخدم بعد ذلك بقبول تثبيت حزمة تطبيقات الأجهزة المحمولة. في حالة موافقة المستخدم، سيتم تنزيل الحزمة على الجهاز المحمول. بعد تنزيل الحزمة ومزامنة الجهاز المحمول مع خادم الإدارة، يتم عرض الجهاز في المجلد **الأجهزة المحمولة** وهو المجلد الفرعي للمجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم.

إدارة أجهزة iOS MDM

يوضح هذا القسم المزايا المتقدمة لإدارة أجهزة iOS MDM من خلال Kaspersky Security Center. يدعم التطبيق الميزات التالية لإدارة أجهزة iOS MDM:

- تحديد إعدادات إدارة أجهزة iOS MDM المدارة في الوضع المركزي وتقييد مزايا الأجهزة بواسطة ملفات تعريف التكوين. يمكنك إضافة أو تعديل ملفات تعريف التكوين وتثبيتها على الأجهزة المحمولة.
- تثبيت التطبيقات على الأجهزة المحمولة عن طريق ملفات تعريف التزويد، من خلال تجاوز متجر التطبيقات (App Store). على سبيل المثال، يمكنك استخدام ملفات تعريف التزويد لتثبيت تطبيقات الشركة الداخلية على أجهزة المحمولة للمستخدم. يحتوي ملف تعريف التزويد على معلومات حول أحد التطبيقات وأحد الأجهزة المحمولة.
- تثبيت التطبيقات على جهاز iOS MDM من خلال متجر التطبيقات (App Store). قبل تثبيت تطبيق على جهاز iOS MDM، يجب إضافة التطبيق إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

كل 24 ساعة، يتم إرسال الإخطار لجميع أجهزة iOS MDM المتصلة لأجل مزامنة البيانات مع خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

لمعلومات حول ملف تعريف التكوين وملف تعريف التزويد، وكذلك التطبيقات المثبتة على جهاز iOS MDM، برجاء الرجوع إلى نافذة خصائص الجهاز.

توقيع ملف تعريف iOS MDM بشهادة

يمكنك التوقيع على ملف تعريف iOS MDM بشهادة. يمكنك استخدام شهادة قمت بإصدارها بنفسك أو يمكنك تلقي شهادة من المراجع المصدقة والموثوقة.

تعرض أجهزة iOS إخلاء مسؤولية لملفات التعريف غير المُوقّعة وتطالب المستخدم بالثقة في المُوقّع عند تثبيت ملف التعريف.

للتوقيع على ملف تعريف iOS MDM بشهادة:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.
2. من قائمة سياق المجلد **الأجهزة المحمولة**، حدد **خصائص**.
3. في نافذة خصائص المجلد، حدد قسم **إعدادات الاتصال لأجهزة iOS**.
4. انقر فوق زر **استعراض** ضمن حقل **تحديد ملف شهادة**.
   النافذة **الشهادة**.
5. في الحقل **نوع الشهادة**، حدد نوع الشهادة العامة أو الخاصة:
   - إذا تم تحديد القيمة **الحاوية PKCS#12**، فحدد ملف الشهادة وكلمة المرور.
   - إذا تم تحديد القيمة **الشهادة X.509**:
     a. حدد ملف المفتاح الخاص (الملف ذو الامتداد *.prk أو *.pem).
     b. حدد كلمة مرور المفتاح الخاص.
     c. حدد ملف المفتاح العام (الملف ذو الامتداد *.cer).
6. انقر على**موافق**.

تم التوقيع على ملف تعريف iOS MDM بشهادة.

إضافة ملف تعريف التكوين

لإنشاء ملف تعريف التكوين، يمكنك استخدام Apple Configurator 2، وهو متوفر على الموقع الإلكتروني لشركة Apple. Apple Configurator 2 لا يعمل إلا على الأجهزة التي تعمل بنظام التشغيل macOS. وإذا لم يكن لديك في حوزتك مثل هذه الأجهزة، يمكنك استخدام أداة تكوين iPhone على الجاز الذي يوجد به وحدة تحكم الإدارة بدلاً من ذلك. لكن شركة Apple Inc. لم تعد تدعم أداة تكوين iPhone.

لإنشاء ملف تعريف تكوين باستخدام أداة تكوين iPhone وإضافته إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM:

1. في شجرة وحدة التحكم، حدد مجلد **إدارة الجهاز المحمول**.
2. في مساحة عمل المجلد **إدارة الجهاز المحمول**، حدد المجلد الفرعي **خوادم الأجهزة المحمولة**.
3. في مساحة عمل المجلد **خوادم الأجهزة المحمولة**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.
4. في قائمة السياق لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد **خصائص**.

   يتم فتح نافذة خصائص خادم الجهاز المحمول.
5. في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM حدد القسم **ملفات تعريف التكوين**.
6. في قسم **ملفات تعريف التكوين** انقر فوق الزر **إنشاء**.

   يتم فتح نافذة **ملف تعريف التكوين الجديد**.
7. في النافذة **ملف تعريف التكوين الجديد**، حدد اسمًا ومعرفًا لملف التعريف.

   يجب أن يكون معرف ملف تعريف التكوين فريدًا؛ يجب تحديد القيمة بتنسيق Reverse-DNS، على سبيل المثال com.companyname.identifier.
8. انقر على**موافق**.

   بعدها أداة تكوين iPhone تبدأ كانت مثبتة لديك.
9. أعد تكوين ملف التعريف في أداة تكوين iPhone المساعدة.

   للحصول على وصف لإعدادات ملف التعريف وإرشادات حول كيفية تكوين ملف التعريف، يُرجى الرجوع إلى الوثائق المضمنة مع أداة تكوين iPhone المساعدة.

بعد تكوين ملف التعريف باستخدام أداة تكوين iPhone المساعدة، يتم عرض ملف تعريف التكوين الجديد في القسم **ملفات تعريف التكوين** في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

يمكنك النقر على الزر **تعديل** لتعديل ملف تعريف التكوين.

يمكنك النقر على الزر **استيراد** لتحميل ملف تعريف التكوين إلى برنامج.

انقر على الزر**تصدير** لحفظ ملف تعريف التكوين إلى ملف.

يجب أن يكون ملف التعريف الذي قمت بإنشائه مثبت على أجهزة iOS MDM.

تثبيت ملف تعريف تكوين إلى جهاز

لتثبيت ملف تعريف التكوين إلى جهاز محمول:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة iOS MDM بحسب نوع بروتوكول (iOS MDM).

3. حدد جهاز محمول المستخدم الذي يجب تثبيت ملف تعريف التكوين عليه.

   يمكنك تحديد العديد من الأجهزة المحمولة لتثبيت ملف التعريف عليهم في وقت واحد.

4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.

5. في النافذة **أوامر إدارة الأجهزة المحمولة**، انتقل إلى القسم **تثبيت ملف التعريف** وانقر فوق الزر **إرسال أمر**.

   يمكنك أيضًا إرسال الأمر إلى الجهاز المحمول عن طريق تحديد **كل الأوامر** في قائمة سياق جهاز المحمول هذا، ثم تحديد **تثبيت ملف التعريف**.

   تفتح النافذة **تحديد ملفات التعريف** بحيث تعرض قائمة بملفات التعريف. حدد من القائمة ملف التعريف الذي يجب تثبيته على الجهاز المحمول. يمكنك تحديد العديد من ملفات التعريف لتثبيتها على الجهاز المحمول في وقت واحد. لتحديد مجموعة من ملفات التعريف، استخدم المفتاح **Shift**. للجمع بين ملفات التعريف في مجموعة، استخدم المفتاح **CTRL**.

6. انقر فوق الزر**موافق** لإرسال الأمر إلى الجهاز المحمول.

   عندما يتم تنفيذ الأمر، سوف يتم تثبيت ملفات تعريف التكوين المحددة على جهاز محمول المستخدم. إذا تم تنفيذ الأمر بنجاح، ستظهر الحالة الحالية للأمر في سجل الأوامر على النحو تم.

   يمكنك النقر فوق الزر **إعادة إرسال** لإرسال الأمر إلى جهاز محمول المستخدم مرة أخرى.

   يمكنك النقر فوق الزر **إزالة من قائمة الانتظار** لإلغاء تنفيذ أمر تم إرساله إذا لم يتم تنفيذ الأمر بعد.

   يعرض القسم **سجل الأمر** الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق **تحديث** لتحديث قائمة الأوامر.

7. انقر فوق **موافق** لإغلاق النافذة **أوامر إدارة الجهاز المحمول**.

يمكنك عرض ملف التعريف الذي قمت بتثبيته وحذفه إذا لزم الأمر.

إزالة ملف تعريف التكوين من جهاز

لإزالة ملف تعريف التكوين من جهاز محمول:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة iOS MDM عن طريق النقر على الرابط **iOS MDM**.

3. حدد جهاز محمول المستخدم الذي يجب إزالة ملف تعريف التكوين من عليه.

   يمكنك تحديد العديد من الأجهزة المحمولة لإزالة ملف التعريف من عليهم في وقت واحد.

4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.

5. في النافذة **أوامر إدارة جهاز المحمول**، انتقل إلى القسم **إزالة ملف التعريف** وانقر فوق الزر **إرسال أمر**.

   يمكنك أيضًا إرسال الأمر إلى الجهاز المحمول عن طريق تحديد **كل الأوامر** من قائمة سياق الجهاز، ثم تحديد **إزالة ملف التعريف**.

   تفتح النافذة **إزالة ملفات تعريف** بحيث تعرض قائمة بملفات التعريف.

6. حدد من القائمة ملف التعريف الذي يجب إزالته من على الجهاز المحمول. يمكنك تحديد العديد من ملفات التعريف لإزالتها من على الجهاز المحمول في وقت واحد. لتحديد مجموعة من ملفات التعريف، استخدم المفتاح **Shift**. للجمع بين ملفات التعريف في مجموعة، استخدم المفتاح **CTRL**.

7. انقر فوق الزر**موافق** لإرسال الأمر إلى الجهاز المحمول.

عند تنفيذ الأمر بنجاح، سوف يتم إزالة ملفات تعريف التكوين المحددة من على جهاز محمول المستخدم. إذا تم تنفيذ الأمر بنجاح، ستظهر الحالة الحالية للأمر على النحو مكتمل.

يمكنك النقر فوق الزر **إعادة إرسال** لإرسال الأمر إلى جهاز محمول المستخدم مرة أخرى.

يمكنك النقر فوق الزر **إزالة من قائمة الانتظار** لإلغاء تنفيذ أمر تم إرساله إذا لم يتم تنفيذ الأمر بعد.

يعرض القسم **سجل الأمر** الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق **تحديث** لتحديث قائمة الأوامر.

8. انقر فوق **موافق** لإغلاق النافذة **أوامر إدارة جهاز المحمول**.

إضافة جهاز جديد بواسطة نشر رابط على ملف تعريف

في وحدة التحكم في الإدارة، يقوم المسؤول بإنشاء ملف تعريف iOS MDM، باستخدام معالج تثبيت الشهادة. ينفذ المعالج الإجراءات التالية:

- يتم نشر ملف تعريف iOS MDM على خادم الويب تلقائيًا.
- يتم إرسال رابط لملف تعريف iOS MDM إلى المستخدم عن طريق رسالة SMS أو البريد الإلكتروني. عند استلام الرابط، يقوم المستخدم بتثبيت ملف تعريف iOS MDM على الجهاز المحمول.
- يتصل الجهاز المحمول أيضًا بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

ونظرًا لسياسة الأمن الأكثر صرامةً التي تم إدخالها بواسطة شركة Apple، عليك إعداد إصدارات بروتوكول TLS 1.1 وTLS 1.2 عند توصيل جهاز محمول يعمل بنظام تشغيل iOS 11 بخادم إدارة يحتوي على ميزة التكامل مع البنية الأساسية للمفاتيح العامة (PKI).

إضافة جهاز جديد من خلال تثبيت ملف التعريف بواسطة المسؤول

لتوصيل جهاز محمول بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عن طريق تثبيت ملف تعريف iOS MDM على هذا الجهاز المحمول، يجب على المسؤول القيام بالإجراءات التالية:

1. في وحدة تحكم الإدارة، افتح معالج تثبيت الشهادة.
2. قم بإنشاء ملف تعريف iOS MDM جديد عن طريق تحديد خانة الاختيار **إظهار الشهادة بعد اكتمال المعالج** في نافذة المعالج.
3. احفظ ملف تعريف iOS MDM.
4. قم بتثبيت ملف تعريف iOS MDM على الجهاز المحمول الخاص بالمستخدم من خلال الأداة المساعدة مكوّن Apple.

يتصل الجهاز المحمول أيضًا بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

ونظرًا لسياسة الأمن الأكثر صرامةً التي تم إدخالها بواسطة شركة Apple، عليك إعداد إصدارات بروتوكول TLS 1.1 وTLS 1.2 عند توصيل جهاز محمول يعمل بنظام تشغيل iOS 11 بخادم إدارة يحتوي على ميزة التكامل مع البنية الأساسية للمفاتيح العامة (PKI).

إضافة ملف تعريف التزويد

لإضافة ملف تعريف التزويد إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM:

1. في شجرة وحدة التحكم، افتح مجلد **إدارة الجهاز المحمول**.
2. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم ، حدد المجلد الفرعي **خوادم الأجهزة المحمولة**.
3. في مساحة عمل المجلد **خوادم الأجهزة المحمولة**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.
4. في قائمة السياق لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد **خصائص**.

   يتم فتح نافذة خصائص خادم الجهاز المحمول.
5. في نافذة خصائص **خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM**، انتقل إلى القسم **ملفات تعريف التزويد**.
6. في القسم **ملفات تعريف التزويد** انقر فوق الزر **استيراد** وحدد المسار إلى ملف تعريف التزويد.

   ستتم إضافة ملف التعريف إلى إعدادات خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

   انقر على الزر**تصدير** لحفظ ملفات تعريف التزويد إلى ملف.

يمكنك تثبيت ملف تعريف التزويد الذي قمت باستيراده على أجهزة iOS MDM.

تثبيت ملف تعريف التزويد إلى جهاز

لتثبيت ملف تعريف التزويد على جهاز محمول:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.
2. في مساحة العمل، قم بتصفية أجهزة iOS MDM بحسب نوع بروتوكول (iOS MDM).
3. حدد جهاز محمول المستخدم الذي يجب تثبيت ملف تعريف التزويد عليه.

   يمكنك تحديد العديد من الأجهزة المحمولة لتثبيت ملف تعريف التزويد في وقت واحد.
4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.
5. في النافذة **أوامر إدارة الأجهزة المحمولة**، انتقل إلى القسم **تثبيت ملف تعريف التزويد** وانقر فوق الزر **إرسال أمر**.

   يمكنك أيضًا إرسال الأمر إلى الجهاز المحمول عن طريق تحديد **كل الأوامر** من قائمة سياق جهاز المحمول هذا، ثم قم بتحديد **تثبيت ملف تعريف التزويد**.

   تفتح النافذة **حدد ملفات تعريف التزويد** بحيث تعرض قائمة بملفات تعريف التزويد. حدد من القائمة ملف تعريف التزويد الذي يجب تثبيته على الجهاز المحمول. يمكنك تحديد العديد من ملفات تعريف التزويد لتثبيتها على الجهاز في وقت واحد. لتحديد مجموعة من ملفات تعريف التزويد، استخدم المفتاح **Shift**. للجمع بين ملفات تعريف التزويد في مجموعة، استخدم المفتاح **Ctrl**.
6. انقر فوق الزر**موافق** لإرسال الأمر إلى الجهاز المحمول.

   عندما يتم تنفيذ الأمر، سوف يتم تثبيت ملفات تعريف التزويد المحددة على جهاز محمول المستخدم. إذا تم تنفيذ الأمر بنجاح، ستظهر الحالة الحالية للأمر في سجل الأوامر على النحو مكتمل.

   يمكنك النقر فوق الزر **إعادة إرسال** لإرسال الأمر إلى جهاز محمول المستخدم مرة أخرى.

   يمكنك النقر فوق الزر **إزالة من قائمة الانتظار** لإلغاء تنفيذ أمر تم إرساله إذا لم يتم تنفيذ الأمر بعد.

يعرض القسم **سجل الأمر** الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق **تحديث** لتحديث قائمة الأوامر.

7. انقر فوق **موافق** لإغلاق النافذة **أوامر إدارة الجهاز المحمول**.

يمكنك عرض ملف التعريف الذي قمت بتثبيته وحذفه إذا لزم الأمر.

إزالة ملف تعريف التزويد إلى جهاز

لإزالة ملف تعريف التزويد من جهاز محمول:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة iOS MDM بحسب نوع بروتوكول (iOS MDM).

3. حدد جهاز محمول المستخدم الذي يجب إزالة ملف تعريف التزويد من عليه.

يمكنك تحديد العديد من الأجهزة المحمولة لإزالة ملف تعريف التزويد من عليها في وقت واحد.

4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.

5. في النافذة **أوامر إدارة جهاز المحمول**، انتقل إلى القسم **إزالة ملف تعريف التزويد** وانقر فوق الزر **إرسال أمر**.

يمكنك أيضًا إرسال الأمر إلى الجهاز المحمول عن طريق تحديد **جميع الأوامر** من قائمة السياق، ثم تحديد **إزالة ملف تعريف التزويد**.

تفتح النافذة **إزالة ملفات تعريف التزويد** بحيث تعرض قائمة بملفات التعريف.

6. حدد من القائمة ملف تعريف التزويد الذي تحتاج إلى إزالته من على الجهاز المحمول. يمكنك تحديد العديد من ملفات تعريف التزويد لإزالتها من على الجهاز في وقت واحد. لتحديد مجموعة من ملفات تعريف التزويد، استخدم المفتاح **Shift**. للجمع بين ملفات تعريف التزويد في مجموعة، استخدم المفتاح **Ctrl**.

7. انقر فوق الزر**موافق** لإرسال الأمر إلى الجهاز المحمول.

عند تنفيذ الأمر، سوف يتم إزالة ملف تعريف التزويد المحدد من على جهاز محمول المستخدم. التطبيقات المرتبطة بملف تعريف التزويد التي تم حذفه لن تكون قابلة للتشغيل. إذا تم تنفيذ الأمر بنجاح، ستظهر الحالة الحالية للأمر على النحو مكتمل.

يمكنك النقر فوق الزر **إعادة إرسال** لإرسال الأمر إلى جهاز محمول المستخدم مرة أخرى.

يمكنك النقر فوق الزر **إزالة من قائمة الانتظار** لإلغاء تنفيذ أمر تم إرساله إذا لم يتم تنفيذ الأمر بعد.

يعرض القسم **سجل الأمر** الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق **تحديث** لتحديث قائمة الأوامر.

8. انقر فوق **موافق** لإغلاق النافذة **أوامر إدارة جهاز المحمول**.

إضافة تطبيق مدار

قبل تثبيت تطبيق على جهاز iOS MDM، يجب إضافة التطبيق إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. يعتبر التطبيق مدارًا إذا تم تثبيته على جهاز من خلال Kaspersky Security Center. يمكن إدارة تطبيق مدار عن بُعد بواسطة Kaspersky Security Center.

لإضافة تطبيق مُدار إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM:

1. في شجرة وحدة التحكم، افتح مجلد **إدارة الجهاز المحمول**.

2. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم ، حدد المجلد الفرعي **خوادم الأجهزة المحمولة**.

3. في مساحة عمل المجلد **خوادم الأجهزة المحمولة**، حدد خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

4. في قائمة السياق لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد **خصائص**.

يؤدي هذا إلى فتح نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

5. في نافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، حدد القسم **التطبيقات المُدارة**.

6. انقر فوق الزر **إضافة** في القسم **التطبيقات المُدارة**.

يتم فتح نافذة **إضافة تطبيق**.

7. في النافذة **إضافة تطبيق**، في الحقل **اسم التطبيق** حدد اسم التطبيق الذي تريد إضافته.

8. في الحقل **معرف Apple ID أو رابط لملف البيان** حدد مُعرف Apple ID للتطبيق الذي تريد إضافته أو حدد رابط إلى ملف البيان الذي يمكن استخدامه لتنزيل التطبيق.

9. إذا أردت إزالة تطبيق مُدار من جهاز محمول المستخدم مع ملف تعريف iOS MDM عند إزالة هذا الأخير، حدد خانة الاختيار **إزالة مع ملف تعريف iOS MDM**.

10. إذا أردت منع النسخ الاحتياطي لبيانات التطبيق من خلال iTunes، حدد خانة الاختيار **منع النسخ الاحتياطي للبيانات**.

11. انقر على**موافق**.

يتم عرض التطبيق المضاف في القسم **التطبيقات المُدارة** لنافذة خصائص خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

تثبيت تطبيق على جهاز محمول:

لتثبيت تطبيق على جهاز محمول iOS MDM:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. حدد جهاز iOS MDM الذي ترغب في تثبيت التطبيق عليه.

يمكنك تحديد العديد من الأجهزة المحمولة لتثبيت التطبيق عليها في وقت واحد.

3. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.

4. في النافذة **أوامر إدارة الأجهزة المحمولة**، انتقل إلى القسم **تثبيت التطبيق** وانقر فوق الزر **إرسال أمر**.

يمكنك أيضًا إرسال الأمر إلى الجهاز المحمول عن طريق تحديد **كل الأوامر** من قائمة سياق جهاز المحمول هذا، ثم تحديد **تثبيت تطبيق**.

تفتح نافذة **تحديد تطبيقات** بحيث تعرض قائمة بملفات التعريف. حدد من القائمة التطبيق الذي يجب تثبيته على الجهاز المحمول. يمكنك تحديد العديد من ملفات التطبيقات لتثبيتها على الجهاز في وقت واحد. لتحديد مجموعة من التطبيقات، استخدم المفتاح **Shift**. للجمع بين التطبيقات في مجموعة، استخدم المفتاح **Ctrl**.

5. انقر فوق الزر **موافق** لإرسال الأمر إلى الجهاز المحمول.

عند تنفيذ الأمر، سوف يتم تثبيت التطبيق المحدد على جهاز محمول المستخدم. إذا تم تنفيذ الأمر بنجاح، ستظهر الحالة الحالية للأمر في سجل الأوامر على النحو مكتمل.

يمكنك النقر فوق الزر **إعادة إرسال** لإرسال الأمر إلى جهاز محمول المستخدم مرة أخرى. يمكنك النقر فوق الزر **إزالة من قائمة الانتظار** لإلغاء تنفيذ أمر تم إرساله إذا لم يتم تنفيذ الأمر بعد.

يعرض القسم **سجل الأمر** الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق **تحديث** لتحديث قائمة الأوامر.

6. انقر فوق **موافق** لإغلاق النافذة **أوامر إدارة الجهاز المحمول**.

يتم عرض معلومات حول التطبيق المثبت في خصائص الجهاز المحمول iOS MDM. يمكنك إزالة التطبيق من الجهاز المحمول من خلال سجل الأوامر أو قائمة سياق الجهاز المحمول.

إزالة تطبيق من جهاز

لإزالة تطبيق من جهاز محمول:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.
   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة iOS MDM بحسب نوع بروتوكول (iOS MDM).

3. حدد جهاز محمول المستخدم الذي يجب إزالة التطبيق من عليه.
   يمكنك تحديد العديد من الأجهزة المحمولة لإزالة التطبيق من عليها في وقت واحد.

4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.

5. في النافذة **أوامر إدارة جهاز المحمول**، انتقل إلى القسم **إزالة التطبيق** وانقر فوق الزر **إرسال أمر**.
   يمكنك أيضًا إرسال الأمر إلى الجهاز المحمول عن طريق تحديد **كل الأوامر** في قائمة السياق للجهاز المحمول، ثم **إزالة التطبيق**.
   تفتح النافذة **إزالة تطبيقات** بحيث تعرض قائمة بالتطبيقات.

6. حدد من القائمة التطبيق الذي تحتاج إلى إزالته من على الجهاز المحمول. يمكنك تحديد العديد من التطبيقات لإزالتها في وقت واحد. لتحديد مجموعة من التطبيقات، استخدم المفتاح **Shift**. للجمع بين التطبيقات في مجموعة، استخدم المفتاح **Ctrl**.

7. انقر فوق الزر**موافق** لإرسال الأمر إلى الجهاز المحمول.
   عند تنفيذ الأمر، سوف يتم إزالة التطبيق المحدد من على جهاز محمول المستخدم. إذا تم تنفيذ الأمر بنجاح، ستظهر الحالة الحالية للأمر على النحو مكتمل.
   يمكنك النقر فوق الزر **إعادة إرسال** لإرسال الأمر إلى جهاز محمول المستخدم مرة أخرى.
   يمكنك النقر فوق الزر **إزالة من قائمة الانتظار** لإلغاء تنفيذ أمر تم إرساله إذا لم يتم تنفيذ الأمر بعد.
   يعرض القسم **سجل الأمر** الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق **تحديث** لتحديث قائمة الأوامر.

8. انقر فوق **موافق** لإغلاق النافذة **أوامر إدارة جهاز المحمول**.

تكوين التجوال على جهاز محمول iOS MDM

لتكوين التجوال:

1. في شجرة وحدة التحكم، افتح مجلد **إدارة الجهاز المحمول**.

2. في المجلد **إدارة الجهاز المحمول**، حدد المجلد الفرعي **الأجهزة المحمولة**.
   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

3. حدد جهاز iOS MDM الذي يملكه المستخدم والذي يتعين عليك تكوين التجوال له.
   يمكنك تحديد العديد من الأجهزة المحمولة لتكوين التجوال عليها في وقت واحد.

4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.

5. في النافذة **أوامر إدارة جهاز المحمول**، انتقل إلى القسم **تكوين التجوال** وانقر فوق الزر **إرسال أمر**.
   كما يمكنك إرسال الأمر إلى الجهاز المحمول عن طريق تحديد **كل الأوامر** > **تكوين التجوال** من قائمة السياق الخاصة بالجهاز.

6. في نافذة **إعدادات التجوال**، حدد الإعدادات ذات الصلة:

- **تمكين تجوال البيانات**

إذا تم تمكين هذا الخيار، فسيتم تمكين تجوال البيانات على الجهاز المحمول الذي يعمل بنظام iOS MDM. يمكن لمستخدم الجهاز المحمول الذي يعمل بنظام iOS MDM تصفح الإنترنت أثناء التجوال.

يتم تعطيل هذا الخيار افتراضيًا.

يتم تكوين التجوال للأجهزة المحددة.

عرض معلومات حول جهاز iOS MDM

لعرض معلومات حول جهاز iOS MDM:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.
   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.
2. في مساحة العمل، قم بتصفية أجهزة iOS MDM عن طريق النقر على الرابط **iOS MDM**.
3. حدد الجهاز المحمول الذي ترغب في عرض معلومات عنه.
4. من قائمة سياق الجهاز المحمول، حدد **خصائص**.
   تفتح نافذة خصائص جهاز iOS MDM.

تعرض نافذة خصائص الجهاز المحمول معلومات حول جهاز iOS MDM المتصل.

قطع اتصال جهاز iOS MDM من الإدارة

لقطع اتصال جهاز iOS MDM من خادم إدارة iOS MDM:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.
   تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.
2. في مساحة العمل، قم بتصفية أجهزة iOS MDM عن طريق النقر على الرابط **iOS MDM**.
3. حدد الجهاز المحمول الذي يجب قطع الاتصال عنه.
4. من قائمة سياق الجهاز المحمول، حدد **حذف**.

سيتم تمييز الجهاز iOS MDM في قائمة الإزالة. سيتم إزالة الجهاز تلقائيًا من قائمة الأجهزة المدارة عقب إزالة السابق من قاعدة بيانات خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. ستتم إزالة الجهاز المحمول من قاعدة بيانات خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في غضون دقيقة واحدة.

عقب قطع اتصال جهاز iOS MDM من الإدارة، ستتم إزالة من الجهاز المحمول جميع ملفات تعريف التكوين المثبتة وملفات تعريف iOS MDM والتطبيقات التي تم تمكين خيار **إزالة مع ملف تعريف iOS MDM** لها.

إرسال الأوامر إلى جهاز

لإرسال أمر إلى جهاز iOS MDM:

1. في وحدة تحكم الإدارة، افتح العقدة **إدارة الجهاز المحمول**.
2. حدد المجلد **الأجهزة المحمولة**.
3. في المجلد **الأجهزة المحمولة**، حدد الجهاز المحمول الذي تريد إرسال الأمر إليه.
4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.
5. في القائمة التي تظهر، حدد الأمر الذي سيتم إرساله إلى الجهاز المحمول.

التحقق من حالة تنفيذ الأوامر التي تم إرسالها

للتحقق من حالة تنفيذ أمر تم إرساله إلى جهاز محمول:

1. في وحدة تحكم الإدارة، افتح العقدة **إدارة الجهاز المحمول**.
2. حدد المجلد **الأجهزة المحمولة**.
3. في المجلد **الأجهزة المحمولة**، حدد الجهاز المحمول الذي سيتم التحقق من حالة تنفيذ الأوامر المحددة عليه.
4. من قائمة سياق الجهاز المحمول، حدد **إظهار سجل الأمر**.

إدارة أجهزة KES

في Kaspersky Security Center، يمكنك إدارة أجهزة KES المحمولة بالطرق التالية:

- إدارة أجهزة KES مركزيًا عبر استخدام الأوامر.
- عرض معلومات حول إعدادات إدارة أجهزة KES.
- تثبيت التطبيقات باستخدام حزم التطبيق المحمول.
- قطع اتصال أجهزة KES من الإدارة.

إنشاء حزمة تطبيقات محمولة لأجهزة KES

يلزم ترخيص Kaspersky Endpoint Security for Android للأجهزة المحمولة لإنشاء حزمة تطبيق محمول لأجهزة KES.

لإنشاء حزمة تطبيقات محمول:

1. في المجلد **التثبيت عن بُعد** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **حزم التثبيت**.
   إن المجلد **التثبيت عن بُعد** هو مجلد فرعي من المجلد **خيارات متقدمة** بشكل افتراضي.

2. انقر على زر **إجراءات إضافية** وحدد **إدارة حزم تطبيقات محمولة** في القائمة المنسدلة.

3. في نافذة **إدارة حزمة تطبيقات محمولة** انقر على الزر **جديد** .

4. يبدأ معالج الحزمة الجديدة. اتبع إرشادات المعالج.

يتم عرض حزمة تطبيقات المحمول التي تم إنشاؤها حديثًا في النافذة **إدارة حزمة تطبيقات محمولة**.

تمكين المصادقة القائمة على الشهادة لأجهزة KES

لتمكين المصادقة القائمة على الشهادة لأجهزة KES:

1. افتح سجل النظام الخاص بالجهاز العميل المثبت عليه خادم الإدارة (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** > تشغيل).

2. انتقل إلى الخلية التالية:

- لأنظمة 32 بت:

KLLIM\independent.\core.\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE

- لأنظمة 64 بت:

ndependent.\core.\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE

3. قن بإنشاء مفتاح بالاسم LP_MobileMustUseTwoWayAuthOnPort13292.

4. حدد REG_DWORD كنوع المفتاح.

5. قم بتعيين قيمة المفتاح 1.

6. قم بإعادة تشغيل خدمة خادم الإدارة.

سيتم تمكين المصادقة الإلزامية القائمة على الشهادة لجهاز KES باستخدام شهادة مشتركة بعد تشغيل خدمة خادم الإدارة.

لا يتطلب الاتصال الأول لجهاز KES بخادم الإدارة شهادة.

بشكل افتراضي، تكون المصادقة الثنائية لأجهزة KES معطلة.

عرض معلومات حول جهاز KES

لعرض معلومات حول جهاز KES:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة KES بحسب نوع بروتوكول (KES).

3. حدد الجهاز المحمول الذي ترغب في عرض معلومات عنه.

4. من قائمة سياق الجهاز المحمول، حدد **خصائص**.

يتم فتح نافذة خصائص جهاز KES.

تعرض نافذة خصائص الجهاز المحمول معلومات حول جهاز KES المتصل.

قطع اتصال جهاز KES بالإدارة

لقطع اتصال جهاز KES بالإدارة، يجب على المستخدم إزالة عميل الشبكة من الجهاز المحمول. بعد قيام المستخدم بإزالة عميل الشبكة، يتم إزالة تفاصيل الجهاز المحمول من قاعدة بيانات خادم الإدارة، ويتمكن المسؤول من إزالة الجهاز المحمول من قائمة الأجهزة المدارة.

لإزالة جهاز KES من قائمة الأجهزة المدارة:

1. في مجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.

تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة KES بحسب نوع بروتوكول (KES).

3. حدد الجهاز المحمول الذي يجب قطع اتصاله بالإدارة.

4. من قائمة سياق الجهاز المحمول، حدد **حذف**.

يتم إزالة الجهاز المحمول من قائمة الأجهزة المدارة.

إذا لم يتم إزالة Kaspersky Endpoint Security for Android من الجهاز، يعود الجهاز المحمول للظهور في قائمة الأجهزة المدارة بعد المزامنة مع خادم الإدارة.

تشفير البيانات وحمايتها

يقلل تشفير البيانات من مخاطر تسرب البيانات غير المقصود في حالة سرقة دفتر الملاحظات أو محرك الأقراص القابل للإزالة أو محرك الأقراص الثابتة، أو في حالة فقدانه أو الوصول غير المصرح به من قِبل المستخدمين والتطبيقات.

يوفر Kaspersky Endpoint Security for Windows وظائف التشفير. يتيح لك Kaspersky Endpoint Security for Windows تشفير الملفات المخزنة على محركات أقراص الجهاز المحلية ومحركات الأقراص القابلة للإزالة وكذلك تشفير محركات الأقراص القابلة للإزالة ومحركات الأقراص الثابتة بشكل كامل.

يتم تكوين قواعد التشفير باستخدام Kaspersky Security Center من خلال تحديد السياسات. يتم تنفيذ التشفير وفك التشفير وفقًا للقواعد الحالية عند تطبيق سياسة.

يتم تحديد توفر ميزة إدارة التشفير بواسطة إعدادات واجهة المستخدم.

يمكن للمسؤول القيام بالإجراءات التالية:

- تكوين تشفير الملف أو فك تشفيره وتنفيذ ذلك على محركات الأقراص المحلية للجهاز.
- تكوين تشفير الملفات على محركات الأقراص القابلة للإزالة وتنفيذه.

- إنشاء قواعد وصول إلى الملفات المشفرة.
- إنشاء ملف مفتاح وتقديمه للمستخدم للوصول إلى الملفات المشفرة إذا تم تقييد تشفير الملفات على جهاز المستخدم.
- تكوين تشفير محرك القرص الثابت وتنفيذه.
- إدارة وصول المستخدم إلى محركات الأقراص الثابتة ومحركات الأقراص القابلة للإزالة المشفرة (إدارة حسابات وكيل المصادقة وإنشاء معلومات للمستخدمين وتقديمها عند طلب اسم الحساب واستعادة كلمة المرور، بالإضافة إلى مفاتيح الوصول للأجهزة المشفرة).
- عرض حالات التشفير وتقارير حول تشفير الملفات.

يتم إجراء هذه العمليات باستخدام أدوات مدمجة في Kaspersky Endpoint Security for Windows. للحصول على إرشادات مفصلة حول كيفية تنفيذ العمليات وتوضيح لمزايا التشفير، يرجى الرجوع إلى التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows.

يدعم Kaspersky Security Center وظائف إدارة التشفير للأجهزة التي تعمل بأنظمة تشغيل macOS. يتم تكوين التشفير باستخدام Kaspersky Endpoint Security 10 Mac tools لإصدارات التطبيق هذه التي تدعم وظائف التشفير. للحصول على تعليمات تفصيلية حول كيفية تنفيذ العمليات ووصف ميزات التشفير، يُرجى الرجوع إلى دليل مسؤول Kaspersky Endpoint Security for Mac.

عرض قائمة بالأجهزة المشفرة

لعرض قائمة بالأجهزة التي تقوم بتخزين المعلومات المشفرة:

1. في شجرة وحدة التحكم الخاصة بخادم الإدارة، حدد المجلد **تشفير البيانات وحمايتها**.
2. افتح قائمة الأجهزة المشفرة بأحد الطرق التالية:
   - بالنقر فوق الرابط **انتقل إلى قائمة محركات الأقراص المشفرة** في القسم **إدارة محركات الأقراص المشفرة**.
   - عن طريق تحديد المجلد **برامج التشغيل المشفرة** في شجرة وحدة التحكم.

تعرض مساحة العمل معلومات حول الأجهزة الموجودة على الشبكة والتي تقوم بتخزين الملفات المشفرة، وحول الأجهزة المشفرة على مستوى برنامج التشغيل. بعد تشفير المعلومات على جهاز، يتم إزالة الجهاز تلقائيًا من القائمة.

يمكنك فرز المعلومات في قائمة الأجهزة بترتيب تصاعدي أو تنازلي في أي عمود.

تحدد إعدادات واجهة المستخدم ما إذا كان المجلد **تشفير البيانات وحمايتها** سيظهر في شجرة وحدة التحكم.

عرض قائمة بأحداث التشفير

عند تشغيل مهام تشفير البيانات أو فك تشفيرها على الأجهزة، يرسل Kaspersky Endpoint Security for Windows معلومات حول أحداث الأنواع التالية إلى Kaspersky Security Center:

- يتعذر تشفير ملف أو فك تشفيره، أو إنشاء أرشيف مشفر نظرًا لفقدان مساحة فارغة على القرص.
- يتعذر تشفير ملف أو فك تشفيره، أو إنشاء أرشيف مشفر نظرًا لمشكلات الترخيص.
- يتعذر تشفير ملف أو فك تشفيره، أو إنشاء أرشيف مشفر نظرًا لفقدان حقوق الوصول.

- تم منع التطبيق من الوصول إلى ملف مشفر.
- أخطاء غير معروفة.

لعرض قائمة بالأحداث التي وقعت أثناء تشفير البيانات على الأجهزة:

1. في شجرة وحدة التحكم الخاصة بخادم الإدارة، حدد المجلد **تشفير البيانات وحمايتها**.
2. افتح قائمة الأحداث التي وقعت أثناء التشفير، بإحدى الطرق التالية:
   - بالنقر على رابط **الانتقال إلى قائمة الأخطاء** في قسم **أخطاء تشفير البيانات**.
   - عن طريق تحديد المجلد **برامج التشغيل المشفرة** في شجرة وحدة التحكم.

تعرض مساحة العمل معلومات حول المشاكل التي حدثت أثناء تشفير البيانات على الأجهزة.

يمكنك أخذ الإجراءات التالية في قائمة أحداث التشفير:

- فرز سجلات البيانات بالترتيب التصاعدي أو التنازلي في أي عمود من الأعمدة.
- قم تنفيذ بحث سريع للسجلات (عن طريق مطابقة نص مع سلسلة فرعية في أي من حقول القائمة).
- تصدير قائمة أحداث إلى ملف نص.

تحدد إعدادات واجهة المستخدم ما إذا كان المجلد **تشفير البيانات وحمايتها** سيظهر في شجرة وحدة التحكم.

تصدير قائمة بأحداث التشفير إلى ملف نص

لتصدير قائمة بأحداث التشفير إلى ملف نص:

1. إنشاء قائمة بأحداث التشفير.
2. من قائمة السياق الخاصة بقائمة الأحداث، حدد **تصدير القائمة**.
   يتم فتح نافذة **تصدير القائمة**.
3. من النافذة **تصدير القائمة**، حدد اسم ملف النص مع قائمة الأحداث، وحدد مجلدًا لحفظه وانقر فوق الزر **حفظ**.
   سيتم حفظ قائمة أحداث التشفير على الملف المحدد.

إنشاء تقارير التشفير وعرضها

يمكنك إنشاء التقارير التالية:

- Report on encryption status of managed devices. يقدم هذا التقرير تفاصيل حول تشفير البيانات لمختلف الأجهزة المدارة. على سبيل المثال، يعرض التقرير عدد الأجهزة التي تنطبق عليها السياسة مع قواعد التشفير المكونة. يمكنك أيضًا معرفة، على سبيل المثال، عدد الأجهزة التي تحتاج إلى إعادة التشغيل. يحتوي التقرير أيضًا على معلومات حول تقنية التشفير وخوارزمية كل جهاز.
- Report on encryption status of mass storage devices. يحتوي هذا التقرير على معلومات مماثلة للتقرير عن حالة تشفير الأجهزة المُدارة، ولكنه يوفر البيانات فقط لأجهزة التخزين كبير السعة ومحركات الأقراص القابلة للإزالة.

- Report on rights to access encrypted drives. يوضح هذا التقرير حسابات المستخدمين التي لها حق الوصول إلى محركات الأقراص المشفرة.
- Report on file encryption errors. يحتوي هذا التقرير على معلومات حول الأخطاء التي حدثت عند تشغيل مهام تشفير البيانات أو فك تشفيرها على الأجهزة.
- Report on blockage of access to encrypted files. يحتوي هذا التقرير على معلومات حول منع وصول التطبيق إلى الملفات المشفرة. هذا التقرير مفيد إذا حاول مستخدم أو تطبيق غير مصرح له الوصول إلى الملفات أو محركات الأقراص المشفرة.

لإنشاء تقرير حول تشفير الأجهزة:

1. في شجرة وحدة التحكم، حدد مجلد **تشفير البيانات وحمايتها**.
2. قم بأحد الإجراءات التالية:
   - لإنشاء التقرير حول حالة تشفير الأجهزة المُدارة، انقر فوق الرابط **عرض تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة**.
     إذا لم تكن قد قمت بتكوين هذا التقرير بعد، سيبدأ معالج قالب التقرير الجديد. اتبع خطوات المعالج.
   - لإنشاء تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة حدد في شجرة وحدة التحكم المجلد الفرعي **برامج التشغيل المشفرة** ثم انقر فوق الزر **عرض تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة**.

يبدأ إنشاء التقرير. يتم عرض التقرير على علامة تبويب **التقارير** الخاصة بالعقدة **خادم الإدارة**.

لإنشاء تقرير حول حقوق الوصول إلى الأجهزة المشفرة:

1. في شجرة وحدة التحكم، حدد مجلد **تشفير البيانات وحمايتها**.
2. قم بأحد الإجراءات التالية:
   - انقر فوق رابط **الإبلاغ عن حقوق الوصول إلى برامج التشغيل المشفرة** في قسم **إدارة محركات الأقراص المشفرة** لبدء معالج قالب التقرير الجديد.
   - حدد المجلد الفرعي **برامج التشغيل المشفرة**، ثم انقر فوق زر **الإبلاغ عن حقوق الوصول إلى برامج التشغيل المشفرة** لبدء معالج قالب التقرير الجديد.
3. اتبع خطوات معالج قالب التقرير الجديد.

يبدأ إنشاء التقرير. يتم عرض التقرير على علامة تبويب **التقارير** الخاصة بالعقدة **خادم الإدارة**.

لإنشاء تقرير حول أخطاء تشفير الملف:

1. في شجرة وحدة التحكم، حدد مجلد **تشفير البيانات وحمايتها**.
2. قم بأحد الإجراءات التالية:
   - انقر فوق الرابط **عرض تقرير حول أخطاء تشفير الملف** في القسم **أخطاء تشفير البيانات** لبدء تشغيل معالج قالب التقرير الجديد.
   - حدد المجلد الفرعي **أحداث التشفير**، ثم انقر فوق الرابط **تقرير حول أخطاء تشفير الملفات** لبدء تشغيل معالج قالب التقارير الجديد.
3. اتبع خطوات معالج قالب التقرير الجديد.

يبدأ إنشاء التقرير. يتم عرض التقرير على علامة تبويب **التقارير** الخاصة بالعقدة **خادم الإدارة**.

لإنشاء تقرير حول حالة تشفير الأجهزة المُدارة:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .

3. انقر فوق الزر **قالب التقرير الجديد** لتشغيل معالج قالب التقرير الجديد.

4. اتبع تعليمات معالج قالب التقرير الجديد. في النافذة **تحديد نوع قالب التقرير**، حدد **تقرير حول حالة تشفير الأجهزة المُدارة** في القسم **غير ذلك**.
بعد الانتهاء من معالج قالب التقرير الجديد، يظهر قالب تقرير جديد في عقدة خادم الإدارة في علامة التبويب **التقارير**.

5. في عقدة خادم الإدارة ذي الصلة على علامة التبويب **التقارير**، حدد قالب التقارير الذي تم إنشاؤه أثناء خطوات التعليمات السابقة.

يبدأ إنشاء التقرير. يتم عرض التقرير على علامة تبويب **التقارير** الخاصة بالعقدة **خادم الإدارة**.

يمكنك أيضًا الحصول على معلومات حول ما إذا كانت حالات تشفير الأجهزة ومحركات الأقراص القابلة للإزالة تتوافق مع سياسة التشفير عن طريق عرض أجزاء المعلومات على علامة التبويب **الإحصاءات** الخاصة بعقدة خادم الإدارة.

لإنشاء تقرير حول حجب الوصول إلى الملفات المشفرة:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.

2. في مساحة عمل العقدة، حدد علامة تبويب **التقارير** .

3. انقر فوق الزر **قالب التقارير الجديد** لبدء تشغيل معالج قالب التقرير الجديد.

4. اتبع تعليمات معالج قالب التقرير الجديد. في النافذة **تحديد نوع قالب التقرير**، حدد **تقرير حول حجب الوصول إلى الملفات المشفرة** في القسم **غير ذلك**.
بعد انتهاء معالج قالب تقرير جديد، يظهر قالب تقارير جديد في القسم **خادم الإدارة**، في علامة التبويب **التقارير**.

5. في عقدة **خادم الإدارة** على علامة التبويب **التقارير**، حدد قالب التقارير الذي تم إنشاؤه أثناء خطوات التعليمات السابقة.

يبدأ إنشاء التقرير. يتم عرض التقرير على علامة تبويب **التقارير** الخاصة بالعقدة **خادم الإدارة**.

نقل مفاتيح التشفير بين خوادم الإدارة

إذا تم تمكين ميزة تشفير البيانات على جهاز مدار، يتم تخزين مفتاح التشفير المطلوب على خادم الإدارة. يتم استخدام مفتاح التشفير للوصول إلى البيانات المشفرة وإدارة سياسة التشفير.

يجب إرسال مفتاح التشفير إلى خادم إدارة آخر في الحالات التالية:

- إذا قمت بإعادة تكوين Network Agent على جهاز مُدار لتعيين الجهاز لخادم إدارة آخر. إذا كان هذا الجهاز يحتوي على بيانات مشفرة، فيجب إرسال مفتاح التشفير إلى خادم الإدارة الهدف. خلاف ذلك، لا يمكن فك تشفير البيانات.

- إذا كنت تقوم بتشفير محرك أقراص قابل للإزالة متصل بجهاز D1 تتم إدارته بواسطة خادم الإدارة S1، ثم تقوم بتوصيل محرك الأقراص القابل للإزالة بجهاز D2 يديره خادم الإدارة S2. للوصول إلى البيانات الموجودة على محرك الأقراص القابل للإزالة، يجب إرسال مفتاح التشفير من خادم الإدارة S1 إلى خادم الإدارة S2.

- تقوم بتشفير ملف على جهاز D1 تتم إدارته بواسطة خادم الإدارة S1، ثم تحاول الوصول إلى الملف على جهاز D2 يديره خادم الإدارة S2. للوصول إلى الملف، يجب إرسال مفتاح التشفير من خادم الإدارة S1 إلى خادم الإدارة S2.

يمكنك نقل مفاتيح التشفير بالطرق التالية:

- تلقائيًا، من خلال تمكين الخيار **استخدام التسلسل الهرمي لخوادم الإدارة للحصول على مفاتيح التشفير** في خصائص خادميّ الإدارة الاثنين الذين يجب نقل مفتاح التشفير بينهما. إذا تم تعطيل هذا الخيار لأحد خوادم الإدارة، فإن النقل التلقائي لمفاتيح التشفير لا يكون ممكنًا.

  عند تمكين خيار **استخدام التسلسل الهرمي لخوادم الإدارة للحصول على مفاتيح التشفير** في إحدى خصائص خادم الإدارة، فإن خادم الإدارة يرسل جميع مفاتيح التشفير المخزنة في المستودع الخاص به إلى خادم الإدارة الرئيسي (إن وجد) على مستوى أعلى في التسلسل الهرمي.

  عند محاولة الوصول إلى البيانات المشفرة، يبحث "خادم الإدارة" أولاً عن مفتاح التشفير في المستودع الخاص به. في حالة تمكين خيار **استخدام التسلسل الهرمي لخوادم الإدارة للحصول على مفاتيح التشفير** ولم يتم العثور على مفتاح التشفير المطلوب في المستودع، كما يقوم خادم الإدارة بإرسال طلب إلى خوادم الإدارة الأساسية (إن وجدت) لتوفير مفتاح التشفير المطلوب. سيتم إرسال الطلب إلى جميع خوادم الإدارة الأساسية حتى إلى الخادم على أعلى مستوى من التسلسل الهرمي.

لا يتوفر الخيار **استخدام التسلسل الهرمي لخوادم الإدارة للحصول على مفاتيح التشفير** في واجهة Web Console. إذا لم يكن لديك وصول إلى وحدة تحكم الإدارة المستندة إلى MMC، فاستخدم خادم الإدارة الأساسي لإدارة الأجهزة المشفرة.

- يدوياً من خادم إدارة واحد إلى آخر عن طريق تصدير واستيراد الملف الذي يحتوي على مفاتيح التشفير.

  يعد تصدير مفاتيح التشفير واستيرادها من الإجراءات المضمنة في ميزة إدارة مفتاح التشفير. للقيام بهذه الإجراءات، قم بتكوين حقوق الوصول لميزة مستخدمي Kaspersky Security Center على النحو التالي:

  - امنح **قراءة** حق الوصول إلى ميزة إدارة مفتاح التشفير لمستخدم يقوم بتصدير مفاتيح التشفير من خادم الإدارة الثانوي.
  - امنح حق الوصول **للكتابة** إلى ميزة إدارة مفتاح التشفير للمستخدم الذي يستورد مفاتيح التشفير إلى خادم الإدارة المستهدف.

لتمكين النقل التلقائي لمفاتيح التشفير بين خوادم الإدارة داخل التسلسل الهرمي:

1. في شجرة وحدة التحكم، حدد خادم الإدارة الذي ترغب في أن تقوم بتمكين النقل التلقائي لمفاتيح التشفير له.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة الخصائص، حدد قسم **خوارزمية التشفير**.
4. تمكين خيار **استخدام التسلسل الهرمي لخوادم الإدارة للحصول على مفاتيح التشفير**.
5. انقر فوق **موافق** لتطبيق التغييرات.

سيتم نقل مفاتيح التشفير إلى خوادم الإدارة الأساسية (إن وجدت) في المزامنة التالية (التزامن الدوري). سيوفر خادم الإدارة هذا أيضًا، عند الطلب، مفتاح تشفير من المستودع الخاص به إلى خادم الإدارة الثانوي.

لنقل مفاتيح التشفير بين خوادم الإدارة يدويًا:

1. في شجرة وحدة التحكم لخادم الإدارة، حدد خادم الإدارة الثانوي الذي تريد منه نقل مفاتيح التشفير.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة الخصائص، حدد قسم **خوارزمية التشفير**.
4. انقر على **تصدير مفاتيح التشفير من خادم الإدارة**.

   تأكد من منح المستخدم الذي يقوم بتصدير مفاتيح التشفير من الخادم حق الوصول **قراءة** ميزة إدارة مفتاح التشفير.

5. في نافذة **تصدير مفاتيح التشفير**:

- انقر على زر **استعراض**، ثم حدد مكان حفظ الملف.
- حدد كلمة مرور لحماية الملف من الوصول غير المصرح به.

تذكر كلمة المرور. لا يمكن استرداد كلمة مرور مفقودة. في حالة فقدان كلمة المرور، يجب عليك تكرار إجراء التصدير. لذلك، قم بتدوين كلمة المرور واحتفظ بها في متناول يديك.

6. انقل الملف إلى خادم إدارة آخر، على سبيل المثال، عبر مجلد مشترك أو محرك أقراص قابل للإزالة.

7. على خادم الإدارة الهدف، تأكد من تشغيل وحدة تحكم إدارة Kaspersky Security Center.

8. في شجرة وحدة التحكم في خادم الإدارة، حدد خادم الإدارة الهدف حيث تريد نقل مفاتيح التشفير إليه.

9. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

10. في نافذة الخصائص، حدد قسم **خوارزمية التشفير**.

11. انقر على **باستيراد مفاتيح التشفير إلى خادم الإدارة**.

تأكد من منح المستخدم الذي يستورد مفاتيح التشفير إلى الخادم حق وصول **الكتابة** إلى ميزة إدارة مفتاح التشفير.

12. في نافذة **استيراد مفاتيح التشفير**:

- انقر على زر **استعراض**، ثم حدد الملف الذي يحتوي على مفاتيح التشفير.
- حدد كلمة المرور.

13. انقر فوق **موافق**.

يتم نقل مفاتيح التشفير إلى خادم الإدارة الهدف.

مستودعات البيانات

يقدم هذا القسم معلومات عن البيانات المخزَّنة على خادم الإدارة والمستخدمة لتعقب حالة الأجهزة العميلة وخدمتها.

يعرض المجلد **المستودعات** من شجرة وحدة التحكم البيانات المستخدمة لتتبع حالات الأجهزة العميلة.

يحتوي المجلد **المستودعات** على الكائنات التالية:

- التحديثات التي تم تنزيلها بواسطة خادم الإدارة والتي يتم توزيعها على الأجهزة العميلة.
- قائمة الأجهزة التي تم اكتشافها على الشبكة.
- المفاتيح التي تم اكتشافها على أجهزة العملاء.
- الملفات التي تم وضعها في مجلدات العزل على الأجهزة بواسطة تطبيقات الأمن.
- الملفات الموضوعة في النسخ الاحتياطي على الأجهزة العميلة.
- الملفات التي تأجل فحصها بواسطة تطبيقات الأمن.

تصدير قائمة كائنات المستودع إلى ملف نص

يمكنك تصدير ملف الكائنات من المستودع إلى ملف نص.

لتصدير قائمة الكائنات من المستودع إلى ملف نص:

1. في شجرة وحدة التحكم، في المجلد **المستودعات** حدد المجلد الفرعي للمستودع ذي الصلة.

2. في المجلد الفرعي للمستودع، حدد **تصدير قائمة** في قائمة السياق.

سيفتح ذلك النافذة **تصدير قائمة**، التي يمكنك أن تحدد فيها اسم ملف النص والمسار إلى المجلد الذي تم توضع فيه.

حزم التثبيت

يضع Kaspersky Security Center حزم تثبيت تطبيقات Kaspersky وبائعي الجهات الخارجية في مستودعات البيانات.

حزمة التثبيت هي مجموعة من الملفات المطلوب تثبيتها على أي تطبيق. تحتوي حزمة التثبيت على إعدادات الإعداد والتكوين الأولي للتطبيق الجاري تثبيته.

إذا كنت ترغب في تثبيت تطبيق على جهاز عميل، عليك إنشاء حزمة تثبيت له أو استخدام حزمة موجودة. يتم تخزين قائمة حزم التثبيت التي تم إنشاؤها في المجلد **التثبيت عن بُعد** بشجرة وحدة التحكم، في المجلد الفرعي **حزم التثبيت**.

الحالات الرئيسية للملفات الموجودة في المستودع

تفحص تطبيقات الأمان الملفات على الأجهزة للكشف عن الفيروسات المعروفة وبرامج أخرى قد تشكل خطرًا، وتعيّن الحالات إلى الملفات، وتضع بعضها في المستودع.

على سبيل المثال, تقوم تطبيقات الأمان بالتالي:

- تحفظ نسخه من ملف في المستودع قبل حذفه.
- عزل الملفات المحتمل إصابتها في المستودع

توجد الحالات الرئيسية للملفات في الجدول الموجود أدناه. يمكنك الحصول على معلومات أكثر تفصيلاً عن الإجراءات المطلوبة بشأن الملفات في التطبيقات الخاصة بأنظمة التعليمات الخاصة بالأمن.

حالات الملفات في المستودع

اسم الحالة	وصف الحالة
مصاب	يحتوي الملف على قسم برموز الفيروسات المعروفة أو البرامج الضارة الأخرى التي توجد معلومات عنها في قواعد بيانات مكافحة الفيروسات الخاصة بـ Kaspersky.
غير مصاب	لم يتم الكشف عن فيروسات أو برامج ضارة أخرى معروفة في الملف.
تحذير	يحتوي الملف على جزء من رمز يتوافق جزئيًا مع قصاصة برمجية لتهديد معروف.
محتمل الإصابة	يحتوي الملف على إما رمز مُعدل لفيروس معروف أو رمز يشبه فيروس غير معروف حتى الآن لـ Kaspersky.
تم وضعه في مجلد بواسطة المستخدم	وضع المستخدم الملف يدويًا في المستودع لأن سلوك الملف يبعث على الشك باحتوائه على بعض التهديدات. يمكن للمستخدم فحص الملف بحثًا عن التهديدات عن طريق استخدام قواعد بيانات حديثة.
اكتشافات إيجابية زائفة	لقد عين أحد تطبيقات Kaspersky الحالة المصابة إلى ملف غير مصاب وذلك لأن رمزه مشابه لرمز الفيروس. بعد الفحص باستخدام قواعد بيانات حديثة، يتم تحديد الملف باعتباره غير مصاب.
تم التنظيف	تم تنظيف الملف بنجاح.

اسم الحالة	وصف الحالة
تم الحذف	تم حذف الملف أثناء المعالجة.
محمي بكلمة مرور	يتعذر معالجة الملف لأنه محمي بكلمة مرور.

تفعيل القواعد في وضع التدريب الذكي

يوفر هذا القسم معلومات حول عمليات الكشف التي تم إجراؤها بواسطة قواعد مراقبة عيوب التكيف في برنامج Kaspersky Endpoint Security for Windows على الأجهزة العميلة.

تقوم القواعد باكتشاف السلوك المخالف على الأجهزة العميلة وقد تقوم بحظره. إذا كانت القواعد سارية في وضع التدريب الذكي، فإنها تقوم باكتشاف السلوك المخالف وإرسال تقارير بشأن كل حالة يحدث فيها مثل هذا السلوك لخادم إدارة Kaspersky Security Center. يتم تخزين هذه المعلومات كقائمة في المجلد الفرعي **يتم تشغيل القاعدة في حالة التدريب الذكي** للمجلد **المستودعات**. يمكنك تأكيد عمليات الكشف باعتبارها صحيحة أو إضافتها باعتبارها استثناءات، حتى لا يتم اعتبار هذا النوع من السلوك مخالفًا بعد الآن.

يتم تخزين معلومات حول عمليات الكشف في سجل الأحداث على خادم الإدارة (مع أحداث أخرى) وفي تقرير مراقبة عيوب التكيف.

لمزيد من المعلومات حول مراقبة عيوب التكيف والقواعد وأوضاعها وحالاتها يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security for Windows.

عرض قائمة بعمليات الكشف التي تم إجراؤها باستخدام قواعد مراقبة عيوب التكيف

قم بما يلي لعرض قائمة بعمليات الكشف التي تم إجراؤها باستخدام قواعد مراقبة عيوب التكيف:

1. حدد من شجرة وحدة التحكم عقدة خادم الإدارة الذي تطلبه.
2. حدد المجلد الفرعي **يتم تشغيل القاعدة في حالة التدريب الذكي** (بشكل افتراضي، يصبح هذا المجلد الفرعي لـ **خيارات متقدمة** ← **المستودعات**).

تعرض القائمة المعلومات التالية بشأن عمليات الكشف التي تم إجراؤها باستخدام قواعد مراقبة عيوب التكيف:

- **مجموعة الإدارة**

اسم مجموعة الإدارة التي ينتمي إليها الجهاز.

- **اسم الجهاز**

اسم الجهاز العميل الذي تم تطبيق القاعدة عليه.

- **الاسم**

اسم القاعدة التي تم تطبيقها.

- **الحالة**

يتم الاستثناء—إذا قام المسؤول بمعالجة هذا العنصر وإضافته باعتباره استثناءً للقواعد. تستمر هذه الحالة إلى حين إجراء المزامنة التالية للجهاز العميل مع خادم الإدارة؛ وبعد إجراء المزامنة، يختفي العنصر من القائمة.

يتم التأكيد—إذا قام المسؤول بمعالجة هذا العنصر وتأكيده. تستمر هذه الحالة إلى حين إجراء المزامنة التالية للجهاز العميل مع خادم الإدارة؛ وبعد إجراء المزامنة، يختفي العنصر من القائمة.

فارغ—إذا لم يقم المسؤول بمعالجة هذا العنصر.

- **إجمالي عدد مرات تشغيل القواعد**

عدد الاكتشافات ضمن قاعدة تجريبية واحدة، وعملية واحدة، وجهاز عميل واحد. يتم احتساب هذا العدد بواسطة Kaspersky Endpoint Security.

- **اسم المستخدم**

اسم مستخدم الجهاز العميل الذي قام بتشغيل العملية التي قامت بتوليد الكشف.

- **مسار معالجة المصدر**

المسار إلى عملية المصدر، أي العملية التي تؤدي الإجراء (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **تجزئة معالجة المصدر**

تجزئة SHA256 لملف العملية المصدر (لمزيد من المعلومات ، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **مسار كائن المصدر**

المسار إلى الكائن الذي بدأ العملية (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **تجزئة كائن المصدر**

تجزئة SHA256 لملف المصدر (لمزيد من المعلومات ، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **مسار معالجة الهدف**

المسار إلى العملية المستهدفة (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **تجزئة معالجة الهدف**

تجزئة SHA256 للملف المستهدف (لمزيد من المعلومات ، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **مسار كائن الهدف**

المسار إلى الكائن المستهدف (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **تجزئة كائن الهدف**

تجزئة SHA256 للملف المستهدف (لمزيد من المعلومات ، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

- **تمت المعالجة**

تاريخ اكتشاف العيوب.

قم بما يلي لعرض خصائص كل عنصر من عناصر المعلومات:

1. حدد من شجرة وحدة التحكم عقدة خادم الإدارة الذي تطلبه.
2. حدد المجلد الفرعي **يتم تشغيل القاعدة في حالة التدريب الذكي** (بشكل افتراضي، يصبح هذا المجلد الفرعي لـ **خيارات متقدمة** ← **المستودعات**).
3. في مساحة عمل **يتم تشغيل القاعدة في حالة التدريب الذكي**، حدد الكائن الذي تريده.
4. قم بأحد الإجراءات التالية:

- انقر فوق رابط **خصائص** في خانة المعلومات التي تظهر على الجانب الأيمن من الشاشة.
- انقر بزر الماوس الأيمن، وحدد **خصائص** من قائمة السياق.

يتم فتح نافذة خصائص الكائن، حيث تعرض معلومات عن العنصر المحدد.

يمكنك التأكيد أو الإضافة إلى الاستثناءات أي عنصر في قائمة عمليات الكشف الخاصة بقواعد مراقبة عيوب التكيف.

لتأكيد عنصر ما،

حدد أحد العناصر (أو عدة عناصر) في قائمة عمليات الكشف وانقر فوق زر **تأكيد**.

سيتم تغيير حالة العنصر (العناصر) إلى **جار التأكيد**.

سوف يساهم التأكيد الخاص بك في الإحصائيات التي تستخدمها القواعد (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security 11 for Windows).

لإضافة عنصر ما كاستثناء،

انقر بزر الماوس الأيمن فوق أحد العناصر (أو عدة عناصر) في قائمة عمليات الكشف وحدد **إضافة إلى الاستثناءات** من قائمة السياق.

يبدأ تشغيل معالج إضافة الإستثناءات. اتبع تعليمات المعالج.

إذا قمت برفض أو تأكيد عنصر ما، فسيتم استثناؤه من قائمة عمليات الكشف بعد إجراء عملية المزامنة التالية للجهاز العميل المزود بخادم الإدارة، ولن يظهر في القائمة بعد الآن.

إضافة استثناءات من قواعد مراقبة عيوب التكيف

يسمح لك معالج إضافة الإستثناءات بإضافة استثناءات من قواعد مراقبة عيوب التكيف لـ Kaspersky Endpoint Security.

يمكنك بدء تشغيل المعالج من خلال أحد الإجراءات الثلاثة أدناه.

لبدء معالج إضافة الإستثناءات من خلال عقدة مراقبة عيوب التكيف:

1. في شجرة وحدة التحكم، حدد عقدة خادم الإدارة المطلوب.
2. حدد **يتم تشغيل القاعدة في حالة التدريب الذكي** (بشكل افتراضي، يصبح هذا المجلد الفرعي لـ**خيارات متقدمة** ← **المستودعات**).
3. في مساحة العمل، انقر بزر الماوس الأيمن فوق أحد العناصر (أو عدة عناصر) في قائمة عمليات الكشف وحدد **إضافة إلى الاستثناءات**.

يمكنك إضافة ما يصل إلى 1000 استثناء في المرة الواحدة. إذا قمت بتحديد المزيد من العناصر وحاولت إضافتها إلى الاستثناءات، فسيتم عرض رسالة خطأ.

يبدأ تشغيل معالج إضافة الإستثناءات.

يمكنك بدء معالج إضافة الإستثناءات من العقد الأخرى في شجرة وحدة التحكم:

- **الأحداث** علامة تبويب النافذة الأساسية لخادم الإدارة (ثم الخيار **طلبات المستخدم** أو الخيار **الأحداث الأخيرة**).
- العمود **تقرير حول حالة قواعد مراقبة عيوب التكيف، عدد عمليات الكشف**.

الخطوة 1. تحديد التطبيق

يمكن تخطي هذه الخطوة إذا كان لديك إصدار واحد فقط من برنامج Kaspersky Endpoint Security for Windows وليس لديك تطبيقات أخرى تدعم قواعد مراقبة عيوب التكيف.

يعرض معالج إضافة الاستثناءات قائمة تطبيقات Kaspersky التي تسمح لك مكوناتها الإضافية للإدارة بإضافة الاستثناءات إلى السياسات المخصصة لهذه التطبيقات. حدد أحد التطبيقات من هذه القائمة وانقر فوق **التالي** للانتقال لتحديد السياسة التي ستتم إضافة الاستثناء لها.

الخطوة 2. تحديد السياسة (السياسات)

يعرض المعالج قائمة السياسات (مع ملفات تعريف السياسة) لبرنامج Kaspersky Endpoint Security.

حدد جميع السياسات وملفات التعريف التي تريد إضافة الاستثناءات لها وانقر فوق **التالي**.

الخطوة 3. معالجة السياسة (السياسات)

يعرض المعالج شريط تقدم أثناء معالجة السياسات. يمكنك مقاطعة عملية معالجة السياسات عن طريق النقر فوق **إلغاء**.

لا يمكن تحديث السياسات الموروثة. إذا لم يكن لديك الحقوق لتعديل سياسة ما، فلن يتم تحديث هذه السياسة أيضًا.

عند معالجة جميع السياسات (أو في حالة مقاطعة المعالجة)، يظهر تقرير. ويعرض أي السياسات التي تم تحديثها بنجاح (أيقونة خضراء) وأي السياسات لم يتم تحديثها (أيقونة حمراء).

هذه هي الخطوة الأخيرة من المعالج. انقر فوق **إنهاء** لإغلاق المعالج.

العزل والنسخ الاحتياطي

قد تقوم تطبيقات مكافحة الفيروسات من Kaspersky، المثبتة على الأجهزة العملاء، بوضع ملفات في العزل أو النسخ الاحتياطي أثناء فحص الجهاز.

العزل هو مستودع خاص لتخزين الملفات محتملة الإصابة بالفيروسات والملفات التي تعذر تنظيفها في وقت اكتشافها.

تم تصميم النسخ الاحتياطي لتخزين النسخ الاحتياطية من الملفات التي تم حذفها أو تعديلها أثناء عملية التنظيف.

يقوم Kaspersky Security Center بإنشاء قائمة تلخص الملفات التي تم وضعها في العزل أو النسخ الاحتياطي بواسطة تطبيقات Kasperskyالموجودة على الأجهزة. يتم من خلال عملاء الشبكة الموجودة على الأجهزة العميلة نقل المعلومات الخاصة بالملفات الموجودة في العزل والنسخ الاحتياطي إلى خادم الإدارة. يمكنك استخدام وحدة تحكم الإدارة لعرض خصائص الملفات المخزنة في المستودعات على الأجهزة، وتشغيل عمليات فحص البرامج الضارة على هذه المستودعات، وحذف الملفات منها. رموز حالات الملف موضّحة في الملحق.

يدعم Kaspersky Endpoint Security العمليات التي تتضمن العزل والنسخ الاحتياطي.

لا يتم من خلال Kaspersky Security Center نسخ الملفات من المستودعات إلى خادم الإدارة. جميع الملفات مخزنة في مستودعات على الأجهزة. يمكنك فقط استرداد ملف من جهاز مثبت عليه تطبيق مكافحة فيروسات ، والذي قام بوضع هذا الملف في المستودع.

تمكين إدارة الملفات الموجودة في المستودعات عن بُعد

لا يمكنك افتراضيًا إدارة الملفات الموجودة في المستودعات على الأجهزة العميلة.

لتمكين إدارة الملفات المخزنة في المستودعات عن بُعد على الأجهزة العميلة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي تريد لها تمكين إدارة الملفات عن بُعد في المستودع.
2. في مساحة عمل المجموعة، افتح علامة التبويب **السياسات**.
3. في علامة التبويب **السياسات**، حدد سياسة تطبيق الأمن الذي وضع الملفات في المستودعات على الأجهزة.
4. في نافذة إعدادات السياسة في مجموعة إعدادات **نقل البيانات إلى خادم الإدارة**، حدد مربعات الاختيار المقابلة للمستودعات التي تريد تمكين الإدارة عن بُعد لها.

يعتمد موقع مجموعة إعدادات **نقل البيانات إلى خادم الإدارة** في نافذة خصائص السياسة وأسماء خانات الاختيار على تطبيق الأمن المستخدم حاليًا.

عرض خصائص ملف موجود في المستودع

لعرض خصائص ملف موجود في العزل أو النسخ الاحتياطي:

1. من شجرة وحدة التحكم، حدد المجلد **المستودعات**، والمجلد الفرعي **العزل** أو **النسخ الاحتياطي**.
2. من مساحة العمل الخاصة بالمجلد **العزل** (**النسخ الاحتياطي**)، حدد الملف الذي ترغب في عرض خصائصه.
3. بتحديد **خصائص** من قائمة سياق الملف.

حذف الملفات من المستودعات

لحذف ملف من العزل أو النسخ الاحتياطي:

1. في شجرة وحدة التحكم، في مجلد **المستودعات**، حدد المجلد الفرعي **العزل** أو **النسخ الاحتياطي**.
2. من مساحة العمل الخاصة بالمجلد **العزل** (**النسخ الاحتياطي**)، حدد الملفات التي ترغب في حذفها باستخدام المفتاحين **Shift** و**Ctrl**.
3. احذف الملفات بإحدى الطرق التالية:
   - بتحديد **حذف** في قائمة سياق الملفات.
   - بالنقر فوق الرابط **حذف** (**حذف** إذا كنت ترغب في حذف ملف واحد) في خانة المعلومات الخاصة بالملفات المحددة.

ستقوم تطبيقات الأمان التي قامت بوضع الملفات في مستودعات الأجهزة العميلة بحذف الملفات نفسها من هذه المستودعات.

استعادة الملفات من المستودعات

لاستعادة ملف من العزل أو النسخ الاحتياطي:

1. من شجرة وحدة التحكم، حدد المجلد **المستودعات**، والمجلد الفرعي **العزل** أو **النسخ الاحتياطي**.
2. من مساحة العمل الخاصة بالمجلد **العزل** (**النسخ الاحتياطي**)، حدد الملفات التي ترغب في استعادتها باستخدام المفتاحين **Shift** و**Ctrl**.
3. يمكنك بدء استعادة الملفات بإحدى الطرق التالية:
   - بتحديد **استعادة** من قائمة سياق الملفات.
   - من خلال النقر فوق الرابط **استعادة** الموجود في خانة المعلومات الخاصة بالملفات المحددة.

ستقوم تطبيقات الأمان التي قامت بوضع الملفات في مستودعات الأجهزة العميلة باستعادة الملفات نفسها من مجلداتها الأصلية.

حفظ ملف من المستودعات إلى القرص

يتيح Kaspersky Security Center إمكانية حفظ نُسخ من الملفات التي وضعها تطبيق الأمان في العزل أو النسخ الاحتياطي على جهاز عميل على القرص. يتم نسخ الملفات إلى المجلد المحدد في الجهاز الذي تم تثبيت Kaspersky Security Center عليه.

لحفظ نسخة من الملف من العزل أو النسخ الاحتياطي إلى محرك الأقراص الثابتة:

1. من شجرة وحدة التحكم، حدد المجلد **المستودعات**، والمجلد الفرعي **العزل** أو **النسخ الاحتياطي**.

2. من مساحة العمل الخاصة بالمجلد **العزل** (**النسخ الاحتياطي**)، حدد ملفًا ترغب في نسخه إلى محرك الأقراص الثابتة.

3. يمكنك بدء النسخ بإحدى الطرق التالية:

- بتحديد **حفظ إلى القرص** في قائمة سياق الملف.
- بالنقر فوق الرابط **حفظ إلى القرص** في خانة المعلومات الخاصة بالملف المحدد.

تطبيق الأمان الذي وضع الملف في العزل على الجهاز العميل سيحفظ نسخة من هذا الملف في المجلد المحدد.

فحص الملفات في العزل

لفحص الملفات المعزولة:

1. من شجرة وحدة التحكم، حدد المجلد **المستودعات** ثم المجلد الفرعي **العزل**.

2. في مساحة عمل المجلد **العزل**، حدد الملفات التي ترغب في فحصها باستخدام المفتاحين `Shift` و`Ctrl`.

3. يمكنك بدء فحص الملف من خلال إحدى الطرق التالية:

- بتحديد **فحص** في قائمة سياق الملف.
- من خلال النقر فوق الرابط **فحص** في خانة معلومات الملفات المحددة.

يقوم التطبيق بتشغيل مهمة الفحص حسب الطلب لتطبيقات الأمن التي وضعت الملفات المحددة في العزل على الأجهزة المُخزّن عليها تلك الملفات.

تهديدات نشطة

يتم تخزين المعلومات حول الملفات التي لم تتم معالجتها المكتشفة على الأجهزة العميلة في المجلد **المستودعات**، بالمجلد الفرعي **تهديدات نشطة**.

يتم إجراء مهام المعالجة والتنظيف التي تم تأجليها بواسطة تطبيق الأمن حسب الطلب أو بعد وقوع حدث معين. يمكنك تكوين المعالجة المؤجلة.

تنظيف ملف غير معالج

لبدء تنظيف ملف غير معالج:

1. من شجرة وحدة التحكم، في المجلد **المستودعات**، حدد مجلد **تهديدات نشطة** الفرعي.

2. في مساحة عمل المجلد **تهديدات نشطة**، حدد الملف الذي ينبغي عليك تنظيفه.

3. بدء تطهير الملف بإحدى الطرق التالية:

- بتحديد **تنظيف** في من قائمة سياق الملف.
- من خلال النقر فوق الرابط **تنظيف** الموجود في خانة المعلومات الخاصة بالملف المحدد.

ستتم عندئذٍ محاولة تنظيف هذا الملف.

إذا تم تنظيف الملف، فيقوم تطبيق الأمن المثبت على الجهاز العميل باسترداده إلى المجلد الأصلي له. تتم إزالة سجل الملف من القائمة في المجلد **تهديدات نشطة**. إذا تعذر تنظيف الملف، فيقوم تطبيق الأمن المثبت على الجهاز بحذفه من ذلك الجهاز. تتم إزالة سجل الملف من القائمة في المجلد **تهديدات نشطة**.

قد تختلف إمكانية تنظيف الملفات وحذفها بناءً على تطبيق الأمان المثبت وإصداره وإعداداته.

حفظ ملف لم تتم معالجته إلى القرص

يتيح Kaspersky Security Center حفظ نسخ الملفات التي لم تتم معالجتها التي يتم العثور عليها على الأجهزة العميلة وذلك على القرص. يشير هذا إلى الملفات التي تم معالجتها أو حذفها بواسطة التطبيق. يتم نسخ الملفات إلى المجلد المحدد في الجهاز الذي تم تثبيت Kaspersky Security Center عليه.

يمكنك حفظ نُسخ من الملفات في حالة حذف الملفات أو تعديلها أثناء التنظيف وكانت نسخها مخزنة في مخزن Kaspersky Endpoint Security for Windows على الجهاز المُدار.

لحفظ نسخة من ملف غير معالج على القرص:

1. من شجرة وحدة التحكم، في المجلد **المستودعات**، حدد مجلد **تهديدات نشطة** الفرعي.
2. في مساحة عمل المجلد **تهديدات نشطة**، حدد الملفات التي ينبغي عليك نسخها على القرص.
3. يمكنك بدء النسخ بإحدى الطرق التالية:

- بتحديد **حفظ إلى القرص** في قائمة سياق الملف.
- بالنقر فوق الرابط **حفظ إلى القرص** في خانة المعلومات الخاصة بالملف المحدد.

يحفظ تطبيق الأمان المثبت على الجهاز العميل الذي يوجد عليه الملف غير المعالج نسخة من هذا الملف إلى المجلد المحدد.

حذف ملفات من المجلد "التهديدات المفعلة"

لحذف ملف من المجلد **تهديدات نشطة**:

1. من شجرة وحدة التحكم، في المجلد **المستودعات**، حدد مجلد **تهديدات نشطة** الفرعي.
2. في مساحة عمل مجلد **تهديدات نشطة**، حدد الملفات التي ينبغي عليك حذفها باستخدام المفتاحين **Shift** و**Ctrl**.
3. احذف الملفات بإحدى الطرق التالية:

- بتحديد **حذف** في قائمة سياق الملفات.
- بالنقر فوق الرابط **حذف** (**حذف** إذا كنت ترغب في حذف ملف واحد) في خانة المعلومات الخاصة بالملفات المحددة.

تطبيق الأمان الذي قام بوضع الملفات في المستودعات على الأجهزة العميلة سيحذف الملفات نفسها من هذه المستودعات. تتم إزالة سجلات الملفات من القائمة في المجلد **تهديدات نشطة**.

(KSN) Kaspersky Security Network

يصف هذا القسم كيفية استخدام بنية أساسية للخدمات عبر الإنترنت تحمل الاسم Kaspersky Security Network (KSN). يوفر القسم التفاصيل حول KSN، وكذلك تعليمات حول كيفية تمكين KSN، وتكوين الوصول إلى KSN، وعرض إحصائيات استخدام خادم وكيل KSN.

وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية)، بالإضافة إلى وظيفة KSN التي قد لا تكون متاحة في البرنامج في الولايات المتحدة الأمريكية.

حول KSN

تعد Kaspersky Security Network (KSN) بنية أساسية للخدمات عبر الإنترنت والتي توفر الوصول إلى قاعدة معارف Kaspersky عبر الإنترنت، والمتضمنة بدورها معلومات حول سمعة الملفات وموارد الويب والبرامج. ويعد استخدام البيانات من Kaspersky Security Network ضمانًا لسرعة استجابات تطبيقات Kaspersky عند مواجهة تهديدات، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية ويقلل من خطر وقوع الحالات الإيجابية الخاطئة. يتيح KSN لك استخدام قواعد بيانات صيت Kaspersky لاسترداد المعلومات حول التطبيقات المثبتة على الأجهزة المُدارة.

يدعم Kaspersky Security Center حلول البنية التحتية التالية:

- KSN هي حل يسمح لك بتبادل المعلومات مع Kaspersky Security Network. بالمشاركة في KSN، فإنك توافق على إرسال معلومات بشكل تلقائي إلى Kaspersky حول تشغيل تطبيقات Kaspersky المثبتة على أجهزة العميل والأجهزة المُدارة عبر Kaspersky Security Center. يتم نقل المعلومات وفقًا لإعدادات وصول KSN الحالية. بالإضافة إلى ذلك، يقوم محللو Kaspersky بتحليل المعلومات المستلمة وإدراجها في السمات وقواعد البيانات الإحصائية الخاصة بشبكة Kaspersky Security Network. يستخدم Kaspersky Security Center هذا الحل افتراضيًا.
- Kaspersky Private Security Network (KPSN) هي حل يتيح لمستخدمي الأجهزة المثبتة بتطبيقات Kaspersky الوصول إلى قواعد بيانات سمات Kaspersky Security Network والبيانات الإحصائية الأخرى دون إرسال البيانات إلى KSN العالمية من أجهزتهم. تم تصميم KPSN لعملاء الشركة الذين يتعذر عليهم المشاركة في Kaspersky Security Network لأحد الأسباب التالية:
  - أجهزة المستخدم غير متصلة بالإنترنت.
  - يحظر القانون نقل أي بيانات خارج الدولة أو خارج الشبكة المحلية للشركة أو تقيد سياسات أمان الشركة ذلك.

قم بإعداد إعدادات الوصول لشبكة Kaspersky Private Security Network في **KSN Proxy settings** الخاصة بنافذة خصائص خادم الإدارة.

يطالبك التطبيق بالانضمام إلى KSN أثناء تشغيل معالج البدء السريع. يمكنك البدء أو التوقف عن استخدام KSN في أي لحظة عند استخدام التطبيق.

يمكنك استخدام KSN وفق بيان KSN الذي تقرأه وتوافق عليه عندما تقوم بتمكين KSN. إذا تم تحديث بيان KSN، فسيتم عرضه لك عند ترقية إصدار من خادم الإدارة. يمكن قبول بيان KSN المحدث أو رفضه. إذا رفضته ستستمر في استخدام KSN وفق الإصدار السابق لبيان KSN الذي قد قبلته من قبل.

عند تمكين KSN، يتحقق Kaspersky Security Center من إمكانية الوصول إلى خوادم KSN. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة. يعد ذلك ضروريًا للتأكد من الحفاظ على مستوى الأمان للأجهزة المُدارة.

تتفاعل أجهزة العميل المدارة بواسطة خادم الإدارة مع KSN عبر الخادم الوكيل لشبكة KSN. يوفر الخادم الوكيل لشبكة KSN الميزات التالية:

- يمكن للأجهزة العميلة إرسال طلبات إلى KSN، والحصول على معلومات من KSN، ونقل المعلومات إلى KSN حتى لو لم يكن لديهم إمكانية الوصول المباشر إلى الإنترنت.
- يخزن خادم وكيل KSN البيانات المعالجة مؤقتًا، مما يقلل الحمل على القناة الخارجية والفترة الزمنية التي يتم قضاؤها لانتظار المعلومات التي يطلبها جهاز عميل.

يمكنك تكوين الخادم الوكيل لشبكة KSN في القسم **KSN Proxy settings** في نافذة خصائص خادم الإدارة.

إعداد الوصول إلى Kaspersky Security Network

يمكنك إعداد الوصول إلى Kaspersky Security Network (KSN) على خادم الإدارة وعلى نقطة التوزيع.

لإعداد وصول خادم الإدارة إلى Kaspersky Security Network (KSN):

1. في شجرة وحدة التحكم، حدد خادم الإدارة الذي ترغب في تكوين وصوله إلى KSN.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة ومن الجزء**الأقسام**، حدد **وكيل KSN** ← **إعدادات وكيل KSN**.

4. في مساحة العمل، مكّن خيار **استخدام خادم الإدارة كخادم وكيل** لاستخدام خدمة وكيل KSN.

يتم إرسال البيانات من الأجهزة العميلة إلى KSN وفقًا لسياسة Kaspersky Endpoint Security، والتي تكون نشطة على الأجهزة العميلة تلك. إذا تم إلغاء خانة الاختيار هذه، فلن يتم إرسال أي بيانات إلى KSN من خادم الإدارة ومن الأجهزة العميلة عبر Kaspersky Security Center. ومع ذلك، يمكن للأجهزة العميلة إرسال بيانات إلى KSN مباشرة (عبر تجاوز Kaspersky Security Center)، وفقًا للإعدادات الخاصة بهم. تحدد سياسة Kaspersky Endpoint Security for Windows المفعلة على الأجهزة العميلة، البيانات التي سيتم إرسالها بشكل مباشر (عبر تجاوز Kaspersky Security Center) من هذه الأجهزة إلى KSN.

5. قم بتعطيل خيار**أوافق على استخدام Kaspersky Security Network**.

إذا تم تحديد هذا الخيار، فسترسل أجهزة العملاء نتائج تثبيت التصحيح إلى Kaspersky. عند تمكين هذا الخيار، تأكد من أنك قد قرأت شروط بيان KSN ووافقت عليها.

إذا كنت تستخدم Kaspersky Private Security Network، قم بتمكين الخيار **تكوين KPSN** وانقر فوق الزر **تحديد ملف من خلال إعدادات وكيل شبكة KSN** لتنزيل إعدادات KPSN (الملفات بامتدادي pkcs7 وpem). وعقب تنزيل الإعدادات، تعرض الواجهة اسم المزود وجهات الاتصال، وكذلك تاريخ إنشاء الملف مع إعدادات شبكة KPSN.

عند تمكين شبكة KPSN، انتبه إلى نقاط التوزيع التي تم تكوينها لإرسال طلبات KSN مباشرةً إلى شبكة KSN السحابية. ستواصل نقاط التوزيع المُثبَّت عليها عميل الشبكة الإصدار 11 (أو إصدار سابق) إرسال طلبات KSN إلى Cloud KSN. إذا أردت إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KPSN، قم بتمكين خيار **توجيه طلبات KSN إلى خادم الإدارة** لكل نقطة توزيع. يمكنك تمكين هذا الخيار في خصائص نقطة التوزيع أو في سياسة عميل الشبكة.

عند تحديد خانة الاختيار **تكوين KPSN**، تظهر رسالة بالتفاصيل حول شبكة KPSN.

في حالة تمكين الخيار **تكوين KPSN** في Kaspersky Security Center، تتلقى هذه التطبيقات معلومات حول دعم شبكة KPSN. وفي نافذة إعدادات التطبيق وفي القسم الفرعي **Kaspersky Security Network** الخاص بالقسم **الحماية المتقدمة من التهديد**، يتم عرض معلومات عن مزود خدمة شبكة KSN موفر شبكة KSN - شبكة KSN أو شبكة KPSN.

إذا كنت تستخدم إصدارات التطبيق الأقدم من Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 أو أقدم من Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent عند تشغيل شبكة KPSN، نوصيك باستخدام خوادم الإدارة الثانوية التي لم يتم تمكين استخدام شبكة KPSN الخاصة لها.

لا يرسل Kaspersky Security Center أي بيانات إحصائية إلى Kaspersky Security Network في حالة تكوين شبكة KPSN في القسم **وكيل KSN** ← **إعدادات وكيل KSN** الخاص بنافذة خصائص خادم الإدارة.

في حالة تكوين إعدادات خادم الوكيل في خصائص خادم الإدارة ولكن بنية الشبكة لديك تتطلب استخدام شبكة KPSN مباشرة، فقم بتمكين الخيار **تجاهل إعدادات الخادم الوكيل عند الاتصال بشبكة KPSN**. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المُدارة إلى شبكة KPSN.

6. تكوين اتصال خادم الإدارة بخدمة وكيل KSN:

- ضمن **إعدادات الاتصال**، بالنسبة إلى **منفذ TCP**، حدد رقم منفذ TCP الذي سيتم استخدامه للاتصال بخادم وكيل KSN. المنفذ الافتراضي للاتصال بخادم وكيل KSN هو 13111.
- إذا كنت تريد أن يتصل خادم الإدارة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد رقم منفذ **منفذ UDP**. بشكل افتراضي، يتم تعطيل هذا الخيار، ويتم استخدام منفذ TCP. إذا تم تمكين هذا الخيار، فإن منفذ UDP الافتراضي للاتصال بخادم وكيل KSN هو 15111.
- إذا كنت تريد أن يتصل خادم الإدارة بخادم وكيل KSN من خلال منفذ HTTPS، فقم بتمكين الخيار **استخدام HTTPS عبر المنفذ** وحدد رقم منفذ. بشكل افتراضي، يتم تعطيل هذا الخيار، ويتم استخدام منفذ TCP. إذا تم تمكين هذا الخيار، فإن منفذ HTTPS الافتراضي للاتصال بخادم وكيل KSN هو 17111.

7. قم بتفعيل خيار **توصيل خوادم الإدارة الثانوية بشبكة KSN عبر خادم الإدارة الأساسي**.

إذا تم تمكين هذا الخيار، فإن خوادم الإدارة الثانوية من أي مستوى تسلسل هرمي تستخدم خادم الإدارة الأساسي كخادم وكيل لشبكة KSN. إذا تم تعطيل هذا الخيار، فستتصل خوادم الإدارة الثانوية بشبكة KSN بنفسهم. وفي هذه الحالة، ستستخدم الأجهزة المدارة خوادم الإدارة الثانوية كخوادم لوكيل KSN

تستخدم خوادم الإدارة الثانوية خادم الإدارة الرئيسي كخادم وكيل إذا كانت خانة الاختيار **استخدام خادم الإدارة كخادم وكيل** في الجزء الأيمن بالقسم **إعدادات وكيل KSN** في خصائص خوادم الإدارة الثانوية محددة.

8. انقر على**موافق**.

سيتم حفظ إعدادات الوصول إلى KSN.

يمكنك أيضًا إعداد وصول نقطة التوزيع لـ KSN، على سبيل المثال، إذا كنت ترغب في تقليل الحمل على خادم الإدارة. ترسل نقطة التوزيع التي تعمل كخادم عميل لشبكة KSN طلبات KSN من الأجهزة المُدارة إلى Kaspersky مباشرة دون استخدام خادم الإدارة.

لإعداد وصول نقطة التوزيع إلى Kaspersky Security Network (KSN):

1. تأكد من أن نقطة التوزيع معينة يدويًا.
2. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.
3. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
4. في نافذة خصائص خادم الإدارة، حدد القسم **نقاط التوزيع**.
5. حدد نقطة التوزيع في القائمة وانقر فوق الزر **خصائص** لفتح نافذة الخصائص الخاصة به.
6. في نافذة خصائص نقطة التوزيع وفي القسم **وكيل KSN**، حدد **الوصول إلى KSN Cloud/KPSN مباشرة عبر الإنترنت**.
7. انقر فوق **موافق**.

ستعمل نقطة التوزيع كخادم وكيل KSN.

تمكين وتعطيل KSN

لتمكين KSN:

1. في شجرة وحدة التحكم حدد خادم الإدارة الذي تريد أن تقوم بتمكين KSN له.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة، في القسم **وكيل KSN**، حدد القسم الفرعي **إعدادات وكيل KSN**.

4. حدد **استخدام خادم الإدارة كخادم وكيل**.

تم تمكين خادم وكيل KSN.

5. قم بتعطيل خيار **أوافق على استخدام Kaspersky Security Network**.

سيتم تمكين KSN.

إذا تم تحديد خانة الاختيار هذه، فسترسل الأجهزة العميلة نتائج تثبيت التصحيح إلى Kaspersky. عند تحديد خانة الاختيار هذه، ينبغي عليك قراءة بنود بيان KSN والموافقة عليها.

6. انقر على **موافق**.

لتعطيل KSN:

1. في شجرة وحدة التحكم حدد خادم الإدارة الذي تريد أن تقوم بتمكين KSN له.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة، في القسم **وكيل KSN**، حدد القسم الفرعي **إعدادات وكيل KSN**.

4. قم بإلغاء تحديد خانة الاختيار **استخدام خادم الإدارة كخادم وكيل** لتعطيل خدمة عميل شبكة KSN، أو قم بإلغاء تحديد خانة الاختيار **أوافق على استخدام Kaspersky Security Network**.

إذا تم إلغاء تحديد خانة الاختيار هذه، فلن ترسل الأجهزة العميلة نتائج تثبيت التصحيح إلى Kaspersky.

إذا كنت تستخدم شبكة KSN خاصة، فقم بإلغاء تحديد خانة الاختيار **تكوين KPSN**.

سيتم تعطيل KSN.

5. انقر على **موافق**.

عرض بيان KSN المقبول

عندما تقوم بتمكين Kaspersky Security Network (KSN)، يجب عليك قراءة بيان KSN وقبوله. يمكنك عرض بيان KSN المقبول في أي وقت.

لعرض بيان KSN المقبول:

1. في شجرة وحدة التحكم، حدد خادم الإدارة الذي قمت بتمكين KSN له.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. في نافذة خصائص خادم الإدارة، في القسم **وكيل KSN**، حدد القسم الفرعي **إعدادات وكيل KSN**.

4. انقر على الرابط **عرض بيان KSN المعتمد**.

في النافذة التي تفتح، يمكنك عرض نص بيان KSN المقبول.

عرض إحصائيات خادم وكيل KSN

خادم وكيل KSN هو خدمة تضمن التفاعل بين البنية الأساسية Kaspersky Security Network والأجهزة العميلة التي يديرها خادم الإدارة.

يوفر لك استخدام خادم وكيل KSN الميزات التالية:

- يمكن للأجهزة العميلة إرسال طلبات إلى KSN ونقل المعلومات إلى KSN حتى ولو لم يكن لديها وصول مباشر إلى الإنترنت.
- يخزن خادم وكيل KSN البيانات المعالجة مؤقتًا، مما يقلل الحمل على القناة الخارجية والفترة الزمنية التي يتم قضاؤها لانتظار المعلومات التي يطلبها جهاز عميل.

في نافذة خصائص خادم الإدارة، يمكنك تكوين خادم وكيل KSN وعرض الإحصائيات حول استخدام خادم وكيل KSN.

لعرض إحصائيات خادم وكيل KSN:

1. في شجرة وحدة التحكم، حدد خادم الإدارة الذي تحتاج إلى عرض إحصائيات KSN له.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في نافذة خصائص خادم الإدارة، في قسم **وكيل KSN**، حدد القسم الفرعي **إحصائيات وكيل KSN**.

   يعرض هذا القسم الإحصائيات الفعلية لعملية خادم وكيل KSN (عدد سجلات ذاكرة التخزين المؤقت، والحزم التي تمت معالجتها في ذاكرة التخزين المؤقت، والحزم المستلمة). وأيضًا، إذا كان خادم الإدارة متصلاً بشبكة KSN، فسيتم عرض رسالة المعلومات المقابلة.

   إذا لزم الأمر، قم باتخاذ الإجراءات الإضافية التالية:

   - انقر فوق **تحديث** لتحديث الإحصائيات حول استخدام الخادم الوكيل لشبكة KSN.
   - انقر فوق الزر **تصدير إلى الملف** لتصدير الإحصائيات إلى ملف CSV.
   - انقر فوق الزر **التحقق من اتصال KSN** للتحقق مما إذا كان خادم الإدارة متصلاً حاليًا بشبكة KSN.
4. انقر فوق الزر **موافق** لإغلاق النافذة خصائص خادم الإدارة.

قبول بيان KSN محدث

أنت تستخدم KSN وفق بيان KSN الذي تقرأه وتوافق عليه عندما تقوم بتمكين KSN. إذا تم تحديث بيان KSN، سيتم عرضه لك عندما تحدث خادم الإدارة أو تقوم بترقيته. يمكن قبول بيان KSN المحدث أو رفضه. إذا رفضته ستستمر في استخدام KSN وفق إصدار بيان KSN الذي قد قبلته من قبل.

بعد تحديث خادم الإدارة أو ترقيته، يتم عرض بيان KSN المحدث تلقائيًا. إذا رفضت بيان KSN المحدث، لا يزال بإمكانك عرضه وقبوله لاحقًا.

لعرض بيان KSN محدث ثم قبوله أو رفضه:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.
2. في تبويب **المراقبة** في قسم **المراقبة**، انقر على رابط **بيان Kaspersky Security Network المقبول قديم**.

   ستفتح نافذة **بيان KSN**.
3. اقرأ بيان KSN بعناية ثم اتخذ قرارك. إذا قبلت بيان KSN المحدث، انقر على زر **أوافق على بنود اتفاقية الترخيص**. إذا رفضت بيان KSN المحدث، انقر على زر **إلغاء**.

بناءً على اختيارك، تواصل KSN العمل وفقًا لشروط بيان KSN الحالي أو المحدث. يمكنك عرض نص بيان KSN المقبول في خصائص خادم الإدارة في أي وقت.

حماية مُحسنة باستخدام Kaspersky Security Network

يقدم Kaspersky طبقة حماية إضافية للمستخدمين من خلال Kaspersky Security Network. تم تصميم طريقة الحماية هذه لمحاربة الهجمات المتكررة المتقدمة والتي ليس لها مدة يومية. تُساهم تقنيات السحابة المدمجة وخبرة محللي فيروسات Kaspersky من Kaspersky Endpoint Security خيارًا غير مسبوق مقابل تهديدات الشبكة الأكثر تعقيدًا.

تتوفر تفاصيل حول الحماية المحسنة في Kaspersky Endpoint Security على موقع ويب Kaspersky.

التحقق مما إذا كانت نقطة التوزيع تعمل كخادم وكيل لشبكة KSN

يمكنك تمكين الخادم الوكيل لشبكة KSN على جهاز مُدار تم تعيينه للعمل كنقطة توزيع. يعمل الجهاز المُدار كخادم وكيل KSN عند تشغيل خدمة ksnproxy على الجهاز. يمكنك التحقق من هذه الخدمة أو تشغيلها أو إيقاف تشغيلها على الجهاز محليًا.

يمكنك تعيين جهاز يعمل بنظام التشغيل Windows أو Linux كنقطة توزيع. وتعتمد طريقة فحص نقطة التوزيع على نظام تشغيل نقطة التوزيع هذه.

للتحقق مما إذا كانت نقطة التوزيع المعتمدة على نظام التشغيل Windows تعمل كخادم وكيل لشبكة KSN:

1. على جهاز نقطة التوزيع، في Windows، افتح **خدمات** (**كل البرامج** ← **الأدوات الإدارية** ← **خدمات**).

2. في قائمة الخدمات، تحقق من تشغيل خدمة ksnproxy.

   إذا كانت خدمة ksnproxy قيد التشغيل، فإن عميل الشبكة الموجود على الجهاز يشارك في Kaspersky Security Network ويعمل كخادم وكيل KSN للأجهزة المدارة المضمنة في نطاق نقطة التوزيع.

   إذا كنت تريد، يمكنك إيقاف تشغيل خدمة ksnproxy. في هذه الحالة، يتوقف عميل الشبكة لنقطة التوزيع عن المشاركة في Kaspersky Security Network. هذا الأمر يتطلب حقوق المسؤول المحلي.

للتحقق مما إذا كانت نقطة التوزيع المعتمدة على نظام التشغيل Linux تعمل كخادم وكيل لشبكة KSN:

1. على جهاز نقطة التوزيع، اعرض قائمة العمليات الجارية.

2. في قائمة العمليات الجارية، تحقق مما إذا كانت العملية `opt/kaspersky/ksc64/sbin/ksnproxy/` قيد التشغيل.

إذا كانت عملية `opt/kaspersky/ksc64/sbin/ksnproxy/` قيد التشغيل، فإن عميل الشبكة الموجود على الجهاز في Kaspersky Security Network ويعمل كخادم وكيل KSN للأجهزة المدارة المضمنة في نطاق نقطة التوزيع.

التبديل بين التعليمات عبر الإنترنت والتعليمات دون الاتصال به

إذا لم يكن لديك اتصال بالإنترنت، فيمكنك استخدام "التعليمات دون الاتصال به".

للتبديل بين التعليمات عبر الإنترنت والتعليمات دون الاتصال به:

1. في النافذة الرئيسية لـ Kaspersky Security Center، حدد **Kaspersky Security Center 15.1** في شجرة وحدة التحكم.

2. انقر فوق رابط **إعدادات الواجهة العامة**.

   يتم فتح نافذة الإعدادات.

3. في نافذة الإعدادات، انقر على **استخدام المساعدة دون الاتصال بالإنترنت**.

4. انقر فوق **موافق**.

يتم تطبيق الإعدادات وحفظها. إذا كنت ترغب في ذلك، فيمكنك تغيير الإعدادات مرة أخرى في أي وقت والبدء في استخدام المساعدة عبر الإنترنت في أي وقت.

تصدير الأحداث إلى أنظمة SIEM

يوضح هذا القسم كيفية تصدير الأحداث التي سجلها Kaspersky Security Center إلى أنظمة معلومات الأمان الخارجية وإدارة الأحداث (SIEM).

تكوين تصدير الحدث إلى أنظمة SIEM

يسمح Kaspersky Security Center بالتكوين بإحدى الطرق التالية: التصدير إلى أي نظام SIEM يستخدم تنسيق Syslog أو التصدير إلى أنظمة QRadar وSplunk وArcSight SIEM التي تستخدم تنسيقات LEEF وCEF أو تصدير الأحداث إلى أنظمة SIEM مباشرةً من قاعدة بيانات Kaspersky Security Center. عند إكمال هذا السيناريو، يرسل خادم الإدارة الأحداث إلى نظام SIEM تلقائيًا.

المتطلبات الأساسية

قبل أن تبدأ في تصدير تكوين الأحداث في Kaspersky Security Center:

- تعرف على المزيد حول طرق تصدير الحدث.
- تأكد من أن لديك قيم إعدادات النظام.

يمكنك تنفيذ خطوات هذا السيناريو بأي ترتيب.

تتكون عملية تصدير الأحداث إلى نظام SIEM من الخطوات التالية:

- **تكوين نظام SIEM لاستقبال الأحداث من Kaspersky Security Center**

  تعليمات للمساعدة: تكوين تصدير الحدث في نظام SIEM

- **تحديد الأحداث التي تريد تصديرها إلى نظام SIEM:**

  تعليمات للمساعدة:

  - وحدة تحكم الإدارة: وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog، ووضع علامة على الأحداث العامة للتصدير بتنسيق Syslog
  - Kaspersky Security Center Web Console: تمييز أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog وتمييز الأحداث العامة للتصدير بتنسيق Syslog

- **قم بتكوين تصدير الأحداث إلى نظام SIEM باستخدام إحدى الطرق التالية:**

  - استخدم TCP أو UDP أو TLS عبر بروتوكولات TCP.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تكوين تصدير الأحداث إلى أنظمة SIEM
- Kaspersky Security Center Web Console: تكوين تصدير الأحداث إلى أنظمة SIEM
  - استخدام تصدير الأحداث بشكل مباشر من قاعدة بيانات Kaspersky Security Center (يتم توفير مجموعة من طرق العرض العامة في قاعدة بيانات Kaspersky Security Center؛ ويمكنك العثور على وصف لهذه العروض العامة في المستند klakdb.chm).

النتائج

بعد تكوين تصدير الأحداث إلى نظام SIEM يمكنك عرض نتائج التصدير إذا قمت بتحديد الأحداث التي تريد تصديرها.

قبل البدء

عند إعداد التصدير التلقائي للأحداث في Kaspersky Security Center، يجب عليك تحديد بعض إعدادات نظام SIEM. يوصى بأن تتحقق من هذه الإعدادات مسبقًا للتحضير لإعداد Kaspersky Security Center.

لتكوين الإرسال التلقائي للأحداث إلى نظام SIEM، يجب أن تكون على علم بالإعدادات التالية:

- **عنوان خادم نظام SIEM**

  عنوان IP للخادم المستخدم حاليًا الذي تم تثبيت نظام SIEM عليه. تحقق من هذه القيمة في إعدادات نظام SIEM لديك.

- **منفذ خادم نظام SIEM**

  رقم المنفذ المستخدم لإنشاء اتصال بين Kaspersky Security Center وخادم نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center وفي إعدادات المستلم لنظام SIEM الخاص بك.

- **البروتوكول**

  البروتوكول المستخدم لنقل الرسائل من Kaspersky Security Center إلى نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center وفي إعدادات المستلم لنظام SIEM الخاص بك.

حول الأحداث في Kaspersky Security Center

يتيح لك Kaspersky Security Center تلقي معلومات عن الأحداث التي تقع أثناء تشغيل خادم الإدارة وتطبيقات Kaspersky المثبتة على الأجهزة المُدارة. يتم حفظ المعلومات حول الأحداث في قاعدة بيانات خادم الإدارة. يمكنك تصدير هذه المعلومات إلى أنظمة SIEM الخارجية. يسمح تصدير معلومات الأحداث إلى أنظمة SIEM لمسؤولي أنظمة SIEM بالاستجابة السريعة لأحداث نظام الأمان التي تحدث في الأجهزة المدارة أو مجموعات الإدارة.

أنواع الأحداث

يتوفر في Kaspersky Security Center الأنواع التالية من الأحداث:

- الأحداث العامة. تحدث هذه الأحداث في جميع تطبيقات Kaspersky المدارة. مثال على حدث عام هو انتشار الفيروسات. لقد حددت الأحداث العامة بناء الجملة والدلالات بدقة. يتم استخدام الأحداث العامة على سبيل المثال، في التقارير ولوحات المعلومات.
- أحداث خاصة بتطبيقات Kaspersky المدارة. يحتوي كل تطبيق من تطبيقات Kaspersky المدارة على مجموعة من الأحداث الخاصة به.

مصادر الحدث

يمكن إنشاء الأحداث من خلال التطبيقات التالية:

- مكونات Kaspersky Security Center:
  - خادم الإدارة
  - عميل الشبكة
  - خادم الأجهزة المحمولة التي تعمل بنظام iOS
- تطبيقات Kaspersky المُدارة

  للحصول على تفاصيل حول الأحداث التي تم إنشاؤها بواسطة تطبيقات Kaspersky المُدارة، يُرجى الرجوع إلى وثائق التطبيق المقابل.

يمكنك عرض القائمة الكاملة للأحداث التي يمكن إنشاؤها بواسطة تطبيق ما في علامة التبويب **Event configuration**. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث في خصائص خادم الإدارة.

مستوى خطورة الأحداث

يحتوي كل حدث على مستوى الأهمية الخاص به. بناء على شروط الحدوث، يمكن تعيين مستويات أهمية مختلفة لأي حدث. توجد أربعة مستويات للأهمية للأحداث:

- حدث حرج هو حدث يشير إلى تكرار مشكلة حرجة قد تؤدي إلى فقدان البيانات أو خلل في التشغيل أو خطأ حرج.
- خلل وظيفي هو حدث يشير إلى تكرار مشكلة خطيرة أو خطأ أو خلل حدث أثناء تشغيل التطبيق أو عند تنفيذ الإجراء.
- تحذير هو حدث ليس خطيرًا بالضرورة، غير أنه يشير إلى مشكلة محتملة في المستقبل. يتم تعيين معظم الأحداث كتحذيرات إذا كان من الممكن استعادة التطبيق بدون فقدان البيانات أو الإمكانيات الوظيفية بعد حدوث هذه الأحداث.
- حدث معلومات هو حدث يحدث لأغراض الإخبار عن إكمال التشغيل بنجاح، أو التشغيل الصحيح للتطبيق، أو إكمال الإجراء.

لكل حدث مدّة تخزين محددة، يمكنك خلالها عرضه في Kaspersky Security Center أو تعديله. لا يتم حفظ بعض البيانات في قاعدة بيانات خادم الإدارة بشكل افتراضي لأن مدّة التخزين المحددة هي صفر. يمكن تصدير الأحداث التي سيتم تخزينها في قاعدة بيانات خادم الإدارة فقط لمدة يوم واحد على الأقل إلى الأنظمة الخارجية.

حول تصدير الحدث

يمكن استخدام تصدير الحدث في الأنظمة المركزية التي تتعامل مع مشكلات الأمان على المستوى التنظيمي والتقني، والتي توفر خدمات مراقبة الأمان، وتجمع المعلومات من الحلول المختلفة. وهذه هي أنظمة SIEM التي توفر التحليل الفوري لتحذيرات الأمان والأحداث التي تنشئها أجهزة الشبكة والتطبيقات، أو مراكز تشغيل الأمان (SOC).

يمكن لهذه الأنظمة استلام البيانات من العديد من المصادر، بما فيها الشبكات والأمان والخوادم وقواعد البيانات والتطبيقات. توفر أنظمة SIEM أيضًا وظيفة تجميع البيانات التي تم رصدها لمساعدتك في تجنب فقدان الأحداث الحرجة. إضافة إلى ذلك، تُجري الأنظمة تحليلاً تلقائيًا للأحداث والتحذيرات المترابطة لإخطار المسؤولين بمشاكل الأمان العاجلة. يمكن تنفيذ التحذير من خلال لوحة معلومات ويمكن إرسالها من خلال قنوات لجهات خارجية مثل البريد الإلكتروني.

تشتمل عملية تصدير الأحداث من Kaspersky Security Center إلى أنظمة SIEM الخارجية على طرفين: Kaspersky Security Center ومستلم الحدث – نظام SIEM. لتصدير حدث بنجاح، يجب عليك تكوين هذا الحدث في نظام SIEM وفي وحدة تحكم إدارة Kaspersky Security Center. لا يهم ما الطرف الذي تقوم بتكوينه أولاً. يمكنك تكوين نقل الأحداث في Kaspersky Security Center ثم تكوين مستلم الأحداث بواسطة نظام SIEM أو العكس.

طرق إرسال الأحداث من Kaspersky Security Center

توجد ثلاث طرق لإرسال الأحداث من Kaspersky Security Center إلى الأنظمة الخارجية:

- إرسال الأحداث من خلال بروتوكول Syslog إلى أي نظام من أنظمة SIEM.

  باستخدام بروتوكول Syslog، يمكنك ترحيل أي من الأحداث التي تحدث في خادم إدارة Kaspersky Security Center وفي تطبيقات Kaspersky المثبتة على الأجهزة المدارة. بروتوكول Syslog هو بروتوكول قياسي لتسجيل الرسائل. يمكنك استخدامه لتصدير الأحداث إلى أي نظام SIEM.

  لهذا الغرض، تحتاج إلى تحديد الأحداث التي تريد ترحيلها إلى نظام SIEM. يمكنك وضع علامة على الأحداث في وحدة تحكم الإدارة أو Kaspersky Security Center Web Console. سيتم ترحيل الأحداث التي تم وضع علامة عليها فقط إلى نظام SIEM. إذا لم تضع علامة على أي شيء، فلن يتم ترحيل أي أحداث.

- إرسال الأحداث من خلال بروتوكولات CEF وLEEF إلى أنظمة QRadar وSplunk وArcSight.

  يمكنك استخدام بروتوكولي CEF وLEEF لتصدير الأحداث العامة . عند تصدير الأحداث عبر بروتوكولات CEF وLEEF، فلن يكون لديك إمكانية تحديد أحداث محددة لتصديرها. وبدلاً من ذلك، يتم تصدير جميع الأحداث العامة. لتحويل أحداث Kaspersky Security Center إلى أحداث بتنسيقي CEF وLEEF، تحتاج إلى استخدام ملف siem_conversion_rules.xml. ويحتوي هذا الملف على قائمة بسمات أحداث Kaspersky Security Center والسمات المقابلة للأحداث بتنسيقي CEF وLEEF. ويحتوي ملف siem_conversion_rules.xml أيضًا على القواعد اللازمة لإنشاء الرسائل المقابلة للأحداث. يتم تضمين هذا الملف في مجموعة توزيع Kaspersky Security Center.

  خلافًا لبروتوكول Syslog، لا تعتبر البروتوكولات CEF وLEEF بروتوكولات عامة. تكون البروتوكولات CEF وLEEF مخصصة لأنظمة SIEM المناسبة (QRadar وSplunk وArcSight). لذا، عند اختيارك لتصدير الأحداث عبر واحد من هذه البروتوكولات، فستستخدم المحلل المطلوب في نظام SIEM.

- بشكل مباشر من قاعدة بيانات Kaspersky Security Center إلى نظام SIEM.

  يمكن استخدام هذه الوسيلة الخاصة بتصدير الأحداث لاستلام الأحداث مباشرةً من طرق العرض العامة لقاعدة البيانات باستخدام استعلامات SQL. يتم حفظ نتائج الاستعلام على ملف XML يمكن استخدامه كبيانات إدخال لنظام خارجي. يمكن تصدير الأحداث المتاحة فقط في الرؤى العامة مباشرة من قاعدة البيانات.

استلام الأحداث بواسطة نظام SIEM

يجب أن يستلم نظام SIEM الأحداث المحللة بشكل صحيح والمستلمة من Kaspersky Security Center. لهذه الأغراض يجب عليك تكوين نظام SIEM على النحو الصحيح. يعتمد التكوين على نظام SIEM المحدد الذي تم استخدامه. ومع ذلك، يوجد عدد من الخطوات العامة في تكوين جميع أنظمة SIEM، مثل تكوين المستلم والمحلل.

حول تكوين تصدير الحدث في نظام SIEM

تشتمل عملية تصدير الأحداث من Kaspersky Security Center إلى أنظمة SIEM الخارجية على طرفين: Kaspersky Security Center ومستلم الحدث – نظام SIEM. يجب عليك تكوين عملية تصدير الأحداث في نظام SIEM الخاص بك وفي Kaspersky Security Center.

تعتمد الإعدادات التي تحددها في نظام SIEM على النظام المحدد الذي تستخدمه. بوجه عام، بالنسبة إلى جميع الأجهزة يتعين عليك إعداد المستلم، ولك الخيار، في إعداد محلل الرسالة لتحليل الأحداث المستلمة.

إعداد المستلم

لاستلام الأحداث التي يرسلها Kaspersky Security Center، يجب عليك إعداد المستلم في نظام SIEM الخاص بك. بوجه عام، يجب تحديد الإعدادات التالية في نظام SIEM.

- **تصدير بروتوكول أو نوع إدخال**

  إنه بروتوكول نقل الرسائل، على سبيل المثال، UDP. يجب أن يكون البروتوكول مطابقًا لما حددته في Kaspersky Security Center.

- **المنفذ**

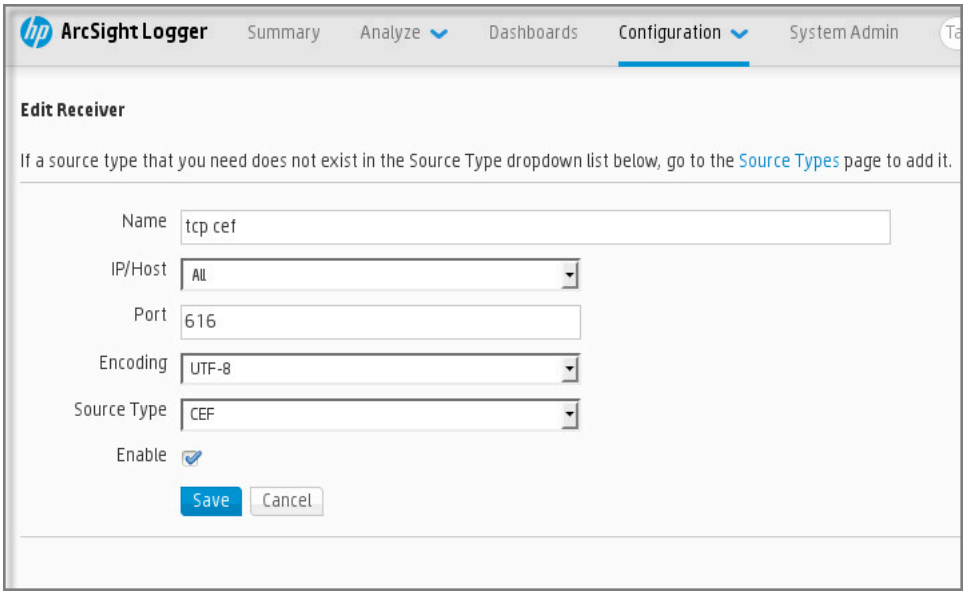
  رقم المنفذ للاتصال بـ Kaspersky Security Center. يجب أن يكون هذا المنفذ مطابقًا لما حددته في Kaspersky Security Center.

- **بروتوكول الرسالة أو نوع المصدر**

  البروتوكول المستخدم لتصدير الأحداث إلى نظام SIEM. يمكن أن يكون أحد البروتوكولات القياسية: Syslog أو CEF أو LEEF. يحدد نظام SIEM محلل الرسالة وفقًا للبروتوكول الذي تحدده.

بناءً على نظام SIEM الذي تستخدمه، قد يتعين عليك تحديد بعض الإعدادات الإضافية للمستلم.

يوضح الشكل أدناه شاشة إعداد جهاز الاستقبال في ArcSight.



إعداد المستلم في ArcSight

محلل الرسالة

يتم تمرير الأحداث التي تم تصديرها إلى أنظمة SIEM كرسائل. يجب تحليل هذه الرسائل على النحو الصحيح حتى يتسنى استخدام معلومات الأحداث بواسطة نظام SIEM. تمثل محللات الرسالة جزءًا من نظام SIEM، إذ تُستخدم لتجزئة محتويات الرسالة في الحقول ذات الصلة، مثل معرف الحدث والخطورة والوصف والمعلمات. يتيح هذا الإجراء لنظام SIEM معالجة الأحداث المستلمة من Kaspersky Security Center حتى يمكن تخزينها في قاعدة بيانات نظام SIEM.

وضع علامة على الأحداث للتصدير إلى أنظمة SIEM بتنسيق Syslog

بعد تمكين التصدير التلقائي للأحداث، يجب عليك تحديد الأحداث التي سيتم تصديرها إلى نظام SIEM الخارجي.

يمكنك تكوين تصدير الأحداث بتنسيق Syslog إلى نظام خارجي وفقًا لأحد الشروط التالية:

- وضع علامة على الأحداث العامة. إذا وضعت علامة على الأحداث التي تريد تصديرها في سياسة، فسيتلقى نظام SIEM الأحداث المحددة التي حدثت في جميع التطبيقات المُدارة من جانب السياسة المحددة. إذا تم تحديد الأحداث التي تم تصديرها في السياسة، فلن تتمكن من إعادة تحديدها لتطبيق فردي مدار بواسطة هذه السياسة.
- وضع علامة على أحداث تطبيق مُدار. إذا قمت بوضع علامة على أحداث تريد تصديرها إلى تطبيق مُدار على جهاز مُدار، فسيتلقى نظام SIEM فقط الأحداث التي حدثت في هذا التطبيق.

وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog

إذا كنت تريد تصدير الأحداث التي حدثت في تطبيق فردي مُدار مثبت على جهاز مُدار، فضع علامة على الأحداث التي تريد تصديرها للتطبيق. إذا تم وضع علامة على الأحداث التي تم تصديرها سابقًا في السياسة، فلن تتمكن من إعادة وضع علامة على الأحداث المحددة لتطبيق فردي مُدار من جانب هذه السياسة.

لوضع علامة على الأحداث التي تريد تصديرها لتطبيق فردي مُدار:

1. في شجرة وحدة التحكم Kaspersky Security Center، حدد العقدة **الأجهزة المُدارة** وانتقل إلى علامة التبويب **الأجهزة**.
2. انقر بزر الماوس الأيمن لفتح قائمة سياق الجهاز ذي الصلة وحدد **خصائص**.
3. في النافذة خصائص الجهاز التي تُفتح، حدد القسم **التطبيقات**.
4. في قائمة التطبيقات التي تظهر، حدد التطبيق الذي تحتاج إلى تصدير أحداثه وانقر فوق الزر **خصائص**.
5. في النافذة خصائص المهمة، حدد القسم **تكوين الحدث**.
6. في قائمة الأحداث التي تظهر، حدد حدثًا أو عدة أحداث من التي تحتاج إلى التصدير إلى نظام SIEM، وانقر فوق الزر **خصائص**.
7. في نافذة خصائص الحدث التي تظهر، حدد خانة الاختيار **تصدير إلى نظام SIEM باستخدام Syslog** لوضع علامة على الأحداث المحددة لتصديرها بتنسيق Syslog. امسح خانة الاختيار **تصدير إلى نظام SIEM باستخدام Syslog** لإلغاء وضع علامة على الأحداث المحددة لتصديرها بتنسيق Syslog.

إذا تم تحديد خصائص الأحداث في السياسة، فلا يمكن تحرير حقول هذه النافذة.

نافذة خصائص الأحداث

8. انقر فوق **موافق** لحفظ التغييرات.

9. انقر فوق **موافق** في النافذة خصائص التطبيق وفي النافذة خصائص الجهاز.

سيتم إرسال الأحداث المحددة إلى نظام SIEM عبر تنسيق Syslog. الأحداث التي قمت فيها بإلغاء تحديد خانة الاختيار **تصدير إلى نظام SIEM باستخدام Syslog**، لن يتم تصديرها إلى نظام SIEM. سيبدأ التصدير بعدما تمكّن التصدير التلقائي على الفور وتحدد الأحداث التي تريد تصديرها. قم بتكوين نظام SIEM لضمان قدرته على استلام الأحداث من Kaspersky Security Center.

وضع علامة على الأحداث العامة للتصدير بتنسيق Syslog

إذا كنت تريد تصدير الأحداث التي حدثت في جميع التطبيقات المُدارة من جانب سياسة محددة، فحدد الأحداث لتصديرها في السياسة. وفي هذه الحالة، لا يمكنك تحديد أحداث لتطبيق فردي مُدار.

وضع علامة على الأحداث العامة للتصدير إلى نظام SIEM:

1. في شجرة وحدة تحكم Kaspersky Security Center، حدد العقدة **السياسات**.

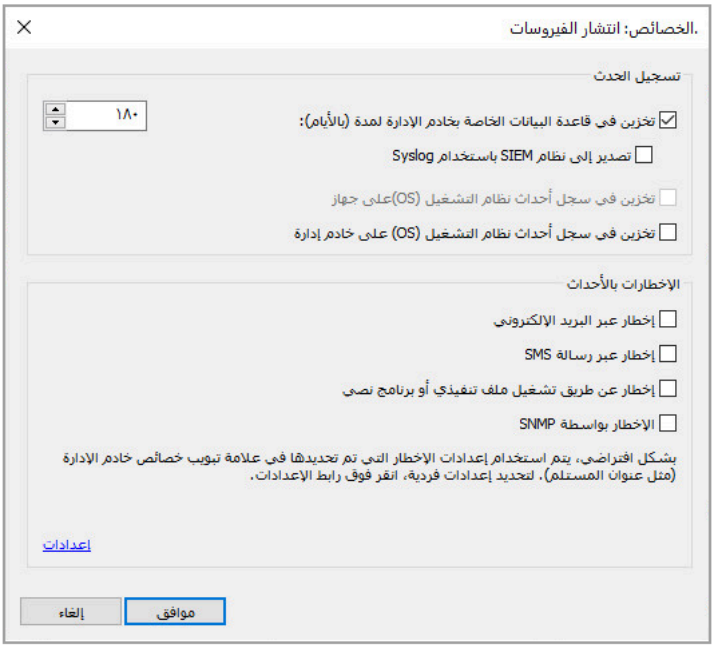
2. انقر بزر الماوس الأيمن لفتح قائمة سياق السياسة ذات الصلة وحدد **خصائص**.

3. في النافذة خصائص السياسة التي تفتح، قم بتحديد القسم **تكوين الحدث**.

4. في قائمة الأحداث التي تظهر، حدد حدثًا أو عدة أحداث من التي تحتاج إلى التصدير إلى نظام SIEM، وانقر فوق الزر **خصائص**.

   إذا كنت بحاجة إلى تحديد كل الأحداث، فانقر فوق الزر **تحديد الكل**.

5. في نافذة خصائص الحدث التي تظهر، حدد خانة الاختيار **تصدير إلى نظام SIEM باستخدام Syslog** لوضع علامة على الأحداث المحددة لتصديرها بتنسيق Syslog. قم بإلغاء تحديد خانة الاختيار **تصدير إلى نظام SIEM باستخدام Syslog** لإلغاء وضع العلامة على الأحداث المحددة لتصديرها بتنسيق Syslog.



نافذة خصائص أحداث خادم الإدارة

6. انقر فوق **موافق** لحفظ التغييرات.

7. في النافذة خصائص السياسة، انقر فوق **موافق**.

سيتم إرسال الأحداث المحددة إلى نظام SIEM عبر تنسيق Syslog. الأحداث التي قمت فيها بإلغاء تحديد خانة الاختيار **تصدير إلى نظام SIEM باستخدام Syslog**، لن يتم تصديرها إلى نظام SIEM. سيبدأ التصدير بعدما تمكّن التصدير التلقائي على الفور وتحدد الأحداث التي تريد تصديرها. قم بتكوين نظام SIEM لضمان قدرته على استلام الأحداث من Kaspersky Security Center.

حول تصدير الأحداث باستخدام تنسيق Syslog

يمكنك استخدام بروتوكول Syslog لتصدير الأحداث التي حدثت في خادم الإدارة وغيره من تطبيقات Kaspersky المثبتة على الأجهزة المُدارة إلى أنظمة SIEM.

Syslog هو البروتوكول القياسي لتسجيل الرسائل. ويسمح بفصل البرامج التي تنشئ الرسائل والنظام الذي يخزنها والبرامج التي تبلغ بها وتحللها. يتم تمييز كل رسالة برمز منشأة، للإشارة إلى نوع البرنامج الذي ينشئ الرسالة ويتم تخصيص مستوى خطورة لها.

يتم تحديد بروتوكول Syslog بواسطة مستندات طلب التعليقات (RFC) التي ينشرها فريق مهام هندسة الإنترنت (معايير الإنترنت). يُستخدم معيار RFC 5424 لتصدير الأحداث من Kaspersky Security Center إلى الأنظمة الخارجية.

في Kaspersky Security Center، يمكنك تكوين تصدير الأحداث إلى الأنظمة الخارجية باستخدام تنسيق Syslog.

تتألف عملية التصدير من خطوتين:

1. تمكين التصدير التلقائي للأحداث. في هذه الخطوة، يتم تكوين Kaspersky Security Center ليرسل الأحداث إلى نظام SIEM. يبدأ Kaspersky Security Center إرسال الأحداث على الفور بعد أن تقوم بتمكين التصدير التلقائي.

2. تحديد الأحداث لتصديرها إلى النظام الخارجي. في هذه الخطوة، تحدد الحدث لتصديره إلى نظام SIEM.

تصدير الأحداث باستخدام تنسيقات CEF وLEEF

يمكنك استخدام تنسيقات CEF وLEEF لتصدير الأحداث العامة إلى أنظمة SIEM، وكذلك الأحداث التي تنقلها تطبيقات Kaspersky إلى خادم الإدارة. تم تحديد مجموعة تصدير الأحداث مسبقًا، ولا يمكنك تحديد أحداث لتصديرها. وقبل إرسال الأحداث إلى نظام SIEM (QRadar أو ArcSight أو Splunk)، من الضروري تفسير أحداث Kaspersky Security Center إلى أحداث بتنسيقي CEF وLEEF باستخدام القواعد المحددة في ملف siem_conversion_rules.xml.

حدد تنسيق التصدير بناءً على نظام SIEM المستخدم. يوضح الجدول أدناه أنظمة SIEM وتنسيقات التصدير المطابقة.

تنسيقات تصدير الحدث إلى نظام SIEM

نظام SIEM	تنسيق التصدير
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (التنسيق الموسع لحدث السجل)— هو تنسيق حدث مخصص لـ IBM Security QRadar SIEM. بحيث يمكن لـ QRadar دمج وتحديد ومعالجة أحداث LEEF. يجب أن تستخدم أحداث LEEF ترميز أحرف UTF-8. يمكنك العثور على المعلومات المفصلة حول بروتوكول LEEF في مركز معرفة IBM.

- CEF (تنسيق الحدث العام)—مقياس لإدارة سجل مفتوح يعمل على تحسين إمكانية التشغيل التفاعلي للمعلومات المرتبطة بالأمان من مختلف أجهزة الشبكة وتطبيقات الأمان. يتيح لك تنسيق CEF استخدام تنسيق تسجيل حدث عام حتى تتمكن من تضمين البيانات بسهولة لتحليلها بواسطة نظام إدارة المؤسسة. يجب أن تستخدم أحداث CEF ترميز أحرف UTF-8.

يمثل التصدير التلقائي إرسال Kaspersky Security Center الأحداث العامة إلى نظام SIEM. يبدأ التصدير التلقائي للأحداث بعد تمكينك له على الفور. يشرح هذا القسم بالتفصيل كيفية تمكين التصدير التلقائي للحدث.

تكوين Kaspersky Security Center لتصدير الأحداث إلى نظام SIEM

يمكنك تمكين التصدير التلقائي للأحداث في Kaspersky Security Center.

يمكن فقط تصدير الأحداث العامة من التطبيقات المُدارة عبر تنسيقات CEF وLEEF. يتم تحديد قواعد التفسير المستخدمة لتحويل الأحداث إلى تنسيقي CEF وLEEF في ملف siem_conversion_rules.xml، وهو ملف مضمن في حزمة توزيع Kaspersky Security Center. يتعذر تصدير الأحداث المخصصة للتطبيق من التطبيقات المُدارة عبر تنسيقات CEF وLEEF. إذا كنت في حاجة لتصدير الأحداث من التطبيقات المُدارة أو مجموعة مخصصة من الأحداث التي تم تكوينها باستخدام سياسات التطبيقات المُدارة، فقم بتصدير الحدث عبر تنسيق Syslog.

لتمكين التصدير التلقائي للأحداث:

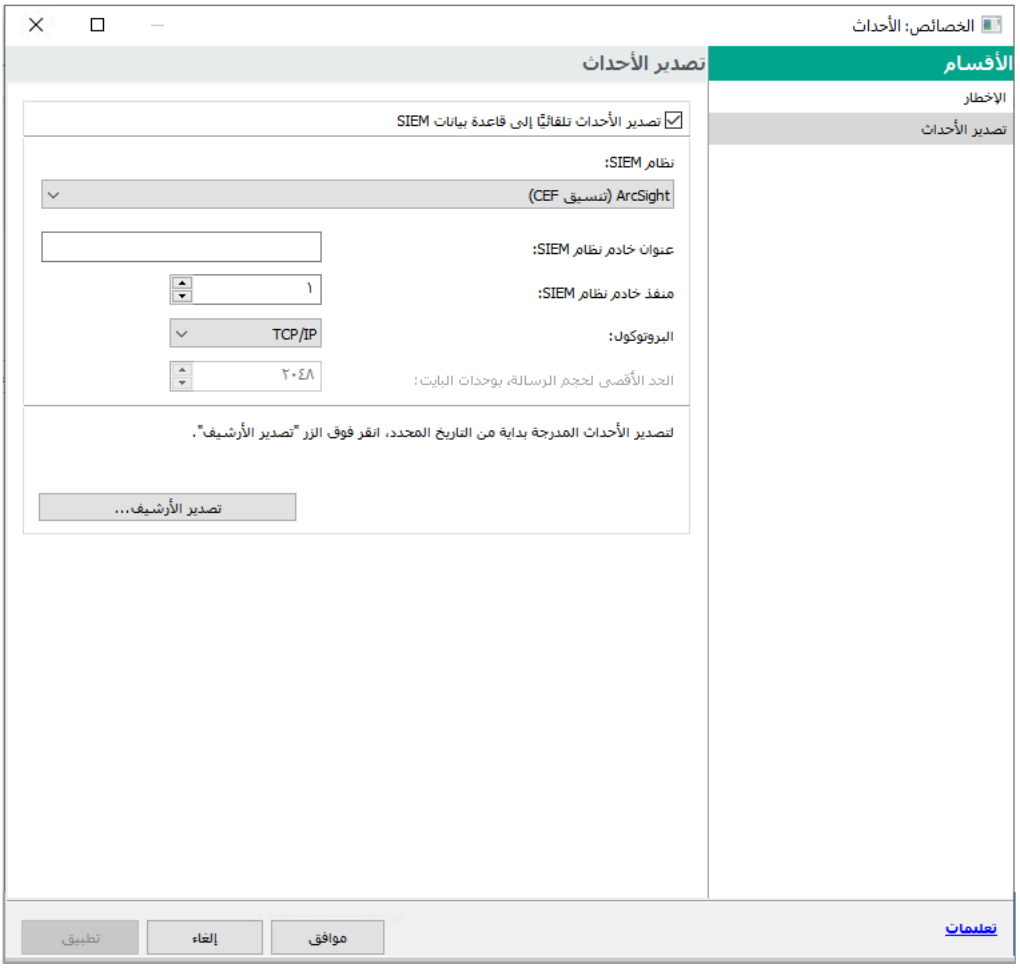
1. في شجرة وحدة تحكم Kaspersky Security Center، حدد خادم الإدارة الذي تريد تصدير أحداثه.

2. في مساحة عمل خادم الإدارة المحدد، حدد علامة التبويب **الأحداث**.

3. انقر فوق سهم القائمة المنسدلة بجوار الرابط **تكوين الإخطارات وتصدير الأحداث**، ثم حدد **تكوين التصدير إلى نظام SIEM** في القائمة المنسدلة.

   يتم فتح النافذة خصائص الأحداث، التي تعرض القسم **تصدير الأحداث**.

4. في القسم **تصدير الأحداث**، حدد إعدادات التصدير التالية:



قسم تصدير الأحداث بنافذة خصائص الأحداث

- **تصدير الأحداث تلقائيًا إلى قاعدة بيانات SIEM**

حدد خانة الاختيار هذه لتمكين التصدير التلقائي إلى أنظمة SIEM. يؤدي تحديد خانة الاختيار هذه إلى تمكين جميع الحقول في قسم **تصدير الأحداث**.

- **نظام SIEM**

حدد نظام SIEM لتصدير الأحداث:QRadar® (تنسيق LEEF)، وArcSight (تنسيق CEF) وSplunk® (تنسيق CEF) وتنسيق Syslog (RFC 5424).

إذا حددت تنسيق Syslog، فيجب عليك تحديد:

الحد الأقصى لحجم الرسالة، بوحدات البايت

حدد أقصى حجم للرسالة (بالبايت) التي يتم ترحيلها إلى نظام SIEM. يتم ترحيل كل حدث في رسالة واحدة. إذا تجاوز الطول الفعلي للرسالة القيمة المحددة، فقد يتم اقتطاع الرسالة أو فقد البيانات. الحجم الافتراضي هو 2048 بايت. يتوفر هذا الحقل فقط إذا قمت بتحديد التنسيق Syslog في الحقل **نظام SIEM**.

- **عنوان خادم نظام SIEM**

حدد عنوان خادم نظام SIEM. يمكن تحديد العنوان كاسم DNS أو NetBIOS أو كعنوان IP.

- **منفذ خادم نظام SIEM**

حدد رقم المنفذ للاتصال بخادم نظام SIEM. يجب أن يكون رقم المنفذ مطابقًا للرقم الذي يستخدمه نظام SIEM الخاص بك لاستلام الأحداث (راجع قسم تكوين نظام SIEM للاطلاع على التفاصيل).

- **البروتوكول**

حدد البروتوكول الذي سيُستخدم لنقل الرسائل إلى نظام SIEM. يمكنك تحديد TCP أو UDP أو TLS عبر بروتوكول TCP.

حدد إعدادات TLS التالية إذا قمت بتحديد TLS عبر بروتوكول TCP:

- **مصادقة خادم SIEM**

اختر إحدى الطرق التالية لمصادقة خادم نظام SIEM:

- **من خلال استخدام شهادات CA**. يمكنك استلام ملف بقائمة الشهادات من مرجع مصدق موثوق به (CA) وتحميل الملف إلى Kaspersky Security Center. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم نظام SIEM موقعة أيضًا من قِبل مرجع مصدق موثوق أم لا.

  لإضافة شهادة موثوقة، انقر فوق زر **استعراض**، ثم قم بتحميل الشهادة.

  إذا قمت بتحديد خيار **من خلال استخدام شهادات CA**، يمكنك تحديد أسماء الموضوعات في حقل **مواضيع شهادات الخادم (اختياري)**. اسم الموضوع هو اسم المجال الذي تم استلام الشهادة من أجله. لا يمكن لـ Kaspersky Security Center الاتصال بخادم نظام SIEM إذا كان اسم المجال لخادم نظام SIEM لا يتطابق مع اسم موضوع شهادة خادم نظام SIEM. ومع ذلك، يستطيع خادم نظام SIEM تغيير اسم المجال الخاص به في حالة تغيير الاسم في الشهادة. للقيام بذلك، حدد أسماء الموضوعات في حقل **مواضيع شهادات الخادم (اختياري)**. إذا تطابق أيٍ من أسماء الموضوعات المحددة مع اسم موضوع شهادة نظام SIEM، فسيتحقق Kaspersky Security Center من صحة شهادة خادم نظام SIEM.

- **باستخدام بصمات SHA1 لشهادات الخادم**. يمكنك تحديد بصمات الإبهام SHA-1 لشهادات نظام SIEM في Kaspersky Security Center. لإضافة بصمة إبهام SHA-1، أدخلها في الحقل الموجود أسفل الخيار.

- **مصادقة العميل**

لمصادقة العميل، يمكنك إدخال شهادتك أو إنشائها في Kaspersky Security Center.

- **إدراج الشهادة**. يمكنك استخدام شهادة استلمتها من أي مصدر، على سبيل المثال، من أي جهة إصدار موثوقة. لإدراج شهادة موجودة، انقر فوق زر **تصفح الشهادة**. في نافذة **الشهادة** المفتوحة، اختر أحد أنواع الشهادات التالية، ثم حدد الشهادة ومفتاحها الخاص:

  - **الشهادة X.509**. قم برفع ملف مع المفتاح الخاص بتنسيق حقل **المفتاح الخاص (*.prk, *.pem.)**، وملف بشهادة في حقل **شهادة (*.cer.)**. للقيام بذلك، انقر فوق زر **استعراض** على يمين الحقل المقابل، ثم أضف الملف المطلوب. كلا الملفين لا يعتمدان على بعضهما البعض وترتيب تحميل الملفات ليس مهمًا. بعد رفع كلا الملفين، حدد كلمة المرور لفك تشفير المفتاح الخاص في حقل **كلمة المرور**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

  - **الحاوية PKCS#12**. ارفع ملف واحد يحتوي على شهادة ومفتاحها الخاص في حقل **ملف الشهادة**. للقيام بذلك، انقر فوق زر **استعراض** الموجود على يمين الحقل، ثم أضف الملف المطلوب. بعد رفع الملف، حدد كلمة المرور لفك تشفير المفتاح الخاص في حقل **كلمة المرور**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- **أنشئ مفتاح**. يمكنك إنشاء شهادة موقعة ذاتيًا في Kaspersky Security Center. انقر على **إنشاء شهادة جديدة**، ثم أدخل اسم موضوع في حقل **الموضوع**. يتم إنشاء شهادة العميل لاسم الموضوع هذا ويتم عرض بصمة SHA-1 لهذه الشهادة في حقل **بصمة SHA1 لشهادة العميل**. نتيجة لذلك، يخزن Kaspersky Security Center الشهادة الموقعة ذاتيًا التي تم إنشاؤها، ويمكنك تمرير الجزء العام من الشهادة أو بصمة SHA1 إلى نظام SIEM.

5. إذا كنت تريد تصدير الأحداث التي حدثت بعد تاريخ محدد في الماضي إلى قاعدة بيانات نظام SIEM، فانقر فوق الزر **تصدير الأرشيف**، ثم حدد تاريخ بدء تصدير الأحداث. سيبدأ تصدير الحدث بشكل افتراضي بعد تمكينك له على الفور.

6. للتحقق من تكوين اتصال نظام SIEM، انقر فوق الزر **اختبار الإعدادات**.

   يحاول التطبيق إنشاء اتصال مع خادم نظام SIEM وإرسال حدث اختبار. إذا لم يتم إنشاء الاتصال، يتم عرض رسالة خطأ. إذا تم إنشاء الاتصال، فلن يتم عرض أي رسالة. يمكنك عرض حدث الاختبار في علامة التبويب **الأحداث**، إذا لزم الأمر.

7. انقر على**موافق**.

   تم تمكين التصدير التلقائي للأحداث.

بعد تمكين التصدير التلقائي للأحداث، يجب عليك تحديد الأحداث التي سيتم تصديرها إلى نظام SIEM.

تصدير الأحداث مباشرة من قاعدة البيانات

يمكنك استعادة الأحداث مباشرة من قاعدة بيانات Kaspersky Security Center دون استخدام واجهة Kaspersky Security Center. يمكنك إما الاستعلام عن الآراء العامة مباشرة واستعادة بيانات الحدث أو إنشاء الآراء الخاصة بك بناءً على الآراء العامة الموجودة وتناولها لجمع البيانات التي تحتاج إليها.

الآراء العامة

لتسهيل الأمر عليك، يتم توفير مجموعة من الآراء العامة في قاعدة بيانات Kaspersky Security Center. يمكنك العثور على وصف طرق العرض العامة هذه في المستند klakdb.chm.

يشتمل الرأي العام v_akpub_ev_event على مجموعة حقول تمثل معلمات الحدث في قاعدة البيانات. في الوثيقة klakdb.chm يمكنك أيضًا العثور على معلومات حول الآراء العامة المطابقة لكيانات Kaspersky Security Center الأخرى، على سبيل المثال، الأجهزة أو التطبيقات أو المستخدمين. يمكنك استخدام هذه المعلومات في استعلاماتك.

يحتوي هذا القسم على تعليمات لتنفيذ استعلام SQL بواسطة أداة klsql2 المساعدة ومثال الاستعلام.

لإنشاء استعلامات SQL أو آراء قاعدة البيانات، يمكنك أيضًا استخدام أي برنامج آخر للتعامل مع قوعد البيانات. يتم ذكر معلومات حول كيفية عرض المعلمات للاتصال بقاعدة بيانات Kaspersky Security Center، مثل اسم المثيل واسم قاعدة البيانات، في القسم المقابل.

تنفيذ استعلام SQL باستخدام أداة klsql2 المساعدة

توضح هذه المقالة كيفية تنزيل أداة klsql2 المساعدة واستخدامها، وكيفية تنفيذ استعلام SQL باستخدام هذه الأداة المساعدة.

لاستخدام أداة klsql2 المساعدة:

1. حدد موقع الأداة المساعدة klsql2 في مجلد تثبيت Kaspersky Security Center. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. لا تستخدم إصدارات الأداة المساعدة klsql2 المخصصة لإصدارات Kaspersky Security Center الأقدم.

2. أنشئ ملفًا بملحق .sql في أي محرر نصوص وضع الملف في المجلد نفسه باستخدام الأداة المساعدة.

3. في ملف .sql الذي تم إنشاؤه، اكتب الاستعلام الذي تريده، ثم احفظ الملف.

4. في الجهاز المثبت عليه خادم إدارة Kaspersky Security Center، في سطر الأوامر، اكتب الأمر التالي لتنفيذ استعلام SQL من الملف .sql واحفظ النتائج على الملف result.xml:

```
o result.xml- <password> p- <username> klsql2 -i src.sql -u
```

حيث <username> و <password> هما بيانات اعتماد حساب المستخدم الذي يمتلك حق الوصول إلى قاعدة البيانات.

5. وإذا لزم الأمر، أدخل معلومات تسجيل الدخول وكلمة المرور لحساب المستخدم الذي يمكنه الوصول إلى قاعدة البيانات.

6. افتح ملفات result.xml التي تم إنشاؤها حديثًا لعرض نتائج استعلام SQL.

يمكنك تحرير الملف .sql وإنشاء أي استعلام SQL للعروض العامة. بعد ذلك، من سطر الأوامر، قم بتنفيذ استعلام SQL واحفظ النتائج في ملف.

مثال لاستعلام SQL في أداة klsql2 المساعدة

يعرض هذا القسم مثالاً لاستعلام SQL، الذي يتم تنفيذه بواسطة أداة klsql2 المساعدة.

توضح الأمثلة التالية استعادة الأحداث التي حدثت في الأجهزة خلال السبعة أيام الماضية، وعرضًا للأحداث التي طُلبت وقت حدوثها، ويتم عرض الأحداث الأخيرة أولاً. ويتم عرض الأحداث الأخيرة أولاً.

مثال لبرنامج Microsoft SQL Server:

```
SELECT
/* معرف الحدث */
,e.nId

/* الوقت الذي وقع فيه الحدث */
,e.tmRiseTime

/* الاسم الداخلي لنوع الحدث */
,e.strEventType

/* الاسم المعروض للحدث */
,e.wstrEventTypeDisplayName

/* الوصف المعروض للحدث */
,e.wstrDescription

/* اسم المجموعة حيث يوجد الجهاز */
,e.wstrGroupName

/* الاسم المعروض للجهاز الذي وقع عليه الحدث */
,h.wstrDisplayName
+ '.' + ((4)AS varchar (255 & (h.nIp / 16777216)))CAST
+ '.' + ((4)AS varchar (255 & (h.nIp / 65536)))CAST
+ '.' + ((4)AS varchar (255 & (h.nIp / 256)))CAST

/* عنوان IP للجهاز الذي وقع عليه الحدث */
as strIp ((4)AS varchar (255 & (h.nIp)))CAST
FROM v_akpub_ev_event e
e.nHostId=INNER JOIN v_akpub_host h ON h.nId
(()GETUTCDATE ,7- ,Day)DATEADD=<WHERE e.tmRiseTime
ORDER BY e.tmRiseTime DESC
```

مثال لبرنامج PostgreSQL:

```
SELECT
/* معرف الحدث */
"nId"."e",

/* الوقت الذي وقع فيه الحدث */
"tmRiseTime"."e",

/* الاسم الداخلي لنوع الحدث */
"strEventType"."e",

/* الاسم المعروض للحدث*/
"wstrEventTypeDisplayName"."e",

/* الوصف المعروض للحدث */
"wstrDescription"."e",

/* الوصف المعروض للحدث */
"wstrGroupName"."e",

/* الاسم المعروض للجهاز الذي وقع عليه الحدث */
"wstrDisplayName"."h",
)
||  '.' ||  ((4)AS VARCHAR ( 255 &( 16777216 / "nIp"."h")))CAST
||  '.' ||  ((4)AS VARCHAR ( 255 &( 65536 / "nIp"."h")))CAST
||  '.' ||  ((4)AS VARCHAR ( 255 &( 256 / "nIp"."h")))CAST

/* عنوان IP للجهاز الذي وقع عليه الحدث */
((4)AS VARCHAR ( 255 &( "nIp"."h")))CAST
"strIp" AS  (
"e" AS  "v_akpub_ev_event" FROM
"nHostId"."e" = "nId"."h" ON "h" AS  "v_akpub_host"  INNER JOIN
((7  AS INT-)CAST <= days)make_interval +  'utc' AT TIME ZONE ()NOW =< "tmRiseTime"."e" WHERE
; DESC "tmRiseTime"."e" ORDER BY
```

مثال لبرنامج MySQL أو MariaDB:

```
SELECT

/* معرف الحدث */
`nId`.`e`,

/* الوقت الذي وقع فيه الحدث */
`tmRiseTime`.`e`,

/* الاسم الداخلي لنوع الحدث */
`strEventType`.`e`,

/* الاسم المعروض للحدث */
`wstrEventTypeDisplayName`.`e`,

/* الوصف المعروض للحدث */
`wstrDescription`.`e`,

/* اسم مجموعة الأجهزة */
`wstrGroupName`.`e`,

/* الاسم المعروض للجهاز الذي وقع عليه الحدث */
`wstrDisplayName`.`h`,
)CONCAT
,'.' ,(4 ,(AS CHAR (255 & (DIV  1677721  `nIp`.`h`)))CAST)LEFT
,'.' ,(4 ,(AS CHAR (255 & (DIV  65536  `nIp`.`h`)))CAST)LEFT
,'.' ,(4 ,(AS CHAR (255 & (DIV  256  `nIp`.`h`)))CAST)LEFT

/* عنوان IP للجهاز الذي وقع عليه الحدث */
(4 ,(AS CHAR (255 & (`nIp`.`h`)))CAST)LEFT
`strIp` AS  (
`e` AS  `v_akpub_ev_event` FROM
`nHostId`.`e` = `nId`.`h` ON `h` AS  `v_akpub_host`  INNER JOIN
(INTERVAL -7  DAY , ( )UTC_TIMESTAMP )ADDDATE =< `tmRiseTime`.`e` WHERE
; DESC `tmRiseTime`.`e` ORDER BY
```

عرض اسم قاعدة بيانات Kaspersky Security Center

قد يكون من المفيد معرفة اسم قاعدة البيانات إذا كنت بحاجة، على سبيل المثال، إلى إرسال استعلام SQL والاتصال بقاعدة البيانات من محرر البرنامج النصي SQL.

لعرض اسم قاعدة بيانات Kaspersky Security Center:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وحدد **خصائص**.
2. في النافذة خصائص خادم الإدارة، من جزء الأقسام، حدد **خيارات متقدمة** ثم **تفاصيل قاعدة البيانات الحالية**.
3. في القسم **تفاصيل قاعدة البيانات الحالية**، لاحظ خصائص قاعدة البيانات التالية (انظر الشكل أدناه):

- **اسم المثيل**

  اسم مثيل قاعدة البيانات Kaspersky Security Center الحالية. القيمة الافتراضية هي .\KAV_CS_ADMIN_KIT.

- **اسم قاعدة البيانات**

  اسم قاعدة بيانات Kaspersky Security Center SQL. القيمة الافتراضية هي KAV.

- **المساحة المخصصة لقاعدة بيانات Kaspersky Security Center**

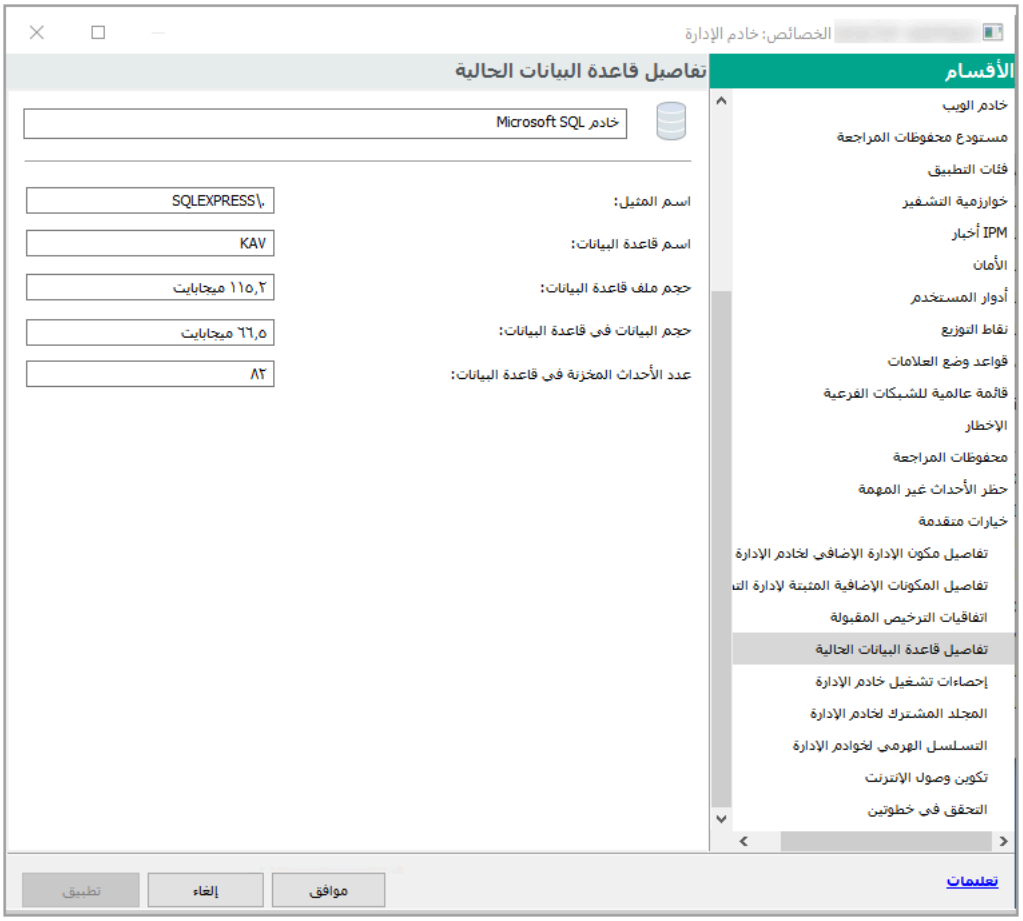
  حجم ملف قاعدة البيانات. إذا كنت تريد تنظيف البيانات غير الضرورية، فقم بتكوين ضغط قواعد البيانات باستخدام المهمة صيانة خادم الإدارة.

- **حجم البيانات في قاعدة البيانات بأكملها**

  الحجم الفعلي للبيانات المستخدمة حاليًا في نظام إدارة قاعدة البيانات. يصف المقال التالي كيفية تشخيص نظام إدارة قاعدة البيانات: حجم قاعدة البيانات يتجاوز الحد الأقصى.

- **عدد الأحداث المخزنة في قاعدة البيانات**

عدد الأحداث المخزنة حاليًا في نظام إدارة قاعدة البيانات. راجع المقال التالي للحصول على التفاصيل: معالجة الأحداث وتخزينها.



قسم يحتوي على معلومات حول قاعدة بيانات خادم الإدارة الحالية.

4. انقر فوق الزر **موافق** لإغلاق النافذة خصائص خادم الإدارة.

استخدام اسم قاعدة البيانات لمعالجة قاعدة البيانات في استعلامات SQL الخاصة بك.

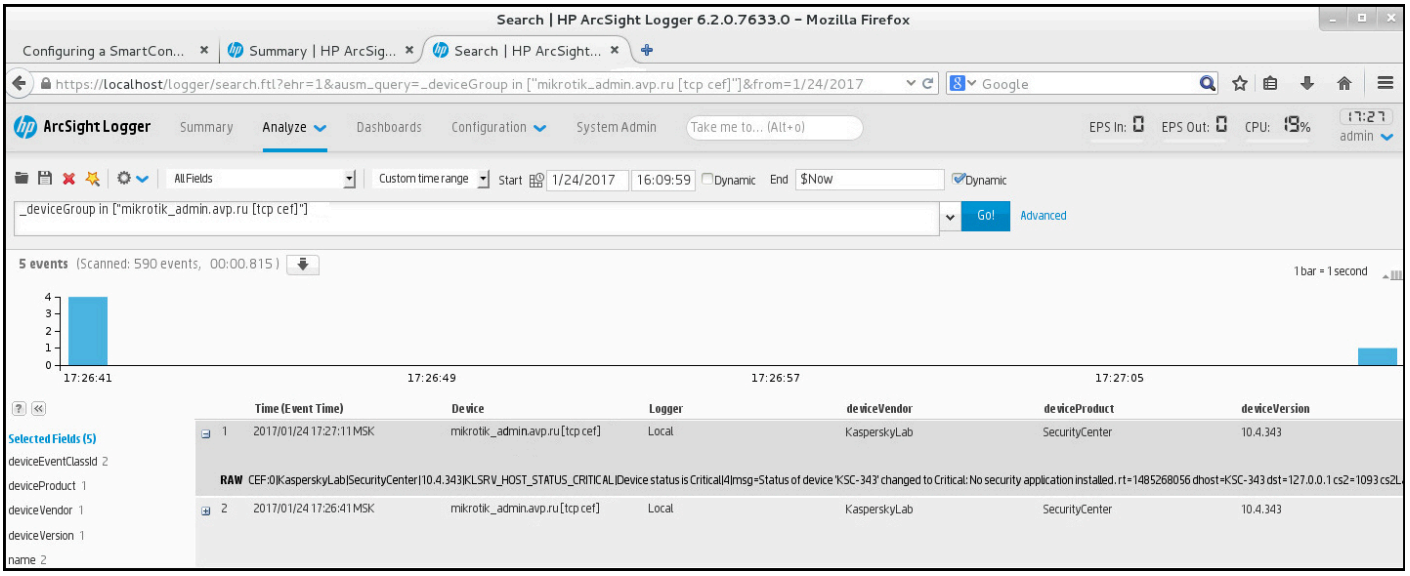
عرض نتائج التصدير

يمكنك التحكم في إكمال إجراء تصدير الحدث بنجاح. وللقيام بهذا الإجراء، تحقق من استلام نظام SIEM الخاص بك للرسائل المشتملة على أحداث التصدير

إذا تم استلام الأحداث المرسلة من Kaspersky Security Center وتحليلها على النحو الصحيح بواسطة نظام SIEM الخاص بك، فسيتم تنفيذ التكوين بشكل صحيح على كلا الجانبين. في الجانب الآخر، تحقق من أن الإعدادات التي حددتها في Kaspersky Security Center مقابلة للتكوين في نظام SIEM الخاص بك.

يوضح الشكل أدناه الأحداث التي تم تصديرها إلى ArcSight. على سبيل المثال، يعتبر الحدث الأول حدثًا مهمًا لخادم الإدارة: "حالة الجهاز حرجة".

يتباين تمثيل أحداث التصدير في نظام SIEM بحسب نظام SIEM الذي تستخدمه.



مثال للأحداث

استخدام SNMP في إرسال الإحصاءات إلى تطبيقات الأطراف الخارجية

هذا القسم يصف كيفية الحصول على معلومات من خادم إدارة باستخدام بروتوكول إدارة الشبكة البسيط (SNMP) في Kaspersky Security Center. Windows يحتوي على عميل SNMP، وهو ينقل إحصاءات أداء خادم الإدارة للتطبيقات الجانبية باستخدام معرفات الكائنات.

يحتوي هذا القسم كذلك على معلومات عن حل المشكلات التي قد تواجهها أثناء استخدام SNMP مع Kaspersky Security Center.

تكوين خدمة SNMP للاستخدام مع Kaspersky Security Center

يصف هذا القسم كيفية تكوين خدمة SNMP على نظام التشغيل Windows للحصول على معلومات من خادم الإدارة باستخدام بروتوكول إدارة الشبكة البسيط (SNMP).

يتم تعطيل دعم SNMP افتراضيًا على نظام Windows.

لتمكين دعم SNMP في نظام التشغيل Windows:

1. انتقل إلى **لوحة التحكم**.
2. افتح قائمة **إضافة أو إزالة البرامج**.
3. انقر على **تشغيل ميزات Windows** أو **إيقاف تشغيلها**.
4. في قائمة ميزات Windows، انتقل إلى ميزة SNMP، ثم انقر على **موافق**.
5. انتقل إلى **لوحة التحكم** ← **أدوات إدارية** ← **خدمات**.

6. اختر **خدمة SNMP** وقم بتشغيلها.

7. تحقق مما إذا كان الاستماع يعمل عن طريق اختباره باستخدام `netstat` للحصول على منفذ UDP قياسي.

يتم تمكين دعم SNMP على نظام التشغيل Windows.

لتكوين خدمات SNMP على نظام التشغيل Windows:

1. تأكد من تثبيت مكون **وكيل SNMP** الخاص بحل Kaspersky Security Center أثناء التثبيت العادي أو الصامت.

2. تأكد من تشغيل **خدمة SNMP** وخدمات **تراكب SNMP** على نظام Windows.

3. تأكد من تثبيت مستعرض ManageEngine MIB على نظامك.

4. في خصائص **خدمة SNMP**، في علامة التبويب **الأمان**، أضف مجتمعين بالصلاحيات التالية:

المجتمع	الحقوق
kaspersky	الإخطار
public	READ WRITE

5. في الحقل **قبول حزم SNMP من هذه الأجهزة المضيفة**، أضف عنوان IP للجهاز حيث تم تثبيت مستعرض ManageEngine MIB، على سبيل المثال، 10.10.10.105.

6. في علامة التبويب **التراكبات**، اكتب `kaspersky` في الحقل **اسم المجتمع**.

7. انقر فوق **موافق** لحفظ التغييرات وإغلاق نافذة خصائص الخدمة.

8. في مستعرض ManageEngine MIB، قم بتحميل ملف adminkit.mib من مجلد تثبيت Kaspersky Security Center. بشكل افتراضي، يوجد ملف adminkit.mib في المجلد <القرص>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp.

9. في الحقل **المضيف** من نافذة مستعرض ManageEngine MIB، أضف عنوان IP للجهاز حيث تم تثبيت خادم إدارة Kaspersky Security Center.

تم تكوين خدمة SNMP للحصول على معلومات من خادم الإدارة باستخدام بروتوكول إدارة الشبكة البسيط (SNMP).

عميل SNMP ومعرفات الكائنات

بالنسبة إلى Kaspersky Security Center، يتم تطبيق عميل SNMP على أنه مكتبة ديناميكية `klsnmpag.dll`، والتي يتم تسجيلها بواسطة المثبت أثناء تثبيت خادم الإدارة. يعمل عميل SNMP داخل عملية `snmp.exe` (وهي إحدى خدمات Windows). تطبيقات الأطراف الخارجية تستخدم SNMP في استلام الإحصائيات التي تأتي في شكل عدادات عن أداء خادم الإدارة.

يحتوي كل عداد على معرف كائن فريد (يشار إليه أيضًا باسم OID). معرف الكائن هو سلسلة من الأرقام المقسمة باستخدام نقاط. تبدأ معرفات كائنات خادم الإدارة بالبادئة 1.3.6.1.4.1.23668.1093. معرف الكائن الخاص بالعداد عبارة عن سلسلة من هذه البادئة مزودة بلاحقة تصف العداد. على سبيل المثال: العداد الذي يحتوي على قيمة OID 1.3.6.1.4.1.23668.1093.1.1.4 له لاحقة بقيمة 1.1.4.

يمكنك استخدام عميل SNMP (مثل Zabbix) لمراقبة حالة نظامك. للحصول على المعلومات، يمكنك البحث عن قيمة OID التي تتوافق مع المعلومات وإدخال هذه القيمة في عميل SNMP الخاص بك. بعدها عميل SNMP سيعيد لك قيمة أخرى تميز حالة نظامك.

قائمة العدادات وأنواع العدادات توجد في ملف `adminkit.mib` على خادم الإدارة. يشير اختصار MIB إلى قاعدة معلومات الإدارة. يمكنك استيراد ملفات `mib.` وتحليلها عبر تطبيق MIB Viewer المصمم لطلب الحصول على قيم العداد وعرضها.

الحصول على عداد سلاسل من معرف كائن.

من أجل استخدام معرف الكائن (OID) لنقل المعلومات إلى تطبيقات الأطراف الخارجية، قد تحتاج إلى الحصول على اسم عداد سلسلة من معرف الكائن هذا.

لمعرفة اسم عداد سلاسل من معرف كائن:

1. افتح ملف `adminkit.mib` الموجود على خادم الإدارة باستخدام محرر نصي.
2. حدد مساحة الاسم التي تصف القيمة الأولى (من اليسار إلى اليمين).

   على سبيل المثال: بالنسبة لمعرف الكائن 1.1.4، ستكون اللاحقة هي `({ kladminkit 1 } =::) "counters"`.
3. حدد مساحة الاسم التي تصف القيمة الثانية.

   على سبيل المثال: بالنسبة لمعرف الكائن 1.1.4، ستكون اللاحقة هي `counters 1`، والتي تمثل `deployment`.
4. حدد مساحة الاسم التي تصف القيمة الثالثة.

   على سبيل المثال: بالنسبة لمعرف الكائن 1.1.4، ستكون اللاحقة هي `deployment 4`، والتي تمثل `hostsWithAntivirus`.

اسم عداد السلسلة هو سلسلة من هذه القيم، على سبيل المثال `MIB base>` `counters.deployment.hostsWithAntivirus.<namespace` وهو يتوافق مع OID بقيمة 1.3.6.1.4.1.23668.1093.1.1.4.

قيم معرفات الكائنات لـ SNMP

يعرض الجدول أدناه قيم وأوصاف معرفات الكائنات (يشار إليها أيضًا باسم OIDs)، المستخدمة في نقل معلومات أداء خادم الإدارة إلى تطبيقات الأطراف الخارجية.

قيم وأوصاف معرفات كائنات SNMP

قيمة معرف الكائن	نوع البيانات الرقمية	معرف الكائن	الوصف
`deploymentStatus`	`} INTEGER {(0)ok ,(1)info ,(2)warning ,(3)critical`	1.3.6.1.4.1.23668.1093.1.1.1.	حالة النشر. يمكن أن تكون الحالة أي مما يلي: • **معلومات**. الترخيص لم يعد صالحًا لعدد N أجهزة. • **تحذير**. واحد مما يلي: يوجد M أجهزة مثبت عليها تطبيقات Kaspersky على إجمالي N في مجموعات خادم الإدارة (M < N). الترخيص L ينتهي على N أجهزة خلال M أيام. المهمة T لتثبيت التطبيقات قد اكتملت بنجاح على N أجهزة، وإعادة التشغيل مطلوبة لعدد M أجهزة. • **حرج**. الترخيص انتهى لعدد N أجهزة. • **جيد**. ولا واحد مما سبق.
`noAntivirusSoftware`	`} INTEGER { (1)on ,(0)off } `	1.3.6.1.4.1.23668.1093.1.1.2.1.	تعرض `deploymentStatus` أن مجموعة خادم الإدارة تحتوي على الكثير من الأجهزة دون تطبيقات مُدارة. تساوي القيمة 1 في حالة العثور على عدد قليل من الأجهزة دون تطبيقات مُدارة، و0 بخلاف ذلك.
`remoteInstallTaskFailed`	`} INTEGER { (1)on ,(0)off } `	1.3.6.1.4.1.23668.1093.1.1.2.2.	تعرض `deploymentStatus` أن مهمة التثبيت عن بُعد قد تعذرت على بعض الأجهزة. يمكن معرفة عدد تلك الأجهزة عبر `hostsRemoteInstallFailed`.
`licenceExpiring`	`} INTEGER { (1)on ,(0)off } `	1.3.6.1.4.1.23668.1093.1.1.2.3.	تعرض `deploymentStatus` أنه يوجد بعض الأجهزة بترخيص ينتهي خلال الأيام السبعة القادمة. يمكن معرفة عدد تلك الأجهزة عبر `hostsLicenseExpiring`.
`licenceExpired`	`} INTEGER { (1)on ,(0)off } `	1.3.6.1.4.1.23668.1093.1.1.2.4.	تعرض `deploymentStatus` أنه يوجد بعض الأجهزة ذات ترخيص منتهي الصلاحية. يمكنك معرفة عدد تلك الأجهزة عبر `hostsLicenseExpired`.
`hostsInGroups`	`Counter32`	1.3.6.1.4.1.23668.1093.1.1.3.	عدد الأجهزة في مجموعات خادم الإدارة.

قيمة معرف الكائن	نوع البيانات الرقمية	معرف الكائن	الوصف
hostsWithAntivirus	Counter32	1.3.6.1.4.1.23668.1093.1.1.4.	عدد الأجهزة في مجموعات خادم الإدارة المثبت عليها تطبيقات مُدارة.
hostsRemoteInstallFailed	Counter32	1.3.6.1.4.1.23668.1093.1.1.5.	عدد الأجهزة التي تعذر عليها مهمة التثبيت عن بُعد.
licenceExpiringSerial	OCTET STRING	1.3.6.1.4.1.23668.1093.1.1.6.	معرف مفتاح ترخيص تنتهي صلاحيته خلال أقل من 7 أيام.
licenceExpiredSerial	OCTET STRING	1.3.6.1.4.1.23668.1093.1.1.7.	معرف مفتاح الترخيص المنتهي.
licenceExpiringDays	Unsigned32	1.3.6.1.4.1.23668.1093.1.1.8.	عدد الأيام قبل انتهاء صلاحية الترخيص. وبالنسبة لهذه المعلمة، تعتبر فترة الترخيص منتهية الصلاحية إذا كان هناك أقل من 7 أيام متبقية حتى تاريخ انتهاء الصلاحية. وإذا تبقت أكثر من 7 أيام على تاريخ انتهاء الصلاحية، فستكون القيمة 0.
hostsLicenceExpiring	Counter32	1.3.6.1.4.1.23668.1093.1.1.9.	عدد الأجهزة ذات ترخيص تنتهي صلاحيته خلال أقل من 7 أيام.
hostsLicenceExpired	Counter32	1.3.6.1.4.1.23668.1093.1.1.10.	عدد الأجهزة التي قد انتهى ترخيصها.
updatesStatus	INTEGER { (0)ok, (1)info, (2)warning, (3)critical }	1.3.6.1.4.1.23668.1093.1.2.1.	الحالة الحالية لتحديث قواعد مكافحة الفيروسات. يمكن أن تكون الحالة أي مما يلي: • **معلومات**. لم يتم تحديث قواعد مكافحة الفيروسات على خادم الإدارة أو على الأجهزة منذ أكثر من يوم واحد، ومر أقل من يوم واحد على تثبيت التطبيق. • **تحذير**. لم يتم تحديث قواعد مكافحة الفيروسات على خادم الإدارة أو على الأجهزة منذ أكثر من 3 أيام. ويمكن تغيير هذه القيمة في إعدادات المجموعة. • **حرج**. لم يتم تحديث قواعد مكافحة الفيروسات على خادم الإدارة أو على الأجهزة منذ أكثر من 7 أيام. ويمكن تغيير هذه القيمة في إعدادات المجموعة. • **جيد**. ولا واحد مما سبق.
serverNotUpdated	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.2.2.1.	لم يتم تحديث خادم الإدارة منذ فترة طويلة. كمية الوقت التي تعتبر طويلة يتم تحديدها في updatesStatus.
notUpdatedHosts	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.2.2.2.	لم يتم تحديث بعض الأجهزة منذ فترة طويلة (بشكل افتراضي، 7 أيام أو أكثر لحالات **حرج** و3 أيام لحالات **تحذير**). يمكنك معرفة عدد تلك الأجهزة عبر hostsNotUpdated.
lastServerUpdateTime	OCTET STRING	1.3.6.1.4.1.23668.1093.1.2.3.	آخر مرة تم فيها تحديث قواعد مكافحة الفيروسات على خادم الإدارة.
hostsNotUpdated	Counter32	1.3.6.1.4.1.23668.1093.1.2.4.	عدد الأجهزة التي تحتوي على قواعد مكافحة الفيروسات التي لم يتم تحديثها منذ فترة طويلة (بشكل افتراضي، 7 أيام أو أكثر للحالة **حرج** و3 أيام للحالة **تحذير**). وإذا كانت هناك أجهزة بحالة تحديث **حرج** فلن يتم وضع أجهزة أخرى في الاعتبار. ويمكنك الحصول على حالة التحديث عبر updatesStatus.
protectionStatus	INTEGER { (0)ok, (2)warning, (3)critical }	1.3.6.1.4.1.23668.1093.1.3.1.	حالة الحماية في الوقت الحقيقي. واحد مما يلي: • **تحذير**. واحد مما يلي: تم الكشف عن وجود اختراق أمني على جهاز ينتمي إلى مجموعة خادم الإدارة. أخطاء التشفير جعلت بعض الأجهزة تغير حالة الحماية لها. لم يتم إجراء فحص كامل منذ مدة طويلة. • **حرج**. لا تعمل الحماية ضد الفيروسات على بعض الأجهزة الموجودة في مجموعات خادم الإدارة. • **جيد**. ولا واحد مما سبق.
antivirusNotRunning	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.3.2.1.	لا يعمل تطبيق أمان على بعض الأجهزة. يمكنك معرفة عدد تلك الأجهزة عبر hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.3.2.2.	لا تعمل الحماية في الوقت الحقيقي على بعض الأجهزة. يمكنك معرفة عدد تلك الأجهزة عبر hostsRealtimeNotRunning.
psRealtimeLevelChanged	Counter32	1.3.6.1.4.1.23668.1093.1.3.2.3.	عدد الأجهزة التي يختلف مستوى حمايتها في الوقت الحقيقي عن المستوى الذي حدده المسؤول
notCuredFound	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.3.2.4.	توجد أجهزة تحتوي على كائنات لم يتم تنظيفها. يمكنك معرفة عدد تلك الأجهزة عبر hostsNotCuredObject.
tooManyThreats	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.3.2.5.	تم العثور على تهديدات على بعض الأجهزة. يمكنك معرفة عدد تلك الأجهزة عبر hostsTooManyThreats.
virusOutbreak	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.3.2.6.	حالة انتشار الفيروس داخل النظام. القيمة تساوي 1 إذا تم العثور على كمية معينة من الفيروسات خلال فترة زمنية معينة، و0 بخلاف ذلك. يتم تحديد مقدار الفيروسات ومقدار الوقت على خادم الإدارة، باستخدام إعدادات Virus attack.

قيمة معرف الكائن	نوع البيانات الرقمية	معرف الكائن	الوصف
psVulnerabilitiesFound	INTEGER { (1)on ,(0)off }	1.3.6.1.4.1.23668.1093.1.3.2.7.	تم اكتشاف ثغرات أمنية.
psEncryptionFaultsFound	INTEGER { (1)on ,(0)off }	1.3.6.1.4.1.23668.1093.1.3.2.8.	تم اكتشاف أخطاء تشفير غيرت حالة حماية الجهاز.
psVulnerableHostsFound	INTEGER { (1)on ,(0)off }	1.3.6.1.4.1.23668.1093.1.3.2.9.	تم اكتشاف ثغرات أمنية على بعض الأجهزة.
psNotScannedLately	INTEGER { (1)on ,(0)off }	1.3.6.1.4.1.23668.1093.1.3.2.10.	تم اكتشاف أجهزة لم يتم إجراء فحص كامل لها لفترة طويلة.
psNagentsNotRunningUntilReboot	INTEGER { (1)on ,(0)off }	1.3.6.1.4.1.23668.1093.1.3.2.11.	أجهزة يبدأ فيها عميل الشبكة فقط بعد اكتشاف عملية إعادة تشغيل.
hostsAntivirusNotRunning	Counter32	1.3.6.1.4.1.23668.1093.1.3.3.	عدد الأجهزة التي لا تعمل عليها تطبيقات الأمان.
hostsRealtimeNotRunning	Counter32	1.3.6.1.4.1.23668.1093.1.3.4.	عدد الأجهزة التي لا تعمل عليها الحماية في الوقت الحقيقي.
hostsRealtimeLevelChanged	Counter32	1.3.6.1.4.1.23668.1093.1.3.5.	عدد الأجهزة المزودة بمستوى غير مقبول من الحماية في الوقت الحقيقي.
hostsNotCuredObject	Counter32	1.3.6.1.4.1.23668.1093.1.3.6.	عدد الأجهزة التي تحتوي على كائنات لم يتم تنظيفها.
hostsTooManyThreats	Counter32	1.3.6.1.4.1.23668.1093.1.3.7.	عدد الأجهزة التي تحتوي على تهديدات.
fullscanStatus	INTEGER { (0)ok ,(1)info , (2)warning , (3)critical }	1.3.6.1.4.1.23668.1093.1.4.1.	حالة الفحص الكامل لمكافحة الفيروسات هي واحدة مما يلي: • **معلومات**. مر أقل من 7 أيام منذ لحظة تثبيت التطبيق. • **تحذير**. لم يتم إجراء الفحص الكامل لمكافحة الفيروسات لأكثر من 7 يوم منذ لحظة تثبيت التطبيق. • **حرج**. لم يتم إجراء الفحص الكامل لمكافحة الفيروسات لأكثر من 14 يوم منذ لحظة تثبيت التطبيق. • **جيد**. ولا واحد مما سبق.
notScannedLately	INTEGER { (0)off ,(1)on }	1.3.6.1.4.1.23668.1093.1.4.2.1.	لم يتم فحص بعض الأجهزة منذ فترة زمنية معينة. يمكنك معرفة عدد تلك الأجهزة عبر `hostsNotScannedLately`. كمية الوقت يتم تحديدها في `fullScanStatus`.
hostsNotScannedLately	Counter32	1.3.6.1.4.1.23668.1093.1.4.3.	عدد الأجهزة التي لم يتم فحصها لفترة زمنية معينة. كمية الوقت يتم تحديدها في `fullScanStatus`.
logicalNetworkStatus	INTEGER { (0)ok ,(1)warning , (2)critical }	1.3.6.1.4.1.23668.1093.1.5.1.	حالة الشبكة المنطقية لخادم الإدارة. واحد مما يلي: • **تحذير**. إذا كان هناك أجهزة بحالة تحذير. لا يمكن الوصول إليها أو إذا كان هناك أجهزة لا تنتمي إلى أي مجموعة خادم إدارة. • **حرج**. إذا كان هناك أجهزة فقدها خادم الإدارة، أو إذا كان هناك أجهزة في حالة حرجة ولا يمكن الوصول إليها. • **جيد**. ولا واحد مما سبق.
notConnectedLongTime	INTEGER { (0)off ,(1)on }	1.3.6.1.4.1.23668.1093.1.5.2.1.	لم يتم توصيل بعض الأجهزة بخادم الإدارة منذ فترة طويلة (7 أيام أو أكثر لجهاز بحالة **تحذير** و4 أيام لجهاز بحالة **حرج**). يمكنك معرفة عدد تلك الأجهزة عبر `hostsNotConnectedLongTime`.
controlLost	INTEGER { (0)off ,(1)on }	1.3.6.1.4.1.23668.1093.1.5.2.2.	توجد أجهزة فقد خادم الإدارة التحكم فيها. يمكنك معرفة عدد تلك الأجهزة عبر `hostsControlLost`.
hostsFound	Counter32	1.3.6.1.4.1.23668.1093.1.5.3.	عدد الأجهزة التي عثر عليها خادم الإدارة التي لا تنتمي إلى أي مجموعة خادم إدارة.
groupsCount	Counter32	1.3.6.1.4.1.23668.1093.1.5.4.	عدد المجموعات داخل خادم الإدارة.
hostsNotConnectedLongTime	Counter32	1.3.6.1.4.1.23668.1093.1.5.5.	عدد الأجهزة التي لم يتم توصيلها بخادم الإدارة لفترة طويلة. كمية الوقت التي تعتبر طويلة يتم تحديدها في `notConnectedLongTime`.
hostsControlLost	Counter32	1.3.6.1.4.1.23668.1093.1.5.6.	عدد الأجهزة التي لا يتحكم فيها خادم الإدارة.

قيمة معرف الكائن	نوع البيانات الرقمية	معرف الكائن	الوصف
eventsStatus	INTEGER { (0)ok, (1)info, (2)warning, (3)critical }	1.3.6.1.4.1.23668.1093.1.6.1.	حالة النظام الفرعي للأحداث هي واحدة مما يلي: • **تحذير**. واحد مما يلي: لم تبحث أجهزة مجموعة خادم الإدارة عن تحديثات Windows منذ مدة طويلة. هناك أجهزة بها مشاكل في الحالة. • **حرج**. واحد مما يلي: يوجد حدث "حرج" على جهاز واحد على الأقل. يوجد حدث "خطأ" على جهاز واحد على الأقل. يوجد حدث مهمة يكتمل دون نجاح على جهاز واحد على الأقل. لم تبحث أجهزة مجموعة خادم الإدارة عن تحديثات Windows منذ مدة طويلة. هناك أجهزة بها مشاكل في الحالة. • **معلومات**. واحد مما يلي: مر أقل من أسبوع على آخر فحص كامل للفيروسات على جميع الأجهزة. اكتملت مهام التثبيت عن بُعد ولا تتطلب أي أجهزة إعادة تشغيل. مر أقل من أسبوع على آخر تحديث لخادم الإدارة. لم يتم تحديث خادم الإدارة منذ فترة طويلة، لكن التحديث قيد التقدم حاليًا. • **جيد**. ولا واحد مما سبق.
criticalEventOccured	INTEGER { (0)off, (1)on }	1.3.6.1.4.1.23668.1093.1.6.2.1.	تعرض eventsStatus وجود بعض الأحداث الحرجة على خادم الإدارة. يمكنك معرفة عدد تلك الأجهزة عبر criticalEventsCount. تساوي القيمة 1 إذا كان هناك حدث حرج واحد على الأقل على أي جهاز، و 0 بخلاف ذلك.
criticalEventsCount	Counter32	1.3.6.1.4.1.23668.1093.1.6.3.	عدد الأحداث الحرجة على خادم الإدارة.

استكشاف الأخطاء وحلها

يسرد هذا القسم حلولاً لبعض المشكلات المعتادة التي قد تواجهها أثناء استخدام خدمة SNMP.

لا يمكن لتطبيق الجهة الخارجية الاتصال بخدمة SNMP

تأكد من تثبيت خدمة SNMP وتكوينها على النحو الموضح في قسم تكوين خدمة SNMP للاستخدام مع Kaspersky Security Center.

تعمل خدمة SNMP، ولكن لا يمكن لتطبيق الجهة الخارجية الحصول على أي قيم

اسمح بتتبع عامل SNMP وتأكد من إنشاء ملف غير فارغ. هذا يعني أن عامل SNMP مسجل ويعمل بشكل صحيح. بعد ذلك اسمح بالاتصالات من خدمة SNMP في إعدادات الخدمة الجانبية. إذا كانت خدمة جانبية تعمل على نفس المضيف كعامل SNMP، يجب لقائمة عناوين IP أن تحتوي إما على عنوان IP لهذا المضيف أو loopback 127.0.0.1.

خدمة SNMP التي تتواصل مع لعملاء يجب تشغيلها في Windows. يمكنك تحديد المسارات لعملاء SNMP في سجل Windows عبر regedit.

- لنظام Windows 10:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents

- لأنظمة Windows Vista و Windows Server 2008:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

يمكنك السماح بتتبع عميل SNMP عبر regedit أيضًا.

- لأنظمة 32 بت:

Debug\SNMP\1.0.0.0\1093\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE

- لأنظمة 64 بت:

ug\SNMP\1.0.0.0\1093\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE
00000004:dword="TraceLevel"
"\\:C"="TraceDir"

القيم لا تتطابق مع حالات وحدة تحكم الإدارة

لتقليل الحمل على خادم الإدارة، يتم تنفيذ التخزين المؤقت للقيم لعميل SNMP. زمن الانتقال بين ذاكرة التخزين المؤقت التي يتم تحقيقها والقيم التي يتم تغييرها على خادم الإدارة قد يتسبب في حدوث حالات عدم تطابق بين القيم التي يتم إرجاعها بواسطة عميل SNMP والقيم الفعلية. عند العمل مع تطبيقات طرف خارجي، يجب أن تضع في اعتبارك هذا التأخير المحتمل.

العمل في بيئة السحابة

يوفر هذا القسم معلومات حول نشر Kaspersky Security Center وصيانته في بيئات السحابة، مثل Amazon Web Services أو Microsoft Azure أو Google Cloud.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية)، بالإضافة إلى وظيفة KSN التي قد لا تكون متاحة في البرنامج في الولايات المتحدة الأمريكية.

حول العمل في بيئة السحابة

لا يعمل Kaspersky Security Center 15.1 مع الأجهزة الموجودة في موقع العمل فحسب، بل يوفر أيضًا ميزات خاصة للعمل في بيئة السحابة. يعمل Kaspersky Security Center مع الأجهزة الافتراضية التالية:

- مثيلات Amazon EC2 (يُشار إليها فيما يلي باسم المثيلات). مثيل Amazon EC2 هو جهاز ظاهري يتم إنشاؤه على أساس منصة Amazon Web Services (AWS). يستخدم Kaspersky Security Center AWS APIKaspersky (واجهة برمجة التطبيقات).
- أجهزة Microsoft Azure الافتراضية. يستخدم Kaspersky Security Center Azure API.
- مثيلات أجهزة Google Cloud الافتراضية. يستخدم Kaspersky Security Center Google API.

يمكنك نشر Kaspersky Security Center على مثيل أو جهاز افتراضي لإدارة حماية الأجهزة في إحدى بيئات السحابة واستخدام الميزات الخاصة بـ Kaspersky Security Center للعمل في إحدى بيئات السحابة. تشتمل هذه الميزات على التالي:

- استخدام أدوات API لاستقصاء الأجهزة في إحدى بيئات السحابة
- استخدام أدوات API لتثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة في إحدى بيئات السحابة
- البحث عن الأجهزة بناءً على ما إذا كانت تنتمي إلى قطاع سحابة محدد

كما يمكنك استخدام مثيل أو جهاز ظاهري الذي يتم نشر خادم إدارة Kaspersky Security Center عليه لحماية الأجهزة الموجودة في مكان العمل (على سبيل المثال، إذا اتضح أن خادم السحابة سيسهل عليك الخدمة والصيانة بشكل أكبر مقارنة بالخادم المادي). وإذا كان الأمر كذلك، فأنت تعمل مع خادم الإدارة كما لو كان خادم الإدارة مثبتًا على جهاز موجود بالفعل في مكان العمل.

في Kaspersky Security Center الذي تم نشره من صورة جهاز Amazon (AMI) (في AWS)أو منتج تتم المحاسبة عليه شهريًا على أساس الاستخدام (في Azure)، يتم تفعيل ميزة إدارة الثغرات الأمنية والتصحيحات تلقائيًا (بما في ذلك التكامل مع أنظمة SIEM)؛ ويتعذر تفعيل إدارة الجهاز المحمول.

يتم تثبيت خادم الإدارة مع وحدة تحكم الإدارة. كما يتم تثبيت برنامج Kaspersky Security for Windows Server تلقائيًا على الجهاز المثبت عليه خادم الإدارة.

يمكنك تكوين Kaspersky Security Center باستخدام معالج تكوين بيئة السحابة، مع مراعاة خصوصيات العمل في بيئة السحابة.

سيناريو: النشر لسيناريو بيئة السحابة

يوضح هذا القسم نشر Kaspersky Security Center للعمل في بيئات السحابة مثل Amazon Web Services وMicrosoft Azure، وGoogle Cloud.

بعد الانتهاء من سيناريو النشر، سيتم بدء تشغيل خادم إدارة Kaspersky Security Center ووحدة تحكم الإدارة وتكوينهما باستخدام المعلمات الافتراضية. سيتم نشر الحماية لمكافحة الفيروسات التي يديرها Kaspersky Security Center على مثيلات Amazon EC2 المحددة أو الأجهزة الافتراضية في Microsoft Azure. يمكنك بعد ذلك ضبط تكوين Kaspersky Security Center وإنشاء بنية معقدة لمجموعات الإدارة، وإنشاء سياسات ومهام متنوعة للمجموعات.

يتكون نشر Kaspersky Security Center في بيئة السحابة من الخطوات التالية:

1. عمل تحضيري
2. نشر خادم الإدارة
3. تثبيت تطبيقات مكافحة الفيروسات من Kaspersky على الأجهزة الظاهرية التي تحتاج إلى الحماية
4. تكوين إعدادات تنزيل التحديث
5. تكوين الإعدادات لإدارة التقارير حول حالة حماية الأجهزة.

يختص معالج تكوين بيئة السحابة بتنفيذ التكوين الأولي. يبدأ تلقائيًا في المرة الأولى التي يتم فيها نشر Kaspersky Security Center من صورة جاهزة للاستخدام. يمكنك بدء المعالج يدويًا في أي وقت. بالإضافة إلى ذلك، يمكنك يدويًا تنفيذ كل الإجراءات التي ينفذها.

نوصيك بتخصيص ساعة واحدة على الأقل لنشر خادم إدارة Kaspersky Security Center في بيئة السحابة، وتخصيص يوم عمل واحد على الأقل لنشر الحماية في بيئة السحابة.

يتم تنفيذ عملية نشر Kaspersky Security Center في بيئة السحابة على المراحل التالية:

1. **التخطيط لتكوين قطاعات السحابة**

تعرف على كيفية عمل Kaspersky Security Center في بيئة السحابة. قم بتخطيط المكان الذي سيتم فيه نشر خادم الإدارة (داخل بيئة السحابة أو خارجها)؛ وحدد أيضًا عدد قطاعات السحابة التي تخطط لحمايتها. إذا كنت تخطط لنشر خادم الإدارة خارج بيئة السحابة، أو كنت تخطط لحماية ما يزيد عن 5000 جهاز، فستحتاج لتثبيت خادم الإدارة على الجهاز يدويًا.

للعمل باستخدام Google Cloud، يمكنك فقط تثبيت خادم الإدارة يدويًا.

2. **تخطيط الموارد**

تأكد من أنك تمتلك كل ما هو مطلوب للنشر.

3. **الاشتراك في Kaspersky Security Center بوصفه صورة جاهزة للاستخدام**

حدد إحدى صور AMI الجاهزة للاستخدام الموجودة في السوق الخاص بـ AWS، أو حدد منتج تتم المحاسبة عليه شهريًا في السوق الخاص بـ Azure، وسدد ثمنها وفقًا لقواعد السوق عند اللزوم، (أو استخدم نموذج BYOL)، واستخدم الصورة لنشر مثيل Amazon EC2 أو الجهاز الافتراضي في Microsoft Azure المثبت عليه Kaspersky Security Center.

هذه المرحلة ضرورية فقط في حال تخطيطك لنشر خادم الإدارة على مثيل/جهاز افتراضي يقع داخل بيئة السحابة وتخطيطك كذلك لنشر الحماية لأجهزة لا يزيد عددها عن 5000 جهاز. وإلا فإن هذه المرحلة غير ضرورية، وبدلاً من ذلك فأنت بحاجة إلى تثبيت خادم الإدارة ووحدة تحكم الإدارة ونظام إدارة قواعد البيانات (DBMS) يدويًا.

هذه الخطوة غير متاحة لـ Google Cloud.

4. **تحديد موقع نظام إدارة قواعد البيانات (DBMS)**

حدد المكان الذي سيتواجد به نظام إدارة قواعد البيانات (DBMS) الخاص بك.

إذا كنت ترغب في استخدام قاعدة بيانات خارج بيئة السحابة، فتأكد من أن لديك قاعدة بيانات عاملة.

إذا كنت تخطط لاستخدام Amazon Relational Database Service (RDS)، فأنشئ قاعدة بيانات باستخدام RDS في بيئة سحابة AWS.

إذا كنت تخطط لاستخدام Microsoft Azure SQL DBMS، فأنشئ قاعدة بيانات باستخدام خدمة قاعدة بيانات Azure في بيئة Microsoft Azure السحابية.

إذا كنت تخطط لاستخدام Google MySQL، أنشئ قاعدة بيانات علىGoogle Cloud (يُرجى الرجوع إلى https://cloud.google.com/sql/docs/mysql للحصول على التفاصيل).

5. **تثبيت خادم الإدارة ووحدة تحكم الإدارة (وحدة الإدارة المستندة إلى البرامج و/أو وحدة التحكم المستندة إلى الويب) في الأجهزة المحددة يدويًا**

قم بتثبيت خادم الإدارة، ووحدة تحكم الإدارة، ونظام إدارة قواعد البيانات يدويًا على الأجهزة المحددة كما هو موضح في سيناريو التثبيت الرئيسي لـ Kaspersky Security Center.

هذه المرحلة ضرورية إذا كنت تخطط لوضع خادم الإدارة خارج بيئة السحابة أو إذا كنت تخطط لنشر الحماية لما يزيد عن 5000 جهاز. ثم تأكد من أن خادم الإدارة الخاص بك يفي بمتطلبات الأجهزة. وإلا فإن هذه المرحلة غير ضرورية ويكفي تسجيل الاشتراك في Kaspersky Security Center كصورة جاهزة للاستخدام في سوق AWS أو سوق Azure أو Google Cloud.

6. **التأكد من أن خادم الإدارة يمتلك الأذونات لاستخدام أدوات API السحابية**

في AWS، قم بإنشاء دور IAM في وحدة التحكم الخاصة بإدارة AWS أو حساب مستخدم IAM. سيسمح دور IAM (أو حساب مستخدم IAM) الذي تم إنشاؤه لـ Kaspersky Security Center بالعمل مع AWS API: استقصاء قطاعات السحابة ونشر الحماية.

قم في Azure بإنشاء اشتراك ومعرف تطبيق مزود بكلمة مرور. يستخدم Kaspersky Security Center البيانات الاعتمادية هذه للعمل مع Azure API: استقصاء قطاعات السحابة ونشر الحماية.

في Google Cloud، قم بتسجيل مشروع، واحصل على معرف مشروعك ومفتاح خاص. يستخدم Kaspersky Security Center البيانات الاعتمادية هذه لاستطلاع قطاعات السحابة باستخدام Google API.

7. **إنشاء دور IAM للمثيلات المحمية (لـ AWS فقط)**

في وحدة التحكم الخاصة بإدارة AWS، قم بإنشاء دور IAM الذي يحدد مجموعة الأذونات الخاصة بتنفيذ الطلبات لخدمات AWS. يتم تعيين هذا الدور الذي تم إنشاؤه حديثًا لاحقًا إلى مثيلات جديدة. دور IAM مطلوب لاستخدام Kaspersky Security Center لتثبيت التطبيقات على المثيلات.

8. **إعداد قاعدة بيانات باستخدام Amazon Relational Database Service أو Microsoft Azure SQL**

إذا كنت تخطط لاستخدام Amazon Relational Database Service (RDS)، فقم بإنشاء مثيل قاعدة بيانات Amazon RDS ومستودع S3 الذي سيتم تخزين قاعدة البيانات الاحتياطية فيه. يمكنك تخطي هذه المرحلة إذا كنت تريد قاعدة بيانات على مثيل EC2 نفسه حيث تم تثبيت خادم الإدارة، أو إذا كنت تريد أن تكون قاعدة البيانات الخاصة بك في مكان آخر.

إذا كنت تخطط لاستخدام Microsoft Azure SQL، فقم بإنشاء حساب تخزين وقاعدة بيانات في Microsoft Azure.

إذا كنت تخطط لاستخدام Google MySQL، قم بتكوين قاعدة بياناتك على Google Cloud (يُرجى الرجوع إلى https://cloud.google.com/sql/docs/mysql للحصول على التفاصيل).

9 ترخيص Kaspersky Security Center للعمل في بيئة السحابة

تأكد من قيامك بترخيص Kaspersky Security Center للعمل في بيئة السحابة وتوفير رمز تنشيط أو ملف مفتاح حتى يمكن للتطبيق إضافته إلى مخزن الترخيص. ويمكن إكمال هذه المرحلة أثناء تكوين بيئة السحابة.

هذه المرحلة مطلوبة إذا كنت تستخدم Kaspersky Security Centerالمثبت من صورة AMI المجانية الجاهزة للاستخدام بناءً على نموذج BYOL، أو إذا كنت تثبّت Kaspersky Security Center يدويًا بدون استخدام صور AMI. في كل حالة من هذه الحالات، ستحتاج إلى Kaspersky Security for Virtualization، أو ترخيص لـ Kaspersky Hybrid Cloud Security، لتفعيل Kaspersky Security Center.

إذا كنت تستخدم Kaspersky Security Center الذي تم تثبيته من صورة جاهزة للاستخدام، فهذه المرحلة ليست ضرورية ولن يتم عرض النافذة المطابقة الخاصة بمعالج تكوين بيئة السحابة.

10 التخويل في بيئة السحابة

قم بتوفير Kaspersky Security Center المزود ببيانات اعتماد AWS أو Azure أو Google Cloud الخاصة بك حتى يتمكن Kaspersky Security Center من العمل مع الأذونات اللازمة. ويمكن إكمال هذه المرحلة أثناء المصادقة في بيئة السحابة.

11 إجراء استقصاء لقطاعات السحابة حتى يتمكن خادم الإدارة من استقبال معلومات حول الأجهزة الموجودة في قطاع السحابة

بدء استقصاء قطاع السحابة. في بيئة AWS، سيتلقى Kaspersky Security Center عناوين جميع المثيلات وأسماءها التي يمكن الوصول إليها استنادًا إلى أذونات دور IAM أو مستخدم IAM. في بيئة Microsoft Azure، سيتلقى Kaspersky Security Center عناوين جميع الأجهزة الظاهرية وأسماءها التي يمكن الوصول إليها استنادًا إلى أذونات دور القارئ.

يمكنك حينئذ استخدام Kaspersky Security Center لتثبيت تطبيقات وبرامج Kaspersky المتوفرة من موردين آخرين على المثيلات أو الأجهزة الظاهرية.

يبدأ Kaspersky Security Center في إجراء الاستقصاء بشكلٍ منتظم، مما يعني أن المثيلات أو الأجهزة الافتراضية الجديدة تم اكتشافها تلقائيًا.

12 تجميع جميع أجهزة الشبكة في مجموعة إدارة السحابة

انقل المثيلات أو الأجهزة الافتراضية المُكتشَفة إلى **الأجهزة المُدارة/مجموعة إدارة السحابة** حتى يتسنى لها أن تكون متاحة للإدارة المركزية. إذا كنت ترغب في تعيين الأجهزة إلى مجموعات فرعية، على سبيل المثال، بناءً على نظام التشغيل المثبت عليها، فيمكنك إنشاء العديد من مجموعات الإدارة داخل **الأجهزة المُدارة/مجموعة السحابة**. يمكنك تمكين النقل التلقائي لجميع الأجهزة التي سيتم اكتشافها أثناء الاستقصاءات الروتينية إلى **الأجهزة المُدارة\مجموعة السحابة**.

13 استخدام عميل الشبكة لاتصال الأجهزة المتصلة بالشبكة بخادم الإدارة

تثبيت عميل الشبكة على الأجهزة في بيئة السحابة. عميل الشبكة هو مكون Kaspersky Security Center الذي يوفر الاتصال بين الأجهزة وخادم الإدارة. يتم تكوين إعدادات عميل الشبكة تلقائيًا بشكل افتراضي.

يمكنك تثبيت عميل الشبكة على كل جهاز محليًا. يمكنك أيضًا تثبيت عميل الشبكة عن بُعد باستخدام Kaspersky Security Center. أو يمكنك تخطي هذه المرحلة وتثبيت عميل الشبكة إلى جانب أحدث إصدارات تطبيقات الأمان.

14 تثبيت أحدث إصدارات تطبيقات الأمان على الأجهزة المتصلة بالشبكة

حدد الأجهزة التي ترغب في تثبيت تطبيقات الأمان عليها، وثبّت أحدث إصدارات الأمان على هذه الأجهزة. يمكنك القيام بالتثبيت إما عن بُعد باستخدام Kaspersky Security Center على خادم الإدارة أو محليًا.

قد تضطر إلى إنشاء حزم التثبيت لهذه البرامج يدويًا.

Kaspersky Endpoint Security for Linux مخصص للمثيلات والأجهزة الظاهرية التي تعمل بنظام التشغيل Linux.

Kaspersky Security for Windows Server مخصص للمثيلات والأجهزة الظاهرية التي تعمل بنظام التشغيل Windows.

15 تكوين إعدادات التحديث

يتم إنشاء مهمة **البحث عن الثغرات الأمنية والتحديثات المطلوبة** تلقائيًا عند بدء تشغيل تكوين بيئة السحابة. كام يمكنك إنشاء المهمة يدويًا. تقوم هذه المهمة باكتشاف تحديثات التطبيق المطلوبة وتنزيلها للتثبيت التالي لأجهزة الشبكة باستخدام أدوات Kaspersky Security Center.

يوصى بإكمال المرحلة التالية بعد اكتمال تكوين بيئة السحابة:

1. **تكوين إدارة التقرير**

يمكنك عرض التقارير في علامة التبويب **المراقبة** في مساحة عمل العقدة **خادم الإدارة**. كما يمكنك تلقي التقارير عن طريق البريد الإلكتروني. تتوفر التقارير المتعلقة بعلامة التبويب **المراقبة** بشكل افتراضي. لتكوين استلام التقارير بواسطة البريد الإلكتروني، حدد عناوين البريد الإلكتروني التي عليها استلام التقارير وقم بتكوين تنسيق التقارير.

النتائج

عند اكتمال السيناريو، يمكنك التأكد من نجاح التكوين الأولي:

- يمكنك الاتصال بخادم الإدارة من خلال وحدة تحكم الإدارة أو Kaspersky Security Center Web Console.
- يتم تثبيت وتشغيل أحدث إصدارات تطبيقات أمان Kaspersky على الأجهزة المُدارة.
- قام Kaspersky Security Center بإنشاء سياسات ومهام افتراضية لجميع الأجهزة المُدارة.

المتطلبات الأساسية لنشر Kaspersky Security Center في بيئة السحابة

قبل بدء نشر Kaspersky Security Center في بيئة السحابة لـ Amazon Web Services أو Microsoft Azure، تأكد من امتلاكك لما يلي:

- وصول إلى الإنترنت
- أحد الحسابات التالية:
  - حساب Amazon Web Services (للعمل مع AWS)
  - حساب Microsoft (للعمل مع Azure)
  - حساب جوجل (للعمل مع Google Cloud)
- واحد مما يلي:
  - ترخيص لـ Kaspersky Security for Virtualization
  - ترخيص لـ Kaspersky Hybrid Cloud Security
  - تمويل لشراء مثل هذا الترخيص (Kaspersky Security for Virtualization أو Kaspersky Hybrid Cloud Security)
  - أموال للدفع مقابل صورة جاهزة للاستخدام في السوق الخاص بـ Azure
- توجيهات لآخر إصدارات من Kaspersky Endpoint Security for Linux و Kaspersky Security for Windows Server

متطلبات الأجهزة لخادم الإدارة في بيئة السحابة

للنشر في البيئات السحابية، تكون متطلبات خادم الإدارة وخادم قاعدة البيانات هي نفسها متطلبات خادم الإدارة الفعلي (اعتمادًا على عدد الأجهزة التي تريد إدارتها). يرجى الرجوع إلى وثائق بيئة السحابة للحصول على التفاصيل.

خيارات الترخيص في بيئة السحابة

يندرج العمل في بيئة السحابة خارج وظائف Kaspersky Security Center الأساسية ولذلك يتطلب ترخيصًا مخصصًا لذلك.

يتوفر خياران لترخيص Kaspersky Security Center للعمل في بيئة السحابة:

- AMI مدفوع الأجر (في Amazon Web Services) أو فواتير SKU الشهرية المستندة على الاستخدام (في Microsoft Azure).

  يمنح هذا ترخيصًا لبرنامج Kaspersky Security Center بالإضافة إلى تراخيص لبرنامج Kaspersky Endpoint Security for Linux وKaspersky Security for Windows Server. عليك أن تدفع وفقًا لقواعد بيئة السحابة التي تستخدمها.

  يتيح لك هذا الطراز عدم امتلاك ما يزيد عن 200 جهاز عميل لخادم إدارة واحد.

- صورة مجانية للاستخدام، وجاهزة للاستخدام باستخدام ترخيص الملكية، وفقًا لنموذج Bring Your Own License (BYOL).

  بالنسبة إلى ترخيص Kaspersky Security Center، يجب أن يكون لديك ترخيصًا لأحد التطبيقات التالية:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  يتيح لك نموذج BYOL امتلاك ما يصل إلى 100 000 جهاز عميل لخادم إدارة واحد. يتيح لك هذا النموذج أيضًا إدارة الأجهزة خارج بيئة في AWS أو Azure أو Google.

  يمكنك اختيار نموذج BYOL في أي من الحالات التالية:

  - إذا كنت تمتلك بالفعل ترخيصًا صالحًا لـ Kaspersky Security for Virtualization.
  - كنت تمتلك بالفعل ترخيصًا صالحًا لـ Kaspersky Hybrid Cloud Security.
  - كنت مستعدًا لشراء ترخيص على الفور قبل نشر Kaspersky Security Center.

  في مرحلة الإعداد الأولي، سيطالبك Kaspersky Security Center برمز التفعيل أو ملف المفتاح.

  إذا اخترت نموذج BYOL، فلن يتعين عليك سداد قيمة Kaspersky Security Center عبر السوق الخاص بـ Azure أو السوق الخاص بـ AWS.

في كلتا الحالتين، يتم تفعيل ميزة إدارة الثغرات الأمنية والتصحيحات تلقائيًا، ويتعذر تفعيل إدارة الجهاز المحمول.

في حال حدوث خطأ عند محاولة تفعيل ميزة دعم البيئة السحابية باستخدام ترخيص Kaspersky Hybrid Cloud Security، استخدم ملف المفتاح.

عند الاشتراك في Kaspersky Security Center، ستحصل على مثيل Amazon Elastic Compute Cloud (Amazon EC2) أو جهاز افتراضي في Microsoft Azure مزود بخادم إدارة Kaspersky Security Center. تتوفر حزم التثبيت لـ Kaspersky Security for Windows Server وKaspersky Endpoint Security for Linux على خادم الإدارة. يمكنك تثبيت هذه التطبيقات على الأجهزة في بيئة السحابة. لا يتعين عليك ترخيص هذه التطبيقات.

إذا كان الجهاز المُدار غير مرئي لخادم الإدارة لفترة تزيد عن أسبوع، فسيتحول التطبيق (Kaspersky Security for Windows Server أو Kaspersky Endpoint Security for Linux) إلى وضع الوظائف المحدودة. لتفعيل التطبيق مرة أخرى، يجب أن تجعل الجهاز المثبت عليه التطبيق مرئيًا لخادم الإدارة مرة أخرى.

خيارات قاعدة البيانات للعمل في بيئة السحابة

يجب أن يكون لديك قاعدة بيانات للعمل مع Kaspersky Security Center. عند نشر Kaspersky Security Center في AWS أو في Microsoft Azure، أو في Google Cloud، أمامك ثلاثة خيارات:

- قم بإنشاء قاعدة بيانات محلية على نفس الجهاز المزود بخادم الإدارة. يأتي Kaspersky Security Center بقاعدة بيانات SQL Server Express التي يمكنها دعم ما يصل إلى 5000 جهاز مُدار. اختر هذا الخيار إذا كان SQL Server Express Edition كافياً لاحتياجاتك.

- قم بإنشاء قاعدة بيانات مجهزة بخدمة قواعد البيانات الارتباطية (RDS) في بيئة سحابة AWS، أو مجهزة بخدمة Azure Database في بيئة سحابة Microsoft Azure. اختر هذا الخيار إذا كنت تريد نظام DBMS غير SQL Express. سيتم نقل البيانات الخاصة بك داخل بيئة السحابة، حيث ستظل هناك ولن تتكبد أية نفقات إضافية. إذا كنت تعمل بالفعل مع Kaspersky Security Center في أماكن العمل ولديك بعض البيانات في قاعدة البيانات الخاصة بك، فيمكنك نقل بياناتك إلى قاعدة البيانات الجديدة.

  للعمل على Google Cloud Platform، يمكنك فقط استخدام خدمة Cloud SQL لـ MySQL.

- استخدم خادم قاعدة بيانات موجود بالفعل. اختر هذا الخيار إذا كان لديك خادم قاعدة بيانات بالفعل وتريد استخدامه في Kaspersky Security Center. إذا كان هذا الخادم موجودًا خارج بيئة السحابة، فسيتم نقل بياناتك عبر الإنترنت، مما قد يؤدي إلى تكبد نفقات إضافية.

يشتمل إجراء نشر Kaspersky Security Center في بيئة السحابة على خطوة خاصة لإنشاء (اختيار) قاعدة بيانات.

العمل في بيئة سحابة Amazon Web Services

يُعلمك هذا القسم بكيفية التحضير لاستخدام Kaspersky Security Center في Amazon Web Services.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

حول العمل في بيئة سحابة Amazon Web Services

يمكنك شراء منتج Kaspersky Security Center في السوق الخاص بـ AWS على شكل صورة جهاز Amazon (AMI)، وهي صورة جاهزة للاستخدام لجهاز ظاهري تم تكوينه مسبقًا. يمكنك الاشتراك في صورة AMI مدفوعة الأجر أو صورة BYOL AMI، وبناءً على تلك الصورة، قم بإنشاء مثيل Amazon EC2 مثبت عليه خادم إدارة Kaspersky Security Center.

للعمل مع منصة AWS، وعلى وجه الخصوص، لشراء التطبيقات من السوق الخاص بـ AWS ولإنشاء المثيلات، ستحتاج إلى حساب Amazon Web Services. يمكنك إنشاء حساب مجاني على https://aws.amazon.com. يمكنك أيضًا استخدام حساب Amazon الحالي.

إذا اشتركت في صورة AMI المتوفرة في السوق الخاص بـ AWS، فستحصل على مثيل يحتوي على Kaspersky Security Center جاهز للاستخدام. لا يتعين عليك تثبيت التطبيق بنفسك. في هذه الحالة، يتم تثبيت Kaspersky Security Center الخاص بك على المثيل دون تدخل من جانبك. بعد التثبيت، يمكنك بدء وحدة تحكم الإدارة والاتصال بخادم الإدارة لبدء استخدام Kaspersky Security Center.

لمعرفة المزيد حول صورة AMI وكيفية عمل السوق الخاص بـ AWS، يرجى زيارة صفحة تعليمات السوق الخاص بـ AWS. للاطلاع على المزيد من المعلومات حول العمل مع منصة Web، واستخدام المثيلات، والمفاهيم ذات الصلة، يرجى الرجوع إلى وثائق خدمات أمازون عبر الإنترنت.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

إنشاء أدوار IAM وحسابات مستخدمي IAM لمثيلات Amazon EC2

يصف هذا القسم الإجراءات الواجب اتخاذها لضمان التشغيل الصحيح لخادم الإدارة. تشمل هذه الإجراءات العمل مع أدوار الهوية وإدارة الوصول (IAM) وحسابات المستخدمين. ويصف كذلك الإجراءات الواجب اتخاذها على الأجهزة العميلة لتثبيت عميل الشبكة عليهم ثم تثبيت Kaspersky Security for Windows Server وKaspersky Endpoint Security for Linux.

التأكد من أن خادم إدارة Kaspersky Security Center لديه الأذونات للعمل مع خدمات AWS

تحدد معايير التشغيل في بيئة سحابة خدمات أمازون عبر الإنترنت أنه ينبغي تعيين دور IAM خاص لمثيل خادم الإدارة للعمل باستخدام خدمات AWS. دور IAM هو كيان IAM يحدد مجموعة الأذونات الخاصة بتنفيذ الطلبات لخدمات AWS. يقدّم دور IAM أذونات لاستقصاء قطاع السحابة وتثبيت تطبيقات على المثيلات.

بعد إنشاء دور IAM وتعيينه إلى خادم الإدارة، ستتمكن من نشر الحماية على المثيلات بدون تقديم أي معلومات إضافية لـ Kaspersky Security Center.

ومع ذلك، قد يكون من المستحسن عدم إنشاء دور IAM لخادم الإدارة في الحالات التالية:

- أن تكون الأجهزة التي تنوي إدارة حمايتها هي مثيلات EC2 وتوجد داخل بيئة سحابة Amazon Web Services ولكن خادم الإدارة يقع خارج البيئة.
- التخطط لإدارة حماية المثيلات ليس فقط داخل قطاع السحابة ولكن أيضًا داخل قطاعات السحابة الأخرى التي تم إنشاؤها بموجب حساب مختلف في AWS. في هذه الحالة، ستحتاج لدور IAM فقط لحماية قطاع السحابة الخاص بك. لن تحتاج لدور IAM لحماية قطاع سحابة أخرى.

في هذه الحالات، بدلاً من إنشاء دور IAM ستحتاج لإنشاء حساب مستخدم IAM، الذي سوف يُستخدم بواسطة Kaspersky Security Center للعمل مع خدمات AWS. قبل بدء استخدام خادم الإدارة، أنشئ حساب مستخدم IAM مزوّد بمفتاح وصول AWS IAM (المُشار إليه فيما بعد أيضًا بمفتاح وصول IAM).

يتطلب إنشاء دور IAM أو حساب مستخدم IAM وجود وحدة التحكم الخاصة بإدارة AWS. للعمل مع وحدة التحكم الخاصة بإدارة AWS، ستحتاج إلى اسم مستخدم وكلمة مرور من حساب في AWS.

إنشاء دور IAM لخادم الإدارة

قبل قيامك بنشر خادم الإدارة، في وحدة التحكم الخاصة بإدارة AWS قم بإنشاء دور IAM يحتوي على الأذونات المطلوبة لتثبيت التطبيقات على المثيلات. لمزيد من التفاصيل، راجع أقسام مساعدة AWS حول أدوار IAM.

لإنشاء دور IAM لخادم الإدارة:

1. افتح وحدة التحكم الخاصة بإدارة AWS وقم بتسجيل الدخول إلى حسابك عبر AWS.
2. في قسم **الأدوار**، قم بإنشاء دور باستخدام الأذونات التالية:

- **AmazonEC2ReadOnlyAccess**، في حال كنت تخطط لتشغيل استقصاء قطاع السحابة فقط ولا تخطط لتثبيت التطبيقات على مثيلات EC2 باستخدام AWS API.
- **AmazonEC2ReadOnlyAccess** و**AmazonSSMFullAccess**، في حال كنت تخطط لتشغيل استقصاء قطاع السحابة وتثبيت التطبيقات على مثيلات EC2 باستخدام AWS API. في هذه الحالة، ستحتاج أيضًا لتعيين دور IAM يحتوي على إذن AmazonEC2RoleforSSM لمثيلات EC2 المحمية.

ستحتاج لتعيين هذا الدور إلى مثيل EC2 الذي ستستخدمه كخادم إدارة.

الدور الذي تم إنشاؤه حديثًا متاح لكل التطبيقات الموجودة على خادم الإدارة. لذلك، يمكن لأي تطبيق يعمل على خادم الإدارة استقصاء قطاعات السحابة أو تثبيت التطبيقات على مثيلات EC2 ضمن قطاع سحابة ما.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

إنشاء حساب مستخدم IAM للعمل مع Kaspersky Security Center

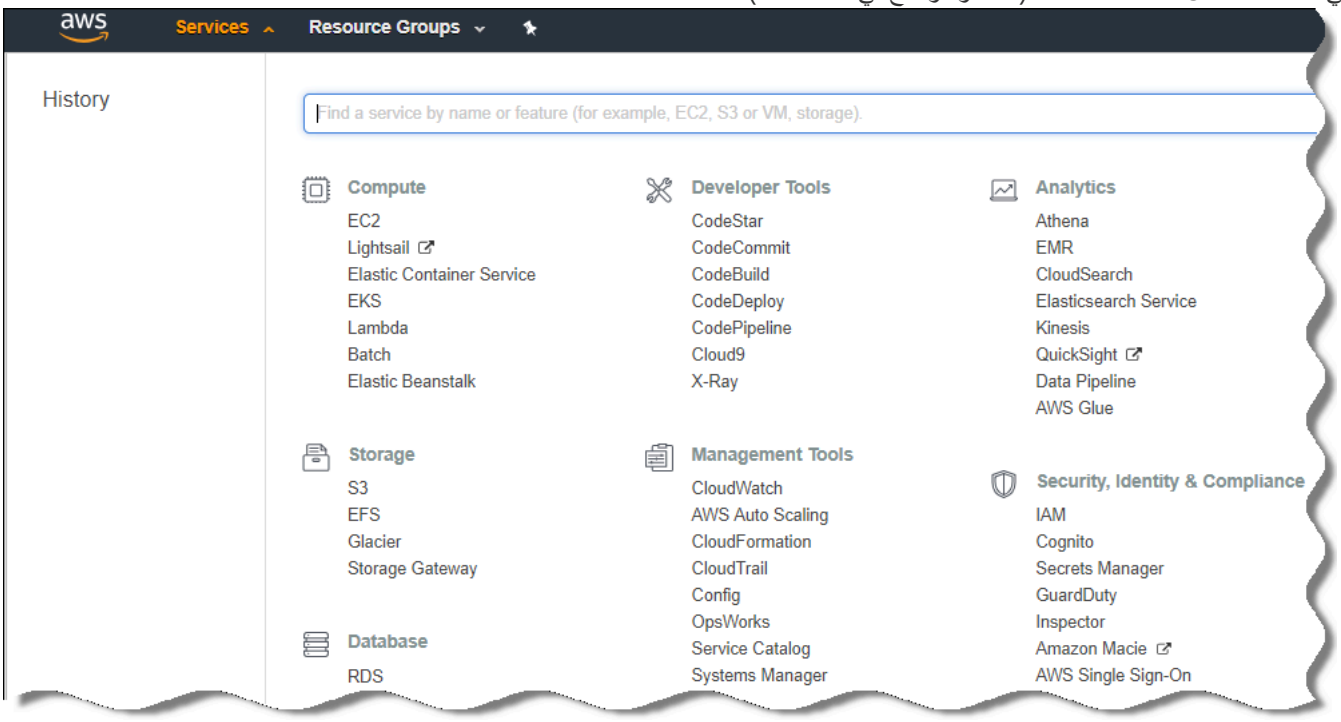
حساب مستخدم IAM مطلوب للعمل مع Kaspersky Security Center إذا لم يتم تعيين دور IAM لديه أذونات اكتشاف الأجهزة وتثبيت التطبيقات على المثيلات لخادم الإدارة. يلزم أيضًا نفس الحساب أو حساب مختلف لمهمة النسخ الاحتياطي لبيانات خادم الإدارة إذا كنت تستخدم مستودع S3. يمكنك إنشاء حساب مستخدم IAM واحد يمتلك كل الأذونات المطلوبة أو يمكنك إنشاء حسابي مستخدم منفصلين.

يتم إنشاء مفتاح وصول IAM الذي تحتاج لتقديمه لـ Kaspersky Security Center خلال التكوين الأولي تلقائيًا لمستخدم IAM. يتألف مفتاح وصول IAM من معرف مفتاح الوصول والمفتاح السري. للحصول على المزيد من التفاصيل حول خدمة IAM، يرجى الرجوع إلى صفحات مراجع AWS التالية:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

لإنشاء حساب مستخدم IAM لديه الأذونات المطلوبة:

1. افتح وحدة التحكم الخاصة بإدارة AWS وقم بتسجيل الدخول من حسابك.
2. في قائمة خدمات AWS، حدد **IAM** (كما هو موضح في الشكل أدناه).



قائمة الخدمات في وحدة التحكم الخاصة بإدارة AWS

تفتح نافذة تحتوي على قائمة بأسماء المستخدمين وقائمة تسمح لك بالعمل مع الأداة.

3. قم بالتنقل خلال نطاقات وحدة التحكم التي تتعامل مع حسابات المستخدمين، وقم بإضافة اسم مستخدم جديد أو أسماء مستخدمين جدد.

4. بالنسبة للمستخدم (المستخدمين) الذي قمت بإضافته، قم بتحديد خصائص AWS التالية:

- نوع الوصول: **وصول برمجي**.
- لم يتم تعيين حدود الأذونات.
- الأذونات:

- **ReadOnlyAccess**—إذا كنت تخطط لتشغيل استقصاء قطاع السحابة فقط ولا تخطط لتثبيت التطبيقات على مثيلات EC2 باستخدام AWS API.
- **ReadOnlyAccess** and **AmazonSSMFullAccess**—إذا كنت تخطط لتشغيل استقصاء قطاع السحابة وتثبيت التطبيقات على مثيلات EC2 باستخدام AWS API. في هذه الحالة، يجب عليك تعيين دور IAM يمتلك إذن AmazonEC2RoleforSSM لمثيلات EC2 المحمية.

بعد إضافتك للأذونات، قم بتفقدهم لضمان الدقة. في حالة وجود تحديد خاطئ، ارجع للشاشة السابقة وقم بالتحديد مرة أخرى.

5. بعد قيامك بإنشاء حساب المستخدم، سيظهر جدول يحتوي على مفتاح وصول IAM لمستخدم IAM الجديد. يظهر معرف مفتاح الوصول في العمود **معرف مفتاح الوصول**. يظهر المفتاح السري على شكل علامات النجمة في العمود **مفتاح الوصول السري**. لعرض المفتاح السري، انقر فوق **إظهار**.

سيتم عرض الحساب الذي تم إنشاؤه حديثًا في قائمة حسابات مستخدمي IAM المقابلة لحسابك في AWS.

عند نشر Kaspersky Security Center في قطاع سحابة، يجب عليك تحديد استخدامك لحساب مستخدم IAM وتقديم معرف مفتاح الوصول ومفتاح الوصول السري لـ Kaspersky Security Center.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

إنشاء دور IAM لتثبيت التطبيقات على مثيلات Amazon EC2

قبل قيامك ببدء نشر الحماية على مثيلات EC2 عن طريق استخدام Kaspersky Security Center، في وحدة التحكم الخاصة بإدارة AWS ، قم بإنشاء دور IAM يحتوي على الأذونات المطلوبة لتثبيت التطبيقات على المثيلات. لمزيد من التفاصيل، راجع أقسام المساعدة من AWS مساعدة AWS حول أدوار IAM.

دور IAM مطلوب وبذلك يمكنك تعيينه لكل مثيلات EC2 التي تخطط لتثبيت تطبيقات الأمان عليها عن طريق استخدام Kaspersky Security Center. إن لم تقم بتعيين ميل لدور IAM يحتوي على الأذونات الضرورية، سينتج خطأ عن تثبيت التطبيقات على هذا المثيل باستخدام أدوات AWS API.

للعمل مع وحدة التحكم الخاصة بإدارة AWS، ستحتاج إلى اسم مستخدم وكلمة مرور من حساب في AWS.

لإنشاء دور IAM لتثبيت التطبيقات على المثيلات

1. افتح وحدة التحكم الخاصة بإدارة AWS وقم بتسجيل الدخول إلى حسابك عبر AWS.
2. في القائمة الموجودة على اليمين، حدد **Roles**.
3. انقر فوق الزر **Create Role**.
4. في قائمة الخدمات التي تظهر، حدد **EC2** ثم من قائمة **Select Your Use case** الخاصة بك حدد **EC2** مرة أخرى.
5. انقر فوق الزر **Next: Permissions**.
6. في القائمة التي تفتح، حدد خانة الاختيار الموجودة بجوار **AmazonEC2RoleforSSM**.
7. انقر فوق الزر **Next: Review**.

8. أدخل اسم ووصف لدور IAM ثم انقر على زر **Create Role**.

يظهر الدور الذي أنشأته في قائمة الأدوار بالاسم والوصف الذي أدخلته.

فيما بعد، يمكنك استخدام الدور الذي أنشأته حديثًا لإنشاء مثيلات EC2 جديدة تنوي حمايتها باستخدام عبر Kaspersky Security Center، بالإضافة إلى ربطها بالمثيلات الحالية.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

استخدام Amazon RDS

يصف هذا القسم أي الإجراءات يجب اتخاذها لإعداد قاعدة بيانات لـAmazon Relational Database Service (RDS) لـ Kaspersky Security Center، ووضعها في مجموعة خيارات، وإنشاء دور IAM للعمل مع قاعدة بيانات RDS، وإعداد مستودع S3 للتخزين، وترحيل قاعدة بيانات موجودة بالفعل إلى RDS.

Amazon RDS هي خدمة ويب تساعد مستخدمي AWS على إعداد وتشغيل وتوسيع نطاق قاعدة بيانات ارتباطية في بيئة سحابة AWS. إذا كنت ترغب بذلك، يمكنك استخدام قاعدة بيانات Amazon RDS للعمل مع Kaspersky Security Center.

يمكنك العمل باستخدام قواعد البيانات التالية:

- خادم Microsoft SQL
- إصدار SQL Express
- تحديث Aurora MySQL 5.7
- معيار MySQL 5.7

إنشاء مثيل Amazon RDS

إذا كنت تريد استخدام Amazon RDS كنظام إدارة قواعد البيانات (DBMS)، فيجب عليك إنشاء مثيل قاعدة بيانات Amazon RDS. يصف هذا القسم كيفية تحديد SQL Express Edition؛ إذا كنت ترغب في العمل مع Aurora MySQL أو Standard MySQL (الإصداران 5.7 و8.0)، فيجب عليك اختيار أحد هذه المحركات.

لإنشاء مثيل قاعدة بيانات Amazon RDS:

1. افتح وحدة التحكم الخاصة بإدارة AWS على الموقع الإلكتروني https://console.aws.amazon.com وقم بتسجيل الدخول من حسابك.
2. باستخدام واجهة AWS، قم بإنشاء قاعدة بيانات مزودة بالإعدادات التالية:
   - المحرك: Microsoft SQL Server ، SQL Express Edition
   - إصدار محرك DB: SQL Server 2014 12.00.5546.0v1
   - فئة مثيل قاعدة البيانات: db.t2.medium
   - نوع التخزين: غرض عام
   - تخزين مخصص: الحد الأدنى 50 جيجا بايت
   - مجموعة الأمن: نفس المجموعة التي سيكون فيها مثيل EC2 المزود بخادم إدارة Kaspersky Security Center

قم بإنشاء معرف واسم مستخدم وكلمة مرور لمثيل RDS الخاص بك.

يمكنك ترك الإعدادات الافتراضية في جميع الحقول الأخرى. أو قم بتغيير الإعدادات الافتراضية إذا كنت تريد تخصيص مثيل Amazon RDS الخاص بك. للحصول على المساعدة، يُرجى الرجوع إلى صفحات معلومات AWS.

3. في الخطوة الأخيرة، يعرض AWS نتائج العملية. إذا كنت ترغب في عرض تفاصيل مثيل Amazon RDS الخاص بك، انقر على **عرض تفاصيل مثيل قاعدة البيانات**. إذا كنت ترغب في المتابعة إلى الإجراء التالي، فابدأ في إنشاء مجموعة خيارات لمثيل Amazon RDS الخاص بك.

قد يستغرق إنشاء مثيل Amazon RDS جديد مدة تصل إلى عدة دقائق. بعد إنشاء المثيل، يمكنك استخدامه للعمل مع بيانات Kaspersky Security Center.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

إنشاء مجموعة خيارات لمثيل Amazon RDS

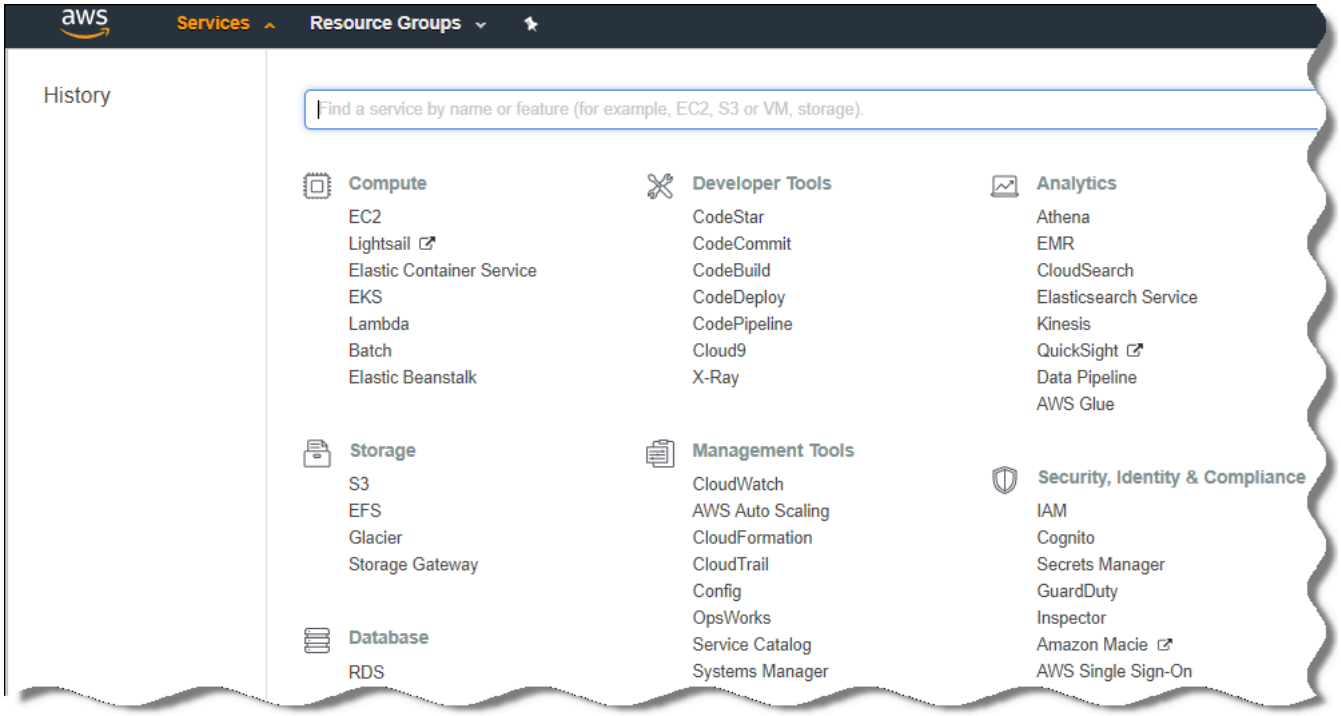
تحتاج إلى وضع مثيل Amazon RDS الخاص بك في مجموعة خيارات.

قم بما يلي لإنشاء مجموعة خيارات لمثيل Amazon RDS الخاص بك:

1. تأكد من أنك في وحدة التحكم الخاصة بإدارة AWS (https://console.aws.amazon.com/) وأنك قمت بتسجيل الدخول إلى حسابك.

2. في سطر القائمة، انقر فوق **خدمات**.

تظهر قائمة الخدمات المتاحة (انظر الشكل أدناه).



قائمة الخدمات في وحدة التحكم الخاصة بإدارة AWS

3. في القائمة، انقر فوق **RDS**.

4. في الجزء الأيسر، انقر فوق **مجموعات الخيارات**.

5. انقر فوق الزر **إنشاء مجموعة**.

6. قم بإنشاء مجموعة خيارات بالإعدادات التالية، إذا اخترت SQL Server في مرحلة إنشاء مثيل Amazon RDS:

- المحرك: SQLserver-ex
- إصدار المحرك الرئيسي: 12.00

إذا اخترت قاعدة بيانات SQL مختلفة في مرحلة إنشاء مثيل Amazon RDS، فاختر محركًا مطابقًا.

يتم إنشاء المجموعة وعرضها في قائمة المجموعات.

بعد إنشاء مجموعة الخيارات، ضع مثيل Amazon RDS الخاص بك في مجموعة الاختيارات هذه.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

تعديل مجموعة الخيارات

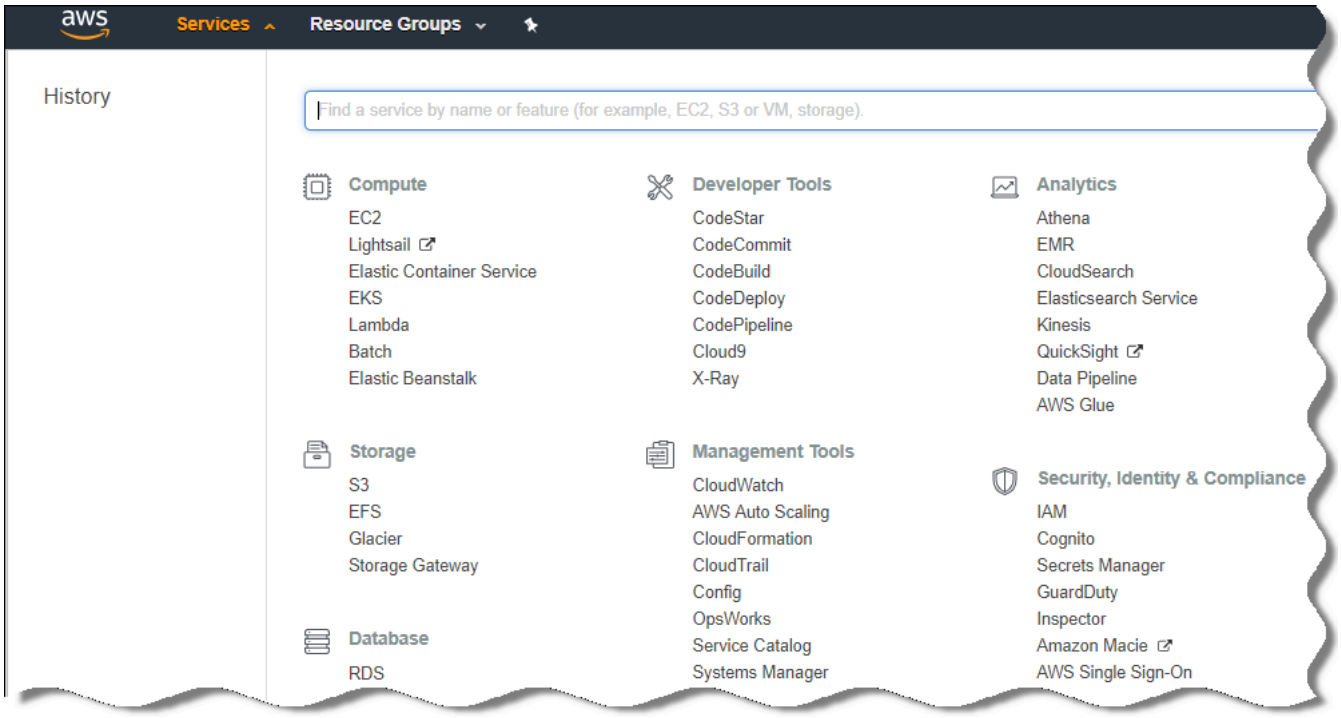
لا يعد التكوين الافتراضي لمجموعة الخيارات التي وضعت فيها مثيل Amazon RDS كافيًا للعمل بقاعدة بيانات Kaspersky Security Center. يجب عليك إضافة خيارات إلى مجموعة الخيارات وإنشاء دور IAM جديد للعمل مع قاعدة البيانات.

قم بما يلي لتعديل مجموعة الخيارات وإنشاء دور IAM جديد:

1. تأكد من أنك في وحدة التحكم الخاصة بإدارة AWS (https://console.aws.amazon.com/) وأنك قمت بتسجيل الدخول إلى حسابك.

2. في سطر القائمة، انقر فوق **خدمات**.

تظهر قائمة الخدمات المتاحة (انظر الشكل أدناه).



قائمة الخدمات في وحدة التحكم الخاصة بإدارة AWS

3. في القائمة ، حدد RDS.

4. في الجزء الأيسر، انقر فوق **مجموعات الخيارات**.

يتم عرض قائمة مجموعات الخيارات.

5. حدد مجموعة الخيارات التي وضعت فيها مثيل Amazon RDS الخاص بك وانقر فوق الزر **إضافة خيار**.

تفتح النافذة **إضافة خيار**.

6. في قسم دور IAM، حدد الخيار **إنشاء دور جديد / نعم** وأدخل اسمًا لدور IAM الجديد.

يتم إنشاء الدور بمجموعة افتراضية من الأذونات. وفي وقتٍ لاحق، سوف يتعين عليك تغيير الأذونات الخاصة به.

7. قم بأحد الإجراءات التالية في قسم مستودع S3:

- إذا لم تقم بإنشاء مثيل مستودع خدمة Amazon S3 لنسخ البيانات احتياطيًا، فحدد الارتباط **إنشاء مستودع S3 جديد** وقم بإنشاء مستودع S3 جديد باستخدام واجهة AWS.
- إذا كنت قد قمت بالفعل بإنشاء مثيل مستودع خدمة Amazon S3 لمهمة النسخ الاحتياطي لبيانات خادم الإدارة، فحدد مستودع S3 الخاص بك من القائمة المنسدلة.

8. الانتهاء من إضافة خيارات بالنقر فوق الزر **إضافة خيار** في أسفل الصفحة.

لقد قمت بتعديل مجموعة الخيارات وإنشاء دور IAM جديد للعمل مع قاعدة بيانات RDS.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

تعديل الأذونات لدور IAM لمثيل قاعدة بيانات Amazon RDS

بعد إضافة خيارات إلى مجموعة الخيارات، يجب عليك تعيين الأذونات المطلوبة لدور IAM الذي قمت بإنشائه للعمل مع مثيل قاعدة بيانات Amazon RDS.

قم بما يلي لتعيين الأذونات المطلوبة لدور IAM الذي قمت بإنشائه للعمل مع مثيل قاعدة بيانات Amazon RDS:

1. تأكد من أنك في وحدة التحكم الخاصة بإدارة AWS (https://console.aws.amazon.com/) وأنك قمت بتسجيل الدخول إلى حسابك.

2. في قائمة الخدمات، حدد **IAM**.

تفتح نافذة تحتوي على قائمة بأسماء المستخدمين وقائمة تسمح لك بالعمل مع الأداة.

3. في القائمة، حدد **الأدوار**.

4. في قائمة أدوار IAM المعروضة في مساحة العمل، حدد الدور الذي قمت بإنشائه عند إضافة خيار لمجموعة الخيارات.

5. باستخدام واجهة AWS، احذف سياسة **<date>-sqlNativeBackup**.

6. باستخدام واجهة AWS، قم بإرفاق سياسة **AmazonS3FullAccess** بالدور.

يتم تعيين الأذونات المطلوبة إلى دور IAM للعمل مع Amazon RDS.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

تحضير مستودع خدمة Amazon S3 لقاعدة البيانات

إذا كنت تخطط لاستخدام قاعدة بيانات Amazon Relational Database System (Amazon RDS)، فعليك إنشاء مثيل مستودع Amazon Simple Storage Service (خدمة Amazon S3) حيث سيتم تخزين النسخة الاحتياطية العادية لقاعدة البيانات. للحصول على معلومات حول خدمة Amazon S3 وحول مستودعات S3، يُرجى الرجوع إلى الرجوع إلى صفحات تعليمات Amazon. لمزيد من المعلومات حول إنشاء مثيل خدمة Amazon S3، يُرجى الرجوع إلى صفحة تعليمات Amazon S3.

قم بما يلي لإنشاء مثيل مستودع خدمة Amazon S3:

1. تأكد أنّ وحدة التحكم الخاصة بإدارة AWS مفتوحة وأنك سجلت الدخول إلى حسابك.
2. في قائمة خدمات AWS، حدد S3.
3. انتقل إلى وحدة التحكم لإنشاء مستودع، واتبع إرشادات المعالج.
4. حدد نفس المنطقة التي يتواجد فيها خادم الإدارة الخاص بك (أو سيكون متواجدًا فيها).
5. عند انتهاء المعالج، تأكد من ظهور المستودع الجديد في قائمة المستودعات.

يتم إنشاء مستودع S3 جديد ويظهر في قائمة المستودعات الخاصة بك. يجب عليك تحديد هذا المستودع عند إضافة خيارات إلى مجموعة الخيارات. سوف يتعين عليك أيضًا تحديد عنوان مستودع S3 الخاص بك في Kaspersky Security Center عندما يقوم Kaspersky Security Center بإنشاء مهمة النسخ الاحتياطي لبيانات خادم الإدارة.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

ترحيل قاعدة البيانات إلى Amazon RDS

يمكنك ترحيل قاعدة بيانات Kaspersky Security Center الخاصة بك من جهاز موجود في مكان العمل إلى مثيل خدمة Amazon S3 الذي يدعم Amazon RDS. لإجراء ذلك، تحتاج إلى مستودع S3 لقاعدة بيانات RDS وحساب مستخدم IAM مزوّد بإذن AmazonS3FullAccess لمستودع S3 هذا.

قم بما يلي لتنفيذ عملية ترحيل قاعدة البيانات هذه:

1. تأكد من قيامك بإنشاء مثيل RDS (يُرجى الرجوع إلى صفحات المراجع لـ Amazon RDS لمزيد من المعلومات).
2. على خادم الإدارة المادي الخاص بك (في أماكن العمل)، قم بتشغيل أداة النسخ الاحتياطي Kaspersky Backup لنسخ بيانات خادم الإدارة احتياطيًا.
   يجب عليك التأكد أن الملف باسم backup.zip.
3. انسخ ملف backup.zip إلى مثيل EC2 المثبت عليه خادم الإدارة.

تأكد من وجود مساحة قرص كافية على مثيل EC2 المثبت عليه خادم الإدارة. في بيئة AWS، يمكنك إضافة مساحة قرص إلى المثيل الخاص بك لاستيعاب عملية ترحيل قاعدة البيانات.

4. على خادم إدارة AWS، ابدأ تشغيل أداة النسخ الاحتياطي Kaspersky Backup مرة أخرى في الوضع التفاعلي.
   يبدأ معالج النسخ الاحتياطي والاستعادة.
5. في الخطوة **حدد إجراء**، حدد **استعادة بيانات خادم الإدارة** وانقر فوق **التالي**.
6. في الخطوة **استعادة الإعدادات**، انقر على زر **استعراض** الموجود بجوار **المجلد المخصص لتخزين النسخ الاحتياطية**.

7. في النافذة **تسجيل الدخول إلى التخزين عبر الإنترنت** التي تفتح، املأ الحقول التالية، ثم انقر فوق **موافق**:

- **اسم مستودع S3**

اسم مستودع S3 الخاص بك.

- **مجلد النسخ الاحتياطي**

حدد موقع مجلد التخزين المقصود للنسخ الاحتياطي.

- **معرف مفتاح الوصول**

معرف مفتاح وصول AWS IAM الذي ينتمي إلى مستخدم IAM الذي يتمتع بالأذونات لاستخدام مستودع S3 (الإذن AmazonS3FullAccess).

- **المفتاح السري**

المفتاح السري AWS IAM الذي ينتمي إلى مستخدم IAM الذي يتمتع بالأذونات لاستخدام مستودع S3 (الإذن AmazonS3FullAccess).

8. حدد الخيار **الترحيل من النسخ الاحتياطي المحلي**. يصبح الزر **استعراض** متاحًا.

9. انقر على زر **استعراض** لاختيار المجلد الموجود في خادم إدارة AWS حيث قمت بنسخ ملف backup.zip.

10. انقر فوق **التالي** واستكمل الإجراءات.

ستتم استعادة بياناتك إلى قاعدة بيانات RDS باستخدام مستودع S3 الخاص بك. يمكنك استخدام قاعدة البيانات هذه للعمل مع Kaspersky Security Center بصورة أكبر في بيئة AWS.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

العمل في بيئة السحابة لـ Microsoft Azure

يوفر هذا القسم معلومات حول نشر Kaspersky Security Center وصيانته في بيئة السحابة التي توفرها Amazon Web Services، وكذلك تفاصيل نشر الحماية على الأجهزة الظاهرية الموجودة في بيئة السحابة هذه.

في Kaspersky Security Center الذي تم نشره من منتج تتم المحاسبة عليه شهريًا على أساس الاستخدام، يتم تفعيل ميزة إدارة الثغرات الأمنية والتصحيحات تلقائيًا، ويتعذر تفعيل إدارة الجهاز المحمول.

حول العمل في Microsoft Azure

للعمل مع منصة Microsoft Azure، وعلى وجه الخصوص، لشراء التطبيقات في السوق الخاص بـ Azure وإنشاء الأجهزة الظاهرية، ستحتاج إلى الحصول على اشتراك Azure. قبل أن تنشر خادم الإدارة، أنشئ معرف تطبيق Azure مع الأذونات المطلوبة لتثبيت التطبيقات على الأجهزة الافتراضية.

إذا قمت بشراء صورة من Kaspersky Security Center في السوق الخاص بـ Azure، فيمكنك نشر جهاز ظاهري مزود بخادم إدارة Kaspersky Security Center جاهز للاستخدام. يجب عليك تحديد إعدادات الجهاز الظاهري، ولكن لا ينبغي عليك تثبيت التطبيق بنفسك. بعد التثبيت، يمكنك بدء وحدة تحكم الإدارة والاتصال بخادم الإدارة لبدء استخدام Kaspersky Security Center.

يمكنك أيضًا استخدام جهاز ظاهري في Azure تم نشر خادم إدارة Kaspersky Security Center عليه لحماية الأجهزة الموجودة في مكان العمل (على سبيل المثال، إذا اتضحت سهولة استخدام وصيانة خادم السحابة أكثر من الخادم المادي). وإذا كان الأمر كذلك، فأنت تعمل مع خادم الإدارة كما لو كان خادم الإدارة مثبتًا على جهاز موجود بالفعل في مكان العمل. إذا كنت لا تخطط لاستخدام أدوات Azure API، فإنك لا تحتاج إلى معرف تطبيق Azure. وفي هذه الحالة، يكون اشتراك Azure كافيًا.

إنشاء اشتراك ومعرف تطبيق وكلمة مرور

للعمل مع Kaspersky Security Center في بيئة Microsoft Azure، تحتاج إلى اشتراك Azure، ومعرف تطبيق Azure، وكلمة مرور تطبيق Azure. يمكنك استخدام اشتراك موجود بالفعل، إذا كان لديك اشتراك بالفعل.

يمنح اشتراك Azure مالكه إمكانية الوصول إلى Microsoft Azure Platform Management Portal وإلى خدمات Microsoft Azure. يمكن للمالك استخدام Microsoft Azure Platform لإدارة الخدمات مثل Azure SQL وAzure Storage.

لإنشاء اشتراك Microsoft Azure،

انتقل إلى https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription واتبع التعليمات المدرجة هناك.

تتوفر المزيد من المعلومات حول إنشاء اشتراك على الموقع الإلكتروني لـ Microsoft. سوف تحصل على معرف اشتراك، والذي ستقدمه لاحقًا إلى Kaspersky Security Center إلى جانب معرف التطبيق وكلمة المرور.

لإنشاء وحفظ معرف تطبيق Azure وكلمة المرور:

1. انتقل إلى https://portal.azure.com وتأكد من قيامك بتسجيل الدخول.
2. اتباع التعليمات على صفحة المراجع، إنشاء معرف التطبيق الخاص بك.
3. انتقل إلى القسم **مفاتيح** في إعدادات التطبيق.
4. في القسم **مفاتيح**، املأ الحقول **الوصف** و**انتهاء الصلاحية** واترك حقل **القيمة** فارغًا.
5. انقر فوق **حفظ**.

   عند قيامك بالنقر فوق **حفظ**، يقوم النظام تلقائيًا بملء حقل **القيمة** بتسلسل طويل من الأحرف. هذا التسلسل هو كلمة مرور تطبيق Azure الخاصة بك (على سبيل المثال، yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). يتم عرض الوصف عند قيامك بإدخاله.
6. انسخ كلمة المرور واحفظها بحيث يمكنك فيما بعد توفير معرف التطبيق وكلمة المرور إلى Kaspersky Security Center.

   يمكنك نسخ كلمة المرور فقط عند إنشائها. لن يتم لاحقًا عرض كلمة المرور بعد الآن ولن تتمكن من استعادتها.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

تعيين دور لمعرف تطبيق Azure

إذا كنت تريد اكتشاف الأجهزة الظاهرية فقط باستخدام اكتشاف الأجهزة، فيجب أن يمتلك معرف تطبيق Azure الخاص بك دور القارئ. إذا كنت لا تريد اكتشاف الأجهزة الظاهرية فحسب، ولكن أيضًا لنشر الحماية على الأجهزة الظاهرية، فيجب أن يمتلك معرف تطبيق Azure الخاص بك دور مساهم الجهاز الظاهري.

اتبع التعليمات الموجودة على الموقع الإلكتروني لـ Microsoft لتعيين دور لمعرف تطبيق Azure الخاص بك.

نشر خادم الإدارة في Microsoft Azure وتحديد قاعدة البيانات

قم بما يلي لنشر خادم الإدارة في بيئة Microsoft Azure:

1. قم بتسجيل الدخول إلى Microsoft Azure باستخدام حسابك.

2. انتقل إلى مدخل Azure.

3. في الجزء الأيسر، انقر فوق علامة الجمع خضراء اللون.

4. اكتب "Kaspersky Hybrid Cloud Security" في حقل البحث في القائمة.

   Kaspersky Hybrid Cloud Security هو مزيج من Kaspersky Security Center وتطبيقي أمان لحماية المثيلات: Kaspersky Endpoint Security for Linux وKaspersky Security for Windows Server.

5. في قائمة النتائج، حدد Kaspersky Hybrid Cloud Security أو Kaspersky Hybrid Cloud Security (BYOL).

   في الجزء الأيمن من الشاشة، تظهر نافذة معلومات.

6. اقرأ المعلومات وانقر فوق الزر إنشاء الموجود في نهاية نافذة المعلومات.

7. املأ جميع الحقول المطلوبة. استخدم تلميحات الأداة للحصول على معلومات والمساعدة.

8. عند تحديد الحجم، حدد أحد الخيارات الثلاثة المميزة بنجمة.

   في معظم الحالات، تكفي 8 جيجابايت (GB) من ذاكرة الوصول العشوائي (RAM). ومع ذلك، يمكنك في Azure زيادة حجم ذاكرة الوصول العشوائي (RAM) وغيرها من موارد الجهاز الظاهري في أي وقت.

9. عند تحديد قاعدة بيانات، حدد واحدًا مما يلي، وفقًا لخطتك:

   - محلي—إذا كنت تريد قاعدة بيانات على نفس الجهاز الظاهري حيث سيتم نشر خادم الإدارة. يأتي Kaspersky Security Center مجهزًا بقاعدة بيانات SQL Server Express. اختر هذا الخيار إذا كان SQL Server Express كافياً لاحتياجاتك.
   - جديد—إذا كنت تريد قاعدة بيانات RDS جديدة في بيئة Azure. اختر هذا الخيار إذا كنت تريد نظام DBMS غير SQL Server Express. سيتم نقل البيانات الخاصة بك إلى بيئة السحابة، حيث ستظل هناك ولن تتكبد أية نفقات إضافية.
   - موجود بالفعل—إذا كنت تريد استخدم خادم قاعدة بيانات موجود بالفعل. في هذه الحالة، سيكون عليك تحديد موقعه. إذا كان هذا الخادم موجودًا خارج بيئة Azure، فسيتم نقل بياناتك عبر الإنترنت، مما قد يؤدي إلى تكبد نفقات إضافية.

10. عند إدخال مُعرّف الاشتراك، استخدم الاشتراك الذي قمت بإنشائه سابقًا.

بعد إجراء عملية النشر، يمكنك الاتصال بخادم الإدارة باستخدام RDP. يمكنك استخدام وحدة تحكم الإدارة للعمل مع خادم الإدارة.

العمل مع Azure SQL

يصف هذا القسم أي الإجراءات يجب اتخاذها لإعداد قاعدة بيانات Microsoft Azure لـ Kaspersky Security Center، وإعداد حساب تخزين Azure، وترحيل قاعدة بيانات موجودة بالفعل إلى Azure SQL.

قاعدة بيانات SQL هي خدمة مدارة لقاعدة بيانات ارتباطية لأغراض عامة في Microsoft Azure.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

إنشاء حساب تخزين Azure

يجب عليك إنشاء حساب تخزين في Microsoft Azure للعمل مع قاعدة بيانات Azure SQL ومن أجل البرامج النصية للنشر.

قم بما يلي لإنشاء حساب تخزين:

1. قم بتسجيل الدخول إلى مدخل Azure.
2. في الجزء الأيسر، حدد **حسابات التخزين** للانتقال إلى نافذة **حسابات التخزين**.
3. في نافذة **حسابات التخزين**، انقر فوق الزر **إضافة** للانتقال إلى نافذة **إنشاء حساب تخزين**.
4. املأ جميع الحقول المطلوبة لإنشاء حساب تخزين:
   - الموقع: يجب أن يكون هو نفسه موقع خادم الإدارة.
   - الحقول الأخرى: يمكنك ترك القيم الافتراضية.

   استخدم تلميحات الأداة للحصول على معلومات حول كل حقل.

   بعد إنشاء حساب التخزين، يتم عرض قائمة حسابات التخزين الخاصة بك.
5. في قائمة حسابات التخزين الخاصة بك، انقر فوق اسم الحساب الذي تم إنشاؤه حديثًا للاطلاع على معلومات حول هذا الحساب.
6. تأكد من أنك تعرف اسم الحساب، ومجموعة الموارد، ومفاتيح الوصول لحساب التخزين هذا. ستحتاج إلى هذه المعلومات للعمل مع Kaspersky Security Center.

يمكنك الرجوع إلى الموقع الإلكتروني لـ Azure للحصول على المساعدة.

إذا كان لديك حساب تخزين بالفعل، فيمكنك استخدامه للعمل مع Kaspersky Security Center.

إنشاء قاعدة بيانات Azure SQL وخادم SQL Server

تحتاج إلى قاعدة بيانات SQL وخادم SQL Server في بيئة Azure.

قم بما يلي لإنشاء قاعدة بيانات Azure SQL وخادم SQL Server:

1. اتبع التعليمات على الموقع الإلكتروني لـ Azure.

   يمكنك إنشاء خادم جديد عندما يطالبك Microsoft Azure بذلك؛ إذا كان لديك خادم Azure SQL Server، يمكنك استخدامه Kaspersky Security Center بدلًا من إنشاء واحد جديد.
2. بعد إنشاء قاعدة بيانات SQL وخادم SQL Server، تأكد من أنك تعرف اسم المورد ومجموعة الموارد الخاصة به:
   a. انتقل إلى https://portal.azure.com وتأكد من قيامك بتسجيل الدخول.
   b. في الجزء الأيسر، حدد **قواعد بيانات SQL**.
   c. انقر فوق اسم قاعدة البيانات من قائمة قواعد البيانات الخاصة بك.

      تفتح نافذة الخصائص.
   d. اسم قاعدة البيانات هو اسم المورد. يتم عرض اسم مجموعة الموارد في قسم **نظرة عامة** في نافذة خصائص.

أنت بحاجة إلى اسم المورد ومجموعة الموارد لقاعدة البيانات المخصصة لترحيل قاعدة البيانات إلى Azure SQL.

ترحيل قاعدة البيانات إلى Azure SQL

بعد نشر خادم الإدارة في بيئة Azure، يمكنك ترحيل قاعدة بيانات Kaspersky Security Center الخاصة بك من جهاز موجود في مكان العمل إلى Azure SQL. أنت بحاجة إلى حساب تخزين Azure لقاعدة بيانات Azure SQL. يجب أيضًا أن يكون لديك Microsoft SQL Server Data-Tier Application Framework (DacFx) وSQLSysCLRTypes على خادم الإدارة الخاص بك.

قم بما يلي لتنفيذ عملية ترحيل قاعدة البيانات هذه:

1. تأكد من أنك قمت بإنشاء حساب تخزين Azure.

2. تأكد من توفر DacFx وSQLSysCLRTypes لديك على خادم الإدارة الخاص بك.

   يمكنك تنزيل إطار عمل تطبيق Microsoft SQL Server Data-Tier (DacFx 17.0.1) و SQLSysCLRTypes (اختر الإصدار المطابق لإصدار SQL Server الخاص بك) من موقع ويب Microsoft الرسمي.

3. على خادم الإدارة المادي لديك (في أماكن العمل)، قم بتشغيل أداة النسخ الاحتياطي Kaspersky لنسخ بيانات خادم الإدارة احتياطيًا من خلال تمكين خيار **الترحيل إلى تنسيق Azure**.

4. انسخ ملف النسخة الاحتياطية إلى خادم إدارة Azure.

> تأكد من وجود مساحة قرص كافية على الجهاز الظاهري Azure حيث تم تثبيت خادم الإدارة. في بيئة Azure، يمكنك إضافة مساحة قرص إلى الأجهزة الظاهرية الخاصة بك لاستيعاب عملية ترحيل قاعدة البيانات.

5. على خادم الإدارة الموجود في بيئة Microsoft Azure، قم بتشغيل أداة النسخ الاحتياطي Kaspersky Backup مرة أخرى في الوضع التفاعلي.

   يبدأ معالج النسخ الاحتياطي والاستعادة.

6. في الخطوة **حدد إجراء**، حدد **استعادة بيانات خادم الإدارة** وانقر فوق **التالي**.

7. في الخطوة **استعادة الإعدادات**، انقر على زر **استعراض** الموجود بجوار **المجلد المخصص لتخزين النسخ الاحتياطية**.

8. في النافذة **تسجيل الدخول إلى التخزين عبر الإنترنت** التي تفتح، املأ الحقول التالية، ثم انقر فوق **موافق**:

   - **اسم حساب تخزين Azure**

     لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

   - **مجلد النسخ الاحتياطي**

     حدد موقع مجلد التخزين المقصود للنسخ الاحتياطي.

   - **معرف اشتراك Azure**

     لقد قمت بإنشاء الاشتراك على مدخل Azure.

   - **كلمة مرور تطبيق Azure**

     لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

     تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

   - **مفتاح وصول تخزين Azure**

     يكون متاحًا في خصائص حساب التخزين الخاص بك، في قسم مفاتيح الوصول. يمكنك استخدام أي من المفاتيح (المفتاح1 أو المفتاح2).

- **اسم خادم Azure SQL Server**

تكون متاحة في خصائص خادم Azure SQL Server الخاص بك.

- **مجموعة مورد خادم Azure SQL Server**

تكون متاحة في خصائص خادم Azure SQL Server الخاص بك.

- **معرف تطبيق Azure**

لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

9. حدد الخيار **الترحيل من النسخ الاحتياطي المحلي**.

يصبح الزر **استعراض** متاحًا.

10. انقر فوق زر **استعراض** لاختيار المجلد الموجود في خادم إدارة Azure حيث قمت بنسخ ملف النسخ الاحتياطي.

11. انقر فوق **التالي** واستكمل الإجراءات.

ستتم استعادة بياناتك إلى قاعدة بيانات Azure SQL باستخدام خدمة تخزين Azure الخاصة بك. يمكنك استخدام قاعدة البيانات هذه للعمل مع Kaspersky Security Center بصورة أكبر في بيئة Azure.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

العمل في Google Cloud

يقدم هذا القسم معلومات بشأن العمل مع Kaspersky Security Center في بيئة سحابية مقدمة من Google.

إنشاء بريد إلكتروني للعميل ومعرف المشروع ومفتاح خاص

يمكنك استخدام Google API للعمل باستخدام Kaspersky Security Center الموجود في Google Cloud. حساب Google مطلوب. يرجى الرجوع إلى وثائق Google على https://cloud.google.com لمزيد من المعلومات.

ستحتاج إلى تزويد Kaspersky Security Center ببيانات الاعتماد التالية:

- **البريد الإلكتروني للعميل**

البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

- **معرف المشروع**

معرف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

- **مفتاح خاص**

المفتاح الخاص هو تسلسل الأحرف التي استلمتها كمفتاح خاص عند تسجيل مشروعك في Google Cloud. قد ترغب في نسخ هذا التسلسل ولصقه لتجنب الأخطاء.

العمل مع Google Cloud SQL لمثيل MySQL

يمكنك إنشاء قاعدة بيانات على Google Cloud واستخدام قاعدة البيانات هذه لـ Kaspersky Security Center.

يعمل Kaspersky Security Center مع MySQL 5.7 و 5.6. لم يتم اختبار الإصدارات الأخرى من MySQL.

لإنشاء قاعدة بيانات MySQL وتكوينها:

في متصفحك، انتقل إلى https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen واتبع التعليمات المتوفرة.

عند تكوين قاعدة بيانات MySQL، استخدم العلامات التالية:

- **Sort_buffer_size** 10000000
- **Join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **low_case_table_names** 1

المتطلبات الأساسية للأجهزة العميلة في بيئة السحابة والتي تكون لازمة للعمل مع Kaspersky Security Center

الأجهزة التي ترغب في تثبيت خادم الإدارة، وعميل الشبكة وتطبيقات الأمان لـ Kaspersky عليها يجب أن تستوفي الشروط التالية:

- يؤدي تكوين مجموعات الأمان إلى توفر المنافذ التالية على خادم الإدارة (الحد الأدنى من المنافذ المطلوبة للنشر):
  - HTTP 8060 (لنقل حزم تثبيت عميل الشبكة وحزم تثبيت تطبيق الأمان من خادم الإدارة إلى المثيلات المحمية)
  - HTTPS 8061(لنقل حزم تثبيت عميل الشبكة وحزم تثبيت تطبيق الأمان من خادم الإدارة إلى المثيلات المحمية)
  - TCP 13000 (لعمليات النقل من المثيلات المحمية والخوادم التابعة إلى خادم الإدارة الرئيسي باستخدام SSL)
  - UDP 13000 (لنقل المعلومات حول إيقاف تشغيل المثيلات إلى خادم الإدارة)
  - TCP 14000 (لعمليات النقل من المثيلات المحمية والخوادم التابعة إلى خادم الإدارة الرئيسي دون استخدام SSL)

- 13291 (للاتصال وحدة تحكم الإدارة بخادم الإدارة)
- 40080—لتشغيل البرامج النصية للنشر

يمكنك تكوين مجموعات الأمان في وحدة التحكم الخاصة بإدارة AWS، أو في مدخل Azure. إذا كنت تعتزم استخدام Kaspersky Security Center بتكوين غير افتراضي، يرجى الرجوع إلى قاعدة المعرفة. تشتمل الأمثلة على التكوينات غير الافتراضية على عدم تثبيت وحدة تحكم الإدارة على جهاز خادم الإدارة ولكن تثبيتها بدلًا من ذلك على محطة العمل الخاصة بك، أو استخدام خادم وكيل KSN.

- المنفذ UDP 15000 متوفر على الأجهزة العميلة (لاستلام الطلبات للتواصل مع خادم الإدارة).
- في بيئة سحابة AWS:
  - إذا كنت تخطط لاستخدام AWS API، فإنه يتم ضبط دور IAM ضمن التطبيقات التي سيتم تثبيتها على المثيلات.
  - في كل مثيل Amazon EC2، يتم تثبيت Systems Manager Agent (عامل SSM) وتشغيله.
  - يتيح عامل SSM لـ Kaspersky Security Center بتثبيت التطبيقات تلقائيًا على الأجهزة ومجموعات الأجهزة دون طلب تأكيد المسؤول في كل مرة.
  - في المثيلات التي تعمل بنظام تشغيل Windows والتي يتم نشرها من صور AMI في وقت لاحق لشهر نوفمبر 2016، يتم تثبيت عامل SSM وتشغيله. سيتعين عليك تثبيت عامل SSM يدويًا على جميع الأجهزة الأخرى. للمزيد من التفاصيل حول تثبيت عامل SSM على الأجهزة التي تعمل بأنظمة تشغيل Windows وLinux، يرجى الرجوع إلى صفحة التعليمات لـ AWS.
- في بيئة السحابة لـ Microsoft Azure:
  - في كل جهاز ظاهري لـ Azure، يتم تثبيت Azure VM Agent وتشغيله.

    يتم بصورة افتراضية إنشاء جهاز ظاهري مثبت عليه Azure VM Agent، ولا يتوجب عليك تثبيته أو تمكينه يدويًا. يرجى الرجوع إلى صفحات التعليمات الخاصة بـ Microsoft للحصول على التفاصيل حول Azure VM Agent على الأجهزة التي تعمل بنظام Windows والأجهزة التي تعمل بنظام Linux.
  - يكون لمعرف تطبيق Azure الخاص بك الأدوار التالية:
    - قارئ (لاكتشاف الأجهزة الظاهرية باستخدام الاستقصاء)
    - مساهم الجهاز الظاهري (لنشر الحماية على الأجهزة الظاهرية)
    - مساهم خادم SQL Server (لاستخدام قاعدة بيانات SQL في بيئة Microsoft Azure)

    إذا كنت ترغب في إجراء جميع هذه العمليات، قم بتعيين الأدوار الثلاثة جميعًا إلى معرف تطبيق Azure الخاص بك.

إنشاء حزم التثبيت المطلوبة لتكوين بيئة السحابة

يتوفر معالج تكوين بيئة السحابة في Kaspersky Security Center إذا كانت لديك حزم التثبيت ومكونات الإدارة الإضافية الخاصة بالبرامج التالية:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

سيكون نشر Kaspersky Endpoint Security for Windows في بيئة سحابية متاحًا بعد الإصدار القادم من Kaspersky Endpoint Security 12.0 for Windows.

- Kaspersky Security for Windows Server

تكون حزم التثبيت هذه مطلوبة لتثبيت التطبيقات على المثيلات أو الأجهزة الظاهرية التي تريد حمايتها. إذا لم يكن لديك حزم التثبيت هذه، يجب عليك إنشائها. وبخلاف ذلك، لا يمكن أن يعمل معالج تكوين بيئة السحابة.

لإنشاء حزم التثبيت:

1. قم بتنزيل أحدث إصدارات من التطبيقات والمكونات الإضافية على موقع ويب Kaspersky:
   - أداة التثبيت ومكوّن الإدارة الإضافي لبرنامج Kaspersky Security for Windows Server
   - المثبت والملفات للتثبيت عن بُعد عبر Kaspersky Security Center والمكون الإضافي للإدارة لتطبيق Kaspersky Endpoint Security for Linux.
2. احفظ جميع الملفات على المثيل (أو الجهاز الظاهري) المثبت عليه خادم الإدارة.
3. قم باستخراج جميع الملفات من الحزم.
4. ابدأ Kaspersky Security Center.
5. في شجرة وحدة التحكم، اذهب إلى **متقدم** ← **التثبيت عن بُعد** ← **حزم التثبيت** ثم انقر على **إنشاء حزمة التثبيت**.
6. حدد **إنشاء حزمة تثبيت Kaspersky**.
7. حدد اسم الحزمة ومسار مثبت التطبيق: kud.<file name>\<folder> ثم انقر على **التالي**.
8. اقرأ اتفاقية ترخيص المستخدم النهائي وحدد خانة الاختيار مؤكدًا على قبولك لشروطها، ثم انقر على **التالي**.

سيتم رفع حزمة التثبيت إلى خادم الإدارة، وستتوفر في قائمة حزم التثبيت.

يتوفر تكوين بيئة سحابة بمجرد أن تنشئ حزم التثبيت وتُثبت المكونات الإضافية للإدارة على خادم الإدارة.

تكوين بيئة السحابة

لتكوين Kaspersky Security Center باستخدام هذه البيئة، يجب أن تمتلك ما يلي:

- بيانات اعتماد محددة لبيئة السحابة:
  - دور IAM الذي تم منحه حق استقصاء قطاع السحابة أو حساب مستخدم IAM الذي تم منحه حق استقصاء قطاع السحابة (للعمل مع Amazon Web Services)
  - معرف تطبيق Azure، وكلمة المرور، والاشتراك (للعمل في بيئة السحابة لـ Microsoft Azure)
  - البريد الإلكتروني لعميل Google ومعرف المشروع والمفتاح الخاص (للعمل مع Google Cloud)
- حزم التثبيت:
  - عميل الشبكة لنظام التشغيل Windows
  - عميل الشبكة لنظام التشغيل Linux
  - Kaspersky Endpoint Security for Linux
  - المكون الإضافي للويب لـ Kaspersky Endpoint Security for Linux

- أحد ما يلي على الأقل:
  - حزمة التثبيت ومكوّن الويب الإضافي لتطبيق Kaspersky Endpoint Security for Windows (موصى به)
  - حزمة التثبيت ومكوّن الويب الإضافي لتطبيق Kaspersky Security for Windows Server

إذا كنت لا ترغب في استخدام إمكانيات بيئة السحابة (إذا كنت ترغب، على سبيل المثال، في إدارة حماية الأجهزة العميلة المادية فقط)، يمكنك إغلاق معالج تكوين بيئة السحابة وتشغيل معالج البدء السريع لخادم الإدارة القياسي يدويًا.

سيبدأ تشغيل عملية تكوين بيئة السحابة تلقائيًا في أول اتصال بخادم الإدارة من خلال وحدة تحكم الإدارة إذا كنت تقوم بنشر Kaspersky Security Center من صورة جاهزة للاستخدام. ويمكنك أيضًا بدء تشغيل معالج تكوين بيئة السحابة يدويًا في أي وقت.

لبدء تشغيل معالج تكوين بيئة السحابة يدويًا:

1. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.
2. في قائمة السياق الخاصة بالعقدة، حدد **كل المهام** ← **تكوين بيئة السحابة**.

يستمر متوسط جلسة العمل 15 دقيقة تقريبًا.

حول معالج تكوين بيئة السحابة

يسمح لك معالج تكوين بيئة السحابة بتكوين Kaspersky Security Center مع أخذ متطلبات العمل في بيئة السحابة في الاعتبار.

يقوم المعالج بإنشاء العناصر التالية:

- سياسة عميل الشبكة مع الإعدادات الافتراضية.
- السياسة لـ Kaspersky Endpoint Security for Linux
- السياسة لتطبيق Kaspersky Security for Windows Server
- مجموعة الإدارة لمثيلات وقاعدة النقل التلقائي للمثيلات إلى مجموعة الإدارة هذه
- مهمة نسخ احتياطي لبيانات خادم الإدارة:
- مهام تثبيت الحماية على الأجهزة التي تعمل بنظام Linux وWindows
- مهام لكل جهاز مدار:
  - فحص البرامج الضارة السريع
  - تنزيل التحديث

إذا حددت خيار ترخيص BYOL، سيقوم تكوين بيئة السحابة أيضًا بتفعيل Kaspersky Security Center باستخدام ملف مفتاح أو رمز تفعيل ويضع المفتاح أو رمز التفعيل في مخزن الترخيص.

الخطوة 1. تحديد طريقة تفعيل التطبيق

لا يتم عرض هذه الخطوة إذا قمت بالتسجيل في واحدة من AMIs الجاهزة للاستخدام (في سوق AWS)، أو SKU للفواتير الشهرية المستندة إلى الاستخدام (في سوق Azure). وفي هذه الحالة، ينتقل المعالج فورًا إلى الخطوة التالية. ومع ذلك، لا يمكنك شراء AMI جاهز للاستخدام لسحابة Google.

إذا قمت بتحديد خيار ترخيص BYOL لـ Kaspersky Security Center، سيطالبك المعالج بتحديد طريقة تفعيل التطبيق.

تفعيل التطبيق باستخدام رمز التنشيط (أو ملف مفتاح) لـ Kaspersky Security for Virtualization أو لـ Kaspersky Hybrid Cloud Security.

يمكنك تفعيل التطبيق بإحدى الطرق التالية:

- عن طريق إدخال رمز تنشيط.

  سيبدأ التفعيل عبر الإنترنت. ستتضمن هذه العملية التحقق من رمز التنشيط المحدد وإصدار ملف المفتاح وتفعيله.

- عن طريق تحديد ملف المفتاح.

  سيتحقق التطبيق من ملف المفتاح وإما أن يقوم بتنشيطه إذا كان يحتوي على المعلومات الصحيحة، أو يطالبك بتحديد ملف مفتاح آخر.

سيضع Kaspersky Security Center مفتاح الترخيص في مخزن الترخيص ويميزه بأنه مفتاح تم توزيعه تلقائيًا على الأجهزة المدارة.

إذا اتصلت بمثيل باستخدام التطبيق Remote Desktop Connection القياسي في Microsoft Windows أو باستخدام تطبيق مماثل، فيجب عليك أن تقوم بتحديد محرك أقراص الجهاز الفعلي الذي تستخدمه للاتصال من خصائص الاتصال عن بُعد. سيضمن لك ذلك الوصول من المثيل إلى الملفات الموجودة على جهازك الفعلي، ويتيح لك تحديد الملف المفتاح.

عند استخدام Kaspersky Security Center الذي تم نشره من صورة AMI مدفوعة الأجر أو لوحدة احتفاظ بمخزون تتم المحاسبة عليها شهريًا حسب الاستخدام، فلن تتمكن من إضافة ملفات المفتاح أو رموز التنشيط إلى مخزن الترخيص.

الخطوة 2. تحديد بيئة السحابة

حدد بيئة السحابة التي تقوم فيها بنشر Kaspersky Security Center: AWS أو Azure.

الخطوة 3. التخويل في بيئة السحابة

AWS

إذا قمت بتحديد AWS، فحدد أن لديك دور IAM يتمتع بالحقوق المطلوبة أو قم بتوفير Kaspersky Security Center بمفتاح وصول AWS IAM. لا يمكن القيام باستقصاء قطاع السحابة بدون دور IAM أو مفتاح وصول AWS IAM.

حدد الإعدادات التالية للاتصال الذي سيتم استخدامه لاستقصاء قطاع السحابة بعد ذلك:

- **اسم الاتصال**

  أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google".

- **استخدام دور AWS IAM**

حدد هذا الخيار إذا قمت بالفعل بإنشاء دور IAM لخادم الإدارة ليستخدم خدمات AWS.

- **استخدم حساب مستخدم AWS IAM**

حدد هذا الخيار إذا كان لديك حساب مستخدم IAM لديه الأذونات المطلوبة ويمكنك إدخال معرّف مفتاح والمفتاح السري.

- **معرف مفتاح الوصول**

يكون معرف مفتاح وصول IAM عبارة عن تسلسل من الحروف الأبجدية الرقمية. لقد تلقيت معرف مفتاح عند إنشائك حساب مستخدم IAM.

هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

- **المفتاح السري**

المفتاح السري الذي تلقيته مع معرف مفتاح الوصول عند إنشائك حساب مستخدم IAM.

تظهر حروف المفتاح السري في صورة علامة النجمة. بعد أن تبدأ في إدخال المفتاح السري، سيظهر الزر **إظهار** . انقر مع الاستمرار فوق هذا الزر لتحديد الفترة الزمنية اللازمة لإظهار الحروف التي أدخلتها.

هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

يتم حفظ الاتصال في إعدادات التطبيق. ويمكنك إنشاء مفتاح وصول AWS IAM واحد فقط من خلال تكوين بيئة السحابة. وبالتالي، يمكنك تحديد المزيد من الاتصالات لإدارة قطاعات السحابة الأخرى.

إذا كنت ترغب في تثبيت التطبيقات على المثيلات من خلال Kaspersky Security Center، فيجب عليك التأكد من أن دور IAM الخاص بك (أو مستخدم IAM الذي يرتبط حسابه بالمفتاح الذي تقوم بإدخاله) لديه جميع الأذونات الضرورية.

Azure

إذا قمت بتحديد Azure، فقم بتحديد الإعدادات التالية للاتصال الذي سيتم استخدامه لاستقصاء قطاع السحابة بعد ذلك:

- **اسم الاتصال**

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google".

- **معرف تطبيق Azure**

لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

- **معرف اشتراك Azure**

لقد قمت بإنشاء الاشتراك على مدخل Azure.

- **كلمة مرور تطبيق Azure**

لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

- **اسم حساب تخزين Azure**

لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

- **مفتاح وصول تخزين Azure**

لقد حصلت على كلمة المرور (المفتاح) عند إنشائك لحساب تخزين Azure لاستخدام Kaspersky Security Center.

يكون المفتاح متاحًا في القسم "نظرة عامة على حساب تخزين Azure"، في القسم الفرعي "المفاتيح".

يتم حفظ الاتصال في إعدادات التطبيق.

Google Cloud

إذا قمت بتحديد Google Cloud، فقم بتحديد الإعدادات التالية للاتصال الذي سيتم استخدامه لاستقصاء قطاع السحابة بعد ذلك:

- **اسم الاتصال**

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google."

- **البريد الإلكتروني للعميل**

البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

- **معرف المشروع**

معرف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

- **مفتاح خاص**

المفتاح الخاص هو تسلسل الأحرف التي استلمتها كمفتاح خاص عند تسجيل مشروعك في Google Cloud. قد ترغب في نسخ هذا التسلسل ولصقه لتجنب الأخطاء.

يتم حفظ الاتصال في إعدادات التطبيق.

الخطوة 4. تكوين المزامنة مع السحابة واختيار إجراءات إضافية

في هذه الخطوة، سيبدأ استقصاء قطاع السحابة وسيتم إنشاء مجموعة إدارة خاصة للمثيلات. تم وضع المثيلات التي تم العثور عليها أثناء الاستقصاء في هذه المجموعة. يتم تكوين جدول استقصاء قطاع السحابة (كل 5 دقائق بشكل افتراضي).

سيتم أيضًا إنشاء قاعدة النقل التلقائي **المزامنة مع السحابة**. بالنسبة إلى كل عملية فحص تالية لشبكة السحابة، سيتم نقل الأجهزة الظاهرية التي تم اكتشافها إلى المجموعة الفرعية المقابلة في المجموعة **الأجهزة المُدارة/السحابة**.

في صفحة **المزامنة مع قطاع السحابة**، يمكنك تحديد الإعدادات التالية:

- **مزامنة هيكل مجموعة الإدارة مع قطاع السحابة**

إذا تم تمكين هذا الخيار، سيتم إنشاء مجموعة **السحابة** تلقائيًا في مجموعة **الأجهزة المُدارة** وسيتم بدء اكتشاف أجهزة السحابة. يتم وضع الأجهزة الظاهرية والمثيلات التي تم اكتشافها أثناء كل عملية فحص لشبكة السحابة في مجموعة السحابة. تتوافق بنية المجموعات الفرعية للإدارة الموجودة ضمن هذه المجموعة مع بنية قطاع السحابة الخاص بك (في AWS، لا يتم تمثيل مناطق التوفر ومجموعات تعيين الموضع في البنية؛ في Azure، لا يتم تمثيل الشبكات الفرعية في البنية). توجد الأجهزة التي لم يتم تحديدها كمثيلات في بيئة السحابة في مجموعة **الأجهزة غير المخصصة**. تسمح لك بنية المجموعة هذه باستخدام مهام التثبيت الجماعية، لتثبيت تطبيقات مكافحة الفيروسات على المثيلات وإعداد سياسات مختلفة للمجموعات المختلفة.

إذا تم تعطيل هذا الخيار، فسيتم أيضًا إنشاء مجموعة **السحابة** وبدء تشغيل اكتشاف أجهزة السحابة كذلك؛ إلا إنه لن يتم إنشاء المجموعات الفرعية التي تتوافق مع بنية قطاع السحابة ضمن المجموعة. توجد جميع المثيلات المكتشفة في مجموعة إدارة **السحابة** ولذلك يتم عرضها في قائمة واحدة. إذا كان استخدامك لـ Kaspersky Security Center يتطلب إجراء مزامنة، فيمكنك تعديل خصائص قاعدة **المزامنة مع السحابة** وفرضها. يؤدي فرض هذه القاعدة إلى حدوث تغيير في بنية المجموعات الفرعية في مجموعة السحابة لكي تتطابق مع بنية قطاع السحابة الخاص بك.

يتم تعطيل هذا الخيار افتراضيًا.

- **نشر الحماية**

إذا تم تحديد هذا الخيار، فسينشئ المعالج مهمة لتثبيت تطبيقات الأمان على المثيلات. بعد انتهاء المعالج، سيبدأ تشغيل معالج نشر الحماية تلقائيًا على الأجهزة في قطاعات السحابة الخاصة بك، وستتمكن من تثبيت عميل الشبكة وتطبيقات الأمان على هذه الأجهزة.

يستطيع Kaspersky Security Center القيام بالنشر باستخدام أدواته الأصلية. إذا لم تكن تمتلك أذونات لتثبيت التطبيقات على مثيلات EC2 أو على الأجهزة الظاهرية لـ Azure، يمكنك تكوين مهمة **التثبيت عن بُعد** يدويًا وتحديد حساب يمتلك الأذونات المطلوبة. في هذه الحالة، لن يعمل التثبيت عن بُعد مع الأجهزة التي تم اكتشافها بواسطة AWS API أو Azure. ستعمل هذه المهمة فقط مع الأجهزة المكتشفة باستخدام استقصاء Active Directory، أو استقصاء مجالات Windows، أو استقصاء نطاق IP.

إذا تم إلغاء تحديد هذا الخيار، فلن يبدأ تشغيل معالج نشر الحماية ولن يتم إنشاء مهام تثبيت تطبيقات الأمان على المثيلات. يمكنك تنفيذ كلا الإجراءين يدويًا في وقت لاحق.

بالنسبة إلى Google Cloud، يمكنك فقط إجراء النشر باستخدام الأدوات الأصلية لـ Kaspersky Security Center. إذا قمت بتحديد Google Cloud، فلا يكون الخيار **نشر الحماية** غير متوفر.

الخطوة 5. تكوين Kaspersky Security Network في بيئة السحابة

تحديد الإعدادات لترحيل المعلومات حول عمليات Kaspersky Security Center إلى قاعدة معارف Kaspersky Security Network. حدد أحد الخيارات التالية:

- **أوافق على استخدام شبكة Kaspersky Security Network**

سيقوم Kaspersky Security Center والتطبيقات المدارة المثبتة على الأجهزة العميلة بنقل تفاصيل عملياته تلقائيًا إلى Kaspersky Security Network. تضمن المشاركة في Kaspersky Security Network التحديثات السريعة لقواعد البيانات التي تشتمل على معلومات حول الفيروسات وغيرها من التهديدات، مما يضمن الاستجابة السريعة للتهديدات الأمنية الطارئة.

- **لا أوافق على استخدام شبكة Kaspersky Security Network**

لن يوفر Kaspersky Security Center والتطبيقات المدارة أية معلومات إلى Kaspersky Security Network.

إذا قمت بتحديد هذا الخيار، فسيتم تعطيل استخدام Kaspersky Security Network.

توصي Kaspersky بالمشاركة في Kaspersky Security Network.

الخطوة 6. تكوين إشعارات البريد الإلكتروني في بيئة السحابة

تكوين تسليم الإخطارات المتعلقة بالأحداث المسجلة أثناء تشغيل تطبيقات Kaspersky على الأجهزة الظاهرية العميلة. وستُستخدم هذه الإعدادات كإعدادات افتراضية لسياسات التطبيق.

لتكوين تسليم الإخطارات المتعلقة بالأحداث التي تجري في تطبيقات Kaspersky، استخدم الإعدادات التالية:

- **المستلمين (عناوين البريد الإلكتروني)**

عناوين البريد الإلكتروني للمستخدمين التي ستقوم التطبيقات بإرسال الإخطارات إليها. يمكنك إدخال عنوان واحد أو أكثر، وفي حالة إدخال أكثر من عنوان، فافصل بينها باستخدام فواصل منقوطة.

- **خوادم SMTP**

عنوان أو عناوين خوادم البريد الخاصة بمؤسستك.

في حالة إدخال أكثر من عنوان واحد، افصل بينها باستخدام فواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

- **منفذ خادم SMTP**

رقم منفذ الاتصال الخاص بخادم SMTP. إذا كنت تستخدم عدة خوادم SMTP، فسيتم إنشاء الاتصال بها من خلال منفذ الاتصال المحدد. رقم المنفذ الافتراضي هو 25.

- **استخدام مصادقة ESMTP**

تمكين دعم مصادقة ESMTP. عند تحديد خانة الاختيار الموجودة في الحقول **اسم المستخدم** و**كلمة المرور**، يمكنك تحديد إعدادات مصادقة ESMTP. تكون خانة الاختيار غير محددة بشكل افتراضي.

يمكنك اختبار إعدادات إخطار البريد الإلكتروني بالنقر فوق الزر **إرسال رسالة اختبار**. إذا تم استلام رسالة الاختبار على العناوين المحددة في حقل **المستلمين (عناوين البريد الإلكتروني)**، فيكون قد تم تكوين الإعدادات بصورة صحيحة.

الخطوة 7. إنشاء تكوين أولي لحماية البيئة السحابية

في هذه الخطوة، يقوم Kaspersky Security Center بإنشاء المهام والسياسات تلقائيًا. ستعرض النافذة **تكوين الحماية الأولية** قائمة بالسياسات والمهام التي تم إنشاؤها بواسطة التطبيق.

إذا قمت باستخدام قاعدة بيانات RDS في بيئة السحابة لـ AWS، فيجب عليك تقديم زوج مفاتيح وصول IAM إلى Kaspersky Security Center عند إنشاء مهمة النسخ الاحتياطي لخادم الإدارة. في هذه الحالة، املأ الحقول التالية:

- **اسم مستودع S3**

اسم مستودع S3 الذي قمت بإنشائه للنسخ الاحتياطي.

- **معرف مفتاح الوصول**

لقد تلقيت معرف المفتاح (عبارة عن تسلسل من الحروف الأبجدية الرقمية) عند إنشائك حساب مستخدم IAM للتعامل مع مثيل تخزين مستودع S3.

يكون الحقل متاحًا في حالة تحديد قاعدة بيانات RDS على مستودع S3.

- **المفتاح السري**

المفتاح السري الذي تلقيته مع معرف مفتاح الوصول عند إنشائك حساب مستخدم IAM.

تظهر حروف المفتاح السري في صورة علامة النجمة. بعد أن تبدأ في إدخال المفتاح السري، سيظهر الزر **إظهار** . انقر مع الاستمرار فوق هذا الزر لتحديد الفترة الزمنية اللازمة لإظهار الحروف التي أدخلتها.

هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

إذا قمت باستخدام قاعدة بيانات Azure SQL في بيئة السحابة لـ Azure، فيتوجب عليك توفير معلومات حول خادم Azure SQL Server الخاص بك إلى Kaspersky Security Center عند إنشاء مهمة النسخ الاحتياطي لخادم الإدارة. في هذه الحالة، املأ الحقول التالية:

- **اسم حساب تخزين Azure**

لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

- **معرف اشتراك Azure**

لقد قمت بإنشاء الاشتراك على مدخل Azure.

- **كلمة مرور تطبيق Azure**

لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

- **معرف تطبيق Azure**

لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

- **اسم خادم Azure SQL Server**

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

- **مجموعة مورد خادم Azure SQL Server**

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

- **مفتاح وصول تخزين Azure**

يكون متاحًا في خصائص حساب التخزين الخاص بك، في قسم مفاتيح الوصول. يمكنك استخدام أي من المفاتيح (المفتاح1 أو المفتاح2).

إذا كنت تقوم بنشر خادم الإدارة في Google Cloud، فعليك تحديد مجلد يتم تخزين النسخ الاحتياطية فيه. حدد مجلدًا على جهازك المحلي أو مجلدًا على مثيل جهاز ظاهري.

سيتوفر الزر **التالي** بعد إنشاء جميع السياسات والمهام الضرورية لتكوين الحد الأدنى من الحماية.

إذا لم يكن الجهاز الذي من المفترض أن تتم عليه المهام مرئيًا لخادم الإدارة، فلن تبدأ المهام إلا عندما يصبح الجهاز مرئيًا. إذا قمت بإنشاء مثيل EC2 جديد أو جهاز ظاهري جديد لـ Azure، فقد يستغرق بعض الوقت قبل أن يصبح مرئيًا لخادم الإدارة. إذا كنت ترغب في تثبيت عميل الشبكة وتطبيقات الأمان على جميع الأجهزة المنشأة حديثًا بأسرع وقتٍ ممكن، تأكد من تمكين خيار **تشغيل المهام الفائتة** لمهام **تثبيت التطبيق عن بُعد**. خلافًا لذلك، فإن الجهاز الظاهري/المثيل لن يحصل على عميل الشبكة وتطبيقات الأمان حتى تبدأ المهمة وفقًا للجدول الخاص بها.

الخطوة 8. تحديد الإجراء عندما يتعين إعادة تشغيل نظام التشغيل أثناء التثبيت (لبيئة السحابة)

إذا قمت مسبقًا بتحديد **نشر الحماية**، فيجب عليك أن تختار ما الذي ستفعله عندما يتوجب إعادة تشغيل نظام التشغيل في الجهاز الهدف. إذا لم تقم بتحديد الخيار **نشر الحماية**، فسيتم تخطي هذه الخطوة.

حدد ما إذا كان سيتم إعادة تشغيل المثيلات إذا كان من الضروري إعادة تشغيل نظام التشغيل الخاص بالجهاز أثناء تثبيت التطبيقات:

- **عدم إعادة تشغيل الجهاز**

  في حالة تحديد هذا الخيار، لن يتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

- **إعادة تشغيل الجهاز**

  في حالة تحديد هذا الخيار، فستتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

إذا كنت ترغب في فرض إغلاق جميع التطبيقات في الجلسات المحظورة على المثيلات قبل إعادة التشغيل، فحدد خانة الاختيار **فرض إغلاق التطبيقات في الجلسات المحظورة**. إذا تم إلغاء تحديد خانة الاختيار هذه، سيتعين عليك إغلاق جميع التطبيقات التي تعمل على المثيلات المحجوبة يدويًا.

الخطوة 9. تلقي التحديثات بواسطة خادم الإدارة

في هذه الخطوة، يمكنك ملاحظة تقدم تنزيل التحديثات اللازمة للتشغيل الصحيح لخادم الإدارة. يمكنك النقر فوق زر **التالي** دون انتظار اكتمال التنزيل للمتابعة إلى الصفحة الأخيرة للمعالج.

اكتمل المعالج.

التحقق من التكوين

للتحقق مما إذا كان Kaspersky Security Center 15.1 قد تم تكوينه على النحو الصحيح للعمل في بيئة السحابة:

1. قم بتشغيل Kaspersky Security Center وتأكد من أنه يمكنك الاتصال بخادم الإدارة عبر وحدة تحكم الإدارة.

2. في شجرة وحدة التحكم، حدد **الأجهزة المُدارة/السحابة**.

3. عند عرض أي من المجموعات الفرعية في المجموعة **الأجهزة المُدارة/السحابة**، تأكد من أن علامة التبويب **الأجهزة** تعرض جميع الأجهزة لتلك المجموعة الفرعية.

   إذا لم يتم عرض الأجهزة، فبإمكانك استقصاء قطاعات السحابة المطابقة يدويًا للعثور عليها.

4. تأكد من أن علامة التبويب **السياسات** تحتوي على سياسات نشطة للتطبيقات التالية:

   - عميل شبكة Kaspersky Security Center
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   إذا لم تكن مدرجة، فبإمكانك إنشائها يدويًا.

5. تأكد من أن علامة التبويب **المهام** تسرد المهام التالية:

   - **النسخ الاحتياطي لبيانات خادم الإدارة**
   - **مهمة التحديث لـ Windows Server**
   - **صيانة خادم الإدارة**
   - **تنزيل التحديثات إلى مستودع خادم الإدارة**

- **البحث عن الثغرات الأمنية والتحديثات المطلوبة**
- **تثبيت الحماية لنظام Windows**
- **تثبيت الحماية لنظام Linux**
- **مهمة الفحص السريع لـ Windows Server**
- **فحص سريع**
- **تثبيت التحديثات لنظام التشغيل Linux**

إذا لم تكن مدرجة، فبإمكانك إنشائها يدويًا.

تم تكوين Kaspersky Security Center 15.1 على النحو الصحيح للعمل في بيئة السحابة.

مجموعة جهاز السحابة

يمكنك إدارة أجهزة السحابة من خلال دمجها في مجموعات. في مرحلة التكوين الأولي لـ Kaspersky Security Center، يتم إنشاء مجموعة الإدارة **الأجهزة المُدارة/السحابة** بشكل افتراضي، ويتم وضع أجهزة السحابة التي تم اكتشافها أثناء الاستقصاء في هذه المجموعة.

إذا قمت بتحديد خيار **مزامنة هيكل مجموعة الإدارة مع قطاع السحابة** عند تكوين المزامنة، فإن بنية المجموعات الفرعية في مجموعة الإدارة هذه متطابقة مع بنية مقاطع السحابة الخاصة بك. (ومع ذلك، في AWS، لا يتم تمثيل مناطق التوفر ومجموعات المواضع في الهيكل؛ وفي Microsoft Azure، لا يتم تمثيل الشبكات الفرعية في الهيكل.) يتم حذف المجموعات الفرعية الفارغة داخل المجموعة التي تم اكتشافها تلقائيًا أثناء الاستقصاء.

يمكنك أيضًا إنشاء مجموعات الإدارة يدويًا عن طريق جمع جميع الأجهزة أو أجهزة محددة.

بشكل افتراضي، ترث المجموعة **الأجهزة المُدارة\السحابة** السياسات والمهام من المجموعة **الأجهزة المُدارة**. يمكنك تغيير الإعدادات إذا تم تحديد خانات الاختيار **التحرير متاح** في خصائص إعدادات السياسات والمهام المطابقة.

استقصاء قطاع الشبكة

يتم استلام معلومات حول بنية الشبكة والأجهزة في هذه الشبكة عن طريق خادم الإدارة من خلال استقصاء منتظم لقطاعات السحابة باستخدام أدوات AWS API، وAzure API، وGoogle API. يستخدم Kaspersky Security Center هذه المعلومات لتحديث محتويات مجلدي **الأجهزة غير المخصصة** و**الأجهزة المُدارة**. إذا قمت بتكوين الأجهزة التي سيتم نقلها إلى مجموعات الإدارة تلقائيًا، فسيتم تضمين الأجهزة التي تم اكتشافها في مجموعات الإدارة.

للسماح لخادم الإدارة باستقصاء قطاعات السحابة، يجب أن يكون لديك الحقوق المطابقة المقدمة مع دور IAM أو حساب مستخدم IAM (في AWS) أو مع معرف التطبيق وكلمة المرور (في Azure) أو مع البريد الإلكتروني للعميل على Google ومعرف مشروع Google والمفتاح الخاص.

يمكنك إضافة وحذف الاتصالات، بالإضافة إلى ضبط جدول الاستقصاء لكل قطاع سحابة.

إضافة اتصالات لاستقصاء قطاع السحابة

لإضافة اتصال لاستقصاء قطاع السحابة لقائمة الاتصالات المتاحة:

1. في شجرة وحدة التحكم، حدد العقدة **اكتشاف الأجهزة** ← **السحابة**.

2. في مساحة عمل النافذة، انقر فوق **تكوين الاستقصاء**.

   تفتح نافذة خصائص تحتوي على قائمة بالاتصالات المتاحة لاستقصاء قطاع السحابة.

3. انقر على زر **إضافة**.

   تفتح النافذة **اتصال**.

4. حدد اسم بيئة السحابة للاتصال الذي سيتم استخدامه لإجراء المزيد من الاستقصاءات على قطاع السحابة:

   بيئة السحابة

   قد تكون البيئة التي توجد بها مثيلات EC2 (أو الأجهزة الظاهرية) عبارة عن نظام Amazon Web Services (AWS) أو Microsoft Azure أو Google Cloud.

   إذا حددت AWS، فحدد الإعدادات التالية:

   - **اسم الاتصال**

     أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

     كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

     إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google".

   - **استخدام دور AWS IAM**

     حدد هذا الخيار إذا قمت بالفعل بإنشاء دور IAM لخادم الإدارة ليستخدم خدمات AWS.

   - **استخدم حساب مستخدم AWS IAM**

     حدد هذا الخيار إذا كان لديك حساب مستخدم IAM لديه الأذونات المطلوبة ويمكنك إدخال معرّف مفتاح والمفتاح السري.

   - **معرف مفتاح الوصول**

     يكون معرف مفتاح وصول IAM عبارة عن تسلسل من الحروف الأبجدية الرقمية. لقد تلقيت معرف مفتاح عند إنشائك حساب مستخدم IAM.

     هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

   - **المفتاح السري**

     المفتاح السري الذي تلقيته مع معرف مفتاح الوصول عند إنشائك حساب مستخدم IAM.

     تظهر حروف المفتاح السري في صورة علامة النجمة. بعد أن تبدأ في إدخال المفتاح السري، سيظهر الزر **إظهار** . انقر مع الاستمرار فوق هذا الزر لتحديد الفترة الزمنية اللازمة لإظهار الحروف التي أدخلتها.

     هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

يسمح لك معالج تكوين بيئة السحابة بتحديد مفتاح وصول AWS IAM واحد فقط. وبالتالي، يمكنك تحديد المزيد من الاتصالات لإدارة قطاعات السحابة الأخرى.

إذا حددت Azure، فحدد الإعدادات التالية:

- **اسم الاتصال**

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google".

- **معرف تطبيق Azure**

لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

- **معرف اشتراك Azure**

لقد قمت بإنشاء الاشتراك على مدخل Azure.

- **كلمة مرور تطبيق Azure**

لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

- **اسم حساب تخزين Azure**

لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

- **مفتاح وصول تخزين Azure**

لقد حصلت على كلمة المرور (المفتاح) عند إنشائك لحساب تخزين Azure لاستخدام Kaspersky Security Center.

يكون المفتاح متاحًا في القسم "نظرة عامة على حساب تخزين Azure"، في القسم الفرعي "المفاتيح".

إذا حددت Google Cloud، فحدد الإعدادات التالية:

- **اسم الاتصال**

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google".

- **البريد الإلكتروني للعميل**

البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

- **معرف المشروع**

معرف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

- **مفتاح خاص**

المفتاح الخاص هو تسلسل الأحرف التي استلمتها كمفتاح خاص عند تسجيل مشروعك في Google Cloud. قد ترغب في نسخ هذا التسلسل ولصقه لتجنب الأخطاء.

5. إذا كنت ترغب، حدد **تعيين جدول الاستقصاء** وتغيير الإعدادات الافتراضية.

يتم حفظ الاتصال في إعدادات التطبيق.

بعد استقصاء قطاع السحابة الجديد لأول مرة، تظهر المجموعة الفرعية المقابلة لذلك القطاع في مجموعة الإدارة **الأجهزة المُدارة/السحابة**.

> إذا قمت بتحديد بيانات اعتماد غير صحيحة، فلن تجد أي مثيلات أثناء استقصاء قطاع السحابة، ولن تظهر مجموعة فرعية جديدة في مجموعة الإدارة **الأجهزة المُدارة/السحابة**.

حذف اتصالات خاصة باستقصاء قطاع السحابة

إذا لم يعد من الضروري استقصاء قطاع السحابة المحدد، فيمكنك حذف الاتصال المطابق لذلك القطاع من قائمة الاتصالات المتاحة. يمكنك أيضًا حذف الاتصال، على سبيل المثال، إذا كانت أذونات استقصاء قطاع السحابة قد تم نقلها إلى حساب مستخدم AWS IAM آخر يحتوي على مفتاح آخر.

لحذف اتصال:

1. في شجرة وحدة التحكم، حدد العقدة **اكتشاف الأجهزة** ← **السحابة**.
2. في مساحة عمل النافذة، حدد **تكوين الاستقصاء**.

   تفتح نافذة تحتوي على قائمة بالاتصالات المتاحة لاستقصاء قطاع السحابة.
3. حدد الاتصال الذي تريد حذفه وانقر فوق الزر **حذف** الموجود في الجانب الأيسر من النافذة.
4. في النافذة التي تفتح انقر فوق الزر **موافق** لتأكيد اختيارك.

إذا قمت بحذف الاتصالات من قائمة الاتصالات المتاحة، فسيتم حذف الأجهزة الموجودة في القطاعات المطابقة تلقائيًا من مجموعات الإدارة المطابقة.

تكوين جدول الاستقصاء

يتم تنفيذ استقصاء قطاع السحابة وفقًا لجدول. يمكنك إعداد تكرار الاستقصاء.

يتم إعداد تكرار التحقق من إرسال البيانات تلقائيًا في غضون 5 دقائق في إعدادات تكوين بيئة السحابة. يمكنك تغيير هذه القيمة في أي وقت وإعداد جدول آخر. ومع ذلك، لا يوصى بتكوين الاستقصاء ليتم تشغيله بصورة متكررة بعد أقل من 5 دقائق لأن ذلك قد يؤدي إلى ظهور أخطاء في تشغيل API.

لتكوين جدول استقصاء قطاع السحابة:

1. في شجرة وحدة التحكم، حدد العقدة **اكتشاف الأجهزة** ← **السحابة**.
2. في مساحة العمل، انقر فوق **تكوين الاستقصاء**.

   تفتح نافذة خصائص السحابة.
3. حدد من القائمة الاتصال الذي تريده وانقر فوق الزر **خصائص**.

   تفتح نافذة خصائص الاتصال.
4. في نافذة الخصائص، انقر فوق الرابط **تعيين جدول الاستقصاء**.

   يتم فتح نافذة **الجدول**.

5. حدد الإعدادات التالية:

- **البدء المُجدول**

خيارات جدول الاستقصاء:

- **كل N أيام**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N دقيقة**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل خمس دقائق، بداية من الوقت الحالي للنظام.

- **حسب أيام الأسبوع**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 00:00:6 مساءً.

- **كل شهر في أيام معينة من الأسابيع المحددة**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكلٍ افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 00:00:6 مساءً.

- **تشغيل المهام الفائتة**

إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تمكين هذا الخيار افتراضيًا.

6. انقر فوق **موافق** لحفظ التغييرات.

يتم تكوين جدول الاستقصاء وحفظه.

تثبيت تطبيقات على الأجهزة في بيئة السحابة

يمكنك تثبيت تطبيقات Kaspersky التالية على الأجهزة في بيئة السحابة: Kaspersky Security for Windows Server (للأجهزة التي تعمل بنظام Windows) وKaspersky Endpoint Security for Linux (للأجهزة التي تعمل بنظام Linux).

يجب أن تفي الأجهزة العميلة التي تنوي تثبيت الحماية عليها بمتطلبات تشغيل Kaspersky Security Center في بيئة السحابة. يجب أن تمتلك ترخيصًا ساري المفعول لتثبيت التطبيقات على مثيلات AWS وعلى الأجهزة الظاهرية في Microsoft Azure أو مثيلات الأجهزة الظاهرية لنظام Google.

يدعم Kaspersky Security Center 15.1 السيناريوهات التالية:

- اكتشاف جهاز عميل بواسطة API؛ وإجراء التثبيت بواسطة API. بالنسبة لبيئات السحابة AWS و Azure، يتم دعم هذا السيناريو.
- اكتشاف الجهاز العميل بواسطة استقصاء Active Directory، أو استقصاء مجالات Windows، أو استقصاء نطاق IP؛ وإجراء التثبيت بواسطة Kaspersky Security Center.
- اكتشاف الجهاز العميل بواسطة Google API؛ وإجراء التثبيت بواسطة Kaspersky Security Center. بالنسبة إلى Google Cloud، يتم دعم هذا السيناريو فقط.

طرق تثبيت التطبيقات الأخرى غير مدعومة.

لتثبيت التطبيقات على الأجهزة الظاهرية، استخدم حزم التثبيت.

لإنشاء مهمة لتثبيت التطبيق عن بُعد على مثيلات باستخدام AWS API أو Azure API:

1. في شجرة وحدة التحكم، حدد مجلد **المهام**.
2. انقر على زر **مهمة جديدة**.

   سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.
3. في الصفحة **تحديد نوع المهمة**، حدد **Install application remotely** كنوع المهمة.
4. في الصفحة **تحديد الأجهزة**، حدد الأجهزة ذات الصلة من مجموعة **الأجهزة المُدارة/السحابة**.
5. إذا لم يكن قد تم تثبيت عميل الشبكة على الأجهزة التي تنوي تثبيت التطبيق عليها بعد، فمن الصفحة **تحديد حساب لتشغيل المهمة**، حدد **يُلزم وجود حساب (عميل الشبكة غير مستخدم)** وانقر فوق الزر **إضافة** في الجزء الأيمن من النافذة. حدد أحد الخيارات التالية في القائمة التي ستظهر:

- **حساب السحابة**

حدد هذا الخيار إذا كنت ترغب في تثبيت التطبيقات على المثيلات في AWS وكان لديك مفتاح وصول AWS IAM مع الأذونات المطلوبة، ولكنك لا تتمتع بدور IAM. حدد هذا الخيار أيضًا إذا كنت ترغب في تثبيت تطبيقات على الأجهزة في بيئة Azure.

في النافذة التي تفتح، قم بتزويد Kaspersky Security Center ببيانات الاعتماد التي تمنحك حقوق تثبيت التطبيقات على الأجهزة ذات الصلة.

حدد بيئة السحابة: AWS أو Azure.

في حقل **اسم الحساب**، قم بإدخال اسم لبيانات الاعتماد هذه. سيتم عرض هذا الاسم في قائمة الحسابات لتشغيل المهمة.

إذا قمت بتحديد AWS، فقم بإدخال بيانات الاعتماد لحساب مستخدم IAM الذي يمتلك حقوق تثبيت التطبيقات على الأجهزة المحددة، في حقول **معرف مفتاح الوصول** و**المفتاح السري**.

إذا قمت بتحديد Azure، فقم بإدخال بيانات الاعتماد لحساب Azure الذي يمتلك حقوق تثبيت التطبيقات على الأجهزة المحددة، في حقول **معرف اشتراك Azure** و**كلمة المرور لتطبيق Azure**.

إذا قمت بتحديد بيانات اعتماد غير صحيحة، فستنتهي مهمة التثبيت عن بُعد مع وجود خطأ على الأجهزة التي تمت جدولتها عليها.

- **الحساب**

بالنسبة للمثيلات التي تعمل بنظام Windows، حدد هذا الخيار في حالة لم تكن تعتزم تثبيت التطبيق باستخدام أدوات AWS أو Azure API. في هذه الحالة، تأكد من تحقيق الأجهزة في قطاع السحابة الخاص بك للشروط اللازمة. يقوم Kaspersky Security Center بتثبيت التطبيقات بنفسه، دون استخدام AWS API أو Azure API.

إذا قمت بتحديد بيانات غير صحيحة، ستنتهي مهمة التثبيت عن بُعد مع وجود خطأ على الأجهزة التي تمت جدولتها عليها.

- **دور IAM**

حدد هذا الخيار إذا كنت ترغب في تثبيت التطبيقات على المثيلات في بيئة AWS وكان لديك دور IAM مع الحقوق المطلوبة.

إذا قمت بتحديد هذا الخيار، ولم يكن لديك دور IAM مع الحقوق المطلوبة، ستنتهي مهمة التثبيت عن بُعد مع وجود خطأ على الأجهزة التي تمت جدولتها عليها.

- **شهادة SSH**

بالنسبة للمثيلات التي تعمل على نظام Linux، حدد هذا الخيار إذا كنت لا تعتزم تثبيت التطبيق باستخدام أدوات AWS API أو Azure API. في هذه الحالة، تأكد من تحقيق الأجهزة في قطاع السحابة الخاص بك للشروط اللازمة. يقوم Kaspersky Security Center بتثبيت التطبيقات بنفسه، دون استخدام AWS API أو Azure API.

لتحديد المفتاح الخاص لشهادة SSH، يمكنك إنشاؤه باستخدام الأداة المساعدة ssh-keygen. لاحظ أن Kaspersky Security Center يدعم تنسيق PEM للمفاتيح الخاصة، لكن الأداة المساعدة ssh-keygen تنشئ مفاتيح SSH بتنسيق OPENSSH افتراضيًا. تنسيق OPENSSH غير مدعوم من قبل Kaspersky Security Center. ولإنشاء مفتاح خاص بتنسيق PEM المدعوم، أضف الخيار -m PEM في الأمر -m PEM. فمثلاً:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<البريد الالكتروني للمستخدم>"
```

يمكنك توفير العديد من بيانات الاعتماد عن طريق النقر فوق الزر **إضافة** لكل واحدة. إذا كانت قطاعات السحابة المختلفة تتطلب بيانات اعتماد مختلفة، قم بتوفير بيانات الاعتماد لجميع القطاعات.

بعد انتهاء المعالج، تظهر مهمة التثبيت عن بُعد للتطبيق في قائمة المهام في مساحة عمل مجلد **المهام**.

في Microsoft Azure، قد تؤدي عملية التثبيت عن بُعد لتطبيقات الأمان على جهاز ظاهري إلى حذف Custom Script Extension المثبّت على هذا الجهاز الظاهري.

عرض خصائص أجهزة السحابة

لعرض خصائص جهاز السحابة:

1. في شجرة وحدة التحكم، في عقدة السحابة **اكتشاف الأجهزة** ← ، حدد العقدة الفرعية التي تتوافق مع المجموعة التي يقع فيها المثيل ذو الصلة.

   إذا لم تكن لديك دراية بالمجموعة التي يقع فيها الجهاز الظاهري ذو الصلة، فاستخدم ميزة البحث:

   a. انقر بزر الماوس الأيمن فوق اسم ملف عقد السحابة **الأجهزة المُدارة** ← ، ثم حدد **بحث** في قائمة السياق.

   b. في النافذة التي تفتح، قم بتنفيذ البحث.

   إذا كان الجهاز الموجود يستوفي المعايير التي حددتها، سيظهر اسمه وتفاصيله في الجزء السفلي من النافذة.

2. انقر بزر الماوس الأيمن فوق اسم العقدة ذات الصلة. في قائمة السياق، حدد **خصائص**.

   في النافذة التي تفتح، تظهر خصائص الكائن.

   يحتوي قسم **معلومات النظام** ← معلومات عامة عن النظام على الخصائص المحددة للأجهزة في بيئة السحابة:

- **تم اكتشاف الجهاز باستخدام API** (**AWS** أو **Azure** أو **Google Cloud**؛ إذا تعذر اكتشاف الجهاز باستخدام أدوات API، فسيتم عرض القيمة **لا**).
- **منطقة السحابة**.
- **Cloud VPC** (لأجهزة AWS وGoogle Cloud فقط).
- **منطقة توفر السحابة** (لأجهزة AWS وGoogle Cloud فقط).
- **شبكة السحابة الفرعية**.
- **مجموعة وضع السحابة** (يتم عرض هذه الوحدة فقط إذا كان المثيل ينتمي إلى مجموعة الموضع؛ وإلا فلن يتم عرضه).

يمكنك النقر فوق الزر **تصدير إلى ملف** لتصدير هذه المعلومات إلى ملف .csv أو .txt.

المزامنة مع السحابة

أثناء عملية تكوين بيئة السحابة، سيتم إنشاء القاعدة المزامنة مع السحابة تلقائيًا. تسمح لك هذه القاعدة بنقل المثيلات التي تم اكتشافها في كل استطلاع تلقائيًا، من المجموعة **الأجهزة غير المخصصة** إلى المجموعة **الأجهزة المُدارة/السحابة**، لتوفير هذه المثيلات للإدارة المركزية. بشكل افتراضي، ستكون القاعدة نشطة بعد إنشائها. يمكنك تعطيل القاعدة أو تعديلها أو فرضها في أي وقت.

لتحرير خصائص قاعدة المزامنة مع السحابة و/أو فرض القاعدة:

1. في شجرة وحدة التحكم، انقر بزر الماوس الأيمن فوق اسم العقدة **اكتشاف الأجهزة**.

2. في قائمة السياق، حدد **خصائص**.

3. من نافذة **الخصائص** التي تفتح، في جزء **الأقسام**، حدد **نقل الأجهزة**.

4. في قائمة قواعد نقل الجهاز في مساحة العمل، حدد **المزامنة مع السحابة** وانقر فوق الزر **خصائص** في الجزء السفلي من النافذة.

   تفتح نافذة خصائص القاعدة.

5. إذا لزم الأمر، حدد الإعدادات التالية في مجموعة إعدادات **قطاعات السحابة**:

- **الجهاز موجود في قطاع السحابة**

لا تنطبق القاعدة إلا على الأجهزة الموجودة في قطاع السحابة المحدد. خلافًا لذلك، فستطبق القاعدة على جميع الأجهزة التي تم اكتشافها.

يتم تحديد هذا الخيار افتراضيًا.

- **تضمين كائنات فرعية**

تطبق القاعدة على جميع الأجهزة الموجودة في القطاع المحدد وفي جميع الأقسام الفرعية السحابية المتداخلة. خلافًا لذلك، فستطبق القاعدة فقط على الأجهزة الموجودة قطاع الجذر.

يتم تحديد هذا الخيار افتراضيًا.

- **نقل الأجهزة من الكائنات المتداخلة إلى المجموعات الفرعية المقابلة**

إذا تم تمكين هذا الخيار، فستنتقل الأجهزة من الكائنات المتداخلة تلقائيًا إلى المجموعات الفرعية التي تتوافق مع بنيتها.

إذا تم تعطيل هذا الخيار، سيتم نقل الأجهزة من الكائنات المتداخلة تلقائيًا إلى جذر المجموعة الفرعية للسحابة دون أي تفريع لاحق.

يتم تمكين هذا الخيار افتراضيًا.

- **إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثًا**

إذا تم تمكين هذا الخيار، في حالة عدم اشتمال بنية مجموعة **الأجهزة المُدارة/السحابة** على مجموعات فرعية تتوافق مع القسم الذي يحتوي على الجهاز، فسيقوم Kaspersky Security Center بإنشاء هذه المجموعات الفرعية. على سبيل المثال، إذا تم اكتشاف شبكة فرعية جديدة أثناء اكتشاف الأجهزة، سيتم إنشاء مجموعة جديدة تحمل نفس الاسم ضمن المجموعة **الأجهزة المدارة/السحابة**.

إذا تم تعطيل هذا الخيار، فلن يقوم Kaspersky Security Center بإنشاء أي مجموعات فرعية جديدة. على سبيل المثال، إذا تم اكتشاف شبكة فرعية جديدة أثناء استقصاء الشبكة، فلن يتم إنشاء مجموعة جديدة تحمل نفس الاسم ضمن المجموعة **الأجهزة المُدارة/السحابة**، وسيتم نقل الأجهزة الموجودة في هذه الشبكة الفرعية إلى المجموعة **الأجهزة المُدارة/السحابة**.

يتم تمكين هذا الخيار افتراضيًا.

- **حذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابة**

إذا تم تمكين هذا الخيار، فسيحذف التطبيق من مجموعة السحابة جميع المجموعات الفرعية التي لا تطابق أي من كائنات السحابة الموجودة.

إذا تم تعطيل هذا الخيار، فسيتم الاحتفاظ بالمجموعات الفرعية التي لا تطابق أي من كائنات السحابة الموجودة.

يتم تمكين هذا الخيار افتراضيًا.

إذا قمت بتمكين الخيار **المزامنة مع السحابة** عند تشغيل تكوين بيئة السحابة، يتم إنشاء قاعدة المزامنة مع السحابة مع تحديد خانات الاختيار **إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثًا** و**حذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابة**.

إذا لم تقم بتمكين الخيار **المزامنة مع السحابة**، فسيتم إنشاء قاعدة المزامنة مع السحابة بحيث تكون هذه الخيارات معطلة (تم إلغاء تحديدها). إذا كان استخدامك لـ Kaspersky Security Center يتطلب أن تتوافق بنية المجموعات الفرعية في المجموعة الفرعية **الأجهزة المُدارة\السحابة** مع بنية قطاعات السحابة، فقم بتمكين الخيارين **إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثًا** و**حذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابة** في خصائص القاعدة، ثم قم بفرض القاعدة.

6. في القائمة المنسدلة **تم اكتشاف جهاز يستخدم API**، حدد واحدة من القيم التالية:
   - **AWS**. يتم اكتشاف الجهاز باستخدام AWS API، أي أن الجهاز يوجد بالفعل في بيئة سحابة AWS.
   - **Azure**. يتم اكتشاف الجهاز باستخدام Azure API، أي أن الجهاز يوجد بالفعل في بيئة سحابة Azure.
   - **Google Cloud**. يتم اكتشاف الجهاز باستخدام Google API، أي أن الجهاز موجود بالفعل في بيئة Google cloud.
   - **لا**. لا يمكن اكتشاف الجهاز باستخدام AWS أو Azure أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة لكن لا يمكن اكتشافه باستخدام واجهة برمجة التطبيق (API).
7. **لا توجد قيمة**. هذا الشرط لا ينطبق. إن لزم الأمر، قم بإعداد خصائص قاعدة أخرى في أقسام أخرى.
8. إذا لزم الأمر، قم بفرض القاعدة عن طريق النقر فوق الزر **فرض** الموجود في الجزء السفلي من النافذة.

   يبدأ معالج تنفيذ القاعدة. اتبع إرشادات المعالج. عند انتهاء المعالج، سيتم تشغيل القاعدة وستتطابق بنية المجموعات الفرعية الموجودة في المجموعة الفرعية **الأجهزة المُدارة\السحابة** مع بنية قطاعات السحابة الخاصة بك.
9. انقر على زر **موافق**.

   يتم إعداد الخصائص وحفظها.

لتعطيل قاعدة المزامنة مع السحابة:

1. في شجرة وحدة التحكم، انقر بزر الماوس الأيمن فوق اسم العقدة **اكتشاف الأجهزة**.
2. في قائمة السياق، حدد **خصائص**.
3. من نافذة **الخصائص** التي تفتح، في جزء **الأقسام**، حدد **نقل الأجهزة**.
4. في قائمة قواعد نقل الجهاز في مساحة العمل، قم بتعطيل (إلغاء تحديد) خيار **المزامنة مع السحابة** وانقر فوق **موافق**.

   يتم تعطيل القاعدة ولن يتم تطبيقها بعد ذلك.

نشر Kaspersky Security Center في Yandex.Cloud

يمكنك نشر Kaspersky Security Center في Yandex.Cloud. لا يتوفر إلا وضع الدفع لكل استخدام؛ قواعد بيانات السحابة غير مدعومة.

في Yandex.Cloud، تتوفر طرق النشر التالية لتطبيقات الأمان:

- من خلال الوسائل الأصلية لـ Kaspersky Security Center، أي عبر مهمة التثبيت عن بُعد (لا يمكن نشر برامج الأمان إلا إذا كان خادم الإدارة والأجهزة الظاهرية المطلوب حمايتها موجودة في نفس قطاع الشبكة)
- عبر نشر البرامج النصية

لنشر Kaspersky Security Center في Yandex.Cloud، يجب أن يكون لديك حساب خدمة في Yandex.Cloud. يجب أن تمنح هذا الحساب إذن marketplace.meteringAgent وربط هذا الحساب بالجهاز الظاهري (يرجى الرجوع إلى https://cloud.yandex.com/en/ للحصول على التفاصيل).

الملاحق

يقدّم هذا القسم معلومات مرجعية وحقائق إضافية تخص استخدام Kaspersky Security Center.

الميزات المتقدمة

يصف هذا القسم مجموعة من الخيارات الإضافية لـ Kaspersky Security Center المصمم لتوسيع وظائف الإدارة المركزية للتطبيقات على الأجهزة.

التشغيل التلقائي لعمليات Kaspersky Security Center. الأداة المساعدة klakaut

يمكنك إجراء تشغيل تلقائي لعمليات Kaspersky Security Center باستخدام الأداة المساعدة klakaut. توجد الأداة المساعدة klakaut ونظام التعليمات الخاص بها في مجلد تثبيت Kaspersky Security Center.

الأدوات المخصصة

يتيح لك Kaspersky Security Center إنشاء قائمة أدوات مخصصة (يُشار إليها أيضًا فيما بعد باسم الأدوات) – أي التطبيقات المفعلة للجهاز العميل في وحدة تحكم الإدارة باستخدام مجموعة **أدوات مخصصة** لقائمة السياق. وسيتم ربط كل أداة في القائمة بأمر قائمة منفصل، تستخدمه وحدة تحكم الإدارة لبدء تشغيل التطبيق المتوافق مع تلك الأداة.

ويبدأ التطبيق في محطة عمل المسؤول. ويمكن أن يقبل التطبيق سمات الجهاز العميل البعيد كخيارات سطر الأوامر (اسم NetBIOS، أو اسم DNS، أو عنوان IP). ويمكن إنشاء الاتصال بالجهاز البعيد باستخدام الاتصال النفقي.

وبشكل افتراضي، تحتوي قائمة الأدوات المخصصة على برامج الخدمة التالية لكل جهاز عميل:

- **تشخيصات عن بعد** هو أداة لتشخيص Kaspersky Security Center عن بُعد.
- **سطح المكتب البعيد** هو مكون Microsoft Windows القياسي المُسمىRemote Desktop Connection.
- **إدارة الكمبيوتر** هو مكون Microsoft Windows قياسي.

لإضافة أداة مخصصة أو إزالتها أو تحرير إعداداتها:

من قائمة سياق الجهاز العميل، حدد **أدوات مخصصة** ← **تكوين أدوات مخصصة**.

تفتح نافذة **أدوات مخصصة**. في هذه النافذة ، يمكنك إضافة أدوات مخصصة أو تعديل إعداداتها باستخدام الزرين **إضافة** و**تعديل**. لإزالة أداة مخصصة ، انقر فوق زر الإزالة الذي يحمل علامة زائد الأحمر (✕).

وضع استنساخ قرص عميل الشبكة

يُعد استنساخ محرك الأقراص الثابتة لجهاز مرجعي طريقة شائعة لتثبيت البرامج على الأجهزة الجديدة. إذا كان عميل الشبكة يعمل في الوضع القياسي على محرك الأقراص الثابت للجهاز المرجعي، فستنشأ المشكلات التالية:

بعد نشر صورة القرص المرجعي مع عميل الشبكة على الأجهزة الجديدة، يتم عرضها في وحدة تحكم الإدارة برمز واحد. تنشأ هذه المشكلة حيث تتسبب عملية الاستنساخ في احتفاظ الأجهزة الجديدة ببيانات داخلية متطابقة، مما يتيح لخادم الإدارة ربط الجهاز بأحد الرموز في وحدة تحكم الإدارة.

يتيح لك وضع نسخ قرص عميل الشبكة تجنب المشكلات باستخدام عرض غير صحيح للأجهزة الجديدة في وحدة تحكم الإدارة بعد النسخ. استخدم هذا الوضع عند نشر برنامج (باستخدام عميل الشبكة) على الأجهزة الجديدة عن طريق نسخ القرص.

في وضع نسخ القرص، يستمر تشغيل عميل الشبكة، ولكن دون الاتصال بخادم الإدارة. عند الخروج من وضع الاستنساخ، يحذف عميل الشبكة البيانات الداخلية، مما يؤدي إلى ربط خادم الإدارة العديد من الأجهزة برمز واحد في وحدة تحكم الإدارة. بمجرد اكتمال استنساخ صورة الجهاز المرجعي، يتم عرض الأجهزة الجديدة في وحدة تحكم الإدارة بشكل صحيح (تحت رموز فردية).

سيناريو استخدام وضع نسخ قرص عميل الشبكة

1. يقوم المسؤول بتثبيت عميل الشبكة على الجهاز المرجعي.
2. يتحقق المسؤول من اتصال عميل الشبكة بخادم الإدارة باستخدام الأداة المساعدة klnagchk.
3. يقوم المسؤول بتمكين وضع استنساخ قرص عميل الشبكة.
4. يقوم المسؤول بتثبيت البرامج والتصحيحات على الجهاز، وإعادة تشغيله حسب الاقتضاء.
5. يستنسخ المسؤول محرك الأقراص الثابتة للجهاز المرجعي على أي عدد من الأجهزة.
6. ويجب أن تفي كل نسخة مستنسخة بالشروط التالية:
   a. يجب تغيير اسم الجهاز.
   b. يجب إعادة تشغيل الجهاز.
   c. يجب تعطيل وضع استنساخ القرص.

تمكين وضع استنساخ القرص وتعطيله باستخدام الأداة klmover

لتمكين أو تعطيل وضع استنساخ قرص عميل الشبكة:

1. قم بتشغيل أداة klmover المساعدة على الجهاز المثبت عليه عميل الشبكة والذي تريد نسخه.
   توجد أداة klmover في مجلد تثبيت عميل الشبكة.
2. لتمكين وضع نسخ القرص، أدخل الأمر التالي في موجه أوامر Windows:
   ```
   klmover -cloningmode 1
   ```
   يتم تبديل عميل الشبكة إلى وضع نسخ القرص.
3. لطلب الحالة الحالية لوضع نسخ القرص، أدخل الأمر التالي في موجه الأوامر:
   ```
   klmover -cloningmode
   ```
   تُظهر نافذة الأداة المساعدة إذا ما تم تمكين وضع نسخ القرص أم تعطيله.
4. لتعطيل وضع استنساخ القرص، أدخل الأمر التالي في سطر أوامر الأداة:
   ```
   klmover -cloningmode 0
   ```

إعداد جهاز مرجعي مع تثبيت وكلاء الشبكة لإنشاء صورة لنظام التشغيل

قد ترغب في إنشاء صورة لنظام تشغيل جهاز مرجعي مزود بعميل شبكة مثبت، ثم نشر الصورة على الأجهزة المتصلة بالشبكة. في هذه الحالة، تقوم بإنشاء صورة لنظام تشغيل جهاز مرجعي، الذي لم يبدأ تشغيل عميل الشبكة عليه بعد. إذا قمت ببدء تشغيل عميل الشبكة على جهاز مرجعي قبل إنشاء صورة لنظام التشغيل، فسيشكل تعريف خادم الإدارة للأجهزة، التي تم نشرها من صورة نظام التشغيل للجهاز المرجعي، مشكلة.

لتحضير الجهاز المرجعي لإنشاء صورة لنظام التشغيل:

1. تأكد من تثبيت نظام التشغيل Windows على الجهاز المرجعي وقم بتثبيت البرامج الأخرى التي تحتاجها على هذا الجهاز.

2. على الجهاز المرجعي، في إعدادات Windows لعمليات الاتصال بالشبكة، افصل الجهاز المرجعي عن الشبكة التي تم تثبيت Kaspersky Security Center من خلالها.

3. على الجهاز المرجعي، أبدأ في التثبيت المحلي لعميل الشبكة باستخدام ملف (setup.exe).

   يبدأ معالج إعداد عميل شبكة Kaspersky Security Center. اتبع إرشادات المعالج.

4. في صفحة **خادم الإدارة** للمعالج، حدد عنوان IP الخاص بخادم الإدارة.

   إذا كنت لا تعرف العنوان الصحيح لخادم الإدارة، أدخل المضيف المحلي. ويمكنك تغيير عنوان IP لاحقًا باستخدام الأداة المساعدة klmover مع مفتاح `address-`.

5. في صفحة **بدء التطبيق** للمعالج، قم بتعطيل خيار **بدء التطبيق أثناء التثبيت**.

6. عند اكتمال تثبيت عميل الشبكة، لا تقم بإعادة تشغيل الجهاز قبل إنشاء صورة لنظام التشغيل.

   إذا قمت بإعادة تشغيل الجهاز، فسيتعين عليك تكرار عملية تحضير جهاز مرجعي برمتها لإنشاء صورة لنظام التشغيل.

7. على الجهاز المرجعي، في سطر الأوامر، قم بتشغيل الأداة المساعدة sysprep وتنفيذ الأمر التالي: `sysprep.exe /generalize /oobe /shutdown`.

   الجهاز المرجعي جاهز لـ إنشاء صورة نظام التشغيل.

تكوين استلام الرسائل من مراقبة سلامة الملف

ترسل التطبيقات المُدارة مثل Kaspersky Security for Windows Server أو Kaspersky Security for Virtualization Light Agent رسائل من مراقبة سلامة الملف إلى Kaspersky Security Center. كما يسمح لك Kaspersky Security Center بمراقبة أي تغييرات تطرأ على مكونات النظام ذات الأهمية الشديدة (مثل خوادم الويب وماكينات الصرف الآلي) والاستجابة السريعة لانتهاكات تكامل هذه الأنظمة. لهذه الأغراض، يمكنك استلام رسائل من مكون مراقبة سلامة الملف. لا يسمح لك مكون مراقبة سلامة الملف بمراقبة نظام الملفات على الجهاز فحسب، بل يسمح لك أيضًا بمراقبة خلايا التسجيل الخاصة به وحالة جدار الحماية وحالة الأجهزة المتصلة.

يجب عليك تكوين Kaspersky Security Center لتلقي رسائل من مكون مراقبة سلامة الملف دون استخدام Kaspersky Security for Windows Server أو Kaspersky Security for Virtualization Light Agent.

لتكوين استلام الرسائل من مراقبة سلامة الملف:

1. افتح سجل النظام الخاص بالجهاز المثبت عليه خادم الإدارة (على سبيل المثال: محليًا، باستخدام الأمر regedit من القائمة **بدء** ← **تشغيل**).

2. انتقل إلى الخلية التالية:

   - لأنظمة 32 بت:

     ServerFlags\1.0.0.0\1093\34\Components\KasperskyLab\SOFTWARE\HKEY_LOCAL_MACHINE

- لأنظمة 64 بت:

rFlags\1.0.0.0\1093\34\Components\KasperskyLab\Wow6432Node\SOFTWARE\HKEY_LOCAL_MACHINE

3. إنشاء مفاتيح:

- قم بإنشاء المفتاح KLSRV_EVP_FIM_PERIOD_SEC لتحديد الفترة الزمنية لحساب عدد الأحداث التي تمت معالجتها. حدد الإعدادات التالية:

  a. حدد KLSRV_EVP_FIM_PERIOD_SEC كاسم المفتاح.

  b. حدد DWORD كنوع المفتاح.

  c. حدد نطاق قيم للفاصل الزمني من 43 200 إلى 172 800 ثانية. بشكل افتراضي، يكون الفاصل الزمني هو 86 400 ثانية.

- قم بإنشاء المفتاح KLSRV_EVP_FIM_LIMIT لتقييد عدد الأحداث المستلمة للفاصل الزمني المحدد. حدد الإعدادات التالية:

  a. حدد KLSRV_EVP_FIM_LIMIT كاسم المفتاح.

  b. حدد DWORD كنوع المفتاح.

  c. حدد نطاق لقيم الأحداث المستلمة من 2 000 إلى 50 000. العدد الافتراضي للأحداث هو 20 000.

- ثم بإنشاء المفتاح KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC لحساب الأحداث بدقة وصولاً إلى الفاصل الزمني المحدد. حدد الإعدادات التالية:

  a. حدد KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC كاسم المفتاح.

  b. حدد DWORD كنوع المفتاح.

  c. حدد نطاق قيم من 120 إلى 600 ثانية. الفاصل الزمني الافتراضي هو 300 ثانية.

- قم بإنشاء المفتاح KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC وبناءً عليه، بعد مرور الفترة الزمنية المحددة، يمكن للتطبيق التحقق مما إذا كان عدد الأحداث التي تمت معالجتها على مدار الفاصل الزمني قد أصبح أقل من الحد المحدد. يتم تنفيذ عملية التحقق هذه عند الوصول إلى حد استلام الأحداث. إذا تم استيفاء هذا الشرط، يستأنف التطبيق حفظ الأحداث على قاعدة البيانات. حدد الإعدادات التالية:

  a. حدد KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC كاسم المفتاح.

  b. حدد DWORD كنوع المفتاح.

  c. حدد نطاق قيم من 600 إلى 3 600 ثانية. الفاصل الزمني الافتراضي هو 1 800 ثانية.

إذا لم يتم إنشاء المفاتيح، فسيتم استخدام القيم الافتراضية.

4. قم بإعادة تشغيل خدمة خادم الإدارة.

سيتم تكوين الحدود على استلام الأحداث من مكون مراقبة سلامة الملف. يمكنك عرض نتائج مكون مراقبة تكامل الملفات في التقارير المسماة **أكثر 10 أجهزة يتم تشغيلها بشكل متكرر على الأجهزة المزودة بقواعد مراقبة سلامة الملف/مراقبة نظام التكامل** و**أكثر 10 أجهزة يتم تشغيلها بشكل متكرر مزودة بقواعد مراقبة سلامة الملف/مراقبة نظام التكامل**.

صيانة خادم الإدارة

تتيح لك صيانة خادم الإدارة إخلاء مساحة في مجلد خادم الإدارة وتقليل حجم قاعدة البيانات عن طريق حذف الكائنات التي لم تعد هناك حاجة إليها. ويساعدك هذا على تحسين الأداء والموثوقية التشغيلية للتطبيق. ونوصي بإجراء الصيانة على خادم الإدارة أسبوعيًا على الأقل.

يتم إجراء صيانة خادم الإدارة باستخدام المهمة المخصصة. يجري التطبيق الإجراءات التالية عند صيانة خادم الإدارة:

- يحذف المجلدات والملفات غير الضرورية من مجلد التخزين.
- يحذف السجلات غير الضرورية من الجداول (المعروفة أيضًا باسم "المؤشرات المتدلية").
- يمسح ذاكرة التخزين المؤقت.
- يحافظ على قاعدة البيانات (إذا كنت تستخدم SQL Server أو PostgreSQL كقاعدة بيانات DBMS):
  - يتحقق من عدم وجود أخطاء في قاعدة البيانات (متاح فقط لأجل SQL Server).
  - إعادة تنظيم فهارس قاعدة البيانات.
  - تحديث إحصائيات قاعدة البيانات.
  - تقليص قاعدة البيانات (إذا لزم الأمر).

لإنشاء مهمة صيانة خادم الإدارة:

1. في شجرة وحدة التحكم، حدد قسم خادم الإدارة الذي تريد إنشاء مهمة صيانة خادم الإدارة له.
2. حدد مجلد **المهام**.
3. في مساحة عمل المجلد **المهام**، انقر على الزر **مهمة جديدة**.
   يبدأ معالج المهمة الجديدة.
4. في النافذة **تحديد نوع المهمة** في المعالج، حدد **صيانة خادم الإدارة** كنوع المهمة، ثم انقر فوق **التالي**.
5. إذا كان يتعين عليك تقليص قاعدة بيانات خادم الإدارة أثناء الصيانة، في نافذة **إعدادات** في المعالج، حدد خانة الاختيار **تقليص قاعدة البيانات**.
6. اتبع بقية تعليمات المعالج.

يتم عرض المهمة التي تم إنشاؤها حديثًا في قائمة المهام في مساحة عمل المجلد **المهام**. يمكن تشغيل مهمة صيانة خادم الإدارة واحدة فقط لخادم إدارة واحد. في حالة إنشاء مهمة صيانة خادم الإدارة بالفعل لخادم الإدارة، لا يمكن إنشاء مهمة صيانة خادم الإدارة جديدة.

الوصول إلى خوادم DNS العامة

إذا لم يكن الوصول إلى خوادم Kaspersky باستخدام نظام DNS ممكنًا، يستطيع Kaspersky Security Center استخدام 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 إلى خوادم DNS هذه على عناوين المجال وعنوان IP العام لخادم الإدارة، لأن التطبيق ينشئ اتصال TCP / UDP بخادم DNS. إذا كان Kaspersky Security Center يستخدم خادم DNS عام، فإن معالجة البيانات تخضع لسياسة الخصوصية الخاصة بالخدمة ذات الصلة.

لتكوين استخدام DNS العام باستخدام الأداة المساعدة klscflag:

1. قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky\Kaspersky Security Center\Lab.

2. لتعطيل استخدام DNS العام، قم بتشغيل الأمر التالي:

```
s Transport -n ForceUseSystemDNS -t d -v 1- "core/.independent." klscflag -fset -pv
```

3. لتمكين استخدام DNS العام، قم بتشغيل الأمر التالي:

```
s Transport -n ForceUseSystemDNS -t d -v 0- "core/.independent." klscflag -fset -pv
```

نافذة طريقة إخطار المستخدم

في النافذة **طريقة إخطار المستخدم**، يمكنك تكوين إخطار المستخدم المتعلق بتثبيت الشهادة على الجهاز المحمول:

- **إظهار رمز الاستجابة السريعة في المعالج**. إذا حددت هذا الخيار، سيتم عرض رابط لحزمة التثبيت في الخطوة الأخيرة من معالج اتصال جهاز المحمول جديد.
- **إرسال رمز الاستجابة السريعة إلى المستخدم**. إذا حددت هذا الخيار، فيمكنك تحديد إعدادات إخطار المستخدم حول اتصال جهاز ما.

في المجموعة **بواسطة البريد الإلكتروني** من الإعدادات، يمكنك تكوين إخطار المستخدم بشأن تثبيت شهادة جديدة على جهازه المحمول باستخدام رسائل البريد الإلكتروني. لا تتوفر طريقة الإخطار هذه إلا في حالة تمكين خادم SMTP.

في المجموعة **عبر رسالة SMS** من الإعدادات، يمكنك تكوين إخطار المستخدم بشأن تثبيت الشهادة على جهازه المحمول باستخدام رسائل SMS. لا تتوفر طريقة الإخطار هذه إلا في حالة تمكين إخطارات رسائل SMS.

انقر فوق الرابط **تحرير رسالة** في مجموعات الإعدادات **بواسطة البريد الإلكتروني** و**عبر رسالة SMS** لعرض رسالة الإخطار وتحريرها، إذا لزم الأمر.

نافذة تحديد الجهاز

اختر تحديدًا من قائمة **تحديد الجهاز**. تحتوي القائمة على التحديدات المحددة مسبقًا والتحديدات التي أنشأها المستخدم.

يمكنك عرض تفاصيل تحديدات الأجهزة في مساحة العمل الخاصة بالقسم **تحديدات الأجهزة**.

نافذة تحديد اسم الكائن الجديد

في النافذة، حدد اسم الكائن الذي تم إنشاؤه حديثًا. لا يمكن أن يحتوي اسم على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

ميزات استخدام واجهة الإدارة

يصف هذا القسم الإجراءات التي يمكن أن تعمل في النافذة الرئيسية لـ Kaspersky Security Center.

شجرة وحدة التحكم

تم تصميم شجرة وحدة التحكم (انظر الشكل أدناه) لعرض التسلسل الهرمي لخوادم الإدارة على شبكة الشركة، وهيكل مجموعات الإدارة الخاصة بها، والكائنات الأخرى للتطبيق، مثل **المستودعات** أو مجلدات **إدارة التطبيق**. يمكن أن تحتوي مساحة الاسم الخاصة بـ Kaspersky Security Center على عدة أجزاء منها أسماء الخوادم المقابلة لخوادم الإدارة المُثبتة والمضمنة في التسلسل الهرمي.

شجرة وحدة التحكم

عقدة خادم الإدارة

جزء **خادم الإدارة – <اسم الجهاز>** هو حاوية تُظهر التنظيم الهيكلي لخادم الإدارة المحدد.

تحتوي مساحة العمل الخاصة بجزء **خادم الإدارة** على معلومات موجزة حول الحالة الحالية للتطبيق والأجهزة المُدارة من خلال خادم الإدارة. يتم توزيع المعلومات في مساحة العمل بين علامات تبويب مختلفة:

- **المراقبة**. تعرض معلومات حول تشغيل التطبيق والحالة الحالية لأجهزة العميل في وضع الوقت الحقيقي. يتم تمييز الرسائل المهمة للمسؤول (مثل الرسائل المتعلقة بالثغرات الأمنية أو الأخطاء أو الفيروسات المكتشفة) بلون محدد. يمكنك استخدام الروابط الموجودة في علامة التبويب **المراقبة** لأداء مهام المسؤول القياسية (على سبيل المثال، تثبيت تطبيق الأمان وتكوينه على أجهزة العميل)، وكذلك للانتقال إلى مجلدات أخرى في شجرة وحدة التحكم.

- **الإحصائيات**. تحتوي على مجموعة من الرسوم البيانية مجمعة حسب المواضيع (حالة الحماية ، وإحصائيات مكافحة الفيروسات، والتحديثات، وما إلى ذلك). تظهر هذه الرسوم البيانية المعلومات الحالية حول تشغيل التطبيق وحالة أجهزة العميل.

- **التقارير**. تحتوي على قوالب للتقارير التي تم إنشاؤها بواسطة التطبيق. في علامة التبويب هذه، يمكنك إنشاء تقارير باستخدام قوالب مُعدة مسبقًا، وكذلك إنشاء قوالب تقارير مخصصة.

- نافذة **الأحداث**. تحتوي على سجلات الأحداث التي تم تسجيلها أثناء تشغيل التطبيق. يتم توزيع هذه السجلات بين الموضوعات لسهولة القراءة والتصفية. في علامة التبويب هذه، يمكنك عرض تحديدات الأحداث التي تم إنشاؤها تلقائيًا، وكذلك إنشاء تحديدات مخصصة.

المجلدات في جزء خادم الإدارة

يتضمن جزء **خادم الإدارة – <اسم الجهاز>** المجلدات التالية:

- **الأجهزة المُدارة**. هذا المجلد مخصص لتخزين، وعرض، وتكوين، وتعديل هيكل مجموعات الإدارة، وسياسات المجموعة، ومهام المجموعة.

- **إدارة جهاز المحمول** هذا المجلد مخصص لإدارة الأجهزة المحمولة. يحتوي مجلد **إدارة جهاز المحمول** على المجلدات الفرعية التالية:

  - **خوادم الأجهزة المحمولة**. مخصص لإدارة خوادم iOS MDM.

  - **الأجهزة المحمولة**. مخصص لإدارة الأجهزة المحمولة وKES وiOS MDM.

  - **الشهادات**. مخصص لإدارة شهادات الأجهزة المحمولة.

- **تحديدات الأجهزة**. هذا المجلد مخصص للاختيار السريع للأجهزة التي تستوفي معايير محددة (تحديد جهاز) بين جميع الأجهزة المُدارة. على سبيل المثال، يمكنك بسرعة تحديد الأجهزة التي لم يتم تثبيت أي تطبيق أمان عليها، ويمكنك الانتقال إلى هذه الأجهزة (عرض القائمة). يمكنك تنفيذ إجراءات محددة على هذه الأجهزة المحددة، على سبيل المثال، تعيين بعض المهام لهم. يمكنك استخدام التحديدات المُعدة مسبقًا أو إنشاء اختياراتك المخصصة.

- **الأجهزة غير المخصصة**. يحتوي هذا المجلد على قائمة بالأجهزة التي لم يتم إدراجها في أي من مجموعات الإدارة. يمكنك تنفيذ بعض الإجراءات على الأجهزة غير المخصصة، على سبيل المثال، نقلها إلى مجموعات الإدارة أو تثبيت التطبيقات عليها.

- **السياسات**. هذا المجلد مخصص لعرض وإنشاء السياسات.

- **المهام**. هذا المجلد مخصص لعرض المهام وإنشاء المهام.

- **تراخيص Kaspersky**. يحتوي على قائمة مفاتيح الترخيص المتاحة لتطبيقات Kaspersky. في مساحة العمل الخاصة بهذا المجلد، يمكنك إضافة مفاتيح ترخيص جديدة إلى مستودع مفتاح الترخيص، ونشر مفاتيح الترخيص للأجهزة المُدارة، وعرض تقرير استخدام مفتاح الترخيص.

- **الخيارات المتقدمة**. يحتوي هذا المجلد على مجموعة من المجلدات الفرعية المتوافقة مع مجموعات متنوعة من مزايا التطبيق.

مجلد متقدم. نقل المجلدات في شجرة وحدة التحكم

يتضمن المجلد **المتقدم** المجلدات الفرعية التالية:

- **حسابات المستخدمين**. يحتوي على قائمة حسابات مستخدمي الشبكة.

- **إدارة التطبيق**. مخصص لإدارة التطبيقات المُثبتة على الأجهزة الموجودة على الشبكة. يحتوي مجلد **إدارة التطبيق** على المجلدات الفرعية التالية:

  - **فئات التطبيق**. مخصص لإدارة فئات التطبيقات المخصصة.

  - **سجل التطبيقات**. يحتوي على قائمة التطبيقات على الأجهزة المُثبت عليها عميل الشبكة.

  - **الملفات التنفيذية**. يحتوي على قائمة الملفات التنفيذية المُخزنة على أجهزة العميل المُثبت عليها عميل الشبكة.

- **الثغرات الأمنية بالبرنامج**. يحتوي على قائمة الثغرات الأمنية في التطبيقات على الأجهزة المُثبت عليها عميل الشبكة.
- **تحديثات البرنامج**. يحتوي على قائمة تحديثات التطبيق التي تلقاها خادم الإدارة، ويمكن توزيعها على الأجهزة.
- **استخدام تراخيص الجهات الخارجية**. يحتوي على قائمة مجموعات التطبيقات المرخصة. يمكنك استخدام مجموعات التطبيقات المرخصة لمراقبة استخدام التراخيص لبرامج الجهات الخارجية (تطبيقات غير Kaspersky) والانتهاكات المحتملة لحد الترخيص.

- **التثبيت عن بُعد**. هذا المجلد مخصص لإدارة التثبيت عن بُعد لأنظمة التشغيل والتطبيقات. يحتوي مجلد **التثبيت عن بُعد** على المجلدات الفرعية التالية:
  - **نشر صور الجهاز**. مخصص لنشر صور أنظمة التشغيل على الأجهزة.
  - **حزم التثبيت**. يحتوي على قائمة حزم التثبيت التي يمكن استخدامها للتثبيت عن بُعد للتطبيقات على الأجهزة.
- **تشفير البيانات وحمايتها**. هذا المجلد مخصص لإدارة عملية تشفير البيانات على محركات الأقراص الثابتة ومحركات الأقراص القابلة للإزالة.
- **استقصاء الشبكة**. يعرض هذا المجلد الشبكة التي تم تثبيت خادم الإدارة فيها. يتلقى خادم الإدارة معلومات حول هيكل الشبكة وأجهزتها من خلال الاستقصاءات الدورية لشبكة Windows وشبكات IP الفرعية و®Active Directory في شبكة الشركة. يتم عرض نتائج الاستقصاءات في مساحات عمل المجلدات المقابلة: **المجالات**،و**نطاقات IP**، و**Active Directory**.
- **المستودعات**. هذا المجلد مخصص للعمليات باستخدام الكائنات المُستخدمة لمراقبة حالة الأجهزة وإجراء الصيانة. يحتوي مجلد **المستودعات** على المجلدات الفرعية التالية:
  - **كشف عيوب التكيف**. يحتوي على قائمة الاكتشافات التي تم إجرائها بواسطة قواعد Kaspersky Endpoint Security التي تعمل في وضع التدريب الذكي على أجهزة العميل.
  - **تحديثات وتصحيحات برامج** Kaspersky. يحتوي على قائمة التحديثات التي تلقاها خادم الإدارة، يمكن توزيعها على الأجهزة.
  - **الأجهزة**. يحتوي على قائمة الأجهزة المتصلة بشبكة المؤسسة.
  - **العزل**. يحتوي على قائمة الكائنات التي تم نقلها إلى العزل بواسطة تطبيقات مكافحة الفيروسات على الأجهزة.
  - **النسخ الاحتياطي**. يحتوي على قائمة بالنسخ الاحتياطي للملفات التي تم حذفها أو تعديلها أثناء التطهير على الأجهزة.
  - **ملفات لم تتم معالجتها**. يحتوي على قائمة الملفات المخصصة للفحص اللاحق بواسطة تطبيقات مكافحة الفيروسات.

يمكنك تغيير مجموعة المجلدات الفرعية المُضمنة في مجلد **الخيارات المتقدمة**. يمكن نقل المجلدات الفرعية الأكثر استخدامًا إلى مستوى أعلى من مجلد **الخيارات المتقدمة**. نادرًا ما يمكن نقل المجلدات الفرعية المُستخدمة إلى مجلد **الخيارات المتقدمة**.

لنقل مجلد فرعي خارج مجلد **الخيارات المتقدمة**:

1. في شجرة وحدة التحكم، حدد المجلد الفرعي الذي تريد نقله خارج مجلد **الخيارات المتقدمة**.
2. في قائمة السياق الخاصة بالمجلد الفرعي، حدد **عرض** ← **نقل من مجلد الخيارات المتقدمة**.

> يمكنك أيضًا نقل مجلد فرعي خارج مجلد **الخيارات المتقدمة** في مساحة عمل المجلد **الخيارات المتقدمة** بالنقر فوق رابط **نقل من مجلد الخيارات المتقدمة** في القسم الذي يحمل اسم هذا المجلد الفرعي.

لنقل مجلد فرعي إلى مجلد **الخيارات المتقدمة**:

1. في شجرة وحدة التحكم، حدد المجلد الفرعي الذي تريد نقله إلى مجلد **الخيارات المتقدمة**.
2. في قائمة السياق الخاصة بالمجلد الفرعي، حدد **عرض** ← **نقل إلى مجلد الخيارات المتقدمة**.

كيفية تحديث البيانات في مساحة العمل

لا يتم تحديث البيانات (على سبيل المثال، حالات أجهزة الكمبيوتر أو الإحصائيات أو التقارير) في مساحة عمل Kaspersky Security Center تلقائيًا.

لتحديث البيانات في مساحة العمل:

- اضغط على المفتاح **F5**.
- من قائمة السياق الخاصة بالكائن في شجرة وحدة التحكم، حدد **تحديث**.
- انقر فوق أيقونة التحديث (🔄) في مساحة العمل.

كيفية التنقل في شجرة وحدة التحكم

للتنقل في شجرة وحدة التحكم، يمكنك استخدام أزرار شريط الأدوات التالية:

- ⬅—خطوة إلى الخلف.
- ➡—خطوة واحدة إلى الأمام.
- ↑—مستوى واحد لأعلى.

كما يمكنك استخدام سلسلة التنقل الموجودة في الزاوية العلوية اليمنى من مساحة العمل. وتحتوي سلسلة التنقل على المسار الكامل لمجلد شجرة وحدة التحكم التي تحاول تحديد موقعها حاليًا. وتمثل جميع العناصر الموجودة في السلسلة، باستثناء آخر عنصر، رابطات إلى كائنات في شجرة وحدة التحكم.

كيفية فتح نافذة خصائص الكائن في مساحة العمل

يمكنك تغيير خصائص معظم كائنات وحدة تحكم الإدارة من خلال نافذة خصائص الكائن.

لفتح نافذة الخصائص الخاصة بالكائن الموجود في مساحة العمل:

- من قائمة السياق الخاصة بالكائن، حدد **خصائص**.
- حدد أحد الكائنات ثم اضغط على المفتاحين **ALT+ENTER**.

كيفية تحديد مجموعة من الكائنات في مساحة العمل

يمكنك تحديد مجموعة من الكائنات في مساحة العمل. يمكنك تحديد مجموعة من الكائنات، على سبيل المثال، لإنشاء مجموعة من الأجهزة التي قد تقوم بإنشاء مهام لها لاحقًا.

لتحديد نطاق الكائنات:

1. حدد أول كائن في النطاق ثم اضغط على المفتاح **Shift**.
2. استمر في الضغط على المفتاح **Shift** ثم حدد آخر كائن في النطاق.

   سيتم تحديد النطاق.

لتجميع كائنات متفرقة:

1. حدد أول كائن في النطاق ثم اضغط على المفتاح **Ctrl**.
2. استمر في الضغط على المفتاح **Ctrl** ثم حدد الكائنات الأخرى التي ترغب في تضمينها في المجموعة.

   سيتم تجميع هذه الكائنات.

كيفية تغيير مجموعة من الأعمدة في مساحة العمل

تتيح وحدة تحكم الإدارة إمكانية تغيير مجموعة الأعمدة المعروضة في مساحة العمل.

لتغيير مجموعة الأعمدة المعروضة في مساحة العمل:

1. في شجرة وحدة التحكم، انقر فوق الكائن الذي ترغب في تغيير مجموعة الأعمدة الخاصة به.
2. في مساحة عمل المجلد، افتح النافذة المخصصة لتكوين مجموعة أعمدة عبر النقر فوق الرابط **إضافة/إزالة أعمدة**.
3. في النافذة **إضافة/إزالة أعمدة**، قم بتحديد مجموعة الأعمدة التي سيتم عرضها.

معلومات مرجعية

توفر جداول هذا القسم معلومات موجزة عن قائمة سياق كائنات وحدة التحكم في الإدارة، وكذلك عن حالات كائنات شجرة وحدة التحكم وكائنات مساحة العمل.

أوامر قائمة السياق

يوضح هذا القسم كائنات وحدة تحكم الإدارة وعناصر قائمة السياق المطابِقة (راجع الجدول الموجود بالأسفل).

الكائن	عنصر القائمة	الغرض من عنصر القائمة
العناصر العامة لقائمة السياق	**بحث**	لفتح نافذة البحث عن أجهزة.
	تحديث	لتحديث عرض الكائن المحدد.
	تصدير قائمة	لتصدير القائمة الحالية إلى ملف.
	خصائص	لفتح نافذة الخصائص الخاصة بالكائن المحدد.
	عرض ← إضافة/إزالة أعمدة	لإضافة أو إزالة أعمدة إلى/من جدول الكائنات في مساحة العمل.
	عرض ← أيقونات كبيرة	لإظهار الكائنات الموجودة في مساحة العمل على شكل رموز كبيرة.
	عرض ← أيقونات صغيرة	لإظهار الكائنات الموجودة في مساحة العمل على شكل رموز صغيرة.
	عرض ← القائمة	لإظهار الكائنات الموجودة في مساحة العمل على شكل قائمة.
	عرض ← جدول	لإظهار الكائنات الموجودة في مساحة العمل على شكل جدول.
	عرض ← تكوين	لتكوين عرض عناصر وحدة تحكم الإدارة.
Kaspersky Security Center	**جديد ← خادم الإدارة**	لإضافة خادم إدارة إلى شجرة وحدة التحكم
<اسم خادم الإدارة>	**الاتصال بخادم الإدارة**	للاتصال بخادم الإدارة.
	قطع الاتصال عن خادم الإدارة	لقطع الاتصال مع خادم الإدارة.
الأجهزة المُدارة	**تثبيت التطبيق**	يتم بدء تشغيل معالج التثبيت عن بُعد.
	عرض ← تكوين الواجهة	لتكوين عرض عناصر الواجهة.
	إزالة	لإزالة خادم الإدارة من شجرة وحدة التحكم.
	تثبيت التطبيق	يتم بدء تشغيل معالج التثبيت عن بُعد الخاص بمجموعة الإدارة.
	إعادة تعيين عداد الفيروسات	لإعادة تعيين عدّادات الفيروسات الخاصة بالأجهزة المضمنة في مجموعة الإدارة.
	عرض تقرير التهديدات	إنشاء تقرير التهديدات ونشاط الفيروسات على الأجهزة المضمنة في مجموعة الإدارة.
	مجموعة ← مجموعة	لإنشاء مجموعة إدارة.
	جميع المهام ← بنية مجموعة جديدة	لإنشاء بنية لمجموعات الإدارة بناءً على بنية المجالات أو Active Directory.
	جميع المهام ← عرض الرسالة	يتم بدء تشغيل معالج رسالة جديدة للمستخدم المعنِي بمستخدمي الأجهزة المضمنة في مجموعة الإدارة.
الأجهزة المُدارة ← خوادم الإدارة	**خادم ← خادم الإدارة الثانوي**	يتم بدء تشغيل معالج إضافة خادم إدارة ثانوي.
	خادم ← خادم الإدارة الافتراضي	يتم بدء تشغيل معالج خادم الإدارة الافتراضي الجديد.
إدارة الجهاز المحمول ← الأجهزة المحمولة	**جديد ← جهاز محمول**	لاتصال جهاز محمول جديد خاص بالمستخدم.
إدارة الجهاز المحمول ← الشهادات	**شهادة ← الشهادة**	لإنشاء شهادة.
	إنشاء ← جهاز محمول	لاتصال جهاز محمول جديد خاص بالمستخدم.
تحديدات الأجهزة	**خيار ← تحديد جديد**	لإنشاء تحديد أجهزة.
	جميع المهام ← استيراد	لاستيراد تحديد من ملف.
تراخيص Kaspersky	**إضافة ملف المفتاح أو رمز التنشيط**	لإضافة مفتاح ترخيص إلى مستودع خادم الإدارة.
	تفعيل التطبيق	يتم بدء تشغيل معالج إنشاء مهمة تفعيل التطبيق.
	تقرير حول استخدام المفاتيح	لإنشاء تقرير حول مفاتيح الترخيص المستخدمة على الأجهزة العميلة وعرضه.
إدارة التطبيق ← فئات التطبيق	**فئة ← الفئة**	لإنشاء فئة تطبيق.
إدارة التطبيق ← سجل التطبيقات	**عامل التصفية**	لإعداد عامل تصفية لقائمة التطبيقات.
	التطبيقات المراقبة	تكوين نشر الأحداث المرتبطة بتثبيت التطبيقات.
	إزالة التطبيقات غير المثبتة	يمحو كل التفاصيل الخاصة بالتطبيقات غير المثبتة على الأجهزة المتصلة بالشبكة من القائمة.
إدارة التطبيق ← تحديثات البرنامج	**قبول اتفاقيات تراخيص التحديثات**	لقبول اتفاقية ترخيص تحديثات البرامج.
إدارة التطبيق ← استخدام تراخيص الجهات الخارجية	**مجموعة ← مجموعة التطبيقات المرخصة**	لإنشاء مجموعة تطبيقات مرخصة.

الكائن	عنصر القائمة	الغرض من عنصر القائمة
التثبيت عن بُعد ← حزم التثبيت	**عرض إصدارات التطبيق الحالية**	لإظهار قائمة بالإصدارات الحديثة من تطبيقات Kaspersky المتوفرة على خوادم الويب.
	حزمة ← حزمة التثبيت	لإنشاء حزمة تثبيت.
	جميع المهام ← تحديث قواعد البيانات	لتحديث قواعد بيانات التطبيقات الموجودة في حِزم التثبيت.
	جميع المهام ← عرض القائمة العامة للحزم المستقلة	لعرض قائمة الحِزم المستقلة التي تم إنشاؤها لحِزم التثبيت.
اكتشاف الأجهزة ← المجالات	**جميع المهام ← نشاط الجهاز**	لإعداد استجابة خادم الإدارة لخمول الأجهزة المتصلة بالشبكة.
اكتشاف الأجهزة ← نطاقات IP	**نطاق IP ← نطاق IP**	لإنشاء نطاق IP.
المستودعات ← تحديثات قواعد بيانات Kaspersky ووحدات البرامج النمطية	**تنزيل التحديثات**	لفتح نافذة خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة.
	إعدادات تنزيل التحديثات	لتكوين مهمة تنزيل التحديثات إلى المستودع الخاصة بخادم الإدارة.
	تقرير عن استخدام قواعد بيانات مكافحة الفيروسات	لإنشاء تقرير حول إصدارات قواعد البيانات وعرضه.
	جميع المهام ← مسح مستودع التحديثات	مسح مستودع تحديثات خادم الإدارة.
المستودعات ← الأجهزة	**جهاز ← الجهاز**	لإنشاء جهاز جديد.

قائمة بالأجهزة المُدارة. وصف الأعمدة

يعرض الجدول التالي أسماء وأوصاف ذات صلة بأعمدة في قائمة الأجهزة المُدارة.

أوصاف الأعمدة في قائمة الأجهزة المُدارة

اسم العمود	القيمة
الاسم	اسم NetBIOS للجهاز العميل. يتم إعطاء أوصاف رموز أسماء الجهاز في الملحق.
نوع نظام التشغيل	نوع نظام التشغيل المثبت على الجهاز العميل.
مجال Windows	اسم مجال Windows الذي يقع فيه الكمبيوتر العميل.
تم تثبيت عميل الشبكة	نتيجة تثبيت عميل الشبكة على الجهاز العميل: نعم، لا، غير معروف.
عميل الشبكة قيد التشغيل	نتيجة تشغيل عميل الشبكة: نعم، لا، غير معروف.
الحماية في الوقت الحقيقي	تم تثبيت تطبيق الأمان: نعم، لا، غير معروف.
آخر اتصال بخادم الإدارة	الفترة الزمنية التي انقضت منذ أن تم توصيل الجهاز العميل بخادم الإدارة.
آخر تحديث لقواعد بيانات مكافحة الفيروسات	الفترة الزمنية التي مرت منذ آخر تحديث للأجهزة المُدارة.
الحالة	الحالة الحالية للجهاز العميل: مقبول، حرج، تحذير.

اسم العمود	القيمة
وصف الحالة	ظروف تغيير حالة الجهاز العميل إلى حرج أو تحذير. يتم تغيير حالة الجهاز إلى تحذير أو حرج في ظل الظروف التالية: • تطبيق الأمان غير مثبت. • تم اكتشاف العديد من الفيروسات. • يختلف مستوى الحماية في الوقت الحقيقي عن المستوى الذي تم تعيينه من قِبل المسؤول. • لم يتم إجراء فحص البرامج الضارة منذ وقت طويل. • قواعد البيانات قديمة. • لم يتم الاتصال منذ فترة طويلة. • تم اكتشاف تهديدات نشطة. • إعادة التشغيل مطلوبة. قد يكون سبب إعادة تشغيل الجهاز أحد الأسباب التالية: • تمت إعادة التشغيل لسبب غير معروف. • لن يتم تشغيل التطبيق حتى تتم إعادة التشغيل. • يلزم إعادة التشغيل لإكمال التحديث؛ يجري تشغيل التطبيق حاليًا. • يلزم إعادة التشغيل لبدء التحديث. • يلزم إعادة التشغيل لإكمال الفحص أو التنظيف. • يلزم إعادة التشغيل لإكمال التثبيت عن بُعد / إلغاء التثبيت. • إكمال تشفير البيانات على القرص. يمكنك تحديد الأسباب عند تكوين تبديل حالات الأجهزة. • تم تثبيت تطبيقات غير متوافقة. • تم اكتشاف ثغرات أمنية بالبرنامج. • لم يتم إجراء التحقق من تحديثات Windows Update منذ وقت طويل. • حالة تشفير غير صالحة. • لا تتوافق إعدادات الجهاز المحمول مع السياسة. • تم اكتشاف مشكلات أمان لم تتم معالجتها. • حالة الجهاز المحددة بواسطة التطبيق. • نفدت مساحة قرص الجهاز. • ستنتهي فترة صلاحية الترخيص قريبًا. يتم تغيير حالة الجهاز إلى حرج فقط لوجود أحد الأسباب التالية: • انتهت صلاحية الترخيص. • أصبح الجهاز غير مُدار. • تم تعطيل الحماية. • تطبيق الأمان ليس قيد التشغيل. يمكن لتطبيقات Kaspersky المُدارة على الأجهزة العميلة إضافة أوصاف الحالة إلى القائمة. يمكن لـ Kaspersky Security Center استلام وصف لحالة جهاز عميل من تطبيقات Kaspersky المُدارة المثبتة على ذلك الجهاز. إذا كانت الحالة التي تم تعيينها للجهاز بواسطة التطبيق المُدار بخلاف الحالة التي عينها Kaspersky Security Center، فستظهر وحدة تحكم الإدارة الحالة الأكثر حرجًا لأمان الجهاز. وعلى سبيل المثال، إذا عين الجهاز المدار الحالة حرج للجهاز في حين أن Kaspersky Security Center عين له الحالة تحذير، فستعرض وحدة تحكم الإدارة الحالة حرج لذلك الجهاز بجانب الوصف المطابق المقدَّم من التطبيق المدار.
تم تحديث المعلومات	الفترة الزمنية التي مرت منذ آخر مزامنة ناجحة للجهاز العميل مع خادم الإدارة (أي منذ آخر فحص للشبكة).
اسم DNS	اسم مجال DNS الخاص بالجهاز العميل؛
مجال DNS	لاحقة DNS الأساسية.
عنوان IP	عنوان IP الخاص بالجهاز العميل؛ ينصح باستخدام عنوان IPv4.
آخر وقت مرئي	الفترة الزمنية التي ظل خلالها الجهاز العميل مرئيًا في الشبكة.
آخر فحص كامل	وقت وتاريخ آخر فحص تم إجراؤه للجهاز العميل بواسطة تطبيق الأمان بناءً على طلب المستخدم.
إجمالي عدد التهديدات المكتشفة	عدد التهديدات التي تم العثور عليها.
حالة الحماية في الوقت الحقيقي	حالة الحماية في الوقت الحقيقي: يجري البدء، قيد التشغيل، قيد التشغيل (الحماية القصوى)، قيد التشغيل (السرعة القصوى)، قيد التشغيل (الإعدادات الموصى بها)، قيد التشغيل (إعدادات مخصصة)، متوقف، متوقف مؤقتًا، فشل.
عنوان IP للاتصال	عنوان IP المستَخدَم للاتصال بخادم إدارة Kaspersky Security Center.
إصدار عميل الشبكة	إصدار عميل الشبكة.
إصدار التطبيق	إصدار تطبيق الأمان المثبت على الجهاز العميل.
تم إصدار قواعد بيانات مكافحة الفيروسات	إصدار قواعد بيانات مكافحة الفيروسات
آخر تشغيل للنظام	وقت وتاريخ آخر تشغيل للجهاز العميل.
إعادة التشغيل مطلوبة	يلزم إعادة تشغيل الجهاز العميل.
نقطة توزيع	اسم الجهاز الذي يعمل بمثابة نقطة توزيع لهذا الجهاز العميل.

اسم العمود	القيمة
الوصف	وصف الجهاز العميل الذي تم استلامه بعد فحص الشبكة.
حالة التشفير	حالة تشفير البيانات للجهاز العميل.
حالة WUA	حالة وكيل تحديث Windows على الجهاز العميل. تتوافق القيمة نعم مع الأجهزة العميلة التي تتلقى التحديثات من خلال Windows Update من خادم الإدارة. تتوافق القيمة لا مع الأجهزة العميلة التي تسترد التحديثات من خلال تحديث Windows Update من موارد أخرى.
حجم نظام التشغيل بالبت	حجم نظام التشغيل المثبت على الجهاز العميل.
حالة الحماية من البريد العشوائي	حالة مكون الحماية من البريد غير المرغوب فيه: قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، غير معروف
حالة منع تسريب البيانات	حالة مكون منع تسريب البيانات: قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، غير معروف
حالة الحماية الخاصة بتعاون الخوادم	حالة مكون تصفية المحتوى: قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، غير معروف
حالة الحماية ضد الفيروسات الخاصة بخوادم البريد	حالة مكون الحماية ضد الفيروسات لخادم البريد: قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، غير معروف
حالة أداة استشعار نقطة النهاية	حالة مكون Endpoint Detection and Response (KATA): قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، غير معروف
تم الإنشاء	الوقت الذي تم فيه إنشاء رمز <اسم الجهاز>. هذه السمة مستخدمة في مقارنة الأحداث السابقة ببعضها.
اسم خادم الإدارة الثانوي أو الافتراضي	اسم خادم الإدارة الثانوي أو الافتراضي. هذا العمود غير متاح إلا في القوائم التي تحتوي على أجهزة من خوادم إدارة مختلفة.
المجموعة الأصلية	اسم مجموعة الإدارة التي يوجد بها رمز <اسم الجهاز>. هذا العمود غير متاح إلا في القوائم التي تحتوي على أجهزة من خوادم إدارة مختلفة.
مُدار بواسطة خادم إدارة مختلف	يمكن لهذه المعلمة أن تتخذ إحدى القيم التالية: • حقيقي إذا اتضح أثناء التثبيت عن بُعد أن تطبيقات الأمان على الجهاز أن الجهاز يديره خادم إدارة مختلف. • زائف بخلاف ذلك.
نظام التشغيل بناء	رقم نسخة نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم نسخة مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.
معرف تحرير نظام التشغيل	معرف إصدار (ID) نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك معرف إصدار مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام معرف الإصدار باستثناء الرقم المحدد.

حالات الأجهزة والمهام والسياسات

يحتوي الجدول أدناه على قائمة رموز معروضة في شجرة وحدة التحكم وفي مساحة عمل وحدة تحكم الإدارة، بجانب أسماء الأجهزة والمهام والسياسات. تحدد هذه الرموز حالات الأهداف.

حالات الأجهزة والمهام والسياسات

الرمز	الحالة
	اكتشاف جهاز مثبت عليه نظام تشغيل لمحطات عمل في النظام وغير مضمن في أي من مجموعات الإدارة.
	تضمين جهاز مثبت عليه نظام تشغيل لمحطات عمل في مجموعة إدارة، بالحالة موافق.
	تضمين جهاز مثبت عليه نظام تشغيل لمحطات عمل في مجموعة إدارة، بحالة تحذير.

	تضمين جهاز مثبت عليه نظام تشغيل لمحطات عمل في مجموعة إدارة، بحالة حرج.
	تضمين جهاز لمحطات العمل في مجموعة إدارة، فقدت اتصالها بخادم الإدارة.
	اكتشاف جهاز مثبت عليه نظام تشغيل لخوادم في النظام وغير مضمن في أي من مجموعات الإدارة.
	تضمين جهاز مثبت عليه نظام تشغيل لخوادم في مجموعة إدارة، بالحالة موافق.
	تضمين جهاز مثبت عليه نظام تشغيل لخوادم في مجموعة إدارة، بحالة تحذير.
	تضمين جهاز مثبت عليه نظام تشغيل لخوادم في مجموعة إدارة، بحالة حرج.
	تضمين جهاز بنظام تشغيل لخوادم في مجموعة إدارة، فقدت اتصالها بخادم الإدارة.
	لم يتم تضمين الجهاز المحمول المكتشف في الشبكة في أي من مجموعات الإدارة.
	تضمين جهاز محمول في مجموعة إدارة، بالحالة موافق.
	تضمين جهاز محمول في مجموعة إدارة، بحالة تحذير.
	تضمين جهاز محمول في مجموعة إدارة، بحالة حرج.
	تم تضمين الجهاز المحمول في مجموعة إدارة فقدت الاتصال بخادم الإدارة.
	تم اكتشاف جهاز حماية UEFI في الشبكة ولكن لم يتم تضمينه في أي مجموعة إدارة. يوجد جهاز حماية UEFI في الشبكة.
	تم اكتشاف جهاز حماية UEFI في الشبكة ولكن لم يتم تضمينه في أي مجموعة إدارة. جهاز حماية UEFI لا يوجد في لشبكة.
	تضمين جهاز حماية UEFI في مجموعة إدارة، بالحالة موافق. يوجد جهاز حماية UEFI في الشبكة.
	تضمين جهاز حماية UEFI في مجموعة إدارة، بالحالة موافق. جهاز حماية UEFI لا يوجد في لشبكة.
	تضمين جهاز حماية UEFI في مجموعة إدارة، بحالة تحذير. يوجد جهاز حماية UEFI في الشبكة.
	تضمين جهاز حماية UEFI في مجموعة إدارة، بحالة تحذير. جهاز حماية UEFI لا يوجد في لشبكة.
	تضمين جهاز حماية UEFI في مجموعة إدارة، بحالة حرج. يوجد جهاز حماية UEFI في الشبكة.
	تضمين جهاز حماية UEFI في مجموعة إدارة، بحالة حرج. جهاز حماية UEFI لا يوجد في لشبكة.
	السياسة المفعلة.
	السياسة غير المفعلة.
	سياسة نشطة موروثة من مجموعة تم إنشاؤها على خادم الإدارة الرئيسي.
	السياسة المفعلة الموروثة من مجموعة مستوى أعلى.
	المهمة (مهمة المجموعة أو مهمة خادم الإدارة أو المهمة لأجهزة خاصة) بالحالة مجدول أو اكتمل بنجاح.
	المهمة (مهمة المجموعة أو مهمة خادم الإدارة أو المهمة لأجهزة خاصة) بالحالة قيد التشغيل.
	المهمة (مهمة المجموعة أو مهمة خادم الإدارة أو المهمة لأجهزة خاصة) بالحالة فشل.
	مهمة موروثة من مجموعة تم إنشاؤها على خادم الإدارة الرئيسي.
	مهمة موروثة من مجموعة مستوى أعلى.

رموز حالة الملف في وحدة تحكم الإدارة

لتسهيل إدارة الملفات في وحدة تحكم إدارة Kaspersky Security Center، يتم عرض الرموز بجانب أسماء الملفات (راجع الجدول أدناه). تشير الرموز إلى الحالات المخصصة للملفات بواسطة تطبيقات Kaspersky المدارة على الأجهزة العميلة. يتم عرض الأيقونات في مساحات عمل المجلدات **العزل**، و**النسخ الاحتياطي**، و**تهديدات نشطة**.

يتم تعيين الحالات إلى الكائنات بواسطة Kaspersky Endpoint Security المثبت على الجهاز العميل الذي يوجد عليه الكائن.

التطابق بين الرموز وحالات الملفات

الرمز	الحالة
	الملف ذو الحالة مصاب.
	الملف ذو الحالة تحذير أو محتمل الإصابة.
	ملف بحالةتتم إضافتها من جانب المستخدم.
	ملف بحالةاكتشافات إيجابية زائفة.
	ملف بحالة تم التنظيف.
	ملف بحالة تم الحذف.
	الملف الموجود في المجلد **العزل** ذي الحالة غير مصاب أو محمي بكلمة مرور أو يجب الإرسال إلى Kaspersky. في حالة عدم وجود وصف للحالة بجانب الرمز، فإن ذلك يعني أن تطبيق Kaspersky المدار على الجهاز العميل قد أبلغ عن حالة غير معروفة إلى Kaspersky Security Center.
	الملف الموجود في المجلد **النسخ الاحتياطي** ذي الحالة غير مصاب أو محمي بكلمة مرور أو يجب الإرسال إلى Kaspersky. في حالة عدم وجود وصف للحالة بجانب الرمز، فإن ذلك يعني أن تطبيق Kaspersky المدار على الجهاز العميل قد أبلغ عن حالة غير معروفة إلى Kaspersky Security Center.
	الملف الموجود في المجلد **تهديدات نشطة** ذي الحالة غير مصاب أو محمي بكلمة مرور أو يجب الإرسال إلى Kaspersky. في حالة عدم وجود وصف للحالة بجانب الرمز، فإن ذلك يعني أن تطبيق Kaspersky المدار على الجهاز العميل قد أبلغ عن حالة غير معروفة إلى Kaspersky Security Center.

البحث عن البيانات وتصديرها

يحتوي هذا القسم على معلومات حول وسائل البحث عن البيانات وتصديرها.

العثور على أجهزة

يتيح لك Kaspersky Security Center العثور على أجهزة بناءً معيار محدد. ويمكن حفظ نتائج البحث في ملف نصي.

تتيح لك ميزة البحث العثور على الأجهزة التالية:

- الأجهزة العميلة في مجموعات الإدارة الخاصة بخادم الإدارة وخوادمه التابعة.
- الأجهزة غير المخصصة بواسطة خادم الإدارة وخوادمه التابعة.

للعثور على الأجهزة العميلة المضمنة في مجموعة إدارة:

1. في شجرة وحدة التحكم، حدد مجلد مجموعة الإدارة.

2. حدد **بحث** من قائمة سياق مجلد مجموعة الإدارة.

3. على علامات تبويب النافذة **بحث**، حدد المعايير للبحث عن أجهزة وانقر فوق الزر **بحث الآن**.

الآن سيتم عرض الأجهزة التي تتوافق مع معايير البحث المحددة في جدول يقع في الجزء السفلي من النافذة **بحث**.

للعثور على الأجهزة غير المخصصة:

1. من شجرة وحدة التحكم، حدد المجلد **الأجهزة غير المخصصة**.

2. حدد **بحث** من قائمة سياق المجلد **الأجهزة غير المخصصة**.

3. على علامات تبويب النافذة **بحث**، حدد المعايير للبحث عن أجهزة وانقر فوق الزر **بحث الآن**.

الآن سيتم عرض الأجهزة التي تتوافق مع معايير البحث المحددة في جدول يقع في الجزء السفلي من النافذة **بحث**.

للبحث عن الأجهزة بصرف النظر عما إذا كانت مضمنة في مجموعة إدارة أم لا:

1. في شجرة وحدة التحكم، حدد العقدة **خادم الإدارة** .

2. في قائمة السياق الخاصة بالعقدة، حدد **بحث**.

3. على علامات تبويب النافذة **بحث**، حدد المعايير للبحث عن أجهزة وانقر فوق الزر **بحث الآن**.

الآن سيتم عرض الأجهزة التي تتوافق مع معايير البحث المحددة في جدول يقع في الجزء السفلي من النافذة **بحث**.

في النافذة **بحث** يمكنك أيضًا البحث عن مجموعات الإدارة وخوادم الإدارة الثانوية باستخدام قائمة منسدلة في الزاوية العلوية اليمنى من النافذة. لا تتوفر وظيفة البحث عن مجموعات الإدارة وخوادم الإدارة الثانوية إذا قمت بفتح النافذة **بحث** من المجلد **الأجهزة غير المخصصة**.

للعثور على أجهزة، يمكنك استخدام التعبيرات المعتادة في حقول النافذة **بحث**.

يتوفر البحث بالنص الكامل في النافذة **بحث**:

- في علامة التبويب **الشبكة**، في الحقل **الوصف**
- في علامة التبويب **الأجهزة**، في الحقول **الجهاز** و**المورّد** و**الوصف**

إعدادات البحث عن الجهاز

فيما يلي أوصاف الإعدادات المستخدمة للبحث عن الأجهزة المدارة. وتُعرض نتائج البحث في الجزء السفلي من النافذة.

الشبكة

من علامة التبويب **الشبكة**، يمكنك تحديد المعايير التي ستُستخدم للبحث عن الأجهزة وفقًا لبيانات الشبكة الخاصة بهم:

- **اسم الجهاز أو عنوان IP**

  اسم شبكة Windows (اسم NetBIOS) للجهاز، أو عنوان IPv4 أو IPv6.

- **مجال Windows**

  عرض كل الأجهزة المضمنة في مجال Windows® المحدد.

- **مجموعة الإدارة**

  عرض الأجهزة المضمنة في مجموعة الإدارة المحددة.

- **الوصف**

  نص في نافذة خصائص الجهاز: في الحقل **الوصف** بالقسم **عام**.

  لوصف النص في الحقل **الوصف**، يمكنك استخدام الرموز التالية:

  - وسط الكلمة:

    - *. تحل محل أية سلسلة بها أي عدد من الحروف.

    مثال:

    لوصف كلمات مثل **الخادم** أو **خاص بالخادم**، يمكنك إدخال **خادم***.

    - ؟. تحل محل أي حرف مفرد.

    مثال:

    لوصف كلمات مثل **نافذة** أو **نوافذ**، يمكنك إدخال **نافذة؟**.

    لا يمكن استخدام نجمة (*) أو علامة استفهام (؟) كأول حرف في الاستعلام.

  - للبحث عن كلمات متعددة:

    - مسافة. تعرض جميع الأجهزة التي يحتوي وصفها على أي كلمة من الكلمات المدرجة.

    مثال:

    للبحث عن عبارة تحتوي على كلمة **تابع** أو **ظاهري**، يمكنك إدخال **تابع ظاهري** في الاستعلام.

    - +. عندما تأتي علامة الزائد قبل كلمة، ستحتوي جميع نتائج البحث على هذه الكلمة.

    مثال:

    للبحث عن عبارة تحتوي على الكلمتين **تابع** و**ظاهري**، أدخل الاستعلام **+تابع+ظاهري**.

    - -. عندما تأتي علامة الناقص قبل كلمة، لن تحتوي نتائج البحث على هذه الكلمة.

    مثال:

    للبحث عن عبارة تحتوي على كلمة **تابع** ولا تحتوي على كلمة **ظاهري**، أدخل الاستعلام **+تابع-ظاهري**.

    - **"<some text>"**. النص الموضوع بين علامتي الاقتباس يجب أن يكون موجودًا في النص.

مثال:

للبحث عن عبارة تحتوي على الكلمة المركّبة **الخادم التابع**، أدخل **"الخادم التابع"** في الاستعلام.

- **نطاق IP**

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.

يتم تعطيل هذا الخيار افتراضيًا.

- **مُدار بواسطة خادم إدارة مختلف**

حدد إحدى القيم التالية:

- **نعم**. يتم اعتبار الأجهزة العميلة التي تتم إدارتها بواسطة خوادم إدارة أخرى فقط.
- **لا**. تتم مراعاة الأجهزة العميلة المُدارة بواسطة خادم الإدارة نفسه.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

العلامات

في علامة التبويب **العلامات**، يمكنك تكوين بحث عن جهاز بناء على الكلمات المفتاحية (العلامات) التي تمت إضافتها سابقًا إلى أوصاف الأجهزة المدارة:

- **تطبيق في حالة مطابقة علامة محددة واحدة على الأقل**

إذا تم تمكين هذا الخيار، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على علامة واحدة من العلامات على الأقل.

إذا تم تعطيل هذا الخيار، فستعرض نتائج البحث فقط الأجهزة التي تحتوي أوصافها على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

- **يجب تضمين العلامة**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

يتم تحديد هذا الخيار افتراضيًا.

- **يجب استثناء العلامة**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي لا تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

Active Directory

في علامة التبويب **Active Directory**، يمكنك تحديد أنه يجب البحث عن الأجهزة في الوحدة التنظيمية لـ Active Directory أو المجموعة. يمكنك أيضًا تضمين الأجهزة من جميع الوحدات التنظيمية المحددة التابعة لـ Active Directory في خانة التحديد. لتحديد الأجهزة، حدد الإعدادات التالية:

- **الجهاز في وحدة Active Directory التنظيمية**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من وحدة Active Directory المؤسسية المحددة في حقل الإدخال.

يتم تعطيل هذا الخيار افتراضيًا.

- **تضمين وحدات تنظيمية تابعة**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من الوحدات المؤسسية التابعة لوحدات Active Directory المؤسسية.

يتم تعطيل هذا الخيار افتراضيًا.

- **هذا الجهاز عضو في مجموعة Active Directory**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من مجموعة Active Directory المحددة في حقل الإدخال.

يتم تعطيل هذا الخيار افتراضيًا.

نشاط الشبكة

في علامة التبويب **نشاط الشبكة**، يمكنك تحديد المعايير التي ستُستخدم للبحث عن الأجهزة وفقًا لنشاط الشبكة الخاص بهم:

- **هذا الجهاز هوعبارة عن نقطة توزيع**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

  - **نعم**. سوف يتضمن التحديد أجهزة الكمبيوتر التي تعمل كنقاط توزيع.
  - **لا**. لن يتم تضمين الأجهزة التي تعمل كنقاط توزيع في التحديد.
  - **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **عدم قطع الاتصال عن خادم الإدارة**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

  - **مُمكّن**. سيتضمن التحديد الأجهزة التي تم تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
  - **معطل**. سيتضمن التحديد الأجهزة التي تم إلغاء تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
  - **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تم تبديل ملف تعريف الاتصال**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

  - **نعم**. سوف يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
  - **لا**. لن يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
  - **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تاريخ آخر اتصال بخادم الإدارة**

يمكنك استخدام خانة الاختيار هذه لتعيين معيار للبحث عن الأجهزة إلى وقت آخر اتصال بخادم الإدارة.

إذا تم تحديد خانة الاختيار هذه، فيمكنك في حقول الإدخال تحديد الفاصل الزمني (التاريخ والوقت) الذي تم خلاله إنشاء آخر اتصال بين عميل الشبكة المثبت على الجهاز العميل وخادم الإدارة. سوف يتضمن الاختيار الأجهزة التي تقع ضمن الفاصل الزمني المحدد.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **تم اكتشاف أجهزة جديدة بواسطة استقصاء الشبكة**

عمليات البحث عن أجهزة جديدة تم اكتشافها بواسطة استقصاء الشبكة على مدار الأيام القليلة الماضية.

إذا تم تمكين هذا الخيار، فسيتضمن التحديد فقط الأجهزة الجديدة التي تم اكتشافها بواسطة خاصية اكتشاف الأجهزة على مدار عدد الأيام المحددة في حقل **فترة الكشف (بالأيام)**.

إذا تم تعطيل هذا الخيار، فسيتضمن التحديد جميع الأجهزة التي تم اكتشافها بواسطة خااصية اكتشاف الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- **الجهاز مرئي**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المرئية في الوقت الحالي على الشبكة.
- **لا**. يشمل التطبيق في التحديد الأجهزة غير المرئية في الوقت الحالي على الشبكة.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

التطبيق

من علامة التبويب **التطبيق**، يمكنك تحديد المعايير التي ستُستخدم للبحث عن الأجهزة وفقًا للتطبيق المدار المحدد:

- **اسم التطبيق**

في القائمة المنسدلة، يمكنك إعداد معيار لتضمين الأجهزة في تحديد عند إجراء بحث باسم تطبيق Kaspersky.

توفر القائمة أسماء التطبيقات مع الأدوات الإضافية للإدارة فقط والمثبتة على محطة عمل المسؤول.

إذا لم يتم تحديد تطبيق، لن يتم تطبيق المعيار.

- **إصدار التطبيق**

في حقل الإدخال، يمكنك تحديد معيار لتضمين الأجهزة في تحديد عند إجراء بحث برقم إصدار تطبيق Kaspersky.

إذا لم يتم تحديد رقم إصدار، لن يتم تطبيق المعيار.

- **اسم التحديث الحرج**

في حقل الإدخال، يمكنك تحديد معيار للأجهزة المشمولة في التحديد عند إجراء بحث باسم التطبيق أو برقم حزمة التحديث.

إذا تم ترك الحقل فارغًا، لن يتم تطبيق المعيار.

- **آخر تحديث للوحدات**

يمكنك استخدام هذا الخيار لتعيين معيار للبحث في الأجهزة على وقت آخر تحديث للوحدات النمطية الخاصة بالتطبيقات المثبتة على تلك الأجهزة.

إذا تم تحديد خانة الاختيار هذه، يمكنك تحديد في حقل الإدخال الفاصل الزمني (الوقت والتاريخ) الذي تم خلاله إجراء التحديث الأخير للوحدات النمطية المثبتة على تلك الأجهزة.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **الجهاز مُدار بواسطة Kaspersky Security Center**

في هذه القائمة المنسدلة، يمكنك تضمين الأجهزة المدارة بواسطة Kaspersky Security Center في التحديد:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المدارة بواسطة Kaspersky Security Center في الاختيار.
- **لا**. يشمل التطبيق الأجهزة الموجودة في التحديد ما لم تكن مدارة من خلال Kaspersky Security Center.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تم تثبيت تطبيق الأمان**

في هذه القائمة المنسدلة، يمكنك تضمين جميع الأجهزة المدارة المثبت عليها تطبيق الأمان في التحديد:

- **نعم**. يشمل التطبيق في الاختيار جميع الأجهزة المدارة بواسطة تطبيق الأمان الذي تم تثبيته:
- **لا**. يشمل التطبيق في الاختيار جميع الأجهزة غير المثبت عليها تطبيق الأمان.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

نظام التشغيل

في علامة التبويب **نظام التشغيل**، يمكنك إعداد المعايير التالية للبحث عن الأجهزة حسب نوع نظام التشغيل (OS) الخاص بهم:

- **إصدار نظام التشغيل**

إذا تم تحديد خانة الاختيار، فيمكنك تحديد نظام تشغيل من القائمة. يتم تضمين الأجهزة المثبت عليها أنظمة التشغيل المحددة في نتائج البحث.

- **حجم نظام التشغيل بالبت**

في القائمة المنسدلة، يمكنك تحديد بنية نظام التشغيل والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز (**غير معروف**, **x86**, **AMD64** أو **IA64**). وبشكل افتراضي، لا يتم تحديد أي خيار في القائمة ومن ثم لا يتم تحديد بنية نظام التشغيل.

- **إصدار حزمة خدمة نظام التشغيل**

في هذا الحقل، يمكنك تحديد إصدار حزمة نظام التشغيل (بتنسيق X.Y)، والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز. وبشكل افتراضي، لا يتم تحديد أي قيمة إصدار.

- **نظام التشغيل بناء**

لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

رقم نسخة نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم نسخة مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.

- **معرف تحرير نظام التشغيل**

لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

معرف إصدار (ID) نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك معرف إصدار مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام معرف الإصدار باستثناء الرقم المحدد.

حالة الجهاز

في علامة التبويب **حالة الجهاز**، يمكنك تحديد معايير البحث عن الجهاز بناء على حالة الجهاز من التطبيق المدار:

- **حالة الجهاز**

القائمة المنسدلة التي يمكنك فيها تحديد إحدى حالات الجهاز: موافق، أو حرج، أو تحذير.

- **حالة الحماية في الوقت الحقيقي**

يمكنك في القائمة المنسدلة تحديد حالة الحماية في الوقت الحقيقي. يتم تضمين الأجهزة مع حالة الحماية في الوقت الحقيقي في التحديد.

- **وصف حالة الجهاز**

يمكنك في هذا الحقل، تحديد خانات الاختيار بجانب الشروط التي تحدد، إن تم استيفائها، إحدى الحالات التالية لجهاز الكمبيوتر: موافق أو حرج أو تحذير.

- **حالة الجهاز المحددة بواسطة التطبيق**

يمكنك في القائمة المنسدلة تحديد حالة الحماية في الوقت الحقيقي. يتم تضمين الأجهزة مع حالة الحماية في الوقت الحقيقي في التحديد.

مكونات الحماية

من علامة التبويب **مكونات الحماية**، يمكنك إعداد المعايير للبحث عن أجهزة العميل حسب حالة الحماية الخاصة بها.

- **تم إصدار قاعدة البيانات**

إذا تم تحديد هذا الخيار، يمكنك البحث عن أجهزة العميل حسب تاريخ إصدار قاعدة بيانات تطبيق مكافحة الفيروسات. في حقول الإدخال، يمكنك تعيين الفاصل الزمني الذي يتم إجراء البحث بناءً عليه.

يتم تعطيل هذا الخيار افتراضيًا.

- **آخر فحص**

إذا تم تمكين هذا الخيار، فيمكنك البحث عن أجهزة العميل حسب وقت آخر فحص للبرامج الضارة. في حقول الإدخال، يمكنك تحديد الفترة الزمنية التي تم فيها آخر فحص للبرامج الضارة.

يتم تعطيل هذا الخيار افتراضيًا.

- **إجمالي عدد التهديدات المكتشفة**

إذا تم تمكين هذا الخيار، يمكنك البحث عن أجهزة العميل حسب عدد الفيروسات التي تم العثور عليها. في حقول الإدخال، يمكنك تعيين قيم الحد الأدنى والأعلى لعدد الفيروسات التي تم العثور عليها.

يتم تعطيل هذا الخيار افتراضيًا.

سجل التطبيقات

في علامة التبويب **سجل التطبيقات**، يمكنك تكوين البحث عن الأجهزة وفقًا للتطبيقات المثبتة عليها:

- **اسم التطبيق**

القائمة المنسدلة التي يمكنك فيها تحديد أي تطبيق. يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **إصدار التطبيق**

يمكنك في حقل الإدخال تحديد إصدار التطبيق المحدد.

- **المورّد**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة لأي تطبيق مثبت على الجهاز.

- **حالة التطبيق**

يمكنك في القائمة المنسدلة تحديد حالة أي تطبيق (مثبت، غير مثبت). سيتم تضمين الأجهزة التي تم تثبيت التطبيق المحدد أو لم يتم تثبيته عليها، بناءً على الحالة المحددة، في التحديد.

- **بحث حسب التحديث**

إذا تم تمكين هذا الخيار، فسيتم إجراء البحث باستخدام تفاصيل تحديثات التطبيقات المثبتة على الأجهزة ذات الصلة. بعد تحديد خانة الاختيار، تتغير الحقول **اسم التطبيق** و**إصدار التطبيق** و**حالة التطبيق** إلى **اسم التحديث** و**إصدار التحديث** و**الحالة** على التوالي.

يتم تعطيل هذا الخيار افتراضيًا.

- **اسم تطبيق الأمان غير المتوافق**

القائمة المنسدلة التي يمكنك فيها تحديد تطبيقات الحماية الخاصة بالجهة الخارجية. خلال البحث، يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **علامة التطبيق**

يمكنك في القائمة المنسدلة تحديد علامة التطبيق. يتم تضمين جميع الأجهزة المثبت عليها تطبيقات مشتملة على العلامة المحددة في الوصف، في تحديد الجهاز.

التسلسل الهرمي لخوادم الإدارة

في علامة التبويب **التسلسل الهرمي لخوادم الإدارة**، حدد مربع الاختيار **تضمين بيانات من خودام الإدارة الثانوية (نزولًا إلى مستوى أقل)** إذا كنت ترغب في أن يتم أخذ المعلومات المخزنة على خوادم الإدارة الثانوية أثناء البحث عن الأجهزة بعين الاعتبار، فيمكنك تحديد حقل الإدخال تحديد مستوى تداخل خادم الإدارة الثانوي الذي يتم من خلاله أخذ المعلومات بعين الاعتبار أثناء البحث عن الأجهزة. تكون خانة الاختيار غير محددة بشكل افتراضي.

الأجهزة الظاهرية

في علامة التبويب **الأجهزة الظاهرية**، يمكنك تكوين البحث عن أجهزة بناءً على ما إذا كانت تعد أجهزة ظاهرية أو جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI):

- **هذا جهاز ظاهري**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

  - **ليس هامًا**.
  - **لا**. البحث عن الأجهزة التي لا تعد أجهزة افتراضية.
  - **نعم**. البحث عن الأجهزة التي تعد أجهزة ظاهرية.

- **نوع الجهاز الظاهري**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة للجهاز الظاهري.

هذه القائمة المنسدلة متاحة إذا تم تحديد القيمة **نعم** أو **ليس هامًا** تم تحديد القيمة **هذا جهاز ظاهري** في القائمة المنسدلة.

- **جزء من البنية الأساسية لسطح المكتب الافتراضي**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- **ليس هامًا**.
- **لا**. البحث عن الأجهزة التي لا تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي.
- **نعم**. البحث عن الأجهزة التي تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI).

الأجهزة

في علامة التبويب **الأجهزة**، فيمكنك تكوين البحث عن أجهزة العميل حسب أجهزتها:

- **الجهاز**

يمكنك في القائمة المنسدلة تحديد نوع الوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.

يدعم الحقل البحث بالنص الكامل.

- **المورّد**

يمكنك في القائمة المنسدلة تحديد اسم الشركة المصنعة للوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.

يدعم الحقل البحث بالنص الكامل.

- **الوصف**

وصف الجهاز أو وحدة الجهاز. سيتم تضمين الأجهزة ذات الوصف المحدد في هذا الحقل في التحديد.

يمكن إدخال وصف الجهاز بأي تنسيق في نافذة خصائص هذا الجهاز. يدعم الحقل البحث بالنص الكامل.

- **رقم المخزون**

سيتم تضمين الأجهزة ذات رقم المخزون والمحدد في هذا الحقل في التحديد.

- **سرعة وحدة المعالجة المركزية (CPU) (بالميجاهرتز)**

نطاق تردد وحدة المعالجة المركزية. سيتم تضمين الأجهزة ذات وحدة المعالجة المركزية التي تتطابق مع نطاق التردد في حقوق الإدخال هذه (شامل) في التحديد.

- **مراكز CPU الظاهرية**

نطاق عدد النوى الظاهري في وحدة معالجة مركزية. سيتم تضمين أجهزة الكمبيوتر ذات وحدات المعالجة المركزية والتي تتطابق مع النطاق في حقوق الإدخال هذه (شامل) في التحديد.

- **حجم القرص الثابت بالجيجابايت**

نطاق القيم لحجم محرك القرص الثابت على الجهاز. سيتم تضمين الأجهزة ذات محركات الأقراص الثابتة والتي تطابق مع النطاق في حقوق الإدخال هذه (شامل) في التحديد.

- **حجم ذاكرة الوصول العشوائي RAM، بالميجابايت**

نطاق القيم لحجم ذاكرة الوصول العشوائي للجهاز. سيتم تضمين الأجهزة التي تحتوي على ذاكرة الوصول العشوائي، والتي تطابق النطاق في حقول الإدخال هذه (ضمناً) في التحديد.

الثغرات الأمنية والتحديثات

في تبويب **الثغرات الأمنية والتحديثات**، يمكنك إعداد معيار البحث عن الأجهزة بحسب مصدر تحديث Windows:

- **تم تبديل WUA إلى خادم الإدارة**

يمكنك تحديد خيار من خيارات البحث التالية من القائمة المنسدلة:

- **نعم**. إذا تم تحديد هذا الخيار، فستشتمل نتائج البحث على الأجهزة التي تتلقى تحديثات من خلال Windows Update من خادم الإدارة.
- **لا**. إذا تم تحديد هذا الخيار، ستشتمل النتائج الأجهزة التي تتلقى تحديثات من خلال Windows Update من مصادر أخرى.

المستخدمون

في علامة التبويب **المستخدمون**، يمكنك إعداد المعايير للبحث عن الأجهزة بحسب حسابات المستخدمين الذين قاموا بتسجيل الدخول إلى نظام التشغيل.

- **آخر مستخدم سجّل الدخول إلى النظام**

إذا تم تمكين هذا الخيار، فانقر فوق زر **استعراض** لتحديد حساب مستخدم. تشتمل نتائج البحث على الأجهزة التي قام مستخدم محدد بإجراء آخر تسجيل دخول عليها إلى النظام.

- **مستخدم قام بتسجيل الدخول إلى النظام مرة واحدة على الأقل**

إذا تم تمكين هذا الخيار، فانقر فوق زر **استعراض** لتحديد حساب مستخدم. ستتضمن نتائج البحث الأجهزة التي قام مستخدم محدد بتسجيل الدخول عليها مرة واحدة على الأقل.

مشاكل تؤثر على الحالة في التطبيقات المُدارة

في علامة التبويب **مشاكل تؤثر على الحالة في التطبيقات المُدارة**، يمكنك إعداد البحث عن الأجهزة بحسب أوصاف حالاتهم التي يوفرها التطبيق المُدار:

- **وصف حالة الجهاز**

يمكنك تحديد خانات الاختيار الخاصة بأوصاف الحالات من تطبيق مدار؛ وفور استلام هذه الحالات، سيتم تضمين الأجهزة في التحديد. في حالة اختيار حالة مدرجة للعديد من التطبيقات، فلديك الخيار لتحديد هذه الحالة في جميع القوائم تلقائيًا.

حالات المكونات في التطبيقات المُدارة

في علامة التبويب **حالات المكونات في التطبيقات المُدارة**، يمكنك إعداد المعايير للبحث عن الأجهزة بحسب حالات المكونات في التطبيقات المدارة:

- **حالة منع تسريب البيانات**

البحث عن الأجهزة حسب حالة منع تسرب البيانات (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **حالة الحماية الخاصة بتعاون الخوادم**

البحث عن الأجهزة حسب حالة حماية تعاون الخادم (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **حالة الحماية ضد الفيروسات الخاصة بخوادم البريد**

البحث عن الأجهزة حسب حالة حماية خادم البريد (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **حالة أداة استشعار نقطة النهاية**

البحث عن الأجهزة حسب حالة المكون أداة استشعار نقطة النهاية (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

التشفير

- **التشفير**

مقياس التشفير المتقدم (AES) خوارزمية التشفير الكتلي المتناظر. في القائمة المنسدلة، يمكنك تحديد حجم مفتاح التشفير (56 بت أو 128 بت أو 192 بت أو 256 بت).

القيم المتوفرة: AES56وAES128وAES192وAES256.

قطاعات السحابة

في علامة التبويب **قطاعات السحابة**، يمكنك تكوين البحث بناءً على ما إذا كان الجهاز ينتمي إلى قطاعات سحابة محددة:

- **الجهاز موجود ضمن قطاع السحابة**

إذا تم تمكين هذا الخيار، فيمكنك النقر فوق زر **استعراض** لتحديد قطاع البحث.

إذا تم أيضًا تمكين خيار **تضمين كائنات فرعية**، فسيتم تشغيل البحث في جميع الكائنات التابعة للقطاع المحدد.

البحث عن النتائج التي تشتمل فقط على أجهزة من القطاع المحدد.

- **تم اكتشاف الجهاز باستخدام واجهة برمجة التطبيقات**

يمكنك تحديد ما إذا كان تم اكتشاف الجهاز بواسطة أدوات API في القائمة المنسدلة:

- **AWS**. يتم اكتشاف الجهاز باستخدام AWS API، أي أن الجهاز يوجد بالفعل في بيئة سحابة AWS.
- **Azure**. يتم اكتشاف الجهاز باستخدام Azure API، أي أن الجهاز يوجد بالفعل في بيئة سحابة Azure.
- **Google Cloud**. يتم اكتشاف الجهاز باستخدام Google API، أي أن الجهاز موجود بالفعل في بيئة Google cloud.
- **لا**. لا يمكن اكتشاف الجهاز باستخدام AWS أو Azure أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة لكن لا يمكن اكتشافه باستخدام واجهة برمجة التطبيق (API).
- **لا توجد قيمة**. هذا الشرط لا ينطبق.

مكونات التطبيق

يحتوي هذا القسم على قائمة المكونات لهذه التطبيقات التي لديها مكونات إدارة إضافية مطابقة مُثبتة في وحدة تحكم الإدارة.

في القسم **مكونات التطبيق**، يمكنك تحديد معايير لتضمين الأجهزة في تحديد وفقًا للحالات ولأرقام الإصدار المكونات التي تشير للتطبيق الذي حددته:

- **الحالة**

البحث عن الأجهزة وفقًا لحالة المكون المُرسلة بواسطة تطبيق إلى خادم الإدارة. يمكنك تحديد أحد الحالات التالية: لا بيانات من الجهاز، أو متوقف، أو بدء التشغيل، أو تم الإيقاف مؤقتًا، أو قيد التشغيل، أو اختلال تشغيل أو غير مثبت. إذا كان للمكون المحدد للتطبيق المُثبت على جهاز مُدار حالة محددة، فإنه يتم تضمين الجهاز في تحديد الجهاز.

الحالات المرسلة بواسطة التطبيقات:

- بدء تشغيل—يكون المكون في عملية التهيئة في الوقت الحالي.
- قيد التشغيل—يكون المكون ممكنًا ويعمل على النحو الصحيح.
- تم الإيقاف مؤقتًا—تم تعليق المكون، على سبيل المثال، بعد إيقاف المستخدم للحماية مؤقتًا في التطبيق المُدار.
- اختلال التشغيل—حدث خطأ أثناء تشغيل المكون.
- متوقف—تم تعطيل المكون وهو لا يعمل في الوقت الحالي.
- غير مثبت—لم يقم المستخدم بتحديد المكون للتثبيت عند تكوين التثبيت المخصص للتطبيق.

بخلاف التطبيقات الأخرى، فإن الحالة لا بيانات من الجهاز لا تُرسل بواسطة التطبيقات. يُظهر هذا الخيار عدم امتلاك التطبيقات لمعلومات حول حالة المكون المحدد. على سبيل المثال، قد يحدث هذا عندما يكون المكون المحدد لا ينتمي لأي من التطبيقات المثبتة على الجهاز، أو عند إيقاف تشغيل الجهاز.

- **الإصدار**

البحث عن الأجهزة وفقًا لرقم الإصدار للمكون الذي حددته في القائمة. يمكنك كتابة رقم الإصدار، على سبيل المثال `3.4.1.0`، ثم تحديد ما إذا كان المكون المحدد يجب أن يمتلك إصدارًا مماثلاً أو إصدارًا سابقًا أو إصدارًا أحدث. يمكنك أيضًا تكوين البحث عن جميع الإصدارات عدا الإصدار المحدد.

استخدام الأقنعة في متغيرات السلسلة

يسمح باستخدام الأقنعة لمتغيرات السلسلة. عند إنشاء الأقنعة، يمكنك استخدام التعبيرات المعتادة التالية:

- حرف بدل (*)—أية سلسلة مكونة من 0 أو أكثر من الحروف.
- علامة استفهام (؟) —أي حرف مفرد.
- [<range>]—أي حرف فردي من نطاق أو مجموعة محددة.
  على سبيل المثال: [0–9] —أي رقم. [abcdef] - أي من الأحرف a، أو b، أو c، أو d، أو e، أو f.

استخدام تعبيرات عادية في حقل البحث

يمكنك استخدام التعبيرات العادية التالية في حقل البحث للبحث عن كلمات وأحرف محددة:

- *. تحل محل أي تسلسل من الأحرف. للبحث عن كلمات مثل Server، أو Servers، أو Server room، أدخل التعبير `Server*` في حقل البحث.
- ؟. تحل محل أي حرف مفرد. للبحث عن كلمات مثل Word أو Ward، أدخل التعبير `rd?W` في حقل البحث.

لا يمكن أن يبدأ النص في حقل البحث برمز. علامة الاستفهام (؟).

- [<نطاق>]. يستبدل أي حرف فردي من نطاق أو مجموعة محددة. للبحث عن أي رقم، أدخل التعبير `[0-9]` في حقل البحث. للبحث عن أحد الأحرف—a، أو b، أو c، أو d, e، أوf—أدخل التعبير `[abcdef]` في حقل البحث.

استخدم التعابير العادية التالية في حقل البحث لإجراء بحث النص الكامل:

- مسافة. النتيجة هي أجهزة الكمبيوتر التي يحتوي وصفها على أية كلمة من الكلمات المدرجة. للبحث عن عبارة تحتوي على كلمات مثل "تابع" أو كلمة "ظاهري" (أو كل منهما)، أدخل التعبير `تابع ظاهري` في حقل البحث.
- علامة الزائد (+)، أو AND أو &&. عندما تأتي علامة الزائد قبل كلمة، ستحتوي جميع نتائج البحث على هذه الكلمة. على سبيل المثال، للبحث عن عبارة تحتوي على كلمة "ثانوي" وكلمة "افتراضي"، يمكنك إدخال أي من التعبيرات التالية في حقل البحث: `+ثانوي+افتراضي`، `وثانوي AND افتراضي`، `وثانوي && افتراضي`.
- OR أو ||. عند وضعها بين كلمتين، فتشير إلى أن إحدى الكلمتين موجودة في النص. للبحث عن عبارة تحتوي على كلمة "ثانوي" أو كلمة "افتراضي"، يمكنك إدخال أحد التعبيرات التالية في حقل البحث: `ثانوي OR افتراضي` أو `ثانوي || افتراضي`.
- علامة ناقص (-). عندما تأتي علامة الناقص قبل كلمة، لن تحتوي نتائج البحث على هذه الكلمة. للبحث عن عبارة يجب أن تحتوي على كلمة "تابع" ويجب ألا تحتوي على كلمة "ظاهري"، يجب أن تقوم بإدخال التعبير `+تابع -ظاهري` في حقل البحث.
- "< بعض النص >". النص الموضوع بين علامتي الاقتباس يجب أن يكون موجودًا في النص. للبحث عن عبارة تجمع بين الكلمتين Secondary Server، يجب أن تقوم بإدخال التعبير `" Secondary Server "` في حقل البحث.

البحث عن النص الكامل متاح في كتل التصفية التالية:

- في كتلة تصفية قائمة الحدث، بواسطة أعمدة **الحدث** وأعمدة **الوصف**.
- في كتلة تصفية حساب المستخدم، بواسطة عمود **الاسم**.
- في كتلة تصفية سجل التطبيقات، حسب العمود **الاسم**، إذا كان القسم **إظهار في القائمة** فيه خاصية **بدون تجميع** محددة باعتبارها معيار التصفية.

تصدير القوائم من مربعات الحوار

في مربعات حوار التطبيق، يمكنك تصدير قوائم الكائنات إلى ملفات نصية.

يمكن تصدير قائمة كائنات لأقسام مربعات الحوار التي تحتوي على الزر **تصدير إلى ملف**.

إعدادات المهام

يسرد هذا القسم جميع إعدادات المهام في Kaspersky Security Center.

إعدادات المهمة العامة

يحتوي هذا القسم على الإعدادات التي يمكنك عرضها وتكوينها لمعظم مهامك. وتعتمد قائمة الإعدادات المتاحة على المهمة التي تكوّنها.

الإعدادات المحددة أثناء إنشاء المهمة

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضًا تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

- إعدادات إعادة تشغيل نظام التشغيل:

- **لا تقم بإعادة تشغيل الجهاز**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **أعد تشغيل الجهاز**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **مطالبة المستخدم باتخاذ إجراء**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **تكرار المطالبة كل (بالدقائق)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **إعادة التشغيل بعد (دقيقة)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- إعدادات جدولة المهام:

قد تختلف أنواع الجدول الزمني حسب المهمة.

- **إعداد البدء المُجدول:**

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N يومًا**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **يدويًا**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- Once

يتم تشغيل المهمة مرة واحدة، في التاريخ والوقت المحددين (افتراضيًا، في اليوم الذي تم إنشاء المهمة فيه).

- Immediately

تعمل المهمة على الفور بعد حفظ إعداداتها.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند تنزيل تحديثات جديدة إلى المستودع**

تعمل المهمة بعد تنزيل التحديثات إلى المستودع. على سبيل المثال، قد ترغب في استخدام هذا الجدول للبحث عن الثغرات الأمنية ومهمة التحديثات المطلوبة.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدم التأخير العشوائي لبدء المهام تلقائيًا**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

- الأجهزة التي سيتم تعيين المهمة إليها:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة**

يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لمهمة تثبيت عميل الشبكة على الأجهزة غير المخصصة.

- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**

يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

- **تعيين مهمة إلى تحديد الجهاز**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

- **تعيين مهمة لمجموعة إدارة**

يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

- إعدادات الحساب:

- **الحساب الافتراضي**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.

يتم تحديد هذا الخيار افتراضيًا.

- **تحديد حساب**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **الحساب**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **كلمة المرور**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

إذا لم يتم تثبيت عميل الشبكة على جهازك المستهدف، فيجب عليك تحديد الحساب الذي سيتم استخدامه على الجهاز المستهدف للوصول إلى مشاركة $admin. يكون الغرض من الحساب الذي تحدده هو نسخ البيانات إلى جهازك فقط. في حالة تثبيت عميل الشبكة على جهازك المستهدف، يتم نسخ البيانات من خلال عميل الشبكة، ولا يلزمك تحديد أي حساب عند إنشاء المهمة.

الإعدادات المحددة بعد إنشاء المهمة

يمكنك تحديد الإعدادات التالية بعد إنشاء المهمة فقط.

- إعدادات المهمة الجماعية:

- **التوزيع للمجموعات الفرعية**

هذا الخيار متاح فقط في إعدادات مهام المجموعة.

عند تمكين هذا الخيار، يتضمن نطاق المهمة ما يلي:

- مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.

- مجموعات الإدارة التابعة لمجموعة الإدارة المحددة على أي مستوى لأسفل من خلال التسلسل الهرمي للمجموعة.

عند تعطيل هذا الخيار، فإن نطاق المهمة يتضمن فقط مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.

يتم تمكين هذا الخيار افتراضيًا.

- **توزيع إلى خوادم الإدارة الثانوية والافتراضية**

عند تمكين هذا الخيار، يتم أيضًا تطبيق المهمة الفعالة على خادم الإدارة الأساسي على خوادم الإدارة الثانوية (بما في ذلك الخوادم الافتراضية). إذا كانت هناك مهمة من نفس النوع موجودة بالفعل على خادم الإدارة الثانوي، فسيتم تطبيق كلا المهمتين على خادم الإدارة الثانوي – المهمة الحالية والموروثة من خادم الإدارة الأساسي.

لا يتوفر هذا الخيار إلا عند تمكين خيار **التوزيع للمجموعات الفرعية**.

يتم تعطيل هذا الخيار افتراضيًا.

- إعدادات الجدولة المتقدمة:

- **قم بتشغيل الأجهزة باستخدام وظيفة Wake-on-LAN قبل بدء المهمة (دقيقة)**

يبدأ نظام التشغيل الموجود على الجهاز في الوقت المحدد قبل بدء المهمة. الفترة الزمنية الافتراضية هي خمس دقائق.

قم بتمكين هذا الخيار إذا كنت تريد تشغيل المهمة على جميع الأجهزة العميلة من نطاق المهام، بما في ذلك تلك الأجهزة التي تم إيقاف تشغيلها عندما تكون المهمة على وشك البدء.

إذا كنت تريد إيقاف تشغيل الجهاز تلقائيًا بعد اكتمال المهمة، فقم بتمكين خيار **أغلق الأجهزة بعد الانتهاء من المهمة**. يمكن العثور على هذا الخيار في النافذة نفسها.

يتم تعطيل هذا الخيار افتراضيًا.

- **أغلق الأجهزة بعد الانتهاء من المهمة**

على سبيل المثال، قد ترغب في تمكين هذا الخيار لمهمة تحديث تثبيت والتي تقوم بتثبيت التحديثات على الأجهزة العميلة كل يوم جمعة بعد ساعات العمل، ثم تقوم بإيقاف تشغيل هذه الأجهزة لعطلة نهاية الأسبوع.

يتم تعطيل هذا الخيار افتراضيًا.

- **أوقف المهمة إذا كانت أطول من (دقيقة)**

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائيًا، سواء أكانت مكتملة أم لا.

قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتًا طويلاً للتنفيذ.

يتم تعطيل هذا الخيار افتراضيًا. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

- إعدادات الإخطار:

- كتلة **تخزين محفوظات المهمة**:

- **على خادم الإدارة لمدة (بالأيام)**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام على خادم الإدارة خلال عدد الأيام المحدد. وعند انقضاء هذه الفترة الزمنية، يتم حذف المعلومات من خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **تخزين في سجل أحداث نظام التشغيل (OS)على جهاز**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة محليًا في سجل أحداث Windows لكل جهاز عميل.

يتم تعطيل هذا الخيار افتراضيًا.

- **تخزين في سجل أحداث نظام التشغيل (OS) على خادم إدارة**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام مركزيًا في سجل أحداث Windows لنظام تشغيل خادم الإدارة (OS).

يتم تعطيل هذا الخيار افتراضيًا.

- **حفظ كل الأحداث**

إذا تم تحديد هذا الخيار، فسيتم حفظ جميع الأحداث المتعلقة بالمهمة في سجلات الأحداث.

- **حفظ الأحداث المتعلقة بتقدم المهمة**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بتنفيذ المهمة في سجلات الأحداث.

- **حفظ نتائج تنفيذ المهمة فقط**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بنتائج المهمة في سجلات الأحداث.

- **إخطار المسؤول بنتائج تنفيذ المهمة**

يمكنك تحديد الطرق التي يتلقى بها المسؤولون إخطارات حول نتائج تنفيذ المهام: عن طريق البريد الإلكتروني، والرسائل النصية القصيرة، وعن طريق تشغيل ملف تنفيذي. لتكوين الإخطار، انقر فوق الرابط **إعدادات**.

يتم تعطيل جميع أساليب الإخطارات بصورة افتراضية.

- **إخطار بالأخطاء فقط**

إذا تم تمكين هذا الخيار، فسيتم إخطار المسؤولين فقط عند اكتمال تنفيذ المهمة مع وجود خطأ.

إذا تم تعطيل هذا الخيار، فسيتم إخطار المسؤولين بعد اكتمال تنفيذ كل مهمة.

يتم تمكين هذا الخيار افتراضيًا.

- إعدادات الأمن
- إعدادات نطاق المهمة

اعتمادًا على كيفية تحديد نطاق المهام، تكون الإعدادات التالية موجودة:

- **الأجهزة**

إذا تم تحديد نطاق المهمة بواسطة مجموعة إدارة، فيمكنك عرض هذه المجموعة. لا توجد تغييرات متاحة هنا. ومع ذلك، يمكنك إعداد **الاستثناءات من نطاق المهمة**.

إذا تم تحديد نطاق مهمة ما بواسطة قائمة من الأجهزة، فيمكنك تعديل هذه القائمة بإضافة أجهزة وإزالتها.

- **تحديد الجهاز**

يمكنك تغيير تحديد الجهاز الذي يتم تطبيق المهمة عليه.

- **الاستثناءات من نطاق المهمة**

يمكنك تحديد مجموعات الأجهزة التي لا يتم تطبيق المهمة عليها. يمكن أن تكون المجموعات المراد استثنائها مجموعات فرعية فقط من مجموعة الإدارة التي يتم تطبيق المهمة عليها.

- **سجل المراجعة**

تنزيل التحديثات إلى إعدادات مهمة مستودع خادم الإدارة

الإعدادات المحددة أثناء إنشاء المهمة

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضًا تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

- **مصادر التحديثات**

ويمكن استخدام الموارد التالية كمصدر للتحديثات لخادم الإدارة:

- خوادم تحديث Kaspersky

خوادم (S)HTTP في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق. يتصل خادم الإدارة افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة لاستخدام بروتوكول HTTP بدلاً من HTTPS.

يتم تحديده بصورة افتراضية.

- خادم الإدارة الأساسي

ينطبق هذا المصدر على المهام التي يتم إنشاؤها لخادم الإدارة الثانوي أو الافتراضي.

- المجلد المحلي أو مجلد الشبكة

مجلد شبكة أو مجلد محلي يحتوي على آخر التحديثات. يمكن أن يكون مجلد الشبكة إما خادم FTP أو خادم HTTP أو مشاركة SMB. إذا تطلب مجلد الشبكة المصادقة، فسيتم دعم بروتوكول SMB فقط. عند تحديد مجلد محلي، يجب عليك تحديد مجلد موجود على الجهاز المُثبت عليه خادم الإدارة.

يجب أن يحتوي مجلد الشبكة أو خادم FTP أو HTTP المستخدم من قبل مصدر التحديث على بنية مجلدات (مع تحديثات) تتطابق مع البنية التي تم إنشاؤها عند استخدام خوادم تحديث Kaspersky.

- **إعدادات أخرى**

فرض التحديث لخوادم الإدارة الثانوية

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة بتشغيل مهام التحديث على خوادم الإدارة الثانوية بمجرد أن يتم تنزيل التحديثات الجديدة. تبدأ مهام التحديث باستخدام مصدر التحديث الذي تم تكوينه في خصائص المهمة على خوادم الإدارة الثانوية.

إذا تم تعطيل هذا الخيار، فستبدأ مهام التحديث على خوادم الإدارة الثانوية وفقًا لجداولها الزمنية.

يتم تعطيل هذا الخيار افتراضيًا.

نسخ التحديثات التي تم تنزيلها إلى مجلدات إضافية

بعد تلقي خادم الإدارة للتحديثات، يقوم بنسخها إلى المجلدات المحددة. استخدم هذا الخيار في حال رغبت في إدارة توزيع التحديثات يدويًا على الشبكة الخاصة بك.

على سبيل المثال، قد ترغب في استخدام هذا الخيار في الموقف التالي: تتكون شبكة المؤسسة الخاصة بك من العديد من الشبكات الفرعية المستقلة، ولا تمتلك الأجهزة على كل شبكة فرعية إمكانية الوصول إلى الشبكات الفرعية الأخرى. ومع ذلك فإن جميع الأجهزة في جميع الشبكات الفرعية تمتلك إمكانية الوصول إلى مشاركة الشبكة العامة. في هذه الحالة، قم بتعيين خادم الإدارة في واحدة من الشبكات الفرعية لتنزيل التحديثات من خوادم تحديث Kaspersky، وقم بتمكين هذا الخيار ثم حدد مشاركة الشبكة هذه. من تنزيل التحديثات إلي مستودع المهام لخوادم إدارة أخرى، قم بتحديد نفس مشاركة الشبكة كمصدر تحديث.

إذا حددت نسخ التحديثات التي تم تنزيلها إلى مجلد محلي، فيجب عليك تحديد مجلد على الجهاز الذي تم تثبيت خادم الإدارة عليه. ويعتمد المسار إلى المجلد على نظام تشغيل الجهاز. ونظرًا لوجود المجلد المحلي على خادم الإدارة المستند إلى نظام Linux، فيجب عليك تحديد مسار POSIX، على سبيل المثال: /path/to/dir.

عند تحديد مجلد شبكة موجود على خادم الإدارة المستند إلى نظام Linux، يجب عليك التأكد من إمكانية الوصول إلى مجلد الشبكة مسبقًا من الجهاز المُثبت عليه خادم الإدارة عن طريق تحميل المجلد. ويتم تنفيذ الوصول إلى المجلد باستخدام بروتوكول SMB.

يتم تعطيل هذا الخيار افتراضيًا.

لا تفرض تحديث الأجهزة وخوادم الإدارة الثانوية إلا عند اكتمال النسخ

تبدأ مهام تنزيل التحديثات على الأجهزة العميلة وخوادم الإدارة الثانوية فقط بعد نسخ تلك التحديثات من مجلد التحديث الرئيسي إلى مجلدات التحديث الإضافية.

يجب تمكين هذا الخيار إذا كانت الأجهزة العميلة وخوادم الإدارة الثانوية تقوم بتنزيل تحديثات من مجلدات شبكة إضافية.

يتم تعطيل هذا الخيار افتراضيًا.

الإعدادات المحددة بعد إنشاء المهمة

يمكنك تحديد الإعدادات التالية بعد إنشاء المهمة فقط.

- **إعدادات** القسم، **محتوى التحديثات** حظر

تنزيل ملفات تفاضلية

يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.

يتم تعطيل هذا الخيار افتراضيًا.

- قسم **التحقق من صحة التحديث**

التحقق من صحة التحديثات قبل التوزيع

سيقوم خادم الإدارة بتنزيل التحديثات من المصدر، وحفظها في مستودع مؤقت، وتشغيل المهمة المحددة في حقل **مهمة التحقق من صحة التحديث**. في حالة اكتمال المهمة بنجاح، يتم نسخ التحديثات من المخزون المؤقت إلى مجلد مشترك على خادم الإدارة ثم توزيعها على جميع الأجهزة التي يعمل عليها خادم الإدارة كمصدر للتحديثات (يتم بدء المهام التي تحتوي على نوع الجدول **عند تنزيل تحديثات جديدة إلى المستودع**). تنتهي مهمة تنزيل التحديثات إلى المستودع فقط بعد اكتمال مهمة التحقق من صحة التحديث.

يتم تعطيل هذا الخيار افتراضيًا.

مهمة التحقق من صحة التحديث

تقوم هذه المهمة بالتحقق من التحديثات التي تم تنزيلها قبل أن يتم توزيعها على جميع الأجهزة التي يعمل عليها خادم الإدارة كمصدر للتحديثات.

في هذا الحقل، يمكنك تحديد مهمة التحقق من صحة التحديث التي تم إنشاؤها مسبقًا. وبدلاً من ذلك، يمكنك إنشاء مهمة التحقق من صحة التحديث الجديدة.

إعدادات مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

الإعدادات المحددة أثناء إنشاء المهمة

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضًا تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

- **مصادر التحديثات**

يمكن استخدام الموارد التالية كمصدر لتحديثات نقطة التوزيع:

- خوادم تحديث Kaspersky

خوادم (S)HTTP في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق.

ويتم تحديد هذا الخيار بصورة افتراضية.

- خادم الإدارة الأساسي

ينطبق هذا المصدر على المهام التي يتم إنشاؤها لخادم الإدارة الثانوي أو الافتراضي.

- المجلد المحلي أو مجلد الشبكة

مجلد شبكة أو مجلد محلي يحتوي على آخر التحديثات. يمكن أن يكون مجلد الشبكة إما خادم FTP أو خادم HTTP أو مشاركة SMB. إذا تطلب مجلد الشبكة المصادقة، فسيتم دعم بروتوكول SMB فقط. عند تحديد مجلد محلي، يجب عليك تحديد مجلد موجود على الجهاز المُثبت عليه خادم الإدارة.

> يجب أن يحتوي مجلد الشبكة أو خادم FTP أو HTTP المستخدم من قبل مصدر التحديث على بنية مجلدات (مع تحديثات) تتطابق مع البنية التي تم إنشاؤها عند استخدام خوادم تحديث Kaspersky.

- **إعدادات أخرى ← مجلد لتخزين التحديثات**

المسار إلى المجلد المحدد لتخزين التحديثات المحفوظة. يمكنك نسخ مسار المجلد المحدد إلى الحافظة. لا يمكنك تغيير المسار إلى مجلد محدد لمهمة جماعية.

الإعدادات المحددة بعد إنشاء المهمة

يمكنك تحديد الإعداد التالي في قسم **إعدادات**، في كتلة **محتوى التحديثات** فقط بعد إنشاء المهمة.

تنزيل ملفات تفاضلية

يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.

يتم تعطيل هذا الخيار افتراضيًا.

البحث عن الثغرات الأمنية والإعدادات المطلوبة لمهمة التحديثات

الإعدادات المحددة أثناء إنشاء المهمة

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضًا تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

- **تم إدراج البحث عن الثغرات الأمنية والتحديثات بواسطة Microsoft**

عند البحث عن الثغرات الأمنية والتحديثات، يستخدم Kaspersky Security Center المعلومات حول تحديثات Microsoft القابلة للتطبيق من مصدر تحديثات Microsoft، المتوفرة في الوقت الحالي.

على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft وتحديثات تطبيقات لجهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

لم يتم إرسال المعلومات المتعلقة بتحديثات Microsoft Windows الاختيارية إلى خادم الإدارة.

- **الاتصال بخادم التحديث لتحديث البيانات**

يتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft. يمكن أن تعمل الخوادم التالية كمصدر لتحديثات Microsoft:

- خادم إدارة Kaspersky Security Center (راجع إعدادات سياسة عميل الشبكة)
- خادم Windows مع خدمات تحديث خادم Microsoft Windows (WSUS) المنشورة في شبكة مؤسستك
- خوادم تحديثات Microsoft

إذا تم تمكين هذا الخيار، فسيتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft لتحديث المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق.

إذا تم تعطيل هذا الخيار، فسيستخدم عميل تحديث Windows على جهاز مُدار المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقتٍ سابق.

يمكن أن يكون الاتصال بمصدر تحديثات Microsoft مستهلكًا للموارد. قد ترغب في تعطيل هذا الخيار، إذا قمت بتعيين اتصال منتظم لمصدر التحديثات هذا في مهمة أخرى أو في خصائص سياسة وكلاء الشبكة في قسم **تحديثات البرنامج والثغرات الأمنية**. إذا كنت لا ترغب في تعطيل هذا الخيار، إذن لتقليل التحميل الزائد على الخادم، يمكنك تكوين جدول المهام لترتيب عملية تأخير بدء المهمة عشوائيًا في غضون 360 دقيقة.

يتم تمكين هذا الخيار افتراضيًا.

يحدد مزيج الخيارات التالية لإعدادات سياسة وكلاء الشبكة طريقة الحصول على التحديثات:

- يتصل عميل Windows Update الموجود على جهاز مُدار بخادم التحديث للحصول على التحديثات فقط في حالة تمكين الخيار **الاتصال بخادم التحديث لتحديث البيانات** في خصائص مهمة Find vulnerabilities and required updates وتم تعيين الخيار **وضع بحث تحديث Windows** على **نشط** في إعدادات سياسة عميل الشبكة.

- إذا لم تكن بحاجة إلى عميل الشبكة لبدء الاتصال بمصدر تحديث Microsoft Windows وتنزيل التحديثات عند إجراء مهمة فحص الثغرات الأمنية، يمكنك ضبط الخيار **وضع بحث تحديث Windows** على **سلبي**، بينما يجب أن يظل الخيار **الاتصال بخادم التحديث لتحديث البيانات** قيد التمكين. ويتيح لك ذلك توفير الموارد واستخدام تحديثات Windows التي تم سبق تلقيها للبحث عن الثغرات الأمنية. ويمكنك استخدام الوضع السلبي إذا كونت تلقي تحديثات Microsoft Windows بطريقة مختلفة. إذا لم يتم تكوين تلقي تحديثات Microsoft Windows بطريقة أخرى، فلا تقم بتعيين الخيار **وضع بحث تحديث Windows** على **سلبي**، لأنه في هذه الحالة، لن يتم تلقي معلومات عن التحديثات مطلقًا.

- بغض النظر عن حالة الخيار **الاتصال بخادم التحديث لتحديث البيانات** (تم تمكينه أو تم تعطيله)، ففي حالة ضبط الخيار **وضع بحث تحديث Windows** على **معطل**، لا يطلب Kaspersky Security Center أي معلومات عن التحديثات.

- **تم إدراج البحث عن الثغرات الأمنية من جهة خارجية والتحديثات بواسطة برنامج Kaspersky**

في حالة تمكين هذا الخيار، فسيبحث Kaspersky Security Center عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في سجل Windows وفي المجلدات المحددة ضمن **تحديد مسارات للبحث المتقدم للتطبيقات في نظام الملفات**. تدار القائمة الكاملة لتطبيقات الجهة الخارجية المدعومة بواسطة Kaspersky.

إذا تم تعطيل هذا الخيار، فلن يقوم Kaspersky Security Center بالبحث عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية. على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft Windows وتحديثات تطبيقات جهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

- **تحديد مسارات للبحث المتقدم للتطبيقات في نظام الملفات**

المجلدات التي يبحث فيها Kaspersky Security Center عن تطبيقات الجهة الخارجية والتي تتطلب إصلاح الثغرات الأمنية وتثبيت التحديث. يمكنك استخدام متغيرات النظام.

حدد المجلدات التي يتم تثبيت التطبيقات بها. تحتوي القائمة بشكلٍ افتراضي على مجلدات النظام التي يتم تثبيت معظم التطبيقات بها.

- **تمكين التشخيصات المتقدمة**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

قم بتثبيت التحديثات المطلوبة وضبط إعدادات مهمة إصلاح الثغرات الأمنية

الإعدادات المحددة أثناء إنشاء المهمة

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضًا تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

- **حدد قواعد لتثبيت التحديثات**

يتم تطبيق تلك القواعد على تثبيت التحديثات على الأجهزة العميلة. إذا لم يتم تحديد قواعد، فلن تقوم المهمة بتنفيذ أي شيء. للحصول على معلومات حول عمليات التشغيل من خلال القواعد، راجع قواعد لتثبيت التحديثات.

- **بدء التثبيت بعد إعادة تشغيل الجهاز أو إيقاف تشغيله**

إذا تم تمكين هذا الخيار، فسيتم تثبيت التحديثات عند إعادة تشغيل الجهاز أو إغلاقه. بخلاف ذلك، يتم تثبيت التحديثات وفقًا لجدول زمني.

استخدم هذا الخيار في حال كان تنزيل التحديثات قد يؤثر على أداء الجهاز.

يتم تعطيل هذا الخيار افتراضيًا.

- **تثبيت مكونات النظام العام المطلوبة**

إذا تم تمكين هذا الخيار، قبل تثبيت التحديث، يقوم التطبيق تلقائيًا بتثبيت كافة مكونات النظام العامة (المتطلبات الأساسية) اللازمة لتثبيت التحديث. على سبيل المثال، يمكن أن تكون تلك المتطلبات الأساسية عبارة عن تحديثات نظام التشغيل.

إذا تم تعطيل هذا الخيار، فقط يتعين عليك تثبيت المتطلبات الأساسية يدويًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **السماح بتثبيت إصدارات التطبيق الجديدة أثناء التحديثات**

إذا تم تمكين هذا الخيار، سيتم السماح بالتحديثات التي تؤدي إلى تثبيت إصدار جديد من تطبيق البرنامج.

إذا تم تعطيل هذا الخيار، فلن تتم ترقية البرنامج. بعد ذلك يمكنك تثبيت إصدارات البرنامج الجديدة يدويًا أو من خلال مهمة أخرى. على سبيل المثال، قد تستخدم هذا الخيار في حال كانت البنية الأساسية الخاصة بشركتك غير مدعومة بواسطة إصدار جديد للبرنامج أو في حال رغبت في التحقق من ترقية في اختبار البنية الأساسية.

يتم تمكين هذا الخيار افتراضيًا.

قد تؤدي ترقية التطبيق إلى حدوث خلل في التطبيقات التابعة المثبتة على أجهزة عميلة.

- **تنزيل التحديثات على الجهاز دون تثبيتها**

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بتنزيل التحديثات على الجهاز ولكن لن يقوم بتنزيلها تلقائيًا. بعد ذلك يمكنك تثبيت التحديثات التي تم تنزيلها يدويًا.

تم تنزيل تحديثات Microsoft إلى مخزن Windows في النظام. يتم تنزيل تحديثات تطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في المجلد المحدد في حقل **تنزيل التحديثات إلى**.

إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائيًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **تنزيل التحديثات إلى**

يتم استخدام هذا المجلد لتنزيل تحديثات خاصة بتطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky وMicrosoft).

- **تمكين التشخيصات المتقدمة**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

الإعدادات المحددة بعد إنشاء المهمة

يمكنك تحديد الإعدادات في الأقسام المدرجة أدناه فقط بعد إنشاء المهمة. للحصول على وصف كامل لإعدادات المهمة، راجع إعدادات المهمة العامة.

- **عام**. في هذا القسم، يتم عرض معلومات عامة حول المهمة. يمكنك أيضًا تحديد الأجهزة التي يجب أن تنطبق عليها مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية:

  - **التوزيع للمجموعات الفرعية**

    هذا الخيار متاح فقط في إعدادات مهام المجموعة.

    عند تمكين هذا الخيار، يتضمن نطاق المهمة ما يلي:

    - مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.

    - مجموعات الإدارة التابعة لمجموعة الإدارة المحددة على أي مستوى لأسفل من خلال التسلسل الهرمي للمجموعة.

    عند تعطيل هذا الخيار، فإن نطاق المهمة يتضمن فقط مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.

    يتم تمكين هذا الخيار افتراضيًا.

  - **توزيع إلى خوادم الإدارة الثانوية والافتراضية**

    عند تمكين هذا الخيار، يتم أيضًا تطبيق المهمة الفعالة على خادم الإدارة الأساسي على خوادم الإدارة الثانوية (بما في ذلك الخوادم الافتراضية). إذا كانت هناك مهمة من نفس النوع موجودة بالفعل على خادم الإدارة الثانوي، فسيتم تطبيق كلا المهمتين على خادم الإدارة الثانوي – المهمة الحالية والموروثة من خادم الإدارة الأساسي.

    لا يتوفر هذا الخيار إلا عند تمكين خيار **التوزيع للمجموعات الفرعية**.

    يتم تعطيل هذا الخيار افتراضيًا.

- التحديثات المراد تثبيتها

  في القسم **تحديثات للتثبيت**، يمكنك عرض قائمة التحديثات التي تقوم المهمة بتثبيتها. يتم فقط عرض التحديثات المتوافقة مع إعدادات المهمة المطبقة.

- اختبار تثبيت التحديثات:

  - **عدم الفحص**. حدد هذا الخيار إذا كنت لا ترغب في إجراء تثبيت اختباري للتحديثات.

  - **تشغيل الفحص على الأجهزة المحددة**. حدد هذا الخيار إذا كنت ترغب في اختبار تثبيت التحديثات على الأجهزة المحددة. انقر فوق الزر **إضافة** وحدد الأجهزة التي تحتاج إلى إجراء تثبيت اختباري للتحديثات عليها.

- **تشغيل الفحص على الأجهزة في المجموعة المحددة**. حدد هذا الخيار إذا كنت ترغب في اختبار تثبيت التحديثات على مجموعة الأجهزة. في الحقل **تحديد مجموعة اختبار**، حدد مجموعة الأجهزة التي تريد إجراء تثبيت اختباري عليها.

- **تشغيل الفحص على النسبة المئوية المحددة من الأجهزة**. حدد هذا الخيار إذا كنت ترغب في اختبار تثبيت التحديثات على بعض أجزاء الأجهزة. في الحقل **نسبة أجهزة الاختبار من كل الأجهزة الهدف**، حدد نسبة الأجهزة التي تريد إجراء تثبيت اختباري للتحديثات عليها.

القائمة العمومية للشبكات الفرعية

يقدم هذا القسم معلومات حول القائمة العمومية للشبكات الفرعية التي يمكنك استخدامها في القواعد.

لتخزين المعلومات حول الشبكات الفرعية لشبكتك، يمكنك إعداد قائمة عمومية بالشبكات الفرعية لكل خادم إدارة تقوم باستخدامه. تساعدك هذه القائمة في مطابقة الأزواج {عنوان IP، القناع} والوحدات الفعلية كمكاتب الفروع. يمكنك استخدام الشبكات الفرعية من هذه القائمة في قواعد وإعدادات الشبكة.

إضافة شبكات فرعية إلى القائمة العمومية للشبكات الفرعية

يمكنك إضافة شبكات فرعية مع أوصافها إلى القائمة العمومية للشبكات الفرعية.

لإضافة شبكة فرعية إلى القائمة العمومية للشبكات الفرعية:

1. حدد من شجرة وحدة التحكم عقدة خادم الإدارة الذي تطلبه.

2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.

3. من النافذة **خصائص** المهمة التي تفتح، في الجزء **الأقسام**، حدد **قائمة عالمية للشبكات الفرعية**.

4. انقر فوق الزر **إضافة**.
   يتم فتح النافذة **شبكة فرعية جديدة**.

5. املأ الحقول التالية:

- **الإعدادات العامة**

عنوان IP الشبكة الفرعية للشبكة الفرعية التي تضيفها.

- **قناع الشبكة الفرعية**

قناع الشبكة الفرعية للشبكة الفرعية التي تقوم بإضافتها.

- **الاسم**

اسم الشبكة الفرعية. يجب أي يكون فريدًا ضمن القائمة العمومية للشبكات الفرعية. إذا قمت بإضافة الاسم الموجود بالفعل في القائمة، ستتم إضافة فهرس، على سبيل المثال: ~~1، ~~2.

- **الوصف**

قد يشتمل الوصف على بعض المعلومات الإضافية حول مكتب الفرع الذي لديه هذه الشبكة الفرعية. سيظهر هذا النص في جميع القوائم التي تكون فيها هذه الشبكة الفرعية، على سبيل المثال، في قائمة قواعد تقييد حركة المرور.

هذا الحقل ليس إلزاميًا ويمكن تركه فارغًا.

6. انقر على **موافق**.

تظهر الشبكة الفرعية في قائمة الشبكات الفرعية.

عرض وتعديل خصائص الشبكة الفرعية في القائمة العمومية للشبكات الفرعية

يمكنك عرض وتعديل خصائص الشبكات الفرعية في القائمة العمومية للشبكات الفرعية.

لعرض أو تعديل خصائص الشبكة الفرعية في القائمة العمومية للشبكات الفرعية:

1. حدد من شجرة وحدة التحكم عقدة خادم الإدارة الذي تطلبه.
2. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
3. في النافذة **الخصائص** التي تفتح، حدد **قائمة عالمية للشبكات الفرعية** من الجزء الأيسر **الأقسام**.
4. في القائمة، حدد الشبكة الفرعية التي تريدها.
5. انقر على زر **خصائص**.

   يتم فتح النافذة **شبكة فرعية جديدة**.
6. إذا لزم الأمر، قم بتغيير إعدادات الشبكة الفرعية.
7. انقر على **موافق**.

إذا قمت بإجراء تغييرات، سيتم تخزينهم.

استخدام عميل الشبكة لأنظمة التشغيل Windows وLinux وmacOS: المقارنة

استخدام عميل الشبكة يتنوع اعتمادًا على نظام التشغيل على الجهاز. تختلف أيضًا إعدادات سياسة عميل الشبكة وحزمة التثبيت بناءً على نظام التشغيل. الجدول أدناه يقارن بين ميزات عميل الشبكة وسيناريوهات الاستخدام المتوفرة لأنظمة التشغيل Windows وmacOS وLinux.

مقارنة ميزة عميل الشبكة

ميزة عميل الشبكة	Windows	Linux	macOS
التثبيت:			
الإنشاء التلقائي لحزمة تثبيت عميل الشبكة بعد تثبيت Kaspersky Security Center	✓	—	—
التثبيت في الوضع الإجباري، استخدام خيارات خاصة في مهمة التثبيت عن بُعد لـ Kaspersky Security Center.	✓	✓	✓
التثبيت عن طريق إرسال روابط الحزم المستقلة التي يتم إنشاؤها بواسطة Kaspersky Security Center إلى مستخدمي الجهاز.	✓	✓	✓
التثبيت عن طريق استنساخ صورة لمحرك القرص الثابت الخاص بالمسؤول والمثبت عليه نظام التشغيل وعميل الشبكة: استخدام الأدوات المقدمة من Kaspersky Security Center للتعامل مع صور القرص.	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	—	—

ميزة عميل الشبكة	Windows	Linux	macOS
التثبيت عن طريق استنساخ صورة لمحرك الأقراص الثابتة الخاص بالمسؤول باستخدام نظام التشغيل ووكيل الشبكة باستخدام أدوات الجهات الخارجية	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓	✓
التثبيت باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد	✓	✓	✓
التثبيت يدويًا، عن طريق تشغيل مثبّتات التطبيق على الأجهزة	✓	✓	✓
تثبيت عميل الشبكة في الوضع الصامت	✓	✓	✓
اتصال جهاز عميل بخادم الإدارة يدويًا. الأداة المساعدة klmover	✓	✓	✓
التثبيت التلقائي للتحديثات والتصحيحات المخصصة لمكونات Kaspersky Security Center	✓	✓	—
التوزيع التلقائي لمفتاح	✓	✓	✓
المزامنة المفروضة	✓	✓	✓ باستثناء خادم الإرسال التلقائي
نقطة توزيع			
استخدام نقطة توزيع	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓	✓
حساب عدد نقاط التوزيع وتكوينهم	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓ بدون استخدام الوعي بموقع الشبكة (NLA).	✓ بدون استخدام الوعي بموقع الشبكة (NLA).
استقصاء الشبكة	✓ • استقصاء شبكة Windows • استقصاء نطاق IP • استقصاء وحدة التحكم في المجال (Microsoft Active Directory) القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓ • استقصاء نطاق IP • استطلاع شبكة لا تتطلب تكوينًا • استقصاء وحدة التحكم في المجال (Microsoft Active Directory، Samba 4 Active Directory)	—
تشغيل خدمة وكيل KSN على جانب نقطة التوزيع	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓	—
تنزيل التحديثات عبر خوادم تحديث Kaspersky إلى مستودعات نقاط التوزيع التي توزع التحديثات على الأجهزة المدارة	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓	— (في حال وجود جهاز أو أكثر من الأجهزة التي تعمل بنظام Linux أو macOS داخل نطاق مهمة تنزيل التحديثات في مستودعات نقاط التوزيع، تكتمل المهمة مع ظهور حالة فشل، حتى إذا تم إكمالها بنجاح على جميع أجهزة Windows).
تثبيت التطبيقات	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	مقيد: لا يمكن إجراء التثبيت الفوري على أجهزة Windows باستخدام نقاط توزيع Linux.	مقيد: لا يمكن إجراء التثبيت الفوري على أجهزة Windows باستخدام نقاط توزيع macOS.
استخدام كخادم إرسال	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓	—

ميزة عميل الشبكة	Windows	Linux	macOS
التعامل مع تطبيقات الجهات الخارجية			
التثبيت عن بُعد للتطبيقات على الأجهزة	✓	—	✓ ارجع إلى المقالة التالية للحصول على التفاصيل: تثبيت التطبيقات عن بُعد على أجهزة macOS.
تحديثات البرنامج	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	—	—
تكوين تحديثات نظام التشغيل في سياسة عميل الشبكة	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	—	—
عرض معلومات حول الثغرات الأمنية بالبرنامج	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	—	—
فحص التطبيقات بحثًا عن ثغرات أمنية	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	—	—
مخزون البرامج المثبتة على الأجهزة	✓	✓	—
الأجهزة الظاهرية			
تثبيت عميل الشبكة على جهاز ظاهري	✓	✓	✓
إعدادات التحسين للبنية الأساسية لسطح المكتب الافتراضي (VDI)	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓	✓
دعم الأجهزة الظاهرية الديناميكية	✓ القيود: غير مدعوم من Network Agent for Microsoft Windows على معالجات Arm.	✓	✓
أخرى			
تدقيق الإجراءات على جهاز عميل بعيد باستخدام مشاركة سطح المكتب لـ Windows	✓	—	—
مراقبة حالة الحماية ضد الفيروسات	✓	✓	✓
إدارة عمليات إعادة تشغيل الجهاز	✓	—	—
دعم عودة نظام الملفات	✓	✓	✓
استخدام عميل الشبكة هذا كبوابة اتصال	✓	✓	✓
مدير الاتصال	✓	✓	✓
تبديل عميل الشبكة من خادم إدارة إلى آخر (تلقائيًا حسب موقع الشبكة)	✓	—	✓
التحقق من اتصال جهاز عميل بخادم الإدارة الأداة المساعدة klnagchk	✓	✓	✓
الاتصال البعيد بسطح مكتب جهاز عميل	✓	—	✓ باستخدام نظام حوسبة الشبكة الافتراضية (VNC).
تنزيل حزمة تثبيت قائمة بذاتها من خلال معالج الترحيل	✓	✓	✓
استطلاع شبكة لا تتطلب تكوينًا	—	✓	—

ميزة عميل الشبكة	Windows	Linux	macOS
عرض معلومات عن مكونات أجهزة العميل	✓	✓ تقتصر المعلومات عن مكونات أجهزة Linux المرسلة إلى خادم الإدارة بواسطة عميل الشبكة المثبت على هذه الأجهزة على المعلومات المحددة في وصف إعدادات الجهاز المُدار لوحدة تحكم الإدارة Kaspersky Security Center و Web Console.	✓ تقتصر المعلومات عن مكونات أجهزة macOS المرسلة إلى خادم الإدارة بواسطة عميل الشبكة المثبت على هذه الأجهزة على المعلومات المحددة في وصف إعدادات الجهاز المُدار لوحدة تحكم الإدارة Kaspersky Security Center و Web Console.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (يشار إليه فيما يلي أيضًا باسم Kaspersky Security Center Web Console) هو تطبيق ويب مصمم لإدارة حالة نظام الأمان لشبكة محمية بواسطة تطبيقات Kaspersky.

يمكنك إجراء ما يلي باستخدام التطبيق:

- إدارة حالة نظام أمان المؤسسة.
- تثبيت تطبيقات Kaspersky على الأجهزة على شبكتك وإدارة التطبيقات المثبتة.
- إدارة السياسات المنشأة للأجهزة الموجودة على شبكتك.
- إدارة حسابات المستخدمين.
- إدارة المهام للتطبيقات المثبتة على أجهزة شبكتك.
- عرض التقارير على حالة نظام الأمان.
- إدارة تسليم التقارير إلى مديري النظام وخبراء تكنولوجيا المعلومات الآخرين.

للحصول على معلومات عن متطلبات الأجهزة والبرامج، راجع متطلبات Web Console.

Kaspersky Security Center Web Console يوفر واجهة ويب تضمن تفاعل بين جهازك وخادم الإدارة على مستعرض. خادم الإدارة هو تطبيق مصمم لإدارة تطبيقات Kaspersky مثبتة على أجهزة شبكتك. يتصل خادم الإدارة بالأجهزة على شبكتك عبر قنوات تحميها طبقة مآخذ التوصيل الآمنة (SSL). عندما توصل Kaspersky Security Center Web Console عبر استخدام مستعرضك، فإن المستعرض ينشئ اتصالًا مع Kaspersky Security Center Web Console Server.

يمكنك تشغيل Kaspersky Security Center Web Console كما يلي:

1. استخدم مستعرض في التوصيل مع Kaspersky Security Center Web Console حيث يتم عرض واجهة بوابة الويب.
2. استخدم عناصر التحكم في بوابة الويب لاختيار أمر ترغب في تشغيله. Kaspersky Security Center Web Console يجري العمليات التالية:

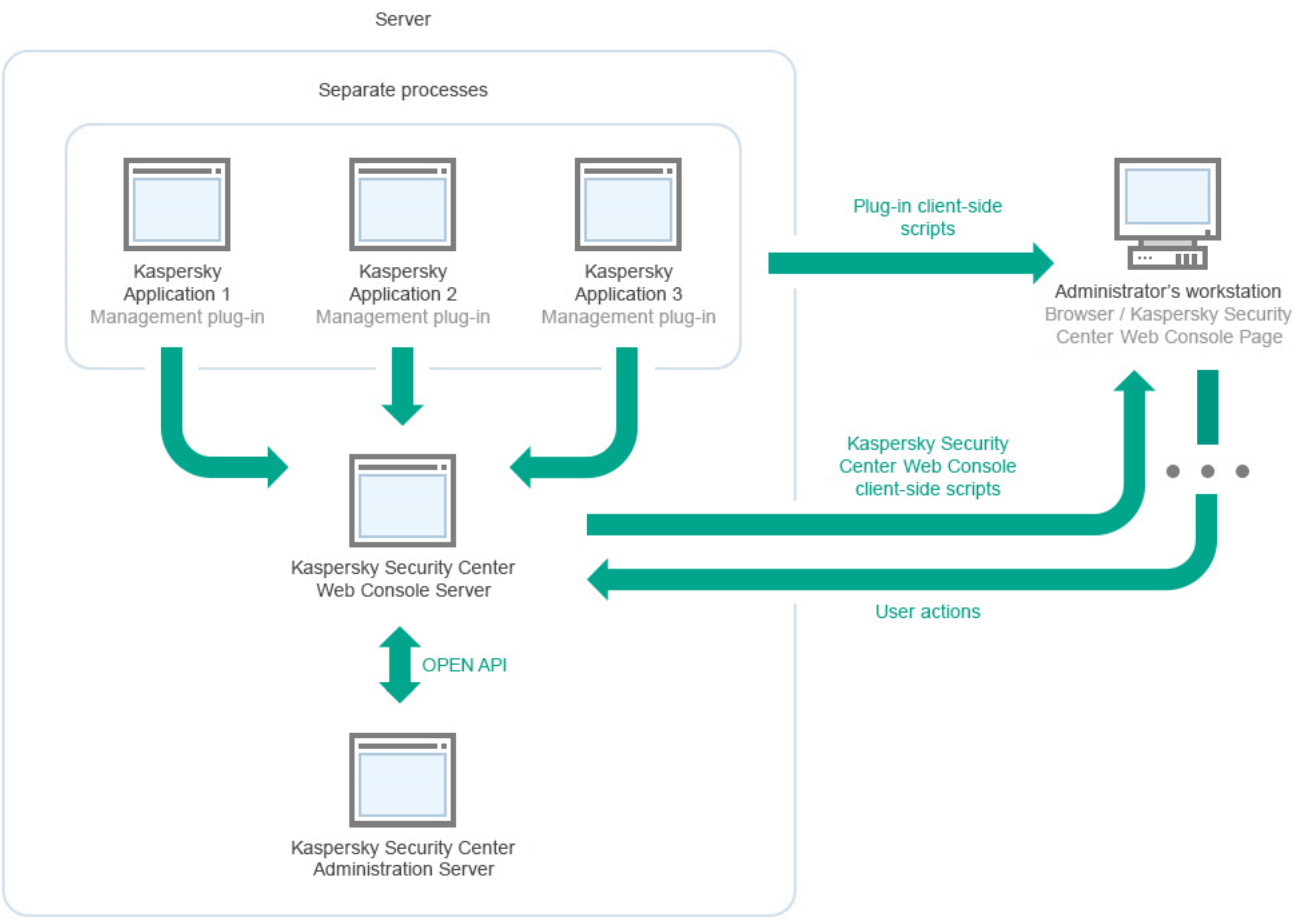
- إذا حددت أمرًا مستخدمًا لاستقبال المعلومات (مثل عرض قائمة بالأجهزة)، يقوم Kaspersky Security Center Web Console بإنشاء طلب للمعلومات من أجل خادم الإدارة ويستقبل البيانات الضرورية ويرسلها إلى المستعرض في تنسيق سهل عرضه.
- إذا اخترت أمرًا مستخدمًا في الإدارة (مثل التثبيت عن بُعد لتطبيق)، يستقبل Kaspersky Security Center Web Console الأمر من المستعرض ويرسله إلى خادم إدارة. بعدها يستقبل التطبيق النتيجة من خادم الإدارة وترسلها إلى المستعرض في تنسيق سهل عرضه.

Kaspersky Security Center Web Console هو تطبيق متعدد اللغات. يمكنك تغيير لغة الواجهة في أي وقت، ودون الحاجة إلى إعادة فتح التطبيق. عندما تقوم بتثبيت Kaspersky Security Center Web Console مع Kaspersky Security Center، فإن لغة واجهة Kaspersky Security Center Web Console تكون نفس لغة ملف التثبيت. أما عندما تقوم بتثبيت Kaspersky Security Center Web Console فقط، يتم تثبيت التطبيق بنفس لغة الواجهة التي يعمل بها نظام التشغيل. إذا كان Kaspersky Security Center Web Console لا يدعم لغة ملف التثبيت أو نظام التشغيل، تكون اللغة الإنجليزية هي اللغة الافتراضية.

إدارة جهاز المحمول ليس مدعومًا في Kaspersky Security Center Web Console. لكن إذا أضفت أجهزة محمولة إلى مجموعة إدارة عبر استخدام Microsoft Management Console، سيتم عرض تلك الأجهزة في Kaspersky Security Center Web Console.

نشر مخطط خادم إدارة Kaspersky Security Center و Kaspersky Security Center Web Console

يوضِّح الشكل أدناه مخطط النشر لكلٍ من خادم إدارة Kaspersky Security Center و Kaspersky Security Center Web Console.



نشر مخطط خادم إدارة Kaspersky Security Center و Kaspersky Security Center Web Console

إدارة المكونات الإضافية لتطبيقات Kaspersky المثبتة على الأجهزة المحمية (مكون إضافي واحد لكل تطبيق) يتم نشرها مع Kaspersky Security Center Web Console Server.

وبصفتك مديرًا، يمكنك الوصول إلى Kaspersky Security Center Web Console عبر استخدام مستعرض على محطة العمل لديك.

عندما تجري إجراءات معينة في Kaspersky Security Center Web Console، يقوم Kaspersky Security Center Web Console Server بالتواصل مع خادم إدارة Kaspersky Security Center من خلال OpenAPI. Kaspersky Security Center Web Console Server يطلب المعلومات المطلوبة من خادم إدارة Kaspersky Security Center ويعرض نتائج عملياتك في Kaspersky Security Center Web Console.

المنافذ التي يستخدمها Kaspersky Security Center Web Console

يسرد الجدول أدناه المنافذ التي يجب أن تكون مفتوحة على الجهاز الذي يتم تثبيت Kaspersky Security Center Web Console Server (ويشار إليه كذلك باسم Kaspersky Security Center Web Console) عليه.

المنافذ التي يستخدمها Kaspersky Security Center Web Console

رقم المنفذ	اسم الخدمة	البروتوكول	غرض المنفذ	النطاق
2001	Kaspersky Security Center خادم المكونات الإضافية.	HTTPS	منفذ واجهة برمجة التطبيقات (API) الذي يُستخدم بواسطة عمليات المكون الإضافي للإدارة لتلقي الطلبات من "Kaspersky Security Center Web Console Management Service"	تشغيل عمليات node.exe الخاصة بإدارة المكونات الإضافية
1329, 2003	خدمة Kaspersky Security Center Web Console	HTTPS	منافذ واجهة برمجة التطبيقات (API) المستخدمة لاستلام الطلبات من "Kaspersky Security Center Web Console Management Service" التي تعمل على الجهاز نفسه.	تحديث مكونات Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	منفذ واجهة برمجة التطبيقات (API) المستخدم لاستلام الطلبات من خدمة "Kaspersky Security Center Web Console Management Service" التي تعمل على الجهاز نفسه.	تشغيل عمليات node.exe من Kaspersky Security Center Web Console
3333	خدمة Kaspersky OSMP KAS	HTTPS	منفذ نقطة نهاية مصادقة OAuth2.0	إدارة الهوية والوصول
4004	Kaspersky OSMP Facade Service	HTTPS	منفذ موفر هوية OAuth2.0	إدارة الهوية والوصول
4444	خدمة Kaspersky OSMP KAS	HTTPS	منفذ نقطة نهاية مصادقة OAuth2.0	إدارة الهوية والوصول
8200	—	HTTP	منفذ API مستخدم في إنشاء شهادات عبر HashiCorp Vault (لمزيد من التفاصيل عنها، يُرجى الرجوع إلى موقع ويب HashiCorp Vault)	تثبيت Kaspersky Security Center Web Console وتحديث مكونات Kaspersky Security Center Web Console
4150, 4151, 4152	قائمة انتظار رسائل Kaspersky Security Center Web Console	HTTPS	منافذ API الخاصة بـ Message Broker المستخدمة للاتصال بين عمليات كل من Kaspersky Security Center Web Console والمكونات الإضافية للإدارة	التفاعل بين Kaspersky Security Center Web Console والمكونات الإضافية للإدارة.

يسرد الجدول أدناه المنافذ التي لا يجب أن تكون مفتوحة على الجهاز حيث تم تثبيت خادمKaspersky Security Center Web Console. ومع ذلك، يستخدم Kaspersky Security Center Web Console هذه المنافذ لإدارة الهوية والوصول.

المنافذ المستخدمة من قبل Kaspersky Security Center لإدارة الهوية والوصول

رقم المنفذ	اسم الخدمة	البروتوكول	غرض المنفذ	النطاق
4445	خدمة Kaspersky OSMP KAS	HTTPS	منفذ إدارة الهوية والوصول الرئيسي الذي يتلقى التكوين من Kaspersky Security Center Web Console لمنفذ نقطة نهاية مصادقة OAuth2.0 (لمزيد من المعلومات حول OAuth 2.0، راجع موقع الويب OAuth)	إدارة الهوية والوصول
2444	Kaspersky OSMP Facade Service	HTTPS	منفذ تكوين إدارة الهوية والوصول	إدارة الهوية والوصول
2445	Kaspersky OSMP Facade Service	HTTPS	منفذ اتصال "Kaspersky OSMP KAS Service" بـ "Kaspersky OSMP Facade Service"	إدارة الهوية والوصول

واجهة Kaspersky Security Center Web Console

تتم إدارة Kaspersky Security Center من خلال واجهة Kaspersky Security Center Web Console.

تحتوي نافذة Kaspersky Security Center Web Console على العناصر التالية:

- القائمة الرئيسية في الجزء الأيمن من النافذة
- منطقة العمل في الجزء الأيسر من النافذة

القائمة الرئيسية

تحتوي القائمة الرئيسية على الأقسام التالية:

- **خادم الإدارة**. يعرض اسم خادم الإدارة الذي تتصل به حاليًا. انقر فوق أيقونة الإعدادات ( ) لفتح خصائص خادم الإدارة.
- **المراقبة وإعداد التقارير**. توفر نظرة عامة على البنية التحتية الخاصة بك وحالات الحماية والإحصائيات.
- **الأصول (الأجهزة)**. يحتوي على أدوات للأصول، بالإضافة إلى المهام وسياسات تطبيق Kaspersky.
- **المستخدمون والأدوار**. يسمح لك بإدارة المستخدمين والأدوار وتكوين حقوق المستخدم عن طريق تعيين الأدوار للمستخدمين وربط ملفات تعريف السياسة بالأدوار.
- **العمليات**. تحتوي على مجموعة متنوعة من العمليات، بما في ذلك ترخيص التطبيق، وعرض وإدارة محركات الأقراص المشفرة وأحداث التشفير، وإدارة تطبيقات الجهات الخارجية. ويوفر لك هذا أيضًا إمكانية الوصول إلى مستودعات التطبيق.
- **الاكتشاف والنشر**. يسمح لك باستقصاء الشبكة لاكتشاف أجهزة العميل، وتوزيع الأجهزة على مجموعات الإدارة يدويًا أو تلقائيًا. يحتوي هذا القسم أيضًا على معالج البدء السريع ومعالج نشر الحماية.
- **السوق**. يحتوي على معلومات عن المجموعة الكاملة من حلول الأعمال من Kaspersky ويتيح لك تحديد الحلول التي تحتاج إليها، ثم متابعة شراء هذه الحلول على موقع ويب Kaspersky.
- **الإعدادات**. يسمح لك بإجراء نسخ احتياطي للحالة الحالية لمكون ويب إضافي لتتمكن من استعادة الحالة المحفوظة لاحقًا. يحتوي على إعداداتك الشخصية المتعلقة بمظهر الواجهة، مثل لغة الواجهة أو السمة.
- **قائمة حسابك**. يحتوي على رابط إلى تعليمات Kaspersky Security Center. ويسمح لك كذلك بتسجيل الخروج من Kaspersky Security Center، وعرض إصدار Kaspersky Security Center Web Console وقائمة المكونات الإضافية للإدارة المثبتة على الويب.

منطقة العمل

تعرض منطقة العمل المعلومات التي تختار عرضها في أقسام نافذة واجهة Kaspersky Security Center Web Console. وتحتوي أيضًا على عناصر تحكم يمكنك استخدامها لتكوين كيفية عرض المعلومات.

تثبيت أقسام القائمة الرئيسية وإلغاء تثبيتها

يمكنك تثبيت أقسام من Kaspersky Security Center Web Console لإضافتها إلى المفضلة والوصول إليها بسرعة من القسم **Pinned** في القائمة الرئيسية.

> إذا لم تكن هناك عناصر مُثبَّتة، فلن يتم عرض القسم **Pinned** في القائمة الرئيسية.

يمكنك تثبيت الأقسام التي تعرض الصفحات فقط. على سبيل المثال، إذا انتقلت إلى **Assets (Devices)** ← **Managed devices**، يتم فتح صفحة تتضمن جدول الأجهزة، مما يعني أنه يمكنك تثبيت قسم **Managed devices**. إذا تم عرض نافذة أو عدم عرض أي عنصر بعد تحديد القسم في القائمة الرئيسية، فلن يمكنك تثبيت هذا القسم.

لتثبيت قسم:

1. في القائمة الرئيسية، مرر مؤشر الماوس فوق القسم الذي تريد تثبيته.

يتم عرض أيقونة الدبوس (📌).

2. انقر فوق أيقونة الدبوس (📌).

يتم تثبيت القسم وعرضه في القسم **Pinned**.

يمكنك أيضًا إزالة العناصر من المفضلة عن طريق إلغاء تثبيتها.

لإلغاء تثبيت قسم:

1. في القائمة الرئيسية، انتقل إلى القسم **Pinned**.

2. قم بتمرير مؤشر الماوس فوق القسم الذي تريد إلغاء تثبيته، ثم انقر فوق أيقونة إلغاء التثبيت (📌).

تم إزالة القسم من المفضلة.

السيناريو: تثبيت وإعداد مبدئي لـ Kaspersky Security Center Web Console

يصف هذا السيناريو كيفية تثبيت خادم إدارة Kaspersky Security Center وKaspersky Security Center Web Console، وإجراء الإعداد الأولي لخادم الإدارة باستخدام معالج البدء السريع، وتثبيت تطبيقات Kaspersky على الأجهزة المدارة باستخدام معالج نشر الحماية.

تثبيت وإعداد مبدئي لـ Kaspersky Security Center Web Console يتم على مراحل:

1. **تثبيت نظام إدارة قواعد البيانات (DBMS)**

قم بتثبيت نظام إدارة قواعد البيانات الذي سيستخدمه Kaspersky Security Center، أو استخدم نظامًا حاليًا.

لمزيد من المعلومات عن كيفية تثبيت نظام إدارة قاعدة البيانات المحدد، يُرجى الرجوع إلى مستنداته.

2. **تثبيت خادم الإدارة، وحدة تحكم الإدارة عميل الشبكة**

يتم تثبيت وحدة تحكم الإدارة وإصدار خادم عميل الشبكة مع خادم الإدارة.

أثناء تثبيت خادم إدارة Kaspersky Security Center، حدد إذا ما كنت تريد تثبيت Kaspersky Security Center Web Console على الجهاز نفسه أم لا. إذا اخترت تثبيت كلا المكونين على الجهاز نفسه، ليس عليك أن تثبت Kaspersky Security Center Web Console بشكل منفصل لأنه يتم تثبيته بشكل تلقائي. إذا كنت تريد تثبيت Kaspersky Security Center Web Console على جهاز مختلف، عليك إذًا بعد تثبيت خادم إدارة Kaspersky Security Center أن تتابع تثبيت Kaspersky Security Center Web Console.

3. **تثبيت Kaspersky Security Center Web Console**

إذا لم تختر تثبيت Kaspersky Security Center Web Console مع خادم إدارة Kaspersky Security Center في الخطوة السابقة، فقم بتثبيت Kaspersky Security Center Web Console بشكل منفصل. يمكنك تثبيت Kaspersky Security Center Web Console على جهاز مختلف أو على نفس الجهاز المثبت عليه خادم الإدارة.

4. **إجراء الإعداد الأولي**

عند اكتمال تثبيت خادم الإدارة، يبدأ تشغيل معالج البدء السريع تلقائيًا عند أول اتصال خادم الإدارة. قم بتنفيذ التكوين الأولي لخادم الإدارة وفقًا للمتطلبات الحالية. أثناء مرحلة التكوين الأولي، يستخدم المعالج الإعدادات الافتراضية لإنشاء السياسات والمهام المطلوبة لنشر الحماية. ومع ذلك، قد لا تكون الإعدادات الافتراضية مثالية لاحتياجات مؤسستك. إذا لزم الأمر، يمكنك تحرير إعدادات السياسات والمهام.

5 **ترخيص Kaspersky Security Center (اختياري)**

Kaspersky Security Center بدعم الوظائف الأساسية لوحدة الإدارة لا يتطلب أي ترخيص. أنت بحاجة إلى ترخيص تجاري إذا كنت ترغب في استخدام واحد أو أكثر من الميزات الإضافية، بما في ذلك إدارة الثغرات الأمنية والتصحيحات، وإدارة الأجهزة المحمولة، والتكامل مع أنظمة SIEM. يمكنك إضافة ملف مفتاح أو رمز تنشيط لهذه الميزات في الخطوة المقابلة من معالج البدء السريع أو يدويًا.

6 **اكتشاف أجهزة الشبكة**

هذه المرحلة هي جزء من معالج البدء السريع. يمكنك كذلك اكتشاف الأجهزة يدويًا. يتلقى Kaspersky Security Center عناوين وأسماء جميع الأجهزة التي تم اكتشافها في الشبكة. بعد ذلك يمكنك استخدام Kaspersky Security Center لتثبيت تطبيقات وبرامج Kaspersky المتوفرة من موردين آخرين في الأجهزة المكتشفة. يبدأ Kaspersky Security Center اكتشاف الأجهزة بشكل منتظم، مما يعني أنه في حالة ظهور أي مثيلات جديدة في الشبكة، سيتم اكتشافها تلقائيًا.

7 **ترتيب الأجهزة في مجموعات الإدارة**

هذه الخطوة جزء من معالج البدء السريع، لكن يمكنك كذلك نقل الأجهزة المكتشفة إلى المجموعات يدويًا.

8 **تثبيت عميل الشبكة وتطبيقات أمان على أجهزة متصلة بالشبكة.**

نشر الحماية على شبكة مؤسسة يشمل تثبيت عميل الشبكة وتطبيقات الأمان (مثل Kaspersky Endpoint Security for Windows) على الأجهزة التي تم اكتشافها بواسطة خادم الإدارة أثناء اكتشاف الأجهزة.

لتثبيت التطبيقات عن بُعد، قم بتشغيل معالج نشر الحماية.

تطبيقات الأمان تحمي الأجهزة من الفيروسات و/أو البرامج الأخرى التي تشكّل تهديدًا. يضمن عميل الشبكة الاتصال بين الجهاز وخادم الإدارة. يتم تكوين إعدادات عميل الشبكة تلقائيًا بشكل افتراضي.

قبل أن تبدأ تثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة المتصلة بالشبكة، تأكد أن هذه الأجهزة يمكن الوصول إليها (تم تشغيلها).

9 **نشر مفاتيح الترخيص على الأجهزة العميلة**

قم بنشر مفاتيح الترخيص على الأجهزة العميلة لتفعيل تطبيقات الأمان المُدارة على هذه الأجهزة.

10 **تثبيت Kaspersky Security for Mobile (اختياري)**

إذا كنت تخطط لإدارة الأجهزة المحمولة الخاصة بالشركة، فاتبع الإرشادات الواردة في تعليمات Kaspersky Security for Mobile للحصول على معلومات عن نشر Kaspersky Endpoint Security for Android.

11 **تكوين سياسات تطبيق Kaspersky**

لتطبيق إعدادات تطبيق مختلفة على أجهزة مختلفة، يمكنك استخدام إدارة أمان مرتكزة على الجهاز و/أو إدارة أمان مرتكزة على المستخدم. يمكن تنفيذ إدارة الأمان المرتكزة على الجهاز باستخدام السياسات والمهام . لا يمكنك تطبيق المهام إلا على الأجهزة التي تلبي الشروط المحددة. ولوضع شروط تصفية الأجهزة، استخدم تحديدات الأجهزة وكذلك العلامات.

12 **مراقبة حالة حماية الشبكة**

يمكنك مراقبة شبكتك باستخدام عناصر واجهة على جزء المعلومات وإنشاء تقارير من تطبيقات Kaspersky وتكوين وعرض تحديدات الأحداث المستلمة من التطبيقات على الأجهزة المُدارة وعرض قوائم الإخطارات.

التثبيت:

يصف هذا القسم تثبيت Kaspersky Security Center وكذلك Kaspersky Security Center Web Console.

تثبيت Kaspersky Security Center (تثبيت قياسي)

يصف هذا الإجراء كيفية تثبيت Kaspersky Security Center. يجب قبل التثبيت أن تقوم بتثبيت نظام لإدارة قواعد البيانات.

لتثبيت Kaspersky Security Center:

1. من حساب يتمتع بامتيازات إدارية، قم بتشغيل الملف التنفيذي ksc_<رقم البنية>_full_<لغة الترجمة>.exe.

2. في نافذة تحديد التطبيق التي تفتح، انقر على **تثبيت Kaspersky Security Center**.

يبدأ معالج إعداد خادم الإدارة Kaspersky Security Center.

3. بدايةً من صفحة الترحيب، انتقل عبر المعالج من خلال استخدام زر **التالي**.

4. إذا كان Microsoft .NET Framework غير مثبتٍ، قم بتثبيته.

5. اقبل شروط اتفاقية الترخيص وكذلك سياسة الخصوصية.

6. حدد نوع التثبيت. ولأغراض التقييم، ننصحك بالاحتفاظ بقيمة **قياسي** الافتراضية.

7. إذا كنت ترغب في تثبيت Kaspersky Security Center Web Console على الجهاز نفسه، حدد خانة الاختيار **تثبيت Kaspersky Security Center Web Console**.

إذا قمت بإلغاء تحديد مربع الاختيار، يمكنك بعد ذلك تثبيت Kaspersky Security Center Web Console بشكل منفصل على الجهاز نفسه أو جهاز آخر.

8. حدد حجم شبكتك. ولأغراض التقييم، ننصحك بالاحتفاظ بقيمة **يوجد أقل من 100 جهاز على الشبكة** الافتراضية.

9. حدد نوع خادم قاعدة البيانات الذي ثبته قبل ذلك.

10. حدد معلمات الاتصال بخادم قاعدة البيانات الذي ثبته من قبل.

11. حدد معلمات التصديق بخادم قاعدة البيانات الذي ثبته من قبل.

12. انقر على زر **تثبيت** لبدء التثبيت.

13. بعد اكتمال التثبيت بنجاح، اختر ما إذا كنت ترغب في بدء وحدة تحكم الإدارة مباشرةً بعد إغلاق المعالج أم لا.

إذا اخترت فتح Kaspersky Security Center Web Console، سوف تفتح شاشة تسجيل الدخول. بعدها سوف تقدر على إجراء التكوين الأولي لخادم الإدارة باستخدام معالج البدء السريع.

لا يمكنك فتح Kaspersky Security Center Web Console إلا إذا كان مثبتًا بالفعل. لا يمكنك فتح Kaspersky Security Center Web Console إذا لم تقم بتثبيته أثناء تثبيت Kaspersky Security Center بشكل منفصل.

14. في نافذة وحدة تحكم الإدارة التي تفتح، انقر على خادم الإدارة المثبت.

15. في نافذة شهادة خادم الإدارة التي تفتح، انقر على زر **نعم** من أجل الاستمرار.

يبدأ معالج البدء السريع لخادم الإدارة إذا لم تقم بتشغيله في وحدة تحكم الإدارة المستندة إلى الويب.

استكشاف الأخطاء وحلها

إذا لم تفتح نافذة شهادة خادم الإدارة وتم عرض أخطاء في الاتصال، جرب ما يلي:

1. في نظام التشغيل Windows، افتح **الخدمات (لوحة التحكم ← الأدوات الإدارية ← الخدمات)**. تأكد أن عميل شبكة Kaspersky Security Center وخادم إدارة Kaspersky Security Center يعملان.

2. على نظام التشغيل Windows، افتح **عارض الأحداث (لوحة التحكم ← الأدوات الإدارية ← عارض الأحداث)** وبعدها حدد **سجلات التطبيقات والخدمات ← سجل أحداث Kaspersky**. تأكد أن السجل لا يحتوي على أخطاء ويحتوي على أحداث مثل **خادم الإدارة <رقم الإصدار> يعمل**.

تثبيت Kaspersky Security Center Web Console

يصف هذا القسم كيفية تثبيت Kaspersky Security Center Web Console Server (يُشار إليه أيضًا باسم Kaspersky Security Center Web Console) بشكل منفصل. يجب قبل التثبيت أن تقوم بتثبيت نظام لإدارة قواعد البيانات (DBMS) وخادم إدارة Kaspersky Security Center.
يمكنك تثبيت Kaspersky Security Center Web Console على نفس الجهاز المثبت عليه Kaspersky Security Center أو على جهاز مختلف.

لتثبيت Kaspersky Security Center Web Console:

1. من حساب يتمتع بامتيازات إدارية، قم بتشغيل ملف التثبيت kscwebconsole-<version number>.<build number>.exe.

   يؤدي هذا إلى تشغيل معالج الإعداد.

2. حدد لغة لمعالج الإعداد.

3. في نافذة الترحيب، انقر على **Next**.

4. في نافذة **License Agreement**، اقرأ شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واقبلها. يستمر التثبيت بعد قبولك اتفاقية ترخيص المستخدم النهائي، وإلا لن يكون زر **Next** متاحًا.

5. في النافذة **Destination folder**، حدد مجلدًا يتم فيه تثبيت Kaspersky Security Center Web Console (المجلد الافتراضي هو %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). في حالة عدم وجود هذا المجلد، يتم إنشاؤه بشكل تلقائي أثناء التثبيت.

   يمكنك تغيير المجلد الوجهة باستخدام زر **Browse**.

6. في نافذة **Kaspersky Security Center Web Console connection settings**، حدد المعلومات التالية:

   - عنوان Kaspersky Security Center Web Console (العنوان الافتراضي هو 127.0.0.1).
   - المنفذ الذي سيستخدمه Kaspersky Security Center Web Console للاتصالات الواردة، أي المنفذ الذي يتيح الوصول إلى Kaspersky Security Center Web Console من مستعرض (افتراضيًا، 8080).

   ننصحك بأن تترك العنوان رقم المنفذ كما هما دون تغيير.

   إذا كنت ترغب، يمكنك النقر على **Test** للتأكد من أن المنفذ المحدد متاحًا.

   إذا كنت ترغب في تفعيل تسجيل أنشطة Kaspersky Security Center Web Console، حدد الخيار المناسب لذلك. إذا لم تحدد هذا الخيار، فلن يتم إنشاء ملفات سجل Kaspersky Security Center Web Console.

7. في نافذة **Account settings**، حدد أسماء الحساب وكلمات المرور.

   نوصي بأن تستخدم الحسابات الافتراضية.

8. في نافذة **Client certificate**، حدد أحد الخيارات التالية:

   - **Generate new certificate**. يُنصح بهذا الخيار إذا لم يكن لديك شهادة مستعرض.
   - **Choose existing certificate**. يمكنك تحديد هذا الخيار إذا كان لديك بالفعل شهادة مستعرض، وفي هذه الحالة حدد مسارها.
   - إذا اخترت إنشاء شهادة جديدة، فعند فتح Kaspersky Security Center Web Console، فقد يخبرك المتصفح أن الاتصال بـ Kaspersky Security Center Web Console ليس خاصًا وأن شهادة Kaspersky Security Center Web Console غير صالحة. يظهر هذا التحذير لأن شهادة Kaspersky Security Center Web Console موقعة ذاتيًا ويتم إنشاؤها تلقائيًا بواسطة Kaspersky Security Center. لإزالة هذا التحذير، أنشئ شهادة موثوقًا بها في بنيتك التحتية وتلبي متطلبات الشهادات المخصصة. بعد ذلك، حدد خيار **Choose existing certificate** من نافذة **Client certificate**، ثم حدد مسار شهادتك المخصصة.

لا يدعم Kaspersky Security Center Web Console الشهادات بتنسيق PFX. لاستخدام مثل هذه الشهادة، يجب أولاً أن تقوم بتحويلها إلى تنسيق PEM المدعوم باستخدام الأداة المساعدة عبر النظام الأساسي OpensSL، مثل Openssl for Windows.

9. في نافذة **Trusted Administration Servers**، تأكد أن خادم الإدارة لديك في القائمة ثم انقر على **التالي** من أجل التقدم إلى آخر نافذة لأداة التثبيت.

إذا كنت بحاجة إلى إضافة خادم إدارة جديد إلى القائمة، انقر فوق الزر **Add**. في النافذة المفتوحة، حدد خصائص خادم الإدارة الجديد الموثوق به:

- **Administration Server name**

  اسم خادم الإدارة الذي سيتم عرضه في نافذة تسجيل الدخول الخاصة بتطبيق Kaspersky Security Center Web Console.

- **Administration Server address**

  عنوان IP للجهاز حيث تقوم بتثبيت خادم الإدارة.

- **Administration Server port**

  منفذ OpenAPI الذي يستخدمه Kaspersky Security Center Web Console للاتصال بخادم الإدارة (القيمة الافتراضية هي 13299).

- **Administration Server certificate**

  يتم تخزين ملف الشهادة على الجهاز المثبت عليه خادم الإدارة. المسار الافتراضي لشهادة خادم الإدارة.

  - بالنسبة لنظام التشغيل Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
  - لنظام التشغيل Linux— / var / opt / kaspersky / klnagent_srv / 1093 / cert /

  إذا قمت بتثبيت Kaspersky Security Center Web Console على الجهاز نفسه حيث تم تثبيت خادم الإدارة ، استخدم أحد المسارات المذكورة أعلاه. بخلاف ذلك، انسخ ملف الشهادة من الجهاز حيث تم تثبيت خادم الإدارة على الجهاز حيث تقوم بتثبيت Kaspersky Security Center Web Console، ثم حدد المسار المحلي للشهادة.

10. في نافذة **Identity and Access Manager (IAM)**، حدد ما إذا كنت تريد تثبيت إدارة الهوية والوصول (يشار إليها أيضًا باسم IAM). إذا اخترت تثبيت الهوية وإجراءات الوصول، فحدد أرقام المنفذ التالية:

- **KAS administrator port**. بشكل افتراضي، يتم استخدام المنفذ 4445 لتلقي التكوين من Kaspersky Security Center Web Console لمنفذ نقطة نهاية مصادقة OAuth2.0.
- **Facade administrator port**. يتم استخدام منفذ 2444 بشكل افتراضي لتكوين إدارة الهوية والوصول.
- **Facade interaction port**. يتم استخدام المنفذ 2445 بشكل افتراضي لاتصال خدمة Kaspersky OSMP KAS بخدمة Kaspersky Osmp Facade

يمكنك إذا كنت ترغب أن تقوم بتغيير أرقام المنافذ الافتراضية. لن تتمكن من تغييرها في المستقبل عبر Kaspersky Security Center Web Console.

11. في آخر نافذة للمثبت، انقر على **Install** من أجل بدء التثبيت.

بعد اكتمال التثبيت بنجاح، سيظهر اختصار على سطح المكتب، ويمكنك تسجيل الدخول إلى Kaspersky Security Center Web Console.

يبدأ معالج البدء السريع لخادم الإدارة إذا لم تقم بتشغيله في وحدة تحكم الإدارة القائمة على وحدة التحكم بالإدارة لـ Microsoft.

إذا لم يتم عرض Kaspersky Security Center Web Console في متصفحك في عنوان URL الذي كتبته، جرّب ما يلي:

1. تأكد أنك حددت اسم المضيف الصحيح أو عنوان IP للجهاز الذي تم تثبيت Kaspersky Security Center Web Console عليه.
2. تأكد أن الجهاز الذي ترغب في تشغيله لديه وصول إلى الجهاز المثبت عليه Kaspersky Security Center Web Console.
3. تحقق من أن إعدادات جدار الحماية على الجهاز المثبت عليه Kaspersky Security Center Web Console تسمح بالاتصالات الواردة من خلال المنفذ 8080 ومن أجل التطبيق node.exe.
4. على نظام التشغيل Windows، افتح **الخدمات**. تأكد أن خدمة Kaspersky Security Center Web Console تعمل.
5. تأكد أنك تقدر على الوصول إلى Kaspersky Security Center باستخدام وحدة تحكم الإدارة.
6. على نظام التشغيل Windows، افتح **عارض الأحداث** ثم حدد **سجلات التطبيقات والخدمات** ← **سجل أحداث Kaspersky**. تأكد أن السجل لا يحتوي على أخطاء.

تثبيت Kaspersky Security Center Web Console المتصل بخادم الإدارة المُثبت على عقد مجموعة تجاوز الفشل

يصف هذا القسم كيفية تثبيت Kaspersky Security Center Web Console Server (المشار إليه فيما يلي أيضًا باسم Kaspersky Security Center Web Console)، والذي يتصل بخادم الإدارة المُثبت على عُقد مجموعة تجاوز الفشل من Kaspersky Security Center أو عُقد مجموعة تجاوز الفشل في Windows Server. قبل تثبيت Kaspersky Security Center Web Console، قم بتثبيت نظام لإدارة قاعدة البيانات (DBMS) وخادم إدارة Kaspersky Security Center على عُقد مجموعة تجاوز الفشل من Kaspersky Security Center أو على عقد مجموعة تجاوز الفشل في Windows Server.

إذا كنت تستخدم نظام مجموعة تجاوز الفشل في Windows Server، فلا نوصي بتثبيت Kaspersky Security Center Web Console على عقدة نظام مجموعة تجاوز الفشل. في حالة فشل العقدة، ستفقد الوصول إلى خادم الإدارة.

لتثبيت Kaspersky Security Center Web Console الذي يتصل بخادم الإدارة المثبت على عُقد مجموعة تجاوز الفشل:

1. نفذ خطوات تثبيت Kaspersky Security Center Web Console، بدءًا من الخطوة 1 إلى الخطوة 8.
2. في الخطوة 9 ، في النافذة **Trusted Administration Servers**، انقر فوق الزر **Add** لإضافة مجموعة تجاوز الفشل كخادم إدارة موثوق به.

   في النافذة المفتوحة، حدد الخصائص التالية:

   - **Administration Server name**

     اسم المجموعة الذي سيتم عرضه في نافذة تسجيل الدخول الخاصة بمكون Kaspersky Security Center Web Console.

   - **Administration Server address**

     اعتمادًا على نوع نظام مجموعة تجاوز الفشل، حدد عنوان المجموعة:

     - **مجموعة تجاوز الفشل من Kaspersky Security Center**. حدد عنوان IP لمحول الشبكة الثانوي كعنوان المجموعة إذا أنشأت المحول عند تحضير عُقد المجموعة. بخلاف ذلك، أدخل عنوان IP الخاص بموازنة تحميل الجهة الخارجية التي تستخدمها.
     - **مجموعة تجاوز الفشل في Windows Server**. حدد عنوان المجموعة الذي حصلت عليه عند إنشاء نظام مجموعة تجاوز الفشل في Windows Server.

- **Administration Server port**

منفذ OpenAPI الذي يستخدمه Kaspersky Security Center Web Console للاتصال بخادم الإدارة (القيمة الافتراضية هي 13299).

- **Administration Server certificate**

توجد شهادة خادم الإدارة في مخزن البيانات المشتركة لمجموعة تجاوز الفشل من Kaspersky Security Center أو مجموعة تجاوز الفشل في Windows Server. المسار الافتراضي لملف الشهادة: <مجلد البيانات المشتركة>\1093\cert\klserver.cer. انسخ ملف الشهادة من تخزين البيانات المشتركة إلى الجهاز حيث تقوم بتثبيت Kaspersky Security Center Web Console. حدد المسار المحلي لشهادة خادم الإدارة.

3. قم بتشغيل التثبيت القياسي لمكون Kaspersky Security Center Web Console.

بعد اكتمال التثبيت بنجاح، سيظهر اختصار على سطح المكتب، ويمكنك تسجيل الدخول إلى Kaspersky Security Center Web Console.

ترقية Kaspersky Security Center Web Console

إذا كنت ترغب في استخدام إصدار أحدث من Kaspersky Security Center Web Console دون إزالة الإصدار المثبت الحالي، يمكنك استخدام إجراء الترقية القياسي المتوفر في مثبت Kaspersky Security Center Web Console.

لترقية Kaspersky Security Center Web Console:

1. باستخدام حساب يتمتع بالحقوق الإدارية، شغل ملف التثبيت exe.<build number>.<version number>-ksc-web-console، حيث يشير <build number> إلى بنية Kaspersky Security Center Web Console الذي يكون رقمه أحدث من الإصدار المثبت لديك حاليًا.

2. في نافذة معالج الإعداد التي تفتح، حدد لغة ثم انقر على **OK**.

3. في نافذة الترحيب، حدد خيار **Upgrade** ثم انقر على **Next**.

4. في نافذة **License Agreement**، اقرأ شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واقبلها. يستمر التثبيت بعد قبولك اتفاقية ترخيص المستخدم النهائي، وإلا لن يكون زر **Next** متاحًا.

5. تقدم في خطوات معالج الإعداد حتى تنهي التثبيت. عند التقدم، يمكنك كذلك تعديل إعدادات Kaspersky Security Center Web Console التي حددتها أثناء التثبيت السابق. عندما تصل إلى خطوة **Ready for Kaspersky Security Center Web Console modification**، انقر على زر **Upgrade**. انتظر حتى يتم تطبيق الإعدادات الجديدة ثم انقر على **Finish** في الخطوة التالية من معالج الإعداد. يمكنك كذلك النقر على رابط **Start Kaspersky Security Center Web Console in your browser** لبدء الإصدار المحسن من Kaspersky Security Center Web Console على الفور.

> تعديل إعدادات Kaspersky Security Center Web Console أثناء الترقية غير متاح إلا في إصدار Kaspersky Security Center Web Console version 12.2 أو أحدث.

يتم ترقية إصدار Kaspersky Security Center Web Console.

شهادات للعمل مع Kaspersky Security Center Web Console

يصف القسم كيفية إصدار واستبدال الشهادات لوحدة تحكم ويب Kaspersky Security Center وكيفية تجديد شهادة لخادم الإدارة إذا كان الخادم يتفاعل مع Kaspersky Security Center Web Console.

إعادة إصدار شهادة Kaspersky Security Center Web Console

تضع معظم المستعرضات حدًا على مدة الصلاحية للشهادة. وكي تكون ضمن ذلك الحد، يتم تحديد مدة صلاحية شهادة Kaspersky Security Center Web Console إلى 397 يومًا. يمكنك استبدال أي شهادة موجودة مستلمة من جهة إصدار شهادات معتمدة بإصدار شهادة موقعة ذاتيًا جديدة بشكل يدوي. كحل بديل، يمكنك إعادة إصدار شهادة Kaspersky Security Center Web Console المنتهية لديك.

لا يتم دعم إعادة إصدار الشهادة تلقائيًا لتطبيق Kaspersky Security Center Web Console. ويجب عليك إعادة إصدار الشهادة منتهية الصلاحية يدويًا.

إذا كنت تستخدم شهادة موقعة ذاتيًا بالفعل، يمكنك إعادة إصدارها عبر ترقية Kaspersky Security Center Web Console من خلال الإجراء القياسي في أداة التثبيت (خيار **Upgrade**).

عند فتح وِ، قد يخبرك المستعرض أن الاتصال بـ Web Console ليس خاصًا وأن شهادة Web Console غير صالحة. يظهر هذا التحذير لأن شهادة Web Console موقعة ذاتيًا ويتم إنشاؤها تلقائيًا بواسطة Kaspersky Security Center. لإزالة أو منع هذا التحذير، يمكنك القيام بأحد الإجراءات التالية:

- حدد شهادة مخصصة عند إعادة إصدارها (خيار موصى به). قم بإنشاء شهادة موثوق بها في بنيتك الأساسية وتفي بمتطلبات الشهادات المخصصة.
- أضف شهادة Kaspersky Security Center Web Console إلى قائمة شهادات المستعرض الموثوق بها بعد إعادة إصدار الشهادة. نوصي باستخدام هذا الخيار فقط إذا لم تتمكن من إنشاء شهادة مخصصة.

لإصدار شهادة جديدة عند تثبيت Kaspersky Security Center Web Console لأول مرة:

1. قم بتشغيل التثبيت الروتيني لـ Kaspersky Security Center Web Console.
2. عندما تصل إلى خطوة **Client certificate** في معالج الإعداد، حدد خيار **Generate new certificate** ثم انقر على زر **Next**.
3. تقدم في خطوات معالج الإعداد الباقية حتى تنهي التثبيت.

   يتم إصدار شهادة جديدة من أجل Kaspersky Security Center Web Console مع مدة صلاحية تبلغ 397 يومًا.

لإعادة إصدار شهادة Kaspersky Security Center Web Console المنتهية:

1. ضمن حساب له حقوق المسؤول، قم بتشغيل ملف التثبيت exe.<build number>.<version number>-ksc-web-console.
2. في نافذة معالج الإعداد التي تفتح، حدد لغة ثم انقر على **OK**.
3. في نافذة الترحيب، حدد خيار **Reissue certificate** ثم انقر على **Next**.
4. في الخطوة التالية، انتظر حتى يكتمل إعادة تكوين Kaspersky Security Center Web Console ثم انقر على **Finish**.

   يتم إعادة إصدار Kaspersky Security Center Web Console لمدة صلاحية أخرى مدتها 397 يومًا.

إذا كنت تستخدم إدارة الهوية والوصول، يجب عليك أيضا إعادة إصدار جميع شهادات TLS من أجل المنافذ التي تستخدمها إدارة الهوية والوصول. يعرض Kaspersky Security Center Web Console إشعارًا عند انتهاء صلاحية الشهادة. يجب عليك اتباع تعليمات الإشعار.

استبدال شهادة Kaspersky Security Center Web Console

بشكل افتراضي، عندما تقوم بتثبيت Kaspersky Security Center Web Console Server، يتم إنشاء شهادة متصفح للتطبيق تلقائيًا. يمكنك استبدال الشهادة التي تم إنشاؤها بشكل تلقائي بأخرى مخصصة.

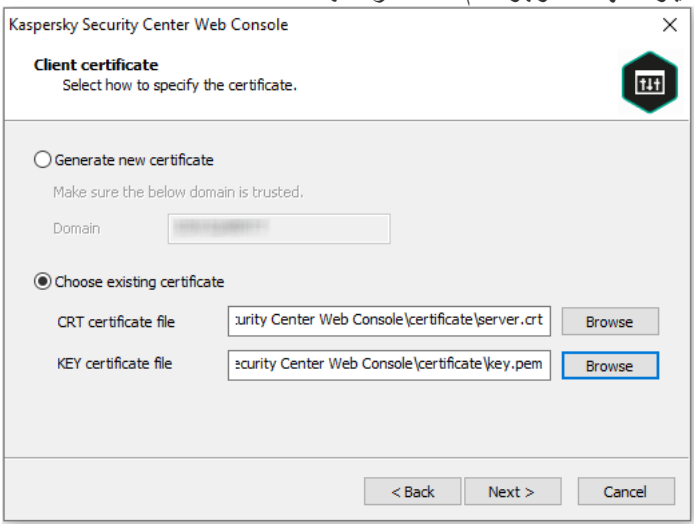
لاستبدال شهادة Kaspersky Security Center Web Console Server بأخرى مخصصة:

1. على الجهاز الذي تم تثبيت Kaspersky Security Center Web Console Server عليه، قم بتشغيل ملف تثبيت -ksc-web-console <version number>.<build number>.exe من حساب يتمتع بمزايا إدارية.

   يؤدي هذا إلى تشغيل معالج الإعداد.

2. في الصفحة الأولى من المعالج، حدد خيار **ترقية**.

3. في صفحة **شهادة العميل**، حدد خيار **اختيار الشهادة الموجودة** ثم حدد مسار الشهادة المخصصة.



تحديد شهادة العميل

4. في الصفحة الأخيرة من المعالج، انقر على **تعديل** لتطبيق الإعدادات الجديدة.

5. بعد اكتمال إعادة تكوين التطبيق بنجاح، انقر على زر **إنهاء**.

يعمل Kaspersky Security Center Web Console مع الشهادة المحددة.

يتم تحديد الشهادات لخوادم الإدارة الموثوقة فيKaspersky Security Center Web Console

يتم استبدال شهادة خادم الإدارة الحالية بأخرى جديدة قبل تاريخ انتهاء الشهادة. يمكنك كذلك استبدال شهادات خادم الإدارة الحالية بشهادة مخصصة. في كل مرة يتم تغيير الشهادة فيها، يجب تحديد الشهادة الجديدة في إعدادات Kaspersky Security Center Web Console. وإذا لم يتم فعل ذلك، لن يقدر Kaspersky Security Center Web Console على الاتصال بخادم الإدارة.

لتحديد شهادة جديدة لخادم الإدارة:

1. على الجهاز المثبت عليه خادم الإدارة، انسخ ملف الشهادة إلى جهاز تخزين بمساحة ضخمة مثلاً.

   بشكل افتراضي، يتم تخزين ملف الشهادة في المجلد التالي:

   - بالنسبة لنظام التشغيل Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\
   - لنظام التشغيل Linux— / var / opt / kaspersky / klnagent_srv / 1093 / cert /

2. على الجهاز المثبت عليه Kaspersky Security Center Web Console، ضع ملف الشهادة ال مجلد محلي.

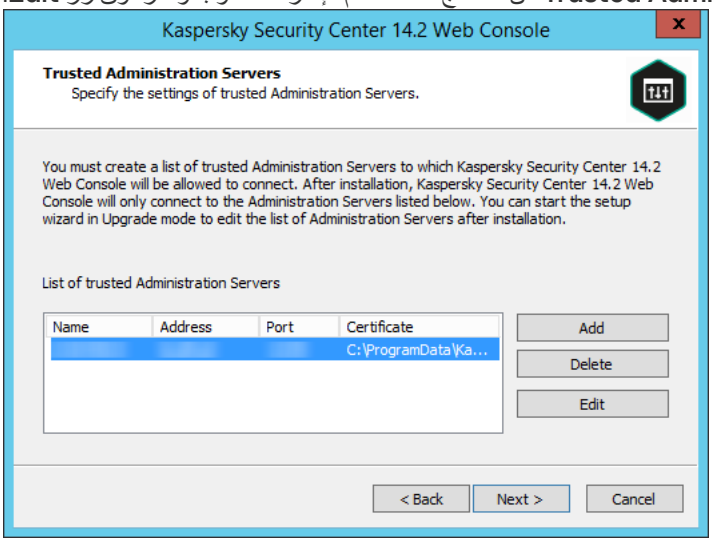
3. قم بتشغيل ملف التثبيت -ksc-web-console <version number>.<build number>.exe ضمن حساب يمتلك امتيازات إدارية.

   يؤدي هذا إلى تشغيل معالج الإعداد.

4. في صفحة المعالج الأولى، حدد خيار **Upgrade**.

اتبع إرشادات المعالج.

5. في صفحة **Trusted Administration Servers** من المعالج، حدد خادم الإدارة المطلوب وانقر فوق زر **Edit**.



تحديد خوادم الإدارة الموثوقة

6. في نافذة **Edit Administration Server** التي تفتح، انقر فوق زر **Browse**، وحدد مسار ملف الشهادة الجديد، ثم انقر فوق زر **Update** لتطبيق التغييرات.

7. في صفحة **Ready for Kaspersky Security Center Web Console modification** من المعالج، انقر فوق زر **Upgrade** لبدء الترقية.

8. بعد اكتمال إعادة تكوين التطبيق بنجاح، انقر على الزر **Finish**.

9. سجل الدخول إلى Kaspersky Security Center Web Console.

يعمل Kaspersky Security Center Web Console مع الشهادة المحددة.

تحويل شهادة PFX إلى تنسيق PEM

لاستخدام شهادة PFX في Kaspersky Security Center Web Console، يجب أن تقوم أولاً بتحويلها إلى تنسيق PEM باستخدام أي أداة مساعدة عبر الأنظمة الأساسية القائمة على OpenSSL.

لتحويل شهادة PFX إلى تنسيق PEM على نظام التشغيل Windows:

1. من أداة مساعدة عبر النظام الأساسي مستندة إلى OpenSSL، قم بتنفيذ الأوامر التالية:

```
clcerts -nokeys -out server.crt- <pfx.filename> openssl pkcs12 -in
nocerts -nodes -out key.pem- <pfx.filename> openssl pkcs12 -in
```

نتيجة لذلك، تحصل على مفتاح عام كملف crt. a ومفتاح خاص كملف pem. محمي بعبارة مرور.

2. تأكد من إنشاء ملفات crt. و pem. في نفس المجلد حيث تم تخزين ملف pfx.

3. إذا احتوى ملف crt. أو pem. على "سمات الحقيبة"، فاحذف هذه السمات باستخدام أي محرر نصوص مناسب، ثم احفظ الملف.

4. أعد تشغيل خدمة Windows.

5. لا يدعم Kaspersky Security Center Web Console الشهادات المحمية بعبارة المرور. لذلك، قم بتشغيل الأمر التالي في أداة مساعدة عبر الأنظمة الأساسية التي تستند إلى OpenSSL لإزالة عبارة مرور من ملف pem.:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

لا تستخدم نفس الاسم لملفات الإدخال والإخراج بصيغة .pem.

ونتيجة لذلك، فإن الملف الجديد الذي يكون بصيغة .pem غير مشفر. لا يتعين عليك إدخال عبارة مرور لاستخدامها.

ملفي .crt و.pem جاهزان للاستخدام، لذا يمكنك تحديدهما من أداة تثبيت Kaspersky Security Center Web Console.

لتحويل شهادة PFX إلى تنسيق PEM على نظام التشغيل Linux:

1. من أداة مساعدة عبر النظام الأساسي مستندة إلى OpenSSL، قم بتنفيذ الأوامر التالية:

```
-/,/-BEGIN CERTIFICATE-/' sed -ne | clcerts -nokeys- <pfx.filename> openssl pkcs12 -in
server.crt < 'END CERTIFICATE-/p
-/,/-BEGIN PRIVATE KEY-/' sed -ne | nocerts -nodes- <pfx.filename> openssl pkcs12 -in
key.pem < 'END PRIVATE KEY-/p
```

2. تأكد أن ملف الشهادة والمفتاح الخاص تم إنشاؤهما إلى الدليل نفسه الموضوع فيه الملف بامتداد .pfx.

3. لا يدعم Kaspersky Security Center Web Console الشهادات المحمية بعبارة المرور. لذلك، قم بتشغيل الأمر التالي في أداة مساعدة عبر الأنظمة الأساسية التي تستند إلى OpenSSL لإزالة عبارة مرور من ملف .pem:

```
openssl rsa -in key.pem -out key-without-passphrase.pem
```

لا تستخدم نفس الاسم لملفات الإدخال والإخراج بصيغة .pem.

ونتيجة لذلك، فإن الملف الجديد الذي يكون بصيغة .pem غير مشفر. لا يتعين عليك إدخال عبارة مرور لاستخدامها.

ملفي .crt و.pem جاهزان للاستخدام، لذا يمكنك تحديدهما من أداة تثبيت Kaspersky Security Center Web Console.

الترحيل من Kaspersky Security Center Windows

يصف هذا القسم ترحيل الأجهزة المدارة والعناصر ذات الصلة (السياسات والمهام والمجموعات والعلامات والعناصر الأخرى) من Kaspersky Security Center Windows إلى:

- Kaspersky Security Center Cloud Console
- حول Kaspersky Security Center Linux

الترحيل إلى Kaspersky Security Center Cloud Console

يمكنك إجراء الترحيل من Kaspersky Security Center Web Console إلى Kaspersky Security Center Cloud Console. بعد ذلك، يمكنك الوصول إلى خادم الإدارة ونظام إدارة قاعدة البيانات (DBMS)، اللذين تتم استضافتهما في بنية Kaspersky الأساسية. لا تحتاج إلى خادم فعلي أو DBMS—كلاهما يتم صيانتهما لك بواسطة خبراء Kaspersky.

يمكنك ترحيل أجهزتك المُدارة التي تعمل بنظام تشغيل Windows أو Linux أو macOS تحت تحكم Kaspersky Security Center Cloud Console. إذا كانت شبكتك تشتمل على تسلسل هرمي للخوادم الإدارية، فيمكنك حفظها في Kaspersky Security Center Cloud Console. بالإضافة إلى ذلك، يمكنك نقل:

- مهام وسياسات التطبيقات المدارة
- المهام العالمية
- تحديدات الجهاز المخصص
- هيكل مجموعة الإدارة والأجهزة المضمنة
- العلامات التي تم تخصيصها للأجهزة المراد تصديرها

بعد الانتهاء من الترحيل، يمكنك إدارة الأجهزة باستخدام Kaspersky Security Center Cloud Console. في الوقت نفسه، يتم الاحتفاظ بالكائنات المنقولة وإعادة تثبيت عميل الشبكة على جميع الأجهزة المدارة.

للحصول على معلومات حول كيفية إجراء الترحيل وقائمة المتطلبات الأساسية، راجع تعليمات Kaspersky Security Center Cloud Console.

الترحيل إلى Kaspersky Next XDR Expert

باتباع هذا السيناريو، يمكنك نقل بنية مجموعة الإدارة والأجهزة المُدارة المضمنة وكائنات المجموعة الأخرى (السياسات والمهام والمهام العامة والعلامات وتحديدات الأجهزة) من Kaspersky Security Center Windows تحت إدارة Kaspersky Next XDR Expert.

القيود:

- يمكن الترحيل فقط من Kaspersky Security Center 14.2 Windows إلى Kaspersky Next XDR Expert بدءًا من الإصدار 1.0.
- يمكنك تنفيذ هذا السيناريو فقط باستخدام Kaspersky Security Center Web Console.

المراحل

يستمر سيناريو الترحيل على مراحل:

1. **اختيار طريقة ترحيل**

تقوم بالترحيل إلى Kaspersky Next XDR Expert من خلال معالج الترحيل. تعتمد خطوات معالج الترحيل على ما إذا كانت خوادم الإدارة لتطبيق Kaspersky Security Center Windows و Kaspersky Next XDR Expert مرتبة في تسلسل هرمي:

- الترحيل باستخدام تسلسل هرمي لخوادم الإدارة:

حدد هذا الخيار إذا كان خادم الإدارة لتطبيق Kaspersky Security Center Windows يعمل كخادم إدارة ثانوي لتطبيق Kaspersky Next XDR Expert. تدير عملية الترحيل والتبديل بين الخوادم داخل Kaspersky Security Center Console. إذا كنت تفضل هذا الخيار، فيمكنك ترتيب خوادم الإدارة في تسلسل هرمي لتبسيط إجراء الترحيل. ولفعل ذلك، أنشئ التسلسل الهرمي قبل بدء الترحيل.

- الترحيل باستخدام ملف تصدير (أرشيف مضغوط)

حدد هذا الخيار إذا لم يتم ترتيب خوادم الإدارة لتطبيق Kaspersky Security Center Windows و Kaspersky Next XDR Expert في تسلسل هرمي. يمكنك إدارة عملية الترحيل باستخدام وحدتي تحكم — على سبيل المثال لتطبيق Kaspersky Security Center Windows و Kaspersky Security Center Console. وفي هذه الحالة، سوف تستخدم ملف التصدير الذي أنشأته وقمت بتنزيله أثناء التصدير من Kaspersky Security Center Windows، وتستورد هذا الملف إلى Kaspersky Next XDR Expert.

2 **تصدير البيانات من Kaspersky Security Center Windows**

افتح Kaspersky Security Center Windows ، ثم قم بتشغيل معالج الترحيل.

3 **استيراد البيانات إلى Kaspersky Next XDR Expert**

تابع معالج الترحيل لاستيراد البيانات التي تم تصديرها إلى Kaspersky Next XDR Expert.

إذا تم ترتيب الخوادم في تسلسل هرمي، يبدأ الاستيراد تلقائيًا بعد تصدير ناجح داخل المعالج نفسه. إذا لم يتم ترتيب الخوادم في تسلسل هرمي، فيمكنك متابعة معالج الترحيل بعد التبديل إلى Kaspersky Next XDR Expert.

4 **نفذ إجراءات إضافية لنقل الكائنات والإعدادات من Kaspersky Security Center Windows إلى Kaspersky Next XDR Expert يدويًا (خطوة اختيارية)**

قد ترغب أيضًا في نقل الكائنات والإعدادات التي لا يمكن نقلها من خلال معالج الترحيل. على سبيل المثال، يمكنك أيضًا تنفيذ ما يلي:

- تكوين المهام العامة لخادم الإدارة
- تكوين إعدادات سياسة عميل الشبكة
- إنشاء حزم تثبيت التطبيقات
- إنشاء الخوادم الافتراضية
- تعيين وتكوين نقاط التوزيع
- تكوين قواعد نقل الجهاز
- تكوين القواعد لوضع العلامات على الأجهزة تلقائيًا
- إنشاء فئات التطبيقات

5 **انقل الأجهزة المُدارة التي تم استيرادها تحت إدارة Kaspersky Next XDR Expert**

لإكمال الترحيل، انقل الأجهزة المُدارة التي تم استيرادها تحت إدارة Kaspersky Next XDR Expert. ويمكنك فعل ذلك بإحدى الطرق التالية:

- من خلال مهمة مجموعة Kaspersky Security Center

  استخدم مهمة تغيير خادم الإدارة لتغيير خادم الإدارة إلى خادم مختلف للأجهزة العميلة المحددة.

- من خلال الأداة المساعدة klmover

  استخدم الأداة المساعدة klmover وحدد إعدادات الاتصال لخادم الإدارة الجديد.

- من خلال تثبيت أو إعادة تثبيت عميل الشبكة على الأجهزة المُدارة

  أنشئ حزمة تثبيت جديدة لعميل الشبكة وحدد إعدادات الاتصال لخادم الإدارة الجديد في خصائص حزمة التثبيت. استخدم حزمة التثبيت لتثبيت عميل الشبكة على الأجهزة المُدارة التي تم استيرادها من خلال مهمة تثبيت عن بُعد.

  يمكنك أيضًا إنشاء واستخدام حزمة تثبيت مستقلة لتثبيت عميل الشبكة محليًا.

6 **تحديث عميل الشبكة إلى أحدث إصدار**

نوصي بترقية عميل الشبكة إلى إصدار Kaspersky Security Center Console نفسه.

7 **تأكد أن الأجهزة المُدارة مرئية على خادم الإدارة الجديد**

على خادم إدارة Kaspersky Next XDR Expert، افتح قائمة الأجهزة المدارة (**Assets (Devices)** ← **Managed devices**) ، وتحقق من القيم في الأعمدة **Visible** و**Network Agent is installed** و**Last connected to Administration Server**.

طرق أخرى لترحيل البيانات

بالإضافة إلى معالج الترحيل، يمكنك أيضًا نقل مهام وسياسات معينة:

- يمكنك تصدير المهام من Kaspersky Security Center Windows، ثم استيراد المهام إلى Kaspersky Next XDR Expert.
- يمكنك تصدير السياسات من Kaspersky Security Center Windows، ثم استيراد السياسات إلى Kaspersky Next XDR Expert. يتم تصدير ملفات تعريف السياسة ذات الصلة واستيرادها مع السياسات المحددة.

الترحيل إلى Kaspersky Security Center Linux

يمكن إجراء الترحيل من Kaspersky Security Center Windows إلى Kaspersky Security Center Linux باستخدام النسخ الاحتياطي لبيانات خادم الإدارة (باستخدام أداة klbackup) ومعالج الترحيل.

يتيح لك الجدول أدناه مقارنة الميزات والقيود الرئيسية للترحيل باستخدام النسخ الاحتياطي لبيانات خادم الإدارة ومعالج الترحيل، لتقرر الأسلوب الأكثر ملاءمة لمؤسستك.

المعلمات	نسخ احتياطي لبيانات خادم الإدارة	معالج الترحيل
عملية الترحيل	إنشاء نسخة احتياطية كاملة لبيانات خادم إدارة Kaspersky Security Center Windows واستعادتها على خادم إدارة Kaspersky Security Center Linux	تحديد بيانات خادم الإدارة وتصديرها للترحيل، واستيراد هذه البيانات إلى خادم إدارة Kaspersky Security Center Linux، وتبديل الأجهزة المُدارة تحت إدارة Kaspersky Security Center Linux
ميزات طريقة الترحيل	• ترحيل كل بيانات خادم الإدارة • ترحيل أي عدد من الأجهزة المُدارة • تُستخدم للحصول على نسخة كاملة من بيانات خادم إدارة Kaspersky Security Center Windows ونقلها إلى خادم إدارة Kaspersky Security Center Linux	• الترحيل الجزئي لبيانات خادم الإدارة • تتوفر إمكانية تحديد كائنات لترحيلها • لا يمكن أن تحتوي مجموعة الإدارة أو المجموعة الفرعية المراد ترحيلها على أكثر من 10000 جهاز • تُستخدم لنقل بيانات خادم الإدارة جزئيًا، بما في ذلك فقط كائنات المجموعة ضمن نطاق الترحيل؛ ويجب استعادة كائنات المجموعة خارج نطاق الترحيل يدويًا
نطاق الترحيل	النقل الكامل لبيانات خادم الإدارة مع عدد غير محدود من الأجهزة المُدارة	• هيكل مجموعة الإدارة • الأجهزة المُدارة المضمنة في مجموعات الإدارة (**لا تزيد عن 10000 جهاز**) • العلامات المخصصة لترحيل الأجهزة • المهام العالمية لعميل الشبكة والتطبيقات المُدارة (ليست لخادم الإدارة) • المهام الجماعية لعميل الشبكة والتطبيقات المدارة • سياسات التطبيقات المُدارة • قوالب التقرير • أدوار المستخدم • المستخدمون الداخليون ومجموعات الأمان • فئات تطبيق مخصصة مع إضافة المحتوى يدويًا • تحديدات الجهاز المخصص
النطاق غير المُرحل	—	• المهام العامة لخادم الإدارة • الأحداث المحفوظة على خادم الإدارة • مستودع حزم توزيع التطبيقات للتثبيت عن بُعد • شهادة خادم الإدارة • مفاتيح الترخيص المستخدمة بواسطة خادم الإدارة والتطبيقات المدارة • خوادم الإدارة الافتراضية • إعدادات سياسة عميل الشبكة • قواعد نقل الجهاز • قواعد وضع العلامات على الأجهزة تلقائيًا • نقاط التوزيع • إعدادات تطبيق Kaspersky المحفوظة على خادم الإدارة
إصدارات Kaspersky Security Center التي تدعم الترحيل	• أي إصدار مدعوم من Kaspersky Security Center Windows • Kaspersky Security Center Linux الإصدار 15.2 أو أحدث	• Kaspersky Security Center Windows الإصدار 14.2 أو أحدث • Kaspersky Security Center Linux الإصدار 15 أو أحدث
أنظمة إدارة قواعد البيانات التي يمكن إجراء الترحيل بينها	• Microsoft SQL Server ← MySQL، MariaDB • Microsoft SQL Server ← PostgreSQL، Postgres Pro (فقط للترحيل من Kaspersky Security Center Windows الإصدار 14.2 أو أحدث مع تثبيت التصحيح إلى Kaspersky Security Center Linux الإصدار 15.3 أو أحدث) • MySQL ← MySQL، MariaDB • MariaDB ← MySQL، MariaDB • PostgreSQL ← PostgreSQL • Postgres Pro ← Postgres Pro (فقط للترحيل من Kaspersky Security Center Windows الإصدار 15.1 أو أحدث إلى Kaspersky Security Center Linux الإصدار 16 أو أحدث)	الترحيل بين أنظمة إدارة قواعد البيانات المدعومة دون قيود

الترحيل إلى Kaspersky Security Center Linux باستخدام النسخ الاحتياطي للبيانات في خادم الإدارة

يمكنك استخدام نسخة احتياطية من البيانات لترحيل بيانات خادم إدارة Kaspersky Security Center Windows إلى Kaspersky Security Center Linux. وقبل الترحيل، تأكد من دعم الميزات الضرورية لتطبيق Kaspersky Security Center Windows في Kaspersky Security Center Linux.

القيود:

- يمكن إجراء الترحيل بين أنظمة إدارة قواعد البيانات التالية:
  - Microsoft SQL Server ← MySQL، MariaDB
  - Microsoft SQL Server ← PostgreSQL و Postgres Pro
  - MySQL ← MySQL، MariaDB
  - MariaDB ← MySQL، MariaDB
  - PostgreSQL ← PostgreSQL
  - Postgres Pro ← Postgres Pro
- يتم دعم ترحيل بيانات خادم الإدارة المخزنة في قاعدة بيانات Microsoft SQL Server أو MySQL أو MariaDB إلى MySQL أو MariaDB للترحيل من أي إصدار مدعوم من Kaspersky Security Center Windows إلى Kaspersky Security Center Linux الإصدار 15.2 أو أحدث.
- يتم دعم ترحيل بيانات خادم الإدارة المخزنة في قاعدة بيانات PostgreSQL إلى PostgreSQL أو Postgres Pro إلى Postgres Pro من Kaspersky Security Center Windows الإصدار 15.1 أو أحدث إلى Kaspersky Security Center Linux الإصدار 16 أو أحدث.
- يتم دعم ترحيل بيانات خادم الإدارة المخزنة في قاعدة بيانات Microsoft SQL Server إلى PostgreSQL أو Postgres Pro للترحيل من Kaspersky Security Center Windows الإصدار 14.2 أو أحدث إلى Kaspersky Security Center Linux الإصدار 15.3 أو أحدث.

  لدعم الترحيل إلى PostgreSQL أو Postgres Pro، يمكنك تنفيذ أحد الإجراءات التالية:

  - تثبيت التصحيح 15.1.0.20748-pf2 لخادم إدارة Kaspersky Security Center Windows. اتصل بالدعم الفني في Kaspersky للحصول على هذا التصحيح.
  - قم بتحديث Kaspersky Security Center Windows إلى الإصدار 15.1.0.22239.
- إذا كنت تستخدم MySQL أو MariaDB كنظام لإدارة قواعد البيانات لتطبيق Kaspersky Security Center Windows و Kaspersky Security Center Linux، فيجب أن تتطابق معلمة `lower_case_table_names` مع نظامي إدارة قواعد البيانات الحالي والجديد.

  قبل إنشاء نسخة احتياطية للبيانات، تحقق من معلمة `lower_case_table_names`. بعد ذلك، عند تثبيت MySQL أو MariaDB لتطبيق Kaspersky Security Center Linux، يجب عليك تعيين هذه المعلمة إلى القيمة نفسها المحددة لهذه المعلمة لنظام Windows.

المراحل

تتم عملية الترحيل باستخدام النسخ الاحتياطي للبيانات على خادم الإدارة على عدة مراحل:

1. **تأكد من امتلاكك حساب المستخدم الداخلي للمسؤول الذي يمكنك استخدامه لتسجيل الدخول إلى خادم الإدارة.**

   سيُستخدم حساب المسؤول لتسجيل الدخول إلى خادم إدارة Kaspersky Security Center Linux. وإذا لم يكن لديك هذا الحساب، وسجلت الدخول باستخدام حساب Windows محلي أو حساب نطاق فقط، فلن تتمكن من تسجيل الدخول إلى خادم إدارة Kaspersky Security Center Linux بعد استعادة النسخة الاحتياطية. ولا يدعم خادم إدارة Kaspersky Security Center Linux تسجيل الدخول باستخدام حساب Windows المحلي. ومن الممكن تسجيل الدخول باستخدام حساب النطاق، لكن قد يتطلب ذلك تكوينًا إضافيًا لخادم الإدارة.

   إذا لم يكن لديك حساب المسؤول، فسوف يتعين عليك إنشاء هذا الحساب بعد استعادة نسخة النسخ الاحتياطي باستخدام الأداة المساعدة kladduser.

2. **إنشاء نسخة احتياطية محدثة لبيانات خادم إدارة Kaspersky Security Center Windows**

اعتمادًا على نوع نظام إدارة قواعد البيانات (DBMS) المستخدم لبرنامج Kaspersky Security Center Windows و Kaspersky Security Center Linux، نفذ أحد الإجراءات التالية:

- للترحيل إلى MySQL أو MariaDB إلى MySQL أو MariaDB: أنشئ نسخة احتياطية باستخدام الأداة المساعدة klbackup أو مهمة النسخ الاحتياطي للبيانات على الأجهزة المثبت عليها خادم الإدارة.
- لترحيل PostgreSQL إلى PostgreSQL و Postgres Pro إلى Postgres Pro: انشئ نسخة احتياطية باستخدام الأداة المساعدة klbackup أو مهمة النسخ الاحتياطي للبيانات على الجهاز المُثبت عليه خادم الإدارة.
- لترحيل Microsoft SQL Server إلى MySQL أو MariaDB: أنشئ نسخة احتياطية باستخدام الأداة المساعدة klbackup مع تمكين خيار **الانتقال إلى تنسيق MySQL / MariaDB**.
- لترحيل Microsoft SQL Server إلى PostgreSQL أو Postgres Pro:

1. اطلب من الدعم الفني من Kaspersky وقم بتثبيت التصحيح 15.1.0.20748-pf2 لخادم الإدارة لدعم الترحيل إلى PostgreSQL و Postgres Pro.

   بدلاً من ذلك، يمكنك تحديث Kaspersky Security Center Windows إلى الإصدار 15.1.0.22239.

2. أنشئ نسخة احتياطية باستخدام الأداة المساعدة klbackup.

   إذا قمت بتشغيل klbackup من سطر الأوامر، استخدم علامة `migrate postgres-`.

   إذا كنت تستخدم واجهة klbackup، فقم بتمكين خيار **Migrate to Postgres format**.

بعد إنشاء نسخة احتياطية، افصل خادم إدارة Kaspersky Security Center Windows عن الشبكة.

3 تحضير جهاز جديد لتثبيت Kaspersky Security Center Linux

في هذه المرحلة من السيناريو، نفذ ما يلي:

1. حدد جهازًا جديدًا لتثبيت خادم الإدارة عليه. ويجب أن يتوافق هذا الجهاز مع متطلبات الأجهزة والبرامج. وتحقق أيضًا من توفر المنافذ المستخدمة على خادم الإدارة.

2. تعيين العنوان نفسه للجهاز الجديد.

   يمكن تعيين اسم NetBIOS و FQDN وعنوان IP الثابت لخادم الإدارة الجديد. ويعتمد ذلك على عنوان خادم الإدارة الذي تم تعيينه في حزمة تثبيت عميل الشبكة عند نشر عملاء الشبكة. وبدلاً من ذلك، يمكنك استخدام عنوان الاتصال الذي يحدد خادم الإدارة الذي يتصل به عميل الشبكة (يمكنك الحصول على هذا العنوان على الأجهزة المُدارة باستخدام الأداة المساعدة klnagchk).

4 تثبيت وتكوين نظام إدارة قواعد البيانات

في هذه المرحلة من السيناريو، نفذ ما يلي:

1. حدد نوع نظام إدارة قاعدة البيانات الذي يوفر الأداء الأمثل. وضع في الاعتبار عدد الأجهزة المتصلة بالشبكة، وتركيب بنية الشبكة، وحجم العمل على الشبكة. يمكنك اختيار أحد الإصدارات المدعومة من DBMSs.

2. قم بتثبيت نظام إدارة قاعدة البيانات وفقًا لنوع نظام إدارة قاعدة البيانات المحدد عند إنشاء نسخة احتياطية. لمزيد من المعلومات عن كيفية تثبيت نظام إدارة قاعدة البيانات المحدد، يُرجى الرجوع إلى مستنداته.

   لا يجب أن يكون إصدار قواعد البيانات الجديد أقل من الإصدار الحالي.

3. تكوين نظام إدارة قواعد البيانات للعمل مع Kaspersky Security Center Linux.

5 **تثبيت Kaspersky Security Center Linux**

قم بتثبيت Kaspersky Security Center Linux على الجهاز الجديد.

سيتم فقدان حساب المستخدم الداخلي للمسؤول الذي أُنشئ أثناء التثبيت، بالإضافة إلى الكائنات الأخرى (المجموعات، السياسات، المهام، المستخدمون) التي أُنشئت قبل استعادة بيانات خادم الإدارة من النسخة الاحتياطية، بعد عملية الاستعادة. وسوف تُستبدل هذه الكائنات لتحل محلها الكائنات الموجودة في النسخة الاحتياطية.

6 **استعادة بيانات خادم الإدارة من النسخة الاحتياطية**

في هذه المرحلة من السيناريو، نفذ ما يلي:

1. استعادة بيانات خادم الإدارة على الجهاز الجديد باستخدام الأداة المساعدة klbackup.

2. إذا لم يكن لديك حساب المستخدم الداخلي للمسؤول الذي كنت تستخدمه لتسجيل الدخول إلى خادم إدارة Kaspersky Security Center Windows وكنت تستخدم حساب Windows محليًا أو حساب نطاق فقط، فأنشئ حساب مسؤول باستخدام الأداة المساعدة kladduser على النحو التالي:

```
<password> opt/kaspersky/ksc64/sbin/kladduser -n ksc -p/
```

حيث يفي المعامل `<password>` بالمتطلبات التالية:

- يجب ألا تقل كلمة مرور المستخدم عن 8 أحرف ولا تزيد عن 256 حرفًا.
- يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
  - الأحرف الكبيرة (A-Z)
  - الأحرف الصغيرة (a-z)
  - الأعداد (0-9)
  - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7 **تثبيت Kaspersky Security Center Web Console وتكوين خادم الإدارة**

في هذه المرحلة من السيناريو، نفذ ما يلي:

1. قم بتثبيت Kaspersky Security Center Web Console.

في حالة تثبيت Kaspersky Security Center Web Console في وقت سابق، فأعد تثبيته باستخدام ملف الاستجابة نفسه.

سجل الدخول إلى Kaspersky Security Center Web Console تحت حساب المستخدم الداخلي للمسؤول.

تستغرق عملية تهيئة البيانات عادةً ما يصل إلى 15 دقيقة بعد استعادة بيانات خادم الإدارة، لكن الوقت يعتمد على أداء الأجهزة وحجم بيانات خادم الإدارة. وخلال هذا الوقت، قد يفشل Kaspersky Security Center Web Console في الاتصال ويعرض أخطاء.

2. تحقق من وظائف ميزات خادم المسؤول الرئيسي عند اكتمال تهيئة البيانات في قواعد البيانات. وتأكد أن خادم الإدارة يتزامن مع الأجهزة المُدارة وتم استرداد بيانات خادم الإدارة.

3. قم باستقصاء وحدات تحكم نطاق لاستعادة المعلومات عن بنية النطاق وحسابات المستخدمين ومجموعات الأمان وأسماء DNS للأجهزة المضمنة في النطاقات.

4. إذا لزم الأمر، قم بإلغاء تثبيت خادم الإدارة وخادم قاعدة البيانات من الجهاز السابق.

يجب ألا تكون هناك خوادم إدارة متعددة على الشبكة نفسها مع عنوان الاتصال وشهادة خادم الإدارة نفسهما.

يتمتع المسؤول بإمكانية الوصول إلى بيانات خادم الإدارة والأجهزة المُدارة التي كانت في Kaspersky Security Center Windows، مع الوضع في الاعتبار الوظائف المدعومة في Kaspersky Security Center Linux.

الترحيل إلى Kaspersky Security Center Linux باستخدام معالج الترحيل

باتباع هذا السيناريو، يمكنك نقل بنية مجموعة الإدارة والأجهزة المُدارة المضمنة وكائنات المجموعة الأخرى (السياسات والمهام والمهام العامة والعلامات وتحديدات الأجهزة)، من Kaspersky Security Center Windows تحت إدارة Kaspersky Security Center Linux. وقبل الترحيل، تأكد من دعم الميزات الضرورية لتطبيق Kaspersky Security Center Windows في Kaspersky Security Center Linux.

القيود:

- لا يمكن إجراء الترحيل إلا من Kaspersky Security Center Windows الإصدار 14.2 أو أحدث إلى Kaspersky Security Center Linux الإصدار 15 أو أحدث.
- يمكنك تنفيذ هذا السيناريو فقط باستخدام Kaspersky Security Center Web Console.

المراحل

يستمر سيناريو الترحيل على مراحل:

1. **اختيار طريقة ترحيل**

يمكنك الترحيل إلى Kaspersky Security Center Linux من خلال معالج الترحيل. تعتمد خطوات معالج الترحيل على ما إذا كانت خوادم الإدارة لحل Kaspersky Security Center Windows وKaspersky Security Center Linux مرتبة في تسلسل هرمي:

- الترحيل باستخدام تسلسل هرمي لخوادم الإدارة:

حدد هذا الخيار إذا كان خادم الإدارة لتطبيق Kaspersky Security Center Windows يعمل كخادم إدارة ثانوي لتطبيق Kaspersky Security Center Linux. أنت تدير عملية الترحيل والتبديل بين الخوادم في مثيل واحد من Kaspersky Security Center Web Console. إذا كنت تفضل هذا الخيار، فيمكنك ترتيب خوادم الإدارة في تسلسل هرمي لتبسيط إجراء الترحيل. ولفعل ذلك، أنشئ التسلسل الهرمي قبل بدء الترحيل.

- الترحيل باستخدام ملف تصدير (أرشيف مضغوط)

حدد هذا الخيار إذا لم يتم ترتيب خوادم الإدارة لحل Kaspersky Security Center Windows وKaspersky Security Center Linux في تسلسل هرمي. يمكنك إدارة عملية الترحيل من خلال مثيلين من Kaspersky Security Center Web Console- مثيل لتطبيق Kaspersky Security Center Windows ومثيل آخر لتطبيق Kaspersky Security Center Linux. وفي هذه الحالة، سوف تستخدم ملف التصدير الذي أنشأته وقمت بتنزيله أثناء التصدير من Kaspersky Security Center Windows وتستورد هذا الملف إلى Kaspersky Security Center Linux.

2. **أنشئ نسخة احتياطية من الشهادة والمفتاح الخاص لخادم إدارة Kaspersky Security Center Windows (خطوة اختيارية)**

قد ترغب في وضع الأجهزة المُدارة تحت إدارة خادم الإدارة الخاص بتطبيق Kaspersky Security Center Linux عن طريق استعادة الشهادة والمفتاح الخاص لخادم الإدارة من نسخة احتياطية. في هذه الحالة، أنشئ نسخة احتياطية من الشهادة والمفتاح الخاص لخادم إدارة Kaspersky Security Center Windows. ثم في المرحلة 6، قم باستعادة الشهادة والمفتاح الخاص.

3. **تصدير البيانات من Kaspersky Security Center Windows**

افتح Kaspersky Security Center Windows ، ثم قم بتشغيل معالج الترحيل.

4. **استيراد البيانات إلى Kaspersky Security Center Linux**

تابع معالج الترحيل لاستيراد البيانات التي تم تصديرها إلى Kaspersky Security Center Linux. إذا تم ترتيب الخوادم في تسلسل هرمي، يبدأ الاستيراد تلقائيًا بعد تصدير ناجح داخل المعالج نفسه. إذا لم يتم ترتيب الخوادم في تسلسل هرمي، فيمكنك متابعة معالج الترحيل بعد التبديل إلى Kaspersky Security Center Linux.

5. **نفذ إجراءات إضافية لنقل الكائنات والإعدادات من Kaspersky Security Center Windows إلى Kaspersky Security Center Linux يدويًا (خطوة اختيارية)**

قد ترغب أيضًا في نقل الكائنات والإعدادات التي لا يمكن نقلها من خلال معالج الترحيل. على سبيل المثال، يمكنك أيضًا تنفيذ ما يلي:

- انقل مفاتيح الترخيص المستخدمة بواسطة خادم الإدارة والتطبيقات المدارة
- تكوين المهام العامة لخادم الإدارة
- تكوين إعدادات سياسة عميل الشبكة
- إنشاء حزم تثبيت التطبيقات
- إنشاء الخوادم الافتراضية
- تعيين وتكوين نقاط التوزيع
- تكوين قواعد نقل الجهاز
- تكوين القواعد لوضع العلامات على الأجهزة تلقائيًا
- إنشاء فئات التطبيقات

6 انقل الأجهزة المدارة المستوردة تحت إدارة Kaspersky Security Center Linux

لإكمال الترحيل، انقل الأجهزة المدارة المستوردة تحت إدارة Kaspersky Security Center Linux. ويمكنك فعل ذلك بإحدى الطرق التالية:

- من خلال الأداة المساعدة klmover

استخدم الأداة المساعدة klmover وحدد إعدادات الاتصال لخادم الإدارة الجديد.

- من خلال مهمة Change Administration Server

أنشئ مهمة تغيير خادم الإدارة، وحدد الأجهزة المدارة المستوردة، وخادم الإدارة الجديد، وإعدادات المهام الأخرى. بعد ذلك، قم بتشغيل المهمة لوضع الأجهزة المدارة تحت إدارة خادم الإدارة لتطبيق Kaspersky Security Center Linux.

- من خلال الإزالة (إذا كان مثبتًا بالفعل) والتثبيت الإضافي لعميل الشبكة على الأجهزة المدارة

أنشئ حزمة تثبيت جديدة لعميل الشبكة وحدد إعدادات الاتصال لخادم الإدارة الجديد في خصائص حزمة التثبيت. وقم بإزالة عميل الشبكة على الأجهزة المدارة المستوردة، ثم استخدم حزمة التثبيت لتثبيت عميل الشبكة على الأجهزة المدارة المستوردة من خلال مهمة تثبيت عن بُعد. يمكنك أيضًا إنشاء واستخدام حزمة تثبيت مستقلة لتثبيت عميل الشبكة محليًا. وللمزيد من المعلومات، راجع تبديل الأجهزة المدارة تحت إدارة Kaspersky Security Center Linux.

- من خلال استعادة الشهادة والمفتاح الخاص لخادم الإدارة من نسخة احتياطية (فقط للترحيل إلى Kaspersky Security Center Linux 15.1 أو أحدث).

قم بتعيين عنوان الشبكة نفسه للجهاز الذي يستخدم خادم الإدارة في Kaspersky Security Center Linux كما هو الحال على خادم الإدارة في Kaspersky Security Center Windows. قم بتشغيل الأداة المساعدة klbackup مع المعلمة `-cert_only` لاستعادة شهادة خادم الإدارة والمفتاح الخاص من نسخة النسخ الاحتياطي التي قمت بحفظها في المرحلة 2. في سطر الأوامر، نفذ الأمر التالي: /
`path to the backup copy of Administration > opt/kaspersky/ksc64/sbin/klbackup -path`
`restore -cert_only- < Server certificate`. وللمزيد من المعلومات، انظر استخدام الأداة المساعدة klbackup لتبديل الأجهزة المدارة تحت إدارة خادم إدارة آخر.

7 تحديث عميل الشبكة إلى أحدث إصدار

نوصي بترقية عميل الشبكة لنظام Linux إلى إصدار Kaspersky Security Center نفسه.

8 تأكد أن الأجهزة المُدارة مرئية على خادم الإدارة الجديد

على خادم إدارة Kaspersky Security Center Linux، افتح قائمة الأجهزة المُدارة (**Assets (Devices)** ← **Managed devices**)، وتحقق من القيم في الأعمدة **Visible** و**Network Agent is installed** و **Last connected to Administration Server**.

طرق أخرى لترحيل البيانات

بالإضافة إلى معالج الترحيل، يمكنك أيضًا نقل مهام وسياسات معينة:

- ويمكنك تصدير المهام من Kaspersky Security Center Windows، ثم استيراد المهام إلى Kaspersky Security Center Linux.
- قم بتصدير سياسات معينة من Kaspersky Security Center Windows، ثم قم باستيراد السياسات إلى Kaspersky Security Center Linux. يتم تصدير ملفات تعريف السياسة ذات الصلة واستيرادها مع السياسات المحددة.

تصدير كائنات المجموعة من Kaspersky Security Center Windows

يتطلب هيكل مجموعة إدارة الترحيل والأجهزة المدارة المدرجة وكائنات المجموعة الأخرى من Kaspersky Security Center Windows إلى Kaspersky Security Center Linux أن تحدد أولاً البيانات للتصدير وإنشاء ملف تصدير. ويحتوي ملف التصدير على معلومات عن كل كائنات المجموعة التي تريد ترحيلها. وسيتم استخدام ملف التصدير للاستيراد التالي إلى Kaspersky Security Center Linux.

يمكنك تصدير العناصر التالية:

- مهام وسياسات التطبيقات المدارة
- المهام العالمية
- تحديدات الجهاز المخصص
- هيكل مجموعة الإدارة والأجهزة المضمنة
- العلامات التي تم تخصيصها للأجهزة المراد تصديرها

قبل بدء التصدير، اقرأ معلومات عامة عن الترحيل إلى Kaspersky Security Center Linux. اختر طريقة الترحيل - باستخدام التسلسل الهرمي لخوادم الإدارة لتطبيق Kaspersky Security Center Windows وKaspersky Security Center Linux أو عدم استخدامه.

لتصدير الأجهزة المدارة ومجموعة الكائنات ذات الصلة من خلال معالج الترحيل:

1. اعتمادًا على ما إذا كانت الخوادم الإدارية لتطبيق Kaspersky Security Center Windows وKaspersky Security Center Linux مرتبة في تسلسل هرمي، نفذ أحد الإجراءات التالية:
   - إذا تم ترتيب الخوادم في تسلسل هرمي، فافتح Kaspersky Security Center Web Console، ثم قم بالتبديل إلى خادم Kaspersky Security Center Windows.
   - إذا لم يتم ترتيب الخوادم في تسلسل هرمي، فافتح Kaspersky Security Center Web Console المتصل بـ Kaspersky Security Center Windows.
2. في القائمة الرئيسية، انتقل إلى **Operations** ← **Migration**.
3. لبدء المعالج واتباع خطواته، حدد المكان الذي تريد نقل بياناتك وإعداداته.
   - إذا كنت تريد نقل بياناتك وإعداداتك إلى Kaspersky Security Center Cloud Console، فحدد **Migrate to Kaspersky Security Center Cloud Console**.
   - إذا كنت تريد نقل بياناتك وإعداداتك إلى Kaspersky Security Center Linux أو Kaspersky Next XDR Expert، فحدد **Migrate to Kaspersky Security Center Linux or Open Single Management Platform**.
4. حدد مجموعة الإدارة أو المجموعة الفرعية لتصديرها. يرجى التأكد من أن مجموعة الإدارة أو المجموعة الفرعية المحددة لا تحتوي على أكثر من 10000 جهاز.

5. حدد التطبيقات المدارة التي سيتم تصدير مهامها وسياساتها. حدد فقط التطبيقات التي يدعمها Kaspersky Security Center Linux. سيستمر تصدير عناصر التطبيقات غير المدعومة، لكنها لن تكون قابلة للتشغيل.

6. استخدم الروابط الموجودة على اليسار لتحديد المهام العامة، وتحديدات الجهاز، والتقارير المراد تصديرها. يسمح لك رابط **Group objects** باستبعاد الأدوار المخصصة، والمستخدمين الداخليين، ومجموعات الأمان، وفئات التطبيقات المخصصة من التصدير.

يتم إنشاء ملف التصدير (أرشيف مضغوط). اعتمادًا على ما إذا كنت تجري الترحيل أم لا باستخدام دعم التدرج الهرمي لخادم الإدارة، يتم حفظ ملف التصدير على النحو التالي:

- في حالة ترتيب الخوادم في تسلسل هرمي، سيتم حفظ ملف التصدير في المجلد المؤقت على Kaspersky Security Center Web Console Server.
- إذا لم يتم ترتيب الخوادم في تسلسل هرمي، سيتم تنزيل ملف التصدير إلى جهازك.

وللترحيل مع دعم التدرج الهرمي لخادم الإدارة، يبدأ الاستيراد تلقائيًا بعد نجاح التصدير. للترحيل بدون دعم التدرج الهرمي لخادم الإدارة، يمكنك استيراد ملف التصدير المحفوظ إلى Kaspersky Security Center Linux يدويًا.

استيراد ملف التصدير إلى Kaspersky Security Center Linux

لنقل معلومات عن الأجهزة المُدارة والكائنات وإعداداتها التي قمت بتصديرها من Kaspersky Security Center Windows، يجب عليك استيرادها إلى Kaspersky Security Center Linux أو Kaspersky Next XDR Expert.

لاستيراد الأجهزة المدارة والكائنات ذات الصلة من خلال معالج الترحيل:

1. اعتمادًا على ما إذا كانت الخوادم الإدارية لـ Kaspersky Security Center Windows و Kaspersky Security Center Linux مرتبة في تسلسل هرمي، قم بأحد الإجراءات التالية:

- في حالة ترتيب الخوادم في تسلسل هرمي، تابع إلى الخطوة التالية من معالج الترحيل بعد اكتمال التصدير. يبدأ الاستيراد تلقائيًا بعد نجاح عملية التصدير داخل هذا المعالج (راجع الخطوة 2 من هذه التعليمات).
- إذا لم يتم ترتيب الخوادم في تسلسل هرمي:

a. افتح Kaspersky Security Center Web Console المتصل بتطبيق Kaspersky Security Center Linux أو Kaspersky Next XDR Expert.

b. في القائمة الرئيسية، انتقل إلى **Operations** ← **Migration**.

c. حدد ملف التصدير (أرشيف ZIP) الذي قمت بإنشائه وتنزيله أثناء التصدير من Kaspersky Security Center Windows. يبدأ تحميل ملف التصدير.

2. بعد تحميل ملف التصدير بنجاح، يمكنك متابعة الاستيراد. إذا كنت تريد تحديد ملف تصدير آخر، فانقر فوق الرابط **تغيير**، ثم حدد الملف المطلوب.

3. يتم عرض التسلسل الهرمي الكامل لمجموعات إدارة Kaspersky Security Center Linux.

حدد خانة الاختيار المجاورة لمجموعة الإدارة المستهدفة التي يجب استعادة كائنات مجموعة الإدارة المُصدرة إليها (الأجهزة المدارة والسياسات والمهام وكائنات المجموعة الأخرى).

4. يبدأ استيراد كائنات المجموعة. لا يمكنك تصغير معالج الترحيل وإجراء أي عمليات متزامنة معه أثناء الاستيراد. انتظر حتى يتم استبدال رموز التحديث (🔄) بجوار جميع العناصر في قائمة الكائنات بعلامات الاختيار الخضراء (✓) وينتهي الاستيراد.

5. عند اكتمال الاستيراد، تظهر البنية المصدرة لمجموعات الإدارة، بما في ذلك تفاصيل الجهاز، ضمن مجموعة الإدارة المستهدفة التي حددتها. إذا كان اسم الكائن الذي قمت باستعادته مطابقًا لاسم كائن موجود بالفعل، سيتم إضافة لاحقة تزايدية إلى آخر اسم الكائن الذي تم استعادته.

إذا تم تحديد تفاصيل الحساب الذي يتم تشغيل المهمة تحته في مهمة تم ترحيلها، فيجب عليك فتح المهمة وإدخال كلمة المرور مرة أخرى بعد اكتمال الاستيراد.

إذا اكتمل الاستيراد مع وجود خطأ، فيمكنك تنفيذ أحد الإجراءات التالية:

- للترحيل مع دعم التدرج الهرمي لخادم الإدارة، يمكنك البدء في استيراد ملف التصدير مرة أخرى.
- للترحيل بدون دعم التدرج الهرمي لخادم الإدارة، يمكنك بدء معالج الترحيل لتحديد ملف تصدير آخر، ثم استيراده مرة أخرى.

يمكنك التحقق مما إذا كان قد تم استيراد كائنات المجموعة المضمنة في نطاق التصدير بنجاح إلى Kaspersky Security Center Linux. ولفعل ذلك، انتقل إلى قسم **Assets (Devices)** وتأكد من ظهور الكائنات المستوردة في الأقسام الفرعية المقابلة.

لاحظ أن الأجهزة المُدارة المستوردة معروضة في القسم الفرعي **Managed devices**، لكنها غير مرئية في الشبكة ولا يتم تثبيت عميل الشبكة عليها (لا توجد قيمة في الأعمدة **Visible**، و**Network Agent is installed** و**Network Agent is running**).

لإكمال الترحيل، تحتاج إلى تبديل الأجهزة المدارة لتكون تحت إدارة Kaspersky Security Center Linux.

تبديل الأجهزة المدارة لتكون تحت إدارة Kaspersky Security Center Linux

بعد الاستيراد الناجح للمعلومات عن الأجهزة المدارة والكائنات وإعداداتها إلى Kaspersky Security Center Linux، تحتاج إلى تبديل الأجهزة المدارة لتكون تحت إدارة Kaspersky Security Center Linux لإكمال الترحيل.

يمكنك نقل الأجهزة المُدارة لتكون تحت Kaspersky Security Center Linux بإحدى الطرق التالية:

- استخدام الأداة المساعدة klmover.
- استخدام مهمة Change Administration Server.
- استعادة الشهادة والمفتاح الخاص لخادم الإدارة من نسخة احتياطية (فقط للترحيل إلى Kaspersky Security Center Linux 15.1 أو أحدث).

  للحصول على التفاصيل، راجع المرحلة 6 من سيناريو الترحيل الرئيسي.
- تثبيت عميل الشبكة على الأجهزة المُدارة من خلال مهمة التثبيت عن بُعد.

لتبديل الأجهزة المدارة لتكون تحت إدارة Kaspersky Security Center Linux عن طريق تثبيت عميل الشبكة:

1. قم بإزالة عميل الشبكة على الأجهزة المُدارة المستوردة التي سيتم تحويلها تحت إدارة Kaspersky Security Center Linux.
2. قم بالتبديل إلى خادم إدارة Kaspersky Security Center Windows.
3. انتقل إلى **Installation packages** ← **Deployment & assignment** ← **Discovery & deployment**، ثم افتح خصائص حزمة تثبيت حالية من عميل الشبكة.

   إذا كانت حزمة تثبيت عميل الشبكة غير موجودة في قائمة الحزم، فقم بتنزيل حزمة جديدة.

   يمكنك أيضًا إنشاء واستخدام حزمة تثبيت مستقلة لتثبيت عميل الشبكة محليًا.
4. في علامة التبويب **Settings**، حدد القسم **Connection**. حدد إعدادات الاتصال لخادم إدارة Kaspersky Security Center Linux.
5. أنشئ مهمة التثبيت عن بعد للأجهزة المدارة المستوردة، ثم حدد حزمة تثبيت عميل الشبكة المعاد تكوينها.

   يمكنك تثبيت عميل الشبكة من خلال خادم إدارة Kaspersky Security Center Windows أو من خلال جهاز يعمل بنظام التشغيل Windows والذي يعمل بمثابة نقطة توزيع. إذا كنت تستخدم خادم الإدارة، فقم بتمكين الخيار **Using operating system resources through Administration Server**. إذا كنت تستخدم نقطة توزيع، فقم بتمكين الخيار **Using operating system resources through distribution points**.
6. وقم بتشغيل مهمة التثبيت عن بُعد.

بعد انتهاء مهمة التثبيت عن بعد بنجاح، انتقل إلى خادم إدارة Kaspersky Security Center Linux وتأكد أن الأجهزة المُدارة مرئية في الشبكة، ومن تثبيت عميل الشبكة وتشغيله عليها (القيمة نعم في الأعمدة **Visible** و**Network Agent is installed** و**Network Agent is running**).

تسجيل الدخول إلى Kaspersky Security Center Web Console وتسجيل الخروج منها

يمكنك تسجيل الدخول إلى Kaspersky Security Center Web Console. بعد أن تقوم بتثبيت خادم الإدارة وخادم Web Console. يجب أن تعلم عنوان الويب لخادم الإدارة ورقم المنفذ المحدد في التثبيت (افتراضيًا يكون المنفذ هو 8080). يجب تفعيل JavaScript في مستعرضك.

يمكنك تسجيل الدخول إلى Kaspersky Security Center Web Console باستخدام الطرق التالية:

- باستخدام مصادقة المجال

إذا اخترت هذه الطريقة، تأكد من تفعيل استقصاء وحدة تحكم المجال وإضافة مستخدمي المجال إلى خادم الإدارة.

- من خلال تحديد اسم مستخدم المجال وكلمة المرور
- من خلال تحديد اسم المستخدم وكلمة المرور الخاصين بالمسؤول

يجب تعيين دور لحساب المستخدم الذي تريد تسجيل الدخول باستخدامه إلى Kaspersky Security Center Web Console. قبل تسجيل الدخول، تأكد من تعيين دور للمجال أو لحساب المستخدم الداخلي. وإلا، سيحدث خطأ في تسجيل الدخول.

تسجيل الدخول باستخدام مصادقة المجال

لتسجيل الدخول إلى Kaspersky Security Center Web Console باستخدام مصادقة المجال:

1. في المستعرض الخاص بك، انتقل إلى https://<عنوان Kaspersky Security Center Web Console>:<رقم المنفذ>
   يتم عرض صفحة تسجيل الدخول.
2. إذا أضفت عدة خوادم موثوقة، حدد خادم الإدارة الذي ترغب في الاتصال به في قائمة خوادم الإدارة.
   إذا أضفت خادم إدارة واحد فقط، فلن يتم عرض قائمة خوادم الإدارة.
3. قم بأحد الإجراءات التالية:
   - انقر فوق الزر **Use domain authentication**.
   - في حالة إنشاء خادم إدارة افتراضي واحد أو أكثر على الخادم وتريد تسجيل الدخول إلى خادم افتراضي باستخدام مصادقة المجال:
     a. انقر على **Show virtual Server options**.
     b. اكتب اسم خادم الإدارة الظاهري الذي حددته أثناء إنشاء الخادم الإفتراضي .
     c. انقر فوق الزر **Use domain authentication**.

4. إذا تم تمكين التحقق بخطوتين لحسابك، فحدد رمز الأمان الذي تم إنشاؤه بواسطة تطبيق المصادقة على الجهاز المحمول.

يمكنك العودة إلى صفحة تسجيل الدخول إذا لزم الأمر.

بعد تسجيل الدخول، سيتم عرض لوحة التحكم، وتحتوي على اللغة والسمة اللذين استخدمتهما في آخر مرة. يمكنك التنقل عبر Kaspersky Security Center Web Console واستخدامه في العمل مع Kaspersky Security Center.

تسجيل الدخول بتحديد اسم المستخدم وكلمة المرور الخاصين بالمسؤول

لتسجيل الدخول إلى Kaspersky Security Center Web Console عن طريق تحديد اسم المستخدم وكلمة المرور الخاصين بالمسؤول:

1. في المستعرض الخاص بك، انتقل إلى https://<عنوان Kaspersky Security Center Web Console>:<رقم المنفذ>

يتم عرض صفحة تسجيل الدخول.

2. إذا أضفت عدة خوادم موثوقة، حدد خادم الإدارة الذي ترغب في الاتصال به في قائمة خوادم الإدارة.

إذا أضفت خادم إدارة واحد فقط، فلن يتم عرض قائمة خوادم الإدارة.

3. قم بأحد الإجراءات التالية:

- لتسجيل الدخول إلى خادم الإدارة باستخدام حساب مستخدم مجال:

a. أدخل اسم المستخدم وكلمة المرور للمسؤول المحلي.

يمكنك إدخال اسم مستخدم مستخدم المجال بأحد التنسيقات التالية:

- `dns.domain@Username`
- `Username\NTDOMAIN`

b. انقر فوق الزر **تسجيل الدخول**.

قبل تسجيل الدخول باستخدام حساب مستخدم المجال، قم باستقصاء وحدة تحكم المجال للحصول على قائمة مستخدمي المجال.

- لتسجيل الدخول إلى خادم الإدارة:

a. أدخل اسم المستخدم وكلمة المرور للمسؤول المحلي.

b. انقر فوق الزر **تسجيل الدخول**.

- في حالة إنشاء خادم إدارة افتراضي واحد أو أكثر على الخادم وتريد تسجيل الدخول إلى خادم افتراضي:

a. انقر على **Show virtual Server options**.

b. اكتب اسم خادم الإدارة الظاهري الذي حددته أثناء إنشاء الخادم الإفتراضي .

c. أدخل اسم المستخدم وكلمة المرور للمسؤول الذي لديه حقوق على خادم الإدارة الإفتراضي.

d. انقر فوق الزر **تسجيل الدخول**.

4. إذا تم تمكين التحقق بخطوتين لحسابك، فحدد رمز الأمان الذي تم إنشاؤه بواسطة تطبيق المصادقة على الجهاز المحمول.

يمكنك العودة إلى صفحة تسجيل الدخول إذا لزم الأمر.

5. إذا تم تمكين فرض تغيير كلمة المرور لحسابك أو انتهت صلاحية كلمة المرور الخاصة بك، فسيتم عرض نافذة تغيير كلمة المرور. وقم بتعيين كلمة مرور جديدة لتسجيل الدخول إلى Kaspersky Security Center Web Console.

بعد تسجيل الدخول، سيتم عرض لوحة التحكم، وتحتوي على اللغة والسمة اللذين استخدمتهما في آخر مرة. يمكنك التنقل عبر Kaspersky Security Center Web Console واستخدامه في العمل مع Kaspersky Security Center.

تسجيل الخروج

لتسجيل الخروج من Kaspersky Security Center Web Console،

في القائمة الرئيسية، انتقل إلى إعدادات حسابك ثم حدد **Sign out**.

سيتم إغلاق Kaspersky Security Center Web Console وستظهر صفحة تسجيل الدخول.

إدارة الهوية والوصول في Kaspersky Security Center Web Console

يوفر هذا القسم معلومات حول إدارة الهوية والوصول (يشار إليها أيضا باسم IAM).

حول إدارة الهوية والوصول

يعد مدير الهوية والوصول (يشار إليه أيضًا باسم IAM) أحد مكوناتKaspersky Security Center Web Console، وهو يتيح لك استخدام تسجيل دخول أحادي (SSO) بين Kaspersky Security Center Web Console وواجهة ويب Kaspersky Industrial CyberSecurity for Networks. يستخدم IAM بروتوكول OAuth 2.0 لضمان ترخيص Kaspersky Industrial CyberSecurity for Networks في Kaspersky Security Center Web Console.

في هذه الحالة، يُشار إلى Kaspersky Industrial CyberSecurity for Networks، والذي يمكنك الوصول إليه عبر Kaspersky Security Center Web Console، باسم خادم الموارد، ويُشار إلى Kaspersky Security Center Web Console وواجهة ويب Kaspersky Industrial CyberSecurity for Networks باسم عملاء OAuth 2.0. خادم الموارد هو برنامج يعمل مع عدة مستخدمين ويتطلب إذنًا. يستخدم العميل رمزًا مميزًا للترخيص على خادم المورد. الرمز المميز هو تسلسل فريد من البايت. عند انتهاء صلاحية الرمز المميز، يتم إعادة إصداره تلقائيًا. يعمل IAM خادم ترخيص واحد لعملاء OAuth 2.0 المتعدد.

يمكنك تثبيت IAM عتد تثبيت Kaspersky Security Center Web Console. يمكنك تمكينه لاحقا في أي وقت في إعداداتKaspersky Security Center Web Console. إذا تم تثبيت خادم Kaspersky Industrial CyberSecurity أو واجهة ويب Kaspersky Industrial CyberSecurity على جهاز يُدار من خلال خادم الإدارة نفسه، فإن IAM يكتشف هذا البرنامج ويعرض إشعارًا في Kaspersky Security Center لإعلامك بهذا. يمكنك تسجيل Kaspersky Industrial CyberSecurity for Networks واستخدام تسجيل الدخول الأحادي لاحقًا لكل من Kaspersky Security Center Web Console وواجهة ويب Kaspersky Industrial CyberSecurity for Networks.

إذا سجلت الخروج من Kaspersky Security Center Web Console، فستنتهي جلستك في واجهة ويب Kaspersky Industrial CyberSecurity for Networks، وسيتعين عليك تسجيل الدخول إلى Kaspersky Security Center Web Console مرة أخرى.

تمكين إدارة الهوية والوصول: سيناريو

المتطلبات الأساسية

قبل البدء، تأكد من الوصول إلى Kaspersky Industrial CyberSecurity for Networks الإصدار 3.1 أو الأحدث.

المراحل

تمكين إدارة الهوية والوصول: (يشار إليها أيضًا باسم IAM) تستمر على مراحل

1. **التحقق من المنافذ الضرورية**

   تأكد من فتح المنافذ 3333 و4004 و4444 على الجهاز حيث تم تثبيت Kaspersky Security Center Web Console. هذه المنافذ مطلوبة لاستخدام OAuth 2.0. يمكنك تغيير أرقام المنفذ الافتراضية إذا كنت تريد ذلك من نافذة إعدادات Kaspersky Security Center Web Console.

   إلى جانب المنافذ 3333 و4004 و4444، يستخدم Kaspersky Security Center Web Console أيضًا المنافذ 4445 و2444 و2445 لأغراض مختلفة.

2. **تثبيت إدارة الهوية والوصول**

   أثناء تثبيت Kaspersky Security Center Web Console، حدد أنك تريد تثبيت إدارة الهوية والوصول. إذا لم تفعل ذلك، قم بتشغيل معالج إعداد Kaspersky Security Center Web Console مرة أخرى.

3. **تكوين إدارة الهوية والوصول**

   في نافذة إعدادات Kaspersky Security Center Web Console، تأكد من تمكين زر **Identity and Access Manager (IAM)**. حدد أيضًا اسم DNS للجهاز المثبت عليه Kaspersky Security Center Web Console: ستتصل تطبيقات العميل بهذا الجهاز.

4. **تحديد إعدادات الرمز المميز**

   في نافذة إعدادات Kaspersky Security Center Web Console، حدد عمر الرموز المميزة ومهلة التوثيق التي سيستخدمها مدير الهوية والوصول. يمكنك استخدام القيم الافتراضية، أو يمكنك تحديد قيمك الخاصة وفقًا لاحتياجاتك.

5. **إدارة الشهادات**

   إذا كنت تفضل استخدام الشهادات التي يقوم بإنشائها خادم الإدارة، فمن ثم في نافذة إعدادات Kaspersky Security Center Web Console، يُرجى تنزيل الشهادات الجذرية للمنافذ التي يستخدمها IAM، ثم توزيعها على محطات عمل مستخدمي Kaspersky Security Center Web Console. بخلاف ذلك، ستعرض متصفحات المستخدمين رسائل خطأ عند محاولة الاتصال بـ Kaspersky Security Center Web Console.

6. **تسجيل خوادم Kaspersky Industrial CyberSecurity for Networks وواجهات ويب Kaspersky Industrial CyberSecurity for Networks**

   عند تثبيت IAM، يعرض Kaspersky Security Center Web Console رسالة تفيد بأن خادم Kaspersky Industrial CyberSecurity for Networks (أو خوادم عدة)، وواحدة أو أكثر من واجهات ويب Kaspersky Industrial CyberSecurity for Networks في انتظار التسجيل. انقر فوق هذه الرسالة لتسجيل Kaspersky Industrial CyberSecurity for Networks Server (أو عدة خوادم) وواجهة ويب (أو واجهات ويب متعددة).

النتائج

بعد إكمال هذا السيناريو، ستتمكن من استخدام SSO وIAM لتطبيق Kaspersky Industrial CyberSecurity for Networks وKaspersky Security Center Web Console.

تكوين إدارة الهوية والوصول في Kaspersky Security Center Web Console

لتكوين Identity and Access Manager وفقًا لاحتياجاتك:

1. في القائمة الرئيسية انتقل الى **إعدادات** ← **Identity and Access Manager**.
2. في قسم **Identity and Access Manager** تأكد من تفعيل إدارة الهوية والوصول.
3. انقر فوق الرابط **Settings** تحت سطر **Network name of the Identity and Access Manager device**.
4. حدد اسم DNS للجهاز الذي قمت بتثبيت إدارة الهوية والوصول عليه. ستتصل تطبيقات العميل بهذا الجهاز.
5. إذا كنت ترغب في ذلك، فقم بتغيير إعدادات الرمز المميز الافتراضية ، وإعدادات الشهادة و أرقام المنافذ بالنقر فوق الرابط **Settings** الموجود ضمن مجموعة الإعدادات ذات الصلة.

إدارة الهوية والوصول ممكّنة وتعمل وفقًا لاحتياجاتك.

تسجيل تطبيق Kaspersky Industrial CyberSecurity for Networks في Kaspersky Security Center Web Console

لبدء العمل مع تطبيق Kaspersky Industrial CyberSecurity for Networks عبر Kaspersky Security Center Web Console، يجب عليك أولاً تسجيله في Kaspersky Security Center Web Console.

لتسجيل تطبيق Kaspersky Industrial CyberSecurity for Networks:

1. تأكد من القيام بما يلي:
   - قمتَ بتنزيل وتثبيت المكون الإضافي للويب لتطبيق Kaspersky Industrial CyberSecurity for Networks.

     ومع ذلك، يمكنك فعل ذلك لاحقًا أثناء انتظار مزامنة خادم Kaspersky Industrial CyberSecurity for Networks مع خادم الإدارة.
   - لقد أكملت سيناريو الاستعدادات لاستخدام تقنية تسجيل الدخول الأحادي (SSO).
   - تم تحديد الإعدادات الضرورية في واجهة ويب Kaspersky Industrial CyberSecurity for Networks في صفحة Kaspersky Security Center. للمزيد من التفاصيل، يرجى الرجوع إلى تعليمات Kaspersky Industrial CyberSecurity for Networks على الإنترنت.
   - لقد قمت بتسجيل الدخول إلى Kaspersky Security Center Web Console ضمن حساب مسؤول.
   - تم تكوين IAM.

2. انقل الجهاز حيث تم تثبيت Kaspersky Industrial CyberSecurity for Networks Server من مجموعة الأجهزة غير المعينة إلى مجموعة الأجهزة المدارة:

a. في القائمة الرئيسية، انتقل إلى **Unassigned devices** ← **Discovery & deployment**.

b. حدد خانة الاختيار بجوار الجهاز المثبت عليه خادم Kaspersky Industrial CyberSecurity for Networks.

c. انقر على زر **Move to group** .

d. في التسلسل الهرمي لمجموعات الإدارة، حدد خانة الاختيار بجوار مجموعة الأجهزة المُدارة.

e. انقر فوق زر **Move**.

3. تابع إلى خصائص الجهاز حيث تم تثبيت خادم Kaspersky Industrial CyberSecurity for Networks.

4. في صفحة خصائص الجهاز، في قسم **عام**، حدد خيار **عمد قطع الاتصال بخادم الإدارة**، ثم انقر فوق زر **الحفظ** .

5. في نافذة خصائص الجهاز، حدد قسم **التطبيقات**.

6. في قسم **التطبيقات**، حدد وكيل شبكة Kaspersky.

7. إذا كان الوضع الحالي للتطبيق متوقف، فانتظر حتى يتغير إلى مُفَعل.

قد تستغرق هذه العملية حوالي 15 دقيقة. إذا لم تقم بعد بتثبيت المكون الإضافي للويب لتطبيق Kaspersky Industrial CyberSecurity for Networks، فيمكنك فعل ذلك الآن أثناء انتظارك.

8. في القائمة الرئيسية انتقل الى **إعدادات** ← **Identity and Access Manager**.

في حقل **طلبات التسجيل**، يتم عرض طلب معلق واحد.

9. انقر على رابط **الإعدادات** تحت حقل **طلبات التسجيل**.

10. في قائمة العملاء المسجلين التي تفتح، حدد مربع الاختيار الموجود بجوار اسم خادم Kaspersky Industrial CyberSecurity for Networks، والذي يتضمن حالة مُعلق، ثم انقر فوق الزر **موافقة**.

إذا كنت لا ترغب في تسجيل خادم Kaspersky Industrial CyberSecurity for Networks، فيمكنك النقر فوق زر رفض والعودة إلى هذه القائمة لاحقًا.

بعد النقر فوق زر **موافقة**، تتغير الحالة إلى موافقة، ثم إلى مستعد. إذا لم تتغير الحالة، يمكنك النقر فوق زر تحديث.

11. أغلق قائمة العملاء المسجلين وتأكد من أن القيمة الموجودة في حقل **العملاء المسجلين** زادت.

12. لإضافة أداة Kaspersky Industrial CyberSecurity for Networks على لوحة المعلومات:

a. في القائمة الرئيسية، انتقل إلى **Dashboard** ← **Monitoring & reporting**.

b. في لوحة المعلومات، انقر على زر **Add or restore web widget**.

c. في قائمة الأدوات التي تفتح، حدد **أخرى**.

d. حدد أداة Kaspersky Industrial CyberSecurity for Networks.

يمكنك الآن المتابعة إلى واجهة ويب Kaspersky Industrial CyberSecurity for Networks باستخدام الرابط الموجود في الأداة.

بعد إكمال إجراء التسجيل، يظهر زر جديد، **Kaspersky Security Center**، على صفحة تسجيل الدخول لواجهة ويب Kaspersky Industrial CyberSecurity for Networks. يمكنك النقر فوق هذا الزر لتسجيل الدخول إلى واجهة ويب Kaspersky Industrial CyberSecurity for Networks تحت بيانات اعتماد Kaspersky Security Center.

مدة صلاحية الرموز المميزة ومهلة التفويض لإدارة الهوية والوصول

عند تكوين إدارة الهوية والوصول (يشار إليها أيضًا باسم IAM)، يجب عليك تحديد الإعدادات الخاصة بعمر الرمز المميز ومهلة التوثيق. تم تصميم الإعدادات الافتراضية لتعكس كلاً من معايير الأمان وتحميل الخادم. ومع ذلك، يمكنك تغيير هذه الإعدادات وفقًا لسياسات مؤسستك.

تقوم إدارة الهوية والوصول (IAM) تلقائيًا بإعادة إصدار رمز مميز عندما توشك صلاحيته على الانتهاء.

يسرد الجدول أدناه إعدادات عمر الرمز المميز الافتراضية.

إعدادات عمر الرمز المميز

الرمز المميز	المهلة الافتراضية (بالثواني)	الوصف
Identity token (id_token)	86400	رمز الهوية الذي يستخدمه عميل OAuth 2.0 (أي، إما Kaspersky Security Center Web Console أو Kaspersky Industrial CyberSecurity Console). يُرسل IAM الرمز المميز للمعرف الذي يحتوي على معلومات حول المستخدم (أي ملف تعريف المستخدم) إلى العميل.
Access token (access_token)	86400	رمز الوصول المستخدم بواسطة العميل OAuth 2.0 للوصول إلى خادم المورد نيابة عن مالك المورد المحدد بواسطة IAM.
Refresh token (refresh_token)	172800	يستخدم العميل OAuth 2.0 هذا الرمز المميز لإعادة إصدار رمز الهوية ورمز الوصول.

يسرد الجدول أدناه المهلات لرمز المصادقة وlogin_consent_request

إعدادات مهلة المصادقة

تعيين	المهلة الافتراضية (بالثواني)	الوصف
Authorization code (auth_code)	3600	مهلة تبادل الرمز للرمز المميز. يرسل العميل OAuth 2.0 هذا الرمز إلى خادم المورد ويحصل على رمز الوصول في المقابل.
Login consent request timeout (login_consent_request)	3600	انتهت مهلة تفويض حقوق المستخدم للعميل OAuth 2.0.

لمزيد من المعلومات حول الرموز المميزة، راجع موقع ويب OAuth.

لتكوين المهلة للعملاء الذين لم يتم اكتشاف أي نشاط للماوس أو لوحة المفاتيح لديهم:

1. في مجلد تثبيت Kaspersky Security Center Web Console، ابحث عن ملف config.json وافتحه. يحتوي الملف على معلمات لتكوين المهلة للعملاء غير النشطين.

2. استخدم المعلمة `clientIdleTimeout` لتحديد الوقت بالملي ثانية الذي يعرض بعده العميل غير النشط نافذة منبثقة للتحذير.

3. استخدم المعلمة `clientLogoutTimeout` لتحديد الوقت بالملي ثانية الذي يتم بعده إنهاء تفويض IAM للعميل غير النشط. يقوم `clientLogoutTimeout` بالعد التنازلي بالتسلسل بعد `clientIdleTimeout`.

تحميل وتوزيع شهادات IAM

بشكل افتراضي، تستخدم إدارة الهوية والوصول الشهادات التي تم إنشاؤها بواسطة خادم الإدارة لمنح المتصفحات الوصول إلى Kaspersky Security Center Web Console. يمكنك حذفها يدويًا، إذا كنت ترغب في ذلك. مهما كانت الشهادة التي تستخدمها، يجب عليك التأكد من أن جميع محطات العمل التي يصل منها مستخدمو Kaspersky Security Center Web Console إلى Kaspersky Security Center Web Console يثقون بهذه الشهادة.

لتنزيل الشهادات وتوزيعها:

1. في القائمة الرئيسية انتقل الى **إعدادات** ← **Identity and Access Manager**.

2. لكل شهادة ، انقر فوق الارتباط **إعدادات** ضمن مجموعة الإعدادات ذات الصلة، ثم قم بأحد الإجراءات التالية:

- إذا كنت ترغب في استخدام الشهادة التي أنشأها خادم الإدارة أثناء تثبيت Kaspersky Security Center Web Console:

  1. حدد **الشهادة التي تم إنشاؤها بواسطة خادم الإدارة** في نافذة خصائص الشهادة التي تفتح.

  2. انقر فوق زر **تنزيل** للخروج من النافذة.

  3. وزع الشهادة التي تم تنزيلها على جميع محطات العمل التي يصل من خلالها مستخدمو Kaspersky Security Center Web Console إلى Kaspersky Security Center Web Console.

- إذا كانت لديك شهادة تريد استخدامها:

  1. حدد **شهادة TLS المخصصة** في نافذة خصائص الشهادة التي تفتح.

  2. حدد ملف الشهادة والمفتاح الخاص.

  3. انقر على زر **موافق**.

  4. وزع الشهادة على جميع محطات العمل التي يصل المستخدمون من خلالها إلى Kaspersky Security Center Web Console أو Kaspersky Industrial CyberSecurity Console.

تمنح الشهادات المستخدمين الوصول إلى Kaspersky Security Center Web Console وKaspersky Industrial CyberSecurity Console.

عليك إعادة إصدار جميع الشهادات في الوقت المناسب. يجب إعادة إنشاء الشهادات التي تم إنشاؤها من خلال خادم الإدارة يدويًا. يجب إعادة إنشاء الشهادات التي تم أنشاؤها من خلال مُثبتKaspersky Security Center Web Console من خلال استخدام المُثبت.

تعطيل إدارة الهوية والوصول

إذا كنت ترغب في ذلك، فيمكنك تعطيل Identity and Access Manager (يشار إليه أيضًا باسم IAM).

لتعطيل IAM،

1. في القائمة الرئيسية انتقل الى **إعدادات** ← **Integration**.

2. في قسم **Identity and Access Manager**، قم بتبديل زر **Identity and Access Manager** إلى تعطيل.

يمكنك تمكين IAM في أي وقت لاحق.

إذا قمت بتحديث Kaspersky Security Center Web Console عبر المثبت، وحددت أنك لا تريد تثبيت IAM، فستتم ترقية Kaspersky Security Center Web Console ولن يتم تثبيت IAM. ستُحذف جميع المعلومات المتعلقة بالتكامل مع Kaspersky Industrial CyberSecurity for Networks من جهازك، بالإضافة إلى ملفات تكوين IAM وملفات السجل.

تكوين مصادقة المجال باستخدام بروتوكولات NTLM وKerberos

Kaspersky Security Center 15.1 يتيح لك استخدام مصادقة المجال في OpenAPI باستخدام بروتوكولي NTLM و Kerberos. يسمح استخدام مصادقة المجال لمستخدم Windows بتمكين المصادقة الآمنة في Kaspersky Security Center Web Console دون الحاجة إلى إعادة إدخال كلمة المرور على شبكة الشركة (تسجيل الدخول الأحادي).

مصادقة المجال في OpenAPI عبر بروتوكول Kerberos عليها القيود التالية:

- يجب مصادقة مستخدم Kaspersky Security Center Web Console في Active Directory باستخدام بروتوكول Kerberos. يجب أن يكون لدى المستخدم تذكرة منح تذاكر Kerberos صالحة (يشار إليها أيضًا باسم TGT). يتم إصدار TGT تلقائيًا عند مصادقتك على المجال.
- يجب عليك تكوين مصادقة Kerberos في المستعرض. لمعرفة التفاصيل، راجع مستندات المستعرض الذي تستخدمه.

إذا كنت ترغب في استخدام مصادقة المجال باستخدام بروتوكولات Kerberos، يجب أن تفي شبكتك بالشروط التالية:

- يجب تشغيل خادم الإدارة تحت اسم حساب المجال.
- يجب تثبيت Kaspersky Security Center Web Console Server على نفس الجهاز حيث تم تثبيت خادم الإدارة.
- يجب عليك تحديد الأسماء الأساسية للخدمة (SPN) التالية لحساب خادم الإدارة:
  - "<server.fqnd.name>/http"
  - "<server>/http"

  هنا <الخادم> هو اسم شبكة جهاز خادم الإدارة، و<server.fqnd.name> هو اسم FQDN لجهاز خادم الإدارة.
- عند الاتصال بوحدة تحكم الإدارة أو Kaspersky Security Center Web Console، يجب تحديد عنوان خادم الإدارة بالضبط كالعنوان الذي تم تسجيل اسم الخدمة الأساسي (SPN) له. يمكنك تحديد إما <server.fqnd.name> أو <server>.
- لتسجيل الدخول بدون كلمة مرور، يجب أن تعمل عملية المستعرض التي يتم فيها فتح Kaspersky Security Center Web Console كمستعرض تحت حساب مجال.

بروتوكولات Kerberos وNTLM غير مدعومة إلا في OpenAPI لـ Kaspersky Security Center 15.1. لم تعد مدعومة في OpenAPI لتطبيق Kaspersky Security Center Linux.

تكوين خادم الإدارة

يصف هذا القسم عملية التكوين وخصائص خادم إدارة Kaspersky Security Center.

تكوين اتصال Kaspersky Security Center Web Console بخادم الإدارة

لتعيين منافذ التوصيل لخادم الإدارة:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **Connection ports**.

   يعرض التطبيق إعدادات التوصيل الرئيسي للخادم المحدد.

Kaspersky Security Center Web Console متصل بخادم الإدارة عبر منفذ SSL رقم TCP 13299. يمكن استخدام نفس المنفذ بواسطة عناصر أتمتة klakaut.

يمكن استخدام منفذ TCP 14000 للاتصال بتطبيق Kaspersky Security Center Web Console ونقاط التوزيع وخوادم الإدارة الثانوية وكائنات التشغيل التلقائي لأداة klakaut بالإضافة إلى تلقي البيانات من الأجهزة العميلة.

عادةً، لا يمكن استخدام منفذ TCP 13000 SSL إلا بواسطة عميل الشبكة وخادم الإدارة الثانوي وخادم الإدارة الرئيسي في منطقة الأجهزة الموصلة مباشرة بالإنترنت. وفي بعض الحالات، قد يلزم توصيل تطبيق Kaspersky Security Center Web Console عبر منفذ SSL رقم 13000:

- إذا كان من المحتمل استخدام منفذ SSL واحد لتطبيق Kaspersky Security Center Web Console ولأنشطة أخرى (تلقي بيانات من الأجهزة العميلة والاتصال بنقاط التوزيع والاتصال بخوادم الإدارة الثانوية).
- إذا كان كائن التشغيل التلقائي لـ klakaut غير متصل بخادم الإدارة مباشرة لكنه متصل عبر نقطة توزيع في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

تكوين تسجيل أحداث الاتصال بخادم الإدارة

يمكن حفظ محفوظات الاتصالات ومحاولات الاتصال بخادم الإدارة أثناء تشغيله إلى ملف سجل. تسمح لك المعلومات الموجودة في الملف بتعقب ليس فقط الاتصالات داخل البنية الأساسية لشبكتك، ولكن أيضًا المحاولات غير المصرح بها للوصول إلى الخادم.

لتسجيل أحداث الاتصال بخادم الإدارة:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **Connection ports**.

3. قم بتفعيل خيار **Log Administration Server connection events** .

   سيتم حفظ جميع الأحداث الأخرى للاتصالات الواردة إلى خادم الإدارة، ونتائج المصادقة، وأخطاء SSL في ملف %ProgramData%\KasperskyLab\adminkit\logs\syslog.SC.

تكوين إعدادات الوصول إلى الإنترنت لخادم الإدارة

يجب تكوين الوصول إلى الإنترنت لاستخدام Kaspersky Security Network، ولتنزيل تحديثات لقواعد بيانات مكافحة الفيروسات لتطبيق Kaspersky Security Center وتطبيقات Kaspersky المُدارة.

لتحديد إعدادات الوصول إلى الإنترنت لخادم الإدارة:

1. في القائمة الرئيسية، انقر على أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد القسم **Configuring internet access**.

3. قم بتمكين الخيار **Use proxy server** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. وفي حالة تمكين هذا الخيار، ستتوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

   - **Address**

     عنوان الخادم الوكيل المستخدم لاتصال Kaspersky Security Center بالإنترنت.

   - **Port number**

     رقم المنفذ الذي سيتم من خلاله إنشاء اتصال وكيل Kaspersky Security Center.

   - **Bypass proxy server for local addresses**

     لن يتم استخدام خادم وكيل للاتصال بالأجهزة في الشبكة المحلية.

   - **Proxy server authentication**

     إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

     يتوفر حقل الإدخال هذا إذا تم تحديد خانة الاختيار **استخدام الخادم الوكيل**.

   - **User name**

     حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

   - **Password**

     تم تعيين كلمة مرور بواسطة المستخدم الذي تم إنشاء اتصال الخادم الوكيل من خلال حسابه (هذا الحقل متاح في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

     لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار** حتى تظهر لك كلمة المرور.

يمكنك أيضًا تكوين الوصول إلى الإنترنت باستخدام معالج البدء السريع.

تعيين الحد الأقصى لعدد الأحداث في مستودع الأحداث

من القسم **Events repository** في النافذة خصائص خادم الإدارة، يمكنك تحرير إعدادات تخزين الأحداث في قاعدة بيانات خادم الإدارة من خلال تقييد عدد سجلات الأحداث أو مدة تخزين السجل. عندما تحدد الحد الأقصى لعدد الأحداث، يقوم التطبيق بحساب مقدار تقريبي لمساحة التخزين المطلوبة للرقم المحدد. يمكنك استخدام هذا الحساب التقريبي لتقييم ما إذا كانت لديك مساحة خالية كافية على القرص لتجنب تجاوز سعة قاعدة البيانات. السعة الافتراضية لقاعدة بيانات خادم الإدارة هي 400 000 حدث. أقصى سعة موصى بها لقاعدة البيانات هي 45 مليون حدث.

يتحقق التطبيق من قاعدة البيانات كل 10 دقائق. وإذا وصل عدد الأحداث إلى القيمة القصوى المحددة بالإضافة إلى 10 000، فسوف يحذف التطبيق الأحداث الأقدم بحيث يبقى الحد الأقصى لعدد الأحداث المحدد فقط.

عند قيام خادم الإدارة بحذف الأحداث القديمة، فلا يمكن حفظ الأحداث الجديدة في قاعدة البيانات. وأثناء هذه الفترة الزمنية، تتم كتابة معلومات حول الأحداث المرفوضة في سجل أحداث Kaspersky. يتم وضع الأحداث الجديدة في قائمة الانتظار ثم حفظها في قاعدة البيانات بعد اكتمال عملية الحذف.

لتقييد عدد الأحداث التي يمكن تخزينها في مستودع الأحداث بخادم الإدارة:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **Events repository**. حدد الحد الأقصى لعدد الأحداث المخزّنة في قاعدة البيانات.

3. انقر على زر **Save**.

بالإضافة إلى ذلك، يمكنك تنفيذ ما يلي:

- تغيير إعدادات أي مهمة لحفظ الأحداث المتعلقة بتقدم المهمة، أو حفظ نتائج تنفيذ المهمة فقط.
- تقليل أو تعطيل فترة التخزين لأحداث خادم الإدارة وعميل الشبكة وتطبيقات Kaspersky المثبتة على الأجهزة المدارة.

عند فعل ذلك، ستقلل من عدد الأحداث الموجودة في قاعدة البيانات، وتزيد من سرعة تنفيذ السيناريوهات المرتبطة بتحليل جدول الأحداث في قاعدة البيانات وخفض خطر الكتابة فوق الأحداث الحرجة بواسطة عدد كبير من الأحداث.

إعدادات الاتصال لأجهزة حماية UEFI

جهاز حماية UEFI هو جهاز مثبت عليه حل أو تطبيق Kaspersky لواجهة البرامج الثابتة الموحدة القابلة للتوسيع (UEFI) المتكاملة على مستوى BIOS. تضمن الحماية المتكاملة أمن الجهاز من الوقت الذي يبدأ فيه تشغيل النظام، ولكن تبدأ الحماية على الأجهزة دون البرامج المتكاملة في العمل بعد بدء تطبيق الأمن فقط. يدعم Kaspersky Security Center إدارة هذه الأجهزة

لتعديل إعدادات اتصال أجهزة حماية UEFI:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد القسم **Additional ports**.

3. قم بتعديل الإعدادات ذات الصلة:

- **Open port for UEFI protection devices and KasperskyOS devices**

  يمكن لأجهزة حماية UEFI الاتصال بخادم الإدارة.

- **Port for UEFI protection devices and KasperskyOS devices**

  يمكنك تغيير رقم المنفذ إذا تم تمكين الخيار **فتح منفذ لأجهزة حماية جهاز UEFI وأجهزة KasperskyOS**. رقم المنفذ الافتراضي هو 13294.

4. انقر على زر **Save**.

يمكن الآن لأجهزة حماية UEFI الاتصال بخادم الإدارة.

إنشاء تسلسل هرمي من خوادم الإدارة: إضافة خادم إدارة تابع

إضافة خادم إدارة تابع (يتم هذا على خادم الإدارة الثانوي المستقبلي)

يمكنك إضافة خادم إدارة كخادم إدارة تابع والذي يقوم بإنشاء تسلسل هرمي "رئيسي/تابع".

لإضافة خادم إدارة تابع متوفر للتوصيل عبر Kaspersky Security Center Web Console:

1. تأكد أن المنفذ 13000 الخاص بخادم الإدارة الرئيسي المستقبلي متوفر لتلقي الاتصالات من خوادم الإدارة الثانوية.
2. انقر على أيقونة الإعدادات ( ) في خادم الإدارة الرئيسي المستقبلي.
3. في صفحة الخصائص التي تفتح، حدد تبويب **Administration Servers**.
4. حدد خانة الاختيار الموجودة بجوار اسم مجموعات الإدارة التي ترغب في إضافة خادم الإدارة إليها.
5. في سطر القائمة، انقر على **Connect secondary Administration Server**.

   يبدأ تشغيل معالج إضافة خادم إدارة ثانوي. انتقل عبر المعالج من خلال استخدام زر **التالي**.
6. املأ الحقول التالية:

- **Connect primary Administration Server to secondary Administration Server in DMZ**

  حدد هذا الخيار إذا كان خادم الإدارة الثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ).

  إذا تم تحديد هذا الخيار، فستحتاج إلى تحديد المعلمة **عنوان الخادم الثانوي**.

  إذا تم تحديد هذا الخيار، يبدأ خادم الإدارة الأساسي الاتصال بخادم الإدارة الثانوي. وبخلاف ذلك، يبدأ خادم الإدارة الثانوي الاتصال بخادم الإدارة الأساسي.

- **Secondary Administration Server display name**

  اسم يتم من خلاله عرض خادم الإدارة الثانوي في التسلسل الهرمي. إذا أردت، يمكنك إدخال عنوان IP كاسم أو يمكنك استخدام اسم مثل "Secondary Server for group 1".

- **Secondary Administration Server address (optional)**

  حدد عنوان IP أو اسم النطاق لخادم الإدارة الثانوي.

  هذه المعلمة مطلوبة في حالة تمكين الخيار **توصيل خادم الإدارة الأساسي بخادم الإدارة الثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت**.

- **Administration Server SSL port**

  حدد رقم منفذ SSL على خادم الإدارة الرئيسي. رقم المنفذ الافتراضي هو 13000.

- **Administration Server API port**

  حدد رقم المنفذ على خادم الإدارة الرئيسي لتلقي الاتصالات عبر OpenAPI. رقم المنفذ الافتراضي هو 13299.

7. حدد الشهادة لخادم الإدارة الثانوي. إذا حددت المعلمة **عنوان الخادم الثانوي**، فيمكنك النقر فوق الزر **إحضار من خادم الإدارة الثانوي** للحصول على الشهادة. وإلا، فانقر فوق الزر **استعراض إلى ملف الشهادة** وحدد موقع ملف الشهادة.

8. حدد الإعدادات التالية:

- أدخل عنوان خادم الإدارة الأساسي المستقبلي.
- إذا كان خادم الإدارة الثانوي المستقبلي يستخدم خادمًا وكيلاً، فأدخل عنوان الخادم الوكيل وبيانات اعتماد المستخدم للاتصال بالخادم الوكيل.

9. أدخل بيانات اعتماد المستخدم الذي يملك حقوق الوصول على خادم الإدارة الثانوي المستقبلي.

10. في حالة تمكين التحقق ثنائي الخطوات وتكوينه، فحدد رمز الأمان الذي تم إنشاؤه بواسطة تطبيق المصادقة.

إذا تم تمكين التحقق ثنائي الخطوات، لكن لم يتم تكوينه للحساب الذي تحدده، فأنشئ التسلسل الهرمي من الخادم الثانوي المستقبلي (راجع الإرشادات أدناه).

إذا كانت إعدادات الاتصال صحيحة، فسيتم إنشاء الاتصال بالخادم الثانوي المستقبلي وبناء التسلسل الهرمي "الأساسي/الثانوي". إذا فشل الاتصال، فتحقق من إعدادات الاتصال أو حدد شهادة الخادم الثانوي المستقبلية يدويًا.

يتم إنشاء الاتصال بين خوادم الإدارة الأولية والثانوية عبر المنفذ 13000. يتم استلام المهام والسياسات من خادم الإدارة الرئيسي وتطبيقها. يتم عرض خادم الإدارة الثانوي على خادم الإدارة الرئيسي في مجموعة الإدارة التي تم إضافته إليها.

إضافة خادم إدارة تابع (يتم هذا على خادم الإدارة الثانوي المستقبلي)

إذا لم تتمكن من التوصيل بخادم الإدارة الثانوي المستقبلي (كأن يكون غير متوفر أو غير متصل مؤقتًا مثلاً)، لا يزال بإمكانك إضافة خادم إدارة تابع.

لإضافة خادم إدارة تابع غير متوفر للتوصيل عبر Kaspersky Security Center Web Console:

1. أرسل ملف الشهادة لخادم الإدارة الأساسي المستقبلي إلى مسؤول النظام في المكتب حيث يوجد خادم الإدارة الثانوي المستقبلي. (يمكنك، على سبيل المثال، كتابة الملف إلى جهاز خارجي مثل ذاكرة البيانات، أو إرساله عبر البريد الإلكتروني.)

   يوجد ملف الشهادة على خادم الإدارة الرئيسي المستقبلي في %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. أعط أمر لمدير النظام المسؤول عن خادم الإدارة الثانوي المستقبلي بفعل ما يلي:

   a. انقر على أيقونة الإعدادات ( ).

   b. في صفحة الخصائص التي تفتح، انتقل إلى قسم **Hierarchy of Administration Servers** من تبويب **General**.

   c. حدد خيار **This Administration Server is secondary in the hierarchy**.

   d. في حقل **Primary Administration Server address**، أدخل اسم شبكة خادم الإدارة الرئيسي المستقبلي.

   e. حدد الملف الذي تم حفظه سابقًا والذي يحتوي على شهادة خادم الإدارة المستقبلي عن طريق النقر على **استعراض**.

   f. إذا لزم الأمر، حدد خانة الاختيار **Connect primary Administration Server to secondary Administration Server in DMZ**.

   g. في حال إجراء الاتصال بخادم الإدارة الثانوي المستقبلي عبر خادم وكيل، حدد خيار **Use proxy server** وحدد إعدادات الاتصال.

   h. انقر على **Save**.

يتم بناء التسلسل الهرمي "رئيسي / تابع". سيبدأ خادم الإدارة الرئيسي في تلقي الاتصال من خادم الإدارة الثانوي باستخدام المنفذ 13000. يتم استلام المهام والسياسات من خادم الإدارة الرئيسي وتطبيقها. يتم عرض خادم الإدارة الثانوي على خادم الإدارة الرئيسي في مجموعة الإدارة التي تم إضافته إليها.

عرض قائمة خوادم الإدارة الثانوية

لعرض قائمة خوادم الإدارة الثانوية (بما في ذلك الخوادم الافتراضية):

في القائمة الرئيسية، انقر فوق اسم خادم الإدارة، بجوار أيقونة الإعدادات ( ).

يتم عرض القائمة المنسدلة لخوادم الإدارة الثانوية (بما في ذلك الخوادم الافتراضية).

يمكنك التقدم إلى أي من خوادم الإدارة هذه بالنقر على أسمائها.

يتم عرض مجموعات الإدارة أيضًا، ولكنها تظهر باللون الرمادي وغير متوفرة في الإدارة في هذه القائمة.

إذا كنت متصلاً بخادم الإدارة الأساسي في Kaspersky Security Center Web Console، ولا يمكنك الاتصال بخادم إدارة افتراضي يُدار بواسطة خادم إدارة ثانوي، يمكنك استخدام إحدى الطرق التالية:

- **قم بتعديل تثبيتKaspersky Security Center Web Console الحالي لإضافة الخادم الثانوي إلى قائمة خوادم الإدارة الموثوقة**. ستتمكن بعد ذلك من الاتصال بخادم الإدارة الافتراضي فيKaspersky Security Center Web Console.

  1. على الجهاز الذي تم تثبيت Kaspersky Security Center Web Console عليه، قم بتشغيل ملف تثبيت version>-ksc-web-console exe.<build number>.<number ضمن حساب يتمتع بمزايا إدارية.

     سيبدأ معالج الإعداد. انتقل عبر المعالج من خلال استخدام زر **التالي**.

  2. حدد خيار **الترقية**.

  3. في خطوة **Modification type**، حدد خيار **تحرير إعدادات الاتصال**.

  4. في خطوة **Trusted Administration Servers**، أضف خادم الإدارة الثانوي المطلوب.

  5. في الخطوة الأخيرة، انقر على **تعديل** لتطبيق الإعدادات الجديدة.

  6. بعد اكتمال إعادة تكوين التطبيق بنجاح، انقر على زر **إنهاء**.

- استخدمKaspersky Security Center Web Console للاتصال مباشرة بخادم الإدارة الثانوي حيث تم إنشاء الخادم الإفتراضي. ستتمكن بعد ذلك من تبديل خادم الإدارة الافتراضي فيKaspersky Security Center Web Console.

- استخدم وحدة تحكم الإدارة القائمة على MMC للاتصال مباشرة بالخادم الإفتراضي.

حذف تسلسل هرمي لخوادم الإدارة

إذا لم تعد ترغب في وجود تسلسل هرمي لخوادم الإدارة، يمكنك إلغاء توصيلهم من التسلسل الهرمي هذا.

لحذف تسلسل هرمي لخوادم الإدارة:

1. في القائمة الرئيسية، انقر على أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة الرئيسي.

2. في الصفحة التي يتم فتحها، انتقل إلى تبويب **Administration Servers**.

3. حدد خادم الإدارة الثانوي في مجموعة الإدارة التي ترغب في حذف خادم الإدارة الثانوي منها.

4. في سطر القائمة، انقر على **Delete**.

5. في النافذة التي تفتح، انقر على **موافق** لتأكيد رغبتك في حذف خادم الإدارة الثانوي.

الآن خادم الإدارة الرئيسي السابق وخادم الإدارة الثانوي السابق مستقلين عن بعضهما. لم يعد التسلسل الهرمي موجودًا.

صيانة خادم الإدارة

تتيح لك صيانة خادم الإدارة إخلاء مساحة في مجلد خادم الإدارة وتقليل حجم قاعدة البيانات عن طريق حذف الكائنات التي لم تعد هناك حاجة إليها. ويساعدك هذا على تحسين تشغيل التطبيق وموثوقيته. نوصيك بصيانة خادم الإدارة كل أسبوع على الأقل.

يتم إجراء صيانة خادم الإدارة باستخدام المهمة المخصصة. يجري التطبيق الإجراءات التالية عند صيانة خادم الإدارة:

- يحذف المجلدات والملفات غير الضرورية من مجلد التخزين.
- يحذف السجلات غير الضرورية من الجداول (المعروفة أيضًا باسم "المؤشرات المتدلية").
- يمسح ذاكرة التخزين المؤقت.
- يحافظ على قاعدة البيانات (إذا كنت تستخدم SQL Server أو PostgreSQL كقاعدة بيانات DBMS):
  - يتحقق من عدم وجود أخطاء في قاعدة البيانات (متاح فقط لأجل SQL Server).
  - إعادة تنظيم فهارس قاعدة البيانات.
  - تحديث إحصائيات قاعدة البيانات.
  - تقليص قاعدة البيانات (إذا لزم الأمر).

يتم إنشاء مهمة Administration Server maintenance تلقائيًا عند تثبيت Kaspersky Security Center. إذا تم حذف مهمة Administration Server maintenance، يمكنك إنشائها يدويًا.

لإنشاء مهمة Administration Server maintenance:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر فوق الزر **Add**.
   سيبدأ معالج المهمة الجديدة.

3. في نافذة **New task settings** من المعالج، حدد **Administration Server maintenance** كنوع المهمة وانقر فوق زر **Next**.

4. اتبع بقية تعليمات المعالج.

يتم عرض المهمة التيتم إنشاؤها في قائمة المهام. يمكن تشغيل مهمة Administration Server maintenance واحدة فقط لخادم إدارة واحد. في حالة إنشاء مهمة Administration Server maintenance بالفعل لخادم الإدارة، لا يمكن إنشاء مهمة Administration Server maintenance الجديدة.

تكوين الواجهة

يمكنك تكوين واجهة Kaspersky Security Center Web Console لعرض أقسام وعناصر الواجهة وإخفائها، وفقًا للمزايا المستخدمة.

لتكوين واجهة Kaspersky Security Center Web Consoleوفقًا لمجموعة المزايا المُستخدمة حاليًا:

1. في القائمة الرئيسية، انتقل إلى إعدادات حسابك ثم حدد **Interface options**.

2. في نافذة **Interface options** التي تفتح، قم بتمكين أو تعطيل الخيارات المطلوبة.

3. انقر فوق **حفظ**.

بعد ذلك، تعرض وحدة التحكم أقسامًا في القائمة الرئيسية وفقًا للخيارات الممكنة. على سبيل المثال ، إذا قمت بتمكين **Show EDR alerts**، فسيظهر قسم المراقبة **Alerts** ← **Monitoring & reporting** في القائمة الرئيسية.

إدارة خوادم الإدارة الافتراضية

يصف هذا القسم الإجراءات التالية لإدارة خوادم لإدارة الافتراضية:

- إنشاء خوادم الإدارة الافتراضية
- تمكين وتعطيل خادم الإدارة الافتراضية
- تعيين مسؤول لخادم الإدارة الافتراضي
- تغيير خادم الإدارة لأجهزة العميل
- حذف خوادم الإدارة الافتراضية

إنشاء خادم إدارة افتراضي

يمكنك إنشاء خوادم إدارة ظاهرية وإضافتها إلى مجموعات الإدارة.

عند إنشاء خادم إدارة افتراضي، فإنه يرث قائمة المستخدمين وجميع حقوق المستخدم لخادم الإدارة الأساسي. إذا كان المستخدم يتمتع بحقوق الوصول إلى الخادم الأساسي، فإن هذا المستخدم يتمتع بحقوق الوصول إلى الخادم الافتراضي أيضًا. بعد الإنشاء، تكوّن حقوق الوصول إلى الخوادم بشكل مستقل.

لإنشاء خادم إدارة افتراضي وإضافته:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

2. في الصفحة التي تفتح، انتقل إلى تبويب **Administration Servers**.

3. حدد مجموعة الإدارة التي ترغب في إضافة خادم إدارة افتراضي لها.
سيُدير خادم الإدارة الافتراضي الأجهزة من المجموعة المحددة (بما في ذلك المجموعات الفرعية).

4. في سطر القائمة، انقر على **New virtual Administration Server**.

5. في الصفحة التي تفتح، حدد خصائص خادم الإدارة الافتراضي الجديد:

- **Name of virtual Administration Server**.
- **Administration Server connection address**

  يمكنك تحديد اسم وعنوان IP لخادم الإدارة.

6. من قائمة المستخدمين، حدد مسؤول خادم الإدارة الافتراضي. يمكنك، إذا كنت ترغب، أن تقوم بتعديل أحد الحسابات الموجودة بالفعل قبل تخصيص دور المدير له أو إنشاء حساب مستخدم جديد.

7. انقر على **Save**.

يتم إنشاء خادم الإدارة الافتراضي الجديد وإضافته إلى مجموعة الإدارة وعرضه في تبويب **Administration Servers**.

إذا كنت متصلاً بخادم الإدارة الأساسي في Kaspersky Security Center Web Console، ولا يمكنك الاتصال بخادم إدارة افتراضي يُدار بواسطة خادم إدارة ثانوي، يمكنك استخدام إحدى الطرق التالية:

- **قم بتعديل تثبيتKaspersky Security Center Web Console الحالي لإضافة الخادم الثانوي إلى قائمة خوادم الإدارة الموثوقة**. ستتمكن بعد ذلك من الاتصال بخادم الإدارة الافتراضي فيKaspersky Security Center Web Console.

  1. على الجهاز الذي تم تثبيت Kaspersky Security Center Web Console عليه، قم بتشغيل ملف تثبيت ksc-web-console-<version>-<build number>.exe ضمن حساب يتمتع بمزايا إدارية.

     سيبدأ معالج الإعداد. انتقل عبر المعالج من خلال استخدام زر **التالي**.

  2. حدد خيار **الترقية**.

  3. في خطوة **Modification type**، حدد خيار **تحرير إعدادات الاتصال**.

  4. في خطوة **Trusted Administration Servers**، أضف خادم الإدارة الثانوي المطلوب.

  5. في الخطوة الأخيرة، انقر على **تعديل** لتطبيق الإعدادات الجديدة.

  6. بعد اكتمال إعادة تكوين التطبيق بنجاح، انقر على زر **إنهاء**.

- استخدمKaspersky Security Center Web Console للاتصال مباشرة بخادم الإدارة الثانوي حيث تم إنشاء الخادم الإفتراضي. ستتمكن بعد ذلك من تبديل خادم الإدارة الافتراضي فيKaspersky Security Center Web Console.

- استخدم وحدة تحكم الإدارة القائمة على MMC للاتصال مباشرة بالخادم الإفتراضي.

تمكين وتعطيل خادم إدارة افتراضي

عند إنشاء خادم إدارة افتراضي جديد، يتم تمكينه افتراضيًا. يمكنك تعطيله أو تمكينه مرة أخرى في أي وقت. يعادل تعطيل أو تمكين خادم الإدارة الظاهري إيقاف تشغيل خادم إدارة فعلي أو تشغيله.

لتمكين أو تعطيل خادم إدارة افتراضي:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

2. في الصفحة التي تفتح، انتقل إلى تبويب **Administration Servers**.

3. حدد خادم الإدارة الافتراضي الذي تريد تمكينه أو تعطيله.

4. في سطر القائمة، انقر على زر **Enable / disable virtual Administration Server**.

يتم تغيير حالة خادم الإدارة الافتراضي إلى ممكّن أو معطل، بناءً على حالته السابقة. يتم عرض الحالة المحدثة بجوار اسم خادم الإدارة.

تعيين مسؤول عن خادم إدارة افتراضي

عند استخدام خوادم الإدارة الافتراضية في مؤسستك، قد ترغب في تعيين مسؤول مخصص لكل خادم إدارة افتراضي. على سبيل المثال، قد يكون هذا مفيدًا عند إنشاء خوادم إدارة افتراضية لإدارة مكاتب أو أقسام منفصلة لمؤسستك، أو إذا كنت أحد موفري MSP وتدير المستأجرين من خلال خوادم الإدارة الافتراضية.

عند إنشاء خادم إدارة افتراضي، فإنه يرث قائمة المستخدمين وجميع حقوق المستخدم لخادم الإدارة الأساسي. إذا كان المستخدم يتمتع بحقوق الوصول إلى الخادم الأساسي، فإن هذا المستخدم يتمتع بحقوق الوصول إلى الخادم الافتراضي أيضًا. بعد الإنشاء، يمكنك تكوين حقوق الوصول إلى الخوادم بشكل مستقل. إذا كنت ترغب في تعيين مسؤول لخادم الإدارة الافتراضي فقط، فتأكد من أن المسؤول لا يملك حقوق الوصول إلى خادم الإدارة الأساسي.

يمكنك تعيين مسؤول لخادم الإدارة الافتراضي من خلال منح حقوق وصول المسؤول إلى خادم الإدارة الافتراضي. يمكنك منح حقوق الوصول المطلوبة بإحدى الطرق التالية:

- قم بتكوين حقوق الوصول للمسؤول يدويًا
- قم بتعيين دور مستخدم واحد أو أكثر للمسؤول

لتسجيل الدخول إلىKaspersky Security Center Web Console، يحدد مسؤول خادم الإدارة الافتراضي اسم خادم الإدارة الافتراضي، واسم المستخدم، وكلمة المرور. يصادق Kaspersky Security Center Web Console المسؤول ويفتح خادم الإدارة الافتراضي الذي يتمتع المسؤول بحقوق الوصول إليه. يتعذر للمسؤول التبديل بين خوادم الإدارة.

المتطلبات الأساسية

قبل أن تبدأ، تأكد من تلبية المتطلبات الأساسية التالية:

- تم إنشاء خادم الإدارة الافتراضي.
- على خادم الإدارة الأساسي، لقد أنشأت حساب للمسؤول الذي تريد تعيينه لخادم الإدارة الافتراضي.
- تتمتع بحق **Modify object ACLs** مباشرةً في المجال الوظيفي **User permissions** ← **General features**.

تكوين حقوق الوصول يدويًا

لتعيين مسؤول لخادم الإدارة الافتراضي:

1. في القائمة الرئيسية، قم بالتبديل إلى خادم الإدارة الافتراضي المطلوب:

   a. انقر فوق أيقونة شيفرون ( ) على يمين اسم خادم الإدارة الحالي.

   b. حدد خادم الإدارة المطلوب.

2. في القائمة الرئيسية، انقر على أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة.

   تفتح نافذة خصائص خادم الإدارة.

3. في علامة التبويب **Access rights**، انقر فوق الزر **Add**.

يتم فتح قائمة موحدة لمستخدمي خادم الإدارة الأساسي وخادم الإدارة الافتراضي الحالي.

4. من قائمة المستخدمين، حدد حساب المسؤول الذي تريد تعيينه لخادم الإدارة الافتراضي، ثم انقر فوق زر **OK**.

يضيف التطبيق المستخدم المحدد إلى قائمة المستخدمين في علامة التبويب **Access rights**.

5. حدد خانة الاختيار بجوار الحساب المضاف، ثم انقر فوق الزر **Access rights**.

6. تكوين الحقوق التي سيتمتع بها المسؤول على خادم الإدارة الافتراضي.

بالنسبة للمصادقة الناجحة، على الأقل، يجب أن يتمتع المسؤول بالحقوق التالية:

- **Read** مباشرة في منطقة الوظائف **Basic functionality** ← **General features**
- **Read** مباشرة في منطقة الوظائف **Virtual Administration Servers** ← **General features**

يحفظ التطبيق حقوق المستخدم المعدلة في حساب المسؤول.

تكوين حقوق الوصول عن طريق تعيين أدوار المستخدم

بدلاً من ذلك، يمكنك منح حقوق الوصول لمسؤول خادم الإدارة الافتراضي من خلال أدوار المستخدم. على سبيل المثال، قد يكون هذا مفيدًا إذا كنت تريد تعيين عدة مسؤولين على نفس خادم الإدارة الافتراضي. إذا كانت هذه هي الحالة، يمكنك تعيين نفس دور المستخدم لحسابات المسؤولين أو أكثر بدلاً من تكوين نفس حقوق المستخدم للعديد من المسؤولين.

لتعيين مسؤول لخادم إدارة افتراضي من خلال تعيين أدوار المستخدم:

1. على خادم الإدارة الأساسي، أنشئ دور مستخدم جديد، ثم حدد كافة حقوق الوصول المطلوبة التي يجب أن يمتلكها المسؤول على خادم الإدارة الافتراضي. يمكنك إنشاء عدة أدوار، على سبيل المثال، إذا كنت تريد فصل الوصول إلى مناطق وظيفية مختلفة.

2. في القائمة الرئيسية، قم بالتبديل إلى خادم الإدارة الافتراضي المطلوب:

   a. انقر فوق أيقونة شيفرون ( ) على يمين اسم خادم الإدارة الحالي.

   b. حدد خادم الإدارة المطلوب.

3. قم بتعيين الدور الجديد أو الأدوار المتعددة لحساب المسؤول.

يقوم التطبيق بتعيين الأدوار لحساب المسؤول.

تكوين حقوق الوصول على مستوى العنصر

بالإضافة إلى تعيين حقوق الوصول على مستوى المنطقة الوظيفية، تستطيع تكوين الوصول إلى عناصر محددة على خادم الإدارة الافتراضي، على سبيل المثال، لمجموعة إدارة معينة أو مهمة. للقيام بذلك، قم بالتبديل إلى خادم الإدارة الافتراضي، ثم قم بتكوين حقوق الوصول من خصائص العنصر.

تغيير خادم الإدارة للأجهزة العميلة

يمكنك تغيير خادم الإدارة الذي يدير الأجهزة العميلة إلى خادم مختلف باستخدام مهمة Change Administration Server. بعد اكتمال المهمة، سيتم وضع الأجهزة العميلة المحددة تحت إدارة خادم الإدارة الذي تحدده.

لا يمكنك استخدام مهمة Change Administration Server لأجهزة العميل المتصلة بخادم الإدارة عبر بوابات الاتصال. وبالنسبة لهذه الأجهزة، يتعين عليك إما إعادة تكوين عميل الشبكة أو إعادة تثبيت عميل الشبكة وتحديد بوابة الاتصال.

لتغيير خادم الإدارة الذي يدير الأجهزة العميلة بخادم آخر:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

3. في خطوة **New task settings** في المعالج، حدد الإعدادات التالية:

   a. في القائمة المنسدلة **Application**، حدد **Kaspersky Security Center**.

   b. في الحقل **Task type**، حدد **Change Administration Server**.

   c. في الحقل **Task name**، حدد اسم المهمة التي تنشئها.

   لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

   d. حدد الأجهزة التي سيتم تعيين المهمة إليها:

   - **Assign task to an administration group**

     يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

     على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

     إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

   - **Specify device addresses manually or import addresses from a list**

     يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

     قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

   - **Assign task to a device selection**

     يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

     على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

4. في خطوة **Task scope** في المعالج، حدد مجموعة الإدارة، أو الأجهزة ذات العناوين المحددة ، أو تحديد الجهاز.

5. في هذه الخطوة من المعالج، تأكد من موافقتك على شروط تغيير خادم الإدارة لأجهزة العميل.

6. في هذه الخطوة من المعالج، حدد خادم الإدارة الذي تريد استخدامه لإدارة الأجهزة المحددة:

- **Change to another primary Administration Server**

لنقل أجهزة العميل إلى خادم إدارة أساسي آخر، حدد إعدادات اتصال خادم الإدارة التالية:

1. في الحقل **Administration Server address**، حدد عنوان خادم الإدارة الأساسي الجديد.

2. في الحقل **Port number**، حدد رقم المنفذ الذي تريد الاتصال به بخادم الإدارة.
   رقم المنفذ الافتراضي هو 14000.

3. في الحقل **SSL port**، حدد رقم منفذ SSL على خادم الإدارة الرئيسي.
   رقم المنفذ الافتراضي هو 13000.

4. إذا لزم الأمر، قم بتمكين الخيار **Use proxy server**.
   وفي حالة تعطيل هذا الخيار، سيتم استخدام الاتصال المباشر لتوصيل الجهاز بخادم الإدارة.
   في حالة تمكين هذا الخيار، حدد معلمات الخادم الوكيل:

   - **Proxy server address**
   - **Proxy server port**

   إذا كان الخادم الوكيل يتطلب المصادقة، في حقلي **User name** و**Password**، حدد اعتمادات الحساب الذي تم إنشاء اتصال بالخادم الوكيل باستخدامه. ونوصي بتحديد بيانات اعتماد حساب لديه الحد الأدنى من الامتيازات المطلوبة فقط لمصادقة الخادم الوكيل.

5. إذا لزم الأمر، قم بتحميل شهادة خادم الإدارة الجديدة.

- **Change to another virtual Server on this primary Server**

حدد هذا الخيار لنقل أجهزة العميل إلى خادم الإدارة الافتراضي على خادم الإدارة الأساسي الحالي. ولفعل ذلك، في القائمة المنسدلة **Name of virtual Administration Server**، حدد خادم الإدارة الافتراضي المطلوب.

7. في الخطوة **Selecting an account to run the task** في المعالج، حدد إعدادات الحساب:

- **Default account**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.
يتم تحديد هذا الخيار افتراضيًا.

- **تحديد حساب**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **Account**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **Password**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

8. إذا كنت تريد تغيير إعدادات المهمة الافتراضية، في خطوة **Finish task creation** في المعالج، قم بتمكين خيار **Open task details when creation is complete**.
   إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. ويمكنك تغيير الإعدادات الافتراضية لاحقًا في أي وقت.

9. انقر على زر **Finish**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

10. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

11. إذا كنت تريد تغيير إعدادات المهمة الافتراضية، في نافذة خصائص المهمة، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك.

12. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

13. قم بتشغيل المهمة التي تم إنشاؤها.

بعد اكتمال المهمة، يتم وضع الأجهزة العميلة التي تم إنشاء المهمة من أجلها تحت إدارة خادم الإدارة المحدد في إعدادات المهمة.

حذف خادم إدارة افتراضي

عند حذف خادم إدارة افتراضي، سيتم أيضًا حذف جميع الكائنات التي تم إنشاؤها على خادم الإدارة، بما في ذلك السياسات والمهام. ستتم إزالة الأجهزة المُدارة من مجموعات الإدارة التي تمت إدارتها بواسطة خادم الإدارة الافتراضي من مجموعات الإدارة. لإعادة الأجهزة التي تخضع لإدارة Kaspersky Security Center، قم بتشغيل استقصاء الشبكة ثم انقل الأجهزة التي تم العثور عليها من مجموعة الأجهزة غير المخصصة إلى مجموعات الإدارة.

لحذف خادم إدارة افتراضي:

1. في القائمة الرئيسية، انقر على أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة.

2. في الصفحة التي تفتح، انتقل إلى تبويب **Administration Servers**.

3. حدد خادم الإدارة الافتراضي الذي تريد حذفه.

4. في سطر القائمة، انقر على **Delete**.

تم حذف خادم الإدارة الافتراضي.

تمكين حماية الحساب من تعديل غير مصرح به

يمكنك تمكين خيار إضافي لحماية حساب المستخدم من التعديل غير المصرح به. إذا كان هذا الخيار مفعلاً، تعديل إعدادات حساب المستخدم يتطلب ترخيص المستخدم الذي يملك حقوق التعديل.

لتمكين حماية الحساب من التعديل غير المصرح به أو تعطيلها:

1. في القائمة الرئيسية، انتقل إلى **Users** ← **Users & roles**.

2. انقر على اسم حساب المستخدم الداخلي الذي ترغب في تحديد حماية الحساب له من التعديل غير المصرح به.

3. في نافذة إعدادات المستخدم التي تفتح، حدد تبويب **Account protection**.

4. في تبويب **Account protection**، حدد **طلب المصادقة للتحقق من خيار إذن تعديل حسابات المستخدمين** إذا كنت ترغب في طلب بيانات الاعتماد في كل مرة يتم فيها تغيير إعدادات الحساب أو تعديلها. بخلاف ذلك، حدد خيار **السماح للمستخدمين بتعديل هذا الحساب دون مصادقة إضافية**.

5. انقر على زر **حفظ**.

بهذا تم تمكين حماية الحساب من التعديل غير المصرح به لحساب المستخدم.

النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة

النسخ الاحتياطي للبيانات يسمح بنقل خادم الإدارة من جهاز إلى آخر دون فقان للبيانات. من خلال النسخ الاحتياطي، يمكنك استعادة البيانات عند نقل قاعدة بيانات خادم الإدارة إلى جهاز آخر، أو عند الترقية إلى إصدار أحدث من Kaspersky Security Center. ويمكنك كذلك استخدام النسخ الاحتياطي للبيانات لنقل بيانات خادم الإدارة من Kaspersky Security Center Windows تحت إدارة Kaspersky Security Center Linux (لا يتم دعم نقل البيانات من Kaspersky Security Center Linux إلى Kaspersky Security Center Windows).

لا يتم نسخ المكونات الإضافية للإدارة المثبتة احتياطيًا. بعد استعادة بيانات خادم الإدارة من نسخة احتياطية، تحتاج إلى تنزيل وإعادة تثبيت المكونات الإضافية للتطبيقات المدارة.

قبل إجراء نسخ احتياطي لبيانات خادم الإدارة، تحقق من إضافة خادم إدارة افتراضي إلى مجموعة الإدارة. وفي حالة إضافة خادم إدارة افتراضي، تأكد من تعيين مسؤول إلى خادم الإدارة الافتراضي هذا قبل إجراء النسخ الاحتياطي. ولا يمكنك منح حقوق وصول المسؤول إلى خادم الإدارة الافتراضي بعد النسخ الاحتياطي. ولاحظ أنه في حالة فقدان بيانات اعتماد حساب المسؤول، فلن تتمكن من تعيين مسؤول جديد لخادم المسؤول الافتراضي.

لإجراء نسخ احتياطي لمجموعة التجاوز الفشل من Kaspersky Security Center أو استعادتها، يجب إيقاف المجموعة بأكملها للصيانة ثم إعادة تشغيلها عند اكتمال النسخ الاحتياطي أو الاستعادة.

يمكنك إنشاء نسخة احتياطية من بيانات خادم الإدارة بإحدى الطرق التالية:

- من خلال إنشاء مهمة نسخ احتياطي للبيانات وتشغيلها عبر وحدة تحكم الإدارة.
- من خلال تشغيل أداة klbackup المساعدة على الجهاز المثبت عليه خادم الإدارة. يتم تضمين الأداة المساعدة هذه في مجموعة توزيع Kaspersky Security Center. بعد تثبيت خادم الإدارة، ستكون الأداة المساعدة موجودة في جذر المجلد الوجهة المحدد عند تثبيت التطبيق.

يتم حفظ البيانات التالية في النسخة الاحتياطية لخادم الإدارة:

- قاعدة بيانات خادم الإدارة (السياسات والمهام وإعدادات التطبيق والأحداث المحفوظة في خادم الإدارة).
- تفاصيل التكوين الخاصة ببنية مجموعات الإدارة والأجهزة العميلة.
- تخزين حزم توزيع التطبيقات للتثبيت عن بُعد.
- شهادة خادم الإدارة.
- محتويات مجلد التحديثات.

  بشكل افتراضي، يكون مسار المجلد هو C:\ProgramData\KasperskyLab\adminkit\1093.\working\share\Updates\

ولا يمكن استعادة بيانات خادم الإدارة إلا باستخدام أداة klbackup المساعدة. ويجب أن تنفذ الاستعادة على مثيل قابل للتشغيل لخادم الإدارة الذي تم تثبيته للتو وله نفس الإصدار (أو أحدث) الذي تم إنشاء النسخة الاحتياطية له.

إنشاء مهمة نسخ احتياطي للبيانات

مهام النسخ الاحتياطي هي مهام خادم الإدارة؛ ويتم إنشاؤها من خلال معالج البدء السريع. إذا تم حذف مهمة منشأة بواسطة معالج البدء السريع، يمكنك إنشاء مهمة يدويًا.

لإنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.
2. انقر فوق الزر **Add**.

   سيبدأ معالج المهمة الجديدة.
3. في نافذة **New task settings** الخاصة بالمعالج، حدد نوع المهمة الذي يحمل الاسم **Backup of Administration Server data**.
4. اتبع بقية تعليمات المعالج.

يمكن إنشاء مهمة **Backup of Administration Server data** في نسخة مفردة فقط. في حالة إنشاء مهمة النسخ الاحتياطي لبيانات خادم الإدارة بالفعل لخادم الإدارة، لا يتم عرضها في نافذة تحديد نوع المهمة لمعالج إنشاء مهمة النسخ الاحتياطي لخادم الإدارة.

لتكوين مهمة النسخ الاحتياطي لبيانات خادم الإدارة:

1. في القائمة الرئيسية ، انتقل إلى **Tasks** ← **Assets (Devices)** ، ثم حدد مهمة **Backup of Administration Server data**.
2. انقر على مهمة **Backup of Administration Server data**.

   ستفتح نافذة خصائص المهمة.
3. إذا لزم الأمر، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك.
4. في القسم **Application settings**، حدد المسار إلى المجلد لتخزين النسخ الاحتياطية لبيانات خادم الإدارة، وقم بتعيين كلمة مرور حماية النسخ الاحتياطي، وعدد النُسخ الاحتياطية إذا لزم الأمر.
5. انقر فوق **Save** لتطبيق التغييرات.

تم تكوين مهمة النسخ الاحتياطي لبيانات خادم الإدارة.

نقل خادم إدارة إلى جهاز آخر

إذا كنت بحاجة إلى استخدام خادم الإدارة على جهاز جديد، فيمكنك نقله بإحدى الطرق التالية:

- انقل خادم الإدارة وخادم قاعدة البيانات إلى جهاز جديد (يمكن تثبيت خادم قاعدة البيانات على الجهاز الجديد مع خادم الإدارة، أو على جهاز آخر).
- احتفظ بخادم قاعدة البيانات على الجهاز السابق وانقل خادم الإدارة فقط إلى جهاز جديد.

لنقل خادم الإدارة وخادم قاعدة البيانات إلى جهاز جديد:

1. على الجهاز السابق، أنشئ نسخة احتياطية من بيانات خادم الإدارة.

   للقيام بذلك، يمكنك تشغيل مهمة النسخ الاحتياطي للبيانات من خلال Kaspersky Security Center Web Console أو تشغيل الأداة المساعدة klbackup.

إذا كنت تستخدم SQL Server كنظام لإدارة قاعدة البيانات لخادم الإدارة، يمكنك ترحيل البيانات من SQL Server إلى MySQL أو MariaDB DBMS. للقيام بذلك، قم بتشغيل الأداة المساعدة klbackup في الوضع التفاعلي لإنشاء نسخة احتياطية للبيانات. قم بتمكين ملف **الانتقال إلى تنسيق MySQL / MariaDB** الخيار في **إعدادات النسخ الاحتياطي** نافذة معالج النسخ الاحتياطي والاستعادة. سينشئ Kaspersky Security Center نسخة احتياطية متوافقة مع MySQL وMariaDB. بعد ذلك، يمكنك استعادة البيانات من النسخة الاحتياطية إلى MySQL أو MariaDB.

يمكنك أيضًا تمكين **الترحيل إلى تنسيق Azure** الخيار إذا كنت تريد ترحيل البيانات من SQL Server إلى Azure SQL DBMS.

2. على الجهاز السابق، اقطع اتصال خادم الإدارة عن الشبكة.

3. حدد جهازًا جديدًا لتثبيت خادم الإدارة عليه. تأكد أن الأجهزة والبرامج الموجودة على الجهاز المحدد تفي بمتطلبات خادم الإدارة وKaspersky Security Center Web Console وعميل الشبكة. تحقق أيضًا من توفر المنافذ المستخدمة في خادم الإدارة.

4. تعيين العنوان نفسه للجهاز الجديد.

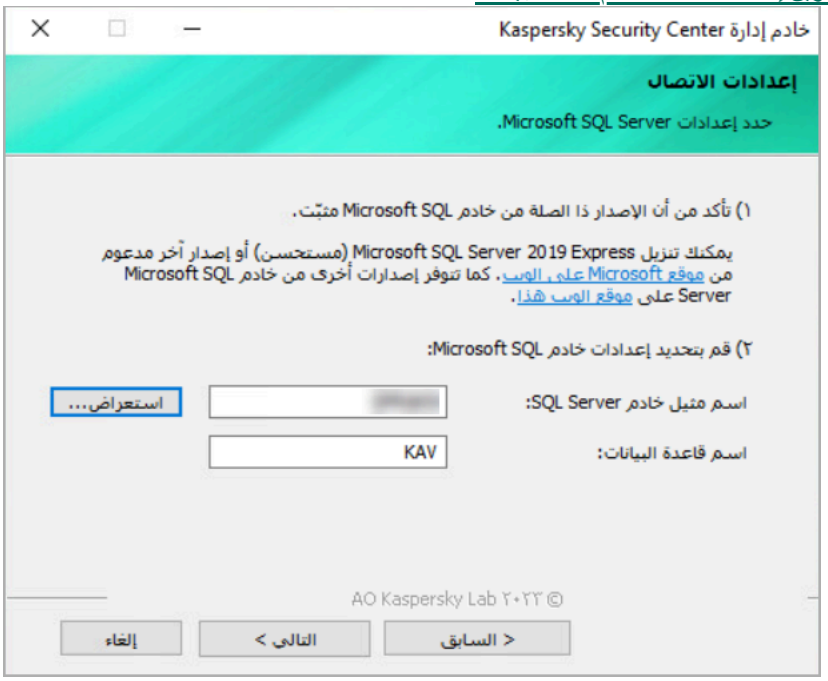
يمكن تعيين اسم NetBIOS وFQDN وعنوان IP الثابت لخادم الإدارة الجديد. ويعتمد ذلك على عنوان خادم الإدارة الذي تم تعيينه في حزمة تثبيت عميل الشبكة عند نشر عملاء الشبكة. وبدلاً من ذلك، يمكنك استخدام عنوان الاتصال الذي يحدد خادم الإدارة الذي يتصل به عميل الشبكة (يمكنك الحصول على هذا العنوان على الأجهزة المُدارة باستخدام الأداة المساعدة klnagchk).

5. إذا لزم الأمر، على جهاز آخر، قم بتثبيت نظام إدارة قاعدة البيانات (DBMS) الذي سيستخدمه خادم الإدارة.

يمكن تثبيت قاعدة البيانات على الجهاز الجديد مع خادم الإدارة، أو على جهاز آخر. تأكد أن هذا الجهاز يلبي متطلبات الأجهزة والبرامج. عند تحديد DBMS، ضع في اعتبارك عدد الأجهزة التي يغطيها خادم الإدارة.

6. قم بتشغيل تثبيت خادم الإدارة على الجهاز الجديد.

7. أثناء تثبيت خادم الإدارة، قم بتكوين إعدادات اتصال خادم قاعدة البيانات.



مثال على نافذة إعدادات الاتصال لـ Microsoft SQL Server

بناءً على المكان الذي تريد تحديد موقع خادم قاعدة البيانات فيه، قم بأحد الإجراءات التالية:

- **احتفظ بخادم قاعدة البيانات على الجهاز السابق**

1. انقر على **استعراض** بجانب **اسم مثيل خادم SQL Server**، ثم حدد اسم الجهاز السابق في القائمة التي تظهر.

   لاحظ أن الجهاز السابق يجب أن يكون متاحًا للاتصال بخادم الإدارة الجديد.

2. أدخل اسم قاعدة البيانات السابقة في ملف **اسم قاعدة البيانات** مجال.

- **انقل خادم قاعدة البيانات إلى جهاز آخر**

1. انقر على **استعراض** بجانب **اسم مثيل خادم SQL Server**، ثم حدد اسم الجهاز في القائمة التي تظهر.

2. أدخل اسم قاعدة البيانات الجديدة في ملف **اسم قاعدة البيانات** مجال.

لاحظ أن اسم قاعدة البيانات الجديدة يجب أن يتطابق مع اسم قاعدة البيانات من الجهاز السابق. يجب أن تكون أسماء قواعد البيانات متطابقة، بحيث يمكنك استخدام النسخة الاحتياطية لخادم الإدارة. اسم قاعدة البيانات الافتراضي هو KAV.

8. بعد اكتمال التثبيت، قم باستعادة بيانات خادم الإدارة على الجهاز الجديد باستخدام الأداة المساعدة klbackup.

إذا كنت تستخدم SQL Server كنظام DBMS على الأجهزة السابقة والجديدة، فلاحظ أن إصدار SQL Server المثبت على الجهاز الجديد يجب أن يكون هو نفسه أو أحدث من إصدار SQL Server المثبت على الجهاز السابق. خلاف ذلك، لا يمكنك استعادة بيانات خادم الإدارة على الجهاز الجديد.

9. افتح Kaspersky Security Center Web Console واتصل بخادم الإدارة.

10. تحقق من أن جميع الأجهزة المُدارة متصلة بخادم الإدارة.

11. قم بإلغاء تثبيت خادم الإدارة وخادم قاعدة البيانات من الجهاز السابق.

يمكنك أيضا استخدام وحدة تحكم الإدارة لنقل خادم الإدارة وخادم قاعدة البيانات إلى جهاز آخر.

التحقق من سلامة الوحدات باستخدام أداتي klscmodchk وintegrity_checker

يحتوي Kaspersky Security Center على وحدات ثنائية متعددة في شكل مكتبات مرتبطة ديناميكيًا وملفات قابلة للتنفيذ وملفات تكوين وملفات واجهة. ويمكن للمتسللين استبدال وحدة قابلة للتنفيذ واحدة أو أكثر أو ملفا تطبيق واحد أو أكثر بملفات أخرى تحتوي على تعليمات برمجية ضارة. لمنع استبدال الوحدة والملف، يوفر Kaspersky Security Center فحصًا لسلامة المكونات باستخدام أداتي klscmodchk وintegrity_checker. وتفحص هذه الأدوات المساعدة الوحدات والملفات للبحث عن أي تغييرات أو أضرار غير مصرح بها. وإذا كان ملف الوحدة أو التطبيق يحتوي على مجموع اختباري غير صحيح، فسيتم اعتباره تالفًا.

تنفذ أداة klscmodchk عمليات فحص السلامة لمكونات Kaspersky Security Center التالية:

- خادم الإدارة
- عميل الشبكة
- المكونات الإضافية للإدارة لوحدة تحكم الإدارة مع ملفات البيان

تنفذ أداة integrity_checker عمليات فحص السلامة لمكونات Kaspersky Security Center التالية:

- خادم الإدارة
- عميل الشبكة
- Kaspersky Security Center Web Console

تتحقق كلتا الأداتين من سلامة الوحدة استنادًا إلى ملف البيان kl_file_integrity_manifest.xml، الذي يعد جزءًا من بناء Kaspersky Security Center ويوجد في مجلد التثبيت. يحتوي ملف بيان المكون على ملفات تعتبر سلامتها مهمة للتشغيل الصحيح لمكون Kaspersky Security Center. ويتم أيضًا التحقق من سلامة ملفات البيان نفسها.

لا يُنصح بشدة بتعديل ملف البيان kl_file_integrity_manifest.xml، حيث سيؤدي ذلك إلى إبطال التوقيع الرقمي والتسبب في فشل فحص السلامة.

للتحقق من سلامة مكون Kaspersky Security Center، قم بتشغيل أحد الأوامر التالية:

- `$ klscmodchk [ parameters ]`

  تقوم الأداة المساعدة klscmodchk بتشغيل الأداة المساعدة `--verbose` باستخدام المعلمة --verbose وتتحقق من سلامة الوحدات.

  المعلمات الخاصة بالأداة المساعدة klscmodchk:

  - `-logfile <log_file_path>`—تحديد المسار إلى ملف على القرص للتسجيل. بشكل افتراضي، يتم إخراج المعلومات إلى وحدة التحكم.
  - `-chkplugins` —التحقق من سلامة وحدات المكون الإضافي للإدارة المثبتة لوحدة تحكم الإدارة التي تتضمن ملفات البيان. وبشكل افتراضي، لا يتم تحديد مكونات الإدارة الإضافية.
  - `-verbose`—إخراج معلومات موسعة أثناء التحقق من السلامة.

- `$ integrity_checker [ parameters ] <manifest_file_path>`

  المعلمات الخاصة بالأداة المساعدة integrity_checker:

  - `--help`—عرض تعليمات الأداة المساعدة integrity_checker.
  - `--version`—عرض إصدار الأداة المساعدة integrity_checker.
  - `--verbose`—عرض معلومات عن تشغيل الأداة المساعدة. وعند إجراء فحص السلامة، يكفي استخدام هذه المعلمة في الأمر.

يتم عرض نتيجة فحص كل ملف بيان بجوار اسم ملف البيان بالتنسيق التالي:

- SUCCEEDED—تم تأكيد سلامة الملف (رمز الإرجاع 0).
- FAILED—لم يتم تأكيد سلامة الملف (رمز الإرجاع غير صفري).

يمكنك أيضًا تكوين فحوصات السلامة لبدء التشغيل تلقائيًا عند تشغيل التطبيق. بشكل افتراضي، يتم تعطيل فحص السلامة التلقائي.

لتمكين فحص السلامة التلقائي:

1. على الجهاز المثبت عليه خادم الإدارة، في موجه أوامر Windows، أدخل الأمر التالي:

```
klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
```

2. أعد تشغيل الجهاز.

تم تمكين الفحص التلقائي للسلامة.

عند التشغيل التالي لبرنامج Kaspersky Security Center، ستعمل الأداة المساعدة klscmodchk مع خادم الإدارة، وستبدأ فحص تكامل الوحدات النمطية. تتم كتابة نتيجة فحوصات السلامة في سجل أحداث Kaspersky.

الإعداد الأولي لتطبيق Kaspersky Security Center Web Console

يرد في هذا القسم الخطوات التي يجب عليك اتخاذها بعد تثبيت Kaspersky Security Center Web Console لإجراء الإعداد الأولي.

معالج البدء السريع (Kaspersky Security Center Web Console)

يقدم هذا القسم معلومات حول معالج البدء السريع لخادم الإدارة.

يتطلب المعالج الوصول إلى الإنترنت. إذا لم يكن لدى خادم الإدارة إمكانية الوصول إلى الإنترنت، نوصيك بتنفيذ جميع خطوات المعالج يدويًا من خلال واجهة Kaspersky Security Center Web Console.

يتيح لك تطبيق Kaspersky Security Center ضبط حد أدنى لمجموعة محددة من الإعدادات الضرورية لإنشاء نظام إدارة مركزية لحماية شبكتك من التهديدات الأمنية. يتم إجراء هذا التكوين من خلال معالج البدء السريع. عند تشغيل المعالج، يمكن إجراء التغييرات التالية على التطبيق:

- أضف ملفات مفاتيح أو أدخل رموز تنشيط يمكن نشرها تلقائيًا على الأجهزة الموجودة ضمن مجموعات الإدارة.
- تكوين التفاعل مع Kaspersky Security Network (KSN). إذا كنت قد سمحت باستخدام KSN، يقوم المعالج بتمكين خدمة خادم وكيل KSN التي تضمن الاتصال بين KSN والأجهزة.
- إعداد تسليم البريد الإلكتروني للإخطارات بالأحداث التي تحدث أثناء تشغيل خادم الإدارة والتطبيقات المُدارة (يتطلب تسليم الإخطار بنجاح تشغيل خدمة Messenger على خادم الإدارة وجميع الأجهزة المستلمة).
- إنشاء سياسة حماية لمحطات العمل والخوادم ومهام فحص البرامج الضارة ومهام تنزيل التحديثات ومهام النسخ الاحتياطي للبيانات لأعلى مستوى بالتسلسل الهرمي للأجهزة المدارة.

لا ينشئ معالج البدء السريع سياسات إلا للتطبيقات التي لا يحتوي مجلد **Managed devices** فيها على أي سياسات. لا ينشئ معالج البدء السريع أي مهام إذا كان قد تم بالفعل إنشاء مهام بنفس الأسماء على أعلى مستوى بالترتيب الهرمي للأجهزة المُدارة.

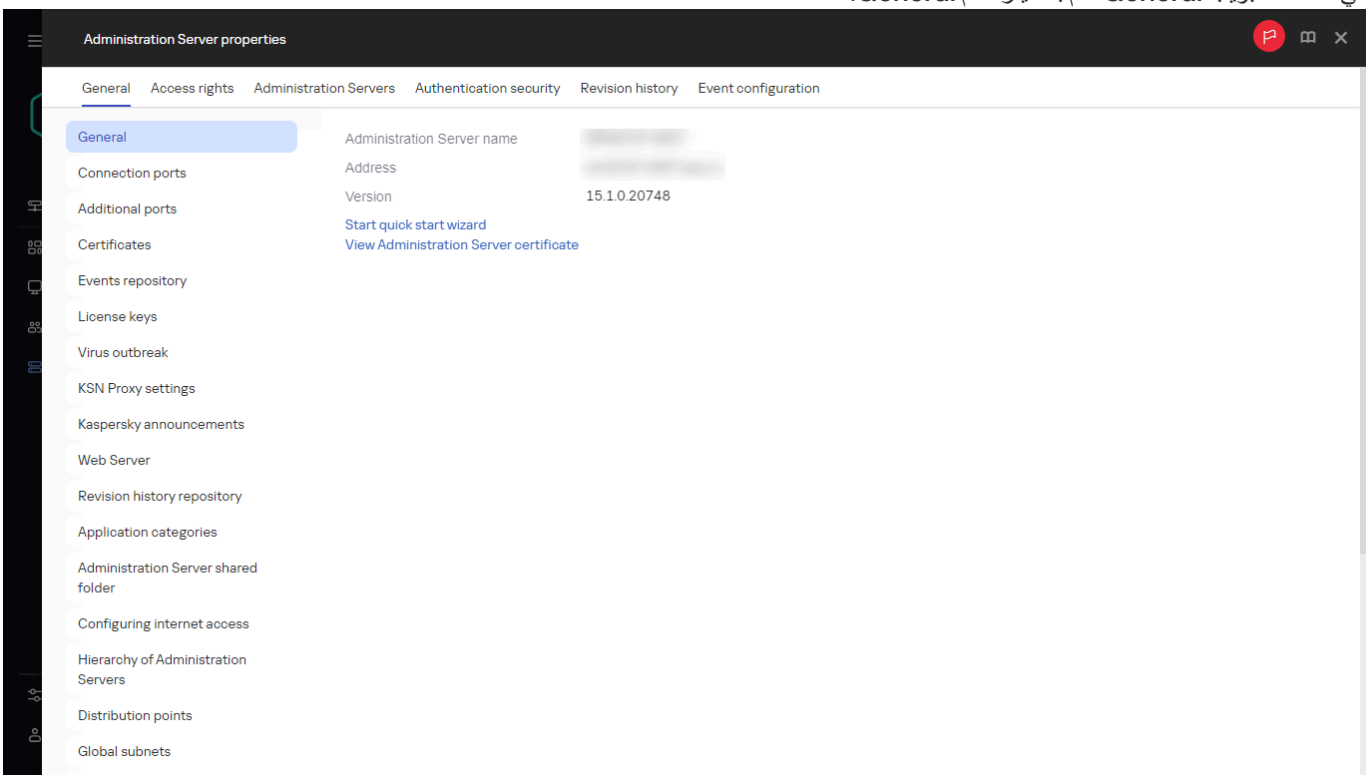
يطالبك التطبيق تلقائيًا بتشغيل معالج البدء السريع بعد تثبيت خادم الإدارة عند أو اتصال به. يمكنك أيضًا بدء تشغيل معالج البدء السريع في أي وقت.

لبدء تشغيل معالج البدء السريع يدويًا:

1. في القائمة الرئيسية، انقر على أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، قم باختيار قسم **General**.



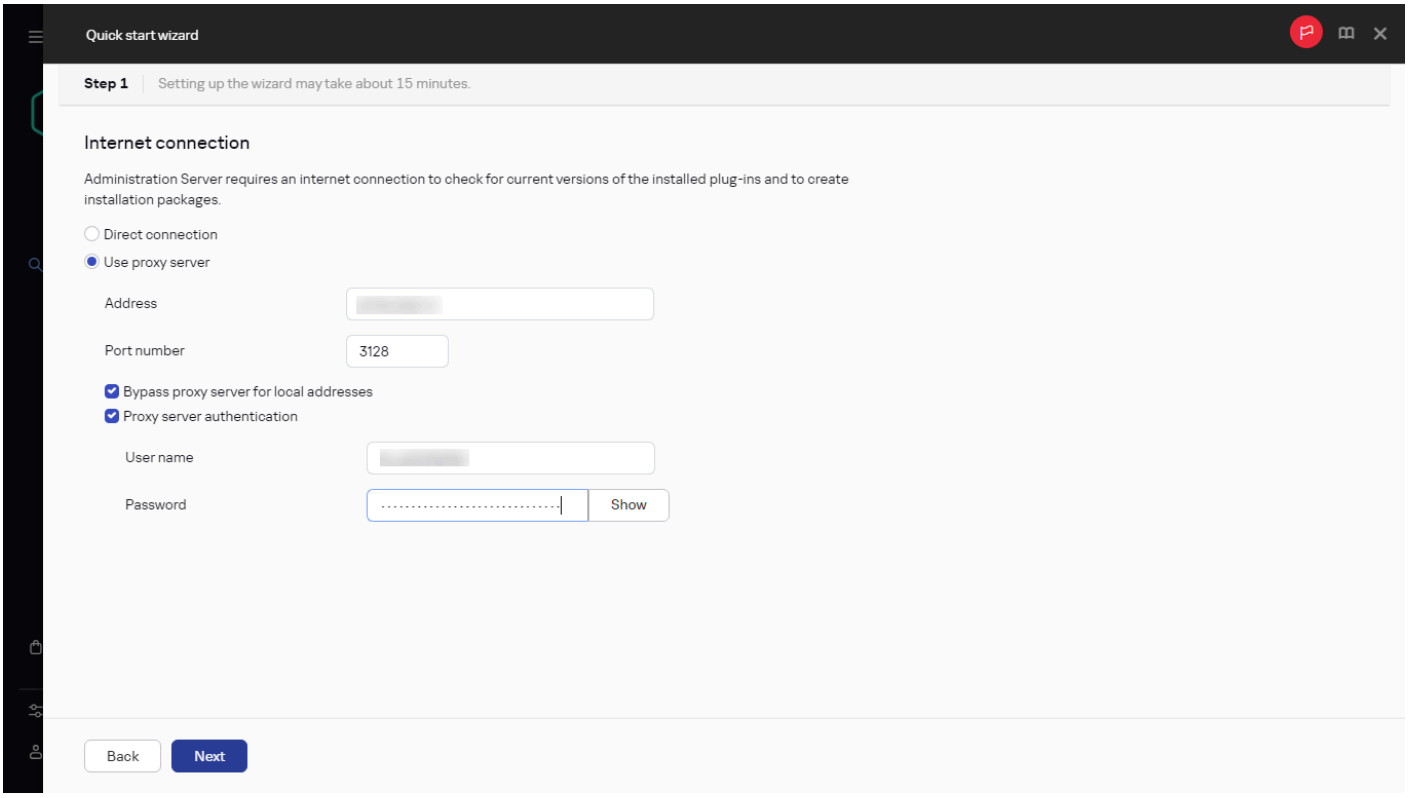
نافذة خصائص خادم الإدارة

3. انقر على**Start quick start wizard**.

سيطالبك المعالج بإجراء التكوين الأولي لخادم الإدارة. اتبع إرشادات المعالج. انتقل عبر المعالج باستخدام زر **Next**.

الخطوة 1. تحديد إعدادات اتصال الإنترنت

حدد إعدادات الوصول إلى الإنترنت لخادم الإدارة. يجب تكوين الوصول إلى الإنترنت لاستخدام Kaspersky Security Network ولتنزيل تحديثات لقواعد بيانات مكافحة الفيروسات لـ Kaspersky Security Center وتطبيقات Kaspersky المُدارة.



إعدادات اتصال الإنترنت

قم بتمكين الخيار **Use proxy server** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. وفي حالة تمكين هذا الخيار، ستتوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

- **Address**

  عنوان الخادم الوكيل المستخدم لاتصال Kaspersky Security Center بالإنترنت.

- **Port number**

  رقم المنفذ الذي سيتم من خلاله إنشاء اتصال وكيل Kaspersky Security Center.

- **Bypass proxy server for local addresses**

  لن يتم استخدام خادم وكيل للاتصال بالأجهزة في الشبكة المحلية.

- **Proxy server authentication**

  إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

  يتوفر حقل الإدخال هذا إذا تم تحديد خانة الاختيار **استخدام الخادم الوكيل**.

- **User name**

  حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

- Password

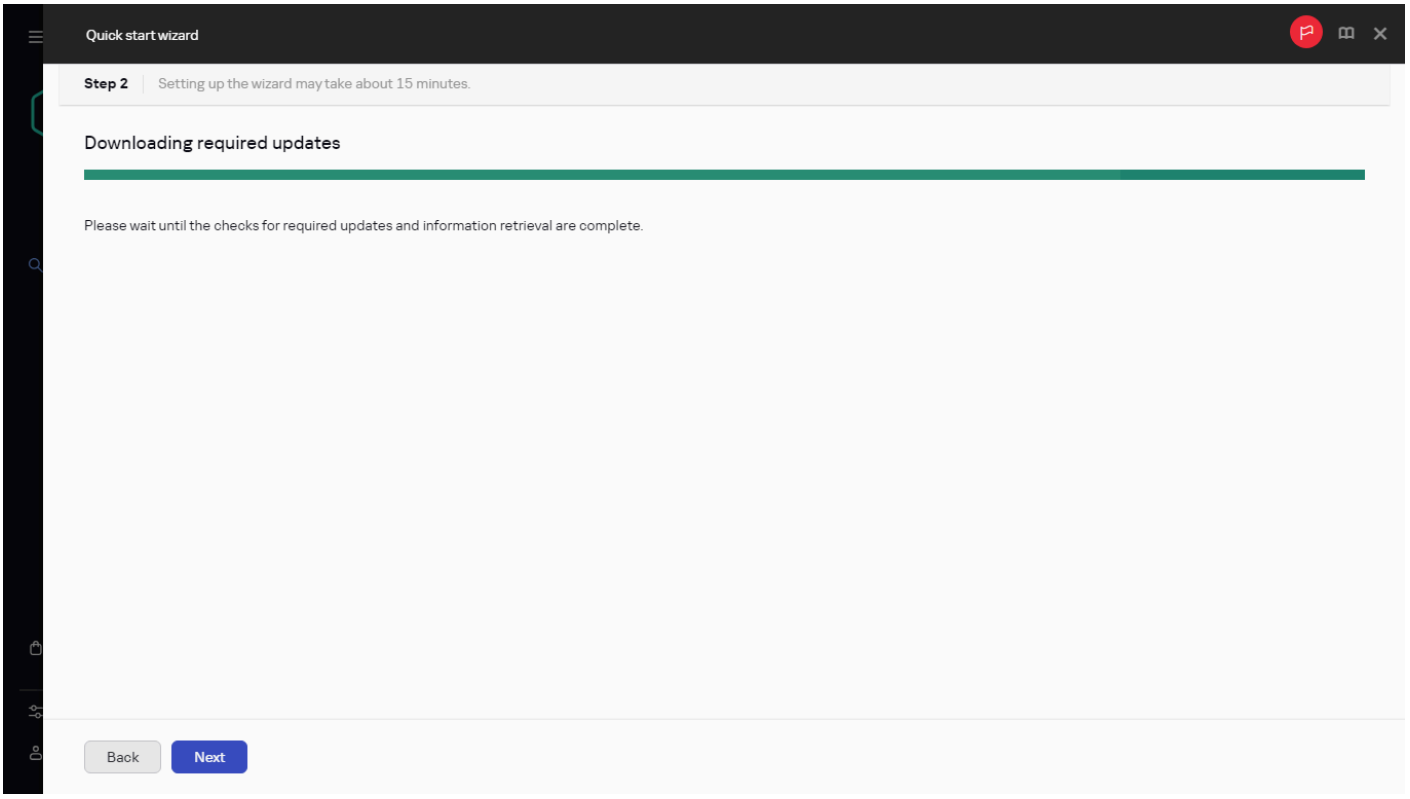
تم تعيين كلمة مرور بواسطة المستخدم الذي تم إنشاء اتصال الخادم الوكيل من خلال حسابه (هذا الحقل متاح في حالة تحديد خانة اختيار **مصادقة الخادم الوكيل**).

لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار** حتى تظهر لك كلمة المرور.

يمكنك تكوين الوصول إلى الإنترنت لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 2. جارٍ تنزيل التحديثات المطلوبة

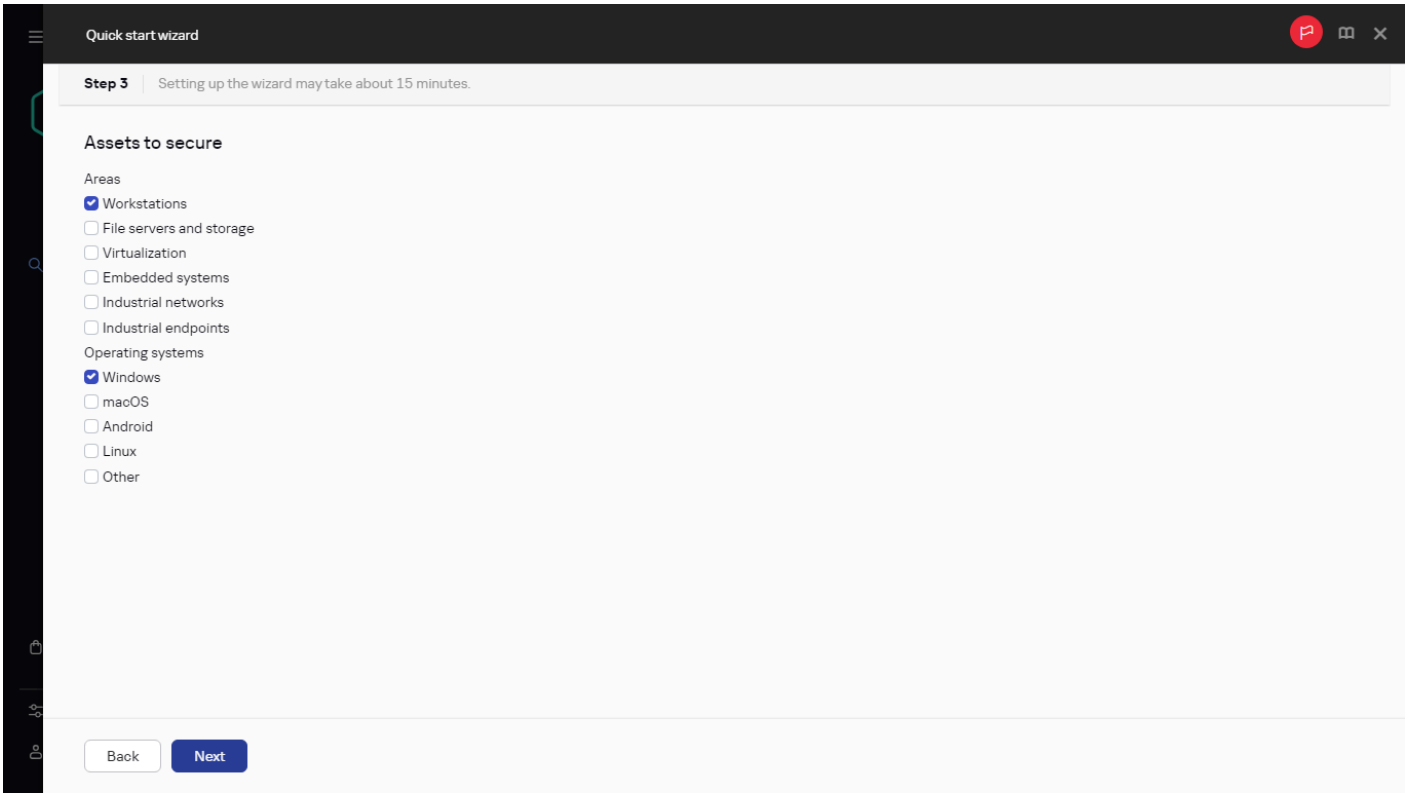
يتم تنزيل التحديثات المطلوبة من خوادم Kaspersky تلقائيًا.



جارٍ تنزيل التحديثات المطلوبة

الخطوة 3. تحديد الأصول التي سيتم حمايتها

حدد مناطق الحماية وأنظمة التشغيل المستخدمة على شبكتك. عند تحديد هذه الخيارات، فإنك تحدد عوامل تصفية مكونات الإدارة الإضافية للتطبيق وحزم التوزيع على خوادم Kaspersky التي يمكنك تنزيلها للتثبيت على أجهزة العملاء في الشبكة لديك.



تحديد الأصول التي سيتم حمايتها

حدد الخيارات:

- **المناطق**

يمكنك تحديد مناطق الحماية التالية:

- **محطات العمل**. حدد هذا الخيار إذا كنت تريد حماية محطات العمل في شبكتك. حسب الإعدادات الافتراضية، يتم تحديد خيار مساحة العمل افتراضيًا.
- **خوادم الملفات والتخزين**. حدد هذا الخيار إذا كنت تريد حماية خوادم الملفات في شبكتك.
- **الأجهزة المحمولة**. حدد هذا الخيار إذا أردت حماية الأجهزة المحمولة التي تمتلكها الشركة أو موظفو الشركة. إذا قمت بتحديد هذا الخيار ولكنك لم تقدم ترخيصًا مع ميزة إدارة الأجهزة المحمولة، فسيتم عرض رسالة تخبرك بضرورة توفير ترخيص مع ميزة إدارة الأجهزة المحمولة. إذا لم تقدم ترخيصًا، فلا يمكنك استخدام ميزة الجهاز المحمول.
- **Virtualization**. حدد هذا الخيار إذا كنت تريد حماية الأجهزة الافتراضية في شبكتك.
- **مكافحة البريد غير المرغوب فيه من Kaspersky**. حدد هذا الخيار إذا أردت حماية خوادم البريد الإلكتروني في مؤسستك من البريد غير المرغوب فيه والاحتيال وتسليم البرامج الضارة.
- **Embedded systems**. حدد هذا الخيار إذا كنت تريد حماية الأنظمة المضمنة التي تستند إلى Windows، مثل ماكينة الصراف الآلي (ATM).
- **Industrial networks**. حدد هذا الخيار إذا كنت تريد مراقبة بيانات الأمان عبر شبكتك الصناعية ومن نقاط نهاية الشبكة المحمية بواسطة تطبيقات Kaspersky.
- **Industrial endpoints**. حدد هذا الخيار إذا كنت تريد حماية العقد الفردية داخل شبكة صناعية.

- **Operating systems**

يمكنك تحديد المنصات التالية:

- Microsoft Windows
- macOS
- Android
- Linux
- أخرى

للحصول على معلومات عن أنظمة التشغيل المدعومة، راجع متطلبات الأجهزة والبرامج لتطبيق Kaspersky Security Center Web Console.

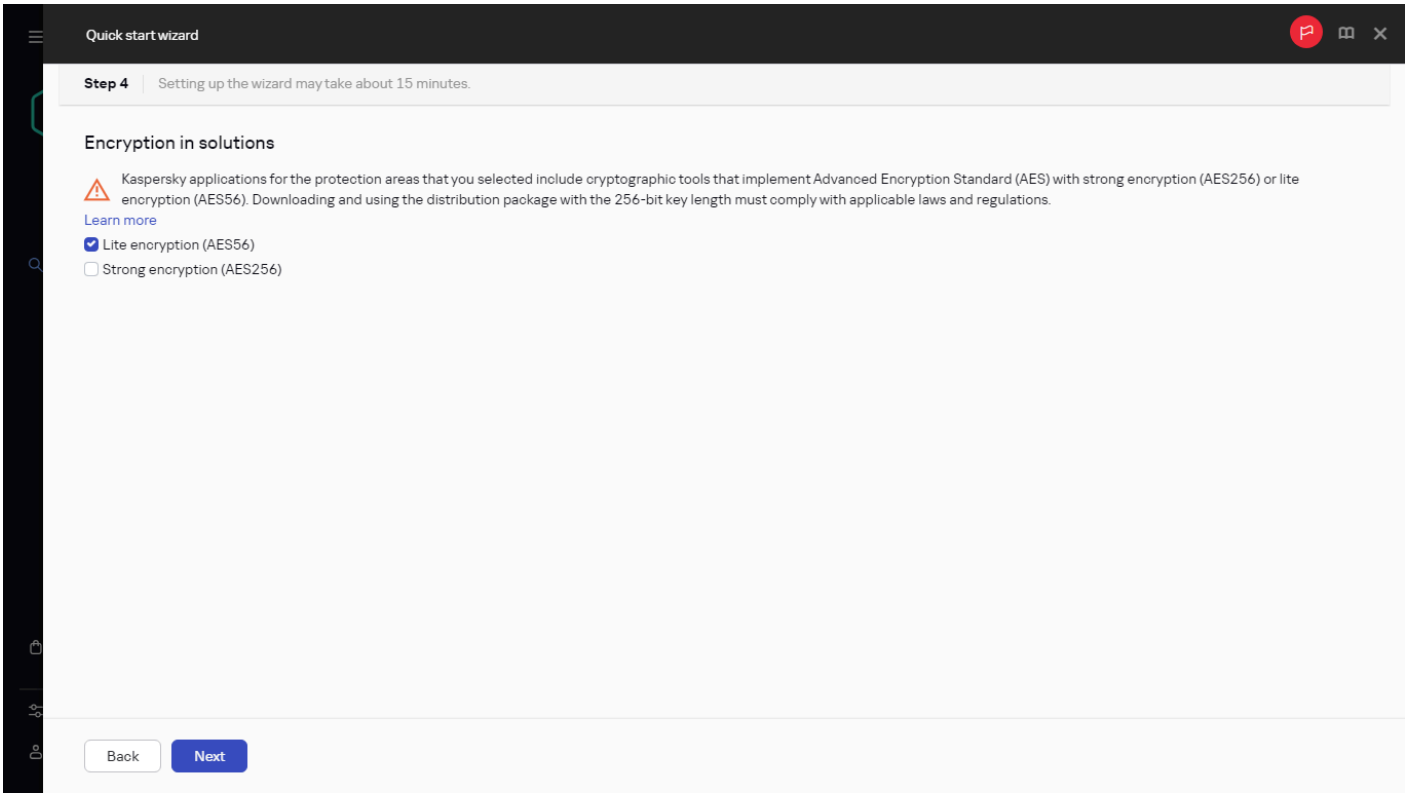
يمكنك تحديد حزم تطبيق Kaspersky من قائمة الحزم المتوفرة لاحقًا، بشكل منفصل عن معالج البدء السريع. لتبسيط البحث عن الحزم المطلوبة، يمكنك ذلك تصفية قائمة الحزم المتاحة حسب معايير متعددة.

الخطوة 4. تحديد التشفير في الحلول

يتم عرض نافذة **Encryption in solutions** فقط إذا حددت **Workstations** كنطاق حماية.

يتضمن Kaspersky Endpoint Security for Windows أدوات تشفير للمعلومات المخزنة على أجهزة العميل القائمة على نظام التشغيل Windows. تحتوي أدوات التشفير هذه على معيار التشفير المتقدم (AES) المطبق بطول مفتاح 256 بت أو 56 بت.

تنزيل واستخدام حزمة التوزيع بطول مفتاح 256 بت يجب أن يتم وفق القوانين واللوائح المعمول بها. لتنزيل حزمة توزيع Kaspersky Endpoint Security for Windows صالحة لاحتياجات مؤسستك، راجع تشريعات البلد التي توجد بها أجهزة العملاء الخاصة بمؤسستك.



تحديد التشفير في الحلول

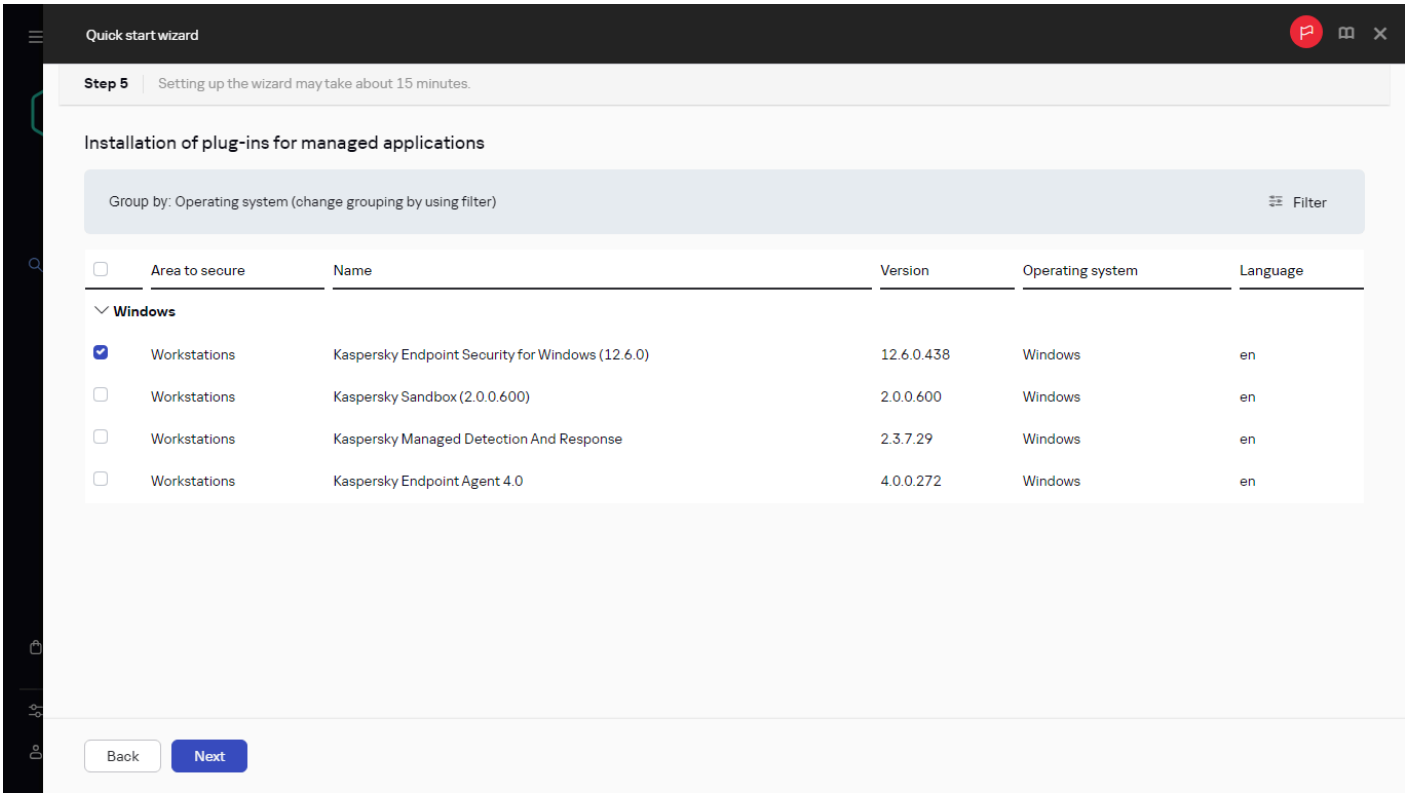
في النافذة **Encryption in solutions**، حدد أحد أنواع التشفير التالية:

- تشفير لايت. يستخدم نوع التشفير هذا طول مفتاح 56 بت.
- تشفير قوي. يستخدم نوع التشفير هذا طول مفتاح 256 بت.

يمكنك تحديد حزمة التوزيع لتطبيق Kaspersky Endpoint Security for Windows بنوع التشفير المطلوب لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 5. تكوين تثبيت المكونات الإضافية للتطبيقات المُدارة

حدد المكونات الإضافية للتطبيقات المُدارة لتثبيتها. تُعرَض قائمة كاملة بالمكونات الإضافية الموجودة على خوادم Kaspersky. يتم تصفية القائمة وفقًا للخيارات المحددة في الخطوة السابقة من المعالج. حسب الإعدادات الافتراضية، تشمل القائمة الكاملة المكونات الإضافية لجميع اللغات. لعرض المكون الإضافي للغة واحدة فقط، استخدم التصفية.



تثبيت المكونات الإضافية للتطبيقات المُدارة

تتضمن قائمة المكونات الإضافية الأعمدة التالية:

- **Area to secure**

  يتم عرض المناطق المحددة لتأمينها في هذا العمود.

- **Type**

  يتم عرض أنواع المكونات الإضافية في هذا العمود.

- **Name**

  تم تحديد المكونات الإضافية حسب مناطق الحماية والأنظمة الأساسية التي حددتها في الخطوة السابقة.

- **Version**

تتضمن القائمة مكونات إضافية لجميع الإصدارات الموجودة على خوادم Kaspersky. حسب الإعدادات الافتراضية، يتم تحديد المكونات الإضافية لأحدث الإصدارات.

- **Latest version**

يوضح هذا العمود ما إذا كان إصدار المكون الإضافي هو أحدث إصدار. في حالة عرض القيمة **true**، فإن المكون الإضافي المقابل هو أحدث إصدار. في حالة عرض القيمة **false**، فإن المكون الإضافي المقابل يوجد له إصدار أحدث.

- **Operating system**

يعرض هذا العمود أنظمة تشغيل المكونات الإضافية.

- **Language**

حسب الإعدادات الافتراضية، تُعرَّف لغة الترجمة الخاصة بالمكون الإضافي بواسطة لغة Kaspersky Security Center التي حددتها عند التثبيت. يمكنك تحديد لغات أخرى في قائمة **إظهار لغة ترجمة وحدة تحكم الإدارة أو** المنسدلة.

بعد تحديد المكونات الإضافية، انقر على **Next** لبدء التثبيت.

يمكنك تثبيت المكونات الإضافية للإدارة لتطبيقات Kaspersky يدويًا، بشكل منفصل عن معالج البدء السريع.

يقوم معالج البدء السريع تلقائيًا بتثبيت المكونات الإضافية المحددة. لتثبيت بعض المكونات الإضافية، يجب عليك قبول شروط اتفاقية ترخيص المستخدم النهائي. اقرأ نص اتفاقية ترخيص المستخدم النهائي المعروض، وحدد خانة الاختيار **I agree to use Kaspersky Security Network** وانقر فوق الزر **Install**. إذا لم تقبل شروط اتفاقية ترخيص المستخدم النهائي، فلن يتم تثبيت المكون الإضافي.

عندما يتم تثبيت جميع المكونات الإضافية المحددة، ينقلك معالج البدء السريع إلى الخطوة التالية تلقائيًا.

الخطوة 6. تثبيت المكونات الإضافية المحددة

يقوم معالج البدء السريع تلقائيًا بتثبيت المكونات الإضافية التي حددتها في الخطوة السابقة. لتثبيت بعض المكونات الإضافية، يجب عليك قبول شروط اتفاقية ترخيص المستخدم النهائي. اقرأ نص اتفاقية ترخيص المستخدم النهائي المعروض، وحدد خانة الاختيار **I agree to use Kaspersky Security Network** وانقر فوق الزر **Install**. إذا لم تقبل شروط اتفاقية ترخيص المستخدم النهائي، فلن يتم تثبيت المكون الإضافي.

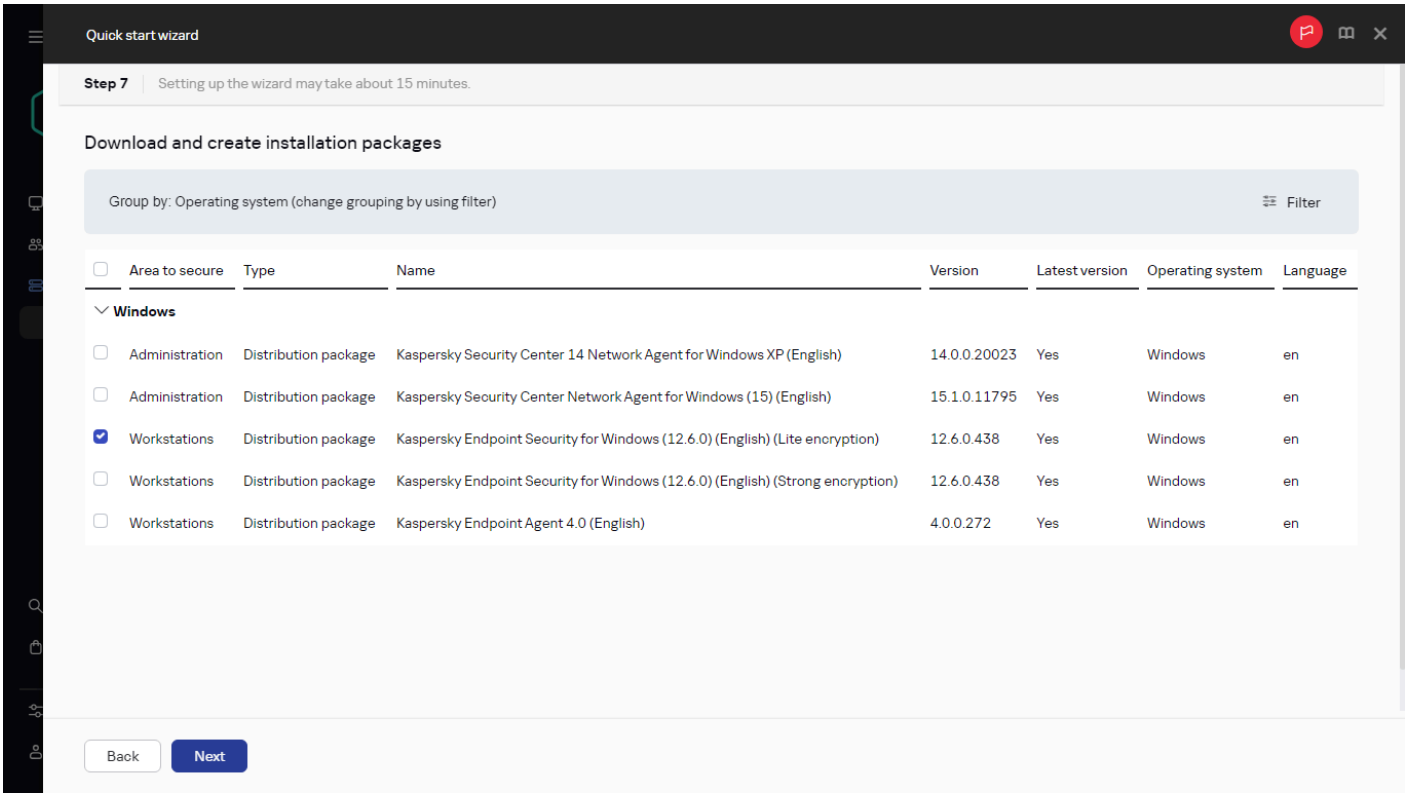
عندما يتم تثبيت جميع المكونات الإضافية المحددة، ينقلك معالج البدء السريع إلى الخطوة التالية تلقائيًا.

الخطوة 7. تنزيل حزم التوزيع وإنشاء حزم التثبيت

حدد حزم التوزيع لتنزيلها.

التوزيعات التطبيقات المُدارة قد يتطلب تثبيت إصدار أدنى محدد من Kaspersky Security Center.

بعد تحديد نوع تشفير في Kaspersky Endpoint Security for Windows، يتم عرض قائمة كاملة بحزم توزيع نوعي التشفير على حد سواء. يتم تحديد حزمة التوزيع في القائمة مع نوع التشفير الذي حددته. يمكنك تحديد حزم التوزيع لأي نوع تشفير. تتوافق لغة حزمة التوزيع مع لغة Kaspersky Security Center. في حالة عدم وجود حزمة توزيع من Kaspersky Endpoint Security for Windows للغة Kaspersky Security Center، يتم تحديد حزمة توزيع اللغة الإنجليزية.



تنزيل حزم التوزيع وإنشاء حزم التثبيت

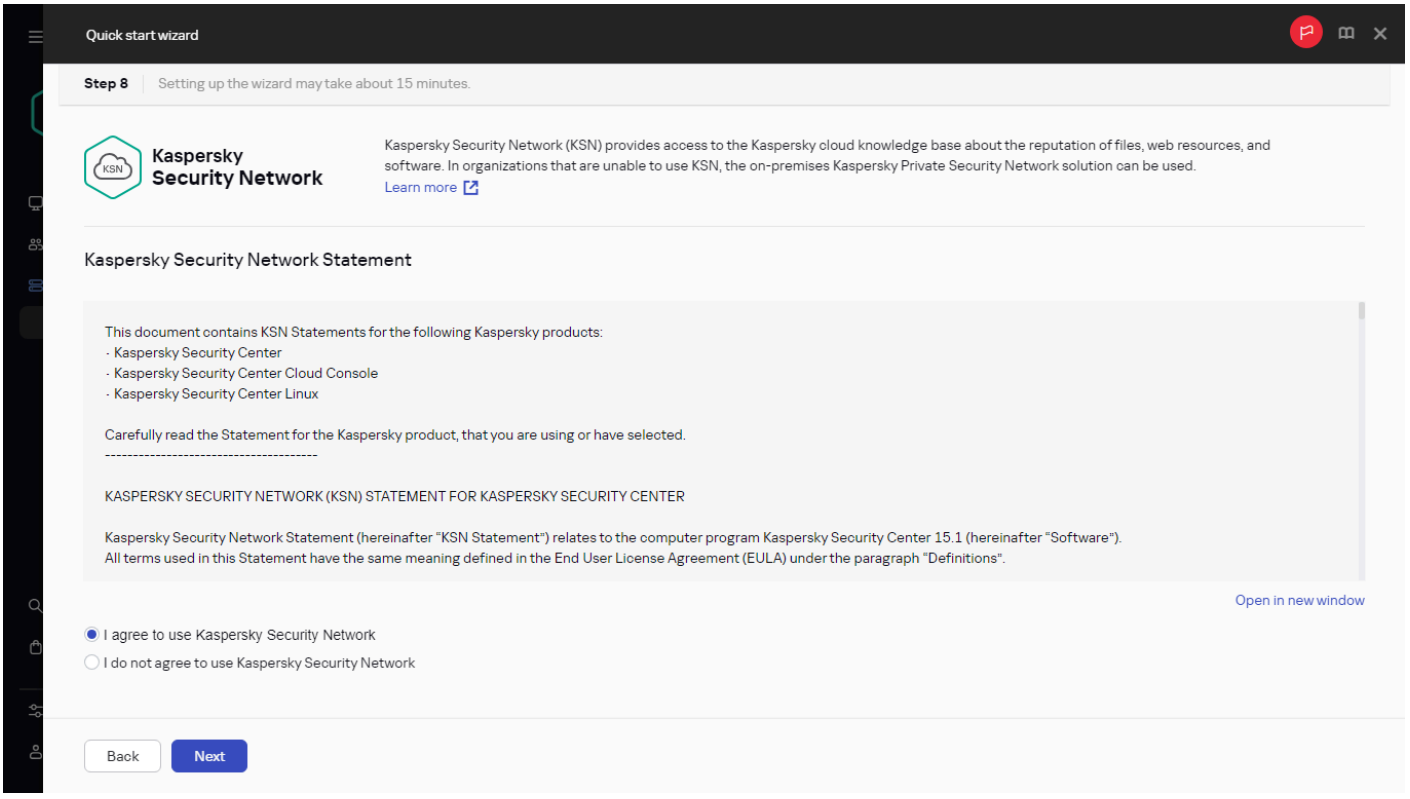
لإنهاء تنزيل بعض حزم التوزيع، يجب عليك قبول EULA. عند النقر على زر **أوافق** ، يُعرَض نص اتفاقية ترخيص المستخدم النهائي. للمضي قدمًا إلى الخطوة التالية، يجب عليك قبول شروط وأحكام اتفاقية ترخيص المستخدم النهائي وأحكامها وشروط سياسة الخصوصية الخاصة بـ Kaspersky وأحكامها. في حالة عدم قبول الشروط والأحكام، فسيتم إلغاء تنزيل الحزمة.

بعد قبولك لشروط اتفاقية ترخيص المستخدم النهائي وأحكامها وشروط سياسة خصوصية Kaspersky وأحكامها، يستمر تنزيل حزم التوزيع. ستستخدم فيما بعد حزم التثبيت لنشر تطبيقات Kaspersky على أجهزة العملاء.

يمكنك تنزيل حزم التوزيع وإنشاء حزم التثبيت لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 8. تكوين Kaspersky Security Network

تحديد الإعدادات لترحيل المعلومات حول عمليات Kaspersky Security Center إلى قاعدة معارف Kaspersky Security Network.



تكوين Kaspersky Security Network

حدد أحد الخيارات التالية:

- **I agree to use Kaspersky Security Network**

سيقوم Kaspersky Security Center والتطبيقات المدارة المثبتة على الأجهزة العميلة بنقل تفاصيل عملياته تلقائيًا إلى Kaspersky Security Network. تضمن المشاركة في Kaspersky Security Network التحديثات السريعة لقواعد البيانات التي تشتمل على معلومات حول الفيروسات وغيرها من التهديدات، مما يضمن الاستجابة السريعة للتهديدات الأمنية الطارئة.

- **I do not agree to use Kaspersky Security Network**

لن يوفر Kaspersky Security Center والتطبيقات المدارة أية معلومات إلى Kaspersky Security Network.

إذا قمت بتحديد هذا الخيار، فسيتم تعطيل استخدام Kaspersky Security Network.

يمكنك إعداد الوصول إلى Kaspersky Security Network (KSN) لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 9. تحديد طريقة تفعيل التطبيق

حدد أحد خيارات تفعيل Kaspersky Security Center التالية:

- **عن طريق إدخال رمز التنشيط الذي تملكه**

رمز التنشيط هو تسلسل فريد مكون من 20 حرفًا أبجديًا رقميًا. حيث تقوم بإدخال رمز تنشيط لإضافة مفتاح الذي يقوم بدوره بتنشيط Kaspersky Security Center. تتلقى رمز التنشيط عبر عنوان البريد الإلكتروني الذي حددته بعد شراء Kaspersky Security Center.

لتفعيل التطبيق باستخدام رمز التفعيل، ستحتاج إلى الوصول إلى الإنترنت لإنشاء اتصال مع خوادم تفعيل Kaspersky.

إذا قمت بتحديد خيار التفعيل هذا، فيمكنك تمكين خيار **Automatically distribute license key to managed devices**.

إذا تم تمكين هذا الخيار، فسيتم نشر مفتاح الترخيص تلقائيًا على الأجهزة المُدارة.

إذا تم تعطيل هذا الخيار، فيمكنك نشر مفتاح الترخيص للأجهزة المُدارة فيما بعد، في جزء **تراخيص Kaspersky** لشجرة وحدة تحكم الإدارة.

- **عن طريق تحديد ملف مفتاح**

ملف المفتاح هو ملف بامتداد .key مقدم لك من Kaspersky. الهدف من ملف المفتاح هو إضافة مفتاح لتنشيط التطبيق.

يتم وصف طرق الحصول على ملف المفتاح في القسم التالي: حول ملف المفتاح.

لتنشيط التطبيق باستخدام ملف المفتاح، لا تحتاج إلى الاتصال بخوادم تنشيط Kaspersky.

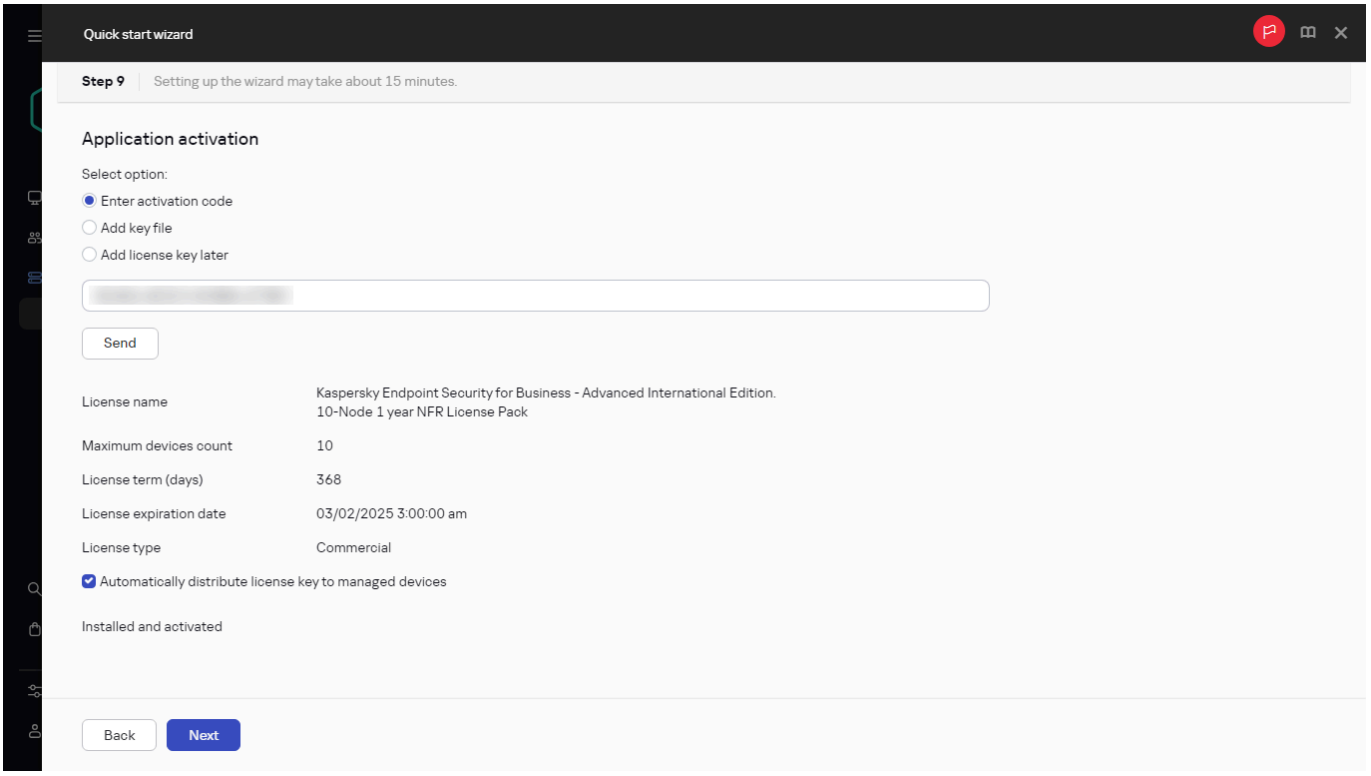
إذا قمت بتحديد خيار التفعيل هذا، فيمكنك تمكين خيار **Automatically distribute license key to managed devices**.

إذا تم تمكين هذا الخيار، فسيتم نشر مفتاح الترخيص تلقائيًا على الأجهزة المُدارة.

إذا تم تعطيل هذا الخيار، فيمكنك نشر مفتاح الترخيص للأجهزة المُدارة فيما بعد، في جزء **تراخيص Kaspersky** لشجرة وحدة تحكم الإدارة.

- **عن طريق تأجيل تفعيل التطبيق**

سيعمل التطبيق باستخدام الوظائف الأساسية، دون إدارة الجهاز المحمول ودون إدارة الثغرات الأمنية والتصحيحات.



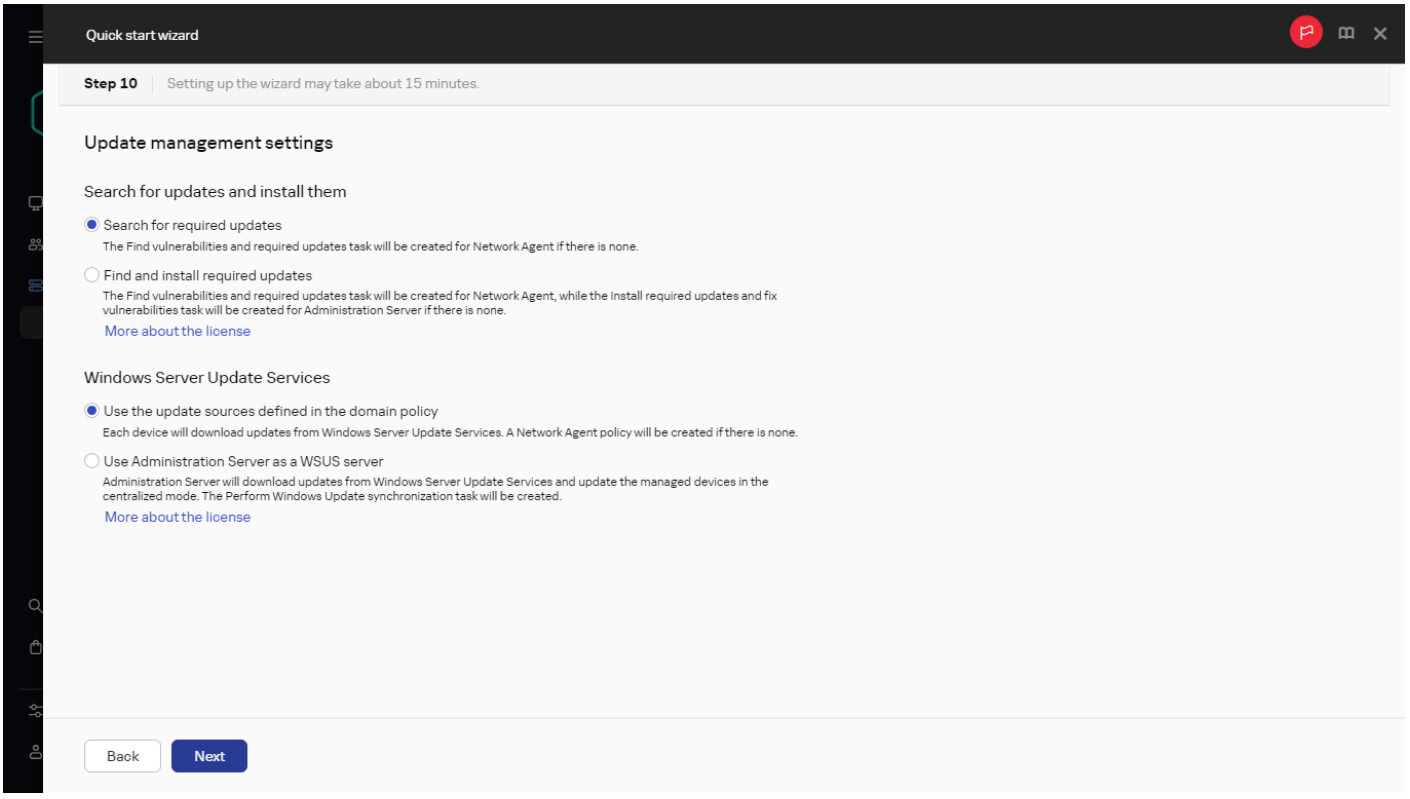
تحديد طريقة تفعيل التطبيق

إذا اخترت تأجيل تنشيط التطبيق، يمكنك إضافة مفتاح ترخيص في أي وقت لاحق عن طريق تحديد **Licensing** ← **Operations**.

عند استخدام Kaspersky Security Center الذي تم نشره من AMI مدفوع أو لمنتج تتم المحاسبة عليه شهريًا على أساس الاستخدام، لا يمكنك تحديد ملف مفتاح أو إدخال رمز.

الخطوة 10. تحديد إعدادات إدارة التحديث من جهة خارجية

لا يتم عرض هذه الخطوة إذا لم يكن لديك ترخيص إدارة الثغرات الأمنية والتصحيحات وكانت مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة موجودة بالفعل.



إعدادات إدارة التحديث من جهة خارجية

لتحديثات برامج الأطراف الخارجية، حدد أحد الخيارات التالية:

- **Search for required updates**

  يتم إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا، إذا لم يكن لديك واحدة.

  ويتم تحديد هذا الخيار بصورة افتراضية.

- **Find and install required updates**

  يتم إنشاء مهام بحث عن الثغرات الأمنية والتحديثات المطلوبة وتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية تلقائيًا، إذا لم يكن لديك واحدة.

  هذا الخيار غير متاح إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

لتحديثات Windows Update، حدد أحد الخيارات التالية:

- **Use the update sources defined in the domain policy**

  ستقوم أجهزة العملاء بتنزيل تحديثات Windows Update وفقًا لإعدادات سياسة المجال الخاصة بك. يتم إنشاء سياسة عميل الشبكة تلقائيًا، إذا لم يكن لديك واحدة.

- **Use Administration Server as a WSUS server**

  تقوم أجهزة العملاء بتنزيل تحديثات Windows Update من خادم الإدارة. يتم إنشاء مهمة إجراء مزامنة Windows Update وسياسة عميل الشبكة تلقائيًا، إذا لم يكن لديك واحدة.

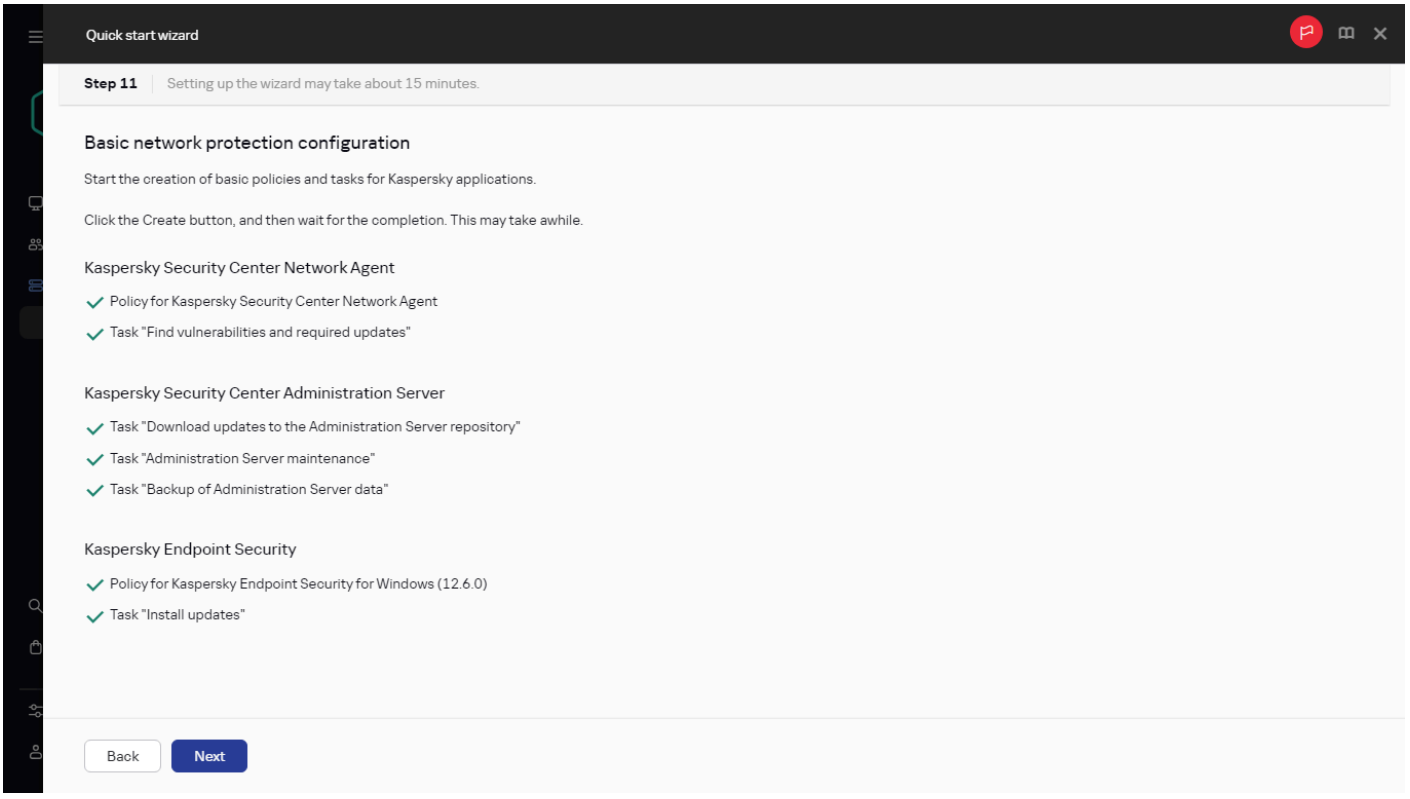
هذا الخيار غير متاح إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

يمكنك إنشاء مهمتي البحث عن الثغرات الأمنية والتحديثات المطلوبة وتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية بشكل منفصل عن معالج البدء السريع. لاستخدام خادم الإدارة كخادم WSUS، أنشئ مهمة تنفيذ مزامنة Windows Update، ثم حدد الخيار **استخدام خادم الإدارة كخادم WSUS** في سياسة عميل الشبكة.

الخطوة 11. إنشاء تكوين أساسي لحماية الشبكة

يمكنك التحقق من قائمة بالسياسات والمهام التي تم إنشاؤها.

انتظار حتى اكتمال إنشاء السياسات والمهام قبل المتابعة إلى الخطوة التالية للمعالج.

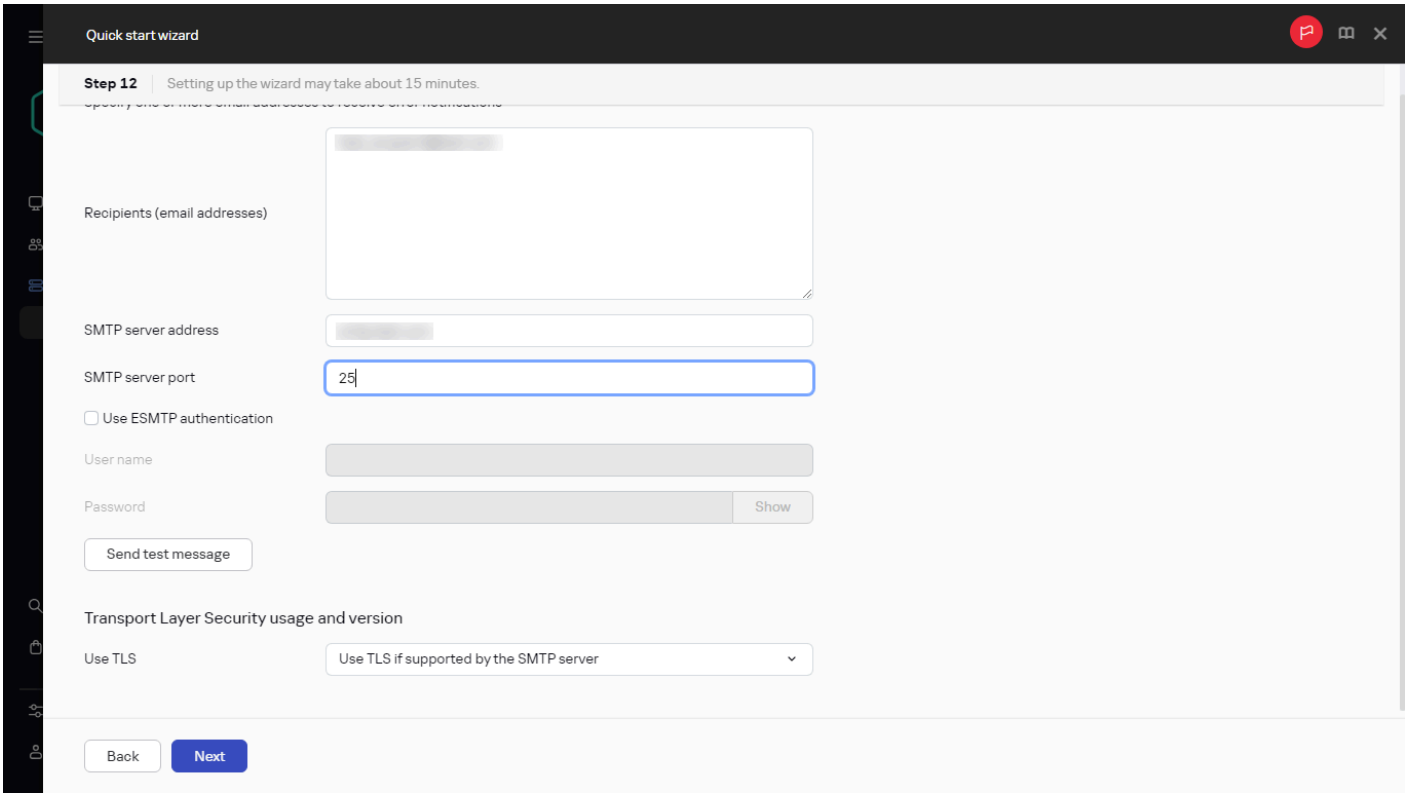


إنشاء تكوين أساسي لحماية الشبكة

يمكنك إنشاء المهام والسياسات الطلوبة لاحقًا، بشكل منفصل عن معالج البدء السريع.

الخطوة 12. تكوين إشعارات البريد الإلكتروني

قم بتكوين تسليم الإخطارات المتعلقة بالأحداث المسجلة أثناء تشغيل تطبيقات Kaspersky على الأجهزة العميلة. وستُستخدم هذه الإعدادات كإعدادات افتراضية لسياسات التطبيق.



تكوين إشعارات البريد الإلكتروني

لتكوين تسليم الإخطارات المتعلقة بالأحداث التي تجري في تطبيقات Kaspersky، استخدم الإعدادات التالية:

- **Recipients (email addresses)**

عناوين البريد الإلكتروني للمستخدمين التي ستقوم التطبيقات بإرسال الإخطارات إليها. يمكنك إدخال عنوان واحد أو أكثر، وفي حالة إدخال أكثر من عنوان، فافصل بينها باستخدام فواصل منقوطة.

- **SMTP server address**

عنوان أو عناوين خوادم البريد الخاصة بمؤسستك.

في حالة إدخال أكثر من عنوان واحد، افصل بينها باستخدام فواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

- **SMTP server port**

رقم منفذ الاتصال الخاص بخادم SMTP. إذا كنت تستخدم عدة خوادم SMTP، فسيتم إنشاء الاتصال بها من خلال منفذ الاتصال المحدد. رقم المنفذ الافتراضي هو 25.

- **Use ESMTP authentication**

تمكين دعم مصادقة ESMTP. عند تحديد خانة الاختيار الموجودة في الحقول **اسم المستخدم** و**كلمة المرور**، يمكنك تحديد إعدادات مصادقة ESMTP. تكون خانة الاختيار غير محددة بشكل افتراضي.

- **Use TLS**

يمكنك تحديد إعدادات TLS للاتصال بخادم SMTP:

- **Do not use TLS**

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

- **Use TLS if supported by the SMTP server**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام اتصال TLS مع خادم SMTP. إذا كان خادم SMTP لا يدعم TLS، فإن خادم الإدارة يتصل بخادم SMTP بدون استخدام TLS.

- **Always use TLS, check server certificate validity**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام إعدادات مصادقة TLS. إذا كان خادم SMTP لا يدعم TLS، فلن يتمكن خادم الإدارة من توصيل خادم SMTP.

> نوصي باستخدام هذا الخيار لتوفير حماية أفضل للاتصال بخادم SMTP. إذا قمت بتحديد هذا الخيار، فيمكنك تعيين إعدادات المصادقة لاتصال TLS.

إذا قمت بتحديد قيمة **Always use TLS, check server certificate validity** فيمكنك تحديد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال من خلال أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. يمكنك أيضًا تحديد شهادة لمصادقة العميل على خادم SMTP.

يمكنك تحديد شهادات لاتصال TLS بالنقر فوق رابط : **Specify certificates**

- تصفح للوصول إلى ملف شهادة خادم SMTP:

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

- تصفح للوصول إلى ملف شهادة العميل:

يمكنك استخدام شهادة استلمتها من أي مصدر، على سبيل المثال، من أي جهة إصدار موثوقة. يجب تحديد الشهادة ومفتاحها الخاص باستخدام أحد أنواع الشهادات التالية:

- شهادة X-509:

يجب تحديد ملف مع الشهادة وملف مع المفتاح الخاص. كلا الملفين لا يعتمدان على بعضهما البعض وترتيب تحميل الملفات ليس مهمًا. عند تحميل كلا الملفين، يجب تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- الحاوية pkcs12:

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك بعد ذلك تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

يمكنك اختبار إعدادات إخطار البريد الإلكتروني الجديدة بالنقر فوق الزر **Send test message**.

يمكنك تكوين إخطارات الحدث لاحقًا، بشكل منفصل عن معالج البدء السريع.

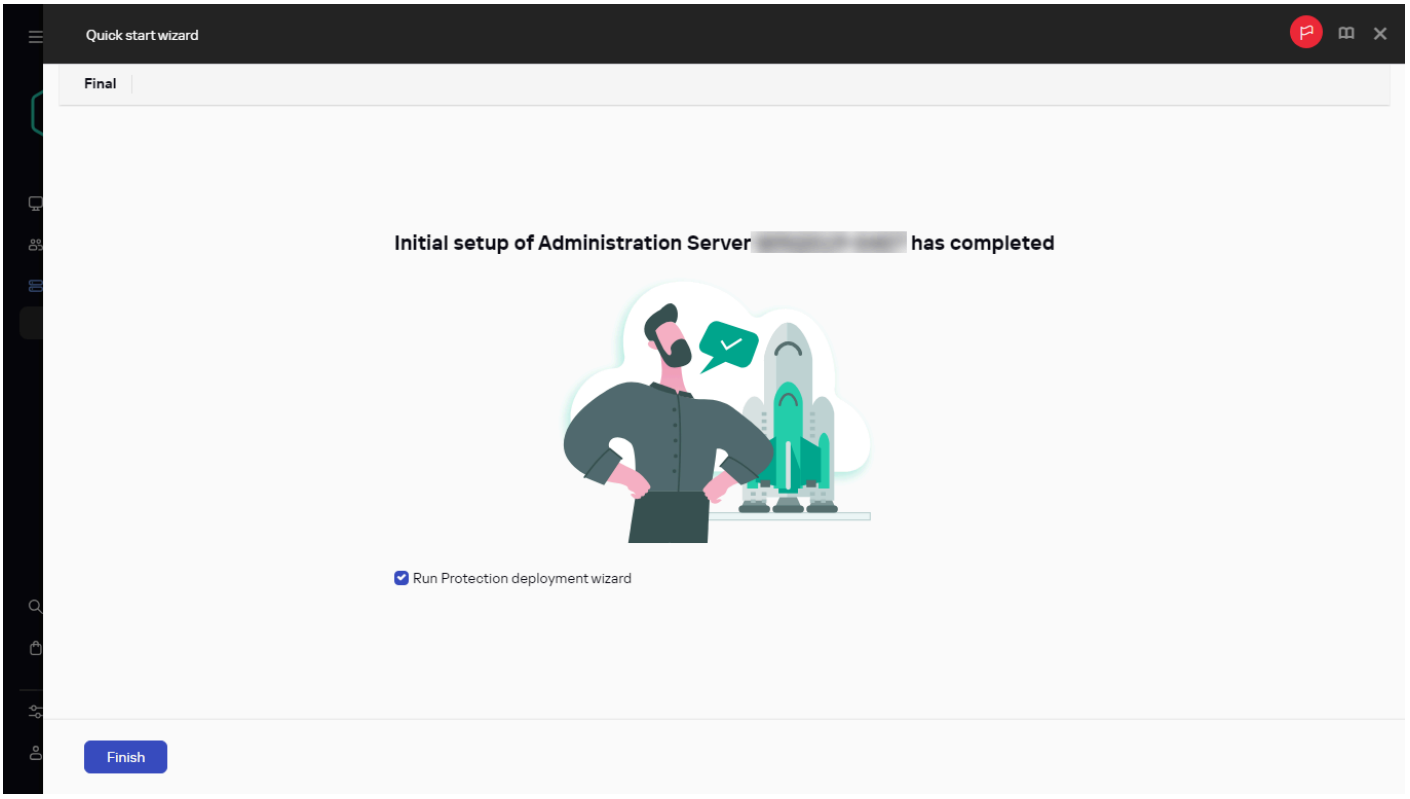
الخطوة 13. إجراء استطلاع على الشبكة

يجري خادم الإدارة تحققًا أوليًا من إرسال البيانات. سيظهر شريط تقدم أثناء الاستطلاع. سيصبح رابط **View detected devices** متاحًا بعدما ينتهي الاستطلاع. يمكنك النقر على الرابط لعرض أجهزة الشبكة التي اكتشفها خادم الإدارة. للعودة إلى معالج البدء السريع، انقر على مفتاح **Escape** .

يمكنك التحقق من إرسال البيانات على شبكتك لاحقًا، بشكل منفصل عن معالج البدء السريع. واستخدم Kaspersky Security Center Web Console لتكوين استقصاء وحدة التحكم في المجال ومجالات Windows ونطاقات IP وشبكات IPv6.

الخطوة 14. إغلاق معالج البدء السريع

في صفحة إكمال معالج البدء السريع، حدد خانة الاختيار **Run Protection deployment wizard** إذا كنت ترغب في بدء التثبيت التلقائي لتطبيقات مكافحة الفيروسات أو عميل الشبكة على الأجهزة الموجودة في شبكتك.



الخطوة الأخيرة في معالج البدء السريع

لإغلاق المعالج، انقر على زر **Finish**.

توصيل الأجهزة خارج المكتب

يصف هذا السيناريو كيفية توصيل الأجهزة الموجودة خارج المكتب (المدارة والموجودة خارج نطاق الشبكة الرئيسية) بخادم الإدارة.

السيناريو: توصيل الأجهزة الموجودة خارج المكتب عن طريق بوابة الاتصال

يوضح هذا السيناريو كيفية توصيل الأجهزة المدارة والموجودة خارج الشبكة الرئيسية بخادم الإدارة.

المتطلبات الأساسية

السيناريو له متطلبات أساسية كالآتي:

- يتم تنظيم منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ) في شبكة مؤسستك.
- يتم نشر خادم إدارة Kaspersky Security Center على شبكة الشركة.

المراحل

يستمر هذا السيناريو على مراحل:

1. **تحديد جهاز عميل في منطقة الأجهزة الموصلة مباشرة بالإنترنت**

   سيتم استخدام هذا الجهاز كبوابة اتصال. يجب أن يستوفي الجهاز الذي تحدده متطلبات بوابات الاتصال.

2. **تثبيت دور عميل الشبكة في بوابة الاتصال**

   نوصي باستخدام التثبيت المحلي لتثبيت عميل الشبكة على الجهاز المحدد.

   بشكلٍ افتراضي، يوجد ملف التثبيت في:\\<server name>\KLSHARE\Pkglnst\<version number>_NetAgent

   في النافذة **بوابة الاتصال** في معالج إعداد عميل الشبكة، حدد **استخدام عميل الشبكة كبوابة اتصال في DMZ**. ينشط هذا الوضع دور بوابة الاتصال بشكل متزامن، ويطلب من عميل الشبكة انتظار الاتصالات من خادم الإدارة بدلاً من إنشاء الاتصالات بخادم الإدارة.

   بدلاً من ذلك، يمكنك تثبيت عميل الشبكة على جهاز Linux وتكوين عميل الشبكة للعمل كبوابة اتصال، ولكن انتبه إلى قائمة قيود عميل الشبكة الذي يعمل على أجهزة Linux.

3. **السماح بالاتصالات بجدران الحماية على بوابة الاتصال**

   للتأكد من أن خادم الإدارة يمكنه الاتصال فعليًا ببوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت، اسمح بالاتصالات بمنفذ TCP رقم 13000 في جميع جدران الحماية بين خادم الإدارة وبوابة الاتصال.

   إذا لم يكن لبوابة الاتصال عنوان IP حقيقي على الإنترنت ولكنها تقع خلف ترجمة عنوان الشبكة (NAT)، فقم بتكوين قاعدة لإعادة توجيه الاتصالات من خلال ترجمة عنوان الشبكة.

4. **قم بإنشاء مجموعة إدارة للأجهزة الخارجية**

   أنشئ مجموعة جديدة تحت مجموعة **Managed devices**. المجموعة الجديدة ستحتوي على الأجهزة المُدارة الخارجية.

5. **توصيل بوابة الاتصال بخادم الإدارة**

   تنتظر بوابة الاتصال التي قمت بتكوينها اتصالاً من خادم الإدارة. ومع ذلك، لا يقوم خادم الإدارة بإدراج الجهاز وبوابة الاتصال بين الأجهزة المدارة. وذلك لأن بوابة الاتصال لم تحاول إنشاء اتصال بخادم الإدارة. لذلك، تحتاج إلى القيام بإجراء خاص للتأكد من أن خادم الإدارة ينشأ اتصالاً ببوابة الاتصال.

   قم بما يلي:

   1. أضف بوابة الاتصال كنقطة توزيع.
   2. انقل بوابة الاتصال من مجموعة **Unassigned devices** إلى المجموعة التي قمت بإنشائها للأجهزة الخارجية.

   تم توصيل بوابة الاتصال وتكوينها.

6. **توصيل الأجهزة المكتبية الخارجية بخادم الإدارة**

   في العادة، لا يتم نقل الأجهزة المكتبية الخارجية داخل المحيط. لذلك أنت بحاجة إلى تكوينها للاتصال بخادم الإدارة من خلال البوابة عند تثبيت عميل الشبكة.

7 **إعداد تحديثات الأجهزة المكتبية الخارجية**

إذا تم تكوين تحديثات تطبيقات الأمان بحيث يتم تنزيلها من خادم الإدارة، فستقوم الأجهزة الخارجية بتنزيل التحديثات من خلال بوابة الاتصال. هذا الأمر له عيبان:

- هذه حركة مرور غير ضرورية، تستهلك عرض النطاق الترددي لقناة الاتصال عبر الإنترنت الخاصة بالشركة.
- هذه ليست بالضرورة أسرع طريقة للحصول على التحديثات. من المحتمل جدًا أنه سيكون من الأرخص والأسرع أن تتلقى الأجهزة الخارجية التحديثات من خوادم Kaspersky.

قم بما يلي:

1. انقل جميع الأجهزة الخارجية إلى مجموعة الإدارة المنفصلة التي سبق لك إنشاؤها.
2. استبعد المجموعة ذات الأجهزة الخارجية من مهمة التحديث.
3. قم بإنشاء مهمة تحديث منفصلة للمجموعة ذات الأجهزة الخارجية.

8 **توصيل أجهزة الكمبيوتر المحمولة المتنقلة بخادم الإدارة**

تقع أجهزة الكمبيوتر المحمولة المتنقلة في نطاق الشبكة في بعض الأحيان وخارجها في أوقات أخرى. للإدارة الفعالة، أنت بحاجة للاتصال بخادم الإدارة بشكل مختلف حسب موقعها. للاستخدام الفعال لحركة المرور، يتطلب أيضًا تلقي تحديثات من مصادر مختلفة حسب موقعها.

أنت بحاجة إلى تكوين القواعد للمستخدمين خارج المكتب : ملفات تعريف الاتصال وأوصاف موقع الشبكة. تحدد كل قاعدة خادم الإدارة الذي يلزم اتصاله بأجهزة الكمبيوتر المحمولة المتنقلة بناءً على موقعها وخادم الإدارة الذي يتطلب تلقي التحديثات منه.

السيناريو: توصيل الأجهزة خارج المكتب من خلال خادم إدارة ثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)

إذا كنت تريد توصيل الأجهزة المدارة الموجودة خارج الشبكة الرئيسية بخادم الإدارة، يمكنك فعل ذلك باستخدام خادم إدارة ثانوي موجود في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ).

المتطلبات الأساسية

قبل البدء، تأكد من إجرائك لما يلي:

- يتم تنظيم منطقة أجهزة موصلة مباشرة بالإنترنت (DMZ) في شبكة مؤسستك.
- يتم نشر خادم إدارة Kaspersky Security Center على الشبكة الداخلية للمؤسسة.

المراحل

يستمر هذا السيناريو على مراحل:

1 **تحديد جهاز عميل في منطقة الأجهزة الموصلة مباشرة بالإنترنت**

في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، حدد جهاز العميل الذي سيتم استخدامه كخادم إدارة ثانوي.

2 **تثبيت خادم إدارة Kaspersky Security Center**

قم بتثبيت خادم إدارة Kaspersky Security Center على جهاز العميل هذا:

3 **إنشاء تسلسل هرمي لخوادم الإدارة**

إذا وضعت خادم إدارة ثانوي في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، فيجب أن يتلقى خادم الإدارة الثانوي اتصالاً من خادم الإدارة الأساسي. ولكي تفعل هذا، أضف خادم إدارة جديد كخادم تابع وبذلك يمكن لخادم الإدارة الرئيسي الاتصال بخادم الإدارة الثانوي عبر المنفذ 13000. عند الجمع بين خادمي إدارة في تسلسل هرمي، تأكد من أنه يمكن الوصول إلى المنفذ 13299 على خادمي الإدارة كليهما. يتصل Kaspersky Security Center Web Console بخادم إدارة عبر المنفذ 13299.

4 **توصيل الأجهزة المُدارة خارج المكتب بخادم الإدارة الثانوي**

يمكنك توصيل الأجهزة خارج المكتب بخادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ) بالطريقة نفسها التي يتم استخدامها لإنشاء الاتصال بين خادم الإدارة والأجهزة المدارة الموجودة في الشبكة الرئيسية. تبدأ الأجهزة المدارة خارج المكتب الاتصال عبر المنفذ 13000.

حول توصيل الأجهزة خارج المكتب

دائمًا ما تقع بعض الأجهزة المُدارة خارج نطاق الشبكة الرئيسية (على سبيل المثال، الأجهزة في الفروع الإقليمية للشركة؛ الأكشاك وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ الأجهزة في المكاتب المنزلية للموظفين). تنتقل بعض الأجهزة خارج المحيط من وقت لآخر (على سبيل المثال، أجهزة الكمبيوتر المحمولة بالمستخدمين الذين يزورون الفروع الإقليمية أو مكاتب العملاء).

ما زلت بحاجة إلى مراقبة حماية الأجهزة خارج المكتب وإدارتها – تلقي معلومات فعلية حول حالة الحماية الخاصة بهم والحفاظ على تطبيقات الأمان الموجودة عليها في حالة محدثة. هذا الأمر ضروري لأنه، على سبيل المثال، إذا تم اختراق مثل هذا الجهاز أثناء وجوده بعيدًا عن الشبكة الرئيسية، فقد يصبح منصة لنشر التهديدات بمجرد اتصاله بالشبكة الرئيسية. لتوصيل الأجهزة خارج المكتب بخادم الإدارة، يمكنك استخدام طريقتين:

- بوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)

  اطلع على نظام حركة مرور البيانات: خادم الإدارة الموجود في الشبكة المحلية، والأجهزة المدارة على الإنترنت، وبوابة الاتصال المستخدمة بالفعل

- خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت

  اطلع على نظام حركة مرور البيانات: خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت والأجهزة المدارة على الإنترنت

بوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت

الطريقة الموصى بها لتوصيل الأجهزة الموجودة خارج المكتب بخادم الإدارة هي تنظيم منطقة الأجهزة الموصلة مباشرة بالإنترنت في شبكة المؤسسة وتثبيت بوابة اتصال فيها. ستتصل الأجهزة الخارجية ببوابة الاتصال، وسيبدأ خادم الإدارة الموجود بداخل الشبكة الاتصال بالأجهزة عبر بوابة الاتصال.

بالمقارنة مع الطريقة الأخرى، تعد هذه الطريقة أكثر أمانًا:

- فهي لا تحتاج إلى فتح الوصول إلى خادم الإدارة من خارج الشبكة.
- لا تشكل بوابة الاتصال المخترقة خطراً كبيراً على سلامة الأجهزة المتصلة بالشبكة. لا تدير بوابة الاتصال أي شيء فعليًا ولا تنشئ أي اتصالات.

ولا تتطلب بوابة الاتصال أيضًا توفر العديد من موارد الأجهزة.

ومع ذلك، فإن هذه الطريقة بها عملية تكوين أكثر تعقيدًا:

- لجعل جهاز يعمل كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت، يتطلب منك تثبيت عميل الشبكة وتوصيله بخادم الإدارة بطريقة محددة.
- لن تتمكن من استخدام نفس العنوان للاتصال بخادم الإدارة في جميع الحالات. في حالة الخروج عن المحيط، لن تحتاج فقط إلى استخدام عنوان مختلف (عنوان بوابة الاتصال)، ولكن سيتطلب منك أيضًا استخدام وضع اتصال مختلف: من خلال بوابة الاتصال.
- كما يتطلب منك تحديد إعدادات اتصال مختلفة لأجهزة الكمبيوتر المحمولة في مواقع مختلفة.

لإضافة بوابة اتصال إلى شبكة تم تكوينها مسبقًا:

1. قم بتثبيت عميل الشبكة في وضع بوابة الاتصال.

2. أعد تثبيت عميل الشبكة على الأجهزة التي تريد توصيلها ببوابة الاتصال المضافة حديثًا.

خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت

هناك طريقة أخرى وهي تثبيت خادم إدارة واحد في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

هذا التكوين أقل أمانًا من الطريقة الأخرى. لإدارة أجهزة الكمبيوتر المحمولة الخارجية في هذه الحالة، يجب أن يقبل خادم الإدارة الاتصالات من أي عنوان على الإنترنت. سيستمر في إدارة جميع الأجهزة ضمن الشبكة الداخلية، لكن من منطقة الأجهزة الموصلة مباشرة بالإنترنت. لذا، قد يتسبب الخادم الذي تم اختراقه في إحداث قدر هائل من الضرر، على الرغم من انخفاض احتمالية وقوع مثل هذا الحدث.

ينخفض الخطر بشكل ملحوظ إذا كان خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت لا يدير الأجهزة ضمن الشبكة الداخلية. يمكن لمزود الخدمة استخدام هذا التكوين، على سبيل المثال، لإدارة أجهزة العملاء.

قد ترغب في استخدام هذه الطريقة في الحالات التالية:

- إذا كنت معتادًا على تثبيت خادم الإدارة وتكوينه ولا ترغب في القيام بإجراء آخر لتثبيت بوابة الاتصال وتكوينها.
- إذا كنت بحاجة إلى إدارة المزيد من الأجهزة. تبلغ السعة القصوى لخادم الإدارة 100 000 جهاز، بينما يمكن لبوابة الاتصال أن تدعم ما يصل إلى 10 000 جهاز.

لهذا الحل أيضًا صعوبات محتملة:

- يتطلب خادم الإدارة توفر المزيد من موارد الأجهزة وقواعد بيانات أخرى.
- سيتم تخزين المعلومات بشأن الأجهزة في قاعدتي بيانات غير مرتبطين بها (بخادم الإدارة الموجود داخل الشبكة وآخر في منطقة الأجهزة الموصلة مباشرة بالإنترنت)، مما يعقد المراقبة.
- لإدارة جميع الأجهزة، يجب ضم خادم الإدارة في شكل تسلسل هرمي، مما يعقد المراقبة وكذلك الإدارة. يفرض مثيل خادم الإدارة الثانوي قيودًا على الهياكل المحتملة لمجموعات الإدارة. عليك أن تقرر طريقة وماهية المهام والسياسات لتوزيعها على مثيل خادم الإدارة الثانوي.
- يعد تكوين الأجهزة الخارجية لاستخدام خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت من الخارج واستخدام خادم الإدارة الرئيسي من الداخل معقدًا أكثر من مجرد تكوينها لاستخدام اتصال مشروط من خلال بوابة.
- مخاطر أمنية عالية. يُعرّض مثيل خادم الإدارة المخترق أجهزة الكمبيوتر المحمولة المدارة للاختراق بسهولة. في حالة حدوث ذلك، يحتاج المخترقون فقط إلى انتظار عودة أحد أجهزة الكمبيوتر المحمولة إلى الاتصال بشبكة المؤسسة حتى يتمكنوا من مواصلة هجومهم على شبكة المنطقة المحلية.

توصيل الأجهزة المكتبية الخارجية بخادم الإدارة

لا يمكن توصيل الأجهزة المكتبية التي دائمًا ما تكون خارج الشبكة الرئيسية (على سبيل المثال، الأجهزة في الفروع الإقليمية للشركة؛ الأكشاك وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ الأجهزة في المكاتب المنزلية للموظفين) بخادم الإدارة مباشرةً. يجب أن تكون متصلة بخادم الإدارة عبر بوابة اتصال مثبتة في منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ). ويتم إجراء هذا التكوين عند تثبيت عميل الشبكة على تلك الأجهزة.

لتوصيل الأجهزة المكتبية الخارجية بخادم الإدارة:

1. قم بإنشاء حزمة تثبيت جديدة لعميل الشبكة.

2. افتح خصائص حزمة التثبيت التي تم إنشاؤها، وانتقل إلى **Advanced** ← **Settings**، ومن ثم حدد الخيار **Connect to Administration Server by using a connection gateway**.

> إعداد **Connect to Administration Server by using a connection gateway** غير متوافق مع إعداد **Use Network Agent as a connection gateway in DMZ**. لا يمكنك تمكين هذين الإعدادين في نفس الوقت.

3. في الحقل **Connection gateway address**، حدد العنوان العام لبوابة الاتصال.

إذا كانت بوابة الاتصال موجودة خلف ترجمة عنوان الشبكة (NAT) وليس لها عنوان عام خاص بها، فقم بتكوين قاعدة بوابة NAT لإعادة توجيه الاتصالات من العنوان العام إلى العنوان الداخلي لبوابة الاتصال.

4. قم بإنشاء حزمة تثبيت مستقلة بناءً على حزمة التثبيت التي تم إنشاؤها.

5. قم بتسليم حزمة التثبيت المستقلة للأجهزة المستهدفة إما إلكترونيًا أو على محرك أقراص قابل للإزالة.

6. قم بتثبيت عميل الشبكة من الحزمة المستقلة.

الأجهزة المكتبية الخارجية متصلة بخادم الإدارة.

حول ملفات التعريف الخاصة باتصال المستخدمين المتواجدين خارج المكتب

قد يحتاج مستخدمو الكمبيوتر المحمول خارج المكتب (يُشار إليهم فيما بعد باسم "الأجهزة") إلى تغيير طريقة الاتصال بخادم الإدارة أو التبديل بين خوادم الإدارة بناءً على الموقع الحالي للجهاز على شبكة المؤسسة.

> إن ملفات تعريف الاتصال مدعومة فقط للأجهزة التي تعمل بنظام Windows و macOS.

استخدام عناوين مختلفة لخادم إدارة واحد

الأجهزة المثبت عليها عميل الشبكة يمكنها الاتصال بخادم الإدارة إما من إنترانت المؤسسة أو من الإنترنت. قد يتطلب هذا الموقف من عميل الشبكة استخدام عناوين مختلفة للاتصال بخادم الإدارة: عنوان خادم الإدارة الخارجي للاتصال بالإنترنت وعنوان خادم الإدارة الداخلي للاتصال بالشبكة الداخلية.

لفعل ذلك، أضف ملف تعريف للاتصال بخادم الإدارة من الإنترنت في خصائص سياسة عميل الشبكة (في القسم **Application settings** ← **Administration Server connection profiles** ← **Connection profiles** ← **Connectivity**). في نافذة إنشاء ملف التعريف، عليك تعطيل خيار **Use to receive updates only**، وتأكد من تحديد خيار **Synchronize connection settings with the Administration Server settings specified in this profile**. إذا كنت تستخدم بوابة اتصال للوصول إلى خادم الإدارة (على سبيل المثال تكوين Kaspersky Security Center كما هو موضح في الوصول إلى الإنترنت: عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت)، فيجب عليك تحديد عنوان بوابة الاتصال في الحقل المقابل لملف تعريف الاتصال.

التبديل بين خوادم الإدارة بناءً على الشبكة الحالية

إذا كان للمؤسسة مكاتب متعددة بها خوادم إدارة مختلفة وتنتقل بعض الأجهزة المثبّت عليها عميل الشبكة فيما بينها، فأنت تحتاج لتوصيل عميل الشبكة بخادم الإدارة الخاص بالشبكة المحلية في المكتب الذي يوجد به الجهاز حاليًا.

في هذه الحالة، يجب إنشاء ملف تعريف للاتصال بخادم الإدارة في خصائص سياسة عميل الشبكة لكل مكتب من المكاتب باستثناء المكتب الرئيسي الذي يوجد به خادم الإدارة الرئيسي. حدد عناوين خوادم الإدارة في ملفات تعريف الاتصال ومن ثم قم بتمكين أو تعطيل خيار **Use to receive updates only**:

- حدد الخيار إذا كنت تريد مزامنة عميل الشبكة باستخدام خادم الإدارة الرئيسي، بينما تستخدم الخادم المحلي لتنزيل التحديثات فقط.
- قم تعطيل هذا الخيار إذا كان يلزم إدارة عميل الشبكة بالكامل بواسطة خادم الإدارة المحلي.

بعد ذلك، يجب عليك إعداد شروط التحويل إلى ملفات التعريف التي تم إنشاؤها حديثًا: على الأقل شرط واحد لكل مكتب من المكاتب، ما عدا المكتب الرئيسي. يتكون غرض كل شرط من الشروط من الكشف عن العناصر الخاصة لبيئة شبكة مكتب ما. إذا تحقق شرط ما، يتم تنشيط ملف التعريف المقابل له. إن لم يتحقق شرط من الشروط، يتم تبديل عميل الشبكة إلى خادم الإدارة الرئيسي.

إنشاء ملف تعريف خاص باتصال المستخدمين المتواجدين خارج المكتب

يتوفر ملف تعريف اتصال خادم الإدارة فقط على الأجهزة التي تعمل بنظام Windows و macOS.

لإنشاء ملف تعريف لاتصال عميل الشبكة بخادم الإدارة للمستخدمين خارج المكتب:

1. إذا أردت إنشاء ملف تعريف اتصال لمجموعة أجهزة مدارة، فافتح سياسة عميل الشبكة لهذه المجموعة. للقيام بذلك، عليك القيام بالإجراءات التالية:
   a. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
   b. انقر على رابط المسار الحالي.
   c. في النافذة التي تفتح، حدد مجموعة الإدارة المطلوبة.
      بعد ذلك، يتم تغيير المسار الحالي.
   d. أضف سياسة عميل الشبكة لمجموعة الأجهزة المدارة. إذا كنت قد قمت بإنشائه بالفعل، فانقر فوق اسم سياسة عميل الشبكة لفتح خصائص السياسة.
2. إذا كنت تريد إنشاء ملف تعريف اتصال لجهاز مُدار معين، فقم بما يلي:
   a. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.
   b. انقر على اسم الجهاز المُدار.
   c. في نافذة خصائص الجهاز المُدار التي تفتح، انتقل إلى علامة التبويب **Applications**.
   d. انقر فوق اسم سياسة عميل الشبكة التي تنطبق على الجهاز المُدار المُحدد.
3. في نافذة الخصائص التي تفتح، انتقل إلى **Application settings** ← **Connectivity** ← **Connection profiles**.
4. من القسم **Administration Server connection profiles**، انقر فوق الزر **Add**.

بشكل افتراضي، قائمة ملفات تعريف الاتصال تحتوي على ملفات تعريف <وضع غير متصل> و<خادم الإدارة الرئيسي>. لا يمكن تعديل ملفات التعريف أو إزالتها.

لا يحدد <Offline mode> أي خادم للاتصال. لذلك، لا يحاول عميل الشبكة، عند الانتقال إلى ملف التعريف ذاك، الاتصال بأي خادم إدارة بينما تعمل التطبيقات المثبتة على الأجهزة العميلة بموجب سياسات خارج المكتب. يمكن استخدام ملف تعريف <وضع غير متصل> في حالة فصل الأجهزة عن الشبكة.

يحدد ملف التعريف <Home Administration Server> الاتصال بخادم الإدارة الذي تم تحديده أثناء تثبيت عميل الشبكة. يتم تطبيق ملف تعريف <خادم الإدارة الرئيسي > عند إعادة اتصال الجهاز بخادم الإدارة الرئيسي بعد تشغيله في شبكة خارجية لبعض الوقت.

5. من النافذة **Configure profile** التي تفتح، قم بتكوين ملف تعريف الاتصال:

- **Profile name**

  يمكنك من خلال حقل الإدخال عرض اسم ملف تعريف الاتصال وتغييره.

- **Administration Server address**

  عنوان خادم الإدارة الذي يجب توصيل الجهاز العميل به أثناء تفعيل ملف التعريف.

- **Port number**

  رقم المنفذ المستخدم في الاتصال.

- **SSL port**

  رقم المنفذ الخاص بالاتصال في حالة استخدام بروتوكول SSL.

- **Use SSL connection**

  في حال تمكين هذا الخيار، يتم تأسيس الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL.

  يتم تمكين هذا الخيار افتراضيًا. نوصي بعدم تعطيل هذا الخيار حتى يظل اتصالك آمنًا.

- حدد خيار **Use proxy server** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. إذا تم تحديد هذا الخيار، ستتوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

  - **Address**

    عنوان الخادم الوكيل المستخدم لاتصال Kaspersky Security Center بالإنترنت.

  - **Port number**

    رقم المنفذ الذي سيتم من خلاله إنشاء اتصال وكيل Kaspersky Security Center.

  - **Proxy server authentication**

    إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

  - **User name**

    حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة اختيار **Proxy server authentication**).

  - **Password**

    تم تعيين كلمة مرور بواسطة المستخدم الذي تم إنشاء اتصال الخادم الوكيل من خلال حسابه (هذا الحقل متاح في حالة تحديد خانة اختيار **Proxy server authentication**).

    لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **Show** حتى تظهر لك كلمة المرور.

- **Connection gateway address**

  عنوان البوابة التي من خلالها يتم اتصال الأجهزة العميلة بخادم الإدارة.

- **Enable out-of-office mode when Administration Server is not available**

  حدد خانة الاختيار هذه للسماح للتطبيقات المثبتة على جهاز عميل باستخدام ملفات تعريف السياسة للأجهزة في وضع الوجود خارج المكتب، بالإضافة إلى سياسات خارج المكتب، عند أي محاولة للاتصال عندما لا يكون خادم الإدارة متاحًا. في حالة عدم تحديد سياسة الوجود خارج المكتب للتطبيق، سيتم استخدام السياسة المفعلة.

في حال تعطيل هذا الخيار، ستستخدم التطبيقات السياسات المفعلة.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **الاستخدام لاستلام التحديثات فقط**

في حال تمكين هذا الخيار، سيتم استخدام ملف التعريف فقط لتنزيل التحديثات بواسطة التطبيقات المثبتة على الجهاز العميل. بالنسبة للعمليات الأخرى، سيتم إنشاء اتصال بخادم الإدارة باستخدام إعدادات الاتصال الأولية المحددة أثناء تثبيت عميل الشبكة.

يتم تمكين هذا الخيار افتراضيًا.

- **مزامنة إعدادات الاتصال مع إعدادات خادم الإدارة المحددة في ملف التعريف هذا**

في حال تمكين هذا الخيار، سيتصل عميل الشبكة بخادم الإدارة باستخدام الإعدادات المحددة في خصائص ملف التعريف.

في حال تعطيل هذا الخيار، سيتصل عميل الشبكة بخادم الإدارة باستخدام الإعدادات الأصلية المحددة أثناء التثبيت.

يتوفر هذا الخيار في حال تعطيل خيار **الاستخدام لاستلام التحديثات فقط**.

يتم تعطيل هذا الخيار افتراضيًا.

تم إنشاء ملف تعريف لاتصال عميل الشبكة بخادم الإدارة للمستخدمين خارج المكتب. عندما يتصل عميل الشبكة بخادم الإدارة باستخدام ملف التعريف هذا، فسوف تستخدم التطبيقات المثبتة على الأجهزة العميلة سياسات مخصصة للأجهزة في وضع الوجود خارج المكتب، أو سياسات خارج المكتب.

حول تبديل عميل الشبكة إلى خوادم إدارة أخرى

يوفر Kaspersky Security Center خيار نقل عميل الشبكة على الجهاز العميل إلى خوادم الإدارة الأخرى في حالة تغيير إعدادات الشبكة التالية:

- **Condition for DHCP server address**—تم تغيير عنوان IP الخاص بخادم بروتوكول تكوين المضيف الديناميكي (DHCP) الخاص بالشبكة.
- **Condition for default connection gateway address**—تم تغيير عنوان بوابة الشبكة الرئيسية.
- **Condition for DNS domain**—تم تغيير لاحقة DNS للشبكة الفرعية.
- **Condition for DNS server address**—تم تغيير عنوان IP الخاص بخادم DNS للشبكة.
- **Condition for WINS server address**—تم تغيير عنوان IP الخاص بخادم WINS للشبكة. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.
- **Condition for name resolvability**-تم تغيير اسم DNS أو NetBIOS للجهاز العميل.
- **Condition for subnet**— تغيير عنوان الشبكة الفرعية والقناع.
- **Condition for Windows domain accessibility**— تغيير حالة مجال Windows الذي يتصل به الجهاز العميل. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.
- **Condition for SSL connection address accessibility** - يستطيع الجهاز العميل أو لا يستطيع (اعتمادًا على الخيار الذي تحدده) إنشاء اتصال SSL بخادم محدد (الاسم:المنفذ). يجب أن تستخدم خادمًا مخصصًا يحتوي على برنامج قادر على التعامل مع الحمل العالي وطلبات عميل الشبكة المتكررة للاتصال. لا تحدد منفذ خادم الإدارة. لكل خادم، يمكنك أيضًا تحديد شهادة SSL. في هذه الحالة، يتحقق وكيل الشبكة من شهادة الخادم بالإضافة إلى التحقق من إمكانية اتصال SSL. إذا لم تتطابق الشهادة، فسيفشل الاتصال.

هذه الميزة مدعومة فقط لوكلاء الشبكة المثبتين على الأجهزة التي تعمل بنظام Windows أو macOS.

يتم تحديد الإعدادات الأولية لاتصال عميل الشبكة بالخادم عند تثبيت عميل الشبكة. وبعد ذلك، في حالة إنشاء قواعد لتبديل عميل الشبكة إلى خوادم إدارة أخرى، سيستجيب عميل الشبكة للتغييرات في إعدادات الشبكة كما يلي:

- إذا كانت إعدادات الشبكة تتوافق مع أي من القواعد التي تم إنشاؤها، فيتم اتصال عميل الشبكة بخادم الإدارة المحدد في هذه القاعدة. تتحول التطبيقات المثبتة على الأجهزة العميلة إلى سياسات خارج المكتب، شريطة أن يتم تمكين هذا السلوك بواسطة قاعدة.
- في حالة عدم تطبيق أي من القواعد، يعود عميل الشبكة إلى الإعدادات الافتراضية للاتصال بخادم الإدارة المحددة أثناء التثبيت. تعود التطبيقات المثبتة على الأجهزة العميلة إلى السياسات المفعلة.
- في حالة تعذر الوصول إلى خادم الإدارة، يستخدم عميل الشبكة سياسات خارج المكتب.

ينتقل Network Agent إلى سياسة الوجود خارج المكتب فقط إذ تم تمكين الخيار **Enable out-of-office mode when Administration Server is not available** في إعدادات سياسة Network Agent.

يتم حفظ إعدادات اتصال عميل الشبكة بخادم الإدارة في ملف تعريف الاتصال. في ملف تعريف الاتصال، يمكنك إنشاء قواعد لتبديل الأجهزة العميلة إلى سياسات خارج المكتب ويمكنك تكوين ملف التعريف كي يستخدم فقط لتنزيل التحديثات.

إنشاء قاعدة تبديل عميل شبكة حسب موقع الشبكة

لا يكون تبديل عميل الشبكة حسب موقع الشبكة متاحًا إلا على الأجهزة التي تعمل بنظام Windows وmacOS.

لإنشاء قاعدة لتبديل عميل الشبكة من خادم إدارة إلى آخر في حالة تغيير إعدادات الشبكة:

1. إذا أردت إنشاء قاعدة لمجموعة أجهزة مدارة، فافتح سياسة عميل الشبكة لهذه المجموعة. للقيام بذلك، عليك القيام بالإجراءات التالية:
   a. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
   b. انقر على رابط المسار الحالي.
   c. في النافذة التي تفتح، حدد مجموعة الإدارة المطلوبة.
   بعد ذلك، يتم تغيير المسار الحالي.
   d. أضف سياسة عميل الشبكة لمجموعة الأجهزة المدارة. إذا كنت قد قمت بإنشائه بالفعل، فانقر فوق اسم سياسة عميل الشبكة لفتح خصائص السياسة.
2. إذا كنت تريد إنشاء قاعدة لجهاز مُدار معين، فقم بما يلي:
   a. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.
   b. انقر على اسم الجهاز المُدار.
   c. في نافذة خصائص الجهاز المُدار التي تفتح، انتقل إلى علامة التبويب **Applications**.
   d. انقر فوق اسم سياسة عميل الشبكة التي تنطبق على الجهاز المُدار المُحدد.
3. في نافذة الخصائص التي تفتح، انتقل إلى **Application settings** ← **Connectivity** ← **Connection profiles**.
4. في القسم **Network location settings**، انقر على زر **Add**.

5. في نافذة الخصائص التي تفتح، قم بتكوين وصف موقع الشبكة وقاعدة التبديل. حدد إعدادات وصف موقع الشبكة التالية:

- **Description**

لا يمكن أن يكون اسم وصف موقع الشبكة أطول من 255 حرف أو يحتوي على رموز خاصة، مثل ("*<>?\/:|).

- **Use connection profile**

يمكنك تحديد ملف تعريف الاتصال الذي يستخدمه عميل الشبكة للاتصال بخادم الإدارة من خلال القائمة المنسدلة. سيستخدم ملف التعريف هذا عند استيفاء شروط وصف موقع الشبكة. يحتوي ملف تعريف الاتصال على إعدادات اتصال عميل الشبكة بخادم الإدارة؛ كما يحدد متى يجب أن تتحول الأجهزة العميلة إلى سياسات خارج المكتب. يتم استخدام ملف التعريف لتنزيل التحديثات فقط.

- **Description enabled**

حدد خانة الاختيار هذه لتمكين استخدام وصف موقع الشبكة الجديد.

6. حدد شروط قاعدة تبديل عميل الشبكة:

- **Condition for DHCP server address**—تم تغيير عنوان IP الخاص بخادم بروتوكول تكوين المضيف الديناميكي (DHCP) الخاص بالشبكة.
- **Condition for default connection gateway address**—تم تغيير عنوان بوابة الشبكة الرئيسية.
- **Condition for DNS domain**—تم تغيير لاحقة DNS للشبكة الفرعية.
- **Condition for DNS server address**—تم تغيير عنوان IP الخاص بخادم DNS للشبكة.
- **Condition for WINS server address**—تم تغيير عنوان IP الخاص بخادم WINS للشبكة. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.
- **Condition for name resolvability**-تم تغيير اسم DNS أو NetBIOS للجهاز العميل.
- **Condition for subnet**— تغيير عنوان الشبكة الفرعية والقناع.
- **Condition for Windows domain accessibility**— تغيير حالة مجال Windows الذي يتصل به الجهاز العميل. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.
- **Condition for SSL connection address accessibility** —يمكن للجهاز العميل أو لا يمكنه (اعتمادًا على الخيار الذي تحدده) إنشاء اتصال SSL بخادم محدد (الاسم:المنفذ). لكل خادم، يمكنك أيضًا تحديد شهادة SSL. في هذه الحالة، يتحقق عميل الشبكة من شهادة الخادم بالإضافة إلى التحقق من إمكانية اتصال SSL. إذا لم تتطابق الشهادة، فسيفشل الاتصال.

> يتم تجميع شروط القاعدة باستخدام عامل التشغيل المنطقي AND. لتشغيل قاعدة التبديل حسب وصف موقع الشبكة، يجب استيفاء شروطها.

7. في قسم الشروط، حدد متى يجب تبديل عميل الشبكة إلى خادم إدارة آخر. لهذا الغرض، انقر فوق الزر "**Add**"، ومن ثم قم بتعيين قيمة الشرط.

كما يجب تمكين الخيار **Matches at least one value from the list** بشكل افتراضي. يمكنك تعطيل هذا الخيار إذا كنت تريد أن يتحقق الشرط مع جميع القيم المحددة.

8. احفظ تغييراتك.

يتم إنشاء قاعدة تبديل جديدة حسب وصف موقع الشبكة، في أي وقت يتم استيفاء شروطها يستخدم عميل الشبكة ملف تعريف الاتصال المحدد في القاعدة للاتصال بخادم الإدارة.

معالج نشر الحماية

للتثبيت تطبيقات Kaspersky، يمكنك استخدام معالج نشر الحماية. يسمح لك معالج نشر الحماية بتثبيت للتطبيقات عن بُعد من خلال حزم التثبيت التي تم إنشاؤها بشكل خاص أو من خلال حزمة التوزيع بشكل مباشر.

يقوم معالج نشر الحماية بتنفيذ الإجراءات التالية:

- تنزيل حزمة تثبيت لتثبيت التطبيق (إذا لم يتم الإنشاء مسبقًا). توجد حزمة التثبيت في **Discovery & deployment ← Deployment & assignment ← Installation packages**. يمكنك استخدام حزمة التثبيت هذه لتثبيت التطبيق في المستقبل.
- تقوم بإنشاء مهمة التثبيت عن بُعد وتشغيلها لأجهزة محددة أو لإحدى مجموعات الإدارة. يتم وضع مهام التثبيت عن بُعد المنشأة حديثًا في قسم **Tasks**. يمكنك بدء هذه المهمة يدويًا لاحقًا. نوع المهمة هو **Install application remotely**.

إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تعمل بنظام التشغيل SUSE Linux Enterprise Server 15، فثبت أول حزمة insserv-Compatible لتكوين عميل الشبكة.

الخطوة 1. بدء معالج نشر الحماية

لبدء معالج نشر الحماية يدويًا،

في القائمة الرئيسية، انتقل إلى **Discovery & deployment ← Deployment & assignment ← Protection deployment wizard**.

سيبدأ معالج نشر الحماية. انتقل عبر المعالج باستخدام زر **Next**.

الخطوة 2. تحديد حزمة التثبيت

حدد حزمة التثبيت للتطبيق الذي ترغب في تثبيته.

إذا لم تكن حزمة التثبيت للتطبيق المطلوب مدرجة، انقر على زر **Add** ثم حدد التطبيق من القائمة.

الخطوة 3. تحديد طريقة لتوزيع ملف المفتاح أو رمز التنشيط

حدد طريقة لتوزيع ملف المفتاح أو رمز التفعيل:

- **Do not add license key to installation package**

  يتم توزيع المفتاح تلقائيًا على كافة الأجهزة التي يتوافق معها:

  - في حالة تمكين التوزيع التلقائي في خصائص المفتاح
  - إذا تم إنشاء مهمة **إضافة مفتاح**.

- **Add license key to installation package**

يتم توزيع المفتاح على الأجهزة بالإضافة إلى حزمة التثبيت.

> لا نوصي بقيامك بتوزيع المفتاح باستخدام هذه الطريقة؛ لأن حقوق الوصول للقراءة المشتركة ممكّنة لمستودع حزم التثبيت.

إذا كانت حزمة التثبيت تحتوي على ملف مفتاح أو رمز تفعيل بالفعل، فستظهر النافذة لكن لن تحتوي إلا على معلومات مفتاح الترخيص.

الخطوة 4. تحديد إصدار عميل الشبكة

إذا حددت حزمة تثبيت تطبيق غير عميل الشبكة، عليك كذلك تثبيت عميل الشبكة الذي سيوصل التطبيق بخادم إدارة Kaspersky Security Center.

حدد أحدث إصدار لعميل الشبكة.

الخطوة 5. تحديد الأجهزة

حدد قائمة بالأجهزة التي سيتم تثبيت التطبيق عليها:

- **Install on managed devices**

إذا تم تحديد هذا الخيار، فسوف يتم إنشاء مهمة التثبيت عن بُعد لمجموعة أجهزة.

- **Select devices for installation**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

الخطوة 6. تحديد إعدادات مهمة التثبيت عن بُعد

في صفحة **Remote installation task settings**، حدد إعدادات تثبيت التطبيق عن بُعد.

في مجموعة الإعدادات **Force installation package download**، حدد كيفية توزيع الملفات المطلوبة لتثبيت التطبيق على الأجهزة العميلة:

- **Using Network Agent**

إذا كان هذا الخيار مفعلاً، سيتم تسليم حزم التثبيت إلى الأجهزة العميلة بواسطة عميل الشبكة المثبت على الأجهزة العميلة هذه.

في حالة تعطيل هذا الخيار، يتم تسليم حزم التثبيت باستخدام أدوات نظام التشغيل للأجهزة العميلة.

ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة.

يتم تمكين هذا الخيار افتراضيًا.

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

إذا تم تفعيل هذا الخيار، سيتم نقل حزم التثبيت إلى الأجهزة العميلة باستخدام أدوات نظام التشغيل من خلال نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت توجد نقطة توزيع واحدة على الأقل في الشبكة.

في حالة تفعيل هذا الخيار **استخدام عميل الشبكة**، يتم تسليم الملفات بواسطة أدوات نظام التشغيل فقط في حالة عدم توفر موارد عميل الشبكة.

يتم تفعيل هذا الخيار افتراضيًا لمهام التثبيت عن بُعد التي تم إنشاؤها على خادم إدارة افتراضي.

عندما تكون جميع نقاط التوزيع المخصصة للجهاز معطلة، فلن يتمكن الجهاز من تلقي التحديثات (قواعد بيانات مكافحة الفيروسات والتصحيحات) وحزم التثبيت.

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

إذا تم تمكين هذا الخيار، يتم نقل الملفات إلى أجهزة العميل باستخدام أدوات نظام التشغيل لأجهزة العميل من خلال خادم الإدارة. يمكنك تفعيل هذا الخيار إذا لم يتم تثبيت عميل شبكة على الجهاز العميل، لكن الجهاز العميل موجود في نفس الشبكة الموجود عليها خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

حدد الإعدادات الإضافية:

- **Do not re-install application if it is already installed**

إذا تم تفعيل هذا الخيار، لن يتم عادة تثبيت التطبيق المحدد إذا كان مثبتًا بالفعل على الجهاز العميل هذا.

إذا تم تفعيل هذا الخيار، سيتم تثبيت التطبيق بأية حال.

يتم تمكين هذا الخيار افتراضيًا.

- **Assign package installation in Active Directory group policies**

في حال تمكين هذا الخيار، سيتم تثبيت حزمة التثبيت باستخدام سياسات مجموعة Active Directory.

يتوفر هذا الخيار فقط إذا تم تحديد حزمة تثبيت عميل الشبكة.

يتم تعطيل هذا الخيار افتراضيًا.

الخطوة 7. إدارة إعادة التشغيل

حدد الإجراء الذي يجب إتمامه إذا كان يجب إعادة تشغيل نظام التشغيل عند تثبيتك للتطبيق:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **Force closure of applications in blocked sessions**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

الخطوة 8. إزالة التطبيقات غير المتوافقة قبل التثبيت

لا تظهر هذه الخطوة إلا إذا كان التطبيق الذي تنشره معروفًا بعدم توافقه مع بعض التطبيقات الأخرى.

حدد الخيار إذا كنت ترغب في أن يقوم Kaspersky Security Center بإزالة التطبيقات غير المتوافقة مع التطبيق الذي تنشره بشكل تلقائي.

يتم عرض كذلك قائمة التطبيقات غير المتوافقة.

إذا لم تحدد هذا الخيار، لن يتم تثبيت التطبيق إلا على الأجهزة التي لا يوجد عليها تطبيقات غير متوافقة.

الخطوة 9. نقل الأجهزة إلى الأجهزة المُدارة

حدد إذا ما كان يجب نقل الأجهزة إلى مجموعة إدارة بعد تثبيت عميل الشبكة أم لا.

- **Do not move devices**

تبقى الأجهزة في المجموعات الموجودة فيها حاليًا. والأجهزة التي لم يتم وضعها في مجموعة تبقى دون تخصيص.

- **Move unassigned devices to group**

يتم نقل الأجهزة إلى مجموعة الإدارة التي تحددها.

يتم تحديد خيار **Do not move devices** بصورة افتراضية. ولأسباب أمنية، قد ترغب في نقل الأجهزة يدويًا.

الخطوة 10. تحديد الحسابات للوصول إلى الأجهزة

أضف الحسابات التي سيتم استخدامها لبدء مهمة التثبيت عن بُعد:

- **No account required (Network Agent installed)**

إذا تم تحديد هذا الخيار، فلا يلزم تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

إذا لم يتم تثبيت عميل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

- **Account required (Network Agent is not used)**

حدد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على الأجهزة التي قمت بتعيين مهمة التثبيت عن بُعد لها. في هذه الحالة، يمكنك تحديد حساب مستخدم أو شهادة SSH لتثبيت التطبيق.

- **Local Account**. إذا تم تحديد هذا الخيار، فحدد الحساب المستخدم الذي سيتم من خلاله تشغيل مثبت التطبيق. انقر على الزر **إضافة**، وحدد **Local Account**، ثم حدد بيانات اعتماد حساب المستخدم.

  يمكنك تحديد عدة حسابات مستخدمين، على سبيل المثال، إذا لم يكن لدى أي منهم جميع الحقوق المطلوبة على جميع الأجهزة التي قمت بتعيين المهمة لها. في هذه الحالة، يتم استخدام جميع الحسابات المضافة لتشغيل المهمة، بترتيب متتالٍ، من أعلى إلى أسفل.

- **شهادة SSH**. إذا كنت ترغب في تثبيت تطبيق على جهاز عميل يستند إلى Linux ، فيمكنك تحديد شهادة SSH بدلاً من حساب المستخدم. انقر على زر **إضافة**، وحدد **شهادة SSH**، ثم حدد المفاتيح الخاصة والعامة للشهادة.

  لإنشاء مفتاح خاص، يمكنك استخدام الأداة المساعدة ssh-keygen. لاحظ أن Kaspersky Security Center يدعم تنسيق PEM للمفاتيح الخاصة، لكن الأداة المساعدة ssh-keygen تنشئ مفاتيح SSH بتنسيق OPENSSH افتراضيًا. تنسيق OPENSSH غير مدعوم من قبل Kaspersky Security Center. ولإنشاء مفتاح خاص بتنسيق PEM المدعوم، أضف الخيار -m PEM في الأمر ssh-keygen. فمثلاً:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<البريد الالكتروني للمستخدم>"
```

الخطوة 11. بدء التثبيت

هذه الصفحة هي الخطوة الأخيرة من المعالج. في هذه الخطوة، تم إنشاء **Remote installation task** وتكوينه بنجاح.

يكون خيار **Run the task after the wizard finishes** غير محدد بصورة افتراضية. إذا حددت هذا الخيار ، فستبدأ **Remote installation task** فورًا بعد إكمال المعالج. إذا لم تحدد هذا الخيار، لن يبدأ **Remote installation task**. يمكنك بدء هذه المهمة يدويًا لاحقًا.

انقر على **OK** لإكمال الخطوة الأخيرة من معالج نشر الحماية.

نشر تطبيقات Kaspersky من خلال Kaspersky Security Center Web Console

يصف هذا القسم تشغيل تطبيقات Kaspersky على أجهزة العميل في مؤسستك من خلال Kaspersky Security Center Web Console.

السيناريو: نشر تطبيقات Kaspersky من خلال Kaspersky Security Center Web Console

يشرح هذا السيناريو كيفية تشغيل تطبيقات Kaspersky من خلال Kaspersky Security Center Web Console. يمكنك استخدام معالج البدء السريع ومعالج نشر الحماية، أو يمكنك إكمال جميع الخطوات الضرورية يدويًا.

تتوافر التطبيقات التالية للنشر باستخدام Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

المراحل

يتقدم نشر تطبيقات Kaspersky في مراحل:

1. **تنزيل مكون الإدارة الإضافي للتطبيق**

هذه المرحلة جزء من معالج البدء السريع. إذا اخترت عدم تشغيل المعالج، قم بتنزيل المكون الإضافي لتطبيق Kaspersky Endpoint Security for Windows يدويًا.

إذا كنت تخطط لإدارة الأجهزة المحمولة الخاصة بالشركة، فاتبع الإرشادات الواردة في تعليمات Kaspersky Security for Mobile لتنزيل مكونات الإدارة الإضافية وتثبيتها لتطبيق Kaspersky Endpoint Security for Android.

2. **تنزيل وإنشاء حزم التثبيت**

هذه المرحلة جزء من معالج البدء السريع.

يتيح لك معالج البدء السريع تنزيل حزمة التثبيت مع مكون الإدارة الإضافي. إذا لم تحدد هذا الخيار عند تشغيل المعالج أو إذا لم تشغل المعالج من الأساس، يجب أن تقوم بتنزيل الحزمة يدويًا.

إذا كنت غير قادر على تثبيت تطبيقات Kaspersky عن طريق Kaspersky Security Center على بعض الأجهزة، مثل أجهزة الموظفين البعيدة، يمكنك إنشاء حزم تثبيت مستقلة للتطبيقات. إذا كنت تستخدم حزمًا مستقلة لتثبيت تطبيقات Kaspersky، فلن تضطر إلى إنشاء مهمة تثبيت عن بُعد وتشغيلها، ولا إنشاء مهام وتكوينها لتطبيق Kaspersky Endpoint Security for Windows.

3. **إنشاء مهمة التثبيت عن بُعد وتكوينها وتشغيلها**

بالنسبة لتطبيق Kaspersky Endpoint Security for Windows، هذه المرحلة جزء من معالج نشر الحماية الذي يبدأ تلقائيًا بعد انتهاء معالج البدء السريع. إذا اخترت عدم تشغيل معالج نشر الحماية، يجب أن تقوم بإنشاء هذه المهمة يدويًا وتكوينها يدويًا.

يمكنك أن تقوم كذلك بإنشاء عدة مهام تثبيت عن بُعد يدويًا لمجموعات إدارة مختلفة أو تحديدات أجهزة مختلفة. يمكنك نشر إصدارات مختلفة من تطبيق واحد في هذه المهام.

تأكد أن جميع الأجهزة على شبكتك مكتشفة ثم قم بتشغيل مهمة (أو مهام) التثبيت عن بُعد.

قم بتثبيت الأداة المساعدة nmap على الأصول المستندة إلى Linux. وهذه الأداة المساعدة مطلوبة لتمكين وظيفة Network Location Awareness.

إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تعمل بنظام التشغيل SUSE Linux Enterprise Server 15، فثبت أول حزمة insserv-Compatible لتكوين عميل الشبكة.

إذا كنت ترغب في تثبيت عميل الشبكة على الأجهزة التي تستخدم نظام التشغيل RED OS 7.3.4 أو أحدث أو MSVSPHERE 9.2 أو أحدث، فقم بتثبيت حزمة libxcrypt-compat لكي يعمل عميل الشبكة بشكل صحيح.

4. **إنشاء وتكوين المهام للتطبيق المُدار**

يجب تكوين مهمة تثبيت التحديث لتطبيق Kaspersky Endpoint Security for Windows.

هذه المرحلة جزء من معالج البدء السريع: يتم إنشاء المهمة وتكوينها تلقائيًا بالإعدادات الافتراضية. إذا اخترت عدم تشغيل المعالج، يجب أن تقوم بإنشاء هذه المهمة يدويًا وتكوينها يدويًا. إذا كنت تستخدم معالج البدء السريع، فتأكد من أن الجدول الزمني للمهمة يلبي متطلباتك. (بشكل افتراضي، يتم تعيين البدء المجدول للمهمة **يدويًا**، ولكن قد ترغب في اختيار خيار آخر.)

يمكن أن يكون لتطبيقات Kaspersky الأخرى مهام افتراضية أخرى. يُرجى الرجوع إلى وثائق التطبيقات المقابلة للمزيد من التفاصيل.

تأكد أن جدول كل مهمة تقوم بإنشائها يفي بمتطلباتك.

5 **تثبيت Kaspersky Security للجوال (اختياري)**

إذا كنت تخطط لإدارة الأجهزة المحمولة الخاصة بالشركة، فاتبع الإرشادات الواردة في تعليمات Kaspersky Security for Mobile للحصول على معلومات عن نشر Kaspersky Endpoint Security for Android.

6 **إنشاء السياسات**

أنشئ السياسة لكل تطبيق يدويًا أو من خلال معالج البدء السريع (مع تطبيق Kaspersky Endpoint Security for Windows). يمكنك استخدام الإعدادات الافتراضية للسياسة، كما يمكنك كذلك تعديل الإعدادات الافتراضية للسياسة وفق احتياجاتك في أي وقت.

7 **تأكيد النتائج**

تأكد أن النشر قد اكتمل بنجاح: بهذا يكون لديك سياسات كل تطبيق ومهامه، وهذه التطبيقات مثبتة على الأجهزة المُدارة.

النتائج

ينتج عن إكمال السيناريو ما يلي:

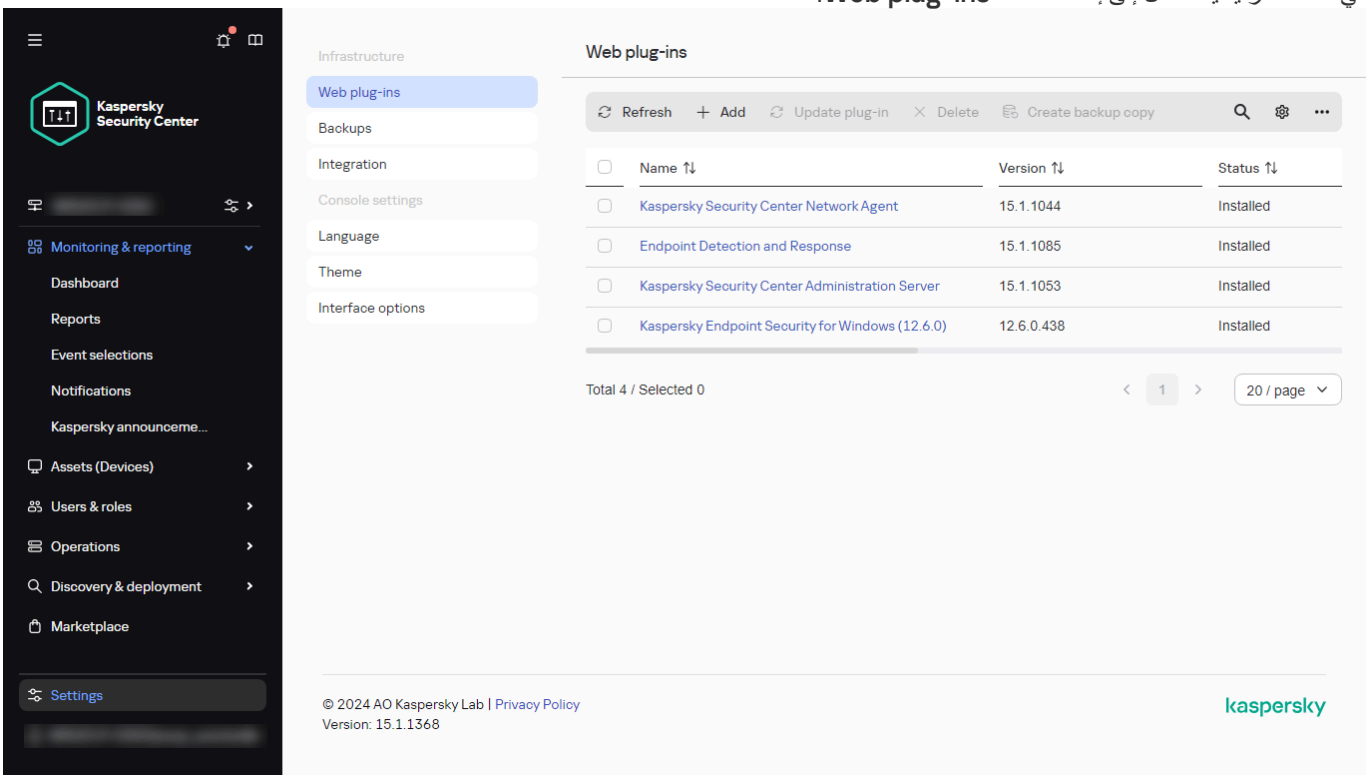
- جميع السياسات والمهام المطلوبة للتطبيقات المحددة تم إنشاؤها.
- جداول المهام مكونة وفق احتياجاتك.
- التطبيقات المحددة منتشرة أو مجدول نشرها على أجهزة العميل المحددة.

الحصول على المكونات الإضافية لتطبيقات Kaspersky

لنشر تطبيق Kaspersky مثل Kaspersky Endpoint Security for Windows، يجب أن تقوم بتنزيل مكون الإدارة الإضافي للتطبيق.

تنزيل مكون إدارة إضافي لتطبيق Kaspersky:

1. في القائمة الرئيسية، انتقل إلى **إعدادات** ← **Web plug-ins**.



قائمة المكونات الإضافية للويب المثبتة

2. في النافذة التي تفتح، انقر على زر **Add**.

   يتم عرض قائمة بالمكونات الإضافية المتاحة.

3. في قائمة المكونات الإضافية المتاحة، حدد المكون الإضافي الذي ترغب في تنزيله (مثل Kaspersky Endpoint Security 11 for Windows) بالنقر على اسمه.

   سيتم عرض صفحة بوصف المكون الإضافي.

4. في صفحة وصف المكون الإضافي، انقر على **Install plug-in**.

5. عندما يكتمل التثبيت، انقر على **OK**.

   يتم تنزيل المكون الإضافي للإدارة بالتكوين الافتراضي ويتم عرضه في قائمة مكونات الإدارة الإضافية.

يمكنك إضافة المكونات الإضافية وتحديث المكونات الإضافية التي تم تنزيلها من ملف. يمكنك تنزيل المكونات الإضافية للإدارة والمكونات الإضافية لإدارة الويب من صفحة ويب الدعم الفني من Kaspersky.

لتنزيل مكون إضافي من ملف أو تحديثه:

1. في القائمة الرئيسية، انتقل إلى **إعدادات** ← **Web plug-ins**.

2. قم بأحد الإجراءات التالية:

   - انقر فوق **Add from file** لتنزيل مكون إضافي من ملف.
   - انقر فوق **Update from file** لتنزيل تحديث مكون إضافي من ملف.

3. حدد الملف وتوقيع الملف.

4. تنزيل الملفات المحددة.

يتم تنزيل المكون الإضافي للإدارة من الملف وعرضه في قائمة مكونات الإدارة الإضافية.

تنزيل حزم التثبيت وإنشائها لتطبيقات Kaspersky

يمكنك إنشاء حزم تثبيت لتطبيقات Kaspersky من خوادم ويب Kaspersky إذا كان خادم الإدارة يملك حق وصول إلى الإنترنت.

لتنزيل حزمة التثبيت وإنشائها لتطبيق Kaspersky:

1. قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل **Installation packages** ← **Deployment & assignment** ← **Discovery & deployment**.
- في القائمة الرئيسية، انتقل إلى **Installation packages** ← **Repositories** ← **Operations**.

يمكنك كذلك عرض إخطارات عن الحزم الجديدة لتطبيقات Kaspersky في قائمة الإخطارات على الشاشة. في حال وجود إخطارات عن حزمة جديدة، يمكنك النقر على الرابط بجوار الإخطار والتقدم إلى قائمة حزم التثبيت المتاحة.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. انقر على **Add**.

يبدأ معالج الحزمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

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

ستظهر قائمة بحزم التثبيت المتاحة على خوادم ويب Kaspersky. تحتوي القائمة على حزم التثبيت للتطبيقات المتوافقة مع الإصدار الحالي لـ Kaspersky Security Center.

4. انقر على اسم حزمة تثبيت، مثل Kaspersky Endpoint Security for Windows (11.1.0).

ستفتح نافذة بها معلومات عن حزمة التثبيت.

يمكنك تنزيل واستخدام حزمة التثبيت التي تتضمن أدوات تشفير تطبق تشفيرًا قويًا، إذا كانت تتوافق مع القوانين واللوائح المعمول بها. لتنزيل حزمة تثبيت Kaspersky Endpoint Security for Windows صالحة لاحتياجات مؤسستك، راجع تشريعات البلد التي توجد بها أجهزة العملاء الخاصة بمؤسستك.

5. اقرأ المعلومات ثم انقر على زر **Download and create installation package**.

إذا كان لا يمكن تحويل حزمة توزيع إلى حزمة تثبيت، سيظهر زر **Download distribution package** بدلاً من زر **Download and create installation package**.

سيبدأ تنزيل حزمة التثبيت إلى خادم الإدارة. يمكنك كذلك إغلاق نافذة المعالج أو التقدم إلى الخطوة التالية في التعليمات. إذا أغلقت نافذة المعالج، ستستمر عملية التنزيل في وضع الخلفية.

إذا كنت ترغب في تعقب عملية تنزيل حزمة التثبيت:

a. في القائمة الرئيسية، انتقل إلى **In progress** ← **Installation packages** ← **Repositories** ← **Operations ()**.

b. تعقب تقدم العملية في عمود **Download progress** وعمود **Download status** للجدول.

سيتم إضافة حزمة التثبيت إلى القائمة في تبويب **Downloaded** عند اكتمال العملية. في حال توقف عملية التنزيل وتبديل حالة التنزيل إلى **Accept EULA**، انقر على اسم حزمة التثبيت ثم تقدم إلى الخطوة التالية في التعليمات.

ستظهر رسالة خطأ إذا كان حجم البيانات الموجودة في حزمة التوزيع المحددة يتخطى الحد الحالي. يمكنك تغيير قيمة الحد ثم التقدم في إنشاء حزمة التثبيت.

6. يتم عرض زر **Show EULA** أثناء عملية التنزيل لبعض تطبيقات Kaspersky. افعل ما يلي إذا ظهر ذلك الزر:

a. انقر على زر **Show EULA** لقراءة اتفاقية ترخيص المستخدم النهائي.

b. اقرأ اتفاقية ترخيص المستخدم النهائي المعروضة على الشاشة ثم انقر على **Accept**.

يستمر التنزيل بعد أن تقبل اتفاقية ترخيص المستخدم النهائي. سيتوقف التنزيل إذا نقرت على **Decline**.

7. انقر على زر **إغلاق** عندما يكتمل التنزيل.

يتم تنزيل حزمة التثبيت المحددة إلى المجلد المشترك لخادم الإدارة في المجلد الفرعي "الحزم". بعد التنزيل، تظهر حزمة التثبيت في قائمة حزم التثبيت.

تغيير حد حجم بيانات حزمة التثبيت المخصصة

الحجم الإجمالي للبيانات التي تم فك ضغطها أثناء إنشاء حزمة تثبيت مخصصة محدود. الحد الافتراضي هو 1 غيغابايت.

ستظهر لك رسالة خطأ إذا حاولت رفع ملف مضغوط يحتوي على بيانات تتخطى الحد الحالي. قد تضطر إلى زيادة قيمة هذا الحد عند إنشاء حزم تثبيت من حزم توزيع كبيرة.

لتغيير قيمة الحد لحجم حزمة التثبيت المستقلة:

1. على جهاز خادم الإدارة، قم بتشغيل موجه الأوامر ضمن الحساب الذي تم استخدامه تثبيت خادم الإدارة.

2. قم بتغيير دليلك الحالي إلى مجلد تثبيت Kaspersky Security Center (عادةً، Kaspersky\(x86) Program Files\:<Disk> Kaspersky Security Center\Lab).

3. اعتمادًا على نوع تثبيت خادم الإدارة، أدخل أحد الأوامر التالية، باستخدام حقوق المسؤول:

- التثبيت المحلي العادي:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <عدد البايت>
```

- التثبيت على مجموعة تجاوز الفشل من Kaspersky Security Center:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <عدد البايت> --klfoc stp
```

- التثبيت على مجموعة تجاوز الفشل في Windows Server:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <عدد البايت> --stp cluster
```

يعتبر <number of bytes> هو عدد البايتات في تنسيق سداسي عشري أو عشري.

على سبيل المثال، إذا كان الحد المطلوب هو 2 جيغابايت، فيمكنك تحديد القيمة العشرية 2147483648 أو القيمة السداسية العشرية 0x80000000. في هذه الحالة، للتثبيت المحلي لخادم الإدارة، يمكنك استخدام الأمر التالي:

```
klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
```

بهذا يتم تغيير حد حجم بيانات حزمة التثبيت المخصصة.

تنزيل حزم التوزيع لتطبيقات Kaspersky

يمكنك في Kaspersky Security Center Web Console تنزيل حزم توزيع وحفظها لتطبيقات Kaspersky. يمكنك استخدام حزم التوزيع في تثبيت التطبيقات يدويًا دون استخدام Kaspersky Security Center.

لتنزيل حزم توزيع وحفظها لتطبيقات Kaspersky:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات Kaspersky** ← **إصدارات التطبيق الحالية**.

ستفتح قائمة بحزم التوزيع والمكونات الإضافية والتصحيحات. لا يعرض Kaspersky Security Center إلا العناصر المتوافقة مع إصداره الحالي فقط.

2. انقر على اسم الحزمة التي ترغب في تنزيلها من القائمة.

سيفتح وصف الحزمة.

3. اقرأ الوصف ثم انقر على زر **Download and create installation package**.

إذا كان لا يمكن تحويل حزمة توزيع إلى حزمة تثبيت، سيظهر زر **Download distribution package** بدلاً من زر **Download and create installation package**.

سيبدأ تنزيل حزمة التثبيت إلى خادم الإدارة.

يتم تنزيل حزمة التثبيت أو التوزيع المحددة إلى المجلد المشترك لخادم الإدارة في المجلد الفرعي **الحزم**. بعد التنزيل، تظهر حزمة التثبيت في قائمة حزم التثبيت.

التحقق من نشر Kaspersky Endpoint Security بنجاح

للتأكد أنك قد قمت بنشر تطبيقات Kaspersky بشكل صحيح، مثل Kaspersky Endpoint Security:

1. باستخدام Kaspersky Security Center Web Console، تأكد أنه يوجد لديك ما يلي:

- سياسة لـ Kaspersky Endpoint Security و/أو تطبيقات أمان أخرى تستخدمها.
- مهام Kaspersky Endpoint Security for Windows: مهمة فحص سريع ومهمة تثبيت التحديث (إذا كنت تستخدم Kaspersky Endpoint Security for Windows).
- مهام لتطبيقات الأمان الأخرى التي تستخدمها.

2. على أحد الأجهزة المُدارة المحددة للتثبيت، تأكد مما يلي:

- يوجد Kaspersky Endpoint Security أو تطبيق أمان آخر من Kaspersky مثبت.
- في Kaspersky Endpoint Security، إعدادات الحماية من تهديدات الملفات والحماية من تهديدات الويب والحماية من تهديدات البريد التي أنشأتها لهذا الجهاز.
- يمكن إيقاف Kaspersky Endpoint Security وبدئه يوميًا.
- يمكن إيقاف مهام المجموعة وبدئها يدويًا.

إنشاء حزم تثبيت مستقلة

يمكنك أنت ومستخدمو الجهاز في مؤسستك استخدام حزم التثبيت المستقلة لتثبيت التطبيقات على الأجهزة يدويًا.

حزمة التثبيت المستقلة عبارة عن ملف تنفيذي (installer.exe) يمكن إيجاده على خادم الويب أو في المجلد المشترك أو إرساله عبر البريد الإلكتروني، أو نقله إلى جهاز عميل بطريقة أخرى. على الجهاز العميل، يمكن للمستخدم تشغيل الملف المستلم محليًا لتثبيت تطبيق دون تدخل Kaspersky Security Center. يمكنك إنشاء حزم التثبيت المستقلة لتطبيقات Kaspersky وتطبيقات الجهات الخارجية لمنصات أنظمة التشغيل Windows وmacOS وLinux. لإنشاء حزمة تثبيت مستقلة لتطبيق جهة ثالثة، يجب عليك إنشاء حزمة تثبيت مخصصة.

تأكد من أن حزمة التثبيت المستقلة غير متاحة لأشخاص غير مصرح بهم.

لإنشاء حزمة تثبيت مستقلة:

1. قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل **Discovery & deployment** ← **Deployment & assignment** ← **Installation packages**.
- في القائمة الرئيسية، انتقل إلى **Operations** ← **Repositories** ← **Installation packages**.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. في قائمة حزم التثبيت، حدد حزمة التثبيت، وفي أعلى القائمة انقر على زر **Deploy**.

3. حدد خيار **Using a stand-alone package** .

يبدأ معالج إنشاء حزمة التثبيت المستقلة. انتقل عبر المعالج باستخدام زر **Next**.

4. تأكد من تمكين خيار **Install Network Agent together with this application** إذا أردت تثبيت عميل الشبكة مع التطبيق المحدد.

يتم عرض الخيار وفقًا للتطبيق الذي تنشئ حزمة تثبيت مستقلة له.

يتم تمكين هذا الخيار افتراضيًا. ننصح بتمكين هذا الخيار إذا لم تكن متأكدًا من تثبيت عميل الشبكة على الجهاز من عدمه. إذا كان عميل الشبكة مثبتًا بالفعل على الجهاز، بعد تثبيت حزمة التثبيت المستقلة مع عميل الشبكة، سيتم تحديث عميل الشبكة إلى الإصدار الأحدث.

إذا قمت بتعطيل هذا الخيار، فلن يتم تثبيت عميل الشبكة على الجهاز ولن تتم إدارة الجهاز.

إذا كانت حزمة التثبيت المستقلة للتطبيق المحدد موجودة بالفعل على خادم الإدارة، يحيطك المعالج علمًا بهذه الحقيقة. في هذه الحالة، يجب عليك تحديد أحد الإجراءات التالية:

- **Create stand-alone installation package**. حدد هذا الخيار إذا كنت على سبيل المثال تريد إنشاء حزمة تثبيت مستقلة لإصدار تطبيق جديد وتريد أيضًا الاحتفاظ بحزمة تثبيت مستقلة قمت بإنشائها لإصدار تطبيق سابق. يتم وضع حزمة التثبيت المستقلة الجديدة في مجلد آخر.
- **Use existing stand-alone installation package**. حدد هذا الخيار إذا أردت استخدام حزمة تثبيت مستقلة. لن يتم بدء عملية إنشاء الحزمة.
- **Rebuild existing stand-alone installation package**. حدد هذا الخيار إذا أردت إنشاء حزمة تثبيت مستقلة للتطبيق نفسه مرة أخرى. يتم وضع حزمة التثبيت المستقلة في المجلد نفسه.

5. في الخطوة **Move to list of managed devices**، يتم تحديد خيار **Do not move devices** بشكل افتراضي. إذا كنت لا تريد نقل الجهاز العميل إلى أي مجموعة إدارية بعد تثبيت عميل الشبكة، فاترك هذا الخيار ممكّنًا.

إذا كنت ترغب في نقل الجهاز العميل بعد تثبيت عميل الشبكة، حدد خيار **Move unassigned devices to this group** ثم حدد مجموعة إدارة ترغب في نقل الجهاز العميل إليها. بشكل افتراضي، يتم نقل الجهاز إلى مجموعة **Managed devices**.

6. عند الانتهاء من عملية إنشاء حزمة التثبيت المستقلة، انقر فوق الزر **إنهاء**.

يتم إغلاق Stand-alone Installation Package Creation Wizard.

يتم إنشاء حزمة التثبيت المستقلة ووضعها في المجلد الفرعي PkgInst الخاص بـمجلد خادم الإدارة المشترك. يمكنك عرض قائمة الحزم المستقلة من خلال النقر على زر **عرض قائمة الحزم المستقلة** أعلى قائمة حزم التثبيت.

عرض قائمة حزم التثبيت المستقلة

يمكنك عرض قائمة حزم التثبيت المستقلة وخصائص كل حزمة تثبيت مستقلة.

لعرض قائمة حزم التثبيت المستقلة لجميع حزم التثبيت:

أعلى القائمة، انقر على زر **View the list of stand-alone packages**.

في قائمة حزم التثبيت المستقلة، يتم عرض الخصائص التالية لها:

- **Package name** . اسم حزمة التثبيت المستقلة الذي يتم تشكيله تلقائيًا كاسم التطبيق الموجود في الحزمة وإصدار التطبيق.
- **Application name**. اسم التطبيق مذكورة في حزمة التثبيت المستقلة.
- **Application version**.
- **Network Agent installation package name**. يتم عرض الخاصية فقط إذا تم تضمين عميل الشبكة في حزمة التثبيت المستقلة.
- **Network Agent version** يتم عرض الخاصية فقط إذا تم تضمين عميل الشبكة في حزمة التثبيت المستقلة.
- **Size**. حجم الملف بالميجا بايت.
- **Group**. اسم المجموعة التي يتم نقل الجهاز العميل إليها بعد تثبيت عميل الشبكة.
- **Created**. تاريخ ووقت إنشاء حزمة التثبيت المستقلة.
- **Modified**. تاريخ ووقت تعديل حزمة التثبيت المستقلة.
- **Path**. المسار الكامل للمجلد الذي يوجد فيه حزمة التثبيت المستقلة.
- **Web address**. عنوان الويب لموقع حزمة التثبيت المستقلة.
- **File hash**. يتم استخدام الخاصية في تأكيد أن حزمة التثبيت المستقلة لم تتغير على يد أطراف خارجيين وأن المستخدم لديه الملف نفسه الذي قد أنشأته ونقلته إلى المستخدم.

لعرض قائمة حزم التثبيت المستقلة لحزمة تثبيت محددة:

حدد حزمة التثبيت في القائمة، وفي أعلى القائمة انقر على زر **View the list of stand-alone packages**.

في قائمة حزم التثبيت المستقلة، يمكنك فعل ما يلي:

- نشر حزمة تثبيت مستقلة على خادم الويب بالنقر على زر **Publish**. حزمة التثبيت المستقلة المنشورة متاحة للتنزيل للمستخدمين الذين أرسلت رابط حزمة التثبيت المستقلة إليهم.
- إلغاء نشر حزمة تثبيت مستقلة على خادم الويب بالنقر على زر **Unpublish**. حزمة تثبيت مستقلة غير منشورة ليست متوفرة للتنزيل إلا من أجلك ومن أجل المديرين الآخرين.
- تنزيل حزمة تثبيت مستقلة على جهازك بالنقر على زر **Download**.
- إرسال بريد إلكتروني به رابط لحزمة التثبيت المستقلة عن طريق النقر على زر **Send by email**
- إزالة حزمة تثبيت مستقلة بالنقر على زر **Remove**.

إنشاء حزمة توزيع مخصصة

يمكنك استخدام حزم التثبيت المخصصة للقيام بما يلي:

- لتثبيت أي تطبيق على جهاز عميل (مثل محرر نص)، عن طريق مهمة مثلاً.
- من أجل إنشاء حزمة تثبيت مستقلة.

حزمة التثبيت المخصصة عبارة عن مجلد به مجموعة من الملفات. المصدر لإنشاء حزمة تثبيت مخصصة هو ملف أرشيف. يحتوي ملف الأرشيف على ملف أو ملفات يجب تضمينها في حزمة التثبيت المخصصة. أثناء إنشاء حزمة تثبيت مخصصة، يمكنك تحديد معلمات سطر الأوامر، مثلاً لتثبيت التطبيق في وضع صامت.

إذا كان لديك مفتاح ترخيص نشط لميزة إدارة الثغرات الأمنية والتصحيحات، يمكنك تحويل إعدادات التثبيت الافتراضية لحزمة التثبيت المخصصة ذات الصلة واستخدام القيم التي يوصي بها خبراء Kaspersky. لا يتم تحويل الإعدادات تلقائيًا أثناء إنشاء حزمة التثبيت المخصصة إلا إذا كان الملف التنفيذي المقابل مدرجًا في قاعدة بيانات Kaspersky للتطبيقات الخارجية.

لإنشاء حزمة تثبيت مخصصة:

1. قم بأحد الإجراءات التالية:
   - في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Deployment & assignment** ← **Installation packages**.
   - في القائمة الرئيسية، انتقل إلى **Operations** ← **Repositories** ← **Installation packages**.

   يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.
2. انقر على **Add**.

   يبدأ معالج الحزمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.
3. حدد **Create an installation package from a file**.
4. حدد اسم الحزمة وانقر فوق الزر **Browse**.

   تفتح نافذة Windows قياسية في مستعرضك كي تتيح لك اختيار ملف لإنشاء حزمة التثبيت.
5. اختر ملفًا مضغوطًا موجودًا على الأقراص المتاحة.

   يمكنك تحميل ملف أرشيف ZIP أو CAB أو TAR أو TAR.GZ. لا يمكن إنشاء حزمة تثبيت من ملف SFX (أرشيف ذاتي الاستخراج).

إذا كنت ترغب في تحويل الإعدادات أثناء تثبيت الحزمة، تأكد أن خانة الاختيار **Convert settings to recommended values for applications recognized by Kaspersky Security Center after the wizard finishes** محددة ثم انقر على **Next**.

سيبدأ رفع الملف إلى خادم إدارة Kaspersky Security Center.

إذا قمت بتفعيل استخدام إعدادات التثبيت الموصى بها، يتحقق Kaspersky Security Center 15.1 مما إذا كان الملف التنفيذي ضمن قاعدة بيانات Kaspersky للتطبيقات الخارجية أم لا. إذا كان التحقق ناجحًا، سترى إخطارًا يعلمك أنه قد تم التعرف على الملف. يتم تحويل الإعدادات ويتم إنشاء حزمة التثبيت المخصصة. لا يلزم اتخاذ إجراءات إضافية. انقر على زر **Finish** لإغلاق المعالج.

6. حدد ملفًا (من قائمة الملفات المستخرجة من الملف المضغوط المختار) وحدد معلمات سطر الأوامر لملف تنفيذي.

يمكنك تحديد معلمات سطر الأوامر لتثبيت التطبيق من حزمة التثبيت في وضع صامت. تحديد معلمات سطر الأوامر أمر اختياري.

لقد بدأت عملية إنشاء حزمة التثبيت.

يحيطك المعالج علمًا عند الانتهاء من العملية.

إذا لم يتم إنشاء حزمة التثبيت، يتم عرض رسالة مناسبة.

7. انقر على زر **Finish** لإغلاق المعالج.

يتم تنزيل حزمة التثبيت التي قمت بإنشائها إلى مجلد الحزم الفرعي الخاص بـمجلد خادم الإدارة المشترك. بعد التنزيل تظهر حزمة التثبيت في قائمة حزم التثبيت.

في قائمة حزم التثبيت المتوفرة على خادم الإدارة، يمكنك فعل ما يلي عن طريق النقر على الرابط الذي به اسم حزمة تثبيت مخصصة:

- عرض الخصائص التالية لحزمة تثبيت:
  - **Name**. اسم حزمة تثبيت مخصص.
  - **Source**. اسم بائع التطبيق.
  - **Application**. اسم التطبيق الموضوع في حزمة التثبيت المخصصة.
  - **Version** . إصدار التطبيق
  - **Language**. لغة التطبيق الموضوعة في حزمة التثبيت المخصصة.
  - **Size (MB)** . حجم حزمة التثبيت.
  - **Operating system**. نوع نظام التشغيل الذي ستعمل عليه حزمة التثبيت.
  - **Created**. تاريخ إنشاء حزمة التثبيت.
  - **Modified**. تاريخ تعديل حزمة التثبيت.
  - **Type**. نوع حزمة التثبيت.
- تغيير اسم الحزمة ومعلمات سطر الأوامر. هذه الميزة غير متوفرة إلا للحزم التي لم يتم إنشاؤها على أساس تطبيقات Kaspersky.

إذا قمت بتحويل إعدادات حزمة التثبيت إلى القيم الموصى بها لعملية إنشاء الحزمة المخصصة، قد يظهر قسمان إضافيان في تبويب **Settings** لخصائص حزمة التثبيت المخصصة: **Settings** و**Installation procedure**.

يحتوي قسم **Settings** على الخصائص التالية وتظهر في جدول:

- **الاسم**. يعرض هذا الجدول الاسم المخصص لمعلمة التثبيت.
- **النوع**. يعرض هذا العمود نوع معلمة التثبيت.
- **القيمة**. يعرض هذا العمود نوع البيانات التي تحددها معلمة التثبيت (قيمة منطقية أو مسار ملف أو رقمية أو مسار أو سلسلة).

يحتوي قسم **Installation procedure** على طاولة تصف الخصائص التالية للتحديث المدرج في حزمة التثبيت المخصصة:

- **الاسم**. اسم الشبكة الفرعية.
- **الوصف**. وصف التحديث.
- **المصدر**. مصدر التحديث، أي ما إذا كان قد تم إصداره بواسطة Microsoft أو بواسطة مطور آخر تابع لجهة خارجية.
- **النوع**. نوع التحديث، أي ما إذا كان مخصصًا لبرنامج تشغيل أو تطبيق.
- **الفئة**. يتم عرض فئة Windows Server Update Services (WSUS) لتحديثات Microsoft (التحديثات المهمة أو تحديثات التعريف أو برامج التشغيل أو حزم الميزات أو تحديثات الأمان أو حزم الخدمة أو الأدوات أو مجموعات التحديثات أو التحديثات أو الترقية).
- **مستوى الأهمية وفق MSRC**. مستوى أهمية التحديث المحدد في مركز استجابة خبراء الأمان من Microsoft (MSRC).
- **مستوى الأهمية**. مستوى أهمية التحديث كما تحدده Kaspersky.
- **مستوى أهمية التصحيح (للتصحيحات المخصصة للاستخدام في تطبيقات Kaspersky)**. مستوى أهمية التصحيح إذا كان مخصصًا لتطبيق Kaspersky.
- **المقال**. معرف المقالة في "قاعدة المعارف" التي تصف التحديث.
- **النشرة**. معرف نشرة الأمان التي تصف التحديث.
- **غير مخصص للتثبيت**. يعرض ما إذا كان التحديث بحالة "غير مخصص للتثبيت" أم لا.
- **للتثبيت**. يعرض ما إذا كان التحديث بحالة "للتثبيت" أم لا.
- **جاري التثبيت**. يعرض ما إذا كان التحديث بحالة "جاري التثبيت" أم لا.
- **مثبت**. يعرض ما إذا كان التحديث بحالة "مثبت" أم لا.
- **تعذر**. يعرض ما إذا كان التحديث بحالة "تعذر" أم لا.
- **إعادة التشغيل مطلوبة**. يعرض ما إذا كان التحديث بحالة "إعادة التشغيل مطلوبة" أم لا.
- **مسجل**. يعرض تاريخ ووقت تسجيل التحديث.
- **مثبت في الوضع التفاعلي**. يعرض ما إذا كان التحديث يتطلب التفاعل مع المستخدم أثناء التثبيت.
- **تم الإبطال**. يعرض التاريخ والوقت اللذين تم فيهما إبطال التحديث.
- **حالة الموافقة على التحديث**. يعرض ما إذا قد تمت الموافقة على التحديث للتثبيت أم لا.
- **المراجعة**. يعرض رقم المراجعة الحالي للتحديث.
- **معرف التحديث**. يعرض معرّف التحديث.

- **إصدار التطبيق**. يعرض رقم الإصدار الذي سيتم تحديث التطبيق إليه.
- **حل محله**. يعرض التحديثات الأخرى التي يمكن أن تحل محل التحديث.
- **يحل محل**. يعرض التحديثات الأخرى التي يمكن أن يحل محلها التحديث.
- **يجب أن توافق على شروط اتفاقية الترخيص**. يعرض ما إذا كان التحديث يتطلب قبول شروط اتفاقية ترخيص المستخدم النهائي أم لا.
- **البائع**. يعرض اسم بائع التحديث.
- **عائلة التطبيق**. يعرض اسم عائلة التطبيقات التي ينتمي إليها التحديث.
- **التطبيق**. يعرض اسم التطبيق الذي ينتمي إليه التحديث.
- **اللغة**. يعرض لغة ترجمة التحديث.
- **غير مخصص للتثبيت (إصدار جديد)**. يعرض ما إذا كان التحديث بحالة "غير مخصص للتثبيت (إصدار جديد)".
- **يتطلب متطلبات أساسية للتثبيت**. يعرض ما إذا كان التحديث بحالة "يتطلب متطلبات أساسية للتثبيت".
- **وضع التنزيل**. يعرض وضع تنزيل التحديث.
- **عبارة عن تصحيح**. يعرض ما إذا كان التحديث عبارة عن تصحيح أم لا.
- **غير مثبت**. يعرض ما إذا كان التحديث بحالة "غير مثبت" أم لا.

توزيع حزم التثبيت على خوادم الإدارة الثانوية

يتيح لك Kaspersky Security Center ذلك إنشاء حزم التثبيت لتطبيقات Kaspersky ولتطبيقات الجهات الخارجية، فضلاً عن توزيع حزم التثبيت على الأجهزة العميلة وتثبيت التطبيقات من الحزم. لتحسين التحميل على خادم الإدارة الأساسي، يمكنك توزيع حزم التثبيت على خوادم الإدارة الثانوية. بعد ذلك، تقوم الخوادم الثانوية بنقل الحزم إلى أجهزة العميل، ومن ثم يمكنك إجراء التثبيت عن بُعد للتطبيقات على أجهزة العميل الخاصة بك.

لتوزيع حزم التثبيت على خوادم الإدارة الثانوية:

1. تأكد من أن خوادم الإدارة الثانوية متصلة بخادم الإدارة الأساسي.
2. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.

   يتم عرض قائمة المهام.
3. انقر على الزر **Add**.

   سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.
4. في صفحة **New task settings** من القائمة المنسدلة **Application**، حدد **Kaspersky Security Center**. ومن قائمة **Task type** المنسدلة، حدد **Distribute installation package**، ثم حدد اسم المهمة.
5. في صفحة **Task scope**، حدد الأجهزة التي تم تعيين المهمة لها بإحدى الطرق التالية:
   - إذا كنت تريد إنشاء مهمة لجميع خوادم الإدارة الثانوية في مجموعة إدارة معينة، فحدد هذه المجموعة، ثم قم بإنشاء مهمة جماعية لها.
   - إذا كنت تريد إنشاء مهمة لخوادم الإدارة الثانوية المحددة، فحدد هذه الخوادم، ثم قم بإنشاء مهمة لها.
6. في صفحة **Distributed installation packages**، حدد حزم التثبيت التي سيتم نسخها إلى خوادم الإدارة الثانوية.

7. حدد حسابًا لتشغيل مهمة توزيع حزمة التثبيت ضمن هذا الحساب. يمكنك استخدام حسابك وترك خيار **Default account** ممكّنًا. أو بدلاً من ذلك، يمكنك تحديد أنه يجب أن يتم تشغيل المهمة ضمن حساب آخر لديه حقوق الوصول الضرورية. وللقيام بذلك، حدد خيار **Specify account**، ثم أدخل بيانات اعتماد هذا الحساب.

8. في صفحة **Finish task creation**، يمكنك تمكين الخيار **Open task details when creation is complete** لفتح نافذة خصائص المهمة ثم تعديل إعدادات المهمة الافتراضية. بخلاف ذلك، يمكنك تكوين إعدادات المهمة لاحقًا في أي وقت.

9. انقر على زر **Finish**.

   يتم عرض المهمة التي تم إنشاؤها لتوزيع حزم التثبيت على خوادم الإدارة الثانوية في قائمة المهام.

10. يمكنك تشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

    بعد اكتمال المهمة، يتم نسخ حزم التثبيت المحددة إلى خوادم الإدارة الثانوية المحددة.

تثبيت التطبيقات باستخدام مهمة التثبيت عن بُعد

يسمح لك Kaspersky Security Center بتثبيت التطبيقات على الأجهزة عن بُعد، باستخدام مهام التثبيت عن بُعد. ويتم إنشاء هذه المهام وتعيينها إلى الأجهزة من خلال المعالج المخصص. لتعيين مهمة بصورة أكثر سرعة وسهولة، يمكنك تحديد الأجهزة (حتى 1000 جهاز) في نافذة المعالج بأي طريقة من الطرق التالية:

- **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة** . في هذه الحالة، يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.
- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**. يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.
- **تعيين مهمة إلى تحديد الجهاز** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في المجموعة المحددة التي تم إنشائها في وقت سابق. يمكنك تحديد المجموعة المحددة مسبقًا أو المجموعة المخصصة التي أنشأتها.
- **تعيين مهمة لمجموعة إدارة** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة تم إنشائها في وقت سابق.

لتجنب المشكلات التي قد تحدث أثناء تثبيت التطبيق على جهاز عميل بدون تثبيت عميل الشبكة، يجب عليك المتابعة كما هو موضح في النشر الإجباري عبر مهمة تثبيت عن بُعد من Kaspersky Security Center.

تثبيت تطبيق عن بُعد

يحتوي هذا القسم على معلومات حول كيفية تثبيت تطبيق عن بُعد على مجموعة إدارة، أو أجهزة ذات عناوين IP محددة، أو مجموعة مختارة من الأجهزة المُدارة.

لتثبيت تطبيق على الأجهزة المحددة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة.

3. في حقل **Task type**، حدد **Install application remotely**.

4. حدد أحد الخيارات التالية:

- **Assign task to an administration group**

يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

- **Specify device addresses manually or import addresses from a list**

يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

- **Assign task to a device selection**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

يتم إنشاء مهمة تثبيت التطبيق عن بُعد للأجهزة المحددة. إذا حددت الخيار **Assign task to an administration group**، فستكون المهمة مجموعة واحدة.

5. في خطوة **Task scope**، حدد مجموعة الإدارة، أو الأجهزة ذات العناوين المحددة ، أو تحديد الجهاز.

تعتمد الإعدادات المتاحة على الخيار المحدد في الخطوة السابقة.

6. في خطوة **حزم التثبيت**، حدد الإعدادات التالية:

- في حقل **تحديد حزمة التثبيت**، حدد حزمة التثبيت للتطبيق الذي تريد تثبيته.
- في مجموعة إعدادات **تنزيل حزمة التثبيت الإجباري**، حدد كيفية توزيع الملفات المطلوبة لتثبيت التطبيق إلى الأجهزة العميلة:

- **Using Network Agent**

إذا كان هذا الخيار مفعلاً، سيتم تسليم حزم التثبيت إلى الأجهزة العميلة بواسطة عميل الشبكة المثبت على الأجهزة العميلة هذه.

في حالة تعطيل هذا الخيار، يتم تسليم حزم التثبيت باستخدام أدوات نظام التشغيل للأجهزة العميلة.

ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة.

يتم تمكين هذا الخيار افتراضيًا.

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

إذا تم تفعيل هذا الخيار، سيتم نقل حزم التثبيت إلى الأجهزة العميلة باستخدام أدوات نظام التشغيل من خلال نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت توجد نقطة توزيع واحدة على الأقل في الشبكة.

في حالة تفعيل هذا الخيار **استخدام عميل الشبكة**، يتم تسليم الملفات بواسطة أدوات نظام التشغيل فقط في حالة عدم توفر موارد عميل الشبكة.

يتم تفعيل هذا الخيار افتراضيًا لمهام التثبيت عن بُعد التي تم إنشاؤها على خادم إدارة افتراضي.

عندما تكون جميع نقاط التوزيع المخصصة للجهاز معطلة، فلن يتمكن الجهاز من تلقي التحديثات (قواعد بيانات مكافحة الفيروسات والتصحيحات) وحزم التثبيت.

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

إذا تم تمكين هذا الخيار، يتم نقل الملفات إلى أجهزة العميل باستخدام أدوات نظام التشغيل لأجهزة العميل من خلال خادم الإدارة. يمكنك تفعيل هذا الخيار إذا لم يتم تثبيت عميل شبكة على الجهاز العميل، لكن الجهاز العميل موجود في نفس الشبكة الموجود عليها خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- في الحقل **أقصى عدد من عمليات التنزيل المتزامنة**، حدد الحد الأقصى المسموح به لعدد أجهزة العميل التي يمكن لخادم الإدارة أن يرسل إليها الملفات في نفس الوقت.

- في الحقل **الحد الأقصى لعدد محاولات التثبيت**، حدد الحد الأقصى المسموح به لعدد مرات تشغيل المثبت.

إذا تم تجاوز عدد المحاولات المحددة في المعلمة، فلن يبدأ Kaspersky Security Center برنامج التثبيت على الجهاز بعد الآن. لإعادة تشغيل مهمة تثبيت التطبيق عن بُعد، قم بزيادة قيمة معلمة **الحد الأقصى لعدد محاولات التثبيت** وابدأ المهمة. وكحل بديل، يمكنك إنشاء مهمة تثبيت تطبيق عن بعد جديدة.

- إذا قمت بالترحيل من تطبيق Kaspersky إلى آخر وكان تطبيقك الحالي محميًا بكلمة مرور، فأدخل كلمة المرور في الحقل **Password to uninstall the current Kaspersky application**. لاحظ أنه أثناء الترحيل، سيتم إلغاء تثبيت تطبيق Kaspersky الحالي الخاص بك.

يتوافر الحقل **Password to uninstall the current Kaspersky application** فقط إذا حددت الخيار **Using Network Agent** في مجموعة الإعدادات **تنزيل حزمة التثبيت الإجباري**.

يمكنك استخدام كلمة مرور إلغاء التثبيت فقط لسيناريو ترحيل Kaspersky Security for Windows Server إلى Kaspersky Endpoint Security for Windows عند تثبيت Kaspersky Endpoint Security for Windows باستخدام مهمة تثبيت التطبيق عن بعد. وقد يؤدي استخدام كلمة مرور إلغاء التثبيت عند تثبيت مكونات أخرى إلى حدوث أخطاء في التثبيت.

لإكمال سيناريو الترحيل بنجاح، تأكد من تلبية المتطلبات الأساسية التالية:

- أنت تستخدم Kaspersky Security Center Network Agent 14.2 لنظام التشغيل Windows أو أحدث.

- تقوم بتثبيت التطبيق على أجهزة تعمل بنظام Windows.

- حدد الإعداد الإضافي:

- **لا تقم بإعادة تثبيت التطبيق إذا كان مثبتًا بالفعل**

إذا تم تفعيل هذا الخيار، لن يتم عادة تثبيت التطبيق المحدد إذا كان مثبتًا بالفعل على الجهاز العميل هذا.

إذا تم تفعيل هذا الخيار، سيتم تثبيت التطبيق بأية حال.

يتم تمكين هذا الخيار افتراضيًا.

- **Verify operating system type before downloading**

قبل نقل الملفات إلى أجهزة العميل، يتحقق Kaspersky Security Center مما إذا كانت إعدادات أداة التثبيت قابلة للتطبيق على نظام تشغيل الجهاز العميل أم لا. إذا لم تكن الإعدادات قابلة للتطبيق، لا ينقل Kaspersky Security Center الملفات ولا يحاول تثبيت التطبيق. على سبيل المثال: لتثبيت تطبيق على أجهزة في مجموعة إدارة تشمل أجهزة تعمل بعدة أنظمة تشغيل مختلفة، يمكنك تعيين مهمة التثبيت إلى مجموعة الإدارة ثم تفعيل هذا الخيار من أجل تخطي الأجهزة التي تعمل بنظام تشغيل غير النظام المطلوب.

عند تثبيت عميل الشبكة عن بُعد على الأجهزة غير المعينة، يحدد Kaspersky Security Center أو نقطة توزيع تلقائيًا نوع نظام تشغيل الجهاز، بغض النظر عن إعداد **Verify operating system type before downloading**.

- **Assign package installation in Active Directory group policies**

في حال تمكين هذا الخيار، سيتم تثبيت حزمة التثبيت باستخدام سياسات مجموعة Active Directory.

يتوفر هذا الخيار فقط إذا تم تحديد حزمة تثبيت عميل الشبكة.

يتم تعطيل هذا الخيار افتراضيًا.

- **مطالبة المستخدمين بإنهاء التطبيقات قيد التشغيل**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- حدد الأجهزة التي تريد تثبيت التطبيق عليها:

- **التثبيت على كل الأجهزة**

سيتم تثبيت التطبيق حتى على الأجهزة التي تدار بواسطة خوادم إدارة أخرى.

ويتم تحديد هذا الخيار بصورة افتراضية. لا يتعين عليك تغيير هذا الإعداد إذا كان لديك خادم إدارة واحد فقط في شبكتك.

- **يتم التثبيت فقط على الأجهزة المُدارة من خلال خادم الإدارة هذا**

سيتم تثبيت التطبيق فقط على الأجهزة التي تدار بواسطة خادم الإدارة هذا. حدد هذا الخيار إذا كان لديك أكثر من خادم إدارة واحد في الشبكة الخاصة بك وكنت ترغب في تجنب التعارض بينها.

- حدد إذا ما كان يجب نقل الأجهزة إلى مجموعة إدارة بعد التثبيت أم لا.

- **عدم نقل الأجهزة**

تبقى الأجهزة في المجموعات الموجودة فيها حاليًا. والأجهزة التي لم يتم وضعها في مجموعة تبقى دون تخصيص.

- **Move unassigned devices to the selected group (only a single group can be selected)**

يتم نقل الأجهزة إلى مجموعة الإدارة التي تحددها.

يرجى ملاحظة أنه يتم تحديد خيار **عدم نقل الأجهزة** بصورة افتراضية. ولأسباب أمنية، قد ترغب في نقل الأجهزة يدويًا.

7. في هذه الخطوة من المعالج، حدد ما إذا كان يجب إعادة تشغيل الأجهزة أثناء تثبيت التطبيقات:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **Force closure of applications in blocked sessions**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

8. إذا لزم الأمر، في الخطوة **حدد حسابات للوصول إلى الأجهزة**، أضف الحسابات التي سيتم استخدامها لبدء مهمة تثبيت التطبيق عن بُعد:

- **لا يلزم وجود حساب (تم تثبيت عميل الشبكة)**

إذا تم تحديد هذا الخيار، فلا يلزم تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

إذا لم يتم تثبيت عميل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

- **يُلزم وجود حساب (عميل الشبكة غير مستخدم)**

حدد هذا الخيار إذا لم يتم تثبيت عميل الشبكة على الأجهزة التي قمت بتعيين مهمة التثبيت عن بُعد لها. في هذه الحالة، يمكنك تحديد حساب مستخدم أو شهادة SSH لتثبيت التطبيق.

- **Local Account**. إذا تم تحديد هذا الخيار، فحدد الحساب المستخدم الذي سيتم من خلاله تشغيل مثبت التطبيق. انقر على الزر **إضافة**، وحدد **Local Account**، ثم حدد بيانات اعتماد حساب المستخدم.

يمكنك تحديد عدة حسابات مستخدمين، على سبيل المثال، إذا لم يكن لدى أي منهم جميع الحقوق المطلوبة على جميع الأجهزة التي قمت بتعيين المهمة لها. في هذه الحالة، يتم استخدام جميع الحسابات المضافة لتشغيل المهمة، بترتيب متتالٍ، من أعلى إلى أسفل.

- **شهادة SSH**. إذا كنت ترغب في تثبيت تطبيق على جهاز عميل يستند إلى Linux ، فيمكنك تحديد شهادة SSH بدلاً من حساب المستخدم. انقر على زر **إضافة**، وحدد **شهادة SSH**، ثم حدد المفاتيح الخاصة والعامة للشهادة.

لإنشاء مفتاح خاص، يمكنك استخدام الأداة المساعدة ssh-keygen. لاحظ أن Kaspersky Security Center يدعم تنسيق PEM للمفاتيح الخاصة، لكن الأداة المساعدة ssh-keygen تنشئ مفاتيح SSH بتنسيق OPENSSH افتراضيًا. تنسيق OPENSSH غير مدعوم من قبل Kaspersky Security Center. ولإنشاء مفتاح خاص بتنسيق PEM المدعوم، أضف الخيار -m PEM في الأمر ssh-keygen. فمثلاً:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "< البريد الالكتروني للمستخدم >"
```

9. في خطوة **إنهاء عملية إنشاء المهمة**، انقر فوق الزر " **إنهاء** " لإنشاء المهمة وإغلاق المعالج.

إذا قمت بتفعيل خيار **Open task details when creation is complete**، ستفتح نافذة إعدادات المهمة. في هذه النافذة، يمكنك التحقق من معلمات المهمة أو تعديلها أو تكوين جدول بدء المهمة، إذا لزم الأمر.

10. في قائمة المهام، حدد المهمة التي قمت بإنشائها، ثم انقر فوق **ابدأ** .

أو بدلاً من ذلك، انتظر حتى تبدأ المهمة وفقًا للجدول الذي حددته في إعدادات المهمة.

عند اكتمال مهمة التثبيت عن بُعد، يتم تثبيت التطبيق المحدد على الأجهزة المحددة.

تثبيت تطبيق من خلال سياسات مجموعة Active Directory

يتيح لك Kaspersky Security Center تثبيت تطبيقات Kaspersky على الأجهزة المدارة باستخدام سياسات مجموعة Active Directory.

يمكنك تثبيت التطبيقات باستخدام سياسات مجموعة Active Directory من خلال حزم التثبيت التي تتضمن عامل الشبكة.

لتثبيت التطبيقات باستخدام سياسات مجموعة Active Directory:

1. قم بتشغيل معالج نشر الحماية. اتبع إرشادات المعالج.

2. في صفحة **Remote installation task settings** الخاصة بمعالج نشر الحماية، قم بتمكين خيار **Assign package installation in Active Directory group policies**.

3. في صفحة **Select accounts to access devices**، حدد خيار **Account required (Network Agent is not used)** .

4. أضف الحساب الذي يمتلك امتيازات المسؤول على الجهاز المثبت عليه Kaspersky Security Center أو الحساب المضمن مجموعة المجالGroup Policy Creator Owners.

5. منح الأذونات للحساب المحدد:

   a. انتقل إلى **لوحة التحكم** ← **الأدوات الإدارية** وافتح **إدارة سياسة المجموعة**.

   b. انقر فوق العقدة مع المجال المطلوب.

   c. انقر فوق قسم **التفويض**.

   d. في القائمة المنسدلة **الإذن**، حدد **ربط عناصر سياسة المجموعة**.

   e. انقر فوق **إضافة**.

   f. في نافذة **تحديد المستخدم أو الكمبيوتر أو المجموعة** التي تفتح، حدد الحساب المطلوب.

   g. انقر فوق **موافق** لإغلاق نافذة **تحديد مستخدم أو كمبيوتر أو مجموعة**.

   h. في قائمة **المجموعات والمستخدمين**، حدد الحساب الذي أضفته للتو وانقر فوق **إعدادات متقدمة** ← **إعدادات متقدمة**.

   i. في قائمة **إدخالات الأذونات**، انقر نقرًا مزدوجًا فوق الحساب الذي أضفته للتو.

   j. امنح الأذونات التالية:

   - **إنشاء عناصر المجموعة**
   - **حذف عناصر المجموعة**

- **إنشاء كائنات مجموعة حاوية السياسة**
- **حذف كائنات مجموعة حاوية السياسة**

k. انقر فوق **موافق** لحفظ التغييرات.

6. حدد الإعدادات الأخرى باتباع تعليمات المعالج.

7. قم بتشغيل مهمة التثبيت عن بُعد يدويًا أو انتظر حتى تبدأ وفق جدولها.

تبدء سلسلة عمليات التثبيت عن بُعد التالية:

1. عندما تشغيل كل مهمة، يتم إنشاء الكائنات التالية في كل مجال يتضمن أي من الأجهزة العميلة من المجموعة المحددة:
   - كائن سياسة المجموعة (GPO) باسم **Kaspersky_AK{GUID}**.
   - مجموعة الأمان التي تتوافق مع GPO. تتضمن مجموعة الأمان هذه أجهزة عميلة مغطاة بواسطة المهمة. ويحدد محتوى مجموعة الأمان نطاق GPO.
2. يقوم Kaspersky Security Center بتثبيت تطبيقات Kaspersky المحددة على الأجهزة العميلة مباشرةً من KLSHARE، أي مجلد الشبكة المشترك للتطبيق. في مجلد تثبيت Kaspersky Security Center، سيتم إنشاء مجلد فرعي احتياطي يحتوي على ملف .msi لتثبيت التطبيق.
3. إذا تمت إضافة الأجهزة الجديدة إلى نطاق المهمة، تتم إضافتها إلى مجموعة الأمان بعد البدء التالي للمهمة. إذا تم تحديد الخيار **Run missed tasks** في جدول المهمة، تتم إضافة الأجهزة إلى مجموعة الأمان فورًا.
4. إذا تم حذف الأجهزة من نطاق المهمة، فيتم حذفها من مجموعة الأمان بعد البدء التالي للمهمة.
5. عند حذف مهمة من Active Directory، يتم أيضًا حذف GPO ورابط GPO ومجموعة الأمان المطابقة أيضًا.

إذا أردت تطبيق نظام تثبيت آخر باستخدام Active Directory، يمكنك تكوين الإعدادات المطلوبة يدويًا. على سبيل المثال، قد يكون هذا مطلوبًا في بعض الحالات:

- عندما لا يتمتع مسؤول الحماية ضد الفيروسات بالحقوق اللازمة لإجراء تغييرات على Active Directory لمجالات معينة.
- عندما يجب تخزين حزمة التثبيت الأصلية في مورد شبكة منفصل
- عندما يكون من الضروري ربط GPO بوحدات محددة في Active Directory

تتوفر الخيارات التالية لاستخدام نظام تثبيت بديل من خلال Active Directory:

- إذا كان المطلوب إجراء التثبيت مباشرةً من مجلد Kaspersky Security Center المشترك، ففي خصائص GPO، يجب عليك تحديد ملف .msi الموجود في المجلد الفرعي exec داخل مجلد حزمة التثبيت الخاصة بالتطبيق المطلوب.
- إذا كان يجب وضع حزمة التثبيت في مورد شبكة آخر، يجب عليك نسخ محتوى مجلد exec بالكامل إلى ذلك المورد، لأنه بالإضافة إلى الملف ذي الامتداد .msi، يحتوي المجلد على ملفات التكوين التي تم إنشاؤها عند إنشاء الحزمة. لتثبيت مفتاح الترخيص مع التطبيق، انسخ ملف المفتاح إلى هذا المجلد أيضًا.

تثبيت التطبيقات على خوادم الإدارة الثانوية

لتثبيت تطبيق على خوادم الإدارة الثانوية:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في خوادم الإدارة الثانوية ذات الصلة.
2. تأكد من توفر حزمة التثبيت التي تتطابق مع التطبيق الجاري تثبيته على كل خادم من خوادم الإدارة الثانوية المحددة. إذا لم تتمكن من العثور على حزمة التثبيت على أي من الخوادم الثانوية، فقم بتوزيعها. لهذا السبب، قم بإنشاء مهمة باستخدام نوع مهمة **Distribute installation package** .

3. قم بإنشاء مهمة لتثبيت التطبيق عن بعد على خوادم الإدارة الثانوية. حدد نوع المهمة **Install application on secondary Administration Server remotely**.

يقوم معالج المهمة الجديدة بإنشاء مهمة للتثبيت عن بُعد للتطبيق المحدد في المعالج على خوادم إدارة ثانوية محددة.

4. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

عند اكتمال مهمة التثبيت عن بُعد، يتم تثبيت التطبيق المحدد على خوادم الإدارة الثانوية.

تحديد إعدادات التثبيت عن بُعد على أجهزة Unix

عندما تقوم بتثبيت تطبيق على جهاز Unix باستخدام مهمة تثبيت عن بُعد، يمكنك تحديد إعدادات Unix الخاصة للمهمة. تتوفر هذه الإعدادات في خصائص المهمة بعد إنشاء المهمة.

لتحديد إعدادات Unix الخاصة لمهمة التثبيت عن بُعد:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على اسم مهمة التثبيت عن بُعد التي ترغب في تحديد إعدادات Unix الخاصة بها.

ستفتح نافذة خصائص المهمة.

3. انتقل إلى **Unix-specific settings** ← **Application settings**.

4. حدد الإعدادات التالية:

- **Set a password for the root account (only for deployment through SSH)**

إذا كان لا يمكن استخدام الأمر sudo على الجهاز المستهدف دون تحديد كلمة المرور، حدد هذا الخيار ثم حدد كلمة المرور لحساب الجذر. Kaspersky Security Center ينقل كلمة المرور في نموذج مشفر إلى الجهاز المستهدف، ويفك تشفير كلمة المرور ثم يبدأ إجراء التثبيت نيابةً عن حساب الجذر باستخدام كلمة المرور المحددة.

> Kaspersky Security Center لا يستخدم الحساب أو كلمة المرور المحددة لإنشاء اتصال SSH.

- **Specify the path to a temporary folder with Execute permissions on the target device (only for deployment through SSH)**

إذا لم يكن الدليل /tmp على الجهاز المستهدف لديه إذن التنفيذ، حدد هذا الخيار ثم حدد المسار إلى الدليل بإذن التنفيذ. Kaspersky Security Center يستخدم الدليل المحدد كدليل مؤقت للوصول عبر SSH. التطبيق يضع حزمة التثبيت في الدليل ويقوم بتشغيل إجراء التثبيت.

5. انقر على زر **Save**.

بهذا تم حفظ إعدادات المهمة المحددة.

تشغيل وإيقاف تطبيقات Kaspersky

يمكنك استخدام مهمة تشغيل التطبيق أو إيقافه لبدء تشغيل تطبيقات Kaspersky وإيقافها على الأجهزة المدارة.

لإنشاء مهمة تشغيل التطبيق أو إيقافه:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

3. في القائمة المنسدلة **Application**، حدد التطبيق الذي تريد إنشاء المهمة له.

   يتم عرض تطبيقات Kaspersky في القائمة إذا سبق لك إضافة مكونات ويب إضافية للإدارة لهذه التطبيقات.

4. في قائمة **Task type**، حدد مهمة **تفعيل التطبيق**.

5. في الحقل **اسم المهمة**، حدد اسم المهمة الجديدة.

   لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

6. حدد الأجهزة التي سيتم تعيين المهمة إليها.

7. في نافذة **Applications**، نفذ ما يلي:

   - حدد خانات الاختيار الموجودة بجوار أسماء التطبيقات التي تريد إنشاء المهمة لها.
   - حدد الخيار **Start application** أو **Stop application**.

8. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في خطوة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

9. انقر على زر **Finish**.

   يتم إنشاء المهمة وعرضها في قائمة المهام.

10. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

11. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك، ثم احفظ الإعدادات.

    سيتم إنشاء المهمة وتكوينها.

إذا كنت تريد تشغيل المهمة، فحددها في قائمة المهام، ثم انقر فوق الزر **Start**.

إدارة الأجهزة المحمولة

يتم تنفيذ إدارة حماية الجهاز المحمول من خلال Kaspersky Security Center باستخدام ميزة إدارة جهاز المحمول، التي تتطلب ترخيصًا مخصصًا. إذا كنت تنوي إدارة الأجهزة المحمولة المملوكة للموظفين في مؤسستك، فقم بتمكين وتهيئة إدارة الأجهزة المحمولة.

تتيح لك إدارة الأجهزة المحمولة إدارة أجهزة Android للموظفين. يتم توفير الحماية من خلال تطبيق Kaspersky Endpoint Security for Android للهاتف المحمول المثبت على الأجهزة. يضمن تطبيق الهاتف المحمول هذا حماية الأجهزة المحمولة من تهديدات الويب والفيروسات والبرامج الأخرى التي تشكل تهديدات. للإدارة المركزية من خلال Kaspersky Security Center Web Console، يجب عليك تثبيت المكونات الإضافية التالية لإدارة الويب على الجهاز حيث تم تثبيت Kaspersky Security Center Web Console:

- Kaspersky Security for Mobile Plug-in
- Kaspersky Endpoint Security for Android Plug-in

للحصول على معلومات عن نشر الحماية وإدارة الأجهزة المحمولة، راجع تعليمات Kaspersky Security for Mobile.

تعديل إعدادات إدارة الأجهزة المحمولة في Kaspersky Security Center Web Console

لتعديل إعدادات إدارة الجهاز المحمول:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد القسم **Additional ports**.

3. قم بتعديل الإعدادات ذات الصلة:

- **Open port for mobile devices**

في حالة تمكين مفتاح التبديل هذا، سيتم فتح منفذ الأجهزة المحمولة على خادم الإدارة.
لا يمكنك استخدام منفذ الأجهزة المحمولة إلا إذا كان مكون إدارة الأجهزة المحمولة مثبتًا.
في حالة تعطيل مفتاح التبديل هذا، لن يتم استخدام منفذ الأجهزة المحمولة على خادم الإدارة.
يتم تعطيل مفتاح التبديل هذا افتراضيًا.

- **Port for mobile device synchronization**

رقم المنفذ المستخدم لإتمام الاتصال بين الأجهزة المحمولة وخادم الإدارة. رقم المنفذ الافتراضي هو 13292.
تم استخدام النظام العشري للسجلات.

- **Port for mobile device activation**

منفذ اتصال Kaspersky Endpoint Security for Android بخوادم تنشيط Kaspersky.
رقم المنفذ الافتراضي هو 17100.

4. انقر على زر **Save**.

يمكن الآن للأجهزة المحمولة الاتصال بخادم الإدارة.

استبدال تطبيقات الأمان من جهة خارجية

قد يتطلب تثبيت تطبيقات الأمان الخاصة بـ Kaspersky عبر Kaspersky Security Center إزالة برنامج الجهة الخارجية غير المتوافق مع التطبيق الذي يتم تثبيته. يوفر Kaspersky Security Center عدة طرق تتعلق بإزالة تطبيقات الجهات الخارجية.

إزالة التطبيقات غير المتوافقة من خلال استخدام برنامج التثبيت

يتوفر هذا الخيار فقط في وحدة تحكم الإدارة القائمة على وحدة تحكم Microsoft Management Console.

يتم دعم وسيلة برنامج التثبيت الخاصة بإزالة التطبيقات غير المتوافقة بواسطة أنواع التثبيت المختلفة. قبل تثبيت تطبيق الأمان، تتم إزالة كل التطبيقات غير المتوافقة تلقائيًا إذا كانت نافذة الخصائص الخاصة بحزمة التثبيت لتطبيق الأمان هذا (القسم **تطبيقات غير متوافقة**) تم تحديد خيار **إلغاء تثبيت التطبيقات غير المتوافقة تلقائيًا** بها.

إزالة التطبيقات غير المتوافقة عند تكوين التثبيت عن بُعد لأحد التطبيقات

يمكنك تمكين الخيار **إلغاء تثبيت التطبيقات غير المتوافقة تلقائيًا** عند تكوين التثبيت عن بُعد لأحد تطبيقات الأمان. في وحدة تحكم الإدارة القائمة على وحدة التحكم Microsoft Management Console (MMC)، يتوفر هذا الخيار في معالج التثبيت عن بُعد. في Kaspersky Security Center Web Console، يمكنك العثور على هذا الخيار في معالج نشر الحماية. عند تمكين هذا الخيار، يزيل Kaspersky Security Center التطبيقات غير المتوافقة قبل تثبيت تطبيق أمان على جهاز مُدار.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إزالة التطبيقات غير المتوافقة باستخدام معالج التثبيت عن بُعد
- Kaspersky Security Center Web Console: إزالة التطبيقات غير المتوافقة قبل التثبيت

إزالة التطبيقات غير المتوافقة من خلال مهمة محددة

لإزالة تطبيقات غير متوافقة، استخدم المهمة **إلغاء تثبيت التطبيق عن بُعد**. يجب أن تعمل هذه المهمة على الأجهزة قبل مهمة تثبيت تطبيق الأمان. على سبيل المثال، في مهمة التثبيت، يمكنك تحديد **عند إكمال مهمة أخرى** كنوع الجدول حيث تكون المهمة الأخرى هي **إلغاء تثبيت التطبيق عن بُعد**.

طريقة إلغاء التثبيت هذه مفيدة عند عدم تمكّن مثبت تطبيق الأمان من إزالة التطبيق غير متوافق بشكل صحيح.

تعليمات إرشادية لوحدة التحكم الإدارية: إنشاء مهمة .

اكتشاف الأجهزة المتصلة بالشبكة

يصف هذا القسم البحث عن أجهزة الشبكة واكتشافها.

يتيح لك Kaspersky Security Center العثور على أجهزة بناءً معيار محدد. يمكنك حفظ نتائج البحث في ملف نصي.

تتيح لك ميزة البحث والاكتشاف العثور على الأجهزة التالية:

- الأجهزة المُدارة في مجموعات الإدارة لخادم إدارة Kaspersky Security Center وخوادم الإدارة الثانوية فيه.
- الأجهزة غير المخصصة التي يديرها خادم إدارة Kaspersky Security Center وخوادم الإدارة الثانوية.

سيناريو: اكتشاف الأجهزة المتصلة بالشبكة

يجب عليك إجراء عملية اكتشاف الأجهزة قبل تثبيت تطبيقات الأمان. يتلقى خادم الإدارة معلومات عن الأجهزة المكتشفة ويسمح لك بإدارة الأجهزة من خلال السياسات. يلزم إجراء استقصاءات منتظمة للشبكة لتحديث قائمة الأجهزة المتوفرة في الشبكة.

قبل أن تبدأ استقصاء الشبكة، تأكد من تمكين بروتوكول SMB. خلاف ذلك، يتعذر على Kaspersky Security Center اكتشاف الأجهزة في الشبكة التي تم استطلاعها. لتمكين بروتوكول SMB، اتبع الإرشادات الخاصة بنظام التشغيل الخاص بك.

يتم اكتشاف الأجهزة المتصلة بالشبكة في المراحل التالية:

1. **اكتشاف الأجهزة**

يوجهك معالج البداية السريعة خلال عملية اكتشاف الأجهزة الأولي، ويساعدك على العثور على الأجهزة المتصلة بالشبكة مثل أجهزة الكمبيوتر والأجهزة اللوحية والهواتف المحمولة. ويمكنك أيضًا إجراء اكتشاف الأجهزة يدويًا.

2. **تكوين الاستقصاءات المجدولة**

حدد نوع (أنواع) الاستقصاء الذي تريد استخدامه بانتظام. وقم بتمكين الأنواع المطلوبة وتكوين جدول الاستقصاء. يمكنك الرجوع إلى التوصيات الخاصة بتكرار استقصاء الشبكة.

3. **إعداد القواعد لإضافة الأجهزة المكتشفة إلى مجموعات الإدارة (اختياري)**

إذا ظهرت أجهزة جديدة على شبكتك، فسيتم اكتشافها أثناء الاستقصاءات المنتظمة وسيتم تضمينها تلقائيًا في المجموعة **الأجهزة غير المخصصة**. يمكنك إعداد قواعد نقل الجهاز لأتمتة تخصيص الأجهزة لمجموعة **الأجهزة المُدارة**. يمكنك أيضًا تكوين قواعد الاستبقاء.

إذا تخطيت الخطوة 3، سيتم تخصيص الأجهزة المكتشفة حديثًا لمجموعة **الأجهزة غير المخصصة**. وإذا كنت تريد ذلك، يمكنك نقل هذه الأجهزة إلى المجموعة **الأجهزة المُدارة** يدويًا. أما إذا قمت بنقل الأجهزة إلى المجموعة **الأجهزة المُدارة** يدويًا، فيمكنك تحليل المعلومات حول كل جهاز وتحديد ما إذا كنت تريد نقله إلى مجموعة إدارة وإذا كان الأمر كذلك، فحدد المجموعة الدقيقة المطلوب النقل إليها.

النتائج

ينتج عن إكمال السيناريو ما يلي:

- يكتشف خادم إدارة Kaspersky Security Center الأجهزة الموجودة على الشبكة ويوفر لك معلومات حولها.
- يتم إعداد الاستقصاءات المستقبلية ويتم إجراؤها وفقًا للجدول المحدد.
- يتم ترتيب الأجهزة المكتشفة حديثًا وفقًا للقواعد التي تم تكوينها. (أو، إذا لم يكن هناك أي قواعد مكونة، فستبقى الأجهزة في مجموعة **الأجهزة غير المخصصة**).

اكتشاف الأجهزة

يصف هذا القسم أنواع اكتشاف الأجهزة المتاحة في Kaspersky Security Center ويوفر معلومات حول استخدام كل نوع.

يتلقى خادم الإدارة معلومات حول بنية الشبكة والأجهزة الموجودة على هذه الشبكة من خلال استقصاء منتظم. يتم تسجيل المعلومات في قاعدة بيانات خادم الإدارة. يمكن لخادم الإدارة استخدام الأنواع التالية من الاستقصاء:

- **استقصاء شبكة Windows**. يستطيع خادم الإدارة تنفيذ نوعين من استقصاء شبكة Windows: السريع والكامل. أثناء إجراء استقصاء سريع، يقوم خادم الإدارة باسترداد المعلومات من قائمة أسماء NetBIOS الخاصة بالأجهزة في جميع مجالات الشبكة ومجموعات العمل فقط. خلال الاستقصاء الكامل، يتم طلب المزيد من المعلومات من كل جهاز عميل مثل اسم نظام التشغيل، وعنوان IP، واسم DNS، واسم NetBIOS. يتم تمكين كل من الاستقصاء السريع والاستقصاء الكامل بصورة افتراضية. قد يفشل استقصاء شبكة Windows في اكتشاف الأجهزة، على سبيل المثال إذا كانت المنافذ UDP 137، وUDP 138، وTCP 139 مغلقة على جهاز التوجيه أو بواسطة جدار الحماية.
- **Domain controller polling**. يسترد خادم الإدارة أو نقطة التوزيع المعلومات عن بنية المجال وأسماء DNS للأجهزة المضمنة في المجال. يتم تمكين هذا النوع من الاستقصاء بشكل افتراضي. ونوصي باستخدام استقصاء وحدة تحكم المجال إذا كانت كل الأجهزة المتصلة بالشبكة أعضاء في مجال. إذا لم يتم تضمين بعض الأجهزة المتصلة بشبكة في المجال، فلا يمكن اكتشاف هذه الأجهزة عن طريق استقصاء وحدة تحكم المجال.

- **استقصاء نطاق IP** يستقصي خادم الإدارة نطاقات IP المحددة باستخدام حزم ICMP أو بروتوكول NBNS ويجمع مجموعة كاملة من البيانات على الأجهزة ضمن نطاقات IP هذه. يتم تعطيل نوع الاستقصاء هذا افتراضيًا. لا يوصى باستخدام هذا النوع من الاستقصاء إذا كنت تستخدم استقصاء شبكة Windows و/أو استقصاء Active Directory.

- **استطلاع شبكة لا تتطلب تكوينًا**. تقوم نقطة توزيع باستقصاء شبكة IPv6 باستخدام شبكات التكوين الصفري (كما يشار إلى Zeroconf). يتم تعطيل نوع الاستقصاء هذا افتراضيًا. يمكنك استخدام استقصاء شبكة لا تتطلب تكوينًا إذا كانت نقطة التوزيع تعمل بنظام Linux.

إذا قمت بإعداد وتمكين قواعد نقل الأجهزة، فسيتم تضمين الأجهزة المكتشفة حديثًا تلقائيًا في المجموعة **الأجهزة المُدارة**. في حالة عدم تمكين أي من قواعد النقل، فسيتم تضمين الأجهزة المكتشفة حديثًا تلقائيًا في المجموعة **الأجهزة غير المخصصة**.

يمكنك تعديل إعدادات اكتشاف الأجهزة لكل نوع. على سبيل المثال، قد ترغب في تعديل جدول الاستقصاء أو تعيين إما استقصاء المجال بالكامل أو فقط مجال محدد.

قبل أن تبدأ استقصاء الشبكة، تأكد من تمكين بروتوكول SMB. خلاف ذلك، يتعذر على Kaspersky Security Center اكتشاف الأجهزة في الشبكة التي تم استطلاعها. لتمكين بروتوكول SMB، اتبع الإرشادات الخاصة بنظام التشغيل الخاص بك.

استقصاء شبكة Windows

حول استقصاء شبكة Windows

أثناء إجراء استقصاء سريع، يقوم خادم الإدارة باسترداد المعلومات من قائمة أسماء NetBIOS الخاصة بالأجهزة في جميع مجالات الشبكة ومجموعات العمل فقط. خلال الاستقصاء الكامل، يتم طلب المعلومات التالية من كل جهاز عميل:

- اسم نظام التشغيل
- عنوان IP
- اسم DNS
- اسم NetBIOS

يتطلب كل من الاستقصاء السريع والكامل ما يلي:

- يجب أن تكون المنافذ UDP 137/138، و TCP 139، و UDP 445، و TCP 445 متاحة على الشبكة.
- تم تمكين بروتوكول SMB.
- يجب استخدام خدمة استعراض الكمبيوتر في Microsoft ويجب تمكين كمبيوتر الاستعراض الأساسي على خادم الإدارة.
- يجب استخدام خدمة استعراض الكمبيوتر في Microsoft ويجب تمكين كمبيوتر الاستعراض الأساسي على الأجهزة العميلة:
  - على جهاز واحد على الأقل، إذا كان عدد الأجهزة المتصلة بالشبكة لا يتجاوز 32.
  - على جهاز واحد على الأقل لكل 32 من الأجهزة المتصلة بالشبكة.

لا يمكن تشغيل الاستقصاء الكامل إلا إذا كان قد سبق تشغيل الاستقصاء السريع مرة واحدة على الأقل.

عرض وتعديل إعدادات استقصاء شبكة Windows

لتعديل خصائص استقصاء شبكة Windows:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment ← Discovery ← Windows domains**.

2. انقر على زر **Properties**.

   تفتح نافذة خصائص مجال Windows.

3. قم بتفعيل أو تعطيل استقصاء شبكة Windows باستخدام زر التبديل **Enable Windows network polling**.

4. قم بتكوين جدول الاستقصاء يجري الاستقصاء السريع كل 15 دقيقة بشكل افتراضي، ويجري الاستقصاء الكامل كل 60 دقيقة.

   خيارات جدول الاستقصاء:

   - **Every N days**

     يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

     بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

   - **Every N minutes**

     يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

   - **By days of week**

     يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

   - **Every month on specified days of selected weeks**

     يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

   - **Run missed tasks**

     إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

     إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

     إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

     يتم تعطيل هذا الخيار افتراضيًا.

5. احفظ خصائص استقصاء شبكة Windows.

   يتم حفظ الخصائص وتطبيقها إلى جميع نطاقات Windows ومجموعات عمله.

إجراء الاستطلاع يدويًا

لإجراء الاستطلاع على الفور،

انقر على **Start quick poll** أو **Start full poll**.

عند اكتمال الاستقصاء، يمكنك عرض قائمة بالأجهزة المكتشفة على صفحة **Windows domains** عن طريق تحديد خانة الاختيار الموجودة بجوار اسم مجال ثم النقر على زر **Devices**.

استقصاء نطاق IP

في البداية يحصل Kaspersky Security Center على نطاقات IP للاستقصاء من إعدادات الشبكة للجهاز المثبت عليه. إذا كان عنوان الجهاز هو 192.168.0.1 وكان قناع الشبكة الفرعية هو 255.255.255.0، فإن Kaspersky Security Center يدرج الشبكة 192.168.0.0/24 في قائمة عناوين الاستقصاء تلقائيًا. يستقصي Kaspersky Security Center جميع العناوين من 192.168.0.1 إلى 192.168.0.254.

بالنسبة لجميع المضيفين المستندين إلى Linux ضمن وحدة تحكم المجال Microsoft Active Directory أو Samba، حدد معلمتي `netbios name` و `workgroup` في الملف `/etc/samba/smb.conf`. وإلا، فقد تحتوي نتائج الاستطلاع على مضيفين مكررين.

يمكن أن يقوم Kaspersky Security Center باستقصاء نطاقات IP عن طريق البحث العكسي عن DNS أو باستخدام بروتوكول NBNS:

- **عكس بحث DNS**

  يحاول Kaspersky Security Center إجراء تحليل اسم عكسي لكل عنوان IP من النطاق المحدد لاسم DNS باستخدام طلبات DNS المعتادة. وفي حال نجاح هذه العملية، يرسل الخادم `ICMP ECHO REQUEST` (هو نفسه أمر اختبار الاتصال) إلى الاسم المستقبل. في حال رد الجهاز، يتم إضافة المعلومات عنه إلى قاعدة بيانات Kaspersky Security Center. تحليل الاسم العكسي ضروري لاستثناء أجهزة الشبكة التي يمكن أن يكون لها عنوان IP لكن ليست حواسيب، مثل طابعات الشبكة أو أجهزة التوجيه.

  تعتمد طريقة الاستقصاء هذه على خدمة DNS المحلية المكونة بشكل صحيح. يجب أن يكون به منطقة بحث عكسي. في الشركات المستخدم فيها Active Directory، توجد هذه المنطقة تلقائيًا. ولكن في هذه الشبكات لا يوفر استقصاء الشبكة الفرعية لعنوان IP معلومات أكثر من استقصاء Active Directory. وبالإضافة إلى ذلك، مديرو الشبكات الصغيرة غالبًا ما لا يقومون بتكوين منطقة البحث العكسي لأنها ليست ضرورية لعمل العديد من خدمات الشركات. ولهذه الأسباب، يكون استقصاء الشبكة الفرعية لعنوان IP معطلاً بشكل افتراضي.

- **بروتوكول NBNS**

  إذا كان تحليل الاسم العكسي غير ممكن في شبكتك لسبب ما، يستخدم Kaspersky Security Center بروتوكول NBNS لاستقصاء نطاقات عناوين IP. إذا أُرجع طلب عنوان IP اسم NetBIOS، ستتم إضافة المعلومات حول هذا الجهاز إلى قاعدة بيانات Kaspersky Security Center.

قبل أن تبدأ استقصاء الشبكة، تأكد من تمكين بروتوكول SMB. خلاف ذلك، يتعذر على Kaspersky Security Center اكتشاف الأجهزة في الشبكة التي تم استطلاعها. لتمكين بروتوكول SMB، اتبع الإرشادات الخاصة بنظام التشغيل الخاص بك.

عرض وتعديل إعدادات استقصاء نطاق IP

لعرض وتعديل خصائص استقصاء نطاق IP:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Discovery** ← **IP ranges**.
2. انقر على زر **Properties**.

   ستفتح نافذة خصائص استقصاء IP.

3. قم بتفعيل أو تعطيل استقصاء IP باستخدام زر التبديل **Allow polling**.

4. قم بتكوين جدول الاستقصاء يتم إجراء استقصاء IP كل 420 دقيقة (7 ساعات) بشكل افتراضي.

عند تحديد الفاصل الزمني للاستقصاء، تأكد أن هذا الإعداد لا يتخطى قيمة معلمة عمر عنوان IP. إذا لم يتم التحقق من عنوان IP عن طريق الاستقصاء أثناء عمر عنوان IP، سيتم إزالة عنوان IP هذا تلقائيًا من نتائج الاستقصاء. بشكل افتراضي، يبلغ العمر الافتراضي لنتائج الاستقصاء 24 ساعة لأن عناوين IP الديناميكية (المعينة باستخدام بروتوكول التكوين الديناميكي للمضيف (DHCP)) تتغير كل 24 ساعة.

خيارات جدول الاستقصاء:

- **Every N days**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **Every N minutes**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

- **By days of week**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

- **Every month on specified days of selected weeks**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

- **Run missed tasks**

إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تعطيل هذا الخيار افتراضيًا.

5. انقر على زر **Save**.

يتم حفظ الخصائص وتطبيقها على جميع نطاقات IP.

إجراء الاستطلاع يدويًا

لإجراء الاستطلاع على الفور،

انقر على **Start poll**.

إضافة نطاق IP وتعديله

في البداية يحصل Kaspersky Security Center على نطاقات IP للاستقصاء من إعدادات الشبكة للجهاز المثبت عليه. إذا كان عنوان الجهاز هو 192.168.0.1 وكان قناع الشبكة الفرعية هو 255.255.255.0، فإن Kaspersky Security Center يدرج الشبكة 192.168.0.0/24 في قائمة عناوين الاستقصاء تلقائيًا. يستقصي Kaspersky Security Center جميع العناوين من 192.168.0.1 إلى 192.168.0.254. يمكنك تعديل نطاقات IP المعينة تلقائيًا أو إضافة نطاقات IP مخصصة.

يمكنك إنشاء نطاق لعناوين IPv4 فقط. إذا قمت بتمكين استقصاء شبكة لا تتطلب تكوينًا، فسيقوم Kaspersky Security Center باستقصاء الشبكة بالكامل.

لإضافة نطاق IP جديد:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Discovery** ← **IP ranges**.
2. لإضافة نطاق IP جديد، انقر على زر **Add**.
3. في النافذة التي تفتح، حدد الإعدادات التالية:
   - **IP range name**

     اسم نطاق IP. قد ترغب في تحديد نطاق IP نفسه كاسمه، مثل "192.168.0.0/24".
   - **الفاصل الزمني لعنوان IP أو عنوان الشبكة الفرعية والقناع**

     عين نطاق IP عن طريق تحديد إما بداية عناوين IP ونهايتها أو عنوان الشبكة الفرعية وقناع الشبكة الفرعية. يمكنك كذلك تحديد أحد نطاقات IP الحالية بالنقر على زر **Browse**.
   - **IP address lifetime (hours)**

     عند تحديد هذه المعلمة، تأكد أنها تتخطى الفاصل الزمني للاستقصاء المعينة في جدول الاستقصاء. إذا لم يتم التحقق من عنوان IP عن طريق الاستقصاء أثناء عمر عنوان IP، سيتم إزالة عنوان IP هذا تلقائيًا من نتائج الاستقصاء. بشكل افتراضي، يبلغ العمر الافتراضي لنتائج الاستقصاء 24 ساعة لأن عناوين IP الديناميكية (المعينة باستخدام بروتوكول التكوين الديناميكي للمضيف (DHCP)) تتغير كل 24 ساعة.
4. حدد **Enable IP range polling** إذا كنت ترغب في استقصاء الشبكة الفرعية أو الفاصل الزمني الذي أضفته. وإذا لم تفعل ذلك، لن يتم استقصاء الشبكة الفرعية أو الفاصل الزمني الذي أضفته.
5. انقر على زر **Save**.

   سيتم إضافة نطاق IP الجديد إلى قائمة نطاقات IP.

يمكنك إجراء الاستقصاء لكل نطاق IP بشكل منفصل عن طريق استخدام زر **Start poll**. عند اكتمال الاستقصاء، يمكنك عرض قائمة بالأجهزة المكتشفة باستخدام زر **Devices**. بشكل افتراضي، تكون فترة حياة نتائج الاستقصاء هو 24 ساعة ويساوي إعداد عمر عنوان IP.

لإضافة شبكة فرعية إلى نطاق IP حالي:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Discovery** ← **IP ranges**.
2. انقر على اسم نطاق IP التي ترغب في إضافة شبكة فرعية له.
3. في النافذة التي تفتح، انقر على زر **Add**.
4. حدد شبكة فرعية باستخدام إما عنوانها وقناعها، أو باستخدام أول وآخر عنوان IP في نطاق IP. أو أضف شبكة فرعية حالية بالنقر على زر **Browse**.

5. انقر على زر **Save**.

سيتم إضافة الشبكة الفرعية الجديدة إلى نطاق IP.

6. انقر على زر **Save**.

سيتم حفظ الإعدادات الجديدة لنطاق IP.

يمكنك إضافة أي عدد تشاء من شبكة فرعية. غير مسموح بتداخل نطاقات IP المسماة، لكن الشبكات الفرعية غير المسماة داخل نطاق IP لا يوجد بها تلك القيود. يمكنك تفعيل وتعطيل الاستقصاء بشكل مستقل لكل نطاق IP.

استطلاع شبكة لا تتطلب تكوينًا

نوع الاستقصاء هذا مدعوم فقط لنقاط التوزيع المستندة إلى Linux.

يمكن لنقطة التوزيع استطلاع الشبكات التي تحتوي على أجهزة بعناوين IPv6. في هذه الحالة، لا يتم تحديد نطاقات IP وتقوم نقطة التوزيع باستقصاء الشبكة بالكامل باستخدام شبكات التكوين الصفري (يشار إليها باسم شبكة لا تتطلب تكوينًا). لبدء استخدام شبكة لا تتطلب تكوينًا، يجب عليك تثبيت أداة استعراض avahi على نقطة التوزيع.

لتمكين استقصاء شبكة IPv6:

1. في القائمة الرئيسية، انتقل إلى **IP ranges** ← **Discovery** ← **Discovery & deployment**.

2. انقر على زر **Properties**.

3. في النافذة التي تفتح، انقر على زر التبديل **Use Zeroconf to poll IPv6 networks**.

بعد ذلك، تبدأ نقطة التوزيع في استقصاء شبكتك. في هذه الحالة، يتم تجاهل نطاقات IP المحددة.

استقصاء وحدة تحكم المجال

يدعم Kaspersky Security Center الاستقصاء عن وحدة تحكم مجال Microsoft Active Directory ووحدة تحكم مجال Samba.

يتيح لك Kaspersky Security Center الاستقصاء عن وحدة تحكم مجال Samba فقط باستخدام نقطة توزيع Linux. بالنسبة لوحدة التحكم لمجال Samba، يتم استخدام Samba 4 كوحدة تحكم لمجال Active Directory .

عند استقصاء وحدة تحكم مجال، يسترد خادم الإدارة أو نقطة توزيع معلومات حول بنية المجال وحسابات المستخدمين ومجموعات الأمان وأسماء DNS للأجهزة المضمنة في المجال.

نوصي باستخدام استقصاء وحدة تحكم المجال إذا كانت كل الأجهزة المتصلة بالشبكة أعضاء في المجال. إذا لم يتم تضمين بعض الأجهزة المتصلة بشبكة في المجال، فلا يمكن اكتشاف هذه الأجهزة عن طريق استقصاء وحدة تحكم المجال.

المتطلبات الأساسية

قبل إجراء استقصاء لوحدة تحكم مجال، تأكد من السماح بالاتصالات بوحدة تحكم المجال من خلال جدار حماية أو خادم وكيل. تأكد أيضًا من تمكين البروتوكولات التالية على وحدة تحكم المجال:

- بروتوكول الوصول إلى الدليل خفيف الوزن (LDAP)
- طبقة المصادقة والأمان البسيطة (SASL)

  يُستخدم هذا البروتوكول في حالة إنشاء اتصال بوحدة تحكم المجال باستخدام مصادقة SASL. ويدعم خادم الإدارة ونقاط التوزيع آلية DIGEST-MD5 فقط.
- بروتوكول الوصول إلى الدليل خفيف الوزن فوق طبقة المآخذ الآمنة (LDAPS)

  يُستخدم هذا البروتوكول إذا كنت بحاجة إلى الاتصال بوحدة تحكم المجال عبر اتصال مشفر.

تأكد من توفر المنافذ التالية على جهاز وحدة تحكم المجال:

- 389 لبروتوكول LDAP والمصادقة البسيطة (بما في ذلك SASL)
- 636 لبروتوكول LDAPS

بالنسبة لجميع المضيفين المستندين إلى Linux ضمن وحدة تحكم المجال Microsoft Active Directory أو Samba، يجب عليك تحديد `netbios name` ومعلمات `workgroup` في الملف `/etc/samba/smb.conf`. وإلا، فقد تحتوي نتائج الاستطلاع على مضيفين مكررين.

إذا كان مجال Microsoft Active Directory يحتوي على عدة وحدات تحكم في المجال، فلن يتم دعم تحديد وحدة تحكم معينة أثناء استقصاء المجال. يتم تأسيس الاتصال مع أول وحدة تحكم في المجال تم اكتشافها. ولضمان المصادقة الصحيحة مع مجال Microsoft Active Directory، يجب أن يتضمن حقل الاسم البديل للموضوع (SAN) الخاص بالشهادة جميع عناوين وحدات تحكم المجال المضمنة في هذا المجال، بالإضافة إلى اسم NetBIOS لمجال Microsoft Active Directory.

استقصاء وحدة تحكم المجال باستخدام خادم الإدارة

يمكنك استخدام خادم الإدارة لاستقصاء وحدة تحكم مجال Microsoft Active Directory فقط.

لاستقصاء وحدة تحكم المجال باستخدام خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Discovery** ← **Domain controllers**.
2. انقر فوق **Polling settings**.

   تفتح النافذة **Domain controller polling settings**.
3. حدد الخيار **Enable domain controller polling**.
4. في القسم **Advanced settings**، حدد نطاق الاستقصاء:

   - **Poll current domain**

     حدد هذا الخيار لاستقصاء المجال الذي ينتمي إليه Kaspersky Security Center.
   - **Poll entire domain forest**

     حدد هذا الخيار لاستقصاء مجموعة المجالات التي ينتمي إليها Kaspersky Security Center.

- **Poll specified domains**

حدد هذا الخيار لاستقصاء مجال بعنوان محدد وبيانات اعتماد المستخدم.

5. إذا لزم الأمر، حدد جدول الاستقصاء. المدة الافتراضية هي ساعة واحدة. يتم استبدال البيانات التي يتم تلقيها في الاستقصاء التالي بالبيانات القديمة بشكل كامل.

تتوفر خيارات جدول الاستقصاء التالية:

- **Every N days**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **Every N minutes**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

- **By days of week**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

- **Every month on specified days of selected weeks**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

- **Run missed tasks**

إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تعطيل هذا الخيار افتراضيًا.

إذا قمت بتغيير حسابات المستخدمين في مجموعة أمان خاصة بالمجال، فسيتم عرض هذه التغييرات في Kaspersky Security Center بعد ساعة من استقصاء وحدة تحكم المجال.

6. انقر فوق **Save** لتطبيق التغييرات.

7. إذا كنت ترغب في إجراء الاستقصاء فورًا، انقر فوق الزر **Start poll**.

استقصاء وحدة تحكم المجال باستخدام نقطة توزيع

يمكنك أيضًا استقصاء وحدة تحكم مجال Microsoft Active Directory ووحدة تحكم مجال Samba باستخدام نقطة توزيع. ويمكن أن يعمل الجهاز المُدار الذي يعمل بنظام التشغيل Windows أو Linux كنقطة توزيع.

بالنسبة لنقطة توزيع نظام Linux، يتم دعم استقصاء وحدة تحكم مجال Microsoft Active Directory ووحدة تحكم مجال Samba.
بالنسبة لنقطة توزيع نظام Windows، يتم دعم استقصاء وحدة تحكم مجال Microsoft Active Directory فقط.
لا يتم دعم الاستقصاء باستخدام نقطة توزيع لنظام Mac.

لتكوين استقصاء وحدة تحكم المجال باستخدام نقطة التوزيع:

1. افتح خصائص نقطة التوزيع.

2. حدد القسم **Domain controller polling**.

3. حدد الخيار **Enable domain controller polling**.

4. حدد وحدة تحكم المجال التي تريد استقصاؤها.

إذا كنت تستخدم نقطة توزيع نظام Linux، في القسم **Poll specified domains**، انقر فوق **Add**، ثم حدد العنوان وبيانات اعتماد المستخدم لوحدة تحكم المجال.

إذا كنت تستخدم نقطة توزيع Windows، يمكنك تحديد أحد الخيارات التالية:

- **Poll current domain**
- **Poll entire domain forest**
- **Poll specified domains**

5. انقر فوق الزر **Set polling schedule** لتحديد خيارات جدول الاستقصاء إذا لزم الأمر.

يبدأ الاستقصاء فقط وفقًا للجدول الزمني المحدد. ولا يتوفر البدء اليدوي للاستقصاء.

بعد اكتمال الاستقصاء، سيتم عرض بنية المجال في القسم **Domain controllers**.

إذا قمت بإعداد وتمكين قواعد نقل الأجهزة، فسيتم تضمين الأجهزة المكتشفة حديثًا تلقائيًا في المجموعة **Managed devices**. في حالة عدم تمكين أي من قواعد النقل، فسيتم تضمين الأجهزة المكتشفة حديثًا تلقائيًا في المجموعة **Unassigned devices**.

يمكن استخدام حسابات المستخدمين المكتشفة لمصادقة المجال في Kaspersky Security Center Web Console.

المصادقة والاتصال بوحدة تحكم المجال

المصادقة والاتصال بوحدة تحكم المجال عند استقصاء مجال

عند استقصاء وحدة تحكم المجال باستخدام نقطة توزيع Linux، تحدد نقطة التوزيع بروتوكول الاتصال لتأسيس الاتصال الأولي بوحدة تحكم المجال. يتم استخدام هذا البروتوكول لجميع الاتصالات المستقبلية بوحدة تحكم المجال. عند إنشاء الاتصال الأولي بوحدة تحكم المجال، يمكنك تغيير خيارات الاتصال باستخدام علامتي عميل الشبكة `KLNAG_LDAP_TLS_REQCERT` و `KLNAG_LDAP_SSL_CACERT`. يمكنك تكوين علامات عميل الشبكة باستخدام klscflag، كما هو موضح في هذه المقالة.

يستمر الاتصال الأولي بوحدة تحكم المجال على النحو التالي:

1. تحاول نقطة توزيع Linux الاتصال بوحدة تحكم المجال عبر LDAPS.

بشكل افتراضي، يكون التحقق من الشهادة غير مطلوب. اضبط علامة `KLNAG_LDAP_TLS_REQCERT` على 1 لفرض التحقق من الشهادة.

القيم المحتملة لعلامة `KLNAG_LDAP_TLS_REQCERT`:

- `0` – يتم طلب الشهادة، لكن إذا لم يتم تقديمها أو فشل التحقق من الشهادة، فسيظل اتصال TLS قد تم إنشاؤه بنجاح (القيمة الافتراضية).
- `1` – مطلوب التحقق الصارم من شهادة خادم LDAP.

بشكل افتراضي ، عندما لا يتم تحديد العلامة KLNAG_LDAP_SSL_CACERT، يتم استخدام المسار المعتمد على نظام التشغيل إلى جهة التصديق (CA) للوصول إلى سلسلة الشهادة. استخدم العلامة KLNAG_LDAP_SSL_CACERT لتحديد مسار مخصص.

2. في حالة فشل اتصال LDAPS، تحاول نقطة توزيع Linux الاتصال بوحدة تحكم المجال عبر اتصال TCP غير مشفر باستخدام SASL (DIGEST-MD5).

تكوين العلامات

يمكنك استخدام الأداة المساعدة klscflag لتكوين العلامات.

في نقطة توزيع Linux، قم بتشغيل سطر الأوامر، ثم قم بتغيير الدليل الحالي إلى الدليل باستخدام الأداة المساعدة klscflag. بشكل افتراضي، على نقطة توزيع Linux، توجد أداة klscflag في /opt/kaspersky/ksc64/sbin.

على سبيل المثال، يفرض الأمر التالي التحقق من الشهادة:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

تكوين وحدة تحكم مجال Samba

يدعم Kaspersky Security Center وحدة تحكم مجال Linux التي تعمل على Samba 4 فقط.

تدعم وحدة تحكم مجال Samba ملحقات المخطط نفسها مثل وحدة تحكم مجال Microsoft Active Directory. يمكنك تمكين التوافق الكامل لوحدة تحكم مجال Samba مع وحدة تحكم مجال Microsoft Active Directory باستخدام ملحق مخطط Samba 4. وهذا إجراء اختياري.

نوصي بتمكين التوافق الكامل لوحدة تحكم مجال Samba مع وحدة تحكم مجال Microsoft Active Directory. وسيضمن ذلك التفاعل الصحيح بين Kaspersky Security Center ووحدة تحكم مجال Samba.

لتمكين التوافق الكامل لوحدة تحكم مجال Samba مع وحدة تحكم مجال Microsoft Active Directory:

1. نفذ الأمر التالي لاستخدام ملحق مخطط RFC2307:

```
samba-tool domain provision --use-rfc2307 --interactive
```

2. قم بتمكين تحديث المخطط في وحدة تحكم مجال Samba. لتنفيذ هذا الأمر، أضف السطر التالي إلى ملف /etc/samba/smb.conf:

```
true = schema update allowed:dsdb
```

في حالة اكتمال تحديث المخطط مع وجود خطأ، تحتاج إلى إجراء استعادة كاملة لوحدة تحكم المجال التي تعمل كمخطط رئيسي.

بالنسبة لجميع المضيفين المستندين إلى Linux ضمن وحدة تحكم المجال Samba، حدد netbios name ومعلمات workgroup في الملف / etc/samba/smb.conf. وإلا، فقد تحتوي نتائج الاستطلاع على مضيفين مكررين.

تكوين قواعد الاستبقاء للأجهزة غير المخصصة

بعد اكتمال استقصاء شبكة Windows، يتم وضع الأجهزة التي تم العثور عليها في مجموعات فرعية من مجموعة إدارة الأجهزة غير المخصصة. يمكن العثور على مجموعة الإدارة هذه في **Windows domains** ← **Discovery** ← **Discovery & deployment**. يمثل مجلد **Windows domains** المجموعة الرئيسية. يحتوي على مجموعات فرعية تمت تسميتها باسم المجالات ومجموعات العمل المطابقة التي تم العثور عليها أثناء إجراء الاستقصاء. قد تحتوي المجموعة الرئيسية أيضًا على مجموعة الإدارة للأجهزة المحمولة. يمكنك تكوين قواعد الاستبقاء للأجهزة غير المخصصة للمجموعة الرئيسية ولكل مجموعة من المجموعات الفرعية. لا تعتمد قواعد الاستبقاء على إعدادات اكتشاف الاستقصاء والعمل حتى إذا تم تعطيل اكتشاف الجهاز.

لا تؤثر قواعد الاحتفاظ بالجهاز على الأجهزة التي تحتوي على محرك أقراص واحد أو أكثر مشفر باستخدام تشفير القرص بالكامل. لا يتم حذف هذه الأجهزة تلقائيًا، يمكنك حذفها يدويًا فقط. إذا كنت بحاجة إلى حذف جهاز يحتوي على محرك أقراص مشفر، قم أولاً بفك تشفير محرك الأقراص، ثم احذف الجهاز.

قم بما يلي لتكوين قواعد الاستبقاء للأجهزة غير المخصصة:

1. في القائمة الرئيسية، انتقل إلى **Windows domains** ← **Discovery** ← **Discovery & deployment**.

2. قم بأحد الإجراءات التالية:

- لتكوين إعدادات المجموعة الأساسية، انقر على زر **Properties**.

  تفتح نافذة خصائص مجال Windows.

- لتكوين إعدادات مجموعة فرعية، انقر على اسمها.

  تفتح نافذة خصائص المجموعة الفرعية.

3. حدد الإعدادات التالية:

- **Remove the device from the group if it has been inactive for longer than (days)**

  إذا تم تمكين هذا الخيار، فيمكنك تحديد الفترة الزمنية التي يتم بعدها إزالة الجهاز تلقائيًا من المجموعة. يتم افتراضيًا توزيع هذا الخيار أيضًا على المجموعات الفرعية. الفاصل الزمني الافتراضي هو 7 أيام.

  يتم تمكين هذا الخيار افتراضيًا.

- **Inherit from parent group**

  إذا تم تمكين هذا الخيار، فإنه يتم توارث فترة الاستبقاء للأجهزة في المجموعة الحالية من المجموعة الرئيسية ولا يمكن تغييرها.

  هذا الخيار متاح فقط للمجموعات الفرعية.

  يتم تمكين هذا الخيار افتراضيًا.

- **Force inheritance in child groups**

  سيتم توزيع قيم الإعداد إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم قفل هذه الإعدادات.

  يتم تعطيل هذا الخيار افتراضيًا.

4. انقر على الزر **Accept**.

تم حفظ وتطبيق التغييرات الخاصة بك.

مخزون المعدات

تتم تعبئة قائمة المكونات (**Operations ← المستودعات ← الأجهزة**) التي تستخدمها لجرد المعدات بطريقتين: تلقائيًا ويدويًا. وبعد كل عملية استقصاء للشبكة، تتم إضافة جميع الأجهزة المكتشفة إلى القائمة تلقائيًا؛ ومع ذلك، يمكنك أيضًا إضافة الأجهزة يدويًا إذا كنت لا ترغب في استقصاء الشبكة. ويمكنك إضافة أجهزة أخرى إلى القائمة يدويًا، على سبيل المثال، أجهزة التوجيه أو الطابعات أو مكونات الأجهزة.

من خصائص جهاز يمكنك عرض معلومات مفصلة حول هذا الجهاز وتحريرها.

قد تحتوي قائمة الأجهزة المكتشفة على أنواع الأجهزة التالية:

- أجهزة الكمبيوتر
- الأجهزة الجوالة
- أجهزة الشبكة
- الأجهزة الظاهرية
- مكونات OEM
- أجهزة الكمبيوتر الطرفية
- الأجهزة المتصلة
- هواتف VoIP
- مستودعات الشبكة

يمكن للمسؤول تخصيص سمة أجهزة المؤسسة للأجهزة المكتشفة. ويمكن تخصيص هذه السمة يدويًا في خصائص جهاز، أو يمكن للمسؤول تحديد معايير للسمة التي سيتم تخصيصها تلقائيًا. في هذه الحالة، يتم تخصيص سمة أجهزة المؤسسة حسب نوع الجهاز.

يسمح Kaspersky Security Center بشطب الأجهزة. ولفعل ذلك، حدد خيار **Written off** في خصائص أحد الأجهزة. الجهاز غير معروض على قائمة الأجهزة.

يمكن للمسؤول إدارة قائمة عناصر التحكم المنطقية القابلة للبرمجة (PLC) في المجلد **الأجهزة**. تتوفر المعلومات المفصلة حول قائمة عناصر التحكم المنطقية البرمجية (PLC) في دليل مستخدم Kaspersky Industrial CyberSecurity for Nodes.

إضافة معلومات حول الأجهزة الجديدة

لإضافة معلومات حول الأجهزة الجديدة على الشبكة:

1. في القائمة الرئيسية، انتقل إلى **Operations ← المستودعات ← الأجهزة**.
2. انقر فوق الزر **Add** لفتح النافذة **جهاز جديد**.
3. في النافذة **جهاز جديد** في القائمة المنسدلة **نوع الجهاز** حدد نوع الجهاز الذي تريد إضافته.
4. انقر على**موافق**.

   تفتح نافذة خصائص الجهاز في القسم **عام**.

5. في القسم **عام** املأ حقول الإدخال بالبيانات الموجودة على الجهاز. يتضمن القسم **عام** الإعدادات التالية:

- **جهاز المؤسسة**. حدد خانة الاختيار إذا كنت ترغب في تعيين سمة المؤسسة إلى الجهاز. باستخدام هذه الميزة، يمكنك البحث عن الأجهزة في مجلد **الأجهزة**.
- **Written off**. حدد خانة الاختيار إذا كنت لا ترغب في عرض الجهاز في قائمة الأجهزة في المجلد **الأجهزة**.

6. انقر على **تطبيق** .

سيتم عرض الجهاز الجديد في مساحة عمل صفحة **الأجهزة**.

تكوين المعايير المستخدمة لتحديد أجهزة المؤسسة

لتكوين معايير اكتشاف أجهزة المؤسسة:

1. في القائمة الرئيسية، انتقل إلى **Operations** ← **المستودعات** ← **الأجهزة**.

2. في أعلى صفحة **الأجهزة**، انقر فوق الرابط **إعداد قاعدة لأجهزة المؤسسة**.
يتم استدعاء لوحة **إعداد قاعدة لأجهزة المؤسسة**.

3. في لوحة **إعداد قاعدة لأجهزة المؤسسة**، قم بتمكين **تعيين سمة جهاز المؤسسة تلقائيًا للجهاز**. وحدد أنواع الأجهزة التي يتم تعيين سمة المؤسسة لها تلقائيًا.

يؤثر هذا الخيار فقط على الأجهزة التي تمت إضافتها من خلال استقصاء الشبكة. بالنسبة للأجهزة المضافة يدويًا، اضبط سمة المؤسسة يدويًا.

4. انقر على **موافق** .

تم تكوين معايير الكشف عن أجهزة المؤسسة.

تطبيقات Kaspersky: الترخيص والتنشيط

يوضح هذا القسم ميزات Kaspersky Security Center المتعلقة بالتعامل مع مفاتيح الترخيص لتطبيقات Kaspersky المُدارة.

يسمح لك Kaspersky Security Center بإجراء توزيع مركزي لمفاتيح الترخيص الخاصة بتطبيقات Kaspersky على الأجهزة العميلة ومراقبة استخدامها وتجديد تراخيصها.

عند إضافة مفتاح ترخيص باستخدام Kaspersky Security Center، يتم حفظ إعدادات مفتاح الترخيص على خادم الإدارة. وبناءً على هذه المعلومات، يصدر التطبيق تقريرًا حول استخدام مفتاح الترخيص ويقوم بإخطار المسؤول بانتهاء صلاحية الترخيص وانتهاك قيود الترخيص المحددة في خصائص مفاتيح التراخيص. يمكنك تكوين إخطارات استخدام مفاتيح التراخيص في إعدادات خادم الإدارة.

ترخيص التطبيقات المُدارة

يجب إصدار ترخيص لتطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال تطبيق ملف المفتاح أو رمز التفعيل على كل تطبيق من التطبيقات. يمكن نشر ملف المفتاح أو رمز التفعيل بالطرق التالية:

- النشر التلقائي
- حزمة تثبيت التطبيق المُدار
- المهمة إضافة مفتاح الترخيص لتطبيق مُدار
- التفعيل اليدوي للتطبيق المُدار

يمكنك إضافة مفتاح ترخيص نشط أو احتياطي جديد بأي من الطرق المذكورة أعلاه. يستخدم تطبيق Kaspersky مفتاحًا نشطًا في الوقت الحالي ويخزن مفتاح احتياطي لتطبيقه بعد انتهاء صلاحية المفتاح النشط. يحدد التطبيق الذي تضيف مفتاح ترخيص له ما إذا كان المفتاح نشطًا أم احتياطيًا. لا يعتمد تعريف المفتاح على الطريقة التي تستخدمها لإضافة مفتاح ترخيص جديد.

النشر التلقائي

إذا كنت تستخدم تطبيقات مدارة مختلفة وكان عليك نشر ملف مفتاح محدد أو رمز تنشيط للأجهزة، فقم باختيار طرق أخرى لنشر ملف المفتاح أو رمز التفعيل هذا.

يتيح لك Kaspersky Security Center نشر مفاتيح الترخيص المتاحة تلقائيًا إلى الأجهزة. على سبيل المثال، يتم تخزين ثلاثة مفاتيح ترخيص في مستودع خادم الإدارة. لقد حددت خانة الاختيار **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها** لجميع مفاتيح الترخيص الثلاثة. تطبيق أمان Kaspersky— على سبيل المثال، تم تثبيت — Kaspersky Endpoint Security for Windows على أجهزة المؤسسة. تم اكتشاف الجهاز الجديد الذي يجب نشر المفتاح إليه. يحدد التطبيق على سبيل المثال، أنه يمكن نشر اثنين من مفاتيح التراخيص المتواجدة في المستودع إلى الجهاز وهما: مفتاح ترخيص باسم Key_1 ومفتاح ترخيص باسم Key_2. يتم نشر أحد هذين المفتاحين إلى الجهاز. وفي هذه الحالة، لا يمكن توقع مفتاح الترخيص الذي سيتم نشره إلى الجهاز لأن النشر التلقائي لمفاتيح التراخيص لا يسمح بإجراء أي نشاط للمسؤول.

عندما يتم نشر مفتاح ترخيص، تتم إعادة احتساب الأجهزة لمفتاح الترخيص هذا. ويجب عليك التأكد من أن عدد الأجهزة التي تم نشر مفتاح الترخيص إليها لا يتجاوز حد الترخيص. إذا تجاوز عدد الأجهزة حد الترخيص، فسيتم تعيين حالة جميع الأجهزة التي لم تكن مشمولة بالترخيص إلى الحالة حرج.

قبل النشر، يجب إضافة ملف المفتاح أو رمز التفعيل إلى مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - التوزيع التلقائي لمفتاح الترخيص

أو

- Kaspersky Security Center Web Console:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - التوزيع التلقائي لمفتاح الترخيص

لاحظ أنه قد لا يتم عرض مفتاح الترخيص الموزع تلقائيًا في مستودع خادم الإدارة الافتراضي في الحالات التالية:

- مفتاح الترخيص غير صالح للتطبيق.
- لا يحتوي خادم الإدارة الافتراضي على أجهزة مُدارة.
- تم استخدام مفتاح الترخيص بالفعل للأجهزة المُدارة بواسطة خادم إدارة افتراضي آخر وتم الوصول إلى الحد الأقصى لعدد الأجهزة.

إضافة ملف المفتاح أو رمز تنشيط إلى حزمة التثبيت الخاصة بتطبيق مُدار

لأسباب تتعلق بالأمان، لا يوصى باستخدام هذا الخيار. قد يتم اختراق ملف المفتاح أو رمز التفعيل المُضاف إلى حزمة التثبيت.

إذا قمت بتثبيت تطبيق مدار باستخدام حزمة تثبيت، يمكنك تحديد رمز تنشيط أو ملف المفتاح في حزمة التثبيت هذه أو في السياسة الخاصة بالتطبيق. سيتم نشر مفتاح الترخيص إلى الأجهزة المُدارة عند إجراء المزامنة التالية للجهاز مع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إنشاء حزمة توزيع
  - تثبيت التطبيقات على الأجهزة العميلة

أو

- Kaspersky Security Center Web Console: إضافة مفتاح ترخيص إلى حزمة تثبيت

النشر من خلال مهمة إضافة مفتاح الترخيص لتطبيق مُدار

إذا اخترت استخدام مهمة إضافة مفتاح الترخيص لتطبيق مُدار، يمكنك تحديد مفتاح الترخيص الذي يجب نشره إلى الأجهزة وتحديد الأجهزة بأية طريقة ملائمة، على سبيل المثال من خلال تحديد مجموعة إدارة أو تحديد جهاز.

قبل النشر، يجب إضافة ملف المفتاح أو رمز التنشيط إلى مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - نشر مفتاح ترخيص على الأجهزة العميلة

أو

- Kaspersky Security Center Web Console:
  - إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
  - نشر مفتاح ترخيص على الأجهزة العميلة

إضافة رمز التفعيل أو ملف المفتاح إلى الأجهزة يدويًا

يمكنك تنشيط تطبيق Kaspersky المثبّت محليًا من خلال استخدام الأدوات المتوفرة في واجهة التطبيق. يرجى الرجوع إلى وثائق التطبيق المثبّت.

إضافة مفتاح ترخيص إلى مستودع خادم الإدارة

لإضافة مفتاح ترخيص إلى مستودع خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **Operations** ← **Licensing** ← **Kaspersky licenses**.
2. انقر على الزر **Add**.
3. اختر ما ترغب في إضافته:
   - **Add key file**
     انقر على زر **Select key file** واذاهب إلى ملف .key الذي ترغب في إضافته.
   - **Enter activation code**
     حدد رمز التفعيل في الحقل النصي ثم انقر على الزر **Send**
4. انقر على زر **Close**.

يتم إضافة مفتاح الترخيص أو عدة مفاتيح ترخيص إلى مستودع خادم الإدارة.

إضافة مفتاح ترخيص خادم الإدارة

لإضافة مفتاح ترخيص خادم الإدارة:

1. في قائمة السياق لخادم الإدارة، حدد **خصائص**.
2. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد القسم **مفاتيح الترخيص**.
3. في القسم **مفتاح الترخيص الفعال**، انقر فوق الزر **تحرير**.
4. في النافذة التي تفتح، أضف مفتاح ترخيص بالنقر فوق الزر **إضافة**.
   سيبدأ Add license key wizard.

بعد انتهاء المعالج، يمكنك التحقق من عرض الميزات في وحدة تحكم الإدارة وفقًا للترخيص المقابل.

نشر مفتاح ترخيص على الأجهزة العميلة

يسمح لك Kaspersky Security Center Web Console بتوزيع مفتاح ترخيص على الأجهزة العميلة تلقائيًا من خلال مهمة **تفعيل التطبيق**. يمكنك استخدام المهمة لتوزيع المفاتيح على مجموعة أجهزة معينة. أثناء توزيع مفتاح ترخيص عبر المهمة، لا يتم أخذ حد الترخيص الخاص بعدد الأجهزة في الاعتبار. استخدم التوزيع التلقائي للمفاتيح لإيقاف توزيع مفتاح ترخيص تلقائيًا عند الوصول إلى حد الترخيص.

إذا قمت بتمكين التوزيع التلقائي لمفتاح ترخيص، فلا تقم بإنشاء مهمة **تفعيل التطبيق** لتوزيع هذا المفتاح على الأجهزة العميلة. وبخلاف ذلك، سيزداد الحمل على خادم الإدارة بسبب المزامنة المتكررة.

قبل النشر، أضف مفتاح ترخيص إلى مستودع خادم الإدارة.

لتوزيع مفتاح ترخيص على الأجهزة العميلة من خلال مهمة **تفعيل التطبيق**:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.
2. انقر على **Add**.

   سيبدأ **معالج المهمة الجديدة**. انتقل عبر المعالج باستخدام زر **Next**.
3. في القائمة المنسدلة **Application**، حدد التطبيق الذي تريد إضافة مفتاح ترخيص له.
4. في قائمة **Task type**، حدد مهمة **تفعيل التطبيق**.
5. في الحقل **اسم المهمة**، حدد اسم المهمة الجديدة.
6. حدد الأجهزة التي سيتم تعيين المهمة إليها.
7. في الخطوة **Selecting a license key** في المعالج، انقر فوق الرابط **إضافة مفتاح** لإضافة مفتاح الترخيص.
8. في جزء إضافة المفاتيح، أضف مفتاح الترخيص باستخدام أحد الخيارات التالية:

لا تحتاج إلى إضافة مفتاح الترخيص إلا إذا لم تقم بإضافته إلى مستودع خادم الإدارة قبل إنشاء مهمة **تفعيل التطبيق**.

- حدد الخيار **Enter activation code** لإدخال رمز تفعيل، ثم نفذ ما يلي:

  a. حدد رمز التفعيل الخاص بك، ثم انقر فوق الزر **Send**.

  تظهر معلومات حول مفتاح الترخيص في جزء إضافة المفتاح.

  b. انقر على زر **Save**.

إذا كنت ترغب في توزيع مفتاح الترخيص على الأجهزة المدارة تلقائيًا، فقم بتمكين الخيار **Automatically distribute license key to managed devices**.

يتم إغلاق جزء إضافة المفتاح.

- حدد الخيار **Add key file** لإضافة ملف مفتاح، ثم نفذ ما يلي:

a. انقر فوق الزر **Select key file**.

b. في النافذة التي تفتح، حدد ملف مفتاح، ثم انقر فوق الزر **فتح**.

تظهر معلومات عن مفتاح الترخيص في جزء إضافة مفتاح الترخيص.

c. انقر على زر **Save**.

إذا كنت ترغب في توزيع مفتاح الترخيص على الأجهزة المدارة تلقائيًا، فقم بتمكين الخيار **Automatically distribute license key to managed devices**.

يتم إغلاق جزء إضافة المفتاح.

9. حدد مفتاح الترخيص في جدول المفاتيح.

10. في خطوة **معلومات الترخيص** في المعالج، قم بإلغاء تحديد خانة الاختيار **استخدام كمفتاح احتياطي** إذا كنت تريد استبدال مفتاح الترخيص الفعال.

على سبيل المثال، يكون ذلك مطلوبًا عندما تتغير المؤسسة، ويكون مفتاح مؤسسة أخرى مطلوبًا على الجهاز؛ أو إذا تمت إعادة إصدار المفتاح، وتنتهي صلاحية الترخيص الجديد قبل الترخيص الحالي. ولتجنب الأخطاء، يجب عليك إلغاء تحديد خانة الاختيار **استخدام كمفتاح احتياطي**.

إذا كنت ترغب في معرفة المزيد من المعلومات عن المشكلات التي قد تحدث عند إضافة مفتاح ترخيص إلى Kaspersky Security Center وطرق حلها، فارجع إلى قاعدة معارف Kaspersky Security Center.

11. في خطوة **Finish task creation** ، قم بتمكين الخيار **Open task details when creation is complete** لتعديل إعدادات المهمة الافتراضية.

إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا.

12. انقر على زر **Finish**.

ينشئ المعالج المهمة. إذا قمت بتمكين الخيار **Open task details when creation is complete**، تفتح نافذة خصائص المهمة تلقائيًا. في هذه النافذة، يمكنك تحديد إعدادات المهمة العامة وتغيير الإعدادات المحددة أثناء إنشاء المهمة، إذا لزم الأمر.

يمكنك أيضًا فتح نافذة خصائص المهمة بالنقر فوق اسم المهمة التي تم إنشاؤها في قائمة المهام.

يتم إنشاء المهمة وتكوينها وعرضها في قائمة المهام.

13. لتشغيل المهمة، حددها في قائمة المهام، ثم انقر على الزر **Start**.

يمكنك أيضًا تعيين جدول لبدء مهمة في علامة التبويب **Schedule** في نافذة خصائص المهمة.

للحصول على وصف تفصيلي لإعدادات البدء المجدولة، راجع إعدادات المهمة العامة.

بعد اكتمال المهمة، يتم نشر مفتاح الترخيص على الأجهزة المحددة.

التوزيع التلقائي لمفتاح الترخيص

يتيح Kaspersky Security Center إمكانية التوزيع التلقائي لمفاتيح الترخيص على الأجهزة المدارة في حالة وجودها في مستودع مفاتيح التراخيص على خادم الإدارة.

لتوزيع أحد مفاتيح التراخيص إلى الأجهزة المدارة تلقائيًا:

1. في القائمة الرئيسية، انتقل إلى **Kaspersky licenses** ← **Licensing** ← **Operations**.

2. انقر على اسم مفتاح الترخيص الذي ترغب في توزيعه إلى الأجهزة تلقائيًا.

3. في نافذة خصائص مفتاح الترخيص التي تفتح، حدد خانة الاختيار **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها**.

4. انقر على زر **Save**.

يتم توزيع مفتاح الترخيص تلقائيًا على جميع الأجهزة المتوافقة.

يتم توزيع مفتاح الترخيص من خلال وسائل عميل الشبكة. لم يتم إنشاء مهام توزيع مفتاح الترخيص للتطبيق.

أثناء التوزيع التلقائي لمفتاح الترخيص، يتم أخذ حد الترخيص على عدد الأجهزة في الاعتبار. يتم تعيين حد الترخيص في خصائص مفتاح الترخيص. عند الوصول إلى حد الترخيص، يتوقف توزيع مفتاح الترخيص هذا على الأجهزة تلقائيًا.

لاحظ أنه قد لا يتم عرض مفتاح الترخيص الموزع تلقائيًا في مستودع خادم الإدارة الافتراضي في الحالات التالية:

- مفتاح الترخيص غير صالح للتطبيق.
- لا يحتوي خادم الإدارة الافتراضي على أجهزة مُدارة.
- تم استخدام مفتاح الترخيص بالفعل للأجهزة المُدارة بواسطة خادم إدارة افتراضي آخر وتم الوصول إلى الحد الأقصى لعدد الأجهزة.

يوزع خادم الإدارة الافتراضي تلقائيًا مفاتيح الترخيص من مخزنه ومن مستودع خادم الإدارة. نوصيك بما يلي:

- استخدم مهمة إضافة مفتاح الترخيص لتحديد مفتاح الترخيص الذي يجب نشره على الأجهزة.
- تجنب تعطيل الخيار **Allow automatic deployment of license keys from this virtual Administration Server to its devices** في إعدادات خادم الإدارة الافتراضي. وبخلاف ذلك، لن يوزع خادم الإدارة الافتراضي مفاتيح الترخيص على الأجهزة، بما في ذلك مفاتيح الترخيص من مستودع خادم الإدارة.

إذا قمت بتحديد خانة الاختيار **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها** في نافذة خصائص مفتاح الترخيص، فسيتم توزيع مفتاح الترخيص على شبكتك على الفور. وإذا لم تحدد هذا الخيار، فيمكنك استخدام مهمة لتوزيع مفتاح ترخيص لاحقًا.

لا يمتد التوزيع التلقائي لمفاتيح الترخيص التي تم تكوينها على خادم الإدارة الأساسي إلى الأجهزة التي تديرها خوادم الإدارة الثانوية غير الافتراضية.

عرض معلومات حول مفاتيح التراخيص قيد الاستخدام

لعرض قائمة بمفاتيح الترخيص المضافة إلى مستودع خادم الإدارة:

في القائمة الرئيسية، انتقل إلى **Kaspersky licenses** ← **Licensing** ← **Operations**.

تحتوي القائمة المعروضة على ملفات المفتاح ورموز التنشيط المضافة إلى مستودع خادم الإدارة.

لعرض معلومات تفصيلية عن مفتاح ترخيص:

1. في القائمة الرئيسية، انتقل إلى **Kaspersky licenses** ← **Licensing** ← **Operations**.

2. انقر على اسم مفتاح الترخيص المطلوب.

يمكنك عرض ما يلي في نافذة خصائص مفتاح الترخيص التي تفتح:

- في تبويب **General**: المعلومات الأساسية عن مفتاح الترخيص
- في تبويب **Devices**: قائمة بأجهزة العميل التي تم استخدام مفتاح الترخيص فيها لتنشيط تطبيق Kaspersky المثبت.

لعرض مفاتيح الترخيص التي تم نشرها إلى جهاز عميل محدد:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.
2. انقر على اسم الجهاز المطلوب.
3. في النافذة خصائص الجهاز التي تُفتح، حدد علامة التبويب **Applications**.
4. انقر على اسم التطبيق الذي ترغب في عرض معلومات عن مفتاح ترخيصه.
5. في نافذة خصائص التطبيق التي تفتح، حدد تبويب **General** ثم افتح قسم **License**.

يتم عرض المعلومات الأساسية حول مفاتيح الترخيص الاحتياطية.

لتحديد الإعدادات المحدثة لمفاتيح ترخيص خادم الإدارة، يقوم خادم الإدارة بإرسال طلب إلى خوادم تفعيل Kaspersky مرة واحدة يوميًا على الأقل. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة.

إزالة مفتاح ترخيص من المستودع

عندما تزيل مفتاح الترخيص المفعل لميزة إضافية لخادم الإدارة، مثل إدارة الثغرات الأمنية والتصحيحات أو إدارة الأجهزة المحمولة، تصبح الميزة المقابلة غير متوفرة. في حالة إضافة مفتاح ترخيص احتياطي، يصبح مفتاح الترخيص الاحتياطي تلقائيًا مفتاح الترخيص المفعل بعد إزالة مفتاح الترخيص المفعل السابق.

عندما تزيل مفتاح الترخيص المفعل المنشور على جهاز مُدار، سيستمر التطبيق في العمل على الجهاز المُدار.

لإزالة ملف مفتاح أو رمز تفعيل من مستودع خادم الإدارة:

1. تحقق من أن خادم الإدارة لا يستخدم ملف مفتاح أو رمز تفعيل تريد إزالته. إذا كان خادم الإدارة يفعل ذلك، فلا يمكنك إزالة المفتاح. لإجراء الفحص:
   a. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
   b. على علامة تبويب **General**، حدد القسم **License keys**.
   c. إذا تم عرض ملف المفتاح المطلوب أو رمز التفعيل المطلوب في القسم الذي يفتح، فانقر على زر **Remove active license key**، ثم قم بتأكيد العملية. بعد ذلك، لا يستخدم خادم الإدارة مفتاح الترخيص الذي تمت إزالته، ولكن يظل المفتاح في مستودع خادم الإدارة. إذا لم يتم عرض ملف المفتاح المطلوب أو رمز التنشيط، فلن يستخدمه خادم الإدارة.
2. في القائمة الرئيسية، انتقل إلى **Operations** ← **Licensing** ← **Kaspersky licenses**.
3. حدد ملف المفتاح المطلوب أو رمز التفعيل المطلوب، ثم انقر على زر **Delete**.

ستتم إزالة ملف المفتاح أو رمز التفعيل المحدد من المستودع.

يمكنك إضافة مفتاح تمت إزالته مرة أخرى أو إضافة مفتاح ترخيص جديد.

إلغاء الموافقة على اتفاقية ترخيص المستخدم النهائي

إذا قررت إيقاف حماية بعض أجهزة العميل لديك، يمكنك إلغاء اتفاقية ترخيص المستخدم النهائي لأي تطبيقات Kaspersky مُدارة. يجب أن تقوم بإلغاء تثبيت التطبيق المحدد قبل إبطال اتفاقية ترخيص المستخدم النهائي له.

يمكن إبطال اتفاقيات ترخيص المستخدم النهائي (EULA) التي تم قبولها على خادم الإدارة الافتراضي أو على خادم الإدارة الرئيسي. يمكن إبطال اتفاقيات ترخيص المستخدم النهائي (EULA) التي تم قبولها على خادم إدارة أساسي فقط.

لإلغاء EULA لتطبيقات Kaspersky المُدارة:

1. افتح نافذة خصائص خادم الإدارة، ومن تبويب **General** حدد قسم **End User License Agreements** .

   يتم عرض قائمة اتفاقيات ترخيص المستخدم النهائي—المقبولة عند إنشاء حزم التثبيت أو عند التثبيت السلس للتحديثات أو عند نشر Kaspersky Security for Mobile.

2. في القائمة، حدد اتفاقية ترخيص المستخدم النهائي التي ترغب في إبطالها.

   يمكنك عرض الخصائص التالية لاتفاقية المستخدم النهائي:

   - تاريخ قبول اتفاقية المستخدم النهائي
   - اسم حساب المستخدم الذي قبل اتفاقية ترخيص المستخدم النهائي

3. انقر على تاريخ قبول أي اتفاقية ترخيص مستخدم نهائي لفتح نافذة خصائصها التي تعرض البيانات التالية:

   - اسم حساب المستخدم الذي قبل اتفاقية ترخيص المستخدم النهائي
   - تاريخ قبول اتفاقية المستخدم النهائي
   - المعرّف الفريد (UID) لاتفاقية ترخيص المستخدم النهائي
   - النص الكامل لاتفاقية ترخيص المستخدم النهائي
   - قائمة بالكائنات (حزم التثبيت والتحديثات السلسة وتطبيقات الأجهزة المحمولة) المرتبطة باتفاقية ترخيص المستخدم النهائي وأسماء وأنواع كل منها

4. في الجزء الأسفل من نافذة خصائص اتفاقية ترخيص المستخدم النهائي، انقر على زر **Revoke License Agreement**.

> في حال وجود أي كائنات (حزم تثبيت ومهامها المقابلة) تمنع إبطال اتفاقية ترخيص المستخدم النهائي، سيتم عرض الإخطار المقابل. لا يمكنك التقدم في الإبطال حتى تحذف هذه الكائنات.

   في النافذة التي تفتح، يتم إعلامك بضرورة إلغاء تثبيت تطبيق Kaspersky المقابل لاتفاقية ترخيص المستخدم النهائي أولاً.

5. انقر على الزر لتأكيد الإبطال.

تم إبطال اتفاقية ترخيص المستخدم النهائي. إذا لم تعد معروضة في قائمة اتفاقيات الترخيص في قسم **End User License Agreements** . ستغلق نافذة خصائص اتفاقية ترخيص المستخدم النهائي، ولن يعد التطبيق مثبتًا.

تجديد تراخيص تطبيقات Kaspersky

يمكنك تجديد ترخيص تطبيق Kaspersky الذي انتهت صلاحيته أو كانت على وشك الانتهاء (في أقل من 30 يومًا).

لتجديد ترخيص منتهي الصلاحية أو على وشك الانتهاء:

1. قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل إلى **Kaspersky licenses** ← **Licensing** ← **Operations**.
- في القائمة الرئيسية، انتقل إلى **Dashboard** ← **Monitoring & reporting** ثم انقر فوق رابط **عرض التراخيص المنتهية الصلاحية** بجوار الإشعار.

يتم فتح نافذة **Kaspersky licenses** ، حيث يمكنك عرض التراخيص وتجديدها.

2. انقر على رابط **Renew license** الموجود بجوار الترخيص المطلوب.

بالنقر فوق رابط تجديد الترخيص، فإنك توافق على نقل المعلومات التالية بشأن Kaspersky Security Center إلى Kaspersky: إصداره، والترجمة التي تستخدمها، ومعرف ترخيص البرنامج (أي معرف الترخيص الذي تقوم بتجديده)، وما إذا كنت اشتريت الترخيص عبر شركة شريكة أم لا.

3. في نافذة خدمة تجديد الترخيص التي تفتح، اتبع التعليمات لتجديد ترخيص.

تم تجديد الترخيص.

في Kaspersky Security Center Web Console، يتم عرض الإشعارات عندما توشك صلاحية الترخيص على الانتهاء وفقًا للجدول التالي:

- 30 أيام قبل انتهاء الصلاحية
- 7 أيام قبل انتهاء الصلاحية
- 3 أيام قبل انتهاء الصلاحية
- 24 ساعة قبل انتهاء الصلاحية
- عندما تنتهي الصلاحية

استخدام Kaspersky Marketplace لاختيار حلول أعمال Kaspersky

Marketplace هو قسم في القائمة الرئيسية يتيح لك عرض النطاق الكامل لحلول الأعمال من Kaspersky، وتحديد الحلول التي تحتاجها، ومتابعة عملية الشراء على موقع ويب Kaspersky. يمكنك استخدام عوامل التصفية لعرض الحلول التي تناسب مؤسستك ومتطلبات نظام أمن المعلومات الخاص بك فقط. عند تحديد حل، يعيد Kaspersky Security Center توجيهك إلى صفحة الويب ذات الصلة على موقع Kaspersky الإلكتروني لمعرفة المزيد حول هذا الحل. تتيح لك كل صفحة ويب متابعة عملية الشراء أو تحتوي على إرشادات حول عملية الشراء.

في قسم **Marketplace**، يمكنك تصفية حلول Kaspersky باستخدام المعايير التالية:

- عدد الأجهزة (نقاط النهاية والخوادم وأنواع الأصول الأخرى) التي تريد حمايتها:
  - 50–250
  - 250–1000
  - أكثر من 1000

- مستوى نضج فريق أمن المعلومات في مؤسستك:
  - **الأسس**

    هذا المستوى نموذجي للمؤسسات التي لديها فريق تكنولوجيا معلومات فقط. يتم حظر أكبر عدد ممكن من التهديدات تلقائيًا.
  - **مثالي**

    هذا المستوى نموذجي للمؤسسات التي لديها فريق تكنولوجيا معلومات فقط. في هذا المستوى، تحتاج الشركات إلى حلول تمكّنها من مواجهة التهديدات والتهديدات السلعية التي تتحايل على الآليات الوقائية القائمة.
  - **خبير**

    هذا المستوى نموذجي للمؤسسات التي لديها فريق تكنولوجيا معلومات فقط. إن فريق أمن تكنولوجيا المعلومات ناضج أو أن لدى الشركة فريق SOC (مركز عمليات الأمن). الحلول المطلوبة تمكن الشركات من مواجهة التهديدات المعقدة والهجمات المستهدفة.
- أنواع الأصول التي ترغب في حمايتها.
  - **نقاط النهاية**: محطات عمل الموظفين، والآلات المادية والافتراضية، والأنظمة المدمجة
  - **الخوادم**: الخوادم المادية والافتراضية
  - **السحابة**: البيئات السحابية العامة أو الخاصة أو المختلطة؛ خدمات سحابية
  - **الشبكة**: شبكة المنطقة المحلية، والبنية التحتية لتكنولوجيا المعلومات
  - **الخدمة**: الخدمات المتعلقة بالأمان التي تقدمها Kaspersky

للعثور على حل أعمال Kaspersky وشرائه:

1. في القائمة الرئيسية، انتقل إلى **Marketplace**.

   يعرض القسم بشكل افتراضي جميع حلول الأعمال المتاحة من Kaspersky.
2. لعرض الحلول التي تناسب مؤسستك فقط، حدد القيم المطلوبة في عوامل التصفية.
3. انقر على الحل الذي تريد شراءه أو تريد معرفة المزيد عنه.

ستتم إعادة توجيهك إلى صفحة ويب الحل. يمكنك اتباع التعليمات على الشاشة لمتابعة عملية الشراء.

تكوين حماية الشبكة

يحتوي هذا القسم على معلومات حول التكوين اليدوي للسياسات والمهام، ومعلومات حول أدوار المستخدم، ومعلومات حول بناء هيكل مجموعة الإدارة والتسلسل الهرمي للمهام.

السيناريو: تكوين حماية الشبكة

ينشئ معالج البدء السريع سياسات ومهام باستخدام الإعدادات الافتراضية. قد يتبين أن هذه الإعدادات دون المستوى الأمثل أو حتى غير مسموح بها من قِبل المؤسسة. لذلك، نوصي بضبط هذه السياسات والمهام وإنشاء سياسات ومهام أخرى، إذا كانت ضرورية للشبكة لديك.

المتطلبات الأساسية

قبل البدء، تأكد من إجرائك لما يلي:

- خادم إدارة Kaspersky Security Center المُثبت
- Kaspersky Security Center Web Console المُثبت (اختياري)
- تم إكمال سيناريو التثبيت الرئيسي لـ Kaspersky Security Center
- عند اكتمال معالج البدء السريع أو إنشاء السياسات والمهام التالية يدويًا في مجموعة إدارة **الأجهزة المُدارة**:
  - سياسة Kaspersky Endpoint Security
  - مهمة جماعية لتحديث Kaspersky Endpoint Security
  - سياسة عميل الشبكة
  - البحث عن الثغرات الأمنية ومهمة التحديثات المطلوبة

يجري تكوين حماية الشبكة على المراحل التالية:

1. **إعداد ونشر سياسات وملفات تعريف السياسة لتطبيق Kaspersky**

لتكوين ونشر إعدادات لتطبيقات Kaspersky المثبتة على الأجهزة المُدارة، يمكنك استخدام نهجين مختلفين لإدارة الأمان- نهج مرتكز على الجهاز أو نهج مرتكز على المستخدم. يمكن الجمع بين هذين النهجين. لتنفيذ إدارة الأمان المرتكزة على الجهاز، يمكنك استخدام الأدوات المتوفرة في وحدة تحكم الإدارة التي تعمل في Microsoft Management Console أو Kaspersky Security Center Web Console. يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال Kaspersky Security Center Web Console فقط.

2. **تكوين المهام للإدارة عن بُعد لتطبيقات Kaspersky**

تحقق من المهام التي تم إنشاؤها بواسطة معالج البدء السريع وقم بضبطهم إذا لزم الأمر.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - يجري إعداد مهمة جماعية لتحديث Kaspersky Endpoint Security
  - جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
- Kaspersky Security Center Web Console:
  - يجري إعداد مهمة جماعية لتحديث Kaspersky Endpoint Security
  - البحث عن الثغرات الأمنية والإعدادات المطلوبة لمهمة التحديثات

إذا لزم الأمر، قم بإنشاء مهام إضافية لإدارة تطبيقات Kaspersky المثبتة على الأجهزة العميلة.

3. **تقييم وتقييد تحميل الحدث على قاعدة البيانات**

يتم نقل المعلومات حول الأحداث التي تحدث أثناء تشغيل التطبيقات المُدارة من جهاز عميل ويتم تسجيلها بقاعدة بيانات خادم الإدارة. لتقييد التحميل على خادم الإدارة، قم بتقييم وتقليل أقصى عدد من الأحداث التي يمكن تخزينها في قاعدة البيانات.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تعيين الحد الأقصى لعدد الأحداث
- Kaspersky Security Center Web Console: تعيين الحد الأقصى لعدد الأحداث

النتائج

عند إكمال هذا السيناريو، ستتم حماية شبكتك عن طريق تكوين تطبيقات ومهام وأحداث Kaspersky التي يتلقاها خادم الإدارة:

- يتم تكوين تطبيقات Kaspersky وفقًا للسياسات وملفات تعريف السياسة.
- تتم إدارة التطبيقات من خلال مجموعة من المهام.
- يتم تعيين الحد الأقصى لعدد الأحداث التي يمكن تخزينها في قاعدة البيانات.

عند إكمال تكوين حماية الشبكة، يمكنك متابعة تكوين التحديثات المنتظمة للتطبيقات وقواعد بيانات Kaspersky.

للحصول على تفاصيل حول كيفية تكوين الاستجابات التلقائية للتهديدات التي اكتشفها Kaspersky Sandbox، يرجى الإشارة إلى تعليمات Kaspersky Sandbox 2.0 عبر الإنترنت.

حول نُهج إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم

يمكنك إدارة إعدادات الأمان من منطلق مزايا الجهاز ومن منطلق أدوار المستخدم. يُطلق على النهج الأول إدارة الأمان المرتكزة على الجهاز ويُطلق على النهج الثاني إدارة الأمان المرتكزة على المستخدم. لتطبيق إعدادات تطبيق مختلفة على أجهزة مختلفة، يمكنك استخدام أي من نوعي الإدارة أو كليهما معًا. لتنفيذ إدارة الأمان المرتكزة على الجهاز، يمكنك استخدام الأدوات المتوفرة في وحدة تحكم الإدارة التي تعمل في Microsoft Management Console أو Kaspersky Security Center Web Console. يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال Kaspersky Security Center Web Console فقط.

تمكنك إدارة الأمان المرتكزة على الجهاز من تطبيق إعدادات تطبيق الأمان المختلفة على الأجهزة المدارة اعتمادًا على الميزات الخاصة بالجهاز. على سبيل المثال، يمكنك تطبيق إعدادات مختلفة على الأجهزة المخصصة في مجموعات الإدارة المختلفة. يمكنك أيضًا التمييز بين الأجهزة باستخدام تلك الأجهزة فيActive Directory أو مواصفات أجهزتهم.

تمكنك إدارة الأمان المرتكزة على المستخدم من تطبيق إعدادات تطبيق الأمان المختلفة على أدوار المستخدم المختلفة. يمكنك إنشاء عدة أدوار للمستخدم وتعيين دور مستخدم مناسب لكل مستخدم وتحديد إعدادات التطبيق المختلفة للأجهزة التي يملكها المستخدمون ذوي الأدوار المختلفة. على سبيل المثال، قد ترغب في تطبيق إعدادات تطبيق مختلفة على أجهزة المحاسبين والمتخصصين في قسم الموارد البشرية. ونتيجة لذلك، عند تنفيذ إدارة الأمان المرتكزة على المستخدم، فكل قسم من—أقسام الحسابات و الموارد البشرية—لديه تكوين الإعدادات الخاصة به لتطبيقات Kaspersky. يحدد تكوين الإعدادات إعدادات التطبيق التي يمكن تغييرها عن طريق المستخدمين والتي يتم تحديدها وقفلها بالقوة عن طريق المسؤول.

باستخدامك لنهج إدارة الأمان المرتكز على المستخدم يمكنك تطبيق إعدادات التطبيق المحددة للمستخدمين الفرديين. قد يكون هذا مطلوبًا عندما يكون للموظف دورًا فريدًا في الشركة أو عندما تريد مراقبة مشاكل الأمان المتعلقة بأجهزة شخص معين. اعتمادًا على دور هذا الموظف في الشركة، يمكنك توسيع أو تقييد حقوق هذا الشخص لتغيير إعدادات التطبيق. على سبيل المثال، قد ترغب في توسيع حقوق مسؤول النظام الذي يدير الأجهزة العميلة في مكتب محلي.

يمكنك أيضًا الجمع بين أساليب إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم. على سبيل المثال: يمكنك تكوين سياسة تطبيق محددة لكل مجموعة إدارة ثم إنشاء ملفات تعريف السياسة لدور مستخدم واحد أو عدة أدوار مستخدم في مؤسستك. في هذه الحالة يتم تطبيق السياسات وملفات تعريف السياسة بالترتيب التالي:

1. يتم تطبيق السياسات التي تم إنشاؤها لإدارة الأمان المرتكزة على الجهاز.
2. يتم تعديلهم بواسطة ملفات تعريف السياسة وفقًا لأولويات ملف تعريف السياسة.
3. يتم تعديل السياسات بواسطة ملفات تعريف السياسة المرتبطة بأدوار المستخدم.

نشر وإعداد السياسة: نهج مرتكز على الجهاز

عند قيامك بإكمال هذا السيناريو، سيتم تكوين التطبيقات على جميع الأجهزة المُدارة وفقًا لسياسات التطبيق وملفات تعريف السياسة التي تحددها.

المتطلبات الأساسية

قبل البدء، تأكد من تثبيت خادم إدارة Kaspersky Security Center و Kaspersky Security Center Web Console (اختياري). إذا قمت بتثبيت Kaspersky Security Center Web Console، فقد ترغب أيضًا في اعتبار إدارة الأمان المعتمد على المستخدم كخيار بديل أو إضافي للنهج المرتكز على الجهاز.

المراحل

يتكون سيناريو الإدارة المرتكزة على الجهاز لتطبيقات Kaspersky من الخطوات التالية:

1. **تكوين سياسات التطبيق**

   قم بتكوين إعدادات تطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال إنشاء سياسة لكل تطبيق. سيتم نشر مجموعة السياسات إلى الأجهزة العميلة.

   عند تكوين حماية شبكتك في معالج البدء السريع، سيُنشئ Kaspersky Security Center السياسة الافتراضية للتطبيقات التالية:

   - Kaspersky Endpoint Security for Windows — للأجهزة العميلة المستندة إلى Windows
   - Kaspersky Endpoint Security for Linux —للأجهزة العميلة المستندة إلى Linux

   إذا قمت باستكمال عملية التكوين باستخدام هذا المعالج، فليس عليك إنشاء سياسة جديدة لهذا التطبيق. الانتقال إلى الإعداد اليدوي لسياسة Kaspersky Endpoint Security.

   إذا كانت لديك بنية هرمية للعديد من خوادم الإدارة و/أو مجموعات الإدارة، فإن خوادم الإدارة الثانوية ومجموعات الإدارة الفرعية ترث السياسات من خادم الإدارة الرئيسي بشكلٍ افتراضي. يمكنك فرض الوراثة من خلال المجموعات الفرعية وخوادم الإدارة الثانوية لمنع أي تعديلات في الإعدادات المكونة في سياسة المنبع. إذا كنت تريد فقط أن يتم توريث جزء من الإعدادات بالقوة، فيمكنك قفلها في سياسة المنبع. ستكون بقية الإعدادات غير المقفلة متاحة للتعديل في السياسات التالية. سوف يتيح لك التسلسل الهرمي للسياسات الذي قمت بإنشائه إدارة الأجهزة بفعالية في مجموعات الإدارة.

   تعليمات للمساعدة:

   - وحدة تحكم الإدارة: إنشاء سياسة
   - Kaspersky Security Center Web Console: إنشاء سياسة

2. **إنشاء ملفات تعريف السياسة (اختياري)**

إذا أردت تشغيل الأجهزة الموجودة ضمن مجموعة إدارة واحدة ضمن إعدادات سياسة مختلفة، فقم بإنشاء ملفات تعريف سياسة لهذه الأجهزة. ملف تعريف السياسة هو مجموعة فرعية مسمّاة لإعدادات السياسة. يتم توزيع هذه المجموعة الفرعية على الأجهزة المستهدفة بالإضافة إلى السياسة، وتلحقها في حالة خاصة تُسمى شرط تفعيل ملف التعريف. تحتوي ملفات التعريف فقط على الإعدادات التي تختلف عن السياسة "الأساسية"، والتي تكون نشطة على الجهاز المُدار.

باستخدام شروط تنشيط ملف التعريف، يمكنك تطبيق ملفات تعريف سياسة مختلفة، على سبيل المثال، على الأجهزة الموجودة في وحدة محددة أو مجموعة أمان في Active Directory، مع وجود تكوين محدد للمكونات، أو تحمل علاماتمحددة. استخدم العلامات لتصفية الأجهزة التي تستوفي معايير محددة. على سبيل المثال، يمكنك إنشاء علامة تسمى Windows، وتحديد على جميع الأجهزة التي تعمل بنظام تشغيل Windows باستخدام هذه العلامة، ثم تحديد هذه العلامة كشرط تفعيل لملف تعريف سياسة. ونتيجة لذلك، ستتم إدارة تطبيقات Kaspersky المثبتة على جميع الأجهزة التي تعمل بنظام Windows عن طريق ملف تعريف السياسة الخاص بها.

تعليمات للمساعدة:

- وحدة تحكم الإدارة:
  - إنشاء ملف تعريف سياسة
  - إنشاء قاعدة تفعيل ملف تعريف سياسة
- Kaspersky Security Center Web Console:
  - إنشاء ملف تعريف سياسة
  - إنشاء قاعدة تفعيل ملف تعريف سياسة

3. **نشر السياسات وملفات تعريف السياسة على الأجهزة المدارة**

بشكل افتراضي، يعمل خادم الإدارة تلقائيًا على المزامنة مع الأجهزة المُدارة كل 15 دقيقة. يمكنك تجنب المزامنة التلقائية وتشغيل المزامنة يدويًا باستخدام الأمر فرض المزامنة. كما يتم فرض التزامن بعد إنشاء أو تغيير سياسة أو ملف تعريف سياسة. وأثناء المزامنة، يتم نشر السياسات وملفات تعريف السياسة الجديدة أو التي تم تغييرها إلى الأجهزة المُدارة.

إذا كنت تستخدم Kaspersky Security Center Web Console، يمكنك التحقق مما إذا كان قد تم تسليم السياسات وملفات تعريف السياسة إلى جهاز. يحدد Kaspersky Security Center تاريخ ووقت التسليم في خصائص الجهاز.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: المزامنة المفروضة
- Kaspersky Security Center Web Console: المزامنة المفروضة

النتائج

عند اكتمال السيناريو المرتكز على الجهاز، يتم تكوين تطبيقات Kaspersky وفقًا للإعدادات التي تم تحديدها ونشرها من خلال التسلسل الهرمي للسياسات.

سيتم تلقائيًا تطبيق سياسات التطبيق الذي تم تكوينه وملفات تعريف السياسة على الأجهزة الجديدة المُضافة إلى مجموعات الإدارة.

إعداد السياسة ونشرها: نهج مرتكز على المستخدم

يصف هذا القسم سيناريو النهج المرتكز على المستخدم للتكوين المركزي لتطبيقات Kaspersky المثبتة على الأجهزة المُدارة. عند قيامك بإكمال هذا السيناريو، سيتم تكوين التطبيقات على جميع الأجهزة المُدارة وفقًا لسياسات التطبيق وملفات تعريف السياسة التي تحددها.

يمكن تنفيذ هذا السيناريو من خلال الإصدار 13 أو إصدار أحدث من Kaspersky Security Center Web Console.

المتطلبات الأساسية

قبل البدء، تأكد من نجاح تثبيت خادم إدارة Kaspersky Security Center و Kaspersky Security Center Web Console وإكمال سيناريو التثبيت الرئيسي. قد ترغب أيضًا في اعتبار إدارة الأمان المرتكزة على المستخدم كخيار بديل أو إضافي للنهج المرتكز على المستخدم. اعرف المزيد عن نهجي الإدارة.

المعالجة

يتكون سيناريو الإدارة المرتكزة على المستخدم لتطبيقات Kaspersky من الخطوات التالية:

1. **تكوين سياسات التطبيق**

قم بتكوين إعدادات تطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال إنشاء سياسة لكل تطبيق. سيتم نشر مجموعة السياسات إلى الأجهزة العميلة.

عندما تقوم بتكوين حماية شبكتك في معالج البدء السريع، سينشئ Kaspersky Security Center السياسة الافتراضية لـ Kaspersky Endpoint Security. إذا قمت باستكمال عملية التكوين باستخدام هذا المعالج، فليس عليك إنشاء سياسة جديدة لهذا التطبيق. الانتقال إلى الإعداد اليدوي لسياسة Kaspersky Endpoint Security.

إذا كانت لديك بنية هرمية للعديد من خوادم الإدارة و/أو مجموعات الإدارة، فإن خوادم الإدارة الثانوية ومجموعات الإدارة الفرعية ترث السياسات من خادم الإدارة الرئيسي بشكلٍ افتراضي. يمكنك فرض الوراثة من خلال المجموعات الفرعية وخوادم الإدارة الثانوية لمنع أي تعديلات في الإعدادات المكونة في سياسة المنبع. إذا كنت إلا ترغب إلا في أن يتم توريث جزء من الإعدادات بالقوة، يمكنك قفلها في سياسة المنبع. ستكون بقية الإعدادات غير المقفلة متاحة للتعديل في السياسات التالية. سوف يتيح لك التسلسل الهرمي للسياسات الذي قمت بإنشائه إدارة الأجهزة بفعالية في مجموعات الإدارة.

تعليمات المساعدة: إنشاء سياسة

2. **تحديد مالكي الأجهزة**

قم بتعيين الأجهزة المُدارة إلى المستخدمين المقابلين.

تعليمات المساعدة: تعيين مستخدم كمالك لجهاز

3. **تعيين أدوار المستخدم القياسية لمؤسستك**

فكر في الأنواع المختلفة للعمل التي عادةً ما يجريها موظفو مؤسستك. يجب أن تقسم جميع الموظفين وفق أدوارهم. يمكنك على سبيل المثال تقسيمهم بناءً على أقسامهم أو مهنهم أو مناصبهم. ستحتاج بعد ذلك إلى إنشاء دور مستخدم لكل مجموعة. ضع في حسبانك أن كل دور مستخدم سيكون له ملف تعريف السياسة الخاص به ويحتوي على إعدادات التطبيق المحددة لهذا الدور.

4. **إنشاء أدوار المستخدم**

قم بإنشاء دور مستخدم وتكوينه لكل مجموعة من الموظفين مما قد حددته في الخطوة السابقة أو استخدم أدوار المستخدم المحددة مسبقًا. ستحتوي أدوار المستخدم على مجموعة من حقوق الوصول إلى مزايا التطبيق.

تعليمات المساعدة: إنشاء دور لمستخدم

5. **تعريف نطاق كل دور مستخدم**

لكل دور من أدوار المستخدم التي تم إنشاؤها، قم بتحديد المستخدمين و/أو مجموعات الأمان ومجموعات الإدارة. لا تنطبق الإعدادات المرتبطة بدور مستخدم إلا على الأجهزة التي تنتمي إلى المستخدمين الذين يملكون هذا الدور، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

تعليمات المساعدة: تحرير نطاق دور المستخدم

6. **إنشاء ملفات تعريف السياسة**

إنشاء ملف تعريف سياسة لكل دور مستخدم في مؤسستك. ملفات تعريف السياسة تحدد الإعدادات التي سيتم تطبيقها إلى التطبيقات المثبتة على أجهزة المستخدمين حسب دور كل مستخدم.

تعليمات المساعدة: إنشاء ملف تعريف سياسة

7 **ربط ملفات تعريف السياسة بأدوار المستخدم**

اربط ملفات تعريف إنشاء السياسة التي تم إنشاؤها بأدوار المستخدم. بعد ذلك سيصبح ملفات تعريف السياسة نشطًا لمستخدم له الدور المحدد. سيتم تطبيق الإعدادات في ملفات تعريف السياسة إلى تطبيقات Kaspersky المثبتة على أجهزة المستخدم.

تعليمات المساعدة: ربط ملفات تعريف السياسة بأدوار

8 **نشر السياسات وملفات تعريف السياسة على الأجهزة المدارة**

بشكل افتراضي، يعمل خادم الإدارة تلقائيًا على المزامنة مع الأجهزة المُدارة كل 15 دقيقة. وأثناء المزامنة، يتم نشر السياسات وملفات تعريف السياسة الجديدة أو التي تم تغييرها إلى الأجهزة المُدارة. يمكنك تجنب المزامنة التلقائية وتشغيل المزامنة يدويًا باستخدام أمر فرض المزامنة. عند اكتمال المزامنة يتم تسليم السياسات وملفات تعريف السياسة وتطبيقها على تطبيقات Kaspersky المثبتة.

يمكنك التحقق مما إذا قد تم تسليم السياسات وملفات تعريف السياسة إلى جهاز أم لا. يحدد Kaspersky Security Center تاريخ ووقت التسليم في خصائص الجهاز.

تعليمات المساعدة: المزامنة المفروضة

النتائج

عند اكتمال السيناريو المرتكز على المستخدم، يتم تكوين تطبيقات Kaspersky وفقًا للإعدادات التي تم تحديدها ونشرها من خلال التسلسل الهرمي السياسات وملفات تعريف السياسة.

بالنسبة لمستخدم جديد، ستحتاج إلى إنشاء حساب جديد والتخصيص للمستخدم أحد أدوار المستخدم التي تم إنشاؤها، وتخصيص الأجهزة إلى المستخدم. سيتم تلقائيًا تطبيق سياسات التطبيق الذي تم تكوينه وملفات تعريف السياسة على أجهزة هذا المستخدم.

إعدادات سياسة عميل الشبكة

لتكوين سياسة عميل الشبكة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. انقر فوق اسم سياسة عميل الشبكة.

   تفتح نافذة الخصائص لسياسة عميل الشبكة.

انظر جدول المقارنة الذي يوضح بالتفصيل كيفية تطبيق الإعدادات أدناه اعتمادًا على نوع نظام التشغيل المستخدم.

General

في علامة التبويب هذه، يمكنك تعديل حالة السياسة وتحديد توريث إعدادات السياسة:

- ضمن **Policy status**، يمكنك تحديد أحد أوضاع السياسة:
  - **Active**

    إذا تم تحديد هذا الخيار، تصبح السياسة نشطة.

    يتم تحديد هذا الخيار افتراضيًا.

- **Inactive**

إذا تم تحديد هذا الخيار، تصبح السياسة غير نشطة، ولكنها تظل مخزنة في مجلد **السياسات**. إذا لزم الأمر، يمكن تنشيط السياسة.

- في مجموعة الإعدادات **Settings inheritance**، يمكنك تكوين توريث السياسة:

- **Inherit settings from parent policy**

إذا تم تمكين هذا الخيار، يتم توريث قيم إعدادات السياسة من سياسة المجموعة ذات المستوى الأعلى؛ ولهذا يتم إلغاء تأمينها.

يتم تمكين هذا الخيار افتراضيًا.

- **Force inheritance of settings in child policies**

إذا تم تمكين هذا الخيار، يتم تنفيذ الإجراءات التالية بعد تطبيق تغييرات السياسة:

- سيتم توزيع قيم إعدادات السياسة إلى سياسات المجموعات الفرعية للإدارة، أي إلى السياسات الفرعية.

- في كتلة **توريث الإعدادات** الخاصة بالقسم **عام** في نافذة الخصائص لكل سياسة فرعية، سيتم تمكين الخيار **توريث الإعدادات من السياسة الأصلية** تلقائيًا.

إذا تم تمكين هذا الخيار، فسيتم تأمين إعدادات السياسة الفرعية.

يتم تعطيل هذا الخيار افتراضيًا.

Event configuration

يمكنك تكوين تسجيل الأحداث وإشعار الحدث في علامة التبويب هذه. يتم توزيع الأحداث وفقًا لمستوى الأهمية في الأقسام التالية في علامة التبويب **Event configuration**:

- **Functional failure**

- **Warning**

- **Info**

في كل قسم، تعرض قائمة نوع الحدث أنواع الأحداث ومصطلح تخزين الحدث الافتراضي على خادم الإدارة (بالأيام). بعد النقر على نوع الحدث، يمكنك تحديد إعدادات تسجيل الأحداث والإشعارات حول الأحداث المحددة في القائمة. بشكل افتراضي، يتم استخدام إعدادات الإخطار العام المحددة لخادم الإدارة الكامل لجميع أنواع الأحداث. ومع ذلك، يمكنك تغيير إعدادات معينة لأنواع الأحداث المطلوبة.

على سبيل المثال ، في **Warning** يمكنك تكوين **Security issue has occurred** نوع الحدث. قد تحدث مثل هذه الأحداث، على سبيل المثال ، عندما تكون مساحة القرص الحرة لنقطة التوزيع أقل من 2 جيجابايت (يلزم توفر 4 جيجابايت على الأقل لتثبيت التطبيقات وتنزيل التحديثات عن بُعد). لتكوين **Security issue has occurred** الحدث، انقر فوقه وحدد مكان تخزين الأحداث التي وقعت وكيفية الإخطار بها.

إذا اكتشف عميل الشبكة مشكلة أمان، فيمكنك إدارة هذه المشكلة باستخدام إعدادات جهاز مُدار.

Settings

في نافذة **الإعدادات**، يمكنك تكوين سياسة عميل الشبكة.

- **Distribute files through distribution points only**

إذا تم تمكين هذا الخيار، فإن عملاء الشبكة على الأجهزة المدارة يستردون التحديثات من نقاط التوزيع فقط.

إذا تم تعطيل هذا الخيار، فسيسترد عملاء الشبكة على الأجهزة المُدارة التحديثات من نقاط التوزيع أو من خادم الإدارة.

> لاحظ أن تطبيقات الأمان على الأجهزة المدارة تسترد التحديثات من مجموعة المصدر الموجودة في مهمة تحديث كل تطبيق أمان. إذا قمت بتمكين **توزيع الملفات عبر نقاط التوزيع فقط**، فتأكد من تعيين Kaspersky Security Center كمصدر تحديث في مهام التحديث.

يتم تعطيل هذا الخيار افتراضيًا.

- **Maximum size of event queue, in MB**

في هذا الحقل، يمكنك تحديد أقصى مساحة يمكن أن تشغلها قائمة انتظار الحدث على محرك الأقراص.

القيمة الافتراضية هي 2 ميجابايت.

- **Application is allowed to retrieve policy's extended data on device**

يقوم عملاء الشبكة المثبت على جهاز تتم إدارته، بنقل معلومات حول سياسة تطبيق الأمان المطبقة على تطبيق الأمان (على سبيل المثال، Kaspersky Endpoint Security for Windows). يمكنك عرض المعلومات المنقولة في واجهة تطبيق الأمان.

يقوم عملاء الشبكة بنقل المعلومات التالية:

- وقت تسليم السياسة إلى الجهاز المُدار.
- اسم السياسة النشطة في لحظة تسليم السياسة إلى الجهاز المُدار.
- اسم سياسة "خارج المكتب" في لحظة تسليم السياسة إلى الجهاز المُدار (غير متوفر لعميل الشبكة لنظام Linux).
- الاسم والمسار الكامل لمجموعة الإدارة التي كانت تحتوي على الجهاز المُدار في لحظة تسليم السياسة إلى الجهاز المُدار.
- قائمة بملفات تعريف السياسة النشطة مع أسمائها وأولوياتها في لحظة تسليم السياسة إلى الجهاز المُدار.

يمكنك استخدام المعلومات لضمان تطبيق السياسة الصحيحة على الجهاز ولأغراض استكشاف الأخطاء وإصلاحها. يتم تعطيل هذا الخيار افتراضيًا.

- **Protect the Network Agent service against unauthorized removal or termination, and prevent changes to the settings**

عند تمكين هذا الخيار، بعد تثبيت عميل الشبكة على جهاز مُدار، يتعذر إزالة المكون أو إعادة تكوينه دون الامتيازات المطلوبة. يتعذر إيقاف خدمة عميل الشبكة. هذا الخيار ليس له أي تأثير على وحدات التحكم في المجال.

قم بتمكين هذا الخيار لحماية عميل الشبكة في محطات العمل التي تعمل بحقوق المسؤول المحلي.

يتم تعطيل هذا الخيار افتراضيًا.

- **Use uninstallation password**

إذا تم تمكين هذا الخيار، يمكنك تحديد كلمة المرور لإلغاء تثبيت أداة klmover وعميل الشبكة عن بُعد بالنقر فوق الزر **تعديل**.

يتم تعطيل هذا الخيار افتراضيًا.

Repositories

في القسم **Repositories**، يمكنك تحديد أنواع الكائنات التي سيتم إرسال تفاصيلها من عميل الشبكة إلى خادم الإدارة. إذا كان تعديل بعض الإعدادات في هذا القسم ممنوعًا في سياسة عميل الشبكة، فلا يمكنك تعديلها.

- **تفاصيل عن التطبيقات التي تم تثبيتها**

إذا تم تمكين هذا الخيار، فسيتم إرسال معلومات التطبيقات المثبتة على أجهزة العميل إلى خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **Include information about patches**

يتم إرسال معلومات حول تصحيحات التطبيقات المثبتة على الأجهزة العميلة إلى خادم الإدارة. قد يؤدي تمكين هذا الخيار إلى زيادة الحمل على خادم الإدارة ونظام إدارة قواعد البيانات (DBMS)، فضلاً عن زيادة حجم قاعدة البيانات.

يتم تمكين هذا الخيار افتراضيًا. إنه متاح فقط لنظام التشغيل Windows.

- **Details of Windows Update updates**

إذا تم تمكين هذا الخيار، فسيتم إرسال معلومات تحديثات Microsoft Windows التي يجب تثبيتها على أجهزة العميل إلى خادم الإدارة.

في بعض الأحيان، حتى في حال تعطيل هذا الخيار، يتم عرض التحديثات في خصائص الجهاز في قسم **التحديثات المتوفرة**. قد يحدث هذا الأمر إذا كانت أجهزة المؤسسة، على سبيل المثال، بها ثغرات أمنية يمكن إصلاحها بواسطة هذه التحديثات.

يتم تمكين هذا الخيار افتراضيًا. إنه متاح فقط لنظام التشغيل Windows.

لم يتم إرسال المعلومات المتعلقة بتحديثات Microsoft Windows الاختيارية إلى خادم الإدارة.

- **Details of software vulnerabilities and corresponding updates**

في حالة تمكين هذا الخيار، يتم إرسال معلومات حول الثغرات الأمنية في برامج الجهات الخارجية (بما في ذلك برامج Microsoft)، والتي تم الكشف عنها على الأجهزة المُدارة، وحول تحديثات البرامج لإصلاح الثغرات الأمنية الخارجية (لا يتضمن ذلك برامج Microsoft) إلى خادم الإدارة.

يعمل تحديد هذا الخيار (**تفاصيل الثغرات الأمنية بالبرنامج والتحديثات المطابقة لها**) على زيادة تحميل الشبكة، وتحميل قرص إدارة الخادم، واستهلاك موارد عميل الشبكة.

يتم تمكين هذا الخيار افتراضيًا. إنه متاح فقط لنظام التشغيل Windows.

لإدارة تحديثات البرامج لبرامج Microsoft، استخدم خيار **تفاصيل تحديثات Windows Update**.

- **تفاصيل سجلات الأجهزة**

يقوم عميل الشبكة المثبت على جهاز بإرسال معلومات حول مكونات الجهاز إلى خادم الإدارة. يمكنك عرض تفاصيل المكونات في خصائص الجهاز.

تأكد من تثبيت الأداة المساعدة lshw على أجهزة Linux التي تريد جلب تفاصيل الأجهزة منها. قد تكون تفاصيل الأجهزة التي يتم جلبها من الأجهزة الافتراضية غير مكتملة بناءً على برنامج مراقب الأجهزة الافتراضية المستخدم.

Software updates and vulnerabilities

في القسم **Software updates and vulnerabilities**، يمكنك تكوين البحث عن تحديثات Windows وتوزيعها، وكذلك تمكين فحص الملفات التنفيذية لاكتشاف الثغرات الأمنية:

- **Use Administration Server as a WSUS server**

إذا تم تمكين هذا الخيار، فسيتم تنزيل تحديثات Windows في خادم الإدارة. يوفر خادم الإدارة تحديثات يمكن تنزيلها لخدمات Windows Update على الأجهزة العميلة في الوضع المركزي عن طريق عملاء الشبكة.

إذا تم تعطيل هذا الخيار، فلن يتم استخدام خادم الإدارة لتنزيل تحديثات Windows. في هذه الحالة، تتلقى الأجهزة العميلة تحديثات Windows بشكل مستقل.

يتم تعطيل هذا الخيار افتراضيًا.

- يمكنك تقييد تحديثات Windows التي يمكن للمستخدمين تثبيتها على أجهزتهم يدويًا باستخدام Windows Update.

في الأجهزة التي تعمل بنظام التشغيل Windows 10، إذا عثر تحديث Windows على تحديثات للجهاز، فلن يتم تطبيق الخيار الجديد الذي عثرت عليه إلا بعد تثبيت التحديثات التي تم العثور عليها **السماح للمستخدمين بإدارة تثبيت تحديثات Windows Update**.

حدد أحد العناصر في القائمة المنسدلة:

- **Allow users to install all applicable Windows Update updates**

يمكن للمستخدمين تثبيت كافة تحديثات Microsoft Windows Update القابلة للتطبيق على الأجهزة الخاصة بهم.

حدد هذا الخيار إذا كنت لا تريد التدخل في تثبيت التحديثات.

عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلًا من خادم الإدارة. يمكن ذلك في حالة عدم قيام خادم الإدارة بتنزيل هذه التحديثات بعد. ينتج عن تنزيل التحديثات من خوادم Microsoft حركة مرور إضافية.

- **Allow users to install only approved Windows Update updates**

يمكن للمستخدمين تثبيت كافة تحديثات Microsoft Windows Update القابلة للتطبيق على الأجهزة الخاصة بهم والمعتمدة من قبلك.

على سبيل المثال، قد ترغب أولًا بالتحقق من تثبيت التحديثات في بيئة اختبار والتأكد من عدم تداخلهم في عملية تشغيل الأجهزة، وبعد ذلك فقط تسمح بتثبيت تلك التحديثات المعتمدة على أجهزة العميل.

عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلًا من خادم الإدارة. يمكن ذلك في حالة عدم قيام خادم الإدارة بتنزيل هذه التحديثات بعد. ينتج عن تنزيل التحديثات من خوادم Microsoft حركة مرور إضافية.

- **Do not allow users to install Windows Update updates**

لا يمكن للمستخدمين تثبيت تحديثات Microsoft Windows Update على الأجهزة الخاصة بهم يدويًا. تم تثبيت جميع التحديثات القابلة للتطبيق كما قمت بتكوينها.

حدد هذا الخيار إذا كنت تريد إدارة تثبيت التحديثات مركزيًا.

على سبيل المثال، قد ترغب في تحسين جدول التحديث لكي لا تصبح الشبكة محملة بشكل زائد. يمكنك جدولة التحديثات بعد ساعات العمل، بحيث لا تتعارض مع إنتاجية المستخدم.

- في مجموعة الإعدادات **Windows Update search mode**، يمكنك تحديد وضع البحث عن التحديثات:

  - **Active**

  إذا تم تحديد هذا الخيار، فسيتم دعم خادم الإدارة من عميل الشبكة الذي يبدأ طلب من وكيل تحديث Windows على الجهاز العميل إلى مصدر تحديث: خوادم Windows Update أو WSUS. ثم يمرر عميل الشبكة المعلومات التي تم الحصول عليها من وكيل تحديث Windows إلى خادم الإدارة.

  لا يصبح الخيار ساريًا إلا إذا تم تحديد الخيار **الاتصال بخادم التحديث لتحديث البيانات** لمهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة.

  يتم تحديد هذا الخيار افتراضيًا.

  - **Passive**

  إذا قمت بتحديد هذا الخيار، فيقوم عميل الشبكة بشكل دوري بتمرير معلومات حول التحديثات التي تم استردادها في آخر عملية مزامنة لـ Windows Update مع مصدر التحديث إلى خادم الإدارة. في حالة عدم إجراء مزامنة لوكيل تحديث Windows مع مصدر تحديث، تصبح المعلومات حول التحديثات على خادم الإدارة غير محدثة.

  حدد هذا الخيار إذا كنت ترغب في الحصول على تحديثات من ذاكرة التخزين المؤقت لمصدر التحديث.

  - **Disabled**

  إذا كان هذا الخيار مجددًا، لا يقوم خادم الإدارة بطلب أي معلومات حول التحديثات.

  حدد هذا الخيار إذا كنت تريد، على سبيل المثال، اختبار التحديثات على جهازك المحلي أولاً.

- **Scan executable files for vulnerabilities when running them**

  إذا تم تمكين هذا الخيار، فيستم مسح الملفات التنفيذية ضوئيا للعثور على الثغرات الأمنية عند تشغيلها.

  يتم تمكين هذا الخيار افتراضيًا.

Restart management

في القسم **Restart management**، يمكنك تحديد الإجراء المراد تنفيذه إذا كان يتعين إعادة تشغيل نظام التشغيل للجهاز المدار لاستخدام أحد التطبيقات بشكل صحيح أو تثبيته أو إلغاء تثبيته:

- **Do not restart the operating system**

  لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the operating system automatically if necessary**

  يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

  سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

  يتم تحديد هذا الخيار افتراضيًا.

  - **Repeat the prompt every (min)**

  إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

  يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Force restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **Force closure of applications in blocked sessions**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

Windows Desktop Sharing

في القسم **Windows Desktop Sharing**، يمكنك تمكين وتكوين مراجعة إجراءات المسؤول التي تم إجراؤها على جهاز عن بُعد عند مشاركة الوصول إلى سطح المكتب:

- **Enable audit**

إذا تم تحديد هذا الاختيار، فسيتم تمكين التدقيق في إجراءات المسؤول التي تمت في الجهاز البعيد. يتم تسجيل إجراءات المسؤول على الجهاز البعيد:

- في سجل الحدث على الجهاز البعيد
- في ملف مزود بامتداد syslog الموجود في مجلد تثبيت عميل الشبكة على الجهاز البعيد
- في قاعدة بيانات الحدث في برنامج Kaspersky Security Center

تتوفر مراجعة إجراءات المسؤول عند تلبية الشروط التالية:

- استخدام ترخيص إدارة الثغرات الأمنية والتصحيحات بالفعل
- تمتع المسؤول بالحق في تشغيل الوصول المشترك لسطح مكتب الجهاز البعيد

إذا تم تعطيل هذا الاختيار، فسيتم تعطيل مراجعة إجراءات المسؤول على الجهاز البعيد.

يتم تعطيل هذا الخيار افتراضيًا.

- **Masks of files to monitor when read**

تحتوي القائمة على أقنعة الملف. عند تمكين المراجعة، يقوم التطبيق بمراقبة ملفات قراءة المسؤول التي تتطابق مع الأقنعة ثم يقوم بحفظ معلومات بشأن الملفات التي تمت قراءتها. تتوفر القائمة إذا تم تحديد خانة الاختيار **تمكين المراجعة**. يمكنك تحرير أُقنعة الملف وإضافة أقنعة جديدة إلى القائمة. ينبغي تحديد كل قناع ملف جديد في القائمة على سطر جديد.

يتم تحديد أقنعة الملف التالية افتراضيًا:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Masks of files to monitor when modified**

تضم القائمة أقنعة الملفات الموجودة على الجهاز البعيد. عند تمكين المراجعة، يقوم التطبيق بمراقبة التغييرات التي تم إجراؤها بواسطة المسؤول في الملفات التي تتطابق مع الأقنعة، ثم يقوم بحفظ معلومات بشأن تلك التعديلات. تتوفر القائمة إذا تم تحديد خانة الاختيار **تمكين المراجعة**. يمكنك تحرير أُقنعة الملف وإضافة أقنعة جديدة إلى القائمة. ينبغي تحديد كل قناع ملف جديد في القائمة على سطر جديد.

يتم تحديد أقنعة الملف التالية افتراضيًا:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Manage patches and updates

في القسم **Manage patches and updates**، يمكنك تكوين تنزيل التحديثات وتوزيعها، وكذلك تثبيت التصحيحات على الأجهزة المدارة:

- **Automatically install applicable updates and patches for components that have the Undefined status**

إذا تم تمكين هذا الخيار، فإنه يتم تثبيت تصحيحات Kaspersky ذات حالة الموافقة غير محدد تلقائيًا على الأجهزة المُدارة على الفور بعد تنزيلها من خوادم التحديث.

إذا تم تعطيل هذا الخيار، فسوف يتم تثبيت تصحيحات Kaspersky التي تم تنزيلها وتعيين الحالة غير محددة لها فقط بعد أن تقوم بتغيير حالتها إلى معتمدة.

يتم تمكين هذا الخيار افتراضيًا.

- **Download updates and anti-virus databases from Administration Server in advance (recommended)**

إذا تم تمكين هذا الخيار، فإنه يتم استخدام الوضع "غير متصل بالإنترنت" الخاص بتنزيل التحديثات. عند تلقي خادم الإدارة للتحديثات، يقوم بإخطار عميل الشبكة (على الأجهزة المثبت عليها) بالتحديثات المطلوبة للتطبيقات المُدارة. وعندما يتلقى عميل الشبكة معلومات حول هذه التحديثات، يقوم بتنزيل الملفات ذات الصلة من خادم الإدارة بشكلٍ مسبق. وعند أول اتصال مع عميل الشبكة، يبدأ خادم الإدارة بتنزيل التحديث. بعد أن يقوم عميل الشبكة بتنزيل جميع التحديثات إلى جهاز عميل، تصبح التحديثات متاحة للتطبيقات على هذا الجهاز.

عندما يحاول تطبيق مُدار على جهاز عميل الوصول إلى عميل الشبكة للحصول على تحديثات، يقوم عميل الشبكة بالتحقق مما إذا كانت جميع التحديثات المطلوبة متوفرة. إذا تم تلقي التحديثات من خادم الإدارة قبل فترة لا تزيد عن 25 ساعة من طلبها بواسطة تطبيق مُدار، فلن يتصل عميل الشبكة بخادم الإدارة ولكنه سيوفر بدلًا من ذلك تحديثات للتطبيق المُدار من خلال ذاكرة التخزين المؤقت المحلية. وقد يتعذر إنشاء اتصال بخادم الإدارة عند توفير عميل الشبكة لتحديثات للتطبيقات الموجودة على الأجهزة العميلة، إلا إن الاتصال غير مطلوب للتحديث.

إذا تم تعطيل هذا الخيار، فإنه لا يتم استخدام الوضع "غير متصل بالإنترنت" الخاص بتنزيل التحديثات. يتم توزيع التحديثات وفقًا لجدول مهمة تنزيل التحديث.

يتم تمكين هذا الخيار افتراضيًا.

Connectivity

يتضمن القسم **Connectivity** ثلاثة أقسام فرعية:

- **Network**
- **Connection profiles**
- **Connection schedule**

في قسم الفرعي **Network** الفرعي، يمكنك تكوين الشبكة بخادم الإدارة وتمكين استخدام منفذ UDP وتحديد رقمه.

- في مجموعة إعدادات **Connect to Administration Server**، يمكنك تكوين الاتصال بخادم الإدارة، وتحديد الفترة الزمنية للمزامنة بين أجهزة العميل وخادم الإدارة:

  - **Synchronization interval (min)**

يقوم عميل الشبكة بمزامنة الجهاز المُدار من خلال خادم الإدارة. نوصي أن تقوم بتعيين فترة المزامنة (يُشار إليها أيضًا باسم heartbeat) إلى 15 دقيقة لكل 10 000 جهاز مُدار.

إذا تم ضبط الفاصل الزمني للمزامنة على أقل من 15 دقيقة، فسيتم إجراء المزامنة كل 15 دقيقة. إذا تم ضبط الفاصل الزمني للمزامنة على 15 دقيقة أو أكثر، فسيتم إجراء المزامنة في الفاصل الزمني المحدد للمزامنة.

- **Compress network traffic**

إذا تم تمكين هذا الخيار، فستتم زيادة سرعة نقل البيانات بواسطة عميل الشبكة عن طريق تقليل مقدار المعلومات الجاري نقلها والتحميل المنخفض الناتج على خادم الإدارة.

قد يزيد التحميل على وحدة المعالجة المركزية الخاصة بالكمبيوتر العميل.

يتم تمكين خانة الاختيار هذه بشكل افتراضي.

- **Open Network Agent ports in Microsoft Windows Firewall**

إذا تم تمكين هذا الخيار، تتم إضافة المنافذ الضرورية لعمل عميل الشبكة وخادم الإدارة إلى قائمة استثناءات جدار الحماية في نظام التشغيل Microsoft Windows.

يتم تمكين هذا الخيار افتراضيًا.

- **Use SSL connection**

في حال تمكين هذا الخيار، يتم إجراء الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL.

يتم تمكين هذا الخيار افتراضيًا.

- **Use the connection gateway on a distribution point (if available), under the default connection settings**

إذا تم تمكين هذا الخيار، فسيتم استخدام بوابة الاتصال في نقطة التوزيع بموجب الإعدادات المحددة في خصائص مجموعة الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **Use UDP port**

إذا كنت بحاجة إلى عميل الشبكة للاتصال بخادم الإدارة من خلال منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد **رقم منفذ UDP**. يتم تمكين هذا الخيار افتراضيًا. ويكون منفذ UDP الافتراضي للاتصال بخادم الإدارة هو 15000.

- **UDP port number**

يمكنك في هذا الحقل إدخال اسم منفذ UDP. رقم المنفذ الافتراضي هو 15000.

تم استخدام النظام العشري للسجلات.

إذا كان الجهاز العميل يعمل بنظام التشغيل Windows XP Service Pack 2، فسوف يقوم جدار الحماية المدمج بمنع منفذ UDP 15000. يجب أن يتم فتح هذا المنفذ يدويًا.

- **Use the distribution point to force a connection to Administration Server**

حدد هذا الخيار إذا كنت قد حددت خيار **استخدم نقطة التوزيع هذه كخادم إرسال** في نافذة إعدادات نقطة التوزيع. بخلاف ذلك، لن تعمل نقطة التوزيع كخادم إرسال.

في القسم الفرعي **Connection profiles**، يمكنك تحديد إعدادات موقع الشبكة وتمكين وضع الوجود خارج المكتب عندما لا يكون خادم الإدارة متاحًا:

- **Network location settings**

تحدد إعدادات موقع الشبكة سمات الشبكة المتصل بها الجهاز العميل وتحدد قواعد تبديل عميل الشبكة من ملف تعريف اتصال خادم الإدارة إلى آخر عند تغيير سمات الشبكة هذه.

- **Administration Server connection profiles**

في هذا القسم يمكنك عرض ملفات التعريف وإضافتها لاتصال عميل الشبكة بخادم الإدارة. في هذا القسم، يمكنك أيضًا إنشاء قواعد لتحويل عميل الشبكة إلى خادم إدارة مختلف عند وقوع الأحداث التالية:

- عند اتصال الجهاز العميل بشبكة محلية مختلفة
- عندما يفقد الجهاز الاتصال بالشبكة المحلية للمؤسسة
- عندما يتم تغيير عنوان بوابة الاتصال أو تعديل عنوان خادم DNS

إن ملفات تعريف الاتصال مدعومة فقط للأجهزة التي تعمل بنظام Windows و macOS.

- **Enable out-of-office mode when Administration Server is not available**

في حال تمكين هذا الخيار، وفي حال وجود اتصال عبر ملف التعريف ذلك، ستقوم التطبيقات المثبتة على الجهاز العميل باستخدام ملفات تعريف السياسة للأجهزة التي في وضع الوجود خارج المكتب، بالإضافة إلى سياسات الوجود خارج المكتب. في حالة عدم تحديد سياسة الوجود خارج المكتب للتطبيق، سيتم استخدام السياسة المفعلة.

في حال تعطيل هذا الخيار، ستستخدم التطبيقات السياسات المفعلة.

يتم تعطيل هذا الخيار افتراضيًا.

في القسم الفرعي **Connection schedule**، يمكنك تحديد الفواصل الزمنية التي يرسل خلالها عميل الشبكة بيانات إلى خادم الإدارة:

- **Connect when necessary**

إذا حددت هذا الخيار، يتم إنشاء الاتصال عندما يتعين على عميل الشبكة إرسال بيانات إلى خادم الإدارة.

يتم تحديد هذا الخيار افتراضيًا.

- **Connect at specified time intervals**

إذا حددت هذا الخيار، يقوم عميل الشبكة بالاتصال بخادم الإدارة في فترات محددة. ويمكنك إضافة فترات زمنية متعددة للاتصال.

Network polling by distribution points

في قسم **Network polling by distribution points**، يمكنك تكوين الاستقصاء التلقائي للشبكة. يمكنك استخدام الخيارات التالية لتمكين الاستقصاء وتعيين تردده:

- **Windows network**

إذا تم تمكين الخيار، فإن خادم الإدارة يجري استقصاء الشبكة تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الروابط **تعيين جدول استقصاء سريع** و**تعيين جدول استقصاء كامل**.

إذا تم تعطيل هذا الخيار، يستطلع خادم الإدارة الشبكة مع الفاصل الزمني المحدد في الحقل **معدل استقصاءات الشبكة (بالدقائق)**.

يمكن تكوين الفاصل الزمني لاكتشاف الجهاز لإصدارات عميل الشبكة التي تسبق الإصدار 10.2 في الحقلين **معدل الاستقصاءات من مجالات Windows (دقيقة)** (لاستطلاع سريع لشبكة Windows) و**معدل استقصاءات الشبكة (بالدقائق)** (لاستطلاع كامل لشبكة Windows).

يتم تعطيل هذا الخيار افتراضيًا.

- **Zeroconf**

إذا تم تمكين هذا الخيار، فستقوم نقطة التوزيع تلقائيًا باستقصاء الشبكة باستخدام أجهزة IPv6 عن طريق شبكات التكوين الصفري (كما يشار إلى شبكة لا تتطلب تكوينًا). في هذه الحالة، يتم تجاهل استقصاء نطاق IP الذي تم تمكينه، لأن نقطة التوزيع تستقصي الشبكة بالكامل.

لبدء استخدام شبكة لا تتطلب تكوينًا، يجب استيفاء الشروط التالية:

- يجب أن تعمل نقطة التوزيع على نظام Linux.

- يجب عليك تثبيت أداة استعراض avahi على نقطة التوزيع.

إذا تم تعطيل هذا الخيار، فإن نقطة التوزيع لا تستقصي الشبكات مع أجهزة IPv6.

يتم تعطيل هذا الخيار افتراضيًا.

- **IP ranges**

إذا تم تمكين الخيار، فإن نقطة التوزيع تجري استقصاء نطاقات IP تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الزر **تعيين جدول الاستقصاء**.

إذا تم تعطيل هذا الخيار، فلن تجري نقطة التوزيع استقصاء نطاقات IP.

يمكن تكوين تردد استقصاء نطاق IP لإصدارات عميل الشبكة السابقة لـ 10.2 في الحقل **الفاصل الزمني للاستقصاء (دقيقة)**. يتوفر الحقل إذا تم تمكين الخيار.

يتم تعطيل هذا الخيار افتراضيًا.

- **Domain controllers**

إذا تم تمكين الخيار، فإن نقطة التوزيع تجري استقصاء Active Directory تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الرابط **تعيين جدول الاستقصاء**.

إذا تم تعطيل هذا الخيار، فلن يجري خادم الإدارة استقصاء Active Directory.

يمكن تكوين تردد استقصاء Active Directory لإصدارات عميل الشبكة السابقة لـ 10.2 في الحقل **الفاصل الزمني للاستقصاء (دقيقة)**. يكون الحقل متاحًا إذا تم تمكين هذا الخيار.

يتم تعطيل هذا الخيار افتراضيًا.

إذا تم تمكين الخيار، فإن نقطة التوزيع تجري استقصاء وحدات تحكم المجال تلقائيًا وفقًا للجدول الذي كونته عن طريق النقر فوق الزر **تعيين جدول الاستقصاء**.

إذا تم تعطيل هذا الخيار، فلن تجري نقطة التوزيع استقصاء وحدات تحكم المجال.

يمكن تكوين تردد استقصاء وحدة تحكم المجال لإصدارات عميل الشبكة السابقة لـ 10.2 في الحقل **الفاصل الزمني للاستقصاء (دقيقة)**. يكون الحقل متاحًا إذا تم تمكين هذا الخيار.

يتم تعطيل هذا الخيار افتراضيًا.

Network settings for distribution points

إذا كانت نقاط التوزيع الخاصة بك تستخدم خادمًا وكيلاً عند الاتصال بالإنترنت، ففي القسم **Network settings for distribution points**، يمكنك تحديد الإعدادات التالية:

- **Use proxy server**

- **Address**

- **Port number**

- **Bypass proxy server for local addresses**

إذا تم تمكين هذا الخيار، فلن يتم استخدام خادم الوكيل للاتصال بالأجهزة على الشبكة المحلية.

يتم تعطيل هذا الخيار افتراضيًا.

- **Proxy server authentication**

إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **User name**
- **Password**

KSN Proxy (distribution points)

في القسم **KSN Proxy (distribution points)**، يمكنك تكوين التطبيق لاستخدام نقطة التوزيع لإعادة توجيه طلبات Kaspersky Security Network (KSN) من الأجهزة المدارة:

- **Enable KSN Proxy on the distribution point side**

تعمل خدمة وكيل KSN على الجهاز المستخدم كنقطة توزيع. استخدم هذه الميزة لإعادة توزيع حركة مرور البيانات في الشبكة وتحسينها.

ترسل نقطة التوزيع إحصاءات KSN المُدرجة في بيان Kaspersky Security Network إلى Kaspersky.

يتم تعطيل هذا الخيار افتراضيًا. يسري تمكين هذا الخيار فقط في حالة تمكين الخيارين **Use Administration Server as a proxy server** و**I agree to use Kaspersky Security Network** في نافذة خصائص خادم الإدارة.

يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل خادم KSN على هذه العقدة.

- **Forward KSN requests to Administration Server**

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المدارة إلى خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **Access KSN Cloud/KPSN directly over the internet**

تعيد نقطة التوزيع توجيه طلبات KSN من الأجهزة المُدارة إلى KSN Cloud أو KPSN. يتم أيضًا إرسال طلبات KSN – التي تم إنشاؤها على نقطة التوزيع نفسها – مباشرةً إلى KSN Cloud أو PKSN.

لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى KPSN مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KPSN، فقم بتمكين خيار **توجيه طلبات KSN إلى خادم الإدارة** لكل نقطة توزيع.

لا يمكن لنقاط التوزيع التي لديها الإصدار 12 المثبت من Network Agent (أو إصدار أقدم)، الوصول إلى KPSN مباشرةً.

- **Port**

رقم منفذ TCP الذي ستستخدمه الأجهزة المُدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

- **UDP port**

إذا كنت بحاجة إلى عميل الشبكة للاتصال بخادم الإدارة من خلال منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد **رقم منفذ UDP**. يتم تمكين هذا الخيار افتراضيًا. ويكون منفذ UDP الافتراضي للاتصال بخادم الإدارة هو 15000.

Updates (distribution points)

في هذا القسم **Updates (distribution points)** يمكنك تمكي ميزة تنزيل الملفات المختلفة، بحيث تأخذ نقاط التوزيع التحديثات في شكل ملفات مختلفة من خوادم تحديث Kaspersky.

Local account management (Linux only)

يتضمن القسم **Local account management (Linux only)** ثلاثة أقسام فرعية:

- **User certificates management**
- **Add or edit applicable local administrator groups**
- **Upload a reference file to protect the sudoers file on the user's device from changes**

في القسم الفرعي **User certificates management**، يمكنك تحديد شهادات الجذر التي تريد تثبيتها. ويمكن استخدام هذه الشهادات، على سبيل المثال، للتحقق من صحة مواقع الويب أو خوادم الويب.

- **Install root certificates**

  إذا تم تمكين هذا الخيار، فسيتم تثبيت الشهادات المضافة إلى الجدول على الأجهزة المحددة.

  إذا تم تعطيل هذا الخيار، فلن يتم تثبيت أي شهادات على الأجهزة المحددة.

  يتم تعطيل هذا الخيار افتراضيًا.

- **إضافة**

  يؤدي الضغط على هذا الزر إلى فتح نافذة يمكنك من خلالها إضافة شهادة.

  يجب أن يكون حجم الشهادة أقل من 10 ميجا بايت.

  يدعم Kaspersky Security Center الشهادات بالامتدادات CER و CRT و CERT و PEM و KEY.

في القسم الفرعي **Add or edit applicable local administrator groups**، يمكنك إدارة مجموعات المسؤولين المحليين. ويتم استخدام هذه المجموعات، على سبيل المثال، عند إلغاء حقوق المسؤول المحلي. ويمكنك أيضًا التحقق من قائمة حسابات المستخدمين المتميزين باستخدام **الإبلاغ عن مستخدمي الأجهزة المميزة (Linux فقط)**.

- **إضافة**

  يؤدي النقر على هذا الزر إلى فتح نافذة، حيث يمكنك إضافة مجموعة مسؤول محلي.

- **تحرير**

  يؤدي النقر على هذا الزر إلى فتح نافذة، حيث يمكنك تحرير مجموعة المسؤول المحلي.

  يصبح هذا الزر متاحًا إذا تم تحديد مربع الاختيار بجوار مجموعة المسؤولين المحليين.

- **حذف**

  يؤدي الضغط على هذا الزر إلى حذف مجموعة المسؤولين المحليين المحددة من الجدول.

  يصبح هذا الزر متاحًا إذا تم تحديد مربع الاختيار بجوار مجموعة المسؤولين المحليين.

في القسم الفرعي **Upload a reference file to protect the sudoers file on the user's device from changes**، يمكنك تكوين التحكم في ملف sudoers. ويتم تعريف المجموعات المميزة ومستخدمي الأجهزة بواسطة ملف sudoers على الجهاز. ويوجد ملف sudoers في `/etc/sudoers`. ويمكنك تحميل ملف sudoers مرجعي لحماية ملف sudoers من التغييرات. وسيؤدي هذا إلى منع التغييرات غير المرغوب فيها في ملف sudoers.

قد يؤدي ملف sudoers المرجعي غير الصالح إلى حدوث خلل في جهاز المستخدم.

- **Control sudoers file**

  إذا تم تمكين هذا الخيار، سيتم استبدال ملف sudoers بملف sudoers المرجعي الحالي.

  إذا تم تعطيل هذا الخيار، سيبقى ملف sudoers دون تغيير.

  يتم تعطيل هذا الخيار افتراضيًا.

- **Reference sudoers file**

  يعرض هذا الحقل اسم ملف sudoers المرجعي الذي تم تحميله.

- **Upload**

  يؤدي النقر على هذا الزر إلى فتح نافذة، حيث يمكنك تحميل ملف sudoers مرجعي.

- **Current reference sudoers file**

  يؤدي النقر فوق هذا الزر إلى إظهار محتويات ملف sudoers الحالي.

Revision history

في علامة التبويب هذه، يمكنك عرض قائمة مراجعات السياسة و الرجوع إلى التغييرات السابقة التي تم إجراؤها على السياسة إذا لزم الأمر.

مقارنة إعدادات نهج عميل الشبكة حسب أنظمة التشغيل

يوضح الجدول أدناه إعدادات سياسة عميل الشبكة التي يمكنك استخدامها في وحدة تحكم الإدارة و Kaspersky Security Center Web Console لتكوين عميل الشبكة مع نظام تشغيل محدد.

إعدادات نهج عميل الشبكة: المقارنة حسب أنظمة التشغيل

قسم السياسة	Windows	macOS	Linux
General	✓	✓	✓
Event configuration	✓	✓	✓
Settings	✓	✓	✓ تتوفر الميزات التالية: • **Distribute files through distribution points only** • **الحجم الأقصى لقائمة انتظار الحدث، بالميجابايت** • **يُسمح للتطبيق باسترداد بيانات السياسة الموسعة على الجهاز**
Repositories	✓	✓ يتوفر خيار **Hardware registry details**.	✓ تتوفر الميزات التالية: • **تفاصيل عن التطبيقات التي تم تثبيتها** • **تفاصيل سجلات الأجهزة**

قسم السياسة	Windows	macOS	Linux
Software updates and vulnerabilities	✓	—	—
Restart management	✓	—	—
Windows Desktop Sharing	✓	—	—
Manage patches and updates	✓	—	—
Connectivity ← Network	✓	✓	✓ فيما عدا خيار Open Network Agent ports in Microsoft Windows Firewall .
Connectivity ← Connection profiles	✓	✓	—
Connectivity ← Connection schedule	✓	✓	✓
Network polling by distribution points	✓ تتوافر فقط خيارات Windows network و IP ranges وDomain controllers.	—	✓ تتوفر الميزات التالية: • Zeroconf • IP ranges • Domain controllers
Network settings for distribution points	✓	✓	✓
KSN Proxy (distribution points)	✓	—	✓
Updates (distribution points)	✓	—	✓
Revision history	✓	✓	✓

تمكين وتعطيل وضع الاستهلاك منخفض الموارد لعميل الشبكة

يسمح لك وضع الاستهلاك المنخفض للموارد بالحد من استخدام ذاكرة الوصول العشوائي (RAM) الخاصة بعميل الشبكة المثبت على جهاز العميل. وبشكل افتراضي، يتم تعطيل وضع الاستهلاك المنخفض للموارد.

في وضع الاستهلاك المنخفض للموارد، لا يتم تنفيذ الوظائف التالية:

- لا يمكن تعيين عميل الشبكة للعمل كنقطة توزيع (إما يدويًا أو تلقائيًا).
- لا يسجل عميل الشبكة معلومات حول حالة عميل الشبكة في ملف نصي منفصل.
- لا يدعم عميل الشبكة النموذج غير المتصل لتنزيل التحديث.
- تم تعطيل المكونات والعمليات التالية:
  - الحصول على معلومات عن التحديثات والثغرات الأمنية من جهة خارجية.
  - تشغيل عميل KSN على جانب نقطة التوزيع.
  - تحميل التحديثات إلى مستودع نقطة التوزيع.
  - تجاوز كتلة خادم DNS.
  - الحصول على معلومات حول مساحة القرص الخالية.

تستأنف المكونات والعمليات عملها بعد تعطيل وضع الاستهلاك المنخفض للموارد.

لتمكين وضع الاستهلاك المنخفض للموارد:

1. نفذ الأمر التالي في سطر الأوامر على الجهاز العميل:

```
klscflag -fset -pv klnagent -n<NetworkAgent\Kaspersky Lab\(x86) Program files\:C
KLNAG_FLAG_TEST_VM_PERF -t d -v 1
```

2. أعد تشغيل عميل الشبكة.

3. للتحقق من تمكين وضع الاستهلاك المنخفض للموارد، في نظام التشغيل Windows، افتح **عارض الأحداث**، ثم حدد **سجلات التطبيقات والخدمات** ← **Kaspersky Event Log**.

   تأكد أن السجل يحتوي على أحداث مثل **Kaspersky Security Center Network Agent الذي يعمل في وضع الاستهلاك المنخفض للموارد**.

   تم تمكين وضع الاستهلاك المنخفض للموارد.

لتعطيل وضع الاستهلاك المنخفض للموارد:

1. نفذ الأمر التالي في سطر الأوامر على الجهاز العميل:

```
klscflag -fset -pv klnagent -n<NetworkAgent\Kaspersky Lab\(x86) Program files\:C
KLNAG_FLAG_TEST_VM_PERF -t d -v 0
```

2. أعد تشغيل عميل الشبكة.

3. للتحقق من تعطيل وضع الاستهلاك المنخفض للموارد، في نظام التشغيل Windows، افتح **عارض الأحداث**، ثم حدد **سجلات التطبيقات والخدمات** ← **Kaspersky Event Log**.

   تأكد أن حدث klnagent الأخير لا يحتوي على الرسالة **يعمل Kaspersky Security Center Network Agent في وضع الاستهلاك المنخفض للموارد**.

   تم تعطيل وضع الاستهلاك المنخفض للموارد.

يمكنك أيضًا تمكين وضع الاستهلاك المنخفض للموارد عن بُعد باستخدام مهمة Execute scripts remotely.

تكوين إعدادات الحماية للتطبيقات المدارة

لتكوين إعدادات الحماية لتطبيقات Kaspersky المدارة، يمكنك استخدام السياسات.

للمزيد من المعلومات عن تكوين سياسات Kaspersky Endpoint Security، راجع التعليمات المقابلة:

- تعليمات Kaspersky Endpoint Security for Windows
- دعم Kaspersky Endpoint Security for Linux
- دعم Kaspersky Endpoint Security for Mac

الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security

إن خيار الجدولة الأمثل والموصى به لإصدار Kaspersky Endpoint Security هو **When new updates are downloaded to the repository** عندما تكون خانة الاختيار **Use automatically randomized delay for task starts** محددة.

إزالة تحديثات تطبيقات أو برامج عن بُعد

لإزالة تطبيقات أو تحديثات برامج عن بُعد من الأجهزة المحددة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.

2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة **Uninstall application remotely**.

4. حدد اسم المهمة التي ترغب في إنشائها.

   لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

5. حدد الأجهزة التي سيتم تعيين المهمة إليها:

6. حدد نوع البرامج التي ترغب في إزالتها ثم حدد التطبيقات أو التحديثات أو التصحيحات التي ترغب في إزالتها:

   - **Uninstall managed application**

   سيتم عرض قائمة بتطبيقات Kaspersky. حدد التطبيق الذي ترغب في إزالته.

   - **Uninstall incompatible application**

   ستظهر قائمة من التطبيقات غير المتوافقة مع تطبيقات أمان Kaspersky أو Kaspersky Security Center. حدد خانات الاختيار الموجودة بجوار التطبيقات التي ترغب في إزالتها.

   - **Uninstall application from applications registry**

   افتراضيًا، سترسل عملاء الشبكة إلى خادم الإدارة معلومات عن التطبيقات المثبتة على الأجهزة المُدارة. يتم تخزين قائمة التطبيقات المثبتة في سجل التطبيقات.

   لتحديد تطبيق من سجل التطبيقات:

   a. انقر على حقل **Application to uninstall** ثم حدد التطبيق الذي ترغب في إزالته.

   إذا حددت Kaspersky Security Center Network Agent، فعند تشغيل المهمة، تعرض الحالة مكتمل بنجاح أن عملية الإزالة بدأت. في حالة إزالة Kaspersky Security Center Network Agent، فلن تتغير الحالة. إذا فشلت المهمة، تتغير الحالة إلى فاشلة.

   b. حدد خيارات إلغاء التثبيت:

   - **Uninstallation mode**

   حدد الطريقة التي ترغب في إزالة التطبيق بها:

   - **Define uninstallation command automatically**

   إذا كان للبرنامج أمر إلغاء تثبيت حدده بائع التطبيق، سيستخدم Kaspersky Security Center هذا الأمر. ننصح بتحديد هذا الخيار.

   - **Specify uninstallation command**

   حدد هذا الخيار إذا كنت ترغب في تحديد أمرك الخاص لإلغاء تثبيت التطبيق.

ننصح بأن تحاول أولاً إزالة التطبيق باستخدام خيار **Define uninstallation command automatically**. إذا تعذر إلغاء التثبيت من خلال الأمر المحدد تلقائيًا، عندها استخدم أمرك الخاص.

اكتب أمر تثبيت في الحقل ثم حدد الخيار التالي:

Use this command for uninstallation only if the default command was not autodetected

يتحقق Kaspersky Security Center مما إذا كان التطبيق المحدد له أمر إلغاء تثبيت قد حدده بائع التطبيق أم لا. في حال العثور على الأمر، سيستخدمه Kaspersky Security Center بدلاً من الأمر المحدد في حقل **Command for application uninstallation**.

ننصح بأن تقوم بتفعيل هذا الخيار.

- **Perform restart after successful application uninstallation**

إذا طلب التطبيق إعادة تشغيل نظام التشغيل على الجهاز المُدار بعد إلغاء التثبيت بنجاح، سيتم إعادة تشغيل نظام التشغيل تلقائيًا.

- **Uninstall the specified application update, patch, or third-party application**

يتم عرض قائمة بالتحديثات والتصحيحات وتطبيقات الأطراف الخارجية. حدد العنصر الذي ترغب في إزالته.

القائمة المعروضة هي قائمة عامة بالتطبيقات والتحديثات، ولا تتوافق مع التطبيقات والتحديثات المثبتة على الأجهزة المُدارة. قبل تحديد عنصر، ننصح بأن تتأكد أن التطبيق أو التحديث مثبت على الأجهزة المحددة في نطاق المهمة. يمكنك عرض قائمة الأجهزة المثبت عليها التطبيق أو التحديث من خلال نافذة الخصائص.

لعرض قائمة الأجهزة:

a. انقر على اسم التطبيق أو التحديث.

تفتح نافذة الخصائص.

b. افتح قسم **Devices**.

يمكنك كذلك عرض قائمة بالتطبيقات والتحديثات المثبتة في نافذة خصائص الجهاز.

7. حدد كيف ستقوم أجهزة العميل بتنزيل أداة إلغاء التثبيت:

- **Using Network Agent**

يتم تسليم الملفات إلى أجهزة العميل بواسطة عميل الشبكة المثبت على أجهزة العميل تلك.

في حال تعطيل هذا الخيار، سيتم تسليم الملفات باستخدام أدوات Microsoft Windows.

ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة.

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

يتم إرسال الملفات إلى الأجهزة العميلة باستخدام أدوات نظام تشغيل خادم الإدارة. يمكنك تفعيل هذا الخيار إذا لم يتم تثبيت عميل شبكة على الجهاز العميل، لكن الجهاز العميل موجود في نفس الشبكة الموجود عليها خادم الإدارة.

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

سيتم نقل الملفات إلى أجهزة العميل باستخدام أدوات نظام التشغيل عبر نقاط التوزيع. يمكنك تفعيل هذا الخيار إذا كانت توجد نقطة توزيع واحدة على الأقل في الشبكة.

إذا كان خيار **Using Network Agent** مفعلاً، يتم تسليم الملفات باستخدام أدوات نظام التشغيل فقط في حالة عدم توفر أدوات عميل الشبكة.

- **Maximum number of concurrent downloads**

العدد الأقصى المسموح به لأجهزة العميل التي يمكن أن ينقل إليها خادم الإدارة ملفات في الوقت نفسه. كلما ارتفع هذا الرقم، ارتفعت سرعة إلغاء تثبيت التطبيق، لكن يرتفع الحمل على خادم الإدارة كذلك.

- **Maximum number of uninstallation attempts**

عند تشغيل مهمة Uninstall application remotely، إذا فشل Kaspersky Security Center في إلغاء تثبيت تطبيق على جهاز مُدار ضمن عدد عمليات تشغيل المثبتات المحددة من خلال المعلمة، سيتوقف Kaspersky Security Center عن توصيل أداة إلغاء التثبيت إلى هذا الجهاز المُدار ولن يبدأ تشغيل المثبت على الجهاز مرةً أخرى.

معلمة **Maximum number of uninstallation attempts** تتيح لك حفظ موارد الجهاز المُدار وكذلك الحد من حركة المرور (إلغاء التثبيت وتشغيل ملف MSI ورسائل الأخطاء).

قد تشير محاولات بدء تشغيل المهمة بشكل متكرر إلى وجود مشكلة في الجهاز تمنع عملية إلغاء التثبيت. يجب أن يحل المدير المشكلة في نطاق العدد المحدد لمحاولات إلغاء التثبيت ثم يقوم بإعادة تشغيل المهمة (يدويًا أو من خلال جدول).

إذا لم تتم عملية إلغاء التثبيت في النهاية، ستعتبر المشكلة غير قابلة للحل، وأي عمليات بدء تشغيل مهمة بعد ذلك ستعتبر مكلفة فيما يخص استهلاك الموارد وحركة المرور بلا داعي.

عند إنشاء المهمة، يتم تعيين عداد المحاولات على 0. تزيد كل عملية بدء تشغيل للمثبت ينتج عنها أخطاء في الجهاز من قراءة العداد.

إذا تم تجاوز عدد المحاولات المحدد في المعلمة وكان الجهاز مستعدًا لعملية إلغاء تثبيت التطبيق، يمكنك زيادة قيمة معلمة **Maximum number of uninstallation attempts** وبدء تشغيل المهمة لإلغاء تثبيت التطبيق. وكحل بديل، يمكنك إنشاء مهمة Uninstall application remotely جديدة.

- **Verify operating system type before downloading**

قبل نقل الملفات إلى أجهزة العميل، يتحقق Kaspersky Security Center مما إذا كانت إعدادات أداة التثبيت قابلة للتطبيق على نظام تشغيل الجهاز العميل أم لا. إذا لم تكن الإعدادات قابلة للتطبيق، لا ينقل Kaspersky Security Center الملفات ولا يحاول تثبيت التطبيق. على سبيل المثال: لتثبيت تطبيق على أجهزة في مجموعة إدارة تشمل أجهزة تعمل بعدة أنظمة تشغيل مختلفة، يمكنك تعيين مهمة التثبيت إلى مجموعة الإدارة ثم تفعيل هذا الخيار من أجل تخطي الأجهزة التي تعمل بنظام تشغيل غير النظام المطلوب.

عند تثبيت عميل الشبكة عن بُعد على الأجهزة غير المعينة، يحدد Kaspersky Security Center أو نقطة توزيع تلقائيًا نوع نظام تشغيل الجهاز، بغض النظر عن إعداد **Verify operating system type before downloading**.

- **Use uninstallation password**

يتم عرض هذه المعلمة إذا حددت في الخطوة السابقة **إلغاء تثبيت التطبيق المُدار**، ثم حددت عميل شبكة Kaspersky Security Center في الحقل **التطبيق المطلوب إلغاء تثبيته**.

إذا عيّنت مسبقًا كلمة مرور إلغاء التثبيت عن بُعد لعميل الشبكة في إعدادات سياسية عميل الشبكة، حدد خانة الاختيار **استخدام كلمة مرور إلغاء التثبيت**، ثم أدخل كلمة مرور إلغاء التثبيت في الحقل **كلمة المرور**. إذا لم تُعيّن كلمة المرور لإلغاء التثبيت عن بُعد لعميل الشبكة، فلا تحدد خانة الاختيار.

8. حدد إعدادات إعادة تشغيل نظام التشغيل:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **Force closure of applications in blocked sessions**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

9. أضف الحسابات التي سيتم استخدامها لبدء مهمة إلغاء التثبيت عن بُعد إذا كان ذلك ضروريًا:

- **No account required (Network Agent installed)**

إذا تم تحديد هذا الخيار، فلا يلزم تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

إذا لم يتم تثبيت عميل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

- **Account required (Network Agent is not used)**

حدد هذا الخيار إذا لم يكن عميل الشبكة مثبتًا على الأجهزة التي قمت بتعيين مهمة إلغاء التثبيت عن بُعد لها. في هذه الحالة، يمكنك تحديد حساب مستخدم أو شهادة SSH لإلغاء تثبيت التطبيق.

- **Local Account**. إذا تم تحديد هذا الخيار، فحدد الحساب المستخدم الذي سيتم من خلاله تشغيل مثبت التطبيق. انقر على الزر **إضافة**، وحدد **Local Account**، ثم حدد بيانات اعتماد حساب المستخدم.

يمكنك تحديد عدة حسابات مستخدمين، على سبيل المثال، إذا لم يكن لدى أي منهم جميع الحقوق المطلوبة على جميع الأجهزة التي قمت بتعيين المهمة لها. في هذه الحالة، يتم استخدام جميع الحسابات المضافة لتشغيل المهمة، بترتيب متتالٍ، من أعلى إلى أسفل.

- **شهادة SSH**. إذا كنت ترغب في إلغاء تثبيت تطبيق من جهاز عميل يستند إلى Linux، فيمكنك تحديد شهادة SSH بدلاً من حساب المستخدم. انقر على زر **إضافة**، وحدد **شهادة SSH**، ثم حدد المفاتيح الخاصة والعامة للشهادة.

لإنشاء مفتاح خاص، يمكنك استخدام الأداة المساعدة ssh-keygen. لاحظ أن Kaspersky Security Center يدعم تنسيق PEM للمفاتيح الخاصة، لكن الأداة المساعدة ssh-keygen تنشئ مفاتيح SSH بتنسيق OPENSSH افتراضيًا. تنسيق OPENSSH غير مدعوم من قبل Kaspersky Security Center. ولإنشاء مفتاح خاص بتنسيق PEM المدعوم، أضف الخيار -m PEM في الأمر ssh-keygen.

فمثلاً:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "< البريد الالكتروني للمستخدم >"
```

10. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

11. انقر على زر **Finish**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

12. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

13. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة .

14. انقر على زر **Save**.

15. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

بمجرد إكمال مهمة إلغاء التثبيت عن بُعد، ستتم إزالة التطبيق المحدد من الأجهزة المحددة

مشاكل إلغاء التثبيت عن بُعد

قد تنتهي أحيانًا عملية إلغاء تثبيت التطبيقات الخارجية عن بُعد بالتحذير التالي: "انتهى إلغاء التثبيت عن بُعد على هذا الجهاز مع تحذيرات: التطبيق المراد إزالته غير مثبت". وتحدث هذه المشكلة عندما يكون التطبيق المراد إلغاء تثبيته قد تم إلغاء تثبيته بالفعل أو تم تثبيته لمستخدم فردي فقط. وتصبح التطبيقات المثبتة لمستخدم فردي (يشار إليها أيضًا باسم تطبيقات المستخدم) غير مرئية ولا يمكن إلغاء تثبيتها عن بُعد إذا لم يتم تسجيل دخول المستخدم.

يختلف هذا السلوك عن التطبيقات المخصصة للاستخدام من قبل مستخدمين متعددين على الجهاز نفسه (يشار إليه أيضًا حسب تطبيقات الجهاز). وتكون تطبيقات كل أجهزة مرئية ويمكن الوصول إليها لجميع مستخدمي الجهاز.

لذلك ، يجب إلغاء تثبيت تطبيقات المستخدم فقط عند تسجيل دخول المستخدم.

مصدر المعلومات عن التطبيقات المثبتة

يسترد عميل الشبكة المعلومات عن البرامج المثبتة على أجهزة Windows من مفاتيح التسجيل التالية:

- Uninstall\CurrentVersion\Windows\Microsoft\Software\HKEY_LOCAL_MACHINE
  يحتوي على معلومات عن التطبيقات المثبتة لجميع المستخدمين.
- Uninstall\CurrentVersion\Windows\Microsoft\Wow6432Node\Software\HKEY_LOCAL_MACHINE
  يحتوي على معلومات عن التطبيقات المثبتة لجميع المستخدمين.
- Uninstall\CurrentVersion\Windows\Microsoft\Software\HKEY_CURRENT_USER
  يحتوي على معلومات عن التطبيقات المثبتة للمستخدم الحالي.
- Uninstall\CurrentVersion\Windows\Microsoft\Software\<...>HKEY_USER
  يحتوي على معلومات عن التطبيقات المُثبتة لمستخدمين معينين.

المهام

يصف هذا القسم المهام التي يستخدمها Kaspersky Security Center.

حول المهام

يقوم Kaspersky Security Center بإدارة تطبيقات Kaspersky security المثبتة على الأجهزة عن طريق إنشاء المهام وتشغيلها. يلزم وجود المهام من أجل تثبيت التطبيقات، وبدء تشغيلها، وإيقافها، وفحص الملفات، وتحديث قواعد البيانات والوحدات النمطية للبرامج، واتخاذ إجراءات أخرى بشأن التطبيقات.

لا يمكن إنشاء المهام لتطبيق محدد باستخدام Kaspersky Security Center Web Console إلا إذا كان المكون الإضافي للإدارة لذلك التطبيق المثبت على Kaspersky Security Center Web Console Server.

يمكن إجراء المهام على خادم الإدارة وعلى الأجهزة.

المهام التي تتم على خادم الإدارة تشمل ما يلي:

- التوزيع التلقائي للتقارير
- تنزيل التحديثات إلى المستودع
- النسخ الاحتياطي لبيانات خادم الإدارة
- صيانة قاعدة البيانات

يتم إجراء أنواع المهام التالية على الأجهزة:

- المهام المحلية—هي المهام التي يتم إجراؤها على جهاز محدد

  يمكن تعديل المهام المحلية إما بواسطة المسؤول باستخدام أدوات وحدة تحكم الإدارة أو بواسطة مستخدم جهاز بعيد (على سبيل المثال، عبر واجهة تطبيق الأمان). في حالة تعديل مهمة محلية بواسطة المسؤول ومستخدم الجهاز المُدار في الوقت نفسه، فستسري التغييرات التي يقوم بها المسؤول حيث أنه يملك أولوية أعلى.

- المهام الجماعية—هي المهام التي يتم إجرائها على كافة الأجهزة الخاصة بمجموعة محددة

  ما لم يتم تحديد خلاف ذلك في خصائص المهمة، تؤثر أيضًا المهمة الجماعية على كافة المجموعات الفرعية الخاصة بالمجموعة المحددة. كما تؤثر المهام الجماعية (بشكل اختياري) على الأجهزة المتصلة بخوادم الإدارة الثانوية والافتراضية التي تم نشرها في هذه المجموعة أو أيٍ من مجموعاتها الفرعية.

- المهام العالمية—هي المهام التي تنفذ على مجموعة من الأجهزة محددة بصرف النظر عما إذا كانت مضمنة في أية مجموعة إدارة أم لا

يمكنك إنشاء أي عدد من المهام الجماعية أو المهام العالمية أو المهام المحلية، وذلك لكل تطبيق.

ويمكنك إجراء تغييرات على إعدادات المهام، وعرض مستوى تقدمها، ونسخها، وتصديرها، واستيرادها، وحذفها.

لا يتم بدء تشغيل المهمة على جهاز إلا إذا كان التطبيق الذي تم إنشاء المهمة له قيد التشغيل.

نتائج تنفيذ المهام المحفوظة في سجل أحداث نظام التشغيل على كل جهاز وفي سجل أحداث نظام التشغيل على خادم الإدارة وفي قاعدة بيانات خادم الإدارة.

لا تقم بتضمين بيانات خاصة في إعدادات المهمة. على سبيل المثال، تجنّب تخصيص كلمة مرور مسؤول المجال.

حول نطاق المهمة

نطاق المهمة هو مجموعة الأجهزة التي يتم تنفيذ المهمة عليها. أنواع النطاق هي التالية:

- لتنفيذ مهمة في الجهاز، يكون الجهاز نفسه هو النطاق.
- لتنفيذ مهمة في خادم الإدارة، يكون خادم الإدارة هو النطاق.
- لتنفيذ مهمة جماعية، تكون قائمة الأجهزة المشمولة في المجموعة هي النطاق.

عند إنشاء مهمة شاملة، يمكنك استخدام الوسائل التالية لتحديد نطاقها:

- تحديد أجهزة معينة يدويًا.

  يمكنك استخدام عنوان IP (أو نطاق IP)، أو اسم NetBIOS أو اسم DNS كعنوان الجهاز.

- استيراد قائمة بالأجهزة من ملف TXT يحتوي على عناوين الأجهزة المراد إضافتها (يجب وضع كل عنوان في سطر منفرد).

  إذا قمت باستيراد قائمة بالأجهزة من ملف أو قمت بإنشاء قائمة يدويًا، وإذا تم تحديد الأجهزة بأسمائها، فيمكن فقط أن تحتوي القائمة على الأجهزة التي تم إدخال معلوماتها في قاعدة بيانات خادم الإدارة. علاوة على ذلك، لا بد أن المعلومات قد تم إدخالها عند اتصال هذه الأجهزة أو أثناء اكتشاف الأجهزة.

- تعيين تحديد جهاز.

  بمرور الوقت، يتغير نطاق المهمة بتغير مجموعة الأجهزة المضمنة في التحديد. يمكن القيام بتحديد أجهزة على أساس سمات الجهاز، بما في ذلك البرنامج المثبت على جهاز ما، وعلى أساس العلامات المعيّنة إلى الأجهزة. تحديد الجهاز هو الطريقة الأكثر مرونة لتحديد نطاق مهمة ما.

  تعمل المهام المخصصة لتحديدات الأجهزة دائمًا وفق جدول بواسطة خادم الإدارة. لا يمكن أن تعمل هذه المهام على أجهزة غير متصلة بخادم الإدارة. إن المهام التي تم تحديد نطاقها باستخدام وسائل أخرى يتم تنفيذها مباشرةً على الأجهزة ولذلك لا تعتمد على اتصال الجهاز بخادم الإدارة.

لا يتم تنفيذ المهام المخصصة لتحديدات الجهاز في الوقت المحلي لجهاز ما؛ وبدلاً من ذلك، يتم تنفيذها في الوقت المحلي لخادم الإدارة. إن المهام التي تم تحديد نطاقها باستخدام وسائل أخرى يتم تنفيذها في الوقت المحلي لجهاز ما.

إنشاء مهمة

لإنشاء مهمة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.
2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. اتبع تعليماته.

3. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.
4. انقر على زر **Finish**.

   يتم إنشاء المهمة وعرضها في قائمة المهام.

لإنشاء مهمة جديدة مخصصة للأجهزة المحددة:

1. في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)**.

   يتم عرض قائمة الأجهزة المُدارة.

2. في قائمة الأجهزة المدارة، حدد خانات الاختيار المجاورة للأجهزة لتشغيل المهمة لها. يمكنك استخدام وظائف البحث والتصفية للعثور على الأجهزة التي تبحث عنها.

3. انقر فوق الزر **تشغيل مهمة**، ثم حدد **إضافة مهمة جديدة**.

يبدأ معالج المهمة الجديدة.

في الخطوة الأولى من المعالج، يمكنك إزالة الأجهزة المحددة لتضمينها في نطاق المهمة. اتبع تعليمات المعالج.

4. انقر على زر **Finish**.

يتم إنشاء المهمة للأجهزة المحددة.

بدء مهمة يدويًا

يبدأ التطبيق المهام وفق إعدادات الجدول المحددة في خصائص كل مهمة. يمكنك بدء مهمة يدويًا في أي وقت من قائمة المهام. وبدلاً من ذلك، يمكنك تحديد الأجهزة في قائمة **Managed devices**، ثم بدء مهمة حالية لها.

لبدء مهمة يدويًا:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. في قائمة المهمة، حدد خانة الاختيار الموجودة بجوار المهمة التي ترغب في بدئها.

3. انقر على زر **Start**.

تبدأ المهمة. يمكنك التحقق من حالة المهمة في عمود **Status** أو بالنقر على زر **Result**.

عرض قائمة المهام

يمكنك عرض قائمة المهام التي تم إنشاؤها في Kaspersky Security Center.

لعرض قائمة المهام،

في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

يتم عرض قائمة المهام. يتم تجميع المهام بأسماء التطبيقات التي ترتبط بها. على سبيل المثال: مهمة Uninstall application remotely متعلقة بخادم الإدارة، ومهمة Find vulnerabilities and required updates تشير إلى عميل الشبكة.

لعرض خصائص مهمة،

انقر على اسم المهمة.

سيتم عرض نافذة خصائص المهمة مع عدة علامات تبويب مسماة. على سبيل المثال: يتم عرض **Task type** في تبويب **General**، ويتم عرض جدول المهمة في تبويب **Schedule**.

إعدادات المهمة العامة

يحتوي هذا القسم على الإعدادات التي يمكنك عرضها وتكوينها لمعظم مهامك. وتعتمد قائمة الإعدادات المتاحة على المهمة التي تكوّنها.

الإعدادات المحددة أثناء إنشاء المهمة

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضًا تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

- إعدادات إعادة تشغيل نظام التشغيل:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **Force closure of applications in blocked sessions**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- إعدادات جدولة المهام:

قد تختلف أنواع الجدول الزمني حسب المهمة.

- إعداد Start task:

- Every N hours

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- Every N days

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- Every N minutes

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- By days of week

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- Monthly

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- Manually

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- Once

يتم تشغيل المهمة مرة واحدة، في التاريخ والوقت المحددين (افتراضيًا، في اليوم الذي تم إنشاء المهمة فيه).

- Immediately

تعمل المهمة على الفور بعد حفظ إعداداتها.

- Every month on specified days of selected weeks

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **When new updates are downloaded to the repository**

تعمل المهمة بعد تنزيل التحديثات إلى المستودع. على سبيل المثال، قد ترغب في استخدام هذا الجدول للبحث عن الثغرات الأمنية ومهمة التحديثات المطلوبة.

- **On virus outbreak**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **On completing another task**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **Run missed tasks**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **Use automatically randomized delay for task starts**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **Use automatically randomized delay for task starts within an interval of**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

- الأجهزة التي سيتم تعيين المهمة إليها:

- **Select networked devices detected by Administration Server**

يتم تعيين المهمة لأجهزة محددة. يمكن أن تشمل الأجهزة المحددة الأجهزة الموجودة في مجموعات الإدارة بالإضافة إلى الأجهزة غير المخصصة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لمهمة تثبيت عميل الشبكة على الأجهزة غير المخصصة.

- **Specify device addresses manually or import addresses from a list**

يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

- **Assign task to a device selection**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

- **Assign task to an administration group**

يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

- إعدادات الحساب:

- **الحساب الافتراضي**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.

يتم تحديد هذا الخيار افتراضيًا.

- **تعيين حساب**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **الحساب**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **كلمة المرور**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

الإعدادات المحددة بعد إنشاء المهمة

يمكنك تحديد الإعدادات التالية بعد إنشاء المهمة فقط.

- إعدادات المهمة الجماعية:

- **Distribute to subgroups**

هذا الخيار متاح فقط في إعدادات مهام المجموعة.

عند تمكين هذا الخيار، يتضمن نطاق المهمة ما يلي:

- مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.

- مجموعات الإدارة التابعة لمجموعة الإدارة المحددة على أي مستوى لأسفل من خلال التسلسل الهرمي للمجموعة.

عند تعطيل هذا الخيار، فإن نطاق المهمة يتضمن فقط مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.

يتم تمكين هذا الخيار افتراضيًا.

- **Distribute to secondary and virtual Administration Servers**

عند تمكين هذا الخيار، يتم أيضًا تطبيق المهمة الفعالة على خادم الإدارة الأساسي على خوادم الإدارة الثانوية (بما في ذلك الخوادم الافتراضية). إذا كانت هناك مهمة من نفس النوع موجودة بالفعل على خادم الإدارة الثانوي، فسيتم تطبيق كلا المهمتين على خادم الإدارة الثانوي - المهمة الحالية والموروثة من خادم الإدارة الأساسي.

لا يتوفر هذا الخيار إلا عند تمكين خيار **Distribute to subgroups**.

يتم تعطيل هذا الخيار افتراضيًا.

- إعدادات الجدولة المتقدمة:

- **Turn on devices by using the Wake-on-LAN function before starting the task**

يبدأ نظام التشغيل الموجود على الجهاز في الوقت المحدد قبل بدء المهمة. الفترة الزمنية الافتراضية هي خمس دقائق.

قم بتمكين هذا الخيار إذا كنت تريد تشغيل المهمة على جميع الأجهزة العميلة من نطاق المهام، بما في ذلك تلك الأجهزة التي تم إيقاف تشغيلها عندما تكون المهمة على وشك البدء.

إذا كنت تريد إيقاف تشغيل الجهاز تلقائيًا بعد اكتمال المهمة، فقم بتمكين خيار **أغلق الأجهزة بعد الانتهاء من المهمة**. يمكن العثور على هذا الخيار في النافذة نفسها.

يتم تعطيل هذا الخيار افتراضيًا.

- **Shut down the devices after completing the task**

على سبيل المثال، قد ترغب في تمكين هذا الخيار لمهمة تحديث تثبيت والتي تقوم بتثبيت التحديثات على الأجهزة العميلة كل يوم جمعة بعد ساعات العمل، ثم تقوم بإيقاف تشغيل هذه الأجهزة لعطلة نهاية الأسبوع.

يتم تعطيل هذا الخيار افتراضيًا.

- **Stop the task if it runs longer than**

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائيًا، سواء أكانت مكتملة أم لا.

قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتًا طويلاً للتنفيذ.

يتم تعطيل هذا الخيار افتراضيًا. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

- إعدادات الإخطار:
  - كتلة **تخزين محفوظات المهمة** :
    - **Store in the Administration Server database for (days)**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام على خادم الإدارة خلال عدد الأيام المحدد. وعند انقضاء هذه الفترة الزمنية، يتم حذف المعلومات من خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **Store in the OS event log on device**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة محليًا في سجل أحداث Windows لكل جهاز عميل.

يتم تعطيل هذا الخيار افتراضيًا.

- **Store in the OS event log on Administration Server**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام مركزيًا في سجل أحداث Windows لنظام تشغيل خادم الإدارة (OS).

يتم تعطيل هذا الخيار افتراضيًا.

- **Save all events**

إذا تم تحديد هذا الخيار، فسيتم حفظ جميع الأحداث المتعلقة بالمهمة في سجلات الأحداث.

- **Save events related to task progress**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بتنفيذ المهمة في سجلات الأحداث.

- **Save only task execution results**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بنتائج المهمة في سجلات الأحداث.

- **قم بإخطار المسؤول بنتائج تنفيذ المهمة**

يمكنك تحديد الطرق التي يتلقى بها المسؤولون إخطارات حول نتائج تنفيذ المهام: عن طريق البريد الإلكتروني، والرسائل النصية القصيرة، وعن طريق تشغيل ملف تنفيذي. لتكوين الإخطار، انقر فوق الرابط **إعدادات**.

يتم تعطيل جميع أساليب الإخطارات بصورة افتراضية.

- **Notify of errors only**

إذا تم تمكين هذا الخيار، فسيتم إخطار المسؤولين فقط عند اكتمال تنفيذ المهمة مع وجود خطأ.

إذا تم تعطيل هذا الخيار، فسيتم إخطار المسؤولين بعد اكتمال تنفيذ كل مهمة.

يتم تمكين هذا الخيار افتراضيًا.

- إعدادات الأمان.
- إعدادات نطاق المهمة.

اعتمادًا على كيفية تحديد نطاق المهام، تكون الإعدادات التالية موجودة:

- **الأجهزة**

إذا تم تحديد نطاق المهمة بواسطة مجموعة إدارة، فيمكنك عرض هذه المجموعة. لا توجد تغييرات متاحة هنا. ومع ذلك، يمكنك إعداد **الاستثناءات من نطاق المهمة**.

إذا تم تحديد نطاق مهمة ما بواسطة قائمة من الأجهزة، فيمكنك تعديل هذه القائمة بإضافة أجهزة وإزالتها.

- **تحديد الجهاز**

يمكنك تغيير تحديد الجهاز الذي يتم تطبيق المهمة عليه.

- **الاستثناءات من نطاق المهمة**

يمكنك تحديد مجموعات الأجهزة التي لا يتم تطبيق المهمة عليها. يمكن أن تكون المجموعات المراد استثنائها مجموعات فرعية فقط من مجموعة الإدارة التي يتم تطبيق المهمة عليها.

- **محفوظات المراجعة**.

تصدير مهمة

يتيح لك Kaspersky Security Center حفظ مهمة وإعداداتها في ملف KLT. يمكنك استخدام ملف KLT هذا لاستيراد المهمة المحفوظة إلى كل من Kaspersky Security Center Windows وKaspersky Security Center Linux.

لتصدير مهمة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.
2. حدد خانة الاختيار الموجودة بجوار المهمة التي ترغب في تصديرها.

لا يمكنك تصدير مهام متعددة في نفس الوقت. إذا قمت بتحديد أكثر من مهمة، فسيتم تعطيل زر **Export**. لا يتوفر أيضًا تصدير مهام خادم الإدارة.

3. انقر على الزر **Export**.
4. في النافذة **حفظ باسم** المفتوحة، حدد اسم ملف المهمة والمسار. انقر على زر **حفظ**.

يتم عرض نافذة **حفظ باسم** فقط إذا كنت تستخدم Google Chrome أو Microsoft Edge أو Opera. إذا كنت تستخدم مستعرضًا آخر، فسيتم حفظ ملف المهمة تلقائيًا في مجلد**التنزيلات**.

استيراد مهمة

يتيح لك Kaspersky Security Center استيراد مهمة من ملف KLT. يحتوي ملف KLT على مهمة تم تصديرها وإعداداته.

لاستيراد مهمة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.
2. انقر على زر **Import**.
3. انقر على زر **Browse** لاختيار ملف المهمة الذي تريد استيراده.

4. في النافذة المفتوحة، حدد المسار إلى ملف مهمة KLT ، ثم انقر على زر **فتح**. لاحظ أنه يمكنك تحديد ملف مهمة واحد فقط.

تبدأ معالجة المهمة.

5. بعد معالجة المهمة بنجاح، حدد الأجهزة التي تريد تعيين المهمة لها. لفعل هذا، حدد أحد الخيارات التالية:

- **Assign task to an administration group**

يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

- **Specify device addresses manually or import addresses from a list**

يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

- **Assign task to a device selection**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

6. حدد نطاق المهمة.

7. انقر على زر **Complete** لإنهاء استيراد المهمة.

يُظهر الإشعار نتائج الاستيراد. إذا تم استيراد المهمة بنجاح، يمكنك النقر على رابط **Details** لعرض خصائص المهمة.

بعد نجاح الاستيراد، يتم عرض المهمة في قائمة المهام. يتم أيضًا استيراد إعدادات المهمة والجدول. ستبدأ المهمة وفقًا لجدولها الزمني.

> إذا كانت المهمة المستوردة حديثًا لها اسم مماثل لمهمة موجودة، فسيتم توسيع اسم المهمة المستوردة بامتداد **(<next sequence number>)** الفهرس، على سبيل المثال: **(1)** و **(2)**.

بدء معالج تغيير كلمة مرور المهام

بالنسبة إلى مهمة غير محلية، يمكنك تحديد حساب الذي بموجبه يجب تشغيل المهمة. يمكنك تحديد الحساب أثناء إنشاء المهمة أو في خصائص مهمة موجودة. إذا تم استخدام الحساب المحدد وفقًا لتعليمات الأمان للمنظمة، قد تتطلب هذه التعليمات تغيير كلمة مرور الحساب من وقت لآخر. عند انتهاء صلاحية كلمة مرور الحساب وتعيينك لكلمة مرور جديدة، لن تبدأ المهام حتى تحدد كلمة المرور الجديدة الصالحة في خصائص المهمة.

يمكّنك "معالج تغيير كلمة مرور المهام" من استبدال كلمة المرور القديمة تلقائيًا بكلمة مرور جديدة في جميع المهام التي يتم فيها تحديد الحساب. بدلاً من ذلك، يمكنك تغيير كلمة المرور هذه يدويًا في خصائص كل مهمة.

لبدء تشغيل معالج تغيير كلمة مرور المهام:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.

2. انقر على **Manage credentials of accounts for starting tasks** .

اتبع إرشادات المعالج.

الخطوة 1. تحديد أوراق الاعتماد

حدد بيانات اعتماد جديدة صالحة حاليًا في نظامك (في Active Directory مثلاً). عندما تقوم بالتبديل إلى الخطوة التالية من المعالج، يتحقق Kaspersky Security Center ما إذا كان اسم الحساب المحدد مطابقًا لاسم الحساب في خصائص كل مهمة غير المحلية. في حالة تطابق أسماء الحساب، يتم استبدال كلمة المرور في خصائص المهمة تلقائيًا بكلمة المرور الجديدة.

لتحديد الحساب الجديد، حدد خيارًا:

- **Use current account**

  يستخدم المعالج اسم الحساب الذي قمت بتسجيل الدخول من خلاله حاليًا إلى Kaspersky Security Center Web Console. بعدها حدد كلمة مرور الحساب يدويًا في حقل **Current password to use in tasks**.

- **Specify a different account**

  حدد اسم الحساب التي يجب بدء المهام من خلاله. بعدها حدد كلمة مرور الحساب في حقل **Current password to use in tasks**.

إذا كنت تملأ حقل **Previous password (optional; if you want to replace it with the current one)**، لا يستبدل Kaspersky Security Center إلا كلمة المرور لتلك المهام التي يوجد فيها كل من اسم الحساب وكلمة المرور القديمة. يتم إجراء الاستبدال تلقائيًا. في جميع الحالات الأخرى، ستحتاج إلى اختيار إجراء لاتخاذه في الخطوة التالية من المعالج.

الخطوة 2. تحديد إجراء لاتخاذه

إذا لم تحدد كلمة المرور السابقة في الخطوة الأولى من المعالج أو لم تتطابق كلمة المرور القديمة المحددة مع كلمات المرور في خصائص المهمة، يجب عليك اختيار إجراء لاتخاذه للمهام التي تم العثور عليها.

لاختيار إجراء لمهمة:

1. حدد خانة الاختيار الموجودة بجوار المهمة التي ترغب في اتخاذ إجراء لها.

2. اتخذ أحد الإجراءات التالية:

- لإزالة كلمة المرور في خصائص المهمة، انقر على **Delete credentials**.

  ستتحول المهمة إلى العمل عبر الحساب الافتراضي.

- لاستبدال كلمة المرور بأخرى جديدة، انقر على **Enforce the password change even if the old password is wrong or not provided**.

- لإلغاء تغيير كلمة المرور، انقر على **No action is selected**.

سيتم تطبيق الإجراءات التي تم اختيارها بعد أن تنتقل إلى الخطوة التالية من المعالج.

الخطوة 3. عرض النتائج

في الخطوة الأخيرة من المعالج، اعرض النتائج لكل المهام التي تم العثور عليها. لإكمال المعالج، انقر على زر **إنهاء**.

إنشاء مهمة تنفيذ البرامج النصية عن بعد

يمكنك إنشاء مهمة تنفيذ البرامج النصية عن بعد لتنفيذ حزمة تثبيت على جهاز عميل ولتثبيت تطبيق عن بُعد.

تحتوي حزمة التثبيت على أرشيف مضغوط يحتوي على مجموعة من البرامج النصية للتنفيذ على الأجهزة العميلة بالإضافة إلى ملف manifest.json. يمكنك معرفة المزيد عن إنشاء هذا النوع من حزم التثبيت في هذه المقالة .

يجب بدء هذه المهمة فقط على الأجهزة التي تحتوي على عميل شبكة لنظام التشغيل Linux.

لبدء تنفيذ مهمة تنفيذ البرامج النصية عن بعد:

1. انتقل إلى **معالج مهمة جديدة** وحدد نوع المهمة **تنفيذ البرامج النصية عن بعد**.
2. أدخل اسم المهمة وحدد الأجهزة التي سيتم تعيين المهمة لها. انقر على الزر **Next**.
3. حدد حزمة تثبيت بناءً على أرشيف مضغوط مع ملف manifest.json للتنفيذ عن بُعد.

   إذا كنت لا تريد إعادة تشغيل المهمة على الأجهزة التي اكتملت فيها بالفعل، فقم بتشغيل الخيار **Do not start this task on devices on which it has already been completed**.
4. حدد حسابًا لتشغيل المهمة.

   إذا حددت الحساب الافتراضي، فسيتم تنفيذ المهمة بواسطة عميل الشبكة (الحساب الجذر).

عند بدء مهمة تنفيذ البرامج النصية عن بعد، لا يمكنك تغيير الحساب الذي تم تعيينه لها. لتغيير الحساب الذي تم تعيين المهمة إليه، أوقف المهمة في إعدادات المهمة وقم بإنشائها مرة أخرى باستخدام تفاصيل الحساب الصحيحة.

5. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية في أي وقت لاحق.
6. انقر على زر **Finish**.

   يتم إنشاء مهمة تنفيذ البرامج النصية عن بعد وتظهر في قائمة المهام.

بعد تلقي البيانات من مهمة تنفيذ البرامج النصية عن بُعد، يُقيد عميل الشبكة الوصول إلى البيانات المستلمة لجميع المستخدمين، باستثناء المسؤول والمستخدم المحدد في إعدادات المهمة.

تثبيت التطبيقات عن بعد على الأجهزة باستخدام مهمة تنفيذ البرامج النصية عن بعد

يمكن استخدام مهمة تنفيذ البرامج النصية عن بعد لتثبيت تطبيق عن بُعد على جهاز عميل من خلال إنشاء حزمة تثبيت مخصصة.

يمكنك معرفة كيفية تحضير أرشيف لهذه المهمة في هذه المقالة.

لإنشاء حزمة تثبيت للتثبيت عن بُعد لتطبيق على جهاز عميل، يجب تضمين الملفات التالية في الأرشيف الذي تريد تحميله لهذه المهمة:

- deb.<package name>
- **install.sh**

```
deb.< اسم الحزمة > sudo apt-get install
```

- manifest.json

مخطط JSON للتثبيت عن بعد لتطبيق

```
}
"version": 1,
"actions": [
{
"type": "execute",
"path": "install.sh",
"args": "<أدخل الوسائط، إذا لزم الأمر>",
"results": [
{
"code": 0,
"next": "continue"
},
{
"default_next": "break"
}
]
}
```

وصف المصفوفات

1. `version` - إصدار ملف البيان والمهمة.

   في الوقت الحاضر، القيمة المقبولة الوحيدة هي 1.

2. تحدد عناصر مجموعة `actions` تكوين وترتيب البرامج النصية التي يتم تنفيذها في المهمة.

   يتوافق ترتيب تنفيذ البرنامج النصي مع مؤشر العنصر (المكان) في المصفوفة.

3. بالنسبة لكل عنصر من عناصر مجموعة `actions`، يتم تعريف العناصر التالية.

   a. `type` - نوع الأمر القابل للتنفيذ من البرامج النصية. وفي الوقت الحاضر، القيمة هي دائمًا `execute`.

   b. `path` - المسار إلى ملف البرنامج النصي في الأرشيف.

   c. `args` - الوسائط التي يتم تمريرها إلى البرنامج النصي كجزء من الأمر القابل للتنفيذ.

   d. `results` - مجموعة تحدد إجراءات إضافية اعتمادًا على نتيجة المهمة.

      1. `code` - القيمة التي تقوم بإرجاع البرنامج النصي.

      2. `next` - الإجراء الذي سيتم إكماله بعد ذلك. يؤدي إجراء `continue` إلى تنفيذ البرنامج النصي التالي (عنصر في مجموعة `actions`)؛ ويؤدي إجراء `break` إلى إيقاف المهمة.

   e. `default_next` - إجراء إذا أعاد البرنامج النصي قيمة غير موجودة في `results`.

عند بدء مهمة تنفيذ البرامج النصية عن بعد، سيقوم عميل الشبكة بتحميل حزمة التثبيت مع التطبيق إلى الجهاز العميل. عندما يتلقى الجهاز العميل حزمة التثبيت، يوزع عميل الشبكة على هذا الجهاز ملف Manifest.json وتحديد ترتيب تنفيذ البرامج النصية والإجراءات اعتمادًا على النتيجة ثم يبدأ التنفيذ.

عند اكتمال مهمة تنفيذ البرامج النصية عن بعد، سيتم تثبيت التطبيق على الجهاز العميل.

تكوين الإخطارات والمراقبة لمهمة تنفيذ البرامج النصية عن بُعد

يمكنك تكوين المراقبة وسلوك حفظ الأحداث والإخطارات لمهمة تنفيذ البرامج النصية عن بعد.

لعرض حالة تنفيذ البرامج النصية عن بعد:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **المهام**.
   يتم عرض قائمة المهام.
2. حدد المهمة وانقر فوق **Device history**.
   يتم عرض تقدم المهمة.

لتكوين سلوك حفظ الحدث:

1. في قائمة المهام، انقر فوق المهمة وانتقل إلى علامة التبويب **Settings**.
2. في قسم **Notifications**، انقر فوق الزر **Settings**.
3. حدد أحد الخيارات التالية لمعرفة كيفية تصرف التطبيق بعد اكتمال المهمة:
   - **Save all events**.
   - **Save events related to task progress**.
   - **Save only task execution results**.
     يتم حفظ الأحداث في **Device history** و**مستودع الأحداث**.
     بشكل افتراضي ، يتم حفظ نتائج تنفيذ المهمة فقط.

> إذا حددت **Save all events**، فلن يتم حفظ سوى نتائج تنفيذ المهمة.

4. إذا كنت تريد الاحتفاظ بالأحداث في قاعدة بيانات خادم الإدارة، أو في سجل الأحداث على خادم الإدارة، أو على الجهاز، فقم بتشغيل الخيار المقابل.

يمكنك معرفة المزيد عن تكوين الإخطارات في هذه المقالة.

تحضير أرشيف لمهمة تنفيذ البرامج النصية عن بُعد

يجب أن يلبي أرشيف مهمة تنفيذ البرامج النصية عن بعد استنادًا إلى ملف manifest.json المتطلبات التالية:

- تنسيق الأرشيف: ZIP.
- الحجم الإجمالي: لا يزيد عن 1 جيجا بايت.
- عدد الملفات والمجلدات في الأرشيف غير محدود.
- يجب أن يتطابق ملف البيان للأرشيف مع المخطط أدناه ويجب تسميته manifest.json. يتم التحقق من صحة مخطط قاعدة البيانات فقط أثناء تنفيذ المهمة على الجهاز.

مخطط JSON لملف البيان ووصف المصفوفات

```
                                                                }
                ,"#json-schema.org/draft-07/schema//:http" :"schema$"
                        ,"Schema for execute scripts task" :"title"
                                                  ,"object" :"type"
                                                   } :"properties"
                                                  } :"version"
                                        ,"integer" :"type"
                                               [1] :"enum"
                                                              ,{
                                                   }:"actions"
                                          ,"array" :"type"
                                                } :"items"
                                     ,"object" :"type"
                                      } :"properties"
                                         } :"type"
                            ,"string" :"type"
                         ["execute"] :"enum"
                                                     ,{
                                         } :"path"
                              "string" :"type"
                                                     ,{
                                         } :"args"
                              "string" :"type"
                                                     ,{
                                       }:"results"
                              ,"array" :"type"
                                    } :"items"
                        ,"object" :"type"
                         } :"properties"
                            } :"code"
                ,"integer" :"type"
                  ,255- :"minimum"
                    255 :"maximum"
                                     ,{
                              }:"next"
                ,"string" :"type"
["continue" ,"break"] :"enum"
                                      {
                                         ,{
                           ] :"required"
                              ,"code"
                               "next"
                                         [
                                             {
                                                     ,{
                                }:"default_next"
                            ,"string" :"type"
                ["continue" ,"break"] :"enum"
                                                  {
                                                        ,{
                                         ] :"required"
                                           ,"type"
                                           ,"path"
                                     "default_next"
                                                        [
```

مثال على ملف البيان

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": {
        "code": 0,
        "next": "continue",
        "default_next": "break"
      }
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": {
        "code": 0,
        "next": "continue",
        "default_next": "break"
      }
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": {
        "code": 0,
        "next": "continue",
        "default_next": "break"
      }
    }
  ]
}
```

- يجب تنظيم الأرشيف على النحو التالي:

```
manifest.json
<file1>
<file2>
<file3>/<folder1>
```

```
<file4>/<folder3>/<folder2>
...
<fileX>
```

manifest.json is the manifest file for the task.

`<file1>, .... , <fileX>` هي مجموعة الملفات التي تحتوي على نصوص برمجية ليتم تنفيذها.

إنشاء حزمة تثبيت بناءً على ملف بيان

لإنشاء حزمة تثبيت بناءً على ملف بيان:

1. قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل إلى **Installation packages** ← **Deployment & assignment** ← **Discovery & deployment**.
- في القائمة الرئيسية، انتقل إلى **Installation packages** ← **Repositories** ← **Operations**.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. انقر على **Add**.

يبدأ معالج الحزمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

3. حدد **Create an installation package for the Execute scripts remotely task based on a ZIP archive with the manifest.json file**.

4. حدد اسم الحزمة وانقر فوق الزر **Browse**.

تفتح نافذة Windows القياسية **فتح** في مستعرضك لتتيح لك اختيار ملف لإنشاء حزمة التثبيت.

5. اختر ملفًا مضغوطًا موجودًا على الأقراص المتاحة. يمكنك معرفة كيفية تحضير أرشيف لهذه المهمة في هذه المقالة.

يبدأ تحميل الملف إلى خادم إدارة Kaspersky Security Center.

لقد بدأت عملية إنشاء حزمة التثبيت.

يحيطك المعالج علمًا عند الانتهاء من العملية.

إذا لم يتم إنشاء حزمة التثبيت، يتم عرض رسالة مناسبة.

6. انقر على زر **Finish** لإغلاق المعالج.

يتم تنزيل حزمة التثبيت التي قمت بإنشائها إلى مجلد الحزم الفرعي الخاص بـمجلد خادم الإدارة المشترك. بعد التنزيل تظهر حزمة التثبيت في قائمة حزم التثبيت.

في قائمة حزم التثبيت المتوفرة على خادم الإدارة، يمكنك النقر فوق الرابط الذي يحمل اسم حزمة التثبيت المخصصة من أجل:

- عرض الخصائص التالية لحزمة تثبيت:
  - **Name**. اسم حزمة تثبيت مخصص.
  - **Source**. اسم بائع التطبيق.
  - **Version**. إصدار التطبيق
  - **Created**. تاريخ إنشاء حزمة التثبيت.

- **Modified**. تاريخ تعديل حزمة التثبيت.
- **Path**. المسار إلى حزمة التثبيت المخصصة على خادم الإدارة.
- تغيير اسم الحزمة ومعلمات سطر الأوامر. تتوفر هذه الميزة فقط للحزم التي لم يتم إنشاؤها بناءً على تطبيقات Kaspersky.

إدارة الأجهزة العميلة

يتيح لك Kaspersky Security Center Linux إدارة أجهزة العميل:

- عرض إعدادات وحالات الأجهزة المُدارة، بما في ذلك المجموعات ومصفوفات الخادم.
- تكوين نقاط التوزيع.
- إدارة المهام.

يمكنك استخدام مجموعات الإدارة لدمج أجهزة العميل في مجموعة يمكن إدارتها كوحدة واحدة. ويمكن تضمين جهاز عميل في مجموعة إدارة واحدة فقط. **Rule conditions** ويمكن تخصيص الأجهزة إلى مجموعة تلقائيًا بناءً على Rule conditions:

- إنشاء قواعد نقل الجهاز.
- نسخ قواعد نقل الجهاز.
- شروط قاعدة نقل الجهاز.

يمكنك استخدام تحديدات الجهاز لتصفية الأجهزة بناءً على شرط. ويمكنك أيضًا تمييز الأجهزة لإنشاء التحديدات، والعثور على الأجهزة، وتوزيع الأجهزة بين مجموعات الإدارة.

إعدادات جهاز مدار

لعرض إعدادات جهاز مُدار:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.

   يتم عرض قائمة الأجهزة المُدارة.

2. في قائمة بالأجهزة المُدارة، انقر على الرابط الذي يحمل اسم الجهاز المطلوب.

   يتم عرض نافذة خصائص الجهاز المحدد.

يتم عرض علامات التبويب التالية في الجزء العلوي من نافذة الخصائص التي تمثل المجموعات الرئيسية للإعدادات:

- **General**

تتضمن علامة التبويب هذه الأقسام التالية:

- يعرض القسم **General** معلومات عامة عن الجهاز العميل. يتم تقديم المعلومات بناءً على البيانات المستلمة أثناء المزامنة الأخيرة للجهاز العميل مع خادم الإدارة:
  - **Name**

    في هذا الحقل، يمكنك عرض اسم كمبيوتر الجهاز وتعديله في مجموعة الإدارة.

- **الوصف**

في هذا الحقل، يمكنك إدخال وصف إضافي للجهاز العميل.

- **حالة الجهاز**

يتم تعيين حالة الجهاز بناء على المعايير التي حددها المسؤول عن حالة الحماية ضد الفيروسات على الجهاز وعن نشاط الجهاز على الشبكة.

- **Full group name**

مجموعة الإدارة التي تتضمن الجهاز العميل.

- **Last update of anti-virus databases**

تاريخ آخر تحديث لقواعد بيانات مكافحة الفيروسات أو التطبيقات على الجهاز.

- **تم الاتصال بخادم الإدارة**

تاريخ ووقت تثبيت عميل الشبكة على آخر جهاز عميل تم توصيله بخادم الإدارة.

- **آخر وقت مرئي**

التاريخ والوقت اللذين كان فيهما الجهاز مرئيًا على الشبكة.

- **Network Agent version**

إصدار عميل الشبكة المثبت.

- **Created**

تاريخ إنشاء الجهاز داخل Kaspersky Security Center.

- **Device owner**

اسم مالك الجهاز. يمكنك تعيين أو إزالة مستخدم كمالك للجهاز بالنقر على الرابط **Manage device owner** .

- **عدم قطع الاتصال عن خادم الإدارة**

إذا تم تمكين هذا الخيار، فسيتم الحفاظ على الاتصال المستمر بين الجهاز المُدار وخادم الإدارة. قد ترغب في استخدام هذا الخيار إذا لم تكن تستخدم خوادم الإرسال، التي توفر مثل هذا الاتصال.

إذا تم تعطيل هذا الخيار، فسيتصل جهاز العميل فقط بخادم الإدارة لمزامنة البيانات أو نقل المعلومات فقط.

الحد الأقصى لعدد الأجهزة التي تم تحديد خيار **عدم قطع الاتصال عن خادم الإدارة** هو 300.

يتم تعطيل هذا الخيار افتراضيًا على الأجهزة المُدارة. يتم تمكين هذا الخيار افتراضيًا على الجهاز حيث تم تثبيت خادم الإدارة ويظل ممكّنًا حتى إذا حاولت تعطيله.

- يعرض قسم **Network** المعلومات التالية عن خصائص الشبكة لجهاز العميل:

- **عنوان IP**

عنوان IP الخاص بالجهاز.

- **مجال Windows**

مجال Windows أو مجموعة العمل، التي تحتوي على الجهاز.

- **اسم DNS**

اسم مجال DNS للجهاز العميل.

- **اسم NetBIOS**

  اسم مجال Windows للجهاز العميل.

- **IPv6 address**

- يوفر قسم **System** معلومات عن نظام التشغيل المثبت على الجهاز العميل:

  - **Operating system**

  - **CPU architecture**

  - **Device name**

  - **Virtual machine type**

    الشركة المصنعة للجهاز الظاهري.

  - **Dynamic virtual machine as part of VDI**

    يعرض هذا الصف ما إذا كان الجهاز العميل عبارة عن جهاز ظاهري ديناميكي كجزء من VDI.

- يوفر القسم **Protection** المعلومات التالية عن الحالة الحالية للحماية ضد الفيروسات على الجهاز العميل:

  - **Visible**

    حالة رؤية الجهاز العميل.

  - **Device status**

    يتم تعيين حالة الجهاز بناء على المعايير التي حددها المسؤول عن حالة الحماية ضد الفيروسات على الجهاز وعن نشاط الجهاز على الشبكة.

  - **Status description**

    حالة حماية جهاز العميل والاتصال بخادم الإدارة.

  - **Protection status**

    يوضح هذا الحقل الحالة الحالية للحماية في الوقت الفعلي على الجهاز العميل.
    عندما تتغير الحالة على الجهاز، يتم عرض الحالة الجديدة في نافذة خصائص الجهاز فقط بعد أن تتم مزامنة الجهاز العميل مع خادم الإدارة.

  - **Last full scan**

    تاريخ ووقت آخر فحص للبرمجيات الضارة تم إجراءه على الجهاز العميل.

  - **Virus detected**

    العدد الإجمالي للتهديدات المكتشفة على الجهاز العميل منذ تثبيت تطبيق الأمان (الفحص الأول) أو منذ آخر إعادة تعيين لعداد الفيروسات.

  - **Objects that have failed disinfection**

    عدد الملفات التي لم تتم معالجتها على الجهاز العميل.
    يتجاهل هذا الحقل عدد الملفات التي لم تتم معالجتها على الأجهزة المحمولة.

  - **حالة تشفير القرص**

الحالة الحالية لتشفير الملفات على محركات أقراص الجهاز المحلية. للحصول على وصف للحالات، انظر تعليمات Kaspersky Endpoint Security for Windows.

- يوفر القسم **Device status defined by application** المعلومات المتعلقة بحالة الجهاز التي حددها التطبيق المُدار المُثبت على الجهاز. يمكن لحالة الجهاز هذه أن تختلف عن الحالة المحددة في Kaspersky Security Center.

- **Applications**

تسرد علامة التبويب هذه جميع تطبيقات Kaspersky المثبتة على الجهاز العميل. وتحتوي علامة التبويب هذه على الزرين **Start** و**Stop** اللذين يتيحان لك بدء تشغيل تطبيق Kaspersky المحدد وإيقافه (باستثناء عميل الشبكة). يمكنك استخدام هذين الزرين إذا كان المنفذ 15000 UDP متاحًا على الجهاز المُدار لاستلام الإخطارات الفورية من خادم الإدارة. إذا كان الجهاز المُدار غير متاح للإخطارات الفورية، لكن تم تمكين وضع الاتصال المستمر بخادم الإدارة (يتم تمكين **عدم قطع الاتصال عن خادم الإدارة** في القسم **عام**)، فإن الزرين **Start** و**Stop** يكونا متاحين أيضًا. وإلا، فعند محاولة بدء تشغيل التطبيق أو إيقاف تشغيله، يتم عرض رسالة خطأ. يمكنك أيضًا النقر على اسم التطبيق لعرض معلومات عامة عن التطبيق وقائمة بالأحداث التي حدث على الجهاز وإعدادات التطبيق.

- **Active policies and policy profiles**

تسرد علامة التبويب هذه السياسات وملفات تعريف السياسة المعينة حاليًا على الجهاز المُدار.

- **المهام**

في علامة التبويب **المهام**، يمكنك إدارة المهام الخاصة بأجهزة العميل: عرض قائمة المهام الحالية وإنشاء مهام جديدة وإزالتها وبدء المهام وإيقافها وتعديل إعداداتها وعرض نتائج التنفيذ. تتوفر قائمة المهام بناءً على البيانات المستلمة أثناء آخر جلسة لمزامنة الكمبيوتر العميل مع خادم الإدارة. يطلب خادم الإدارة تفاصيل حالة المهمة من الجهاز العميل. وإذا كان المنفذ 15000 UDP متاحًا على الجهاز المُدار لاستلام الإخطارات الفورية من خادم الإدارة، يتم عرض حالة المهمة ويتم تمكين الأزرار الخاصة بإدارة المهمة. إذا تعذر على خادم التنبيهات الوصول إلى الجهاز المدار، لكن تم تمكين وضع الاتصال المستمر بخادم الإدارة (يتم تمكين خيار **عدم قطع الاتصال عن خادم الإدارة** في القسم **عام**)، فإن الإجراءات الخاصة بالمهام تكون متاحة أيضًا.

إذا لم يتم إنشاء الاتصال، فلن يتم عرض الحالة ويتم تعطيل الأزرار.

- **الأحداث**

علامة التبويب **الأحداث** تعرض الأحداث المسجلة على خادم الإدارة للجهاز العميل المحدد.

يمكنك تصدير ونسخ وحذف أحداث الجهاز.

- **مشاكل الأمان**

في علامة التبويب **مشاكل الأمان**، يمكنك عرض مشاكل الأمان وتحريرها وإنشاؤها للجهاز العميل. يمكن إنشاء مشاكل الأمان إما تلقائيًا من خلال تطبيقات Kaspersky المُدارة المثبتة على الجهاز العميل أو يدويًا من قبل المسؤول. على سبيل المثال، إذا قام بعض المستخدمين بنقل برامج ضارة من محركات الأقراص القابلة للإزالة الخاصة بهم إلى الأجهزة بانتظام، فيمكن للمسؤول إنشاء مشكلة أمان. يمكن للمسؤول توفير وصف مختصر للحالة والإجراءات الموصى بها (مثل الإجراءات التأديبية التي سيتم اتخاذها ضد المستخدم) في نص مشكلة الأمان، ويمكنه إضافة رابط للمستخدم أو المستخدمين.

يُطلق على مشكلة أمان تم اتخاذ جميع الإجراءات المطلوبة بشأنها تمت المعالجة. قد يتم اختيار وجود مشاكل أمان غير معالجة كشرط لتغيير حالة الجهاز إلى حرج أو تحذير.

يحتوي هذا القسم على قائمة بمشاكل الأمان التي تم إنشاؤها للجهاز. يتم تصنيف مشاكل الأمان بحسب مستوى الخطورة وبحسب النوع. يتم تحديد نوع مشكلة أمان بواسطة تطبيق Kaspersky، الذي يقوم بإنشاء مشكلة الأمان. يمكنك تمييز مشاكل الأمان التي تمت معالجتها في القائمة عن طريق تحديد خانة الاختيار الموجودة في العمود **تمت المعالجة**.

- **العلامات**

في علامة التبويب **العلامات**، يمكنك إدارة قائمة الكلمات الأساسية المستخدمة للعثور على أجهزة العميل: قم بعرض قائمة بالعلامات الحالية وتعيين علامات من القائمة وتكوين قواعد وضع العلامات تلقائيًا وإضافة علامات جديدة وإعادة تسمية العلامات القديمة وإزالة العلامات.

- Advanced

تتضمن علامة التبويب هذه الأقسام التالية:

- **سجل التطبيقات**. في هذا القسم، يمكنك عرض سجل التطبيقات المثبتة على الجهاز العميل والتحديثات الخاصة بها؛ بالإضافة إلى إعداد عرض سجل التطبيقات.

  يتم توفير معلومات حول التطبيقات المثبتة في حالة تثبيت عميل الشبكة على الجهاز العميل الذي يقوم بإرسال المعلومات المطلوبة إلى خادم الإدارة. يمكنك تكوين إرسال المعلومات إلى خادم الإدارة في نافذة خصائص عميل الشبكة أو سياستها في القسم **المستودعات**.

  النقر على اسم التطبيق يفتح نافذة تحتوي على تفاصيل التطبيق وقائمة بحزم التثبيت المثبتة للتطبيق.

- **الملفات التنفيذية**. يعرض هذا القسم الملفات التنفيذية التي تم العثور عليها على الجهاز العميل.

- **Distribution points**. يوفر هذا القسم قائمة بنقاط التوزيع التي يتفاعل معها الجهاز.

  - **تصدير إلى الملف**

    انقر على زر **تصدير إلى ملف** لحفظ قائمة نقاط التوزيع صالتي يتفاعل معها الجهاز إلى ملف. بشكل افتراضي يقوم التطبيق بتصدير قائمة الأجهزة إلى ملف CSV.

  - **خصائص**

    انقر على زر **خصائص** لعرض نقطة التوزيع التي يتفاعل معها الجهاز وتكوينها.

- **سجل الأجهزة**. في هذا القسم، يمكنك عرض معلومات عن الأجهزة المثبتة على الجهاز العميل.

  في حالة تثبيت عميل الشبكة على جهاز يعمل بنظام Windows، فإنه يرسل إلى خادم الإدارة المعلومات التالية عن أجهزة الجهاز:

  - الذاكرة العشوائية
  - أجهزة تخزين كبيرة السعة
  - اللوحة الأم
  - CPU
  - محولات الشبكة
  - الشاشات
  - محول الفيديو
  - بطاقة الصوت

  في حالة تثبيت عميل الشبكة على جهاز يعمل بنظام Linux أو macOS، فإنه يرسل إلى خادم الإدارة المعلومات التالية فقط عن مكونات الجهاز، إذا وفر نظام التشغيل هذه المعلومات:

  - إجمالي حجم RAM
  - الحجم الإجمالي لأجهزة التخزين عالية السعة
  - اللوحة الأم
  - CPU
  - محولات الشبكة

- **Available updates**. يعرض هذا القسم تحديثات البرامج التي تم العثور عليها على هذا الجهاز والتي لم يتم تثبيتها بعد.

- **الثغرات الأمنية بالبرنامج**. يوفر هذا القسم معلومات حول الثغرات الأمنية في تطبيقات الجهة الخارجية المثبتة على أجهزة العميل.

لحفظ الثغرات الأمنية في ملف، حدد خانات الاختيار الموجودة بجوار الثغرات الأمنية التي ترغب في حفظها ثم انقر على زر **Export to CSV** أو زر **Export to TXT**.

يحتوي القسم على الإعدادات التالية:

- **إظهار الثغرات الأمنية التي يمكن إصلاحها فقط**

إذا تم تمكين هذا الخيار، فسيعرض القسم الثغرات الأمنية التي يمكن إصلاحها عن طريق استخدام تصحيح.

إذا تم تعطيل هذا الخيار، فسيعرض القسم كل من الثغرات الأمنية التي يمكن إصلاحها باستخدام تصحيح، والثغرات الأمنية التي لم يتم إصدار تصحيح لها.

يتم تمكين هذا الخيار افتراضيًا.

- **Vulnerability properties**

انقر على اسم ثغرة أمنية لبرنامج في القائمة لعرض خصائص الثغرة الأمنية للبرنامج المحددة في نافذة منفصلة. في النافذة، يمكنك إجراء ما يلي:

- تجاهل الثغرات الأمنية في البرامج على هذا الجهاز الذي تتم إدارته(في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console).
- عرض قائمة الإصلاحات الموصى بها للثغرة الأمنية.
- حدد تحديثات البرامج يدويًا لإصلاح الثغرات الأمنية (في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console).
- عرض مثيلات الثغرات الأمنية.
- عرض قائمة المهام الحالية لإصلاح الثغرات الأمنية وإنشاء مهام جديدة لإصلاح الثغرات الأمنية.

- **تشخيصات عن بعد**. في هذا القسم، يمكنك إجراء التشخيصات عن بُعد للأجهزة العميلة .

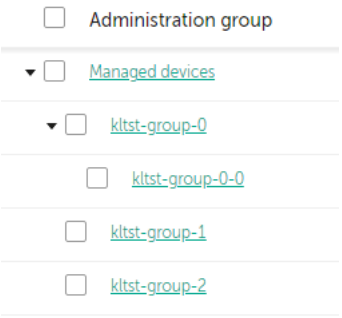
إذا كنت تستخدم PostgreSQL أو MariaDB أو MySQL DBMS، فإن علامة التبويب **الأحداث** قد تعرض قائمة غير كاملة بالأحداث للجهاز العميل المحدد. ويحدث هذا عندما يخزن نظام إدارة قواعد البيانات (DBMS) قدرًا كبيرًا جدًا من الأحداث. ويمكنك زيادة عدد الأحداث المعروضة عن طريق تنفيذ أي مما يلي:

- إزالة الأحداث غير الضرورية.
- تقليل مدة التخزين للأحداث غير الضرورية.

للاطلاع على قائمة كاملة بالأحداث التي تم تسجيلها على خادم الإدارة للجهاز، استخدم التقارير.

إنشاء مجموعات إدارة

فورًا بعد تثبيت Kaspersky Security Center، الترتيب الهرمي لمجموعات الإدارة لا يحتوي إلا على مجموعة إدارة واحدة اسمها **Managed devices**. عند إنشاء ترتيب هرمي لمجموعات الإدارة، يمكنك إضافة أجهزة، بما في ذلك الأجهزة الظاهرية، إلى مجموعة **Managed devices** وكذلك إضافة المجموعات المتداخلة (انظر الشكل أدناه).



عرض الترتيب الهرمي لمجموعات الإدارة

لإنشاء مجموعة إدارة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Hierarchy of groups**.
2. في هيكل مجموعة الإدارة، حدد مجموعة الإدارة التي ستشمل مجموعة الإدارة الجديدة.
3. انقر على الزر **Add**.
4. في نافذة **Name of the new administration group** التي تفتح، أدخل اسمًا للمجموعة، ثم انقر على زر **Add**.

   مجموعة الإدارة الجديدة ذات الاسم المحدد ستظهر في الترتيب الهرمي لمجموعات الإدارة.

يتيح التطبيق إنشاء تسلسل هرمي لمجموعات الإدارة بناءً على هيكل Active Directory أو هيكل شبكة المجال. وكذلك، يمكنك إنشاء هيكل من المجموعات من ملف نصي.

لإنشاء هيكل لمجموعات الإدارة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Hierarchy of groups**.
2. انقر على زر **Import**.

   يبدأ معالج بنية مجموعة الإدارة الجديدة. اتبع إرشادات المعالج.

إضافة أجهزة إلى مجموعة إدارة يدويًا

يمكنك نقل أجهزة إلى مجموعات إدارة تلقائيًا عن طريق إنشاء قواعد لنقل الأجهزة، أو يدويًا عن طريق نقل الأجهزة من إحدى مجموعات الإدارة إلى مجموعة أخرى أو عن طريق إضافة أجهزة إلى مجموعة إدارة محددة. يصف هذا القسم كيفية إضافة أجهزة إلى مجموعة إدارة.

لإضافة جهاز أو أكثر إلى مجموعة إدارة محددة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.
2. انقر على رابط **المسار الحالي:** `<current path>` فوق القائمة.

3. في النافذة التي تفتح، حدد مجموعة الإدارة التي تريد إضافة الأجهزة إليها

4. انقر على زر **Add devices**.

يبدأ تشغيل معالج نقل الأجهزة.

5. أنشئ قائمة الأجهزة التي ترغب في إضافتها إلى مجموعة الإدارة.

لا يمكنك إضافة إلى الأجهزة التي تمت إضافة معلومات حولها بالفعل إلى قاعدة بيانات خادم الإدارة إما عند اتصال الجهاز أو بعد اكتشاف الجهاز.

حدد كيف ترغب في إضافة أجهزة إلى القائمة:

- انقر على زر **Add devices** ثم حدد الأجهزة بإحدى الطرق التالية:
  - حدد أجهزة من قائمة الأجهزة التي اكتشفها خادم الإدارة.
  - حدد عنوان IP لجهاز أو نطاق IP.

يجب ألا يحتوي نطاق IP على أكثر من 1048576 عنوانًا.

  - حدد اسم NetBIOS أو اسم DNS لجهاز.

يجب ألا يحتوي حقل اسم الجهاز على مسافات بين الأحرف أو الأحرف المحظورة التالية: \ / * : ; ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

- انقر على زر **Import devices from file** لاستيراد قائمة بالأجهزة من ملف .txt. كل عنوان جهاز أو اسم جهاز يجب أن يُحدد على سطر منفصل.

يجب ألا يحتوي الملف على مسافات بين الأحرف أو الأحرف المحظورة التالية: \ / * : ; ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. اعرض قائمة بالأجهزة التي يجب إضافتها إلى مجموعة الإدارة. يمكنك تعديل القائمة بإضافة أجهزة أو إزالتها.

7. بعد التأكد أن القائمة صحيحة، انقر على زر **Next**.

سيعالج المعالج قائمة الجهاز ويعرض النتيجة. يتم إضافة الأجهزة التي تمت معالجتها بنجاح إلى مجموعة الإدارة ويتم عرضها في قائمة الأجهزة بأسماء أنشأها خادم الإدارة.

نقل أجهزة أو مجموعات إلى مجموعة إدارة يدويًا

يمكنك نقل أجهزة من مجموعة إدارة إلى أخرى أو من مجموعة الأجهزة غير المخصصة إلى مجموعة إدارة.

يمكنك أيضًا نقل المجموعات أو مصفوفات الخادم من مجموعة إدارة إلى أخرى. عندما تنقل مجموعة أو مصفوفة خادم إلى مجموعة أخرى، فإن جميع عقدها تنتقل معها، لأن المجموعة وأي من عُقدها تنتمي دائمًا إلى مجموعة الإدارة نفسها. عند تحديد عقدة مجموعة واحدة في علامة التبويب **Devices**، يصبح الزر **Move to group** غير متاح.

لنقل جهاز أو عدة أجهزة أو مجموعات إلى مجموعة إدارة محددة:

1. افتح مجموعة الإدارة التي ترغب في نقل أجهزة منها. لفعل هذا، قد بأحد الإجراءات التالية:

- لفتح مجموعة إدارة، في القائمة الرئيسية ، انتقل إلى **Assets (Devices)** ← **Managed devices**، وانقر فوق ارتباط المسار في الحقل **Current path**، وحدد مجموعة الإدارة في الجزء الأيمن الذي يفتح.
- لفتح مجموعة **Unassigned devices**، في القائمة الرئيسة، انتقل إلى **Discovery & deployment** ← **Unassigned devices**.

2. إذا كانت مجموعة الإدارة تحتوي على مجموعات أو مصفوفات خادم، يتم تقسيم القسم **Managed devices** إلى علامتي تبويب—علامة التبويب **Devices** وعلامة التبويب **Clusters and server arrays**. افتح علامة التبويب الخاصة بالعنصر الذي تريد نقله.

3. حدد خانات الاختيار الموجودة بجوار الأجهزة أو المجموعات التي ترغب في نقلها إلى مجموعة أخرى.

4. انقر على زر **Move to group** .

5. في التسلسل الهرمي لمجموعات الإدارة، حدد خانة الاختيار الموجودة بجوار مجموعة الإدارة التي ترغب في نقل الأجهزة أو المجموعات المحددة إليها.

6. انقر فوق زر **Move**.

يتم نقل الأجهزة أو المجموعات المحددة إلى مجموعة الإدارة المحددة.

إنشاء قواعد نقل الجهاز

يمكنك تعيين قواعد نقل الجهاز التي تخصص تلقائيًا الأجهزة لمجموعات الإدارة.

لإنشاء قاعدة نقل:

1. في القائمة الرئيسية، انتقل إلى علامة التبويب **Assets (Devices)** ← **Moving rules**.

2. انقر على **Add**.

3. في النافذة التي تفتح، حدد المعلومات التالية في تبويب **General**:

- **Rule name**

  أدخل اسمًا للقاعدة الجديدة.

  إذا كنت تنسخ قاعدة، ستحصل القاعدة الجديدة على نفس اسم قاعدة المصدر، ولكن يُضاف فهرس بتنسيق () إلى الاسم، مثل: (1).

- **Administration group**

  حدد مجموعة الإدارة التي سيتم نقل الأجهزة إليها تلقائيًا.

- **القاعدة النشطة**

  إذا تم تفعيل هذا الخيار، يتم تفعيل القاعدة وتبدأ في العمل بعد حفظها.

  في حال تعطيل هذا الخيار، يتم إنشاء القاعدة ولكن لا يتم تفعيلها لن تعمل القاعدة حتى تقوم بتفعيل هذا الخيار.

- **Move only devices that do not belong to an administration group**

  إذا تم تفعيل هذا الخيار، لن يتم نقل إلا الأجهزة غير المعينة إلى المجموعة المحددة.

  إذا تم تعطيل هذا الخيار، سيتم نقل الأجهزة التي تنتمي إلى مجموعات إدارة أخرى بالفعل وكذلك الأجهزة غير المعينة إلى المجموعة المحددة.

- **Apply rule**

يمكنك تحديد أي من الخيارات التالية:

- **Run once for each device**

يتم تطبيق القاعدة مرة واحدة لكل جهاز يتوافق مع معاييرك.

- **Run once for each device, then at every Network Agent reinstallation**

يتم تطبيق القاعدة مرة واحدة لكل جهاز يتوافق مع المعايير الخاصة بك، ثم لا يتم تطبيق ذلك إلا عند إعادة تثبيت عميل الشبكة على هذه الأجهزة.

- **Apply rule continuously**

يتم تطبيق القاعدة وفقًا للجدول الزمني الذي يقوم خادم الإدارة بإعداده تلقائيًا (كل عدة ساعات في العادة).

4. في علامة تبويب **Rule conditions**، حدد معيارًا واحدًا على الأقل يتم من خلاله نقل الأجهزة إلى مجموعة إدارة.

5. انقر على **Save**.

يتم إنشاء قاعدة النقل. يتم عرضها في قائمة قواعد النقل.

كلما ارتفع المركز في القائمة، زادت أولوية القاعدة. ولزيادة أو تقليل أولوية قاعدة نقل، انقل القاعدة لأعلى أو لأسفل في القائمة، على التوالي، باستخدام الماوس.

إذا تم تحديد الخيار **Apply rule continuously**، فسيتم تطبيق قاعدة النقل بغض النظر عن إعدادات الأولوية. يتم تطبيق هذه القواعد وفقًا للجدول الزمني الذي يقوم خادم الإدارة بإعداده تلقائيًا.

إذا توافقت سمات الجهاز مع شروط قواعد متعددة، يتم نقل الجهاز إلى المجموعة الهدف الخاصة بالقاعدة ذات الأولوية الأعلى (أي التي لها أعلى رتبة في قائمة القواعد).

نسخ قواعد نقل الجهاز

يمكنك نسخ قواعد النقل، على سبيل المثال إذا كنت ترغب في وضع عدة قواعد متماثلة لعدة مجموعات إدارة مختلفة.

لنسخ قاعدة نقل موجودة بالفعل:

1. قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل إلى علامة التبويب **Assets (Devices)** ← **Moving rules**.
- في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Deployment & assignment** ← **Moving rules**.

يتم عرض قائمة قواعد النقل.

2. حدد خانة الاختيار الموجودة بجوار القاعدة التي ترغب في نسخها.

3. انقر على **Copy** .

4. في النافذة التي تفتح، قم بتغيير المعلومات التالية في تبويب **General** أو لا تقم بأي تغييرات إذا كنت لا ترغب إلا في نسخ القاعدة دون تغيير إعداداتها:

- **Rule name**

أدخل اسمًا للقاعدة الجديدة.

إذا كنت تنسخ قاعدة، ستحصل القاعدة الجديدة على نفس اسم قاعدة المصدر، ولكن يُضاف فهرس بتنسيق () إلى الاسم، مثل: (1).

- **Administration group**

حدد مجموعة الإدارة التي سيتم نقل الأجهزة إليها تلقائيًا.

- **القاعدة النشطة**

إذا تم تفعيل هذا الخيار، يتم تفعيل القاعدة وتبدأ في العمل بعد حفظها.

في حال تعطيل هذا الخيار، يتم إنشاء القاعدة ولكن لا يتم تفعيلها لن تعمل القاعدة حتى تقوم بتفعيل هذا الخيار.

- **Move only devices that do not belong to an administration group**

إذا تم تفعيل هذا الخيار، لن يتم نقل إلا الأجهزة غير المعينة إلى المجموعة المحددة.

إذا تم تعطيل هذا الخيار، سيتم نقل الأجهزة التي تنتمي إلى مجموعات إدارة أخرى بالفعل وكذلك الأجهزة غير المعينة إلى المجموعة المحددة.

- **Apply rule**

يمكنك تحديد أي من الخيارات التالية:

- **Run once for each device**

يتم تطبيق القاعدة مرة واحدة لكل جهاز يتوافق مع معاييرك.

- **Run once for each device, then at every Network Agent reinstallation**

يتم تطبيق القاعدة مرة واحدة لكل جهاز يتوافق مع المعايير الخاصة بك، ثم لا يتم تطبيق ذلك إلا عند إعادة تثبيت عميل الشبكة على هذه الأجهزة.

- **Apply rule continuously**

يتم تطبيق القاعدة وفقًا للجدول الزمني الذي يقوم خادم الإدارة بإعداده تلقائيًا (كل عدة ساعات في العادة).

5. في علامة تبويب **Rule conditions**، حدد معيارًا واحدًا على الأقل للأجهزة التي تريد نقلها تلقائيًا.

6. انقر على **Save**.

تم إنشاء قاعدة النقل الجديدة. يتم عرضها في قائمة قواعد النقل.

شروط قاعدة نقل الجهاز

عند إنشاء قاعدة أو نسخها لنقل أجهزة العميل إلى مجموعات الإدارة، في علامة التبويب **Rule conditions**، يمكنك تعيين الشروط لنقل الأجهزة. لتحديد الأجهزة التي تريد نقلها، يمكنك استخدام المعايير التالية:

- العلامات المخصصة لأجهزة العميل.
- معلمات الشبكة. على سبيل المثال، يمكنك نقل الأجهزة بعناوين IP من نطاق محدد.
- التطبيقات المُدارة المثبتة على أجهزة العميل، على سبيل المثال، عميل الشبكة أو خادم الإدارة.
- الأجهزة الافتراضية، وهي أجهزة العميل.
- معلومات حول الوحدة التنظيمية لـ Active Directory (OU) مع الأجهزة العميلة.
- معلومات حول مقطع سحابي مع أجهزة العميل.

أدناه، يمكنك العثور على وصف حول كيفية تحديد هذه المعلومات في قاعدة نقل الجهاز.

إذا حددت عدة شروط في القاعدة، فسيعمل عامل التشغيل المنطقي AND وستنطبق جميع الشروط في نفس الوقت. إذا لم تحدد أي خيارات أو احتفظت ببعض الحقول فارغة، فإن هذه الشروط لا تنطبق.

علامة تبويب Tags

في علامة التبويب هذه، يمكنك تكوين قاعدة نقل الجهاز بناءً على علامات الجهاز التي تمت إضافتها مسبقًا إلى أوصاف أجهزة العميل. للقيام بذلك، حدد العلامات المطلوبة. يمكنك أيضًا تمكين الخيارات التالية:

- **Apply to devices without the specified tags**

إذا تم تمكين هذا الخيار، فسيتم استبعاد جميع الأجهزة ذات العلامات المحددة من قاعدة نقل الجهاز. إذا تم تعطيل هذا الخيار، فإن قاعدة نقل الجهاز تنطبق على الأجهزة التي تحتوي على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

- **Apply if at least one specified tag matches**

إذا تم تمكين هذا الخيار، فسيتم تطبيق قاعدة نقل الجهاز على الأجهزة العميلة التي تحتوي على علامة واحدة على الأقل من العلامات المحددة. إذا تم تعطيل هذا الخيار، فإن قاعدة نقل الجهاز تنطبق على الأجهزة التي تحتوي على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

علامة تبويب Network

في علامة التبويب هذه، يمكنك تحديد بيانات الشبكة للأجهزة التي تراها قاعدة نقل الجهاز:

- **Device name on the Windows network**

اسم شبكة Windows (اسم NetBIOS) للجهاز، أو عنوان IPv4 أو IPv6.

- **Windows domain**

تنطبق قاعدة نقل الجهاز على جميع الأجهزة المضمنة في مجال Windows المحدد.

- **DNS name of the device**

اسم مجال DNS لجهاز العميل الذي تريد نقله. املأ هذا الحقل إذا كانت شبكتك تتضمن خادم DNS.

إذا تم تعيين ترتيب حساس لحالة الأحرف لقاعدة البيانات التي تستخدمها في Kaspersky Security Center، احتفظ بالحالة عند تحديد اسم DNS للجهاز. خلاف ذلك، لن تعمل قاعدة نقل الجهاز.

- **DNS domain**

تنطبق قاعدة نقل الجهاز على جميع الأجهزة المضمنة في لاحقة DNS الرئيسية المحددة. املأ هذا الحقل إذا كانت شبكتك تتضمن خادم DNS.

- **IP range**

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.

يتم تعطيل هذا الخيار افتراضيًا.

- **IP address for connection to Administration Server**

إذا تم تمكين هذا الخيار، يمكنك تعيين عناوين IP التي تتصل بها الأجهزة العميلة بخادم الإدارة. للقيام بذلك، حدد نطاق IP الذي يتضمن جميع عناوين IP الضرورية.

يتم تعطيل هذا الخيار افتراضيًا.

- **Device is in IP range**

إذا تم تمكين هذا الخيار، فيمكنك تحديد نطاق IP الذي أضفته مسبقًا في القسم **IP ranges**. ويجب أن تكون الأجهزة ذات الصلة مدرجة في نطاق IP المحدد.

يتم تعطيل هذا الخيار افتراضيًا.

- **Connection profile changed**

حدد إحدى القيم التالية:

- **نعم**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي تم تغيير ملف تعريف الاتصال بها.
- **لا**. تنطبق قاعدة نقل الجهاز فقط على أجهزة العميل التي لم يتغير ملف تعريف الاتصال الخاص بها.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

- **Managed by a different Administration Server**

حدد إحدى القيم التالية:

- **نعم**. تنطبق قاعدة نقل الجهاز فقط على أجهزة العميل المُدارة بواسطة خوادم الإدارة الأخرى. تختلف هذه الخوادم عن الخادم الذي تقوم بتكوين قاعدة نقل الجهاز عليه.
- **لا**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي يديرها خادم الإدارة الحالي.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

علامة تبويب Applications

في علامة التبويب هذه، يمكنك تكوين قاعدة نقل الجهاز بناءً على التطبيقات المدارة وأنظمة التشغيل المثبتة على الأجهزة العميلة:

- **Network Agent is installed**

حدد إحدى القيم التالية:

- **نعم**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي تم تثبيت عميل الشبكة عليها.
- **لا**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي لم يتم تثبيت عميل الشبكة عليها.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

- **Applications**

حدد التطبيقات المُدارة التي يجب تثبيتها على الأجهزة العميلة، لذلك تنطبق قاعدة نقل الجهاز على هذه الأجهزة. على سبيل المثال، يمكنك تحديد **Kaspersky Security Center 15 Network Agent** أو **Kaspersky Security Center 15 Administration Server** .

إذا لم تحدد أي تطبيق مُدار، فلن يتم تطبيق الشرط.

- **Operating system version**

يمكنك استبعاد أجهزة العميل بناءً على إصدار نظام التشغيل. لهذا الغرض، حدد أنظمة التشغيل التي يجب تثبيتها على أجهزة العميل. نتيجة لذلك، يتم تطبيق قاعدة نقل الجهاز على الأجهزة العميلة بأنظمة التشغيل المحددة.

إذا لم تقم بتمكين هذا الخيار، فلن يتم تطبيق الشرط. يتم تعطيل هذا الخيار بشكل افتراضي.

- **Operating system bit size**

يمكنك استبعاد أجهزة العميل حسب أحجام بت نظام التشغيل. في حقل **Operating system bit size**، يمكنك تحديد إحدى القيم التالية:

- **غير معروف**
- **x86**
- **AMD64**
- **IA64**

للتحقق من حجم بت نظام التشغيل لأجهزة العميل:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← قسم **Managed devices**.
2. انقر على الزر **إعدادات الأعمدة** (⚙) على اليسار.
3. حدد خيار **Operating system bit size**، ثم انقر على زر **Save**.

   بعد ذلك، يتم عرض حجم بت نظام التشغيل لكل جهاز مُدار.

- **Operating system service pack version**

في هذا الحقل، يمكنك تحديد إصدار حزمة نظام التشغيل (بتنسيق X.Y)، والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز. وبشكل افتراضي، لا يتم تحديد أي قيمة إصدار.

- **User certificate**

حدد إحدى القيم التالية:

- **Installed**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة المحمولة المزودة بشهادة الهاتف المحمول.
- **Not installed**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة المحمولة بدون شهادة الهاتف المحمول.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

- **Operating system build**

> لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم نسخة مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين قاعدة نقل الجهاز لجميع أرقام النسخة باستثناء الرقم المحدد.

- **Operating system release number**

> لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم إصدار مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين قاعدة نقل الجهاز لجميع أرقام الإصدار باستثناء الرقم المحدد.

علامة تبويب Virtual machines

في علامة التبويب هذه، يمكنك تكوين قاعدة نقل الجهاز وفقًا لما إذا كانت أجهزة العميل عبارة عن أجهزة افتراضية أو جزءًا من بنية أساسية لسطح المكتب الافتراضي (VDI):

- **This is a virtual machine**

  يمكنك في القائمة المنسدلة تحديد واحدة مما يلي:

  - **N/A**. الشرط لا ينطبق.
  - **لا**. نقل الأجهزة التي لا تعد أجهزة افتراضية.
  - **نعم**. نقل الأجهزة التي تعد أجهزة ظاهرية.

- **Virtual machine type**
- **Part of Virtual Desktop Infrastructure**

  يمكنك في القائمة المنسدلة تحديد واحدة مما يلي:

  - **N/A**. الشرط لا ينطبق.
  - **لا**. نقل الأجهزة التي ليست جزءًا من VDI.
  - **نعم**. نقل الأجهزة التي تُعد جزءًا من VDI

علامة التبويب Domain controller

في علامة التبويب هذه، يمكنك تحديد أنه من الضروري نقل الأجهزة المضمنة في الوحدة التنظيمية للمجال. يمكنك أيضًا نقل الأجهزة من جميع الوحدات التنظيمية الفرعية للوحدة التنظيمية للمجال المحدد:

- **Device is included in the following organizational unit**

  إذا تم تمكين هذا الخيار، يتم تطبيق قاعدة نقل الجهاز على الأجهزة من الوحدة التنظيمية للمجال المحددة في القائمة ضمن الخيار.

  يتم تعطيل هذا الخيار افتراضيًا.

- **Include child organizational units**

  إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من الوحدات المؤسسية التابعة لوحدات Active Directory المؤسسية.

  يتم تعطيل هذا الخيار افتراضيًا.

- **Move devices from child units to corresponding subgroups**
- **Create subgroups corresponding to containers of newly detected devices**
- **Delete subgroups that are not present in the domain**
- **Device is included in the following domain security group**

  إذا تم تمكين هذا الخيار، فسيتم تطبيق قاعدة نقل الجهاز على الأجهزة من مجموعة أمان المجال المحددة في القائمة ضمن الخيار.

  يتم تعطيل هذا الخيار افتراضيًا.

علامة التبويب Cloud segments

في علامة التبويب هذه، يمكنك تحديد أنه من الضروري نقل الأجهزة التي تنتمي إلى قطاعات سحابية معينة:

- **Device is in a cloud segment**

إذا حددت هذا الخيار، فسيتم تطبيق قاعدة نقل الجهاز على الأجهزة العميلة التي تنتمي إلى قطاع السحابة. يمكنك تحديد مقطع السحابة المطلوب حتى شبكة فرعية في القائمة الموجودة أسفل الخيار.

يتم تعطيل هذا الخيار بشكل افتراضي.

- **Include child objects**

إذا حددت هذا الخيار، فإن قاعدة نقل الجهاز لا تنطبق فقط على مقطع السحابة المحدد، ولكن أيضًا على الكائنات الفرعية لهذا المقطع.

يتم تعطيل هذا الخيار بشكل افتراضي.

- **Move devices from nested objects to corresponding subgroups**
- **Create subgroups corresponding to containers of newly detected devices**
- **Delete subgroups for which no match is found in the cloud segments**
- **Device discovered by using the API**

يمكنك تحديد ما إذا كان تم اكتشاف الجهاز بواسطة أدوات API في القائمة المنسدلة:

- **AWS**. يتم اكتشاف الجهاز باستخدام AWS API، أي أن الجهاز يوجد بالفعل في بيئة سحابة AWS.
- **Azure**. يتم اكتشاف الجهاز باستخدام Azure API، أي أن الجهاز يوجد بالفعل في بيئة سحابة Azure.
- **Google Cloud**. يتم اكتشاف الجهاز باستخدام Google API، أي أن الجهاز موجود بالفعل في بيئة Google cloud.
- **لا**. لا يمكن اكتشاف الجهاز باستخدام AWS أو Azure أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة لكن لا يمكن اكتشافه باستخدام واجهة برمجة التطبيق (API).
- **لا توجد قيمة**. هذا الشرط لا ينطبق.

حول مصفوفات المجموعات والخادم

يدعم Kaspersky Security Center تقنية المجموعة. إذا قام عميل الشبكة بإرسال معلومات لخادم الإدارة لتأكيد أن التطبيق المثبت على جهاز عميل أصبح جزءًا من مصفوفة خادم، فيصبح هذا الجهاز العميل عقدة نظام المجموعة.

إذا كانت مجموعة الإدارة تحتوي على مجموعات أو مصفوفات خادم، فإن صفحة **Managed devices** تعرض علامتي تبويب - واحدة الأجهزة الفردية، وواحدة للمجموعات ومصفوفات الخادم. بعد اكتشاف الأجهزة المدارة كعُقد لنظام المجموعة، تتم إضافة المجموعة ككائن فردي إلى علامة التبويب **Clusters and server arrays**.

يتم إدراج عقد المجموعة أو مصفوفة الخادم في علامة التبويب **Devices**، جنبًا إلى جنب مع الأجهزة المدارة الأخرى. ويمكنك عرض خصائص العُقد كأجهزة فردية وتنفيذ عمليات أخرى، لكن لا يمكنك حذف عقدة مجموعة أو نقلها إلى مجموعة إدارة أخرى بشكل منفصل عن المجموعة الخاصة بها. ويمكنك فقط حذف أو نقل مجموعة كاملة.

يمكنك إجراء العمليات التالية باستخدام المجموعات أو مصفوفات الخادم:

- عرض الخصائص
- نقل المجموعة أو صفيف الخادم إلى مجموعة إدارة أخرى

  عندما تنقل مجموعة أو مصفوفة خادم إلى مجموعة أخرى، فإن جميع عقدها تنتقل معها، لأن المجموعة وأي من عُقدها تنتمي دائمًا إلى مجموعة الإدارة نفسها.

- حذف

من المعقول حذف مجموعة أو مصفوفة خادم فقط في حالة عدم وجود المجموعة أو مصفوفة الخادم في شبكة المؤسسة بعد الآن. إذا كانت المجموعة لا تزال مرئية على شبكتك وعميل الشبكة لديك ولا يزال تطبيق الأمان من Kaspersky مثبتًا على عُقد المجموعة، فإن Kaspersky Security Center يعيد المجموعة المحذوفة وعُقدها مرة أخرى إلى قائمة الأجهزة المدارة تلقائيًا.

خصائص مجموعة أو مصفوفة خادم

لعرض إعدادات مجموعة أو مصفوفة خادم:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices** ← **Clusters and server arrays**.

   يتم عرض قائمة المجموعات ومصفوفات الخادم.

2. انقر فوق اسم المجموعة أو مصفوفة الخادم المطلوبة.

   يتم عرض نافذة خصائص المجموعة أو مصفوفة الخادم المحددة.

General

يعرض القسم **General** معلومات عامة حول نظام المجموعة أو مصفوفة الخادم. يتم تقديم المعلومات بناءً على البيانات المستلمة أثناء المزامنة الأخيرة لعُقد المجموعة مع خادم الإدارة:

- **Name**
- **الوصف**
- **مجال Windows**

  مجال Windows أو مجموعة العمل، التي تحتوي على المجموعة أو مصفوفة الخادم.

- **اسم NetBIOS**

  اسم شبكة Windows للمجموعة أو مصفوفة الخادم.

- **اسم DNS**

  اسم مجال DNS للمجموعة أو مصفوفة الخادم.

المهام

في علامة التبويب **المهام**، يمكنك إدارة المهام المعينة للمجموعة أو مصفوفة الخادم: عرض قائمة المهام الحالية؛ وإنشاء أخرى جديدة؛ وإزالة المهام وبدئها وإيقافها؛ وتعديل إعدادات المهمة؛ وعرض نتائج التنفيذ. تتعلق المهام المدرجة بتطبيق أمان Kaspersky المثبت على عقد المجموعة. يتلقى Kaspersky Security Center قائمة المهام وتفاصيل حالة المهمة من عقد المجموعة. إذا لم يتم إنشاء اتصال، فلا يتم عرض الحالة.

Nodes

تعرض علامة التبويب هذه قائمة بالعقد المضمنة في المجموعة أو مصفوفة الخادم. ويمكنك النقر فوق اسم عقدة لعرض نافذة خصائص الجهاز.

تطبيق Kaspersky

قد تحتوي نافذة الخصائص أيضًا على علامات تبويب إضافية تتضمن المعلومات والإعدادات المتعلقة بتطبيق أمان Kaspersky المثبت على عقد المجموعة.

عرض وتكوين الإجراءات عندما تكون حالة الأجهزة غير نشطة

إذا كانت الأجهزة العميلة ضمن مجموعة ما غير نشطة، فبإمكانك الحصول على إشعارات عنها. يمكنك أيضًا حذف مثل هذه الأجهزة تلقائيًا.

لعرض أو تكوين الإجراءات عندما تكون حالة الأجهزة في المجموعة غير نشطة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Hierarchy of groups**.
2. انقر على اسم مجموعات الإدارة المطلوبة.

   ستفتح نافذة خصائص مجموعة الإدارة.
3. في نافذة الخصائص، انتقل إلى تبويب **Settings**.
4. قم بتفعيل الخيارات التالية أو تعطيلها في قسم **Inheritance**:

- **Inherit from parent group**

سيتم توريث الإعدادات الموجودة في هذا القسم من المجموعة الرئيسية التي تم تضمين الجهاز العميل بها. إذا تم تمكين هذا الخيار، فسيتم قفل الإعدادات الموجودة ضمن **نشاط الجهاز على الشبكة** من إحداث أي تغييرات.

يكون هذا الخيار متاحًا فقط إذا كانت مجموعة الإدارة لديها مجموعة رئيسية.

يتم تمكين هذا الخيار افتراضيًا.

- **Force inheritance of settings in child groups**

سيتم توزيع قيم الإعداد إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم قفل هذه الإعدادات.

يتم تعطيل هذا الخيار افتراضيًا.

5. في قسم **Device activity**، قم بتمكين أو تعطيل الخيارات التالية:

- **Notify the administrator if the device has been inactive for longer than (days)**

إذا تم تمكين هذا الخيار، فسوف يتلقى المسؤول إشعارات حول الأجهزة غير المفعلة. يمكنك تحديد الفاصل الزمني الذي يتم بعد حلوله إنشاء حدث **استمر الجهاز في حالة عدم النشاط على الشبكة منذ فترة طويلة**. الفاصل الزمني الافتراضي هو 7 أيام.

يتم تمكين هذا الخيار افتراضيًا.

- **Remove the device from the group if it has been inactive for longer than (days)**

إذا تم تمكين هذا الخيار، فيمكنك تحديد الفترة الزمنية التي يتم بعدها إزالة الجهاز تلقائيًا من المجموعة. الفاصل الزمني الافتراضي هو 60 أيام.

يتم تمكين هذا الخيار افتراضيًا.

6. انقر على **Save**.

تم حفظ وتطبيق التغييرات الخاصة بك.

حول حالات الجهاز

يخصص Kaspersky Security Center حالة لكل جهاز مُدار. تعتمد الحالة الخاصة على ما إذا كانت الشروط التي حددها المستخدم قد استوفيت أم لا. في بعض الحالات، عند تعيين حالة لجهازٍ ما، يأخذ Kaspersky Security Center في الاعتبار علامة رؤية الجهاز على الشبكة (انظر الجدول أدناه). على سبيل المثال: إذا تم تعيين الحالة حرج إلى جهاز مُدار بسبب عدم استيفاء شرط Databases are outdated ثم بعد ذلك تم تعيين علامة الرؤية للجهاز، يتم تعيين حالة موافق إلى الجهاز. إذا لم يعثر Kaspersky Security Center على جهاز على الشبكة في غضون ساعتين، سيتم تعيين علامة رؤية الجهاز إلى غير مرئي.

الحالات كما يلي:

- حرج أو حرج/مرئي
- تحذير أو تحذير/مرئي
- موافق أو موافق/مرئي

يسرد الجدول أدناه الشروط الافتراضية التي يجب استيفائها لتعيين الحالة حرج أو تحذير إلى جهاز، مع جميع القيم المحتملة.

شروط تعيين الحالة إلى الجهاز

الشرط	وصف الشرط	القيم المتوفرة
Security application is not installed	عميل الشبكة مثبّت على الجهاز، إلا أن تطبيق الأمان غير مثبّت.	• زر التبديل قيد التشغيل. • زر التبديل متوقف.
Too many viruses detected	تم العثور على بعض الفيروسات على الجهاز عن طريق تنفيذ إحدى مهام اكتشاف الفيروسات، على سبيل المثال مهمة فحص البرامج الضارة، ويتجاوز عدد الفيروسات التي تم العثور عليها القيمة المحددة.	أكثر من 0.
Real-time protection level differs from the level set by the Administrator	الجهاز مرئي على الشبكة، إلا أن مستوى الحماية في الوقت الحقيقي يختلف عن المستوى الذي حدده المسؤول (في الشرط) لحالة الجهاز.	• متوقف. • متوقف مؤقتًا. • قيد التشغيل.
Malware scan has not been performed in a long time	يكون الجهاز مرئيًا على الشبكة ويتم تثبيت تطبيق أمان على الجهاز، لكن لا يتم تشغيل أي من مهمة فحص البرامج الضارة ولا مهمة فحص محلية خلال الفاصل الزمني المحدد. لا ينطبق الشرط إلا على الأجهزة التي تمت إضافتها إلى قاعدة بيانات خادم الإدارة قبل 7 أيام أو أكثر.	أكثر من يوم واحد.
Databases are outdated	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لم يتم تحديث قواعد بيانات مكافحة الفيروسات على هذا الجهاز خلال الفاصل الزمني المحدد. لا ينطبق الشرط إلا على الأجهزة التي تمت إضافتها إلى قاعدة بيانات خادم الإدارة قبل يوم واحد أو أكثر.	أكثر من يوم واحد.
Not connected in a long time	يتم تثبيت عميل الشبكة على الجهاز، ولكن لم يتم اتصال الجهاز بخادم الإدارة خلال الفاصل الزمني المحدد نظرًا لإيقاف تشغيل الجهاز.	أكثر من يوم واحد.
Active threats are detected	يتجاوز عدد الكائنات التي لم تتم معالجتها في المجلد **Active threats** القيمة المحددة.	أكثر من 0 عناصر.

الشرط	وصف الشرط	القيم المتوفرة
Restart is required	الجهاز مرئي على الشبكة، إلا إن أحد التطبيقات يتطلب إعادة تشغيل الجهاز لمدة أطول من الفاصل الزمني المحدد ولأحد الأسباب المحددة.	أكثر من 0 دقائق.
Incompatible applications are installed	الجهاز مرئي على الشبكة، إلا إن مخزون البرنامج المنفَّذ عبر عميل الشبكة قد اكتشف تطبيقات غير متوافقة مثبتة على الجهاز.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Software vulnerabilities have been detected	الجهاز مرئي على الشبكة وعميل الشبكة مثبت على الجهاز، إلا أن مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة قد اكتشفت وجود ثغرات أمنية بمستوى الخطورة المحدد في التطبيقات المثبّتة على الجهاز.	• حرج. • مرتفع. • متوسط. • تجاهل إذا تعذر إصلاح الثغرات الأمنية. • تجاهل إذا تم تعيين تحديث للتثبيت.
License expired	الجهاز مرئي على الشبكة، إلا إن الترخيص قد انتهى.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
License expires soon	الجهاز مرئي على الشبكة، إلا أن الترخيص سينتهي على الجهاز خلال فترة أقل من عدد الأيام المحدد.	أقل من 0 يوم.
Check for Windows Update updates has not been performed in a long time	الجهاز مرئي على الشبكة، لكن لم يتم تشغيل مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة خلال الفاصل الزمني المحدد.	أكثر من يوم واحد.
Invalid encryption status	عميل الشبكة مثبت على الجهاز، إلا إن نتيجة تشفير الجهاز مساوية للقيمة المحددة.	• لا تتفق مع السياسة بسبب رفض المستخدم (بالنسبة للأجهزة الخارجية فقط). • لا تتوافق مع السياسة بسبب وجود خطأ. • إعادة التشغيل مطلوبة عند تطبيق السياسة. • لم يتم تحديد سياسة تشفير. • غير مدعوم • عند تطبيق السياسة.
Mobile device settings do not comply with the policy	إعدادات الجهاز المحمول تختلف عن الإعدادات المحددة في سياسة Kaspersky Endpoint Security for Android أثناء التحقق من قواعد الامتثال.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Unprocessed security issues detected	تم العثور على بعض مشكلات الأمان التي لم تتم معالجتها على الجهاز. يمكن إنشاء مشاكل الأمان إما تلقائيًا من خلال تطبيقات Kaspersky المُدارة المثبتة على الجهاز العميل أو يدويًا من قبل المسؤول.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Device status defined by application	تم تحديد حالة الجهاز بواسطة التطبيق المدار. يمكن أن يكون للأجهزة المدارة حالة محددة بواسطة التطبيقات المدارة بغض النظر عن إعدادات Kaspersky Security Center. بعد أن تعيد هذه الحالة إحدى الحالات المحددة بواسطة Kaspersky Security Center، يُعين خادم الإدارة الحالة الأكثر أهمية للجهاز الذي تتم إدارته بواسطة التطبيق المُدار والتي يتم تعيينها بواسطة خادم الإدارة. وتمتلك الحالات المحددة بواسطة التطبيقات المدارة أوصافًا تنقلها التطبيقات المدارة. ويمكنك عرض الأوصاف في قائمة الأجهزة المدارة، في العمود **Status description**.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Device is out of disk space	مساحة القرص الشاغرة على الجهاز أقل من القيمة المحددة أو أنه يتعذر مزامنة الجهاز مع خادم الإدارة. يتم تغيير الحالة حرج أو تحذير إلى الحالة جيد عند مزامنة الجهاز بنجاح مع خادم الإدارة وتكون المساحة الفارغة على الجهاز أكبر من أو تساوي القيمة المحددة.	أكثر من 0 ميجابايت
Device has become unmanaged	أثناء اكتشاف الأجهزة، تم التعرف على الجهاز بأنه مرئي على الشبكة، لكن فشلت أكثر من ثلاث محاولات للمزامنة مع خادم الإدارة.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Protection is disabled	الجهاز مرئي على الشبكة، إلا إنه قد تم تعطيل تطبيق الأمان على الجهاز لمدة أطول من الفاصل الزمني المحدد. في هذه الحالة، تكون حالة تطبيق الأمان متوقف أو فشل، ويختلف عما يلي: جارٍ البدء أو قيد التشغيل أو معلق.	أكثر من 0 دقائق.
Security application is not running	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لا يعمل.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.

يسمح لك Kaspersky Security Center بإعداد التبديل التلقائي لحالة الجهاز في مجموعة إدارة عند استيفاء الشروط المحددة. عند استيفاء الشروط المحددة، يتم تعيين الجهاز العميل إلى إحدى الحالات التالية: حرج أو تحذير. عند عدم استيفاء الشروط المحددة، يتم تعيين حالة الجهاز العميل على موافق .

يمكن وجود حالات مختلفة لقيم مختلفة لنفس الشرط. على سبيل المثال: إذا كان الشرط **Databases are outdated** له قيمة **أكثر من 3 أيام** بشكل افتراضي، سيتم تعيين حالة تحذير إلى الجهاز العميل؛ أما إذا كان بقيمة **أكثر من 7 يومًا**، سيتم تعيين حالة حرج إلى الجهاز.

إذا قمت بترقية Kaspersky Security Center من الإصدار السابق، قيم شرط **Databases are outdated** لتخصيص الحالة تتغير إلى حرجة أو تحذير أو لا تتغير.

تكوين تبديل حالات الجهاز

يمكنك تغيير الشروط لتعيين الحالة حرجة أو تحذير لجهازٍ ما.

لتمكين تغيير حالة الجهاز إلى حرجة:

1. في القائمة الرئيسية، انتقل إلى **Hierarchy of groups** ← **Assets (Devices)**.
2. في قائمة المجموعات التي تفتح، انقر على الرابط الذي يحمل اسم المجموعة التي ترغب في تغييرها بتبديل حالات الجهاز.
3. في نافذة الخصائص التي تفتح، حدد تبويب **Device status**.
4. في الجزء الأيسر، حدد **Critical**.
5. في الجزء الأيمن في قسم **Set to Critical if these are specified**، قم بتفعيل الشرط لتبديل جهاز إلى حالة حرج.

لا يمكنك تغيير سوى الإعدادات غير المقفلة في السياسة الأصلية.

6. حدد زر الراديو الموجود بجوار الشرط في القائمة.
7. في الزاوية العلوية اليسرى من القائمة، انقر على زر **Edit**.
8. حدد القيمة المطلوبة للحالة المحددة.
   لا يمكن تعيين القيم لكل حالة.
9. انقر على **OK**.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار عى حرج .

لتمكين تغيير حالة الجهاز إلى تحذير:

1. في القائمة الرئيسية، انتقل إلى **Hierarchy of groups** ← **Assets (Devices)**.
2. في قائمة المجموعات التي تفتح، انقر على الرابط الذي يحمل اسم المجموعة التي ترغب في تغييرها بتبديل حالات الجهاز.
3. في نافذة الخصائص التي تفتح، حدد تبويب **Device status**.
4. في الجزء الأيمن، حدد **Warning**.
5. في الجزء الأيمن في قسم **Set to Warning if these are specified**، قم بتفعيل الشرط لتبديل جهاز إلى حالة تحذير.

لا يمكنك تغيير سوى الإعدادات غير المقفلة في السياسة الأصلية.

6. حدد زر الراديو الموجود بجوار الشرط في القائمة.

7. في الزاوية العلوية اليسرى من القائمة، انقر على زر **Edit**.

8. حدد القيمة المطلوبة للحالة المحددة.

لا يمكن تعيين القيم لكل حالة.

9. انقر على **OK**.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار عى تحذير .

الاتصال البعيد بسطح مكتب جهاز عميل

يمكن للمسؤول الحصول على وصول عن بُعد لسطح مكتب جهاز عميل من خلال عميل الشبكة المثبت على الجهاز. ومن الممكن أيضًا الاتصال عن بُعد بجهاز من خلال عميل الشبكة في حالة إغلاق منافذ TCP وUDP بالجهاز العميل.

عند إنشاء اتصال مع الجهاز، يكون للمسؤول حق الوصول الكامل للمعلومات المُخزنة على هذا الجهاز ليتمكن من إدارة التطبيقات المثبتة عليه.

يجب السماح بالاتصال عن بُعد في إعدادات نظام التشغيل للجهاز المُدار المستهدف. على سبيل المثال، في Windows 10، يسمى هذا الخيار **بالسماح باتصالات المساعدة عن بُعد لهذا الكمبيوتر** (يمكنك العثور على هذا الخيار في **لوحة التحكم** ← **النظام والأمان** ← **النظام** ← **الإعدادات عن بُعد**). إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات، فيمكنك تمكين هذا الخيار بالقوة عند إجراء اتصال بجهاز مُدار. إذا لم يكن لديك ترخيص، فقم بتمكين هذا الخيار محليًا على الجهاز المُدار المستهدف. إذا تم تعطيل هذا الخيار، فلن يتم الاتصال عن بُعد.

لإنشاء اتصال عن بُعد بجهاز ، يجب أن يكون لديك أداتان:

- أداة كاسبيرسكي تسمى klsctunnel. يجب تخزين هذه الأداة على محطة عمل المسؤول. يمكنك استخدام هذه الأداة المساعدة لربط الاتصال بين جهاز عميل وخادم الإدارة.

  يتيح Kaspersky Security Center باتصالات TCP عبر الأنفاق من وحدة تحكم الإدارة عبر خادم الإدارة ثم عبر عميل الشبكة إلى منفذ محدد على جهاز مُدار. الأنفاق مصممة لتوصيل تطبيق عميل على جهاز مثبّت عليه وحدة تحكم الإدارة إلى منفذ TCP على جهاز مُدار—في حالة عدم إمكانية الاتصال المباشر بين وحدة تحكم الإدارة والجهاز المستهدف.

  نفق اتصال بين جهاز عميل بعيد وخادم الإدارة مطلوب في حالة عدم توفر المنفذ المستخدم لاتصال خادم الإدارة على الجهاز. قد لا يتوفر المنفذ الموجود على الجهاز في الحالات التالية:

  - اتصال الجهاز البعيد بشبكة محلية تستخدم آلية NAT.
  - الجهاز البعيد يعتبر جزء من الشبكة المحلية الخاصة بخادم الإدارة، لكن تم غلق منفذه بواسطة جدار الحماية.

- يسمى مكون Microsoft Windows القياسي بالاتصال بسطح المكتب عن بُعد. يتم إنشاء اتصال سطح المكتب عن بُعد عبر أداة Windows القياسية mstsc.exe وفقًا لإعدادات الأداة.

  تم إنشاء اتصال بجلسة سطح المكتب البعيد الحالية للمستخدم دون علم المستخدم. بمجرد اتصال المسؤول بالجلسة، يتم قطع اتصال مستخدم الجهاز من الجلسة دون إخطار مسبق.

الاتصال عن بُعد بسطح مكتب الجهاز العميل:

1. في وحدة تحكم الإدارة المعتمدة على MMC, في قائمة السياق لخادم الإدارة، اختر **خصائص**.

2. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **إعدادات اتصال خادم الإدارة** ← **منافذ الاتصال**.

3. تأكد من أن خيار **افتح منفذ بروتوكول سطح المكتب البعيد (RDP) الخاص بـ Web Console** ممكّن.

4. في Kaspersky Security Center Web Console، انتقل إلى **Assets (Devices)** ← **Managed devices**.

5. في الحقل **Current path** أعلى قائمة الأجهزة المُدارة، انقر فوق ارتباط المسار.

6. في الجزء الأيمن الذي يفتح، حدد مجموعة الإدارة التي تحتوي على الجهاز الذي تريد الوصول إليه.

7. حدد خانة الاختيار بجوار اسم الجهاز الذي تريد الوصول إليه.

8. انقر على زر **Connect to Remote Desktop**.

يتم فتح النافذة Remote Desktop (Windows only).

9. تمكين خيار **السماح باتصال سطح المكتب عن بُعد على الجهاز المُدار** . في هذه الحالة، سيتم إجراء الاتصال حتى إذا كانت الاتصالات عن بُعد ممنوعة حاليًا في إعدادات نظام التشغيل على الجهاز المُدار.

يتوفر هذا الخيار فقط إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات.

10. انقر على زر **Download** لتنزيل الأداة المساعدة klsctunnel.

11. انقر على زر **Copy to clipboard** لنسخ النص من حقل النص. هذا النص هو كائن ثنائي كبير (BLOB) يحتوي على الإعدادات المطلوبة لإجراء اتصال بين خادم الإدارة والجهاز المُدار.

BLOB صالح لمدة 3 دقائق. إذا انتهت صلاحيته، فأعد فتح نافذة Remote Desktop (Windows only) لإنشاء BLOB جديد.

12. قم بتشغيل الأداة المساعدة klsctunnel.

يتم فتح نافذة الأداة.

13. قم بلصق النص المنسوخ في حقل النص.

14. إذا كنت تستخدم الخادم الوكيل، فحدد خانة الاختيار **استخدام الخادم الوكيل**، ثم حدد إعدادات اتصال الخادم الوكيل.

15. انقر على الزر **فتح المنفذ**.

يتم فتح نافذة تسجيل دخول اتصال سطح المكتب عن بُعد.

16. حدد بيانات اعتماد الحساب الذي قمت بتسجيل الدخول من خلاله حاليًا إلى Kaspersky Security Center Web Console.

17. انقر فوق زر **اتصال**.

عند إجراء الاتصال بالجهاز، يُتاح سطح المكتب في نافذة الاتصال عن بُعد لـ Microsoft Windows.

الاتصال بالأجهزة من خلال مشاركة سطح المكتب لـ Windows

يمكن للمسؤول الحصول على وصول عن بُعد لسطح مكتب جهاز عميل من خلال عميل الشبكة المثبت على الجهاز. ومن الممكن أيضًا الاتصال عن بُعد بجهاز من خلال عميل الشبكة في حالة إغلاق منافذ TCP وUDP بالجهاز العميل.

يمكن للمسؤول الاتصال بالجلسة الموجودة على جهاز عميل بدون فصل اتصال المستخدم في هذه الجلسة. وفي هذه الحالة، سيشارك المسؤول ومستخدم الجلسة على الجهاز الوصول إلى سطح المكتب.

لإنشاء اتصال عن بُعد بجهاز ، يجب أن يكون لديك أداتان:

- أداة كاسبيرسكي تسمى klsctunnel. يجب تخزين هذه الأداة على محطة عمل المسؤول. يمكنك استخدام هذه الأداة المساعدة لربط الاتصال بين جهاز عميل وخادم الإدارة.

  يتيح Kaspersky Security Center باتصالات TCP عبر الأنفاق من وحدة تحكم الإدارة عبر خادم الإدارة ثم عبر عميل الشبكة إلى منفذ محدد على جهاز مُدار. الأنفاق مصممة لتوصيل تطبيق عميل على جهاز مثبّت عليه وحدة تحكم الإدارة إلى منفذ TCP على جهاز مُدار—في حالة عدم إمكانية الاتصال المباشر بين وحدة تحكم الإدارة والجهاز المستهدف.

نفق اتصال بين جهاز عميل بعيد وخادم الإدارة مطلوب في حالة عدم توفر المنفذ المستخدم لاتصال خادم الإدارة على الجهاز. قد لا يتوفر المنفذ الموجود على الجهاز في الحالات التالية:

- اتصال الجهاز البعيد بشبكة محلية تستخدم آلية NAT.
- الجهاز البعيد يعتبر جزء من الشبكة المحلية الخاصة بخادم الإدارة، لكن تم غلق منفذه بواسطة جدار الحماية.

- مشاركة سطح المكتب لـ Windows. عند الاتصال بجلسة موجودة لسطح مكتب بعيد، يتلقى مستخدم الجلسة على الجهاز طلبًا للاتصال من المسؤول. لن توجد أي معلومات بشأن نشاط عن بُعد على الجهاز وسوف يتم حفظ نتائجه في التقارير التي تم إنشاؤها بواسطة Kaspersky Security Center.

  يمكن للمسؤول تكوين مراجعة لنشاط المستخدم على جهاز عميل بعيد. أثناء المراجعة، يحفظ التطبيق معلومات بشأن ملفات على الجهاز العميل تم فتحها و/أو تعديلها من خلال المسؤول.

للاتصال بسطح مكتب الجهاز العميل عبر مشاركة سطح المكتب لـ Windows، ينبغي عليك تلبية الشروط التالية:

- يلزم تثبيت Microsoft Windows Vista أو إصدار نظام تشغيل أحدث على محطة عمل المسؤول. لا يفرض نوع نظام التشغيل المستخدم على الجهاز الذي يستضيف خادم الإدارة قيودًا على الاتصال عبر مشاركة سطح المكتب لـ Windows.

  للتحقق مما إذا كانت ميزة Windows Desktop Sharing مضمنة في إصدار Windows، تأكد من وجود مفتاح CLSID \\ {5C86-480F-A914-0FF8885A1B3F-32BE5ED2} في سجل Windows.

- يتم تثبيت Microsoft Windows Vista أو إصدار أحدث على الجهاز العميل.
- يستخدم Kaspersky Security Center ترخيصًا لإدارة الثغرات الأمنية والتصحيحات.

للاتصال بسطح مكتب جهاز عميل من خلال مشاركة سطح المكتب لـ Windows:

1. في وحدة تحكم الإدارة المعتمدة على MMC, في قائمة السياق لخادم الإدارة، اختر **خصائص**.
2. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **إعدادات اتصال خادم الإدارة** ← **منافذ الاتصال**.
3. تأكد من أن خيار **افتح منفذ بروتوكول سطح المكتب البعيد (RDP) الخاص بـ Web Console** ممكّن.
4. في Kaspersky Security Center Web Console، انتقل إلى **Assets (Devices)** ← **Managed devices**.
5. في الحقل **Current path** أعلى قائمة الأجهزة المُدارة، انقر فوق ارتباط المسار.
6. في الجزء الأيمن الذي يفتح، حدد مجموعة الإدارة التي تحتوي على الجهاز الذي تريد الوصول إليه.
7. حدد خانة الاختيار بجوار اسم الجهاز الذي تريد الوصول إليه.
8. انقر على زر **Windows Desktop Sharing**.

   يتم فتح معالج Windows Desktop Sharing.
9. انقر على زر **Download** لتنزيل أداة klsctunnel المساعدة، وانتظر اكتمال عملية التنزيل.

   إذا كان لديك بالفعل أداة klsctunnel المساعدة، فتخط هذه الخطوة.
10. انقر على الزر **Next**.
11. حدد الجلسة على الجهاز الذي تريد الاتصال به، ثم انقر فوق زر **Next**.
12. يجب على المستخدم السماح بجلسة مشاركة سطح المكتب على جهاز الهدف في مربع الحوار الذي يفتح. بخلاف ذلك، فإن الجلسة غير ممكنة.

    بعد أن يؤكد مستخدم الجهاز جلسة مشاركة سطح المكتب، يتم فتح الصفحة التالية للمعالج.

13. انقر على زر **Copy to clipboard** لنسخ النص من حقل النص. هذا النص هو كائن ثنائي كبير (BLOB) يحتوي على الإعدادات المطلوبة لإجراء اتصال بين خادم الإدارة والجهاز المُدار.

BLOB صالح لمدة 3 دقائق. إذا انتهت صلاحيته، فقم بإنشاء BLOB جديد.

14. قم بتشغيل الأداة المساعدة klsctunnel.

يتم فتح نافذة الأداة.

15. قم بلصق النص المنسوخ في حقل النص.

16. إذا كنت تستخدم الخادم الوكيل، فحدد خانة الاختيار **استخدام الخادم الوكيل**، ثم حدد إعدادات اتصال الخادم الوكيل.

17. انقر على الزر **فتح المنفذ**.

يتم بدء مشاركة سطح المكتب في نافذة جديدة. إذا كنت ترغب في التفاعل مع الجهاز، انقر فوق أيقونة القائمة ( ) في الزاوية العلوية اليمنى من النافذة، ثم حدد **الوضع التفاعلي**.

تحديدات الأجهزة

تحديدات الأجهزة هي أداة لتصفية الأجهزة وفق شروط محددة. يمكنك استخدام تحديدات الأجهزة لإدارة عدة أجهزة: يمكن على سبيل المثال عرض تقرير حول هذه الأجهزة فقط أو من أجل نقل جميع هذه الأجهزة إلى مجموعة أخرى.

يوفر Kaspersky Security Center نطاق كبير التحديدات المحددة مسبقًا (مثل **الأجهزة ذات الحالة حرج**، **Active**، **Protection is disabled**، **threats are detected**). لا يمكن حذف التحديدات المحددة مسبقًا. يمكنك كذلك إنشاء وتكوين تحديدات إضافية يحددها المستخدم.

يمكنك في ""تحديدات من تعريف المستخدم" تعيين نطاق البحث وتحديد جميع الأجهزة أو الأجهزة المُدارة أو الأجهزة غير المخصصة. معلمات البحث محددة في الشروط. يمكنك في تحديد الجهاز إنشاء عدة شروط ذات معلمات بحث مختلفة. يمكنك على سبيل المثال إنشاء شرطين وتحديد نطاقات IP مختلفة في كلٍ منها. في حال تحديد عدة شروط، يعرض التحديد الأجهزة التي تفي بأي من هذه الشروط. وعلى العكس، معلمات البحث في نطاق شرط تكون متراكبة. في حال تحديد نطاق IP واسم تطبيق مثبت في شرط، لن يتم عرض إلا هذه الأجهزة حيث يوجد التطبيق مثبت وعنوان IP ينتمي إلى نطاق محدد.

عرض قائمة الأجهزة من تحديد جهاز

يسمح لك Kaspersky Security Center بعرض قائمة الأجهزة من تحديد جهاز.

لعرض قائمة الأجهزة من تحديد الجهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Device selections** أو القسم **Discovery & deployment** ← **Device selections**.

2. في قائمة التحديد، انقر على اسم تحديد الجهاز.

تعرض الصفحة جدولاً يتضمن معلومات عن الأجهزة المضمنة في تحديد الجهاز.

3. يمكنك تجميع بيانات جدول الجهاز وتصفيتها على النحو التالي:

- انقر فوق أيقونة الإعدادات (⚙)، ثم حدد الأعمدة المراد عرضها في الجدول.
- انقر فوق أيقونة عامل التصفية (▽)، ثم حدد معيار عامل التصفية وطبقه في القائمة التي تم استدعاؤها.

يتم عرض جدول الأجهزة التي تم تصفيتها.

يمكنك تحديد جهاز واحد أو عدة أجهزة في تحديد الجهاز والنقر فوق الزر **New task** لإنشاء مهمة سيتم تطبيقها على هذه الأجهزة.

لنقل الأجهزة المحددة من تحديد الجهاز إلى مجموعة إدارة أخرى، انقر فوق الزر **Move to group**، ثم حدد مجموعة الإدارة المستهدفة.

إنشاء تحديد جهاز

لإنشاء تحديد جهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Device selections**.

   سيتم عرض صفحة بقائمة تحديدات الأجهزة.

2. انقر على الزر **Add**.

   ستفتح نافذة **Device selection settings**.

3. أدخل اسم التحديد الجديد.

4. حدد المجموعة التي تحتوي على الأجهزة التي سيتم تضمينها في تحديد الجهاز:

   - **Find any devices** —البحث عن الأجهزة التي تلبي معايير التحديد والمضمنة في مجموعة **Managed Devices** أو المجموعة **Unassigned devices**.
   - **Find managed devices** —البحث عن الأجهزة التي تلبي معايير التحديد والمضمنة في المجموعة **Managed Devices**.
   - **Find unassigned devices** — البحث عن الأجهزة التي تلبي معايير التحديد والمضمنة في المجموعة **Unassigned devices**.

   يمكنك تمكين خانة الاختيار **Include data from secondary Administration Servers** لتمكين البحث عن الأجهزة التي تلبي معايير التحديد وتديرها خوادم الإدارة الثانوية.

5. انقر على الزر **Add**.

6. في النافذة التي تفتح، حدد الشروط التي يجب تحقيقها لتضمين الأجهزة في هذا التحديد ثم انقر على زر **OK**.

7. انقر على زر **Save**.

   يتم إنشاء تحديد الجهاز وإضافته إلى قائمة تحديدات الأجهزة.

تكوين تحديد جهاز

لتكوين تحديد جهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Device selections**.

   سيتم عرض صفحة بقائمة تحديدات الأجهزة.

2. حدد تحديد الجهاز المحدد من قبل المستخدم، وانقر على زر **Properties**.

   ستفتح نافذة **Device selection settings**.

3. في علامة تبويب **General**، انقر على رابط **New condition**.

4. حدد الشروط التي يجب تحقيقها لتضمين الأجهزة في هذا التحديد.

5. انقر على زر **Save**.

   يتم تطبيق الإعدادات وحفظها.

فيما يلي أوصاف شروط تعيين الأجهزة في تحديد. يتم تجميع الشروط باستخدام المعامل المنطقي OR: سيحتوي التحديد على أجهزة تتوافق على الأقل مع شرط واحد من الشروط الواردة.

General

في القسم **General**، يمكنك تغيير اسم شرط التحديد وتحديد ما إذا كان يجب عكس هذا الشرط أم لا:

Invert selection condition

يتم تعطيل هذا الخيار افتراضيًا.

إذا قمت بتمكين هذا الخيار، فسيتم عكس حالة التحديد المحددة. سيتضمن التحديد جميع الأجهزة التي لا تتوافق مع الحالة.

يوضح المثال التالي منطق عمل الانعكاس:

- **الشرط** : يوجد على جهازك نظام تشغيل من نوع Linux ورقم الإصدار 00.0.000.
- **الحالة المعكوسة** : يوجد على جهازك نظام تشغيل ليس (من النوع Linux ورقم الإصدار 00.0.000)، وهو ما يعادل ما يلي:
  يوجد نظام تشغيل من نوع ليس Linux أو رقم الإصدار ليس 00.0.000.

وبالتالي، ستتضمن المجموعة المحددة الأجهزة التي تحتوي على نظام تشغيل، على سبيل المثال، من نوع Windows ورقم الإصدار 00.0.000، أو نوع Linux وأي رقم إصدار آخر بخلاف 00.0.000.

Network infrastructure

في القسم **Network**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لبيانات الشبكة الخاصة بها:

- **Device name**

  اسم شبكة Windows (اسم NetBIOS) للجهاز، أو عنوان IPv4 أو IPv6.

- **Domain**

  عرض كل الأجهزة المضمنة في مجال Windows® المحدد.

- **Administration group**

  عرض الأجهزة المضمنة في مجموعة الإدارة المحددة.

- **Description**

  نص في نافذة خصائص الجهاز: في الحقل **الوصف** بالقسم **عام**.

  لوصف النص في الحقل **الوصف**، يمكنك استخدام الرموز التالية:

  - وسط الكلمة:
    - *. تحل محل أية سلسلة بها أي عدد من الحروف.

    مثال:

    لوصف كلمات مثل **الخادم** أو **خاص بالخادم**، يمكنك إدخال **خادم***.

    - ؟. تحل محل أي حرف مفرد.

    مثال:

    لوصف كلمات مثل **نافذة** أو **نوافذ**، يمكنك إدخال **نافذة؟**.

لا يمكن استخدام نجمة (*) أو علامة استفهام (؟) كأول حرف في الاستعلام.

- للبحث عن كلمات متعددة:
  - مسافة. تعرض جميع الأجهزة التي يحتوي وصفها على أي كلمة من الكلمات المدرجة.

مثال:
للبحث عن عبارة تحتوي على كلمة **تابع** أو **ظاهري**، يمكنك إدخال **تابع ظاهري** في الاستعلام.

  - **+**. عندما تأتي علامة الزائد قبل كلمة، ستحتوي جميع نتائج البحث على هذه الكلمة.

مثال:
للبحث عن عبارة تحتوي على الكلمتين **تابع** و**ظاهري**، أدخل الاستعلام **+تابع+ظاهري**.

  - **-**. عندما تأتي علامة الناقص قبل كلمة، لن تحتوي نتائج البحث على هذه الكلمة.

مثال:
للبحث عن عبارة تحتوي على كلمة **تابع** ولا تحتوي على كلمة **ظاهري**، أدخل الاستعلام **+تابع-ظاهري**.

  - **"<some text>"**. النص الموضوع بين علامتي الاقتباس يجب أن يكون موجودًا في النص.

مثال:
للبحث عن عبارة تحتوي على الكلمة المركّبة **الخادم التابع**، أدخل **"الخادم التابع"** في الاستعلام.

- **IP range**

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.
يتم تعطيل هذا الخيار افتراضيًا.

- **Managed by a different Administration Server**

حدد إحدى القيم التالية:

- **نعم**. تنطبق قاعدة نقل الجهاز فقط على أجهزة العميل المُدارة بواسطة خوادم الإدارة الأخرى. تختلف هذه الخوادم عن الخادم الذي تقوم بتكوين قاعدة نقل الجهاز عليه.
- **لا**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي يديرها خادم الإدارة الحالي.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

في القسم الفرعي **Domain controller**، يمكنك تكوين معايير لتضمين الأجهزة في مجموعة بناءً على عضوية المجال:

- **Device is in a domain organizational unit**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من وحدة المجال المحددة في حقل الإدخال.
يتم تعطيل هذا الخيار افتراضيًا.

- **This device is a member of the domain security group**

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من مجموعة أمان المجال المحددة في حقل الإدخال.
يتم تعطيل هذا الخيار افتراضيًا.

في القسم الفرعي **Network activity** يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لنشاط الشبكة الخاص بها:

- **Acts as a distribution point**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. سوف يتضمن التحديد أجهزة الكمبيوتر التي تعمل كنقاط توزيع.
- **لا**. لن يتم تضمين الأجهزة التي تعمل كنقاط توزيع في التحديد.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **Do not disconnect from the Administration Server**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **مُمكّن**. سيتضمن التحديد الأجهزة التي تم تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
- **معطل**. سيتضمن التحديد الأجهزة التي تم إلغاء تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **Connection profile switched**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. سوف يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
- **لا**. لن يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **Last connected to Administration Server**

يمكنك استخدام خانة الاختيار هذه لتعيين معيار للبحث عن الأجهزة إلى وقت آخر اتصال بخادم الإدارة.

إذا تم تحديد خانة الاختيار هذه، فيمكنك في حقول الإدخال تحديد الفاصل الزمني (التاريخ والوقت) الذي تم خلاله إنشاء آخر اتصال بين عميل الشبكة المثبت على الجهاز العميل وخادم الإدارة. سوف يتضمن الاختيار الأجهزة التي تقع ضمن الفاصل الزمني المحدد.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **New devices detected by network poll**

عمليات البحث عن أجهزة جديدة تم اكتشافها بواسطة استقصاء الشبكة على مدار الأيام القليلة الماضية.

إذا تم تمكين هذا الخيار، فسيتضمن التحديد فقط الأجهزة الجديدة التي تم اكتشافها بواسطة خاصية اكتشاف الأجهزة على مدار عدد الأيام المحددة في حقل **فترة الكشف (بالأيام)**.

إذا تم تعطيل هذا الخيار، فسيتضمن التحديد جميع الأجهزة التي تم اكتشافها بواسطة خاصية اكتشاف الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- **Device is visible**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المرئية في الوقت الحالي على الشبكة.
- **لا**. يشمل التطبيق في التحديد الأجهزة غير المرئية في الوقت الحالي على الشبكة.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

في القسم الفرعي **Cloud segments**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد وفقًا لقطاعات السحابة الخاصة بها:

- **Device is in a cloud segment**

إذا تم تمكين هذا الخيار، يمكنك اختيار الأجهزة من القطاعات السحابية في AWS وAzure وGoogle.

إذا تم أيضًا تمكين خيار **Include child objects**، فسيتم تشغيل البحث في جميع الكائنات التابعة للقطاع المحدد.

البحث عن النتائج التي تشتمل فقط على أجهزة من القطاع المحدد.

- **Device discovered by using the API**

يمكنك تحديد ما إذا كان تم اكتشاف الجهاز بواسطة أدوات API في القائمة المنسدلة:

- **نعم**. يتم اكتشاف الجهاز باستخدام واجهة برمجة تطبيقات AWS أو Azure أو Google.
- **لا**. لا يمكن اكتشاف الجهاز باستخدام واجهة برمجة تطبيقات AWS أو Azure أو Google. أي أن الجهاز إما خارج بيئة السحابة أو موجود في بيئة السحابة، لكن لا يمكن اكتشافه باستخدام واجهة برمجة تطبيقات.
- دون قيمة. هذا الشرط لا ينطبق.

Device statuses

في القسم الفرعي **Managed device status**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على وصف حالة الأجهزة من تطبيق مدار:

- **Device status**

القائمة المنسدلة التي يمكنك فيها تحديد إحدى حالات الجهاز: موافق، أو حرج، أو تحذير.

- **Real-time protection status**

يمكنك في القائمة المنسدلة تحديد حالة الحماية في الوقت الحقيقي. يتم تضمين الأجهزة مع حالة الحماية في الوقت الحقيقي في التحديد.

- **وصف حالة الجهاز**

يمكنك في هذا الحقل، تحديد خانات الاختيار بجانب الشروط التي تحدد، إن تم استيفائها، إحدى الحالات التالية لجهاز الكمبيوتر: موافق أو حرج أو تحذير.

في القسم الفرعي **Status of components in managed applications**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على حالات المكونات في التطبيقات المُدارة:

- **Data Leakage Prevention status**

البحث عن الأجهزة حسب حالة منع تسرب البيانات (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **Collaboration servers protection status**

البحث عن الأجهزة حسب حالة حماية تعاون الخادم (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **Anti-virus protection status of mail servers**

البحث عن الأجهزة حسب حالة حماية خادم البريد (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

- **Endpoint Sensor status**

البحث عن الأجهزة حسب حالة المكون أداة استشعار نقطة النهاية (غير معروف، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

في القسم الفرعي **Status-affecting problems in managed applications**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لقائمة المشكلات المحتملة التي يتم اكتشافها بواسطة تطبيق مُدار. إذا كانت مشكلة واحدة على الأقل من المشكلات التي حددتها موجودة على جهاز، فسيتم تضمين الجهاز في القسم. في حالة اختيار مشكلة مدرجة للعديد من التطبيقات، فلديك الخيار لتحديد هذه المشكلة في جميع القوائم تلقائيًا.

يمكنك تحديد خانات الاختيار الخاصة بأوصاف الحالات من تطبيق مدار؛ وفور استلام هذه الحالات، سيتم تضمين الأجهزة في التحديد. في حالة اختيار حالة مدرجة للعديد من التطبيقات، فلديك الخيار لتحديد هذه الحالة في جميع القوائم تلقائيًا.

System details

في القسم **Operating system**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لنوع نظام التشغيل الخاص بهم.

- **Platform type**

إذا تم تحديد خانة الاختيار، فيمكنك تحديد نظام تشغيل من القائمة. يتم تضمين الأجهزة المثبت عليها أنظمة التشغيل المحددة في نتائج البحث.

- **Operating system service pack version**

في هذا الحقل، يمكنك تحديد إصدار حزمة نظام التشغيل (بتنسيق X.Y)، والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز. وبشكل افتراضي، لا يتم تحديد أي قيمة إصدار.

- **Operating system bit size**

في القائمة المنسدلة، يمكنك تحديد بنية نظام التشغيل والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز (**غير معروف**, **x86**, **AMD64** أو **IA64**). وبشكل افتراضي، لا يتم تحديد أي خيار في القائمة ومن ثم لا يتم تحديد بنية نظام التشغيل.

- **Operating system build**

> لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

رقم نسخة نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم نسخة مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.

- **Operating system release number**

> لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

معرف إصدار (ID) نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك معرف إصدار مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام معرف الإصدار باستثناء الرقم المحدد.

في القسم **Virtual machines**، يمكنك إعداد المعايير لتضمين الأجهزة في التحديد بناءً على ما إذا كانت تعد أجهزة ظاهرية أو جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI):

- **This is a virtual machine**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- **Undefined**.
- **لا**. البحث عن الأجهزة التي لا تعد أجهزة افتراضية.
- **نعم**. البحث عن الأجهزة التي تعد أجهزة ظاهرية.

- **نوع الجهاز الافتراضي**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة للجهاز الظاهري.

هذه القائمة المنسدلة متاحة إذا تم تحديد القيمة **نعم** أو **ليس هامًا** تم تحديد القيمة **هذا جهاز ظاهري** في القائمة المنسدلة.

- **جزء من البنية الأساسية لسطح المكتب الافتراضي**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- Undefined.
- **لا**. البحث عن الأجهزة التي لا تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي.
- **نعم**. البحث عن الأجهزة التي تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI).

في القسم الفرعي **Hardware registry**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على الأجهزة المثبتة:

تأكد من تثبيت الأداة المساعدة lshw على أجهزة Linux التي تريد جلب تفاصيل الأجهزة منها. قد تكون تفاصيل الأجهزة التي يتم جلبها من الأجهزة الافتراضية غير مكتملة بناءً على برنامج مراقب الأجهزة الافتراضية المستخدم.

- Device

يمكنك في القائمة المنسدلة تحديد نوع الوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.

يدعم الحقل البحث بالنص الكامل.

- Vendor

يمكنك في القائمة المنسدلة تحديد اسم الشركة المصنعة للوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.

يدعم الحقل البحث بالنص الكامل.

- Device name

اسم الجهاز الموجود في شبكة Windows. سيتم تضمين الجهاز ذي الاسم المحدد في التحديد.

- Description

وصف الجهاز أو وحدة الجهاز. سيتم تضمين الأجهزة ذات الوصف المحدد في هذا الحقل في التحديد.

يمكن إدخال وصف الجهاز بأي تنسيق في نافذة خصائص هذا الجهاز. يدعم الحقل البحث بالنص الكامل.

- Device vendor

اسم الشركة المصنعة للجهاز. سيتم تضمين الأجهزة التي تنتجها الشركة المصنعة المحددة في هذا الحقل في التحديد.

يمكنك إدخال اسم الشركة المصنعة في نافذة خصائص جهاز.

- Serial number

سيتم تضمين جميع وحدات الأجهزة ذات الرقم التسلسلي المحددة في هذا الحقل في التحديد.

- Inventory number

سيتم تضمين الأجهزة ذات رقم المخزون والمحدد في هذا الحقل في التحديد.

- User

سيتم تضمين جميع وحدات أجهزة المستخدم المحدد في هذا الحقل في التحديد.

- Location

موقع جهاز أو وحدة أجهزة (على سبيل المثال، في المقر الرئيسي أو مكتب فرعي). سيتم تضمين أجهزة الكمبيوتر أو الأجهزة الأخرى التي تم نشرها في الموقع المحدد في هذا الحقل في التحديد.

يمكنك وصف موقع جهاز بأي تنسيق في نافذة خصائص هذا الجهاز.

- **CPU clock rate, in MHz, from**

أدنى معدل لساعة وحدة المعالجة المركزية. سيتم تضمين الأجهزة المزودة بوحدة معالجة مركزية تطابق نطاق معدل الساعة المحدد في حقول الإدخال (ضمناً) في التحديد.

- **CPU clock rate, in MHz, to**

أقصى معدل لساعة وحدة المعالجة المركزية. سيتم تضمين الأجهزة المزودة بوحدة معالجة مركزية تطابق نطاق معدل الساعة المحدد في حقول الإدخال (ضمناً) في التحديد.

- **Number of virtual CPU cores, from**

الحد الأدنى لعدد أنوية وحدة المعالجة المركزية الافتراضية. سيتم تضمين الأجهزة المزودة بوحدة معالجة مركزية تطابق نطاق عدد الأنوية الافتراضية المحدد في حقول الإدخال (ضمناً) في التحديد.

- **Number of virtual CPU cores, to**

أقصى عدد من أنوية وحدة المعالجة المركزية الافتراضية. سيتم تضمين الأجهزة المزودة بوحدة معالجة مركزية تطابق نطاق عدد الأنوية الافتراضية المحدد في حقول الإدخال (ضمناً) في التحديد.

- **Hard drive volume, in GB, from**

الحد الأدنى لحجم محرك الأقراص الثابت على الجهاز. سيتم تضمين الأجهزة المزودة بمحرك أقراص ثابت يطابق نطاق الحجم المحدد في حقول الإدخال (ضمناً) في التحديد.

- **Hard drive volume, in GB, to**

الحد الأقصى لحجم محرك الأقراص الثابت على الجهاز. سيتم تضمين الأجهزة المزودة بمحرك أقراص ثابت يطابق نطاق الحجم المحدد في حقول الإدخال (ضمناً) في التحديد.

- **RAM size, in MB, from**

الحد الأدنى لحجم ذاكرة الوصول العشوائي على الجهاز. وسيتم تضمين الأجهزة ذات ذاكرة الوصول العشوائي التي تطابق نطاق الحجم المحدد في حقول الإدخال (ضمنًا) في التحديد.

- **RAM size, in MB, to**

الحد الأقصى لحجم ذاكرة الوصول العشوائي على الجهاز. وسيتم تضمين الأجهزة ذات ذاكرة الوصول العشوائي التي تطابق نطاق الحجم المحدد في حقول الإدخال (ضمنًا) في التحديد.

Third-party software details

في القسم الفرعي **Applications registry**، يمكنك إعداد معايير البحث عن الأجهزة وفقًا للتطبيقات المثبتة عليها:

- **Application name**

القائمة المنسدلة التي يمكنك فيها تحديد أي تطبيق. يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **Application version**

يمكنك في حقل الإدخال تحديد إصدار التطبيق المحدد.

- **Vendor**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة لأي تطبيق مثبت على الجهاز.

- **Application status**

يمكنك في القائمة المنسدلة تحديد حالة أي تطبيق (مثبت، غير مثبت). سيتم تضمين الأجهزة التي تم تثبيت التطبيق المحدد أو لم يتم تثبيته عليها، بناءً على الحالة المحددة، في التحديد.

- **Find by update**

إذا تم تمكين هذا الخيار، فسيتم إجراء البحث باستخدام تفاصيل تحديثات التطبيقات المثبتة على الأجهزة ذات الصلة. بعد تحديد خانة الاختيار، تتغير الحقول **اسم التطبيق** و**إصدار التطبيق** و**حالة التطبيق** إلى **اسم التحديث** و**إصدار التحديث** و**الحالة** على التوالي.

يتم تعطيل هذا الخيار افتراضيًا.

- **Name of incompatible security application**

القائمة المنسدلة التي يمكنك فيها تحديد تطبيقات الحماية الخاصة بالجهة الخارجية. خلال البحث، يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **Application tag**

يمكنك في القائمة المنسدلة تحديد علامة التطبيق. يتم تضمين جميع الأجهزة المثبت عليها تطبيقات مشتملة على العلامة المحددة في الوصف، في تحديد الجهاز.

- **Apply to devices without the specified tags**

إذا تم تمكين هذا الخيار، فسيتضمن التحديد أجهزة أوصافها لا تحتوي على أي من العلامات المحددة.

إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار.

يتم تعطيل هذا الخيار افتراضيًا.

في القسم الفرعي **Vulnerabilities and updates**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لمصدر Windows Update الخاص بها:

WUA is switched to Administration Server

يمكنك تحديد خيار من خيارات البحث التالية من القائمة المنسدلة:

- **نعم**. إذا تم تحديد هذا الخيار، فستشتمل نتائج البحث على الأجهزة التي تتلقى تحديثات من خلال Windows Update من خادم الإدارة.
- **لا**. إذا تم تحديد هذا الخيار، ستشتمل النتائج الأجهزة التي تتلقى تحديثات من خلال Windows Update من مصادر أخرى.

Details of Kaspersky applications

في القسم الفرعي **Kaspersky applications**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على التطبيق المدار المحدد:

- **Application name**

في القائمة المنسدلة، يمكنك إعداد معيار لتضمين الأجهزة في تحديد عند إجراء بحث باسم تطبيق Kaspersky.

توفر القائمة أسماء التطبيقات مع الأدوات الإضافية للإدارة فقط والمثبتة على محطة عمل المسؤول.

إذا لم يتم تحديد تطبيق، لن يتم تطبيق المعيار.

- **Application version**

في حقل الإدخال، يمكنك تحديد معيار لتضمين الأجهزة في تحديد عند إجراء بحث برقم إصدار تطبيق Kaspersky.

إذا لم يتم تحديد رقم إصدار، لن يتم تطبيق المعيار.

- **Critical update name**

يمكنك في القائمة المنسدلة تحديد حالة أي تطبيق (مثبت، غير مثبت). سيتم تضمين الأجهزة التي تم تثبيت التطبيق المحدد أو لم يتم تثبيته عليها، بناءً على الحالة المحددة، في التحديد.

في حقل الإدخال، يمكنك تحديد معيار للأجهزة المشمولة في التحديد عند إجراء بحث باسم التطبيق أو برقم حزمة التحديث.

إذا تم ترك الحقل فارغًا، لن يتم تطبيق المعيار.

- **Select the period of the last update of modules**

يمكنك استخدام هذا الخيار لتعيين معيار للبحث في الأجهزة على وقت آخر تحديث للوحدات النمطية الخاصة بالتطبيقات المثبتة على تلك الأجهزة.

إذا تم تحديد خانة الاختيار هذه، يمكنك تحديد في حقل الإدخال الفاصل الزمني (الوقت والتاريخ) الذي تم خلاله إجراء التحديث الأخير للوحدات النمطية المثبتة على تلك الأجهزة.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **Device is managed through Administration Server**

في هذه القائمة المنسدلة، يمكنك تضمين الأجهزة المدارة بواسطة Kaspersky Security Center في التحديد:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المدارة بواسطة Kaspersky Security Center في الاختيار.
- **لا**. يشمل التطبيق الأجهزة الموجودة في التحديد ما لم تكن مدارة من خلال Kaspersky Security Center.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **Security application is installed**

في هذه القائمة المنسدلة، يمكنك تضمين جميع الأجهزة المدارة المثبت عليها تطبيق الأمان في التحديد:

- **نعم**. يشمل التطبيق في الاختيار جميع الأجهزة المدارة بواسطة تطبيق الأمان الذي تم تثبيته:
- **لا**. يشمل التطبيق في الاختيار جميع الأجهزة غير المثبت عليها تطبيق الأمان.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

في القسم الفرعي **Anti-virus protection**، يمكنك إعداد معايير لتضمين الأجهزة في تحديد بناءً على حالة الحماية الخاصة بها:

- **Databases released**

إذا تم تحديد هذا الخيار، يمكنك البحث عن أجهزة العميل حسب تاريخ إصدار قاعدة بيانات تطبيق مكافحة الفيروسات. في حقول الإدخال، يمكنك تعيين الفاصل الزمني الذي يتم إجراء البحث بناءً عليه.

يتم تعطيل هذا الخيار افتراضيًا.

- **Database records count**

إذا تم تمكين هذا الخيار، فيمكنك البحث عن أجهزة العميل حسب عدد سجلات قواعد البيانات. في حقول الإدخال، يمكنك تعيين القيم الحد الأدنى والأعلى لسجلات قاعدة بيانات مكافحة الفيروسات.

يتم تعطيل هذا الخيار افتراضيًا.

- **Last scanned**

إذا تم تمكين هذا الخيار، فيمكنك البحث عن أجهزة العميل حسب وقت آخر فحص للبرامج الضارة. في حقول الإدخال، يمكنك تحديد الفترة الزمنية التي تم فيها آخر فحص للبرامج الضارة.

يتم تعطيل هذا الخيار افتراضيًا.

- **Threats detected**

إذا تم تمكين هذا الخيار، يمكنك البحث عن أجهزة العميل حسب عدد الفيروسات التي تم العثور عليها. في حقول الإدخال، يمكنك تعيين قيم الحد الأدنى والأعلى لعدد الفيروسات التي تم العثور عليها.

يتم تعطيل هذا الخيار افتراضيًا.

في القسم الفرعي **Encryption**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على خوارزمية التشفير المحددة:

Encryption algorithm

مقياس التشفير المتقدم (AES) خوارزمية التشفير الكتلي المتناظر. في القائمة المنسدلة، يمكنك تحديد حجم مفتاح التشفير (56 بت أو 128 بت أو 192 بت أو 256 بت).

القيم المتوفرة: AES56وAES128وAES192وAES256.

> يحتوي القسم الفرعي **Application components** على قائمة بمكونات تلك التطبيقات التي تحتوي على مكونات إضافية إدارية مقابلة مثبتة في Kaspersky Security Center Web Console.

في القسم الفرعي **Application components**، يمكنك تحديد معايير لتضمين الأجهزة في تحديد وفقًا للحالات ولأرقام الإصدار المكونات التي تشير للتطبيق الذي حددته:

- **Status**

البحث عن الأجهزة وفقًا لحالة المكون المُرسلة بواسطة تطبيق إلى خادم الإدارة. يمكنك تحديد إحدى الحالات التالية: لا ينطبق، متوقف، متوقف مؤقتًا، جارٍ البدء، قيد التشغيل، فشل، غير مثبت غير مدعوم من الترخيص. إذا كان للمكون المحدد للتطبيق المُثبت على جهاز مُدار حالة محددة، فإنه يتم تضمين الجهاز في تحديد الجهاز.

الحالات المرسلة بواسطة التطبيقات:

- متوقف—تم تعطيل المكون وهو لا يعمل في الوقت الحالي.
- تم الإيقاف مؤقتًا—تم تعليق المكون، على سبيل المثال، بعد إيقاف المستخدم للحماية مؤقتًا في التطبيق المُدار.
- بدء تشغيل—يكون المكون في عملية التهيئة في الوقت الحالي.
- قيد التشغيل—يكون المكون ممكنًا ويعمل على النحو الصحيح.
- فشل— حدث خطأ أثناء تشغيل المكون.
- غير مثبت—لم يقم المستخدم بتحديد المكون للتثبيت عند تكوين التثبيت المخصص للتطبيق.
- غير مدعوم من الترخيص — لا يغطي الترخيص المكون المحدد.

بخلاف الحالات الأخرى، فإن الحالة لا ينطبق لا تُرسل بواسطة التطبيقات. يُظهر هذا الخيار عدم امتلاك التطبيقات لمعلومات حول حالة المكون المحدد. على سبيل المثال، قد يحدث هذا عندما يكون المكون المحدد لا ينتمي لأي من التطبيقات المثبتة على الجهاز، أو عند إيقاف تشغيل الجهاز.

- **الإصدار**

البحث عن الأجهزة وفقًا لرقم الإصدار للمكون الذي حددته في القائمة. يمكنك كتابة رقم الإصدار، على سبيل المثال `3.4.1.0`، ثم تحديد ما إذا كان المكون المحدد يجب أن يمتلك إصدارًا مماثلاً أو إصدارًا سابقًا أو إصدارًا أحدث. يمكنك أيضًا تكوين البحث عن جميع الإصدارات عدا الإصدار المحدد.

Tags

في القسم **Tags**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على الكلمات المفتاحية (العلامات) التي تمت إضافتها سابقًا إلى أوصاف الأجهزة المدارة:

Apply if at least one specified tag matches

إذا تم تمكين هذا الخيار، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على علامة واحدة من العلامات على الأقل.

إذا تم تعطيل هذا الخيار، فستعرض نتائج البحث فقط الأجهزة التي تحتوي أوصافها على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

لإضافة علامات إلى المعيار ، انقر فوق الزر **Add** وحدد العلامات بالنقر فوق حقل الإدخال **Tag**. حدد ما إذا كنت تريد تضمين أو استثناء الأجهزة ذات العلامات المحددة في تحديد الجهاز.

- **Must be included**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

يتم تحديد هذا الخيار افتراضيًا.

- **Must be excluded**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي لا تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

Users

في القسم **Users**، يمكنك إعداد المعايير لتضمين الأجهزة في التحديد بحسب حسابات المستخدمين الذين قاموا بتسجيل الدخول إلى نظام التشغيل.

- **Last user who logged in to the system**

إذا تم تمكين هذا الخيار، يمكنك تحديد حساب المستخدم لتكوين المعيار. وتشمل نتائج البحث الأجهزة التي قام مستخدم محدد بإجراء آخر تسجيل دخول عليها إلى النظام.

- **User who logged in to the system at least once**

إذا تم تمكين هذا الخيار، فانقر فوق زر **استعراض** لتحديد حساب مستخدم. ستتضمن نتائج البحث الأجهزة التي قام مستخدم محدد بتسجيل الدخول عليها مرة واحدة على الأقل.

تصدير قائمة الأجهزة من تحديد جهاز

يتيح لك Kaspersky Security Center حفظ معلومات عن الأجهزة من تحديد جهاز وتصديرها كملف CSV أو ملف TXT.

لتصدير قائمة الأجهزة من تحديد الجهاز:

1. افتح الجدول الذي يتضمن الأجهزة من تحديد الجهاز.
2. استخدم إحدى الطرق التالية لتحديد الأجهزة التي تريد تصديرها:
   - لتحديد أجهزة معينة، حدد خانات الاختيار المجاورة لها.
   - لتحديد جميع الأجهزة من صفحة الجدول الحالية، حدد خانة الاختيار في رأس جدول الجهاز، ثم حدد خانة الاختيار **تحديد الكل في الصفحة الحالية**.
   - لتحديد كل الأجهزة من الجدول، حدد خانة الاختيار الموجودة في رأس جدول الأجهزة، ثم حدد خانة الاختيار **تحديد الكل**.
3. انقر فوق الزر **Export to CSV** أو **Export to TXT**. سيتم تصدير كل المعلومات عن الأجهزة المحددة المدرجة في الجدول.

لاحظ أنه إذا طبقت معيار عامل التصفية على جدول الأجهزة، فسيتم فقط تصدير البيانات التي تمت تصفيتها من الأعمدة المعروضة.

إزالة أجهزة من مجموعات الإدارة في تحديد

عند العمل مع تحديد جهاز، يمكنك إزالة الأجهزة من مجموعات الإدارة في هذا التحديد، دون التبديل إلى مجموعات الإدارة التي يجب إزالة هذه الأجهزة منها.

لإزالة الأجهزة من مجموعات إدارة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Device selections** أو القسم **Discovery & deployment** ← **Device selections**.

2. في قائمة التحديد، انقر على اسم تحديد الجهاز.

   تعرض الصفحة جدولاً يتضمن معلومات عن الأجهزة المضمنة في تحديد الجهاز.

3. حدد الأجهزة التي ترغب في إزالتها، ثم انقر على **Delete**.

   يتم إزالة الأجهزة المحددة من مجموعات الإدارة الخاصة بها.

علامات الجهاز

يتيح Kaspersky Security Center لك وضع علامات على الأجهزة. العلامة هي ملصق جهاز يمكن استخدامها لتجميع الأجهزة أو وصفها أو العثور عليها. يمكن استخدام العلامات المخصصة للأجهزة لإنشاء تحديدات، وللعثور على الأجهزة وتوزيعها بين مجموعات الإدارة.

يمكنك وضع علامة على الأجهزة يدويًا أو تلقائيًا. إذا كنت تريد وضع علامة على جهاز فردي، يمكنك استخدام وضع العلامات اليدوي. ويتم تنفيذ وضع العلامات التلقائية بواسطة Kaspersky Security Center بإحدى الطرق التالية:

- وفقًا لقواعد وضع العلامات المحددة.
- عن طريق تطبيق.

لا نوصيك باستخدام طرق مختلفة للوسم لتعيين نفس العلامة نفسها. على سبيل المثال، في حالة تعيين العلامة بواسطة القاعدة، فليس من المستحسن تعيين هذه العلامة يدويًا للأجهزة.

في حالة تعيين العلامات بواسطة القواعد، فسيتم وضع علامات على الأجهزة تلقائيًا عند استيفاء القواعد المحددة. تتطابق كل قاعدة فردية مع كل علامة. تنطبق القواعد على خصائص شبكة الجهاز ونظام التشغيل والتطبيقات المثبتة على الجهاز وخصائص الجهاز الأخرى. على سبيل المثال: إذا كان لديك بنية أساسية مدمجة لأجهزة حقيقية ومثيلات Amazon EC2، والأجهزة الظاهرية من Microsoft Azure، يمكنك وضع قاعدة ستخصص علامة `[Azure]` لجميع الأجهزة الظاهرية من Microsoft Azure. يمكنك بعد ذلك استخدام هذه العلامة عند إنشاء تحديد جهاز; وسيساعدك هذا في ترتيب جميع الأجهزة الافتراضية من Microsoft Azure وتعيين مهمة لها.

يمكنك إضافة قاعدة واحدة فقط لوضع العلامات التلقائي لكل علامة. وإذا أنشأت قاعدة جديدة للعلامة ذاتها، فسيتم استبدال السابقة.

يتم إزالة علامة تلقائيًا من جهاز في الحالات التالية:

- عندما يتوقف الجهاز عن تلبية شروط القاعدة التي تخصص العلامة.
- عندما يتم تعطيل القاعدة التي تخصص العلامة أو حذفها.

قائمة العلامات وقائمة القواعد على كل خادم إدارة مستقلة عن جميع خوادم الإدارة الأخرى، بما في ذلك خادم إدارة أساسي أو خوادم إدارة ظاهرية ثانوية. لا يتم تطبيق القاعدة إلا على الأجهزة التي توجد في خادم الإدارة نفسه الذي تم إنشاء القاعدة عليه.

إنشاء علامة لجهاز

لإنشاء علامة لجهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tags** ← **Device tags**.
2. انقر على **Add**.
   ستفتح نافذة علامة جديدة.
3. في حقل **Tag**، أدخل اسم العلامة.
4. انقر على **Save**لحفظ التغييرات.

تظهر العلامة الجديدة في قائمة علامات الجهاز.

إعادة تسمية علامة جهاز

لإعادة تسمية علامة جهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tags** ← **Device tags**.
2. انقر على اسم العلامة التي ترغب في إعادة تسميتها.
   ستفتح نافذة الخصائص.
3. في حقل **Tag**، قم بتغيير اسم العلامة.
4. انقر على **Save**لحفظ التغييرات.

تظهر العلامة المحدثة في قائمة علامات الجهاز.

حذف علامة جهاز

لحذف علامة جهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tags** ← **Device tags**.
2. من القائمة، حدد علامة الجهاز التي ترغب في حذفها.
3. انقر على زر **Delete**.
4. في النافذة التي تفتح، انقر على **Yes**.

سيتم حذف علامة الجهاز. يتم إزالة العلامة المحذوفة بشكل تلقائي من جميع الأجهزة التي تخصيصها إليها.

لا يتم إزالة العلامة التي حذفتها بشكل تلقائي من قواعد وضع العلامات تلقائيًا. بعد حذف العلامة، لا يتم تخصيصها إلى جهاز جديد إلا عندما يفي الجهاز بمتطلبات قاعدة تخصص العلامة.

لا تتم إزالة العلامة المحذوفة تلقائيًا من الجهاز في حالة تعيين هذه العلامة للجهاز عن طريق تطبيق أو عميل الشبكة. ولإدارة هذه العلامات، استخدم الأداة المساعدة klscflag.

عرض الأجهزة التي تم تعيين علامة لها

لعرض الأجهزة التي تم تعيين علامة لها:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tags** ← **Device tags**.
2. انقر على رابط **View devices** بجوار العلامة التي ترغب في عرض الأجهزة المخصصة لها.

   ستتم إعادة توجيهك إلى القسم **Managed devices** في القائمة الرئيسية، مع تصفية الأجهزة حسب العلامة التي قمت بالنقر فوق الرابط **View devices** لها.
3. إذا كنت تريد العودة إلى قائمة علامات الجهاز، فانقر فوق الزر **السابق** في المستعرض.

بعد عرض الأجهزة التي تم تعيين العلامة لها، يمكنك إما إنشاء علامة جديدة وتعيينها أو تعيين العلامة الموجودة لأجهزة أخرى. وفي هذه الحالة، يجب عليك إزالة عامل التصفية حسب العلامة، وتحديد الأجهزة، ثم تعيين العلامة.

عرض العلامات المعينة إلى جهاز

لعرض العلامات المعينة إلى جهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.
2. انقر على اسم الجهاز الذي ترغب في عرض علاماته.
3. في النافذة خصائص الجهاز التي تُفتح، حدد علامة التبويب **Tags**.

   يتم عرض قائمة العلامات المعينة للجهاز المحدد. في العمود **Tag assigned** يمكنك عرض كيفية تعيين العلامة.

في شريط الأدوات، يمكنك إجراء ما يلي:

- تعيين علامة أخرى للجهاز.
- إزالة علامة معينة بالفعل.
- عرض كل علامات الجهاز الموجودة على خادم الإدارة.

لا يمكنك عرض العلامات المعينة محليًا على الأجهزة.

وضع علامة على جهاز يدويًا

لتخصيص علامة إلى جهاز يدويًا:

1. اعرض العلامات المخصصة للجهاز الذي ترغب في تخصيص علامة أخرى له.
2. انقر على **Add**.

3. في النافذة التي تفتح، قم بأحد الإجراءات التالية:

- لإنشاء علامة جديدة وتخصيصها، حدد **Create new tag** ثم حدد اسم العلامة الجديدة.
- لتحديد علامة موجودة، حدد **Assign existing tag** ثم حدد العلامة الضرورية في القائمة المنسدلة.

4. انقر على **OK** لتطبيق التغييرات.

5. انقر على **Save**لحفظ التغييرات.

يتم تخصيص العلامة المحددة إلى الجهاز.

إزالة علامة معينة من جهاز

لإزالة علامة من جهاز:

1. في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)**.
2. انقر على اسم الجهاز الذي ترغب في عرض علاماته.
3. في النافذة خصائص الجهاز التي تُفتح، حدد علامة التبويب **Tags**.
4. حدد خانة الاختيار الموجودة بجوار العلامة التي ترغب في إزالتها.
5. في أعلى القائمة، انقر فوق الزر **Unassign tag?**.
6. في النافذة التي تفتح، انقر على **Yes**.

يتم إزالة العلامة من الجهاز.

لا يتم حذف علامة الجهاز غير المخصصة. يمكنك، إذا كنت ترغب، حذفها يدويًا .

لا يمكنك إزالة العلامات التي تم تعيينها للجهاز يدويًا بواسطة التطبيقات أو عميل الشبكة. ولإدارة هذه العلامات، استخدم الأداة المساعدة klscflag.

عرض قواعد وضع العلامات على الأجهزة تلقائيًا

لعرض قواعد وضع العلامات على الأجهزة تلقائيًا،

قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل إلى **Auto-tagging rules** ← **Tags** ← **Assets (Devices)**.
- في القائمة الرئيسية، انتقل إلى **Device tags** ← **Tags** ← **Assets (Devices)**، ثم انقر فوق الرابط **Set up auto-tagging rules**.
- اعرض العلامات المخصصة لجهاز ثم انقر على زر **Settings**.

ستظهر قائمة بقواعد وضع العلامات على الأجهزة تلقائيًا.

تحرير قاعدة لوضع علامات على الأجهزة تلقائيًا

لتحرير قاعدة لوضع علامات على الأجهزة تلقائيًا:

1. اعرض قواعد وضع العلامات على الأجهزة تلقائيًا.

2. انقر على اسم القاعدة التي ترغب في تحريرها.

   ستفتح نافذة إعدادات القاعدة.

3. قم بتحرير الخصائص العامة للقاعدة:

   a. قم بتغيير اسم القاعدة في حقل **Rule name**.

   لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا.

   b. قم بأحد الإجراءات التالية:

   - قم بتمكين القاعدة عن طريق تبديل زر التبديل إلى **Rule enabled**.
   - قم بتعطيل القاعدة عن طريق تبديل زر التبديل إلى **Rule disabled**.

4. قم بأحد الإجراءات التالية:

   - إذا كنت ترغب في إضافة شرط جديد، انقر على زر **Add** ثم حدد إعدادات الشرط الجديد في النافذة التي تفتح.
   - إذا كنت ترغب في تحرير شرط موجود، انقر على اسم الشرط الذي ترغب في تحريره ثم على تحرير إعدادات الشرط.
   - إذا كنت ترغب في حذف شرط، حدد خانة الاختيار الموجودة بجوار اسم الشرط الذي ترغب في حذفه ثم انقر على **Delete**.

5. انقر على **OK** في نافذة إعدادات الشروط.

6. انقر على **Save**لحفظ التغييرات.

   تظهر القاعدة التي تم تحريرها في القائمة.

إنشاء قاعدة لوضع علامات على الأجهزة تلقائيًا

لإنشاء قاعدة لوضع علامات على الأجهزة تلقائيًا:

1. اعرض قواعد وضع العلامات على الأجهزة تلقائيًا.

2. انقر على **Add**.

   ستفتح نافذة إعدادات قاعدة جديدة.

3. قم بتكوين الخصائص العامة للقاعدة:

   a. أدخل اسم القاعدة في حقل **Rule name**.

   لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا.

b. قم بأحد الإجراءات التالية:

- قم بتمكين القاعدة عن طريق تبديل زر التبديل إلى **Rule enabled**.
- قم بتعطيل القاعدة عن طريق تبديل زر التبديل إلى **Rule disabled**.

c. أدخل اسم علامة الجهاز الجديدة في حقل **Tag** أو حدد واحدة من علامات الجهاز الموجودة من القائمة.
لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا.

4. انقر على زر **Add** في قسم الشروط من أجل إضافة شرط جديد.
ستفتح نافذة إعدادات شرط جديد.

5. أدخل اسم الشرط.
لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. يجب أن يكون الاسم فريدًا داخل القاعدة.

6. قم بإعداد بدء تشغيل القاعدة حسب الشروط التالية. يمكنك تحديد العديد من الشروط.

- **Network**: خصائص الشبكة للجهاز، مثل اسم الجهاز في شبكة Windows، أو تضمين الجهاز في مجال أو شبكة IP فرعية.

إذا تم تعيين ترتيب حساس لحالة الأحرف لقاعدة البيانات التي تستخدمها في Kaspersky Security Center، احتفظ بالحالة عند تحديد اسم DNS للجهاز. وبخلاف ذلك، لن تعمل قاعدة وضع العلامات التلقائي.

- **Applications**— وجود عميل الشبكة على الجهاز ونوع نظام التشغيل والإصدار والبنية.
- **Virtual machines**: الأجهزة التي تنتمي إلى نوع معين من الأجهزة الظاهرية.
- **Domain controller**—وجود الجهاز في الوحدة التنظيمية لـ Active Directory، وعضوية الجهاز في مجموعة Active Directory.
- **Applications registry**—وجود تطبيقات لبائعين مختلفين على الجهاز.

7. انقر فوق **OK** لحفظ التغييرات.
يمكنك إعداد العديد من الشروط لقاعدة واحدة إن لزم الأمر. في هذه الحالة، سيتم تعيين العلامة إلى الجهاز عند استيفائه لشرط واحد على الأقل.

8. انقر على **Save**لحفظ التغييرات.

يتم فرض تطبيق القاعدة التي تم إنشائها حديثًا على الأجهزة المُدارة بواسطة خادم الإدارة المحدد. إذا كانت إعدادات الجهاز مستوفية لشروط القاعدة، يتم تعيين العلامة إلى الجهاز.

يتم تطبيق القاعدة بعد ذلك في الحالات التالية:

- بشكل تلقائي ودوري، حسب حمل العمل على الخادم
- بعد أن تنتهي من تحرير القاعدة
- عندما تبدأ تشغيل القاعدة يدويًا
- بعد أن يكتشف خادم الإدارة تغييرًا في إعدادات جهاز يفي بشروط القاعدة أو إعدادات مجموعة تحتوي على هذا الجهاز

يمكن إنشاء العديد من قواعد وضع العلامات. يمكن تعيين جهاز فردي بالعديد من العلامات إذا قمت بإنشاء العديد من قواعد وضع العلامات وإذا تم استيفاء الشروط الخاصة بهذه القواعد في وقت واحد. يمكنك عرض قائمة بجميع العلامات التي تم تعيينها في خصائص الجهاز.

قواعد التشغيل لوضع العلامات على الأجهزة تلقائيًا

عند تشغيل قاعدة، العلامة المحددة في خصائص هذه القاعدة يتم تخصيصها إلى الأجهزة التي تلبي القواعد المحددة في خصائص القاعدة نفسها. يمكنك لا يمكنك تشغيل إلا القواعد المفعلة.

لتشغيل قواعد وضع العلامات على الأجهزة تلقائيًا:

1. اعرض قواعد وضع العلامات على الأجهزة تلقائيًا.
2. حدد خانات الاختيار الموجودة بجوار القواعد المفعلة التي ترغب في تشغيلها.
3. انقر على زر **Run rule** .

سيتم تشغيل القواعد المحددة.

حذف قاعدة لوضع علامات على الأجهزة تلقائيًا

لحذف قاعدة لوضع علامات على الأجهزة تلقائيًا:

1. اعرض قواعد وضع العلامات على الأجهزة تلقائيًا.
2. حدد خانة الاختيار الموجودة بجوار القاعدة التي ترغب في حذفها.
3. انقر على **Delete**.
4. في النافذة التي تفتح، انقر على **Delete** مرة أخرى.

سيتم حذف القاعدة المحددة. يتم إلغاء تخصيص العلامة التي كانت محددة في خصائص هذه القاعدة من جميع الأجهزة التي كانت مخصصة لها.

لا يتم حذف علامة الجهاز غير المخصصة. يمكنك، إذا كنت ترغب، حذفها يدويًا .

إدارة علامات الجهاز باستخدام الأداة المساعدة klscflag

لتعيين مجموعة من العلامات لجهاز، تحتاج إلى تشغيل الأداة المساعدة klscflag على جهاز العميل الذي تريد تعيين العلامات له.

وتكتب الأداة المساعدة klscflag فوق العلامات الحالية المخصصة للأجهزة. ويعني هذا أنه يمكنك إضافة أو إزالة العلامات عن طريق تحديد مجموعة العلامات المطلوبة في الأمر. لا تحتوي الأداة المساعدة على أوامر منفصلة لإضافة أو إزالة العلامات الفردية. وبدلاً من ذلك، يمكنك تعديل مجموعة العلامات بأكملها.

عند تحديد أسماء العلامات في الأوامر مثل klscflag، يوصى باستخدام نهج ثابت للحالة، مثل استخدام الأحرف الكبيرة. ويمكن أن يساعد استخدام الأحرف الكبيرة في تجنب المشكلات المحتملة مع العلامات التي تختلف فقط في حالة الأحرف، وذلك اعتمادًا على تكوين نظام إدارة قاعدة البيانات (DBMS).

ولتعيين علامات لجهازك باستخدام الأداة المساعدة klscflag:

1. قم بتشغيل موجه الأوامر في Windows باستخدام حقوق المسؤول، ثم قم بتغيير الدليل الحالي إلى الدليل الذي يحتوي على الأداة المساعدة klscflag. توجد الأداة المساعدة klscflag في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي هو <Disk>:\Program Files (x86)\Kaspersky\NetworkAgent\Lab.

2. أدخل أحد الأوامر التالية:

- لتعيين مجموعة من العلامات:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv
     = ss_type|" svt ARRAY_T -ss- "["\TAG NAME 3"\,"\TAG NAME 2"\,"\TAG NAME 1"\]"
                                                                    ";"\SS_PRODINFO"\
```

حيث "["\TAG NAME 3"\,"\TAG NAME 2"\,"\TAG NAME 1"\] هي قائمة العلامات التي تريد تعيينها لجهازك.

وإذا تركت الأقواس المربعة فارغة، فسيؤدي هذا إلى إزالة جميع العلامات من الأجهزة:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv
                                                    ";"\SS_PRODINFO"\ = ss_type|" svt ARRAY_T -ss- "[]"
```

- لتعيين علامة جديدة لمجموعة موجودة من العلامات:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv
  svt ARRAY_T -- "["\TAG NAME 3"\,"\TAG NAME 2"\,"\TAG NAME 1"\,"\NEW TAG NAME"\]"
                                                                    ";"\SS_PRODINFO"\ = ss_type|" ss
```

حيث NEW TAG NAME هو اسم العلامة التي تريد تعيينها لجهازك و TAG NAME 1 و TAG NAME 2 و TAG NAME 3 هي أسماء العلامات المخصصة بالفعل للجهاز.

- لإزالة علامة معينة دون إزالة العلامات الأخرى المخصصة بالفعل للأجهزة، قم بتشغيل الأمر باستخدام مجموعة العلامات المحدثة.

على سبيل المثال، إذا كانت علاماتك الحالية هي TAG NAME 1 و TAG NAME 2 و TAG NAME 3 وتريد إزالة TAG NAME 2، فقم بتشغيل الأمر التالي:

```
klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv
   ";"\SS_PRODINFO"\ = ss_type|" svt ARRAY_T -ss- "["\TAG NAME 3"\,"\TAG NAME 1"\]"
```

3. إعادة تشغيل خدمة عميل الشبكة.

تقوم الأداة المساعدة klscflag بتعيين العلامات المحددة لجهازك.

4. إذا كنت تريد التأكد من أن الأداة المساعدة klscflag قامت بتعيين العلامات المحددة بنجاح، اعرض العلامات المخصصة للجهاز.

بدلاً من ذلك، يمكنك تعيين علامات الجهاز يدويًا.

السياسات وملفات تعريف السياسة

يمكنك في Kaspersky Security Center Web Console إنشاء سياسات لتطبيقات Kaspersky. يصف هذا القسم السياسات وملفات تعريف السياسة، كما يوفر تعليمات حول إنشائها وتعديلها.

حول السياسات وملفات تعريف السياسة

السياسة هي مجموعة من إعدادات تطبيقات Kaspersky التي تنطبق على مجموعة إدارة ومجموعاتها الفرعية. يمكنك تثبيت عدة تطبيقات Kaspersky على أجهزة مجموعة إدارة. Kaspersky Security Center يوفر سياسة واحدة لكل تطبيق من تطبيقات Kaspersky في مجموعة الإدارة. السياسة لها إحدى الحالات التالية (انظر الجدول أدناه):

حالة السياسة

الحالة	الوصف
نشطة	السياسة الحالية المطبقة على الجهاز. يمكن أن تكون سياسة واحدة نشطة لتطبيق Kaspersky في كل مجموعة إدارة. الأجهزة تطبق قيم الإعدادات لسياسة نشطة لتطبيق Kaspersky.
غير نشطة	سياسة غير مطبقة حاليا على جهاز.
خارج المكتب	إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.

تعمل السياسات وفق القواعد التالية:

- يمكن تكوين عدة سياسات بقيم مختلفة لتطبيق واحد.
- يمكن تفعيل سياسة واحدة فقط للتطبيق الحالي.
- يمكنك تفعيل سياسة غير نشطة عند وقوع حدث معين. ويعني ذلك، على سبيل المثال، أنه يمكنك تنفيذ إعدادات مكافحة الفيروسات الأكثر صرامة أثناء انتشار الفيروسات.
- يمكن أن يكون للسياسة سياسات فرعية.

بشكل عام، يمكنك استخدام السياسات كاستعدادات لحالات الطوارئ، مثل هجمات الفيروسات. على سبيل المثال: في حال وجود هجمة عبر محركات الفلاش، يمكنك تنشيط سياسة تحجب الوصول إلى محركات أقراص الفلاش. في هذه الحالة، تصير السياسة المفعلة الحالية غير نشطة تلقائيًا.

من أجل منع الاحتفاظ بسياسات متعددة (على سبيل المثال عندما تفترض مناسبات مختلفة تغيير عدة إعدادات فقط)، يمكنك استخدام ملفات تعريف السياسة.

ملف السياسة التعريفي عبارة عن مجموعة فرعية من قيم إعدادات السياسة لها اسم، والتي تحل محل قيم إعدادات السياسة. ملف تعريف السياسة يؤثر على فاعلية تكوين الإعدادات على جهاز مُدار. الإعدادات الفعالة هي مجموعة من إعدادات السياسة وإعدادات ملفات تعريف السياسة وإعدادات التطبيق المحلية المطبقة حاليا للجهاز.

تعمل ملفات التعريفية للسياسة وفقًا للقواعد التالية:

- يسري ملف السياسة التعريفي عند حدوث حالة تفعيل معينة.
- ملفات تعريف السياسة تحتوي على قيم الإعدادات التي تختلف من إعدادات السياسة.
- تنشيط ملف تعريف السياسة يغير الإعدادات الفعالة للجهاز المُدار.
- يمكن أن تتضمن سياسة ما على 100 ملف تعريف سياسة بحد أقصى.

حول القفل والإعدادات المقفولة

كل إعداد سياسة به رمز زر قفل (🔒). الجدول أدناه يوضح حالات زر القفل:

حالات زر القفل

الحالة	الوصف
Undefined	في حال عرض قفل مفتوح بجوار إعداد وكان زر التبديل معطلاً، هذا الإعداد غير مخصص في السياسة. يمكن لمستخدم أن يغير هذه الإعدادات في واجهة التطبيق المُدار. هذه الأنواع من الإعدادات تسمى غير مقفولة.
Enforce	في حال عرض قفل مقفول بجوار إعداد وكان زر التبديل مفعلاً، هذا الإعداد مطبق على الأجهزة التي تسير السياسة عليها. لا يمكن للمستخدم تعديل قيم هذه الإعدادات في واجهة التطبيق المُدار. هذه الأنواع من الإعدادات تسمى مقفولة.

نوصي بشدة بإغلاق الأقفال لإعدادات السياسة التي تريد تطبيقها على الأجهزة المدارة. يمكن إعادة تعيين إعدادات السياسة غير المؤمّنة من خلال إعدادات تطبيق Kaspersky على جهاز مُدار.

يمكنك استخدام زر قفل لإجراء الإجراءات التالية:

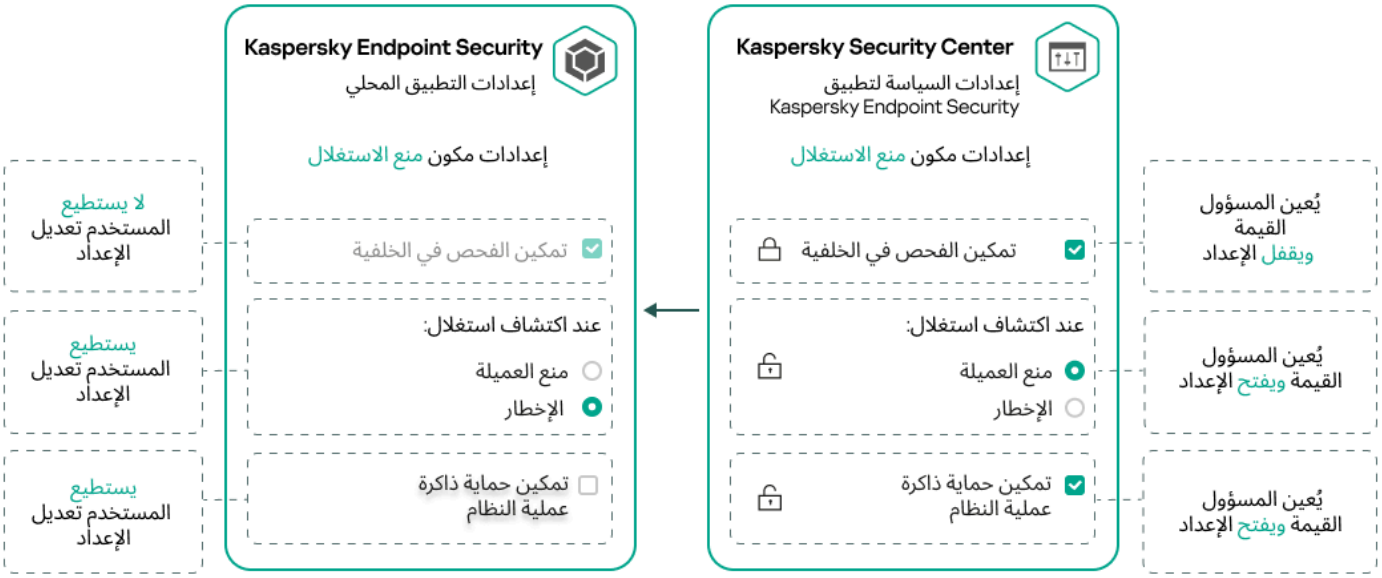
- قفل الإعدادات لسياسة مجموعة إدارة فرعية
- قفل الإعدادات لتطبيق Kaspersky على جهاز مُدار

وبالتالي يتم استخدام إعداد مقفول في تنفيذ الإعدادات الفعالة على جهاز مُدار.

عملية تنفيذ الإعدادات الفعالة تشمل الإجراءات التالية:

- الجهاز المُدار يطبق قيم إعدادات تطبيق Kaspersky.
- الجهاز المُدار يطبق قيم الإعدادات المقفولة لسياسة.

تحتوي السياسة وتطبيق Kaspersky المُدار على نفس مجموعة الإعدادات. عندما تقوم بتكوين إعدادات السياسة، إعدادات تطبيق Kaspersky تغيّر القيم على الجهاز المُدار. لا يمكنك تعديل الإعدادات المقفولة على جهاز مُدار (راجع الشكل أدناه):



الأقفال وإعدادات تطبيق Kaspersky

التسلسل الهرمي للسياسات، واستخدام ملفات تعريف السياسة

يوفّر هذا القسم معلومات عن التسلسل الهرمي للسياسات وملفات تعريف السياسة وتوريثها.

التسلسل الهرمي للسياسات

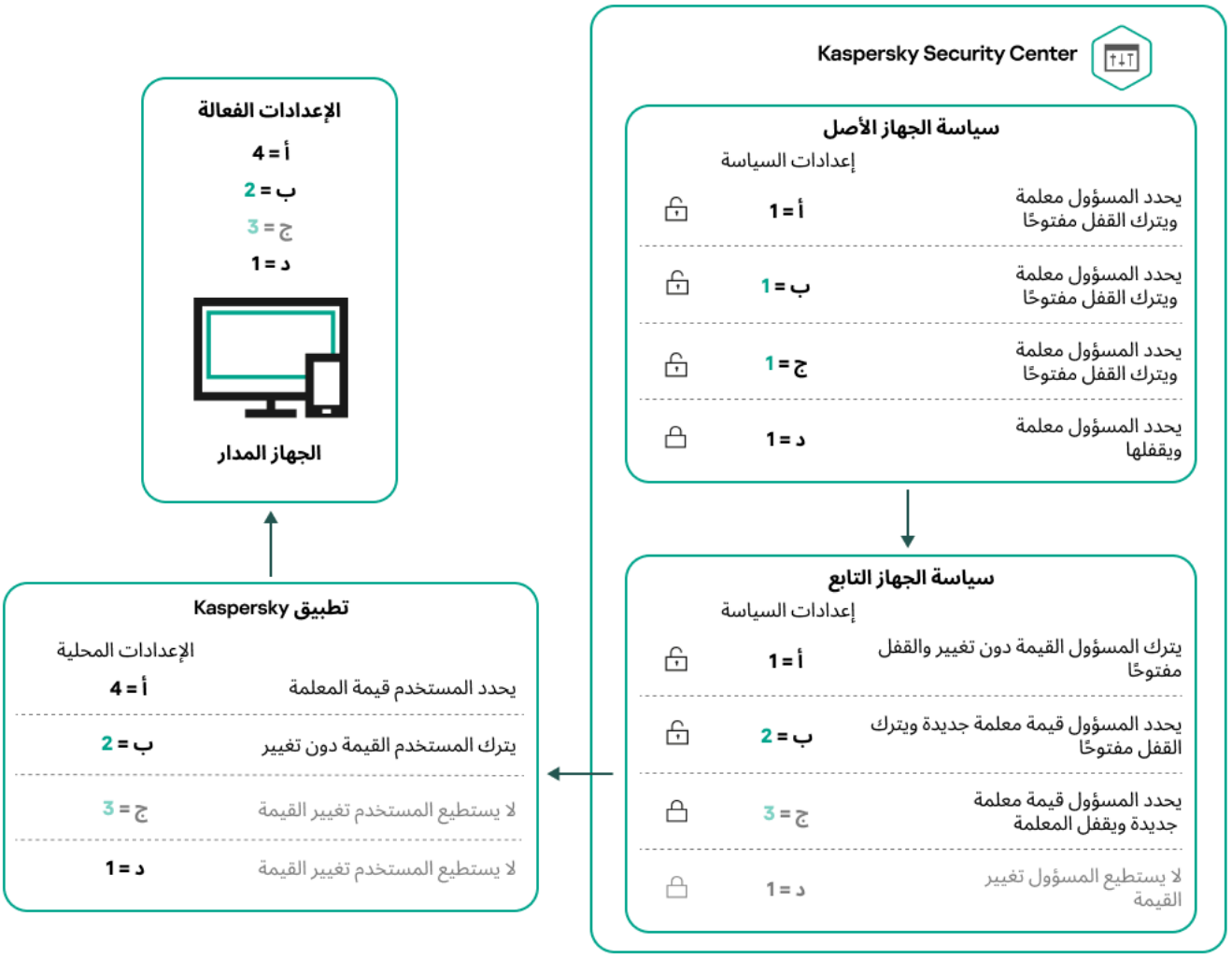
في حال وجود أجهزة مختلفة بحاجة إلى إعدادات مختلفة، يمكنك تنظيم الأجهزة في مجموعات إدارة.

يمكنك تحديد سياسة لمجموعة إدارة واحدة. يمكن وراثة إعدادات السياسة. التوريث يعني استقبال قيم إعدادات السياسة في مجموعات فرعية (مجموعات تابعة) من سياسة لمجموعة إدارة من مستوى أعلى (أصلية).

فيما يلي، تتم الإشارة إلى سياسة المجموعة الأصلية أيضًا بالسياسة الأصلية. تتم الإشارة إلى سياسة المجموعة الفرعية (المجموعة التابعة) أيضًا بالسياسة التابعة.

بشكل افتراضي، توجد مجموعة أجهزة مُدارة واحدة على الأقل على خادم الإدارة. إذا كنت ترغب في إنشاء مجموعات مخصصة، يتم إنشاؤها كمجموعات فرعية (مجموعات تابعة) داخل مجموعة الأجهزة المُدارة.

سياسات التطبيق نفسه تتصرف على بعضها وفق تسلسل هرمي لمجموعات الإدارة. الإعدادات المقفولة من سياسة مجموعة إدارة مستوى أعلى (أصلية) سوف تعيد تعيين قيم إعدادات السياسة لمجموعة فرعية (انظر الشكل أدناه).

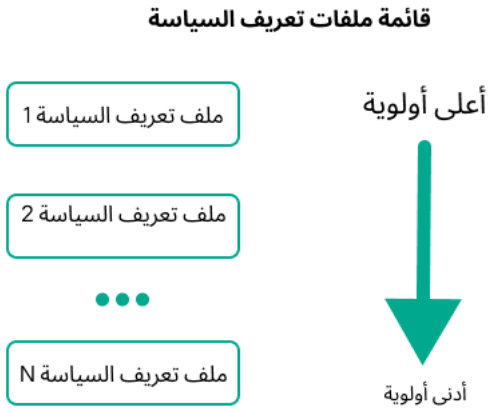


التسلسل الهرمي للسياسات

ملفات تعريف السياسة في التسلسل الهرمي للسياسات

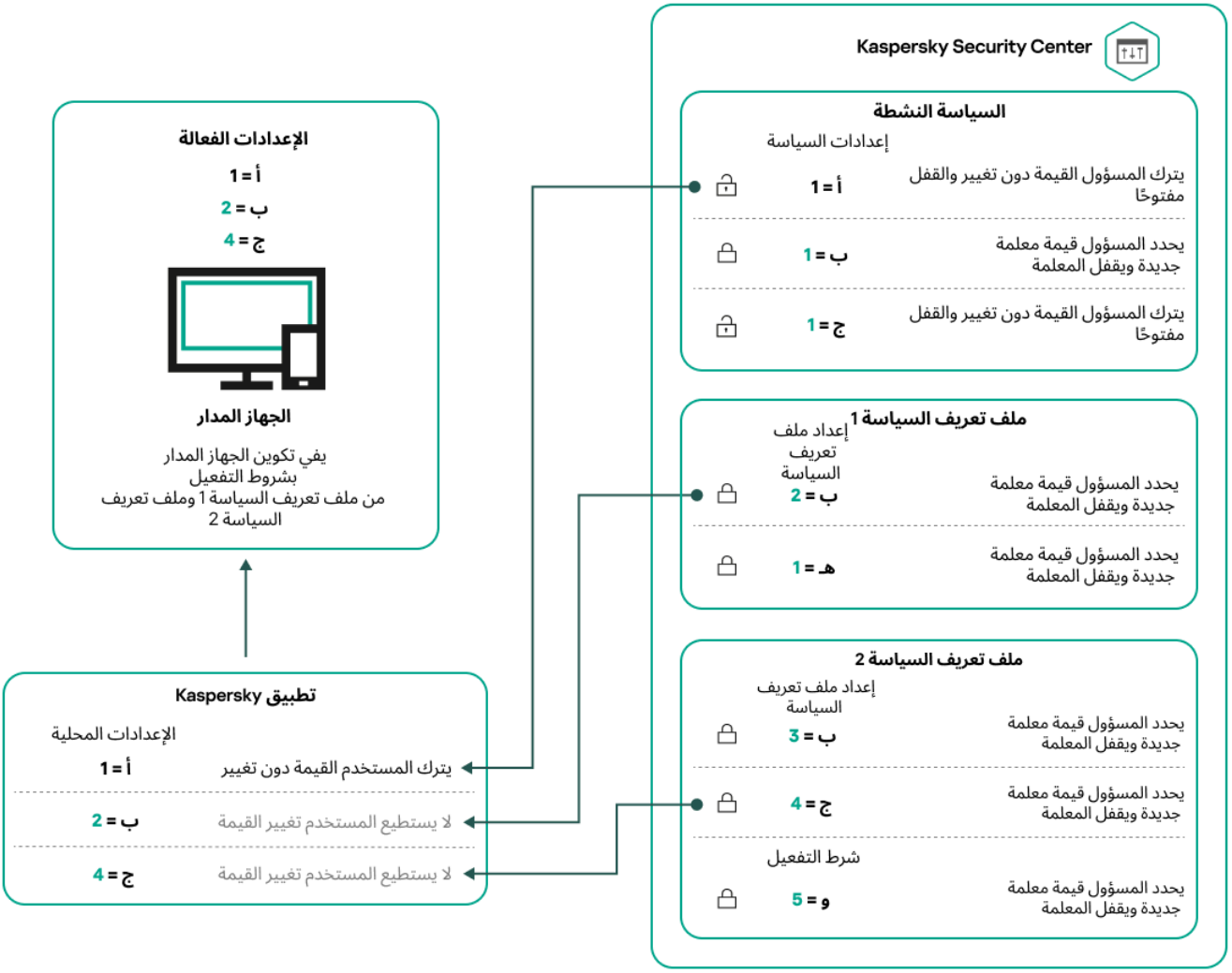
ملفات تعريف السياسة لها شروط تعيين الأولوية التالية:

- وضع الملف في قائمة ملف تعريف السياسة يشير إليه أولويته. يمكنك تغيير أولوية ملف تعريف سياسة. الموضع الأعلى في القائمة يشير إلى الأولوية الأعلى (انظر الشكل أدناه).



تعريف الأولوية لملف تعريف السياسة

- شروط التنشيط لملفات تعريف السياسة لا تعتمد على بعضها. يمكن تنشيط عدة ملفات تعريف سياسة في وقت واحد. في حال وجود عدة ملفات تعريف سياسة تؤثر على الإعداد نفسه، يأخذ الجهاز قيمة الإعداد من ملف تعريف السياسة صاحب أعلى أولوية (انظر الشكل أدناه).

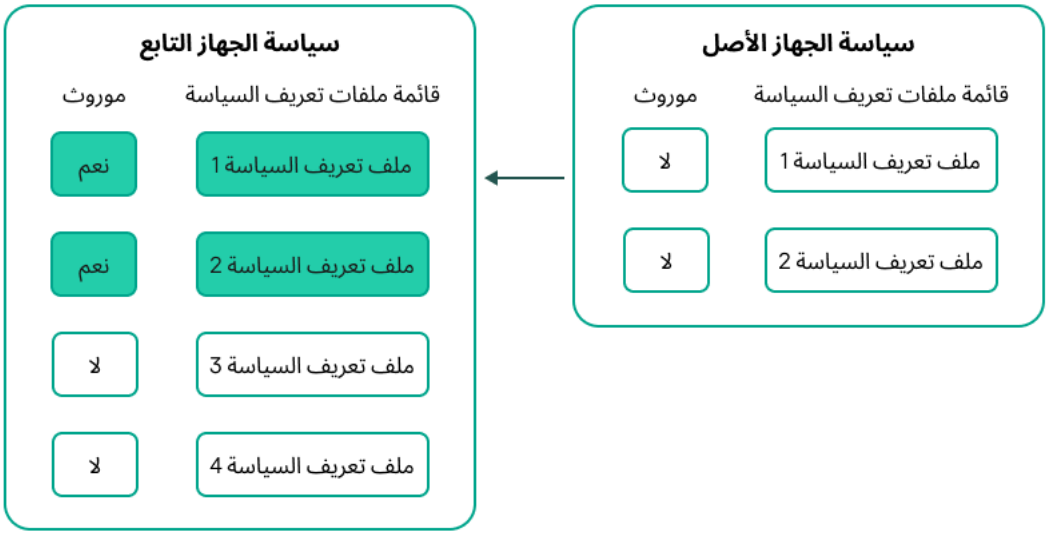


تكوين الجهاز المُدار يفي بشروط التنشيط لعدة ملفات تعريف سياسة

ملفات تعريف السياسة في التسلسل الهرمي للتوريث

ملفات تعريف السياسة من سياسات مستوى تسلسل هرمي مختلف تمتثل بالشروط التالية:

- سياسة المستوى الأقل ترث ملفات تعريف السياسة من سياسة المستوى الأعلى. ملف تعريف السياسة الموروث من سياسة مستوى أعلى يحصل على أولوية أعلى من مستوى ملف تعريف السياسة الأصلي.
- لا يمكنك تغيير أولوية ملف تعريف سياسة موروث (انظر الشكل أدناه).

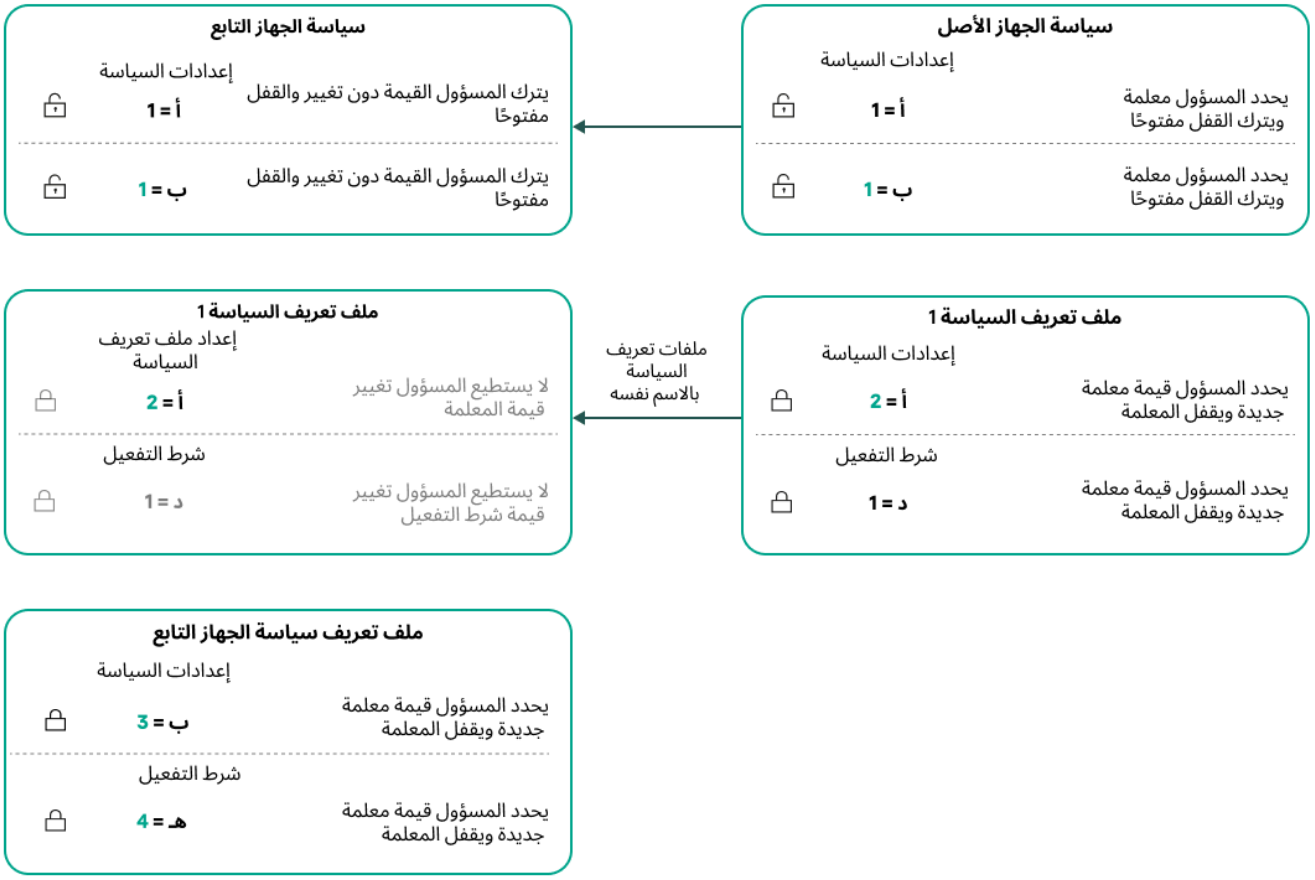


توريث ملفات تعريف السياسة

ملفات تعريف السياسة بالاسم نفسه

في حال وجود سياستين بالاسم نفسه في مستويين مختلفين في التسلسل الهرمي، تعمل هاتان السياساتان وفق القواعد التالية:

- الإعدادات المقفولة وشرط تنشيط ملف التعريف لملف تعريف سياسة مستوى أعلى تغيّر إعدادات وشرط تنشيط ملف التعريف لملف تعريف سياسة مستوى أقل (انظر الشكل أدناه).



يرث ملف التعريف الفرعي قيم الإعدادات من الملف التعريفي للسياسة الرئيسية

- لا تغيّر الإعدادات غير المقفولة وشرط تفعيل ملف التعريف لملف تعريف سياسة من مستوى أعلى إعدادات وشرط تفعيل ملف التعريف لملف تعريف سياسة من مستوى أقل.

كيفية تنفيذ الإعدادات على جهاز مُدار

تنفيذ إعدادات فعالة على جهاز مُدار يمكن أن يتم وصفه كما يلي:

- يتم أخذ قيم جميع الإعدادات التي لم يتم قفلها من السياسة.
- بعدها يتم استبدالها بقيم إعدادات التطبيق المُدار.
- وبعدها يتم تطبيق قيم الإعدادات المقفولة من السياسة الفعالة. قيم الإعدادات المقفولة تغير قيم الإعدادات الفعالة غير المقفولة.

إدارة السياسات

يصف هذا القسم إدارة السياسات ويوفِّر معلومات عن عرض قائمة السياسات وإنشاء سياسة وتعديل سياسة ونسخ سياسة ونقل سياسة والمزامنة المفروضة وعرض مخطط حالة توزيع السياسة وحذف سياسة.

عرض قائمة السياسات

يمكنك عرض قوائم السياسات التي تم إنشاؤها لخادم الإدارة أو أي مجموعة إدارة.

لعرض قائمة السياسات:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Hierarchy of groups**.

2. في هيكل مجموعة الإدارة، حدد مجموعة الإدارة التي ترغب في عرض قائمة السياسات لها.

تظهر قائمة السياسات في تنسيق جدولي. يكون الجدول فارغًا في حال عدم وجود سياسات. يمكنك عرض عواميد الجدول أو إخفائها أو تغيير ترتيبها أو عرض السطور التي تحتوي على قيمة تحددها أو استخدام البحث.

إنشاء سياسة

يمكنك إنشاء سياسات، ويمكنك كذلك تعديل السياسات الموجودة وحذفها.

لإنشاء سياسة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.

2. حدد مجموعة الإدارة التي سيتم إنشاء السياسة لها:

   - لمجموعة الجذر.

     في هذه الحالة يمكنك الانتقال إلى الخطوة التالية.

   - لمجموعة فرعية:

     a. انقر على رابط المسار الحالي الموجود أعلى النافذة.

     b. في اللوحة التي تفتح، انقر فوق الرابط الذي يحمل اسم المجموعة الفرعية المطلوبة.

     يتغير المسار الحالي ليعكس المجموعة الفرعية المحددة.

3. انقر على **Add**.

   تفتح نافذة **Select application**.

4. حدد التطبيق الذي ترغب في إنشاء سياسة له.

5. انقر على **Next**.

   تفتح نافذة إعدادات السياسة الجديدة مع وجود تبويب **General** محدد.

6. يمكنك إذا كنت ترغب تغيير الاسم الافتراضي والحالة الافتراضية وإعدادات التوارث الافتراضية للسياسة.

7. حدد تبويب **Application settings**.

   أو يمكنك النقر على **Save** والخروج. ستظهر السياسة في قائمة السياسات، ويمكنك تحرير إعداداتها لاحقًا.

8. في علامة التبويب **Application settings**، حدد في الجزء الأيمن الفئة التي تريدها، وفي الجزء الأيسر قم بتحرير إعدادات السياسة. يمكنك تحرير إعدادات السياسة في كل فئة (قسم).

تعتمد مجموعة الإعدادات على التطبيق الذي تنشئ سياسة له. لمزيد من التفاصيل ، يُرجى الرجوع إلى ما يلي:

- تكوين خادم الإدارة
- إعدادات سياسة عميل الشبكة
- وثائق Kaspersky Endpoint Security for Windows

لمعرفة تفاصيل عن إعدادات تطبيقات الأمان الأخرى، يمكنك الرجوع إلى وثائق التطبيق المقابل.
عند تحرير الإعدادات، يمكنك النقر على **Cancel** لإلغاء العملية الأخيرة.

9. انقر على **Save** لحفظ السياسة.

ستظهر السياسة في قائمة السياسات.

تعديل سياسة.

لتعديل سياسة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. انقر على السياسة التي ترغب في تعديلها.
ستفتح نافذة إعدادات السياسة.
3. حدد الاعدادات العامة وإعدادات التطبيق الذي تقوم بإنشاء سياسة له. لمزيد من التفاصيل ، يُرجى الرجوع إلى ما يلي:
- تكوين خادم الإدارة
- إعدادات سياسة عميل الشبكة
- وثائق Kaspersky Endpoint Security for Windows

لمعرفة تفاصيل عن إعدادات تطبيقات الأمان الأخرى، يمكنك الرجوع إلى وثائق ذلك التطبيق.

4. انقر على **Save**.

سيتم حفظ التغييرات التي تم إجراؤها على السياسة في خصائص السياسة، وسيتم عرضها في قسم **Revision history**.

إعدادات السياسة العامة

General

في تبويب **General**، يمكنك تعديل حالة السياسة وتحديد توريث إعدادات السياسة:

- في الكتلة **Policy status**، يمكنك تحديد أحد أوضاع السياسة:
  - **Active**

    إذا تم تحديد هذا الخيار، تصبح السياسة نشطة.
    يتم تحديد هذا الخيار افتراضيًا.

- **Out-of-office**

  إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.

- **Inactive**

  إذا تم تحديد هذا الخيار، تصبح السياسة غير نشطة، ولكنها تظل مخزنة في مجلد **السياسات**. إذا لزم الأمر، يمكن تنشيط السياسة.

- في مجموعة الإعدادات **Settings inheritance**، يمكنك تكوين توريث السياسة:

  - **Inherit settings from parent policy**

    إذا تم تمكين هذا الخيار، يتم توريث قيم إعدادات السياسة من سياسة المجموعة ذات المستوى الأعلى؛ ولهذا يتم إلغاء تأمينها.

    يتم تمكين هذا الخيار افتراضيًا.

  - **Force inheritance of settings in child policies**

    إذا تم تمكين هذا الخيار، يتم تنفيذ الإجراءات التالية بعد تطبيق تغييرات السياسة:

    - سيتم توزيع قيم إعدادات السياسة إلى سياسات المجموعات الفرعية للإدارة، أي إلى السياسات الفرعية.
    - في كتلة **توريث الإعدادات** الخاصة بالقسم **عام** في نافذة الخصائص لكل سياسة فرعية، سيتم تمكين الخيار **توريث الإعدادات من السياسة الأصلية** تلقائيًا.

    إذا تم تمكين هذا الخيار، فسيتم تأمين إعدادات السياسة الفرعية.

    يتم تعطيل هذا الخيار افتراضيًا.

Event configuration

يتيح لك تبويب **Event configuration** تكوين تسجيل الحدث وإخطار الحدث. يتم توزيع الأحداث حسب مستوى الأهمية على علامات التبويب التالية:

- **Critical**

  لا يتم عرض قسم **Critical** في خصائص سياسة عميل الشبكة.

- **Functional failure**
- **Warning**
- **Info**

في قسم البحث، تعرض القائمة أنواع الأحداث ومدّة تخزين الحدث الافتراضية على خادم الإدارة (بالأيام). النقر على نوع حدث يتيح لك تحديد الإعدادات التالية:

- **Event registration**

  يمكنك تحديد عدد أيام تخزين الحدث، وكذلك تحديد مكان تخزين الحدث:

  - **Export to SIEM system by using Syslog**
  - **Store in the OS event log on device**
  - **Store in the OS event log on Administration Server**

- **Event notifications**

يمكنك تحديد ما إذا كنت ترغب في أن يتم إخطارك بالحدث أم لا بإحدى الطرق التالية:

- **Notify by email**
- **Notify by SMS**
- **Notify by running an executable file or script**
- **Notify by SNMP**

يتم بشكل افتراضي استخدام إعدادات الإخطار المحددة في تبويب خصائص خادم الإدارة (مثل عنوان المستلم). يمكنك إذا كنت ترغب تغيير هذه الإعدادات في تبويبي **Email, SMS** و**Executable file to be run**.

Revision history

تبويب **Revision history** يتيح لك عرض قائمة بمراجعات السياسة و[التراجع عن تغييرات](#) تمت إلى السياسة عند الضرورة.

تمكين خيار توريث سياسة وتعطيله

لتمكين خيارات التوريث أو تعطيله في سياسة:

1. افتح السياسة المطلوبة.
2. افتح علامة التبويب **General**.
3. تمكين توريث سياسة أو تعطيله:

- في حالة تمكين **Inherit settings from parent policy** في سياسة فرعية ويقوم بدير بقفل بعض الإعدادات في السياسة الأصلية، بهذا لا يمكنك تغيير هذه الإعدادات في السياسة التابعة.
- في حالة تعطيل **Inherit settings from parent policy** في سياسة تابعة، يمكنك إذًا تغيير كل الإعدادات في السياسة التابعة حتى في حالة قفل بعض الإعدادات في السياسة الأصلية.
- في حالة تفعيل **Force inheritance of settings in child policies** في المجموعة الأصلية، يقوم هذا بتفعيل خيار **Inherit settings from parent policy** لكل سياسة تابعة. وفي هذه الحالة، لا يمكنك تعطيل هذا الخيار لأية سياسة تابعة. يتم فرض توريث كل الإعدادات التي تم قفلها في السياسة الأصلية في المجموعات التابعة ولا يمكنك تغيير هذه الإعدادات في المجموعات التابعة.

4. انقر على زر **Save** لحفظ التغييرات، أو انقر على زر **Cancel** لرفض التغييرات.

يتم افتراضيًا تمكين خيار **Inherit settings from parent policy** لسياسة جديدة.

إذا كانت السياسة تتضمن ملفات تعريف، تقوم السياسات التابعة بتوريث ملفات التعريف هذه.

نسخ سياسة

يمكنك نسخ السياسات من مجموعة إدارة إلى أخرى.

لنسخ سياسة إلى مجموعة إدارة أخرى:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. حدد خانة الاختيار الموجودة بجوار السياسة (أو السياسات)التي ترغب في نسخها.

3. انقر على زر **Copy**.

تظهر شجرة مجموعات الإدارة على الجانب الأيمن من الشاشة.

4. حدد في تلك الشجرة المجموعة المستهدفة، أي المجموعة التي ترغب في نسخ السياسة (أو السياسات) إليها.

5. انقر على زر **Copy**الموجود في الجزء السفلي من الشاشة.

6. انقر على **OK** لتأكيد العملية.

سيتم نسخ السياسة (أو السياسات) إلى المجموعة المستهدفة بجميع ملفات تعريفها. حالة كل سياسة منسوخة في المجموعة المستهدفة ستكون **Inactive**. يمكنك تغيير الحالة إلى **Active** في أي وقت.

في حالة وجود سياسة باسم مطابق لاسم السياسة المنقولة حديثًا في المجموعة المستهدفة بالفعل، سيتم الإضافة إلى اسم السياسة المنقولة حديثًا بوضع المؤشر (<رقم التسلسل التالي>) في آخر الاسم، مثل (1).

نقل سياسة

يمكنك نقل السياسات من مجموعة إدارة إلى أخرى. إذا كنت مثلاً ترغب في حذف مجموعة لكنك لا تزال ترغب في استخدام سياساتها في مجموعة أخرى. قد ترغب في هذه الحالة في نقل السياسة من المجموعة القديمة إلى المجموعة الجديدة قبل حذف المجموعة القديمة.

عند نقل سياسة إلى مجموعة إدارة أخرى، يتم مسح سجل مراجعة السياسة. تعرض علامة التبويب **سجل المراجعة** معلومات عن أحدث تغيير فقط.

لنقل سياسة إلى مجموعة إدارة أخرى:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.

2. حدد خانة الاختيار الموجودة بجوار السياسة (أو السياسات)التي ترغب في نقلها.

3. انقر فوق زر **Move**.

تظهر شجرة مجموعات الإدارة على الجانب الأيمن من الشاشة.

4. حدد في تلك الشجرة المجموعة المستهدفة، أي المجموعة التي ترغب في نقل السياسة (أو السياسات) إليها.

5. انقر على زر **Move**الموجود في الجزء السفلي من الشاشة.

6. انقر على **OK** لتأكيد العملية.

إذا كانت سياسة غير موروثة من المجموعة المصدر، سيتم نقلها إلى المجموعة المستهدفة بجميع ملفات تعريفها. حالة السياسة في المجموعة المستهدفة هي **Inactive**. يمكنك تغيير الحالة إلى **Active** في أي وقت.

إذا كانت سياسة موروثة من المجموعة المصدر، سوف تبقى في المجموعة المصدر. سيتم نسخ ها إلى المجموعة المستهدفة بجميع ملفات تعريفها. حالة السياسة في المجموعة المستهدفة هي **Inactive**. يمكنك تغيير الحالة إلى **Active** في أي وقت.

في حالة وجود سياسة باسم مطابق لاسم السياسة المنقولة حديثًا في المجموعة المستهدفة بالفعل، سيتم الإضافة إلى اسم السياسة المنقولة حديثًا بوضع المؤشر (<رقم التسلسل التالي>) في آخر الاسم، مثل (1).

تصدير سياسة

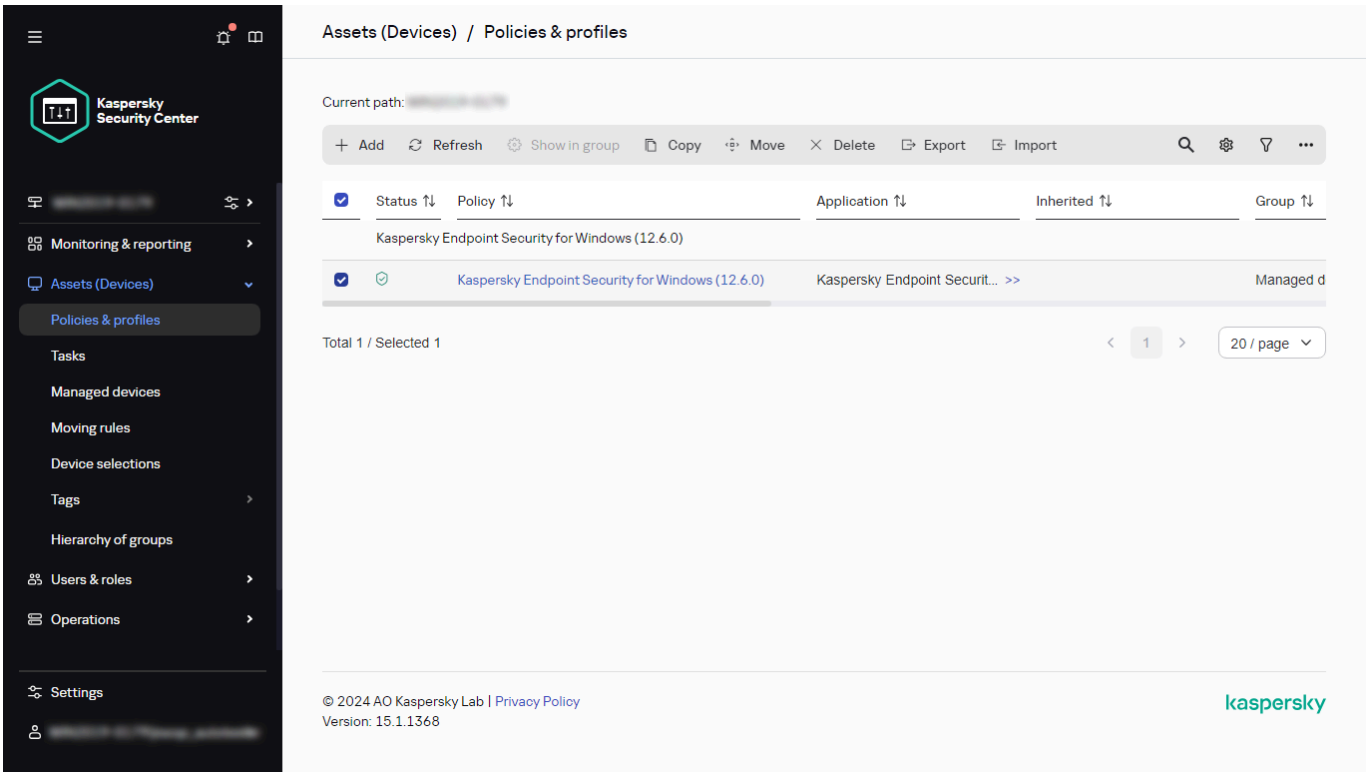
يتيح لك Kaspersky Security Center حفظ السياسة وإعداداتها وملفات تعريف السياسة في ملف KLP. يمكنك استخدام ملف KLP هذا لاستيراد السياسة المحفوظة إلى كل من Kaspersky Security Center Windows و Kaspersky Security Center Linux.

لتصدير سياسة:

1. في القائمة الرئيسية، انتقل إلى **Policies & profiles** ← **Assets (Devices)**.

2. حدد خانة الاختيار الموجودة بجوار السياسة التي ترغب في تصديرها.

يتعذر تصدير سياسات متعددة في نفس الوقت. إذا قمت بتحديد أكثر من سياسة فسيتم تعطيل زر **Export**.



3. انقر على الزر **Export**.

4. في النافذة **حفظ باسم** المفتوحة، حدد اسم ملف السياسة والمسار. انقر على زر **حفظ**.

يتم عرض نافذة **حفظ باسم** فقط إذا كنت تستخدم Google Chrome أو Microsoft Edge أو Opera. إذا كنت تستخدم متصفح آخر، فسيتم حفظ ملف المهمة تلقائيًا في مجلد **التنزيلات**.

استيراد سياسة

يتيح لك Kaspersky Security Center سياسة من ملف KLP. يحتوي ملف KLP على السياسة المصدرة وإعداداتها وملفات تعريف السياسة.

لاستيراد سياسة:

1. في القائمة الرئيسية، انتقل إلى **Policies & profiles** ← **Assets (Devices)**.

2. انقر على زر **Import**.

3. انقر على زر **Browse** لاختيار ملف السياسة الذي تريد استيرادها.

4. في النافذة المفتوحة، حدد المسار إلى ملف سياسة KLP، ثم انقر على زر **فتح**. لاحظ أنه يمكنك تحديد ملف سياسة واحد فقط.

تبدأ معالجة السياسة.

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

6. انقر على زر **Complete** لإنهاء استيراد السياسة.

يُظهر الإشعار نتائج الاستيراد. إذا تم استيراد السياسة بنجاح، يمكنك النقر على رابط **Details** لعرض السياسة.

بعد نجاح الاستيراد، يتم عرض السياسة في قائمة السياسات. يتم أيضًا استيراد إعدادات وملفات تعريف السياسة. بغض النظر عن حالة السياسة التي تم تحديدها أثناء التصدير، فإن السياسة المستوردة غير نشطة. يمكنك تغيير حالة السياسة في خصائص السياسة.

إذا كانت السياسة المستوردة حديثًا لها اسم مطابق لاسم سياسة موجودة، فسيتم توسيع اسم السياسة المستوردة بامتداد فهرس (**next sequence>**) **<number>** ، على سبيل المثال: **(1)** و **(2)**.

عرض مخطط حالة توزيع السياسة

يمكنك في Kaspersky Security Center أن تعرض حالة تطبيق السياسة على كل جهاز في مخطط حالة توزيع السياسة.

لعرض مخطط حالة توزيع السياسة على كل جهاز:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. حدد خانة الاختيار الموجودة بجوار اسم السياسة التي ترغب في عرض حالة توزيعها على الأجهزة.
3. حدد رابط **Distribution** في القائمة التي تظهر.
   ستفتح نافذة **نتائج توزيع <اسم السياسة>**.
4. في نافذة **نتائج توزيع <اسم السياسة>** التي تفتح، سيتم عرض **وصف الحالة** للسياسة.

يمكنك تغيير عدد النتائج المعروضة في قائمة توزيع السياسة. العدد الأقصى للأجهزة هو 100 000.

لتغيير عدد الأجهزة المعروضة في قائمة نتائج توزيع السياسة:

1. في القائمة الرئيسية، انتقل إلى إعدادات حسابك وحدد **Interface options**.
2. في **حد الأجهزة المعروضة في نتائج توزيع السياسة**، أدخل عدد الأجهزة (بحد أقصى 100 000).
   العدد الافتراضي هو 5000.
3. انقر على **Save**.
   يتم حفظ الإعدادات وتطبيقها.

حذف سياسة

يمكنك حذف سياسة إذا كنت لم تعد بحاجة إليها. لا يمكنك حذف سياسة إلا إذا لم تكن موروثة في مجموعة الإدارة المحددة. إذا كانت سياسة موروثة، لا يمكنك حذفها إلا في مجموعة المستوى الأعلى التي تم إنشاؤها لها.

لحذف سياسة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. حدد خانة الاختيار الموجودة بجوار السياسة التي ترغب في حذفها ثم انقر على **Delete**.
   يصبح زر **Delete** غير متوفر (أي باهتًا) إذا حدد سياسة موروثة.
3. انقر على **OK** لتأكيد العملية.

يتم خذف السياسة مع جميع ملفات تعريفها.

إدارة ملفات تعريف السياسة

يصف هذا القسم إدارة ملفات تعريف السياسة ويوفِّر معلومات عن عرض ملفات تعريف سياسة وتغيير أولوية ملف تعريف سياسة وإنشاء ملف تعريف سياسة وتعديل ملف تعريف سياسة ونسخ ملف تعريف سياسة وإنشاء قاعدة تفعيل ملف تعريف سياسة وحذف ملف تعريف سياسة.

عرض ملفات تعريف سياسة

لعرض ملفات سياسة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. انقر على اسم السياسة التي ترغب في عرض ملفات تعريفها.
   ستفتح نافذة خصائص السياسة مع تحديد تبويب **General**.
3. افتح تبويب **Policy profiles**.

تظهر قائمة ملفات تعريف السياسة في تنسيق جدولي. إذا لم يكن للسياسة ملفات تعريف، سيظهر جدول فارغ.

تغيير أولوية ملف تعريف سياسة

لتغيير أولوية ملف تعريف سياسة:

1. تقدم إلى قائمة ملفات تعريف السياسة التي تريدها.
   ستظهر قائمة ملفات تعريف السياسة.
2. في تبويب **Policy profiles**، حدد خانة الاختيار الموجودة بجوار ملف تعريف السياسة الذي ترغب في تغيير أولويته.
3. قم بتعيين موقع جديد لملف تعريف السياسة في القائمة بالنقر على **Prioritize** أو **Deprioritize**.
   كلما ارتفع موقع ملف تعريف السياسة في القائمة، ارتفعت أولويته.
4. انقر على زر **Save**.

يتم تغيير أولوية ملف تعريف السياسة المحدد وتطبيقه.

إنشاء ملف تعريف سياسة

لإنشاء ملف تعريف سياسة:

1. تابع إلى قائمة ملفات تعريف السياسة التي تريدها.
   ستظهر قائمة ملفات تعريف السياسة. إذا لم يكن للسياسة ملفات تعريف، سيظهر جدول فارغ.
2. انقر على **Add**.
3. يمكنك إذا كنت ترغب تغيير الاسم الافتراضي وإعدادات التوارث الافتراضية للسياسة.

4. حدد تبويب **Application settings**.

أو يمكنك النقر على **Save**والخروج. سيظهر الملف الذي أنشأته في قائمة ملفات تعريف السياسة، ويمكنك تحرير إعداداته لاحقًا.

5. في علامة التبويب **Application settings**، حدد في الجزء الأيمن الفئة التي تريدها، وفي الجزء الأيسر قم بتحرير إعدادات ملف التعريف. يمكنك تحرير إعدادات ملف تعريف السياسة في كل فئة (قسم).

عند تحرير الإعدادات، يمكنك النقر على **Cancel** لإلغاء العملية الأخيرة.

6. انقر على **Save** لحفظ ملف التعريف.

سيظهر ملف التعريف في قائمة ملفات تعريف السياسة.

تعديل ملف تعريف سياسة

تتوفر القدرة على تحرير ملف تعريف سياسة لسياسات Kaspersky Endpoint Security for Windows فقط.

لتعديل ملف تعريف سياسة

1. تقدم إلى قائمة ملفات تعريف السياسة التي تريدها.

ستظهر قائمة ملفات تعريف السياسة.

2. في تبويب **Policy profiles**، انقر على ملف تعريف السياسة الذي ترغب في تعديله.

يتم فتح نافذة خصائص ملف تعريف السياسة.

3. قم بتكوين ملف التعريف في نافذة الخصائص:

- إذا كان ذلك ضروريًا، من تبويب **General** قم بتغيير اسم ملف التعريف ثم قم بتمكين ملف التعريف أو تعطيله.
- قم بتحرير قواعد تفعيل ملف تعريف.
- قم بتحرير إعدادات التطبيق.

لمعرفة تفاصيل عن إعدادات تطبيقات الأمان، يُرجى الرجوع إلى وثائق التطبيق المقابل.

4. انقر على **Save**.

سوف يتم تطبيق الإعدادات التي قمت بتعديلها إما بعد مزامنة الجهاز مع خادم الإدارة (إذا كان ملف تعريف السياسة نشطًا)، أو بعد تشغيل قاعدة تفعيل (إذا كان ملف التعريف غير نشط).

إزالة ملف تعريف سياسة

يمكنك نسخ ملف تعريف سياسة إلى السياسة الحالية أو سياسة أخرى، كأن ترغب مثلاً في وجود ملفات تعريف متطابقة لسياسات مختلفة. يمكنك كذلك استخدام النسخ إذا كنت ترغب في امتلاك ملفي تعريف أو أكثر لا يختلفون إلا في عدد صغير من الإعدادات.

لنسخ ملف تعريف سياسة:

1. تقدم إلى قائمة ملفات تعريف السياسة التي تريدها.

ستظهر قائمة ملفات تعريف السياسة. إذا لم يكن للسياسة ملفات تعريف، سيظهر جدول فارغ.

2. في تبويب **Policy profiles**، حدد ملف تعريف السياسة الذي ترغب في نسخه.

3. انقر على **Copy** .

4. في النافذة التي تفتح، حدد السياسة التي ترغب في نسخ ملف التعريف إليها.

يمكنك نسخ ملف تعريف سياسة إلى السياسة نفسها أو إلى سياسة تحددها.

5. انقر على **Copy** .

يتم نسخ ملف تعريف السياسة إلى السياسة التي حددتها. يحصل ملف التعريف المنسوخ حديثًا على أقل أولوية. إذا نسخت ملف التعريف إلى السياسة نفسها، سيتم تمديد اسم ملف التعريف المنسوخ حديثًا بإضافة مؤشر (). على سبيل المثال: (1)، (2).

يمكنك لاحقًا تغيير إعدادات ملف التعريف، ويشمل ذلك اسمه وأولويته، لكن لن يتغير ملف تعريف السياسة الأصلي في هذه الحالة.

إنشاء قاعدة تفعيل ملف تعريف سياسة

لإنشاء قاعدة تفعيل ملف تعريف سياسة:

1. تقدم إلى قائمة ملفات تعريف السياسة التي تريدها.

ستظهر قائمة ملفات تعريف السياسة.

2. في تبويب **Policy profiles**، انقر على ملفات تعريف السياسة التي تحتاج إلى إنشاء قاعدة تفعيل لها.

إذا كانت قائمة ملفات تعريف السياسة فارغة، يمكنك إنشاء ملف تعريف سياسة.

3. حدد قسم **Activation rules**، وانقر على زر **Add**.

ستفتح نافذة بها قواعد تفعيل ملف تعريف السياسة.

4. حدد اسمًا للقاعدة.

5. حدد خانات الاختيار المجاورة للشروط التي يجب أن تؤثر على تفعيل ملف تعريف السياسة الذي تقوم بإنشائه:

- **General rules for policy profile activation**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناءً على حالة الوضع غير المتصل بالإنترنت للجهاز وقاعدة الاتصال بخادم الإدارة والعلامات المعينة للجهاز.

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

- **Device status**

يحدد شرط ظهور الجهاز على الشبكة:

- **Online**: الجهاز موجود على الشبكة، لذا يتوفر خادم الإدارة.
- **Offline**: الجهاز موجود على شبكة خارجية، وهذا يعني أن خادم الإدارة غير متاح.
- **N/A**: لن يتم تطبيق المعيار.

- **Rule for Administration Server connection is active on this device**

اختر شرط تفعيل ملف تعريف السياسة (سواء تم تنفيذ القاعدة أو لم يتم تنفيذها) وحدد اسم القاعدة.

تحدد القاعدة موقع الشبكة للجهاز للاتصال بخادم الإدارة، والذي يجب استيفاء شروطه (أو عدم استيفاء شروطه) لتفعيل ملف تعريف السياسة.

يمكن إنشاء وصف موقع شبكة الأجهزة للاتصال بخادم الإدارة أو تكوينه في قاعدة نقل عميل شبكة.

- **Rules for specific device owner**

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

- **Device owner**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف وتمكينها على الجهاز وفقًا لمالكه. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- الجهاز ينتمي للمالك المحدد (العلامة "=").
- الجهاز لا ينتمي للمالك المحدد (العلامة"#").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد مالك الجهاز عندما يتم تحديد هذا الخيار. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **Device owner is included in an internal security group**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة عضوية المالك في مجموعة أمان داخلية خاصة بـ Kaspersky Security Center. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- مالك الجهاز عضو في مجموعة الأمان الداخلية المحددة (الرمز "=").
- مالك الجهاز ليس عضوًا في مجموعة الأمان الداخلية المحددة (العلامة "#").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد مجموعة أمان من Kaspersky Security Center. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **Rules for hardware specifications**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناءً على حجم الذاكرة وعدد المعالجات المنطقية.

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

- **RAM size, in MB**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة حجم ذاكرة الوصول العشوائي على ذلك الجهاز. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- حجم ذاكرة الوصول العشوائي للجهاز أصغر من القيمة المحددة (علامة "<").
- حجم ذاكرة الوصول العشوائي للجهاز أكبر من القيمة المحددة (علامة ">").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد حجم ذاكرة الوصول العشوائي على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **Number of logical processors**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة عدد المعالجات المنطقية على ذلك الجهاز. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- عدد المعالجات المنطقية على الجهاز أقل من أو يساوي القيمة المحددة العلامة ("<").
- عدد المعالجات المنطقية على الجهاز أكبر من أو يساوي القيمة المحددة (العلامة ">").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد عدد المعالجات المنطقية على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **Rules for role assignment**

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

Activate policy profile by specific role of device owner

حدد هذا الخيار لتكوين وتمكين قاعدة تفعيل ملف التعريف على الجهاز بناءً على دور المالك. قم بإضافة الدور يدويًا من قائمة الأدوار الموجودة.

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه.

- **Rules for tag usage**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناءً على العلامات المعينة للجهاز. يمكنك تفعيل ملف تعريف السياسة للأجهزة التي تملك العلامات المحددة أو لا تملكها.

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

- **Tag**

في قائمة العلامات، حدد قاعدة لتضمين الجهاز في ملف تعريف السياسة عن طريق تحديد خانات الاختيار المقابلة للعلامات ذات الصلة.

يمكنك إضافة علامات جديدة إلى القائمة عن طريق إدخالها في الحقل الموجود أعلى القائمة والنقر فوق الزر **إضافة**.

يتضمن الملف التعريفي للسياسة أجهزة بها أوصاف تحتوي جميع العلامات المحددة. إذا تم إلغاء خانات الاختيار، لن يتم تطبيق المعيار. بشكل افتراضي، خانات الاختيار هذه غير محددة.

- **Apply to devices without the specified tags**

مكّن هذا الخيار إذا كان يتعين عليك عكس تحديد علاماتك.

في حال تمكين هذا الخيار، سيتضمن ملف تعريف السياسة أجهزة بها أوصاف لا تحتوي على أي من العلامات المحددة. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار.

يتم تعطيل هذا الخيار افتراضيًا.

- **Rules for Active Directory usage**

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناء على وجود الجهاز في الوحدة التنظيمية لـ Active Directory، أو عضوية الجهاز (أو عضوية مالكه) في مجموعة أمن Active Directory.

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

- **Device owner's membership in an Active Directory security group**

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز الذي يكون مالكه عضوًا في مجموعة الأمان المحددة. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **Device membership in Active Directory security group**

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف تعريف السياسة على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **Device allocation in Active Directory organizational unit**

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف تعريف السياسة على الجهاز المدمج في الوحدة التنظيمية المحددة لـ Active Directory. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف.

يتم تعطيل هذا الخيار افتراضيًا.

يعتمد عدد الصفحات الإضافية للمعالج على الإعدادات التي تحددها في الخطوة الأولى. يمكنك تعديل قواعد تفعيل ملف تعريف السياسة في وقت لاحق.

6. تحقق من قائمة المعلمات التي تم تكوينها. إذا كانت القائمة صحيحة، انقر على **Create**.

سيتم حفظ ملف التعريف. سيتم تفعيل ملف التعريف على الجهاز عند تشغيل قواعد التنشيط.

يتم عرض قواعد تفعيل ملف تعريف السياسة التي تم إنشاؤها لملف تعريف السياسة في خصائص ملف تعريف السياسة في تبويب **Activation rules**. يمكنك تعديل أي من قواعد تفعيل ملف تعريف السياسة أو إزالتها.

يمكن تشغيل العديد من قواعد التفعيل في آن واحد.

إزالة ملف تعريف سياسة

لحذف ملف تعريف سياسة:

1. تقدم إلى قائمة ملفات تعريف السياسة التي تريدها.

   ستظهر قائمة ملفات تعريف السياسة.

2. في تبويب **Policy profiles**، حدد خانة الاختيار الموجودة بجوار ملف تعريف السياسة الذي ترغب في حذفه ثم انقر على **Delete**.

3. في النافذة التي تفتح، انقر على **Delete** مرة أخرى.

يتم حذف ملف تعريف السياسة. إذا ورث السياسة مجموعة مستوى أقل، يبقى ملف التعريف في تلك المجموعة لكنه يصبح الملف الشخصي لسياسة تلك المجموعة. يتم هذا للتخلص من التغيير الكبير في إعدادات التطبيقات المُدارة المثبتة على الأجهزة في مجموعات المستوى الأدنى.

تشفير البيانات وحمايتها

تشفير البيانات يقلل من مخاطر تسرب البيانات غير المقصود في حالة سرقة الحاسوب المحمول أو محرك الأقراص الثابتة، أو في حالة فقدانه أو الوصول غير المصرح به من قِبل مستخدمين وتطبيقات.

تطبيقات Kaspersky التالية تدعم تشفير:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

يمكنك عرض بعض عناصر الواجهة المتعلقة بميزة إدارة التشفير أو إخفائها باستخدام إعدادات واجهة المستخدم.

لا نوصي بتمكين التشفير في البنية التحتية لسطح المكتب الافتراضي (VDI).

تشفير البيانات في Kaspersky Endpoint Security for Windows

يمكنك إدارة أنواع التشفير التالية:

- تشفير محرك BitLocker على الأجهزة التي تعمل بنظام تشغيل Windows للخوادم
- تشفير قرص Kaspersky على الأجهزة التي تعمل بنظام التشغيل Windows لمحطة العمل

باستخدام هذه المكونات من Kaspersky Endpoint Security for Windows، يمكنك، على سبيل المثال، تمكين أو تعطيل التشفير، أو عرض قائمة محركات الأقراص المشفرة، أو إنشاء وعرض تقارير حول التشفير.

يمكنك تكوين التشفير عن طريق تحديد سياسة Kaspersky Endpoint Security for Windows في Kaspersky Security Center. يجري Kaspersky Endpoint Security for Windows التشفير وفك التشفير وفق السياسة المفعلة. للحصول على إرشادات مفصلة حول كيفية تكوين القواعد ووصف لمزايا التشفير، يرجى الرجوع إلى التعليمات من Kaspersky Endpoint Security for Windows.

تشفير البيانات في Kaspersky Endpoint Security for Mac

يمكنك استخدام تشفير FileVault على الأجهزة التي تعمل بنظام macOS. أثناء العمل على Kaspersky Endpoint Security for Mac، يمكنك تفعيل هذا التشفير أو تعطيله.

يمكنك تكوين التشفير عن طريق تحديد سياسات Kaspersky Endpoint Security for Mac في Kaspersky Security Center Cloud Console. يجري Kaspersky Endpoint Security for Mac التشفير وفك التشفير وفق السياسة المفعلة. للحصول على وصف تفصيلي حول مزايا التشفير، يرجى الرجوع إلى التعليمات من Kaspersky Endpoint Security for Mac.

عرض قائمة ببرامج التشغيل المشفرة

في Kaspersky Security Center، يمكنك عرض تفاصيل حول محركات الأقراص والأجهزة المشفرة التي تم تشفيرها على مستوى محرك الأقراص. بعد فك تشفير المعلومات على محرك أقراص، يتم إزالة محرك الأقراص تلقائيًا من القائمة.

لعرض قائمة ببرامج التشغيل المشفرة،

في القائمة الرئيسية ، انتقل إلى **Operations** ← **Data encryption and protection** ← **Encrypted drives**.

إذا لم يكن القسم موجودًا في القائمة، فهذا يعني أنه مخفي. في إعدادات واجهة المستخدم، قم بتمكين خيار **Show data encryption and protection** لعرض القسم.

تصدير قائمة برامج التشغيل المشفرة إلى CSV أو ملف TXT. للقيام بذلك، انقر على **Export to CSV** أو زر **Export to TXT**.

عرض قائمة بأحداث التشفير

عند تشغيل مهام تشفير البيانات أو فك تشفيرها على الأجهزة، يرسل Kaspersky Endpoint Security for Windows معلومات حول أحداث الأنواع التالية إلى Kaspersky Security Center:

- يتعذر تشفير ملف أو فك تشفيره، أو إنشاء أرشيف مشفر نظرًا لفقدان مساحة فارغة على القرص.
- يتعذر تشفير ملف أو فك تشفيره، أو إنشاء أرشيف مشفر نظرًا لمشكلات الترخيص.
- يتعذر تشفير ملف أو فك تشفيره، أو إنشاء أرشيف مشفر نظرًا لفقدان حقوق الوصول.
- تم منع التطبيق من الوصول إلى ملف مشفر.
- أخطاء غير معروفة.

لعرض قائمة بالأحداث التي وقعت أثناء تشفير البيانات على الأجهزة،

في القائمة الرئيسية ، انتقل إلى **Operations** ← **Data encryption and protection** ← **Encryption events**.

إذا لم يكن القسم موجودًا في القائمة، فهذا يعني أنه مخفي. في إعدادات واجهة المستخدم، قم بتمكين خيار **Show data encryption and protection** لعرض القسم.

تصدير قائمة برامج التشغيل المشفرة إلى CSV أو ملف TXT. للقيام بذلك، انقر على **Export to CSV** أو زر **Export to TXT**.

بدلاً من ذلك، يمكنك فحص قائمة أحداث التشفير لكل جهاز مُدار.

لعرض أحداث التشفير لجهاز مُدار:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.
2. انقر فوق اسم الجهاز المُدار.
3. في علامة تبويب **General**، انتقل إلى جزء **Protection**.
4. انقر على رابط **View data encryption errors**.

إنشاء تقارير التشفير وعرضها

يمكنك إنشاء التقارير التالية:

- Report on encryption status of managed devices. يقدم هذا التقرير تفاصيل حول تشفير البيانات لمختلف الأجهزة المدارة. على سبيل المثال، يعرض التقرير عدد الأجهزة التي تنطبق عليها السياسة مع قواعد التشفير المكونة. يمكنك أيضًا معرفة، على سبيل المثال، عدد الأجهزة التي تحتاج إلى إعادة التشغيل. يحتوي التقرير أيضًا على معلومات حول تقنية التشفير وخوارزمية كل جهاز.
- Report on encryption status of mass storage devices. يحتوي هذا التقرير على معلومات مماثلة للتقرير عن حالة تشفير الأجهزة المُدارة، ولكنه يوفر البيانات فقط لأجهزة التخزين كبير السعة ومحركات الأقراص القابلة للإزالة.
- Report on rights to access encrypted drives. يوضح هذا التقرير حسابات المستخدمين التي لها حق الوصول إلى محركات الأقراص المشفرة.
- Report on file encryption errors. يحتوي هذا التقرير على معلومات حول الأخطاء التي حدثت عند تشغيل مهام تشفير البيانات أو فك تشفيرها على الأجهزة.
- Report on blockage of access to encrypted files. يحتوي هذا التقرير على معلومات حول منع وصول التطبيق إلى الملفات المشفرة. هذا التقرير مفيد إذا حاول مستخدم أو تطبيق غير مصرح له الوصول إلى الملفات أو محركات الأقراص المشفرة.

يمكنك إنشاء أي تقرير في **Monitoring & reporting** ← **Reports**. بدلا من ذلك، في قسم **Operations** ← **Data encryption and protection** يمكنك إنشاء تقارير التشفير التالية:

- Report on encryption status of mass storage devices
- Report on rights to access encrypted drives
- Report on file encryption errors

لإنشاء تقرير تشفير في قسم **Data encryption and protection**:

1. تأكد أنك قمت بتفعيل خيار **Show data encryption and protection** في خيارات الواجهة.
2. في خصائص السياسة، افتح علامة التبويب **Event configuration**.
3. في القسم **حرج**، انقر فوق **Add event** وحدد مربع الاختيار بجوار الحدث خطأ في تطبيق قواعد تشفير / فك تشفير الملفات.
4. انقر على**OK**.
5. في القائمة الرئيسية ، انتقل إلى **Operations** ← **Data encryption and protection**.

6. افتح أحد الأقسام التالية:

- يُنشئ **Encrypted drives** تقريرًا عن حالة تشفير أجهزة التخزين كبير السعة أو تقرير حول حقوق الوصول إلى محركات الأقراص المشفرة.
- تنشئ **Encryption events** تقريرًا عن أخطاء تشفير الملف.

7. انقر على اسم التقرير الذي ترغب في إنشائه.

يبدأ إنشاء التقرير.

منح حق الوصول إلى محرك أقراص مشفر في وضع عدم الاتصال

يمكن لمستخدم طلب الوصول إلى جهاز مشفر، مثلاً عندما لا يكون Kaspersky Endpoint Security for Windows مثبتًا على الجهاز المُدار. بعد أن تستقبل الطلب، يمكنك إنشاء ملف مفتاح وصول وإرساله إلى المستخدم. جميع حالات الاستخدام والإرشادات المفصلة متوفرة في Kaspersky Endpoint Security for Windows.

لمنح حق الوصول إلى محرك أقراص مشفر في وضع عدم الاتصال:

1. احصل على ملف طلب وصول من مستخدم (ملف بامتداد FDERTC). اتبع التعليمات الواردة في تعليمات Kaspersky Endpoint Security for Windows لإنشاء الملف في Kaspersky Endpoint Security for Windows.

2. في القائمة الرئيسية ، انتقل إلى **Encrypted drives** ← **Data encryption and protection** ← **Operations**.

   ستظهر قائمة ببرامج التشغيل المشفرة.

3. حدد محرك الأقراص الذي طلب المستخدم الوصول إليه.

4. انقر على زر **Grant access to the device in offline mode**.

5. في النافذة التي تفتح، حدد المكون الإضافي المقابل لتطبيق Kaspersky المستخدم في تشفير محرك الأقراص المحدد.

> في حال تشفير محرك أقراص بتطبيق Kaspersky ليس مدعومًا من Kaspersky Security Center Web Console، استخدم وحدة تحكم إدارة مستندة على Microsoft Management Console من أجل منح الوصول دون اتصال.

6. اتبع التعليمات الواردة في تعليمات Kaspersky Endpoint Security for Windows (انظر توسيع الكتل في نهاية القسم).

بعد ذلك، يطبق المستخدم استخدام الملف المستلم في الوصول إلى محرك الأقراص المشفر وقراءة البيانات المخزنة على محرك الأقراص.

المستخدمين وأدوار المستخدمين

يصف هذا القسم المستخدمين وأدوار المستخدمين، كما يوفر تعليمات لإنشائها وتعديلها ولتخصيص أدوار ومجموعات للمستخدمين ولربط ملفات تعريف السياسة بأدوار.

حول أدوار المستخدم

دور المستخدم (المشار إليه كذلك باسم الدور) هو كائن يحتوي على مجموعة حقوق ومزايا. يمكن ربط دور بإعدادات تطبيقات Kaspersky المثبتة على جهاز مستخدم. يمكنك تعيين دور لمجموعة من المستخدمين أو إلى مجموعة من مجموعات الأمان في أي مستوى في التسلسل الهرمي لمجموعات الإدارة أو خوادم الإدارة ، أو على مستوى كائنات محددة.

إذا كنت تدير الأجهزة من خلال تسلسل هرمي لخوادم الإدارة التي تتضمن خوادم الإدارة الافتراضية، فلاحظ أنه لا يمكنك إنشاء أدوار مستخدم أو تعديلها أو حذفها إلا من خادم إدارة فعلي. إذا تستطيع نشر أدوار المستخدم إلى خوادم الإدارة الثانوية، بما في ذلك الافتراضية.

يمكنك ربط أدوار المستخدم بملفات تعريف السياسة. في حالة تخصيص دور لمستخدم، فسيحصل هذا المستخدم على إعدادات الأمان الضرورية لتأدية المهام الوظيفية.

يمكن ربط دور المستخدم بمستخدمي الأجهزة في مجموعة إدارة محددة.

نطاقات دور المستخدم

نطاق دور المستخدم هو مجموعة من المستخدمين ومجموعات الإدارة. لا تنطبق الإعدادات المرتبطة بدور مستخدم إلا على الأجهزة التي تنتمي إلى المستخدمين الذين يملكون هذا الدور، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

فائدة استخدام الأدوار

فائدة استخدام الأدوار هي أنك لن تضطر إلى تحديد إعدادات الأمان لكل جهاز من الأجهزة المُدارة أو لكل مستخدم من المستخدمين على حدة. عدد المستخدمين والأجهزة في الشركة قد يكون كبيرًا، لكن عدد المهام الوظيفية المختلفة التي تتطلب إعدادات أمان مختلفة أقل بدرجة كبيرة.

الاختلافات عن استخدام ملفات تعريف السياسة

ملفات تعريف السياسة من خصائص السياسة التي تم إنشاؤها لكل تطبيق من تطبيقات Kaspersky على حدة. يرتبط الدور بالعديد من ملفات تعريف السياسة التي تم إنشاؤها لتطبيقات مختلفة. وبالتالي الدور هو وسيلة لتوحيد الإعدادات لكل نوع مستخدم معين في مكان واحد.

عرض حسابات المستخدمين والجلسات

يتيح Kaspersky Security Center إدارة حسابات المستخدمين ومجموعات الحسابات. يدعم التطبيق نوعين من الحسابات:

- حسابات موظفي المؤسسة. يقوم خادم الإدارة باسترداد بيانات حسابات هؤلاء المستخدمون عند استقصاء شبكة المؤسسة.
- حسابات المستخدمين الداخليين. يتم تطبيق تلك الحسابات عند استخدام خوادم إدارة افتراضية. يتم إنشاء واستخدام حسابات المستخدمين الداخليين فقط ضمن Kaspersky Security Center.

يمكنك عرض قائمة حسابات المستخدمين وجلساتهم بإحدى الطرق التالية:

- في القائمة الرئيسية، انتقل إلى **Users & groups** ← **Users & roles**.
- في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)** ← رابط <device name> ← علامة التبويب **General** ← القسم **General** ← القسم **Sessions**.

  يعرض القسم **Sessions** حسابات المستخدمين ذات الجلسات النشطة على الأجهزة التي تعمل بنظام Windows.

يتم عرض قائمة حسابات المستخدمين والجلسات بشكل صحيح إذا تم استيفاء المتطلبات التالية:

- استخدم عميل الشبكة من إصدار خادم الإدارة نفسه أو إصدار أحدث.
- يتم تمكين استقصاء Active Directory لعرض حسابات مستخدمي المجال.
- على الأجهزة المدارة التي تعمل بنظام Windows، تعمل خدمة **الخادم** (**LanmanServer**).

تكوين حقوق الوصول إلى ميزات التطبيق. التحكم في الوصول على أساس الدور

يوفر Kaspersky Security Center تسهيلات للوصول إلى ميزات Kaspersky Security Center أو تطبيقات Kaspersky المُدارة.

يمكنك تكوين حقوق الوصول إلى ميزات التطبيق لمستخدمي Kaspersky Security Center بإحدى الطرق التالية:

- عن طريق تكوين الحقوق لكل مستخدم أو مجموعة من المستخدمين بشكل فردي.
- عن طريق إنشاء أدوار المستخدم القياسية مع مجموعة محددة مسبقًا من الحقوق وتعيين هذه الأدوار للمستخدمين اعتمادًا على مدى نطاق واجباتهم.

يهدف تطبيق أدوار المستخدم إلى تبسيط وتقصير الإجراءات الروتينية لتكوين حقوق وصول المستخدمين إلى ميزات التطبيق. يتم تكوين حقوق الوصول ضمن دور ما وفقًا للمهام القياسية ونطاق واجبات المستخدمين.

يمكن تعيين أسماء لأدوار المستخدمين وفقًا لأغراض كل منها. يمكنك إنشاء عدد غير محدود من الأدوار في التطبيق.

يمكنك استخدام أدوار المستخدم المحددة مسبقًا مع مجموعة الحقوق المكونة بالفعل، أو إنشاء أدوار جديدةوتكوين الحقوق المطلوبة بنفسك.

حقوق الوصول إلى ميزات التطبيق

يوضح الجدول أدناه ميزات Kaspersky Security Center مع حقوق الوصول لإدارة المهام والتقارير والإعدادات المرتبطة بها وتنفيذ إجراءات المستخدم المرتبطة.

لتنفيذ إجراءات المستخدم المدرجة في الجدول، يجب أن يكون لدى المستخدم الحق المحدد بجوار الإجراء.

تنطبق حقوق **Read** و**Write** وExecute على أي مهمة أو تقرير أو إعداد. بالإضافة إلى هذه الحقوق، يجب أن يكون لدى المستخدم حق **Perform operations on device selections** لإدارة المهام أو التقارير أو الإعدادات في تحديدات الجهاز.

تنتمي جميع المهام والتقارير والإعدادات وحزم التثبيت المفقودة في الجدول إلى المنطقة الوظيفية **General features: Basic functionality**.

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
General features: Management of administration groups	Write	• إضافة جهاز إلى مجموعة الإدارة: Write • حذف الجهاز من مجموعة الإدارة: Write • أضف مجموعة إدارة إلى مجموعة إدارة أخرى: Write • حذف مجموعة إدارة من مجموعة إدارة أخرى: Write	لا شيء	لا شيء	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
General features: Access objects regardless of their ACLs	**Read**	الحصول على وصول Read لجميع الكائنات: **Read**	لا شيء	لا شيء	تم تصميم المنطقة الوظيفية **General features: Access objects regardless of their ACLs** لأغراض التدقيق. وعندما يتم منح المستخدمين حقوق **Read** في هذه المنطقة الوظيفية، فإنهم يحصلون على الوصول الكامل إلى حق **Read** إلى جميع الكائنات ويستطيعون تنفيذ أي مهام تم إنشاؤها في مجموعات مختارة من الأجهزة المتصلة بخادم الإدارة عبر عميل الشبكة مع حقوق المسؤول المحلي (الجذر لنظام التشغيل Linux). ونوصي بمنح هذه الحقوق بعناية لمجموعة محدودة من المستخدمين الذين يحتاجون إليها لأداء واجباتهم الرسمية. يتم منح الوصول بغض النظر عن الحقوق الأخرى، حتى لو كانت تمنع الوصول إلى حق Read إلى كائنات معينة.
General features: Basic functionality	• **Read** • **Write** • **Execute** • **Perform operations on device selections**	• قواعد نقل الجهاز (إنشاء أو تعديل أو حذف) للخادم الافتراضي: **Write, Perform operations on device selections** • احصل على شهادة مخصصة لبروتوكول Mobile (LWNGT): **Read** • تعيين شهادة بروتوكول Mobile (LWNGT) المخصصة: **Write** • احصل على قائمة الشبكة المعرفة من قبل NLA: **Read** • إضافة أو تعديل أو حذف قائمة الشبكة المعرفة من قبل NLA: **Write** • اعرض قائمة مجموعات التحكم في الوصول: **Read** • اعرض سجل أحداث Kaspersky: **Read** • اعرض مفتاح الاسترداد لاستعادة الوصول إلى قرص ثابت تم تشفيره بواسطة BitLocker: **Execute**	• "تنزيل التحديثات إلى مستودع خادم الإدارة" • "تسليم التقارير" • "توزيع حزم التثبيت" • "تثبيت التطبيق عن بُعد على خوادم الإدارة الثانوية"	• "تقرير حالة الحماية" • "تقرير التهديدات" • "تقرير حول الأجهزة الأكثر إصابة" • "تقرير حول حالة قواعد بيانات مكافحة الفيروسات" • "تقرير الأخطاء" • "الإبلاغ عن هجمات الشبكة" • "تقرير موجز عن تطبيقات حماية نظام البريد المثبتة" • "تقرير موجز عن تطبيقات الدفاع المحيطي المثبتة" • "تقرير موجز عن التطبيقات المثبتة" • "تقرير حول مستخدمي الأجهزة المصابة" • "تقرير حول الحوادث" • "تقرير حول الأحداث" • "تقرير حول نشاط نقاط التوزيع" • "تقرير حول خوادم الإدارة الثانوية" • "تقرير حول أحداث التحكم في الجهاز" • "تقرير الثغرات الأمنية" • "تقرير حول التطبيقات المحظورة" • "تقرير حول التحكم في الويب" • "تقرير حول حالة تشفير الأجهزة المُدارة" • "تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة" • "تقرير حول أخطاء تشفير الملف"	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
				• "تقرير حول حجب الوصول إلى الملفات المشفرة" • "تقرير حول حقوق الوصول إلى الأجهزة المشفرة" • "تقرير حول أذونات المستخدم الفعالة" • "تقرير حول الحقوق"	
General features: Deleted objects	• Read • Write	• اعرض الكائنات المحذوفة في سلة المحذوفات: **Read** • حذف كائنات من سلة المحذوفات: **Write**	لا شيء	لا شيء	لا شيء
General features: Event processing	• Delete events • Edit event notification settings • Edit event logging settings • Write	• تغيير إعدادات تسجيل الأحداث: **Edit event logging settings** • تغيير إعدادات إشعار الأحداث: **Edit event notification settings** • حذف الأحداث: **Delete events**	لا شيء	لا شيء	الإعدادات: • إعدادات تفشي الفيروسات: عدد عمليات كشف الفيروسات المطلوبة لإنشاء حدث اندلاع فيروسات • إعدادات تفشي الفيروسات: فترة زمنية لتقييم عمليات كشف الفيروسات • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة البيانات • فترة زمنية لتخزين الأحداث من الأجهزة المحذوفة
General features: Operations on Administration Server	• Read • Write • Execute • Modify object ACLs • Perform operations on device selections	• حدد منافذ خادم الإدارة لاتصال عميل الشبكة: **Write** • حدد منافذ وكيل التنشيط الذي تم تشغيله على خادم الإدارة: **Write** • حدد منافذ وكيل التفعيل للجوال التي تم تشغيلها على خادم الإدارة: **Write** • حدد منافذ خادم الويب لتوزيع الحزم المستقلة: **Write** • حدد منافذ خادم الويب لتوزيع ملفات تعريف MDM: **Write** • حدد منافذ SSL لخادم الإدارة للاتصال عبر Kaspersky Security Center Web Console: **Write** • حدد منافذ خادم الإدارة لاتصال الهاتف المحمول: **Write** • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة: **Write** • حدد الحد الأقصى لعدد الأحداث التي يمكن أن يرسلها خادم الإدارة: **Write** • حدد الفترة الزمنية التي يمكن خلالها إرسال الأحداث بواسطة خادم الإدارة: **Write**	• "النسخ الاحتياطي لبيانات خادم الإدارة" • "صيانة قاعدة البيانات"	لا شيء	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
General features: Kaspersky application deployment	• Manage Kaspersky patches • Read • Write • Execute • Perform operations on device selections	اقبل تثبيت التصحيح أو ارفضه: **Manage Kaspersky patches**	لا شيء	• "تقرير حول استخدام مفتاح الترخيص بواسطة خادم الإدارة الافتراضي" • "تقرير حول إصدارات برامج Kaspersky" • "تقرير التطبيقات غير المتوافقة" • "تقرير حول إصدارات تحديثات وحدة برامج Kaspersky" • "تقرير نشر الحماية"	حزمة التثبيت: "Kaspersky"
General features: License key management	• Export key file • Write	• تصدير ملف مفتاح: **Export key file** • تعديل إعدادات مفتاح ترخيص خادم الإدارة: **Write**	لا شيء	لا شيء	لا شيء
General features: Enforced report management	• Read • Write	• إنشاء التقارير بغض النظر عن قوائم ACL الخاصة بهم: **Write** • تنفيذ التقارير بغض النظر عن قوائم ACL الخاصة بهم: **Read**	لا شيء	لا شيء	لا شيء
General features: Hierarchy of Administration Servers	Configure hierarchy of Administration Servers	تسجيل خوادم الإدارة الثانوية أو تحديثها أو حذفها: **Configure hierarchy of Administration Servers**	لا شيء	لا شيء	لا شيء
General features: User permissions	Modify object ACLs	• تغيير خصائص "الأمان" لأي كائن: **Modify object ACLs** • إدارة أدوار المستخدم: **Modify object ACLs** • إدارة المستخدمين الداخليين: **Modify object ACLs** • إدارة مجموعات الأمان: **Modify object ACLs** • إدارة الأسماء المستعارة: **Modify object ACLs**	لا شيء	لا شيء	لا شيء
General features: Virtual Administration Servers	• Manage virtual Administration Servers • Read • Write • Execute • Perform operations on device selections	• الحصول على قائمة خوادم الإدارة الافتراضية: **Read** • الحصول على معلومات حول خادم الإدارة الافتراضي: **Read** • إنشاء خادم إدارة افتراضي أو تحديثه أو حذفه: **Manage virtual Administration Servers** • نقل خادم الإدارة الافتراضي إلى مجموعة أخرى: **Manage virtual Administration Servers** • تعيين أذونات خادم الإدارة الافتراضي: **Manage virtual Administration Servers**	لا شيء	"تقرير حول نتائج تثبيت تحديثات برامج الجهات الخارجية"	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
General features: Encryption Key Management	Write	استيراد مفاتيح التشفير: **Write**	لا شيء	لا شيء	لا شيء
Mobile Device Management: General	• Connect new devices • Send only information commands to mobile devices • Send commands to mobile devices • Manage certificates • Read • Write	• الحصول على بيانات استعادة خدمة إدارة المفاتيح: **Read** • حذف شهادات المستخدم: **Manage certificates** • الحصول على الجزء العام لشهادة المستخدم: **Read** • تحقق مما إذا تم تمكين البنية الأساسية للمفتاح العام: **Read** • تحقق من حساب البنية التحتية للمفتاح العام: **Read** • احصل على قوالب البنية التحتية للمفتاح العام: **Read** • احصل على قوالب البنية التحتية للمفتاح العام عن طريق شهادة استخدام المفتاح الموسع: **Read** • تحقق مما إذا تم إبطال شهادة البنية التحتية للمفتاح العام: **Read** • تحديث إعدادات إصدار شهادة المستخدم: **Manage certificates** • الحصول على إعدادات إصدار شهادة المستخدم: **Read** • احصل على الحزم حسب اسم المنتج والإصدار: **Read** • تعيين أو إلغاء شهادة المستخدم: **Manage certificates** • تجديد شهادة المستخدم: **Manage certificates** • تعيين علامة شهادة المستخدم: **Manage certificates** • تشغيل إنشاء حزمة تثبيت MDM؛ إلغاء إنشاء حزمة تثبيت MDM: **Connect new devices**	لا شيء	لا شيء	لا شيء
System management: Connectivity	• Start RDP sessions • Connect to existing RDP sessions • Initiate tunneling • Save files from devices to the administrator's workstation • Read • Write • Execute • Perform operations on device selections	• إنشاء جلسة مشاركة سطح المكتب: **Start RDP sessions** • إنشاء جلسة RDP: **Connect to existing RDP sessions** • إنشاء نفق: **Initiate tunneling** • حفظ قائمة شبكة المحتوى: **Save files from devices to the administrator's workstation**	لا شيء	"تقرير حول مستخدمي الأجهزة"	لا شيء
System management: Hardware inventory	• Read • Write	• الحصول على كائن مخزون الأجهزة أو تصديره: **Read** • إضافة جرد الأجهزة أو	لا شيء	• "تقرير حول سجل الأجهزة" • "تقرير حول تغييرات التكوين"	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
	• Execute • Perform operations on device selections	تعيينه أو حذفه: **Write**		• "تقرير حول الأجهزة"	
System management: Network Access Control	• Read • Write	• عرض إعدادات CISCO: **Read** • تغيير إعدادات CISCO: **Write**	لا شيء	لا شيء	لا شيء
System management: Operating system deployment	• Deploy PXE servers • Read • Write • Execute • Perform operations on device selections	• نشر خادم PXE: **Deploy PXE servers** • عرض قائمة بخوادم PXE: **Read** • بدأ عملية التثبيت على عملاء PXE أو أوقفها: **Execute** • إدارة برامج التشغيل لـ WinPE وصور نظام التشغيل: **Write**	"إنشاء حزمة التثبيت على مرجع صورة نظام التشغيل للجهاز"	لا شيء	حزمة التثبيت: "صورة نظام التشغيل"
System management: Vulnerability and patch management	• Read • Write • Execute • Perform operations on device selections	• عرض خصائص تصحيح الطرف الثالث: **Read** • تغيير خصائص تصحيح الطرف الثالث: **Write**	• "مزامنة Windows Update" • "تثبيت تحديثات Windows Update" • "إصلاح الثغرات الأمنية" • "قم بتثبيت التحديثات المطلوبة وضبط إعدادات مهمة إصلاح الثغرات الأمنية"	"تقرير تحديثات البرامج"	لا شيء
System management: Remote installation	• Read • Write • Execute • Perform operations on device selections	• عرض خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: **Read** • تغيير خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: **Write**	لا شيء	لا شيء	حزم التثبيت: • "تطبيق مخصص " • "حزمة VAPM"
System management: Software inventory	• Read • Write • Execute • Perform operations on device selections	لا شيء	لا شيء	• "تقرير حول التطبيقات المثبتة" • "تاريخ تقرير سجل التطبيقات" • "تقرير حول حالة مجموعات التطبيقات المرخصة" • "تقرير حول مفاتيح ترخيص برامج الجهات الخارجية"	لا شيء
System management: Execute scripts remotely	• Read • Write • Execute • Perform operations on device selections	يستطيع المستخدم عرض خصائص المهمة: **Read** يستطيع المستخدم إنشاء حزمة تثبيت أو حذفها أو تعديلها: **Write** يمكن للمستخدم تشغيل مهمة: **Write**. يتم تنفيذ البرامج النصية على أجهزة Linux العميلة بامتيازات الجذر.	"تنفيذ البرامج النصية عن بعد"	لا شيء	لا شيء

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
		يمكن للمستخدم تشغيل مهمة أو جدولتها للتشغيل: **Execute** يستطيع المستخدم تشغيل مهمة على مجموعة مختارة من الأجهزة: **Perform operations on device selections**			

أدوار المستخدم المحددة مسبقًا

توفر أدوار المستخدم المعينة لمستخدمي Kaspersky Security Center مجموعات من حقوق الوصول إلى ميزات التطبيق.

> لا يمكن تعيين دور للمستخدمين الذين تم إنشاؤهم على خادم افتراضي على خادم الإدارة.

يمكنك استخدام أدوار المستخدم المحددة مسبقًا المصحوبة بمجموعة من الحقوق المكونة بالفعل، أو إنشاء أدوار جديدة. عند إنشاء دور جديد، يجب عليك تعيين نطاق الدور وتعيين حقوق الوصول إلى ميزات Kaspersky Security Center بنفسك. يمكن ربط بعض أدوار المستخدم المحددة مسبقًا والمتوفرة في Kaspersky Security Center بمناصب وظيفية محددة، على سبيل المثال، **المدقق**، **مسؤول الأمن**، **المشرف** (هذه الأدوار موجودة في Kaspersky Security Center بدءًا من الإصدار 11). تم تكوين حقوق الوصول لهذه الأدوار مسبقًا وفقًا للمهام القياسية ونطاق واجبات الوظائف المرتبطة. يوضح الجدول أدناه كيف يمكن ربط الأدوار يمكن ربط الأدوار بمناصب وظيفية محددة.

أمثلة على أدوار المناصب الوظيفية المحددة

الدور	التعليق
مدقق الحسابات	للسماح بجميع عمليات العرض وتنفيذ أي مهام تم إنشاؤها على مجموعة مختارة من الأجهزة المتصلة بخادم الإدارة عبر وكيل الشبكة مع حقوق المسؤول المحلي (الجذر لنظام Linux). ونوصي بتعيين هذا الدور بعناية لمجموعة محدودة من المستخدمين الذين يحتاجون إليه لأداء واجباتهم الرسمية.
المشرف	يسمح بتنفيذ جميع عمليات العرض، لا يسمح بتنفيذ عمليات أخرى. يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمان تكنولوجيا المعلومات في مؤسستك.
مسؤول الأمن	يسمح بتنفيذ جميع عمليات العرض ويسمح بإدارة التقارير ويمنح أذونات محدودة في **إدارة النظام**: نطاق **الاتصال**. يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمان تكنولوجيا المعلومات في مؤسستك.

يوضح الجدول أدناه حقوق الوصول المعينة لكل دور مستخدم محدد مسبقًا.

حقوق الوصول لأدوار المستخدم المحددة مسبقًا

الدور	الوصف
مسؤول خادم الإدارة	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **معالجة الحدث** • **التسلسل الهرمي لخوادم الإدارة** • **خوادم الإدارة الافتراضية** • **إدارة النظام**: • **الاتصال** • **مخزون الأجهزة** • **مخزون البرنامج** تمنح حقوق **قراءة وكتابة** في منطقة الوظائف **الميزات العامة: إدارة مفتاح التشفير**.

الدور	الوصف
مشغّل خادم الإدارة	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **خوادم الإدارة الافتراضية** • **إدارة النظام**: • **الاتصال** • **مخزون الأجهزة** • **مخزون البرنامج**
مدقق الحسابات	للسماح بجميع العمليات في المجالات الوظيفية ، في **الميزات العامة** : • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **الكائنات المحذوفة** • **إدارة التقارير المفروضة** يمكنك تعيين هذا الدور لشخص يقوم بإجراء تدقيق لمؤسستك.
مسؤول التثبيت	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **نشر برنامج Kaspersky** • **إدارة مفتاح الترخيص** • **إدارة النظام**: • **نشر نظام التشغيل** • **إدارة الثغرات الأمنية والتصحيحات** • **التثبيت عن بُعد** • **مخزون البرنامج** منح حقوق **القراءة والتنفيذ** في **الميزات العامة: المجالات الوظيفية لخوادم الإدارة الافتراضية**.
مشغّل التثبيت	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **نشر برنامج Kaspersky** (يمنح أيضًا **تصحيحات إدارة Kaspersky** مباشرةً في هذه المنطقة) • **خوادم الإدارة الافتراضية** • **إدارة النظام**: • **نشر نظام التشغيل** • **إدارة الثغرات الأمنية والتصحيحات** • **التثبيت عن بُعد** • **مخزون البرنامج**
مسؤول Kaspersky Endpoint Security	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات تمنح حقوق **قراءة وكتابة** في منطقة الوظائف **الميزات العامة: إدارة مفتاح التشفير**.
مشغّل Kaspersky Endpoint Security	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات

الدور	الوصف
المسؤول الرئيسي	يسمح بجميع العمليات في المجالات الوظيفية، باستثناء المجالات التالية، في **الميزات العامة**: • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **إدارة التقارير المفروضة** تمنح حقوق **قراءة وكتابة** في منطقة الوظائف **الميزات العامة: إدارة مفتاح التشفير**.
المشغل الرئيسي	يمنح حقوق **القراءة والتنفيذ** (إن أمكن) في جميع المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **الكائنات المحذوفة** • **العمليات على خادم الإدارة** • **نشر تطبيق Kaspersky** • **خوادم الإدارة الافتراضية** • **إدارة جهاز المحمول: عام** • **إدارة النظام**، بما في ذلك جميع الميزات • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات
إدارة جهاز المحمول	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • **إدارة جهاز المحمول: عام**
مشّغل إدارة جهاز المحمول	يمنح حقوق **القراءة** و**التنفيذ** في **الميزات العامة**: المجالات الوظيفية**للوظائف الأساسية**. يمنح **قراءة** و**إرسال أوامر المعلومات فقط إلى الأجهزة المحمولة** في المجال الوظيفي **إدارة جهاز المحمول: عام**.
مسؤول الأمن	يسمح بجميع العمليات في المجالات الوظيفية التالية، في **الميزات العامة**: • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **إدارة التقارير المفروضة** تمنح **قراءة** و**كتابة** و**تنفيذ** و**حفظ الملفات من الأجهزة على محطة عمل المسؤول** و**تنفيذ العمليات على حقوق تحديدات الأجهزة** في منطقة الوظائف **إدارة النظام: الاتصال**. يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمان تكنولوجيا المعلومات في مؤسستك.
مستخدم Self Service Portal	يسمح بجميع العمليات في **إدارة جهاز المحمول: المجالات الوظيفية لـ Self Service Portal**. هذه الميزة غير مدعومة في Kaspersky Security Center 11 والإصدار الأحدث.
المشرف	يمنح حق **القراءة** في **الميزات العامة**: **الوصول إلى الكائنات، بغض النظر عن قوائم التحكم في الوصول ACLs** و**الميزات العامة**: المجالات الوظيفية **لإدارة التقارير المفروضة**. يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمان تكنولوجيا المعلومات في مؤسستك.
مسؤول إدارة الثغرات الأمنية والتصحيحات	يسمح بجميع العمليات في **الميزات العامة**: المجالات الوظيفية **للوظائف الأساسية** و**إدارة النظام** (بما في ذلك جميع الميزات).
مشغّل إدارة الثغرات الأمنية والتصحيحات	يمنح حقوق **القراءة** و**التنفيذ** (إن أمكن) في **الميزات العامة**: المجالات الوظيفية **للوظائف الأساسية** و**إدارة النظام** (بما في ذلك جميع الميزات).

تعيين حقوق الوصول إلى كائنات محددة

بالإضافة إلى تعيين حقوق الوصول على مستوى الخادم، يمكنك تكوين الوصول إلى كائنات محددة، على سبيل المثال، لمهمة محددة. يتيح لك التطبيق تحديد حقوق الوصول لأنواع الكائنات التالية:

- مجموعات الإدارة
- المهام
- تقارير
- تحديدات الأجهزة
- مجموعات الأحداث المحددة

لتعيين حقوق الوصول إلى كائن معين:

1. اعتمادًا على نوع الكائن، في القائمة الرئيسية، انتقل إلى القسم المقابل:

- **Assets (Devices)** ← **Hierarchy of groups**
- **Assets (Devices)** ← **Tasks**
- **Monitoring & reporting** ← **Reports**
- **Assets (Devices)** ← **Device selections**
- **Monitoring & reporting** ← **Event selections**

2. افتح خصائص الكائن الذي تريد تكوين حقوق الوصول إليه.

لفتح نافذة خصائص مجموعة إدارة أو مهمة، انقر فوق اسم الكائن. يمكن فتح خصائص الكائنات الأخرى باستخدام الزر الموجود على شريط الأدوات.

3. في نافذة الخصائص، افتح قسم **Access rights**.

تفتح قائمة المستخدمين. المستخدمين المدرجين ومجموعات الأمان لديهم حقوق الوصول إلى الكائن. بشكل افتراضي، إذا كنت تستخدم تسلسلاً هرميًا لمجموعات الإدارة أو الخوادم، فإن حقوق الوصول والقائمة موروثة من مجموعة الإدارة الأصل أو الخادم الأساسي.

4. لتتمكن من تعديل القائمة، قم بتمكين خيار **Use custom permissions**.

5. تكوين حقوق الوصول:

- استخدم أزرار **Add** و **Delete** لتعديل القائمة.
- حدد حقوق الوصول لمستخدم أو لمجموعة أمان. قم بأحد الإجراءات التالية:

- إذا كنت تريد تحديد حقوق الوصول يدويًا، فحدد المستخدم أو مجموعة الأمان، وانقر على زر **Access rights**، ثم حدد حقوق الوصول.
- إذا كنت تريد تعيين دور المستخدم للمستخدم أو لمجموعة الأمان، حدد المستخدم أو مجموعة الأمان، وانقر على **Roles**، ثم حدد الدور الذي تريد تعيينه.

6. انقر على زر **Save**.

تم تكوين حقوق الوصول إلى الكائن.

تعيين حقوق الوصول للمستخدمين ومجموعات الأمان

يمكنك منح المستخدمين ومجموعات الأمان حقوق الوصول لاستخدام الميزات المختلفة لخادم الإدارة، مثل Kaspersky Endpoint Security for Linux.

لتعيين حقوق الوصول لمستخدم أو مجموعة أمان:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **Access rights**، حدد خانة الاختيار المجاورة لاسم المستخدم أو مجموعة الأمان التي سيتم تعيين الحقوق إليها، ثم انقر فوق الزر **Access rights**.

لا يمكنك تحديد عدة مستخدمين أو مجموعات أمان في الوقت نفسه. وإذا حددت أكثر من عنصر واحد، فسيتم تعطيل الزر **Access rights**.

3. تكوين مجموعة الحقوق للمستخدم أو المجموعة:

a. قم بتوسيع العقدة بميزات خادم الإدارة أو تطبيق Kaspersky آخر.

b. حدد خانة الاختيار **سماح** أو **رفض** بجوار الميزة أو حق الوصول الذي تريده.

المثال 1: حدد خانة الاختيار **سماح** بجوار عقدة **تكامل التطبيق** لمنح جميع حقوق الوصول المتاحة لميزة تكامل التطبيق (**قراءة** و**كتابة** و**تنفيذ**) لمستخدم أو مجموعة.

المثال 2: قم بتوسيع عقدة **إدارة مفتاح التشفير**، ثم حدد خانة الاختيار **سماح** بجوار إذن **الكتابة** لمنح حق الوصول **للكتابة** إلى ميزة إدارة مفتاح التشفير لمستخدم أو مجموعة.

4. بعد تكوين مجموعة حقوق الوصول، انقر فوق **موافق**.

سيتم تكوين مجموعة الحقوق للمستخدم أو مجموعة المستخدمين.

يتم تقسيم أذونات خادم الإدارة (أو مجموعة الإدارة) إلى المناطق التالية:

- General features:
  - Management of administration groups
  - Access objects regardless of their ACLs
  - Basic functionality
  - Deleted objects
  - Encryption Key Management
  - Event processing
  - Operations on Administration Server (فقط في نافذة خصائص خادم الإدارة)
  - Device tags
  - Kaspersky application deployment
  - License key management
  - Application integration
  - Enforced report management
  - Hierarchy of Administration Servers
  - User permissions
  - Virtual Administration Servers
- Mobile Device Management:
  - General
  - Self Service Portal

- System Management:
  - Connectivity
  - Execute scripts remotely
  - Hardware inventory
  - Network Access Control
  - Operating system deployment
  - Vulnerability and patch management
  - Remote installation
  - Software inventory

إذا لم يتم اختيار **سماح** ولا **رفض** لحق وصول، فحينئذ يُعتبر حق الوصول غير محدد: يتم رفضه إلى حين رفضه صراحة أو السماح به للمستخدم.

تمثل حقوق المستخدم مجموع ما يلي:

- حقوق المستخدم الخاصة به
- حقوق جميع الأدوار التي تم تعيينها لهذا المستخدم
- حقوق جميع عناصر مجموعة الأمان التي ينتمي إليها المستخدم
- حقوق جميع الأدوار التي تم تعيينها لمجموعات الأمان التي ينتمي إليها المستخدم

إذا كان لدى أحد هذه الحقوق على الأقل حالة **رفض** للحصول على الإذن، فعندئذ يتم رفض منح المستخدم هذا الإذن، حتى إذا سمحت به المجموعات الأخرى أو تركته غير محدد.

يمكنك أيضًا إضافة مستخدمين ومجموعات أمان إلى نطاق دور المستخدم لاستخدام ميزات مختلفة لخادم الإدارة. لن يتم تطبيق الإعدادات المرتبطة بدور المستخدم إلا على الأجهزة التي تنتمي إلى المستخدمين الذين يمتلكون هذا الدور، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

إضافة حساب خاص بمستخدم داخلي

إذا كنت تريد إضافة حساب مستخدم، فتأكد أن حسابك يحتوي على قوائم التحكم في الوصول الخاصة بتعديل الكائنات في منطقة الوظائف الميزات العامة: أذونات المستخدم.

لإضافة حساب مستخدم داخلي جديد إلى Kaspersky Security Center:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users**.
2. انقر على **Add**.
3. في النافذة **Add user** التي تفتح، حدد الإعدادات الخاصة بحساب المستخدم الجديد:
   - **Name**
   - **Password**

يجب أن تتوافق كلمة المرور مع القواعد التالية:

- يجب أن يتراوح طول كلمة المرور من 8 إلى 256 حرفًا.
- يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
  - الأحرف الكبيرة (A-Z)
  - الأحرف الصغيرة (a-z)
  - الأعداد (0-9)
  - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

لرؤية كلمة المرور التي تم إدخالها، انقر فوق 👁.

يمكنك تفعيل الخيار **User must change password at first sign-in** لإجبار المستخدم على تغيير كلمة المرور عند مصادقة المستخدم لأول مرة.

4. احفظ التغييرات لإكمال إنشاء حساب المستخدم الجديد.

تتم إضافة حساب مستخدم جديد إلى قائمة المستخدمين.

لتسجيل الدخول باستخدام حساب مستخدم داخلي تم إنشاؤه على Kaspersky Security Center Web Console، يجب عليك تعيين دور للحساب. قبل تسجيل الدخول، تأكد من وجود دور لحساب المستخدم الداخلي. وإلا، سيحدث خطأ في تسجيل الدخول.

إنشاء مجموعة أمان

لإنشاء مجموعة أمان:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Groups**.
2. انقر على **Add**.
3. في النافذة **إنشاء مجموعة أمان** التي تفتح، حدد الإعدادات التالية لمجموعة الأمان الجديدة:
   - **Group name**
   - **Description**
4. انقر على **Save**لحفظ التغييرات.

يتم إضافة مجموعة أمان جديدة إلى قائمة المجموعة.

تحرير حساب خاص بمستخدم داخلي

إذا كنت تريد تحرير حساب مستخدم، فتأكد أن حسابك يحتوي على قوائم التحكم في الوصول الخاصة بتعديل الكائنات في منطقة الوظائف الميزات العامة: أذونات المستخدم.

قم بما يلي لتحرير حساب مستخدم داخلي في Kaspersky Security Center:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users**.
2. انقر على اسم حساب المستخدم الذي ترغب في تحريره.
3. في نافذة إعدادات المستخدم التي تفتح، قم بتغيير إعدادات حساب المستخدم في تبويب **General**:

- **User status**

يمكنك عند الضرورة وضع زر التبديل على **Disabled** لمنع المستخدم من التوصيل بالتطبيق. يمكنك تعطيل حساب، مثلاً بعد ترك الموظف للشركة.

- **Name**
- **Full name**
- **Description**
- **Email address**
- **Main phone**
- **Password**

إذا لزم الأمر، يمكنك تعيين كلمة مرور جديدة لاتصال المستخدم بتطبيق Kaspersky Security Center على النحو التالي:

a. انقر فوق الزر **Change password**، ثم قم بتعيين كلمة مرور جديدة لحساب المستخدم.
يجب أن تتوافق كلمة المرور مع القواعد التالية:

- يجب أن يتراوح طول كلمة المرور من 8 إلى 256 حرفًا.
- يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
  - الأحرف الكبيرة (A-Z)
  - الأحرف الصغيرة (a-z)
  - الأعداد (0-9)
  - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

لرؤية كلمة المرور التي تم إدخالها، انقر فوق 👁.

b. إذا لزم الأمر، قم بتمكين الخيار **User must change password at first sign-in** لفرض تغيير كلمة المرور عند مصادقة المستخدم التالية.

c. إذا كان حساب المستخدم محميًا ضد التعديل غير المصرح به، فيجب عليك التأكد من امتلاكك للأذونات اللازمة لتغيير هذا الحساب. في النافذة **Account protection**، حدد بيانات اعتماد الحساب الذي يحتوي على حق تعديل قوائم التحكم في الوصول للكائنات في منطقة الوظائف الميزات العامة: أذونات المستخدم.

4. في تبويب **Authentication security**، يمكنك تحديد إعدادات الأمان لهذا الحساب.

5. في تبويب **Groups**، يمكنك إضافة المستخدم إلى مجموعات الأمان.

6. في تبويب **Devices**، يمكنك تخصيص الأجهزة إلى المستخدم.

7. في تبويب **Roles**، يمكنك تخصيص الأدوار إلى المستخدم.

8. احفظ التغييرات لاستكمال تحرير حساب المستخدم.

يظهر حسابات المستخدم المحدث في قائمة المستخدمين.

تحرير مجموعة أمان

لتحرير مجموعة أمان:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Groups**.

2. انقر على اسم مجموعة الأمان التي ترغب في تحريرها.

3. في نافذة إعدادات المجموعة التي تفتح، قم بتغيير إعدادات مجموعة الأمان:

- في علامة التبويب **General**، يمكنك تغيير إعدادات **Name** و**Description**. تتوفر هذه الإعدادات فقط لمجموعات الأمان الداخلية.
- في علامة التبويب **Users**، يمكنك إضافة مستخدمين إلى مجموعة الأمان. ويتوفر هذا الإعداد فقط للمستخدمين الداخليين ومجموعات الأمان الداخلية.
- في علامة التبويب **Roles**، يمكنك تخصيص دور إلى مجموعة الأمان.

4. انقر على **Save**لحفظ التغييرات.

يتم تطبيق التغييرات على مجموعة الأمان.

تعيين دور لمستخدم أو لمجموعة أمان

لتعيين دور لمستخدم أو لمجموعة أمان:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users** أو **Groups**.

2. حدد اسم المستخدم أو مجموعة الأمان التي تريد تعيين دور لها.

يمكنك تحديد العديد من الأسماء.

3. في سطر القائمة، انقر على الزر **Assign role**.

سيبدأ معالج تعيين الدور.

4. اتبع إرشادات المعالج: حدد الدور الذي تريد تعيينه للمستخدمين أو مجموعات الأمان المحددة، ثم حدد نطاق الدور.

نطاق دور المستخدم هو مجموعة من المستخدمين ومجموعات الإدارة. لا تنطبق الإعدادات المرتبطة بدور مستخدم إلا على الأجهزة التي تنتمي إلى المستخدمين الذين يملكون هذا الدور، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

يتم تعيين الدور مع مجموعة الحقوق للعمل مع خادم الإدارة للمستخدم (أو المستخدمين، أو مجموعة الأمان). في قائمة المستخدمين أو مجموعات الأمان، تظهر خانة اختيار في العمود **Has assigned roles**.

لا يمكن تعيين دور للمستخدمين الذين تم إنشاؤهم على خادم افتراضي على خادم الإدارة.

إضافة حسابات المستخدمين إلى مجموعة أمان داخلية

يمكنك إضافة حسابات المستخدمين الداخليين فقط إلى مجموعة أمان داخلية.

لإضافة حسابات المستخدمين إلى مجموعة أمان داخلية:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users**.
2. حدد خانات الاختيار الموجودة بجوار حسابات المستخدمين التي ترغب في إضافتها إلى مجموعة أمان.
3. انقر على زر **Assign group**.
4. في النافذة **Assign group** التي تفتح، حدد مجموعة الأمان التي ترغب في إضافة حسابات المستخدمين إليها.
5. انقر على زر **حفظ**.

يتم إضافة حسابات المستخدمين إلى مجموعة الأمان. ويمكنك أيضًا إضافة مستخدمين داخليين إلى مجموعة أمان باستخدام إعدادات المجموعة.

تعيين مستخدم كمالك للجهاز

للحصول على معلومات عن تعيين مستخدم كمالك للجهاز المحمول، راجع تعليمات Kaspersky Secure Mobility Management.

لتعيين مستخدم كمالك للجهاز:

1. إذا كنت ترغب في تعيين مالك لجهاز متصل بخادم إدارة افتراضي، فقم أولاً بالتبديل إلى خادم الإدارة الظاهري:
   a. في القائمة الرئيسية، انقر فوق أيقونة الشارة (▶) إلى يمين اسم خادم الإدارة الحالي.
   b. حدد خادم الإدارة المطلوب.
2. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users**.

تفتح قائمة المستخدمين. إذا كنت متصلاً حاليًا بخادم إدارة افتراضي، فستشمل القائمة مستخدمين من خادم الإدارة الظاهري الحالي وخادم الإدارة الأساسي.

3. انقر على اسم حساب المستخدم الذي ترغب في تعيينه كمالك جهاز.
4. في نافذة إعدادات المستخدم التي تفتح، حدد علامة تبويب **Devices**.
5. انقر على **Add**.

6. من قائمة الجهاز، حدد الجهاز التي ترغب في تعيينه إلى المستخدم.

7. انقر على **OK**.

يتم إضافة الجهاز المحدد إلى قائمة الأجهزة المعينة للمستخدم.

يمكنك إجراء العملية نفسها في **Managed devices** ← **Assets (Devices)** عن طريق النقر على اسم الجهاز الذي ترغب في تعيينه ثم النقر على رابط **Manage device owner**.

تكوين التحقق بخطوتين لجميع المستخدمين

يصف هذا السيناريو كيفية تمكين المصادقة الثنائية لجميع المستخدمين وكيفية استثناء حسابات المستخدمين من المصادقة الثنائية. إذا لم تقم بتمكين المصادقة الثنائية لحسابك قبل تمكينها للمستخدمين الآخرين، فإن التطبيق يفتح النافذة لتمكين المصادقة لحسابك أولاً. يصف هذا السيناريو أيضًا كيفية تمكين المصادقة الثنائية لحسابك الخاص.

إذا قمت بتمكين المصادقة الثنائية لحسابك، يمكنك المتابعة إلى مرحلة تمكين المصادقة الثنائية لجميع المستخدمين.

المتطلبات الأساسية

قبل ان تبدا:

- تأكد من أن حساب المستخدم الخاص بك لديه حقوق تعديل قوائم التحكم في الوصول للكائن مباشرة في المجال الوظيفي **الميزات العامة: أذونات المستخدم** لتعديل إعدادات الأمان لحسابات المستخدمين الآخرين.
- تأكد من تثبيت المستخدمين الآخرين لخادم الإدارة لتطبيق مصادقة على أجهزتهم.

المراحل

تمكين المصادقة الثنائية لجميع المستخدمين يتم في مراحل:

1. **تثبيت تطبيق مصادقة على جهاز**

   يمكنك تثبيت أي تطبيق يدعم خوارزمية كلمة المرور لمرة واحدة المستندة إلى الوقت (TOTP)، مثل:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - معرف Yandex
   - Avanpost Authenticator
   - Aladdin 2FA

   للتحقق مما إذا كان Kaspersky Security Center يدعم تطبيق المصادقة الذي تريد استخدامه، قم بتمكين التحقق ثنائي الخطوات لجميع المستخدمين أو لمستخدم معين.

وتقترح إحدى الخطوات أن تحدد رمز الحماية الذي تم إنشاؤه بواسطة تطبيق المصادقة. إذا نجح ذلك، فإن Kaspersky Security Center يدعم المصادقة المحددة.

لا نوصي بشدة بتثبيت تطبيق المصادقة على الجهاز نفسه الذي تم من خلاله إنشاء الاتصال بخادم الإدارة.

2 **مزامنة وقت تطبيق المصادقة مع وقت الجهاز المثبت عليه خادم الإدارة.**

تأكد من مزامنة الوقت على الجهاز الذي يحتوي على تطبيق المصادقة والوقت على الجهاز الذي يحتوي على خادم الإدارة مع التوقيت العالمي المنسق (UTC)، باستخدام مصادر الوقت الخارجية. بخلاف ذلك ، قد تحدث حالات فشل أثناء المصادقة وتفعيل التحقق ثنائي الخطوات.

3 **تمكين المصادقة الثنائية لحسابك واستلم المفتاح السري لحسابك**

تعليمات للمساعدة:

- بالنسبة لوحدة تحكم الإدارة المستندة إلى MMC: تمكين المصادقة الثنائية لحسابك الخاص
- بالنسبة لـ Kaspersky Security Center Web Console: تمكين المصادقة الثنائية لحسابك الخاص

بعد أن تقوم بتمكين المصادقة الثنائية لحسابك، يمكنك تمكين المصادقة الثنائية لجميع المستخدمين.

4 **تمكين المصادقة الثنائية لجميع المستخدمين**

يجب على المستخدمين الذين تم تمكين المصادقة الثنائية لهم استخدامها في تسجيل الدخول إلى خادم الإدارة.

تعليمات للمساعدة:

- بالنسبة لوحدة تحكم الإدارة المستندة إلى MMC: تمكين المصادقة الثنائية لجميع المستخدمين
- بالنسبة لمكون Kaspersky Security Center Web Console: تمكين المصادقة الثنائية لجميع المستخدمين

5 **تحرير اسم مُصدِر رمز الأمان**

إذا كان لديك عدة خوادم إدارة بأسماء متماثلة، قد تضطر إلى تغيير أسماء مُصدري رموز الأمان للتعرف بشكل أفضل على خوادم الإدارة المختلفة.

تعليمات للمساعدة:

- بالنسبة لوحدة تحكم الإدارة المستندة إلى MMC: تحرير اسم مُصدِر رمز الأمان
- بالنسبة لـ Kaspersky Security Center Web Console: تحرير اسم مُصدِر رمز الأمان

6 **استثناء حسابات المستخدمين التي لا تحتاج إلى تمكين المصادقة الثنائية لها**

إذا لزم الأمر، يمكنك استبعاد المستخدمين من التحقق على خطوتين. المستخدمين الذين لديهم حسابات مستثناة لا يتعين عليهم استخدام المصادقة الثنائية لتسجيل الدخول إلى خادم الإدارة.

تعليمات للمساعدة:

- بالنسبة لوحدة تحكم الإدارة المستندة إلى MMC: استثناء الحسابات من المصادقة الثنائية
- بالنسبة لمكون Kaspersky Security Center Web Console: استثناء الحسابات من المصادقة الثنائية

7 **تكوين المصادقة ثنائية الخطوات لحسابك الخاص**

إذا لم يتم استثناء المستخدمين من التحقق ثنائي الخطوات ولم يتم تكوين التحقق ثنائي الخطوات لحساباتهم بعد، سيلزمهم تكوينه في النافذة التي تفتح عند تسجيل الدخول إلى Kaspersky Security Center. وإلا فلن يتمكنوا من الوصول إلى خادم الإدارة وفقًا لحقوقهم.

تعليمات للمساعدة:

- فيما يتعلق بوحدة تحكم الإدارة المستندة إلى MMC: تكوين المصادقة ثنائية الخطوات لحسابك الخاص
- فيما يتعلق بـ Kaspersky Security Center Web Console: تكوين المصادقة ثنائية الخطوات لحسابك الخاص

النتائج

عند الانتهاء من هذا السيناريو:

- تم تمكين المصادقة الثنائية لحسابك.
- تم تمكين المصادقة الثنائية لجميع حسابات المستخدمين لخادم الإدارة، باستثناء حسابات المستخدمين التي تم استثناءها.

عن المصادقة الثنائية

عند تمكين التحقق ثنائي الخطوات لحساب ما، يلزم وجود رمز أمان للاستخدام مرة واحدة، بالإضافة إلى اسم المستخدم وكلمة المرور، لتسجيل الدخول إلى وحدة تحكم الإدارة أو Kaspersky Security Center Web Console. مع تمكين مصادقة المجال، يحتاج المستخدم فقط إلى إدخال رمز أمان للاستخدام مرة واحدة.

لاستخدام التحقق بخطوتين، قم بتثبيت تطبيق مصادقة ينشئ رموز أمان للاستخدام مرة واحدة على الجهاز المحمول أو الكمبيوتر. ويمكنك استخدام أي تطبيق يدعم خوارزمية كلمة المرور لمرة واحدة المستندة إلى الوقت (TOTP)، مثل:

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- معرف Yandex
- Avanpost Authenticator
- Aladdin 2FA

للتحقق مما إذا كان Kaspersky Security Center يدعم تطبيق المصادقة الذي تريد استخدامه، قم بتمكين التحقق ثنائي الخطوات لجميع المستخدمين أو لمستخدم معين.

وتقترح إحدى الخطوات أن تحدد رمز الحماية الذي تم إنشاؤه بواسطة تطبيق المصادقة. إذا نجح ذلك، فإن Kaspersky Security Center يدعم المصادقة المحددة.

نوصي بشدة بحفظ المفتاح السري أو رمز الاستجابة السريعة والاحتفاظ به في مكان آمن. سيساعدك هذا في استعادة الوصول إلى Kaspersky Security Center Web Console في حالة فقدان الوصول إلى الجهاز المحمول.

لتأمين استخدام Kaspersky Security Center، يمكنك تمكين المصادقة الثنائية لحسابك الخاص وتمكين المصادقة الثنائية لجميع المستخدمين.

يمكنك استثناء حسابات من المصادقة الثنائية. يمكن أن يكون هذا ضروريًا لحسابات الخدمة التي لا يمكنها تلقي رمز أمان للمصادقة.

القواعد والقيود

لتتمكن من تفعيل التحقق ثنائي الخطوات لجميع المستخدمين وتعطيل التحقق ثنائي الخطوات لمستخدمين معينين:

- تأكد من تعديل قوائم التحكم في الوصول للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.
- تمكين المصادقة الثنائية لحسابك.

لتتمكن من تعطيل التحقق ثنائي الخطوات لجميع المستخدمين:

- تأكد من تعديل قوائم التحكم في الوصول للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.
- سجّل الدخول إلى Kaspersky Security Center Web Console باستخدام التحقق ثنائي الخطوات.

إذا كانت المصادقة الثنائية مفعلة لحساب مستخدم على خادم إدارة Kaspersky Security Center الإصدار 13 أو أحدث، لن يقدر المستخدم على تسجيل الدخول إلى Kaspersky Security Center Web Console 12 أو 12.1 أو 12.2.

إعادة إصدار المفتاح السري

يستطيع أي مستخدم إعادة إصدار المفتاح السري المستخدم في التحقق ثنائي الخطوات. وعندما يسجل المستخدم الدخول إلى خادم الإدارة باستخدام المفتاح السري المعاد إصداره، يتم حفظ المفتاح السري الجديد لحساب المستخدم. وإذا أدخل المستخدم المفتاح السري الجديد بشكل غير صحيح، فلن يتم حفظ المفتاح السري الجديد، ويظل المفتاح السري الحالي صالحًا.

رمز الحماية له معرّف يشار إليه باسم اسم المُصدر. اسم مُصدر رمز الأمان يُستخدم كمُعرّف لخادم الإدارة في تطبيق المصادقة. اسم مُصدر رمز الأمان له قيمة افتراضية مماثلة لاسم خادم الإدارة. يمكنك تغيير اسم مُصدر رمز الأمان. إذا قمت بتغيير اسم جهة إصدار رمز الأمان، يجب عليك إصدار مفتاح سري جديد وتمريره إلى تطبيق المصادقة.

تمكين التحقق بخطوتين لحسابك الخاص (Web Console)

يمكنك تمكين المصادقة الثنائية لحسابك الخاص.

قبل أن تقوم بتمكين التحقق بخطوتين لحسابك، تأكد من تثبيت تطبيق مصادقة على الجهاز المحمول. تأكد أن الوقت المحدد في تطبيق المصادقة متزامن مع الوقت المحدد للجهاز المثبت عليه خادم الإدارة.

لتمكين المصادقة الثنائية لحساب مستخدم:

1. في القائمة الرئيسية، انتقل إلى **Users** ← **Users & roles**.
2. انقر على اسم حسابك.
3. في نافذة إعدادات المستخدم التي تفتح، حدد علامة التبويب **Authentication security**.
4. في علامة التبويب **Authentication security**:
   a. حدد الخيار **Request user name, password, and security code (two-step verification)**. انقر على زر **حفظ**.
   b. في نافذة التحقق ثنائي الخطوات التي تفتح، انقر فوق **View how to set up two-step verification**.
   أدخل المفتاح السري في تطبيق المصادقة أو انقر فوق **View QR code** وامسح رمز الاستجابة السريعة ضوئيًا بواسطة تطبيق المصادقة على الجهاز المحمول لاستلام رمز الأمان لمرة واحدة.
   c. في نافذة المصادقة الثنائية، حدد رمز الأمان الذي أنشأه تطبيق المصادقة ثم انقر على زر **Check and apply**.
5. انقر على زر **حفظ**.

تم تمكين المصادقة الثنائية لحسابك.

تمكين التحقق بخطوتين لحسابك الخاص (القائم على MMC)

قبل أن تقوم بتمكين التحقق بخطوتين لحسابك، تأكد من تثبيت تطبيق مصادقة على الجهاز المحمول. تأكد من أن الوقت المحدد في تطبيق المصادقة متزامن مع وقت خادم الإدارة.

لتمكين المصادقة الثنائية لحسابك:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.
2. في نافذة خصائص خادم الإدارة، اذهب إلى لوحة **الأقسام**، وفيها حدد **خيارات متقدمة** ثم **المصادقة الثنائية**.
3. في قسم **المصادقة الثنائية**، انقر فوق زر **الإعداد**.

إذا تم تمكين التحقق ثنائي الخطوات بالفعل لحسابك، فإن النقر فوق الزر **إعداد** يعيد تعيين المفتاح السري حتى تتمكن من إعادة تكوين التحقق ثنائي الخطوات.

في نافذة خصائص المصادقة الثنائية التي تفتح، يتم عرض المفتاح السري.

4. أدخل المفتاح السري في تطبيق المصادقة لتلقي رمز الحماية لمرة واحدة. ويمكنك تحديد المفتاح السري في تطبيق المصادقة يدويًا أو مسح رمز الاستجابة السريعة ضوئيًا بواسطة تطبيق المصادقة على الجهاز المحمول.
5. حدد رمز الحماية الذي تم إنشاؤه عبر تطبيق المصادقة ثم انقر على الزر **موافق** للخروج من نافذة خصائص التحقق بخطوتين.
6. انقر على زر **تطبيق**.
7. انقر على زر **موافق**.

بهذا تم تمكين المصادقة الثنائية لحسابك الخاص.

تمكين التحقق بخطوتين المطلوب لجميع المستخدمين (Web Console)

يمكنك تمكين المصادقة الثنائية لجميع مستخدمي خادم الإدارة إذا كان حسابك لديه حقوق تعديل قوائم التحكم في الوصول للكائن للمجال الوظيفي **الميزات العامة: أذونات المستخدم** وإذا كان مصرحًا لك استخدام المصادقة الثنائية.

لتمكين المصادقة الثنائية لجميع المستخدمين:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في تبويب **Authentication security** في نافذة الخصائص، قم بتبديل زر التبديل لخيار **المصادقة الثنائية لجميع المستخدمين** إلى وضع التمكين.

3. إذا لم تقم بتمكين المصادقة الثنائية لحسابك، فإن التطبيق يفتح نافذة لتمكين المصادقة الثنائية لحسابك الخاص أولاً.

a. في نافذة التحقق ثنائي الخطوات، انقر فوق **View how to set up two-step verification**.

b. أدخل المفتاح السري في تطبيق المصادقة يدويًا أو انقر فوق **View QR code** وامسح رمز الاستجابة السريعة ضوئيًا بواسطة تطبيق المصادقة على الجهاز المحمول لاستلام رمز الأمان لمرة واحدة.

c. في نافذة المصادقة الثنائية، حدد رمز الأمان الذي أنشأه تطبيق المصادقة ثم انقر على زر **Check and apply**.

بهذا تم تمكين المصادقة الثنائية لجميع المستخدمين. من الآن فصاعدًا، مستخدمو خادم الإدارة، بما في ذلك المستخدمين الذين تمت إضافتهم بعد تمكين المصادقة الثنائية لجميع المستخدمين، يتعين عليهم تكوين المصادقة الثنائية لحساباتهم، باستثناء المستخدمين الذين تم استثنائهم من المصادقة الثنائية.

تمكين التحقق بخطوتين لجميع المستخدمين (القائم على MMC)

يمكنك تمكين المصادقة الثنائية لجميع مستخدمي خادم الإدارة إذا كان حسابك لديه حقوق تعديل قوائم التحكم في الوصول للكائن للمجال الوظيفي **الميزات العامة: أذونات المستخدم** وإذا كان مصرحًا لك استخدام المصادقة الثنائية.

لتمكين المصادقة الثنائية لجميع المستخدمين:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.

2. في نافذة خصائص خادم الإدارة، في لوحة **الأقسام**، حدد **خيارات متقدمة** ثم **المصادقة الثنائية**.

3. انقر على زر **تعيين كمطلوب** لتمكين المصادقة الثنائية لجميع المستخدمين.

4. إذا لم تقم بتمكين المصادقة الثنائية لحسابك، فإن التطبيق يفتح نافذة لتمكين المصادقة الثنائية لحسابك الخاص أولاً.

a. أدخل المفتاح السري في تطبيق المصادقة لتلقي رمز الحماية لمرة واحدة. يمكنك تحديد المفتاح السري في تطبيق المصادقة يدويًا أو مسح رمز الاستجابة السريعة ضوئيًا بواسطة تطبيق المصادقة على الجهاز المحمول لاستلام رمز الأمان لمرة واحدة.

b. حدد رمز الحماية الذي تم إنشاؤه عبر تطبيق المصادقة ثم انقر على الزر **موافق** للخروج من نافذة خصائص التحقق بخطوتين.

5. في قسم **المصادقة الثنائية**، انقر على زر **تطبيق**، ثم انقر على زر **موافق**.

بهذا تم تمكين المصادقة الثنائية لجميع المستخدمين. من الآن فصاعدًا، يتعين على جميع مستخدمي خادم الإدارة، بما في ذلك المستخدمين الذين تمت إضافتهم بعد تمكين هذا الخيار، تكوين المصادقة الثنائية لحساباتهم، باستثناء المستخدمين الذين تكون حساباتهم مستثناة من المصادقة الثنائية.

تعطيل التحقق بخطوتين لحساب مستخدم (Web Console)

يمكنك تعطيل المصادقة الثنائية لحسابك الخاص، وكذلك لحساب أي مستخدم آخر.

يمكنك تعطيل التحقق بخطوتين لحساب مستخدم آخر إذا كان حسابك يحتوي على حق تعديل قوائم التحكم في الوصول (ACL) للكائن مباشرة في المجال الوظيفي **الميزات العامة: أذونات المستخدم** وما إذا كان مصرحًا لك باستخدام التحقق بخطوتين.

لتعطيل المصادقة الثنائية لحساب مستخدم:

1. في القائمة الرئيسية، انتقل إلى **Users** ← **Users & roles**.

2. انقر على حساب المستخدم الداخلي الذي ترغب في تعطيل المصادقة الثنائية له. قد يكون هذا هو حسابك الخاص أو حساب أي مستخدم آخر.

3. في نافذة إعدادات المستخدم التي تفتح، حدد تبويب **Account protection**.

4. في تبويب **Account protection**، حدد خيار **Request only user name and password** إذا كنت ترغب في تعطيل المصادقة الثنائية لحساب مستخدم.

5. انقر على زر **حفظ**.

بهذا تم تعطيل المصادقة الثنائية لحساب المستخدم.

إذا كنت ترغب في استعادة الوصول لمستخدم لا يمكنه تسجيل الدخول إلى Kaspersky Security Center Web Console باستخدام التحقق بخطوتين، فقم بتعطيل التحقق بخطوتين لحساب المستخدم هذا، ثم حدد الخيار **Request only user name and password** كما هو موضح أعلاه. بعد ذلك، سجل الدخول إلى Kaspersky Security Center Web Console تحت حساب المستخدم الذي قمت بتعطيل التحقق بخطوتين له، ثم قم بتمكين التحقق مرة أخرى.

تعطيل التحقق بخطوتين لحساب مستخدم (القائم على MMC)

لتعطيل المصادقة الثنائية لحسابك الشخصي:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.

2. في نافذة خصائص خادم الإدارة، في لوحة **الأقسام**، حدد **خيارات متقدمة** ثم **المصادقة الثنائية**.

3. في قسم **المصادقة الثنائية**، انقر على زر **تعطيل**.

4. انقر على زر **تطبيق**.

5. انقر على زر **موافق**.

تم تعطيل المصادقة الثنائية لحسابك.

يمكنك تعطيل المصادقة الثنائية لحسابات المستخدمين الآخرين. يوفر هذا الحماية في حالة فقد المستخدم لجهازه المحمول أو كسره على سبيل المثال.

يمكنك تعطيل التحقق بخطوتين لجميع مستخدمي خادم الإدارة إذا كان لديك حق تعديل قوائم التحكم في الوصول للكائنات مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم** وإذا كان مصرحًا لك باستخدام التحقق بخطوتين. باتباع الخطوات أدناه، يمكنك تعطيل المصادقة الثنائية لحسابك الخاص أيضًا.

لتعطيل المصادقة الثنائية لأي حساب مستخدم:

1. في شجرة وحدة التحكم، افتح مجلد **حسابات المستخدمين**.

   مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **متقدم** بشكل افتراضي.

2. في مساحة العمل، انقر نقرًا مزدوجًا على حساب المستخدم الذي ترغب في تعطيل المصادقة الثنائية له.

   بالنسبة لجميع حسابات المستخدمين التي تم تمكين التحقق بخطوتين لها، يتم تعيين العمود **2FA مطلوب** على **نعم**.

3. في نافذة **الخصائص:<اسم المستخدم>** التي تفتح، حدد قسم **المصادقة الثنائية**.

4. في قسم **المصادقة الثنائية**، حدد الخيارات التالية:

- إذا كنت ترغب في تعطيل المصادقة الثنائية لحساب مستخدم، انقر على زر **تعطيل**.
- إذا كنت ترغب في استثناء حساب المستخدم هذا من المصادقة الثنائية لجميع المستخدمين، حدد خيار **يمكن للمستخدم تمرير المصادقة باستخدام اسم المستخدم وكلمة المرور فقط**.

5. انقر على زر **تطبيق**.

6. انقر على زر **موافق**.

تم تعطيل المصادقة الثنائية لحساب المستخدم.

إذا كنت ترغب في استعادة الوصول لمستخدم لا يمكنه تسجيل الدخول إلى وحدة تحكم الإدارة باستخدام التحقق بخطوتين، فقم بتعطيل التحقق بخطوتين لحساب المستخدم هذا وحدد الخيار **يمكن للمستخدم تمرير المصادقة باستخدام اسم المستخدم وكلمة المرور فقط** في خطوة **التحقق بخطوتين** كما هو موضح أعلاه. بعد ذلك، سجل الدخول إلى وحدة تحكم الإدارة تحت حساب المستخدم الذي عطلت التحقق بخطوتين له، ثم قم بتمكين التحقق مرة أخرى.

تعطيل التحقق بخطوتين المطلوب لجميع المستخدمين (Web Console)

يمكنك التحقق بخطوتين المطلوب لجميع المستخدمين إذا تم تمكين التحقق بخطوتين لحسابك، وكان حسابك يتمتع بحق تعديل قوائم التحكم في الوصول للكائنات مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**. إذا لم تكن المصادقة الثنائية ممكنة لحسابك، يجب عليك تمكين المصادقة الثنائية لحسابك قبل تعطيلها لجميع المستخدمين.

لتعطيل المصادقة الثنائية لجميع المستخدمين:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في تبويب **Authentication security** في نافذة الخصائص، قم بتبديل زر التبديل لخيار **المصادقة الثنائية لجميع المستخدمين** إلى وضع التعطيل.

بهذا تم تعطيل المصادقة الثنائية لجميع المستخدمين. لا ينطبق تعطيل التحقق بخطوتين لجميع المستخدمين على حسابات محددة تم تمكين التحقق بخطوتين لها مسبقًا بشكل منفصل.

تمكين التحقق بخطوتين المطلوب لجميع المستخدمين (القائم على MMC)

يمكنك تعطيل التحقق بخطوتين المطلوب لجميع مستخدمي خادم الإدارة إذا كان لديك حق تعديل قوائم التحكم في الوصول للكائنات مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم** وإذا كان مصرحًا لك باستخدام التحقق بخطوتين.

لتعطيل المصادقة الثنائية لجميع المستخدمين:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.

2. في نافذة خصائص خادم الإدارة، في لوحة **الأقسام**، حدد **خيارات متقدمة** ثم **المصادقة الثنائية**.

3. انقر على زر **تعيين كاختياري** لتعطيل المصادقة الثنائية لجميع المستخدمين.

4. انقر على زر **تطبيق** في قسم **المصادقة الثنائية**.

5. انقر على زر **موافق** في قسم **المصادقة الثنائية**.

بهذا تم تعطيل المصادقة الثنائية لجميع المستخدمين. لا ينطبق تعطيل التحقق بخطوتين لجميع المستخدمين على حسابات محددة تم تمكين التحقق بخطوتين لها مسبقًا بشكل منفصل.

استثناء الحسابات من التحقق بخطوتين (Web Console)

يمكنك استثناء حسابات مستخدمين من المصادقة الثنائية إذا كان لديك حق تعديل قوائم التحكم في الوصول للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.

إذا تم استثناء حساب مستخدم من قائمة المصادقة الثنائية لجميع المستخدمين، لن يتعين على هذا المستخدم استخدام المصادقة الثنائية.

استثناء الحسابات من المصادقة الثنائية لجميع المستخدمين قد يكون ضروريًا لحسابات الخدمة التي لا يمكنها تمرير رمز الأمان أثناء المصادقة.

إذا كنت ترغب في استثناء بعض حسابات المستخدمين من المصادقة الثنائية:

1. يجب عليك إجراء استقصاء وحدة تحكم مجال Microsoft Active Directory من أجل تحديث قائمة مستخدمي خادم الإدارة إذا كنت ترغب في استثناء حسابات Active Directory.

2. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.

3. في تبويب **Authentication security** في نافذة الخصائص، في جدول استثناءات المصادقة الثنائية، انقر على زر **Add**.

4. في النافذة التي تفتح:

   a. حدد حسابات المستخدمين التي ترغب في استثناءها.

   b. انقر على زر **OK**.

بهذا تم استثناء حسابات المستخدمين المحددة من المصادقة الثنائية.

استثناء الحسابات من التحقق بخطوتين (القائم على MMC)

يمكنك استثناء حساب من المصادقة الثنائية إذا كان حسابك له حق تعديل قوائم التحكم في الوصول للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.

إذا تم استثناء حساب مستخدم من المصادقة الثنائية، يمكن لهذا المستخدم تسجيل الدخول إلى وحدة تحكم الإدارة أو Kaspersky Security Center Web Console دون استخدام المصادقة باستخدام المصادقة الثنائية.

استثناء الحسابات من المصادقة الثنائية لجميع المستخدمين قد يكون ضروريًا لحسابات الخدمة التي لا يمكنها تمرير رمز الأمان أثناء المصادقة.

لاستثناء حساب مستخدم من المصادقة الثنائية:

1. إذا كنت ترغب في استثناء حساب Active Directory، قم بإجراء استقصاء Active Directory لتحديث قائمة مستخدمي خادم الإدارة.

2. في شجرة وحدة التحكم، افتح مجلد **حسابات المستخدمين**.
   مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **متقدم** بشكل افتراضي.

3. في مساحة العمل، انقر نقرًا مزدوجًا على حساب المستخدم الذي ترغب في استثنائه من المصادقة الثنائية.

4. في نافذة **الخصائص:<اسم المستخدم>** التي تفتح، حدد قسم **المصادقة الثنائية**.

5. في القسم المفتوح، حدد خيار **يمكن للمستخدم تمرير المصادقة باستخدام اسم المستخدم وكلمة المرور فقط**.

6. في قسم **المصادقة الثنائية**، انقر على زر **تطبيق**، ثم انقر على زر **موافق**.

تم استثناء حساب المستخدم هذا من المصادقة الثنائية. يمكنك التحقق من الحسابات المستثناة في قائمة حسابات المستخدمين.

تحرير اسم مُصدِر رمز الأمان (Web Console)

يمكن أن يكون لديك العديد من المعرفات (يطلق عليها المصدرون) لخوادم الإدارة المختلفة. يمكنك تغيير اسم مُصدر رمز الأمان إذا كان مثلاً خادم الإدارة يستخدم بالفعل اسمًا مشابهًا لمُصدر رمز الأمان لخادم إدارة آخر. بشكل افتراضي، اسم مُصدر رمز الأمان هو نفسه اسم خادم الإدارة.

بعد أن تقوم بتغيير اسم مُصدر رمز الأمان، يجب عليك إعادة إصدار مفتاح سري جديد وتمريره إلى تطبيق المصادقة.

لتحديد اسم جديد لمصدِر رمز الأمان:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.

2. في نافذة إعدادات المستخدم التي تفتح، حدد تبويب **Account protection**.

3. في تبويب **Account protection**، انقر على رابط **تحرير**.
   قسم **تحرير مُصدِر رمز الأمان** سيفتح.

4. حدد اسم مُصدِر رمز أمان جديد.

5. انقر على زر **موافق**.

بهذا تم تحديد اسم مُصدر رمز أمان جديد لخادم الإدارة.

تحرير اسم مُصدِر رمز الأمان (القائم على MMC)

يمكن أن يكون لديك العديد من المعرفات (يطلق عليها المصدرون) لخوادم الإدارة المختلفة. يمكنك تغيير اسم مُصدر رمز الأمان إذا كان مثلاً خادم الإدارة يستخدم بالفعل اسمًا مشابهًا لمُصدر رمز الأمان لخادم إدارة آخر. بشكل افتراضي، اسم مُصدر رمز الأمان هو نفسه اسم خادم الإدارة.

بعد أن تقوم بتغيير اسم مُصدر رمز الأمان، يجب عليك إعادة إصدار مفتاح سري جديد وتمريره إلى تطبيق المصادقة.

لتحديد اسم جديد لمُصدِر رمز الأمان:

1. في شجرة وحدة التحكم لـ Kaspersky Security Center، افتح قائمة سياق مجلد **خادم الإدارة** وبعدها حدد **خصائص**.

2. في نافذة خصائص خادم الإدارة، في لوحة **الأقسام**، حدد **خيارات متقدمة** ثم **المصادقة الثنائية**.

3. حدد اسم مُصدر رمز أمان جديد في حقل **مُصدر رمز الحماية**.

4. انقر على زر **تطبيق** في قسم **المصادقة الثنائية**.

5. انقر على زر **موافق** في قسم **المصادقة الثنائية**.

بهذا تم تحديد اسم مُصدر رمز أمان جديد لخادم الإدارة.

تكوين التحقق بخطوتين لحسابك الخاص (Web Console)

في المرة الأولى التي تسجل فيها الدخول إلى Kaspersky Security Center بعد تمكين التحقق ثنائي الخطوات، تفتح نافذة تكوين التحقق ثنائي الخطوات لحسابك الخاص.

قبل أن تقوم بتكوين التحقق بخطوتين لحسابك، تأكد من تثبيت تطبيق مصادقة على الجهاز المحمول.

تأكد من مزامنة الوقت على الجهاز الذي يحتوي على تطبيق المصادقة والوقت على الجهاز الذي يحتوي على خادم الإدارة مع التوقيت العالمي المنسق (UTC)، باستخدام مصادر الوقت الخارجية.

لتكوين المصادقة ثنائية الخطوات لحسابك:

1. أنشئ رمز أمان لمرة واحدة باستخدام تطبيق المصادقة على الجهاز المحمول. لفعل هذا، نفذ أحد الإجراءات التالية:
   - أدخل المفتاح السري في تطبيق المصادقة يدويًا.
   - انقر فوق **View QR code** وافحص رمز الاستجابة السريعة ضوئيًا باستخدام تطبيق المصادقة.

   سيتم عرض رمز أمان على الجهاز المحمول.
2. في نافذة تكوين التحقق ثنائي الخطوات، حدد رمز الأمان الذي أنشأه تطبيق المصادقة ثم انقر على الزر **Check and apply**.

   تم تكوين المصادقة ثنائية الخطوات لحسابك. يمكنك الوصول إلى خادم الإدارة وفقًا لحقوقك.

تكوين التحقق بخطوتين لحسابك الخاص (القائم على MMC)

في المرة الأولى التي تسجل فيها الدخول إلى Kaspersky Security Center بعد تمكين التحقق ثنائي الخطوات، تفتح نافذة تكوين التحقق ثنائي الخطوات لحسابك الخاص.

قبل أن تقوم بتكوين التحقق بخطوتين لحسابك، تأكد من تثبيت تطبيق مصادقة على الجهاز المحمول. تأكد من مزامنة الوقت على الجهاز الذي يحتوي على تطبيق المصادقة والوقت على الجهاز الذي يحتوي على خادم الإدارة مع التوقيت العالمي المنسق (UTC)، باستخدام مصادر الوقت الخارجية.

لتكوين المصادقة ثنائية الخطوات لحسابك:

1. أنشئ رمز أمان لمرة واحدة باستخدام تطبيق المصادقة على الجهاز المحمول. لفعل هذا، نفذ أحد الإجراءات التالية:
   - أدخل المفتاح السري في تطبيق المصادقة يدويًا.
   - امسح رمز الاستجابة السريعة (QR) ضوئيًا باستخدام تطبيق المصادقة.

   سيتم عرض رمز أمان على الجهاز المحمول.
2. في النافذة **قم بإعداد التحقق المزدوج**، حدد رمز الأمان الذي أنشأه تطبيق المصادقة ثم انقر على الزر **موافق**.

   تم تكوين المصادقة ثنائية الخطوات لحسابك. يمكنك الوصول إلى خادم الإدارة وفقًا لحقوقك.

إنشاء مفتاح سري جديد

لا يمكنك إنشاء مفتاح سري جديد للمصادقة الثنائية لحسابك إلا إذا تم التصريح لك باستخدام المصادقة الثنائية.

لإنشاء مفتاح سري جديد لحساب مستخدم:

1. في القائمة الرئيسية، انتقل إلى **Users** ← **Users & roles**.
2. انقر على اسم حساب المستخدم الذي ترغب في إنشاء مفتاح سري جديد له للمصادقة الثنائية.
3. في نافذة إعدادات المستخدم التي تفتح، حدد تبويب **Account protection**.
4. في تبويب **Account protection**، انقر على رابط **Generate a new secret key**.
5. في نافذة المصادقة ثنائية الخطوات التي تفتح، حدد مفتاح أمان جديدًا تم إنشاؤه بواسطة تطبيق المصادقة.
6. انقر على زر **Check and apply** .

بهذا تم إنشاء مفتاح سري جديد للمستخدم.

إذا فقدت الجهاز المحمول، يمكنك تثبيت تطبيق المصادقة على جهاز محمول آخر وإنشاء مفتاح سري جديد لاستعادة الوصول إلى Kaspersky Security Center Web Console.

منع المستخدمين الجدد من إعداد التحقق ثنائي الخطوات لأنفسهم

لزيادة تحسين أمان الوصول إلى Kaspersky Security Center Web Console، يمكنك منع المستخدمين الجدد من إعداد التحقق بخطوتين لأنفسهم.

وفي حالة تمكين هذا الخيار، فلن يتمكن المستخدم الذي عطل التحقق ثنائي الخطوات، مثل مسؤول المجال الجديد، من تكوين التحقق بخطوتين لنفسه. لذلك، لا يمكن المصادقة على هذا المستخدم على خادم الإدارة ولا يمكنه تسجيل الدخول إلى Kaspersky Security Center Web Console دون الحصول على موافقة من مسؤول Kaspersky Security Center آخر تم تمكين التحقق بخطوتين بالفعل لأجله.

يتوفر هذا الخيار في حالة تمكين التحقق بخطوتين لجميع المستخدمين.

لمنع المستخدمين الجدد من إعداد التحقق بخطوتين لأنفسهم

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب **Authentication security** في نافذة الخصائص، قم بتبديل زر التبديل **Prohibit new users from setting up two-step verification for themselves** إلى وضع التمكين.

لا يؤثر هذا الخيار على حسابات المستخدمين المضافة إلى استثناءات التحقق بخطوتين.

لمنح Kaspersky Security Center Web Console حق الوصول إلى مستخدم تم تعطيل ميزة التحقق بخطوتين له، أوقف تشغيل الخيار **Prohibit new users from setting up two-step verification for themselves**، واطلب من المستخدم تمكين التحقق بخطوتين، ثم قم بتشغيل الخيار مرة أخرى.

تعيين مستخدم كمالك لجهاز Linux بعد تثبيت عميل الشبكة

للسماح للمستخدم بالتسجيل كمالك لجهاز Linux:

1. في Kaspersky Security Center Web Console، انتقل إلى **Deployment & assignment** ← **Discovery & deployment** ← **حزم التثبيت**.

   تفتح قائمة حزم التثبيت.

2. انقر على حزمة تثبيت عميل الشبكة.

   تفتح نافذة الخصائص الخاصة بحزمة التثبيت.

3. في نافذة خصائص حزمة المُثبت، انقر فوق **إعدادات** ← **خيارات متقدمة**.

4. في القسم **User registration as a device owner (Linux only)**، قم بتشغيل الخيار **Allow running the user registration utility after Network Agent installation**، ثم انقر فوق **حفظ**.

يمكن تشغيل الأداة المساعدة لتسجيل المستخدم كمالك للجهاز عبر سطر الأوامر على جهاز العميل.

لتسجيل مستخدم كمالك لجهاز Linux على الجهاز العميل:

1. نفذ الأمر التالي في سطر الأوامر على الجهاز العميل:

```
opt/kaspersky/klnagent64/bin/nagregister -set_owner/ $
```

2. أدخل اسم المستخدم وكلمة المرور إذا طُلب منك ذلك.

   إذا تم تضمين تسجيل الدخول وكلمة المرور في ملف الإجابة أو حزمة المُثبت الخاصة بعميل الشبكة، فنفذ الأمر التالي في سطر الأوامر على الجهاز العميل:

```
opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended/ $
```

إذا تم تضمين المستخدم في مجموعة أمان داخلية، فيجب أن يحتوي تسجيل الدخول على اسم المستخدم.

إذا تم تضمين المستخدم في مجموعة أمان Active Directory، فيجب أن يحتوي تسجيل الدخول على اسم المستخدم واسم المجال.

إذا تم تشغيل التحقق بخطوتين للمستخدم، فيجب عليك إدخال كلمة المرور لمرة واحدة المعتمدة على الوقت (TOTP) من التطبيق.

سيتم تسجيل المستخدم كمالك للجهاز.

حذف مستخدم أو مجموعة أمان

لا يمكنك حذف إلا المستخدمين الداخليين أو مجموعات الأمان الداخلية.

لحذف مستخدم أو مجموعة أمان:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users** أو **Groups**.

2. حدد خانة الاختيار الموجودة بجوار المستخدم أو مجموعة الأمان التي ترغب في حذفها.

3. انقر على **Delete**.

4. في النافذة التي يتم فتحها، انقر على **OK**.

يتم حذف المستخدم أو مجموعة الأمان.

تغيير كلمة المرور لحساب مستخدم

قد تحتاج إلى تغيير كلمة المرور لحسابك الخاص أو لحساب مستخدم آخر إذا كانت صلاحية كلمة المرور الحالية على وشك الانتهاء أو إذا كنت تريد تغييرها إلى كلمة مرور أكثر أمانًا.

يجب أن تتوافق كلمة المرور مع القواعد التالية:

- يجب أن يتراوح طول كلمة المرور من 8 إلى 256 حرفًا.
- يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
  - الأحرف الكبيرة (A-Z)
  - الأحرف الصغيرة (a-z)
  - الأعداد (0-9)
  - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

تغيير كلمة المرور لحسابك الخاص

لتحرير كلمة المرور لحسابك:

1. في القائمة الرئيسية، انتقل إلى إعدادات حسابك ثم حدد **Change password**.

2. أدخل كلمة المرور الحالية، ثم حدد كلمة المرور الجديدة للاتصال بـ Kaspersky Security Center.

   لرؤية كلمة المرور التي تم إدخالها، انقر فوق 👁.

3. إذا كان حسابك محميًا ضد التعديل غير المصرح به، فيجب عليك التأكد من امتلاكك للأذونات اللازمة لتغيير هذا الحساب. في النافذة **Account protection**، حدد بيانات اعتماد حسابك الخاص أو الحساب الذي يحتوي على تعديل قوائم التحكم في الوصول إلى الكائنات في منطقة الوظائف الميزات العامة: أذونات المستخدم.

4. إذا تم تمكين التحقق بخطوتين للحساب الذي استخدمته في الخطوة السابقة، فأدخل رمز الأمان الذي تم إنشاؤه بواسطة تطبيق المصادقة على الجهاز المحمول.

تغيير كلمة المرور لحساب المستخدم الداخلي

لتحرير كلمة المرور لحساب مستخدم داخلي:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users**.

2. انقر على اسم حساب المستخدم الذي ترغب في تحريره.

3. في نافذة إعدادات المستخدم التي تفتح، في علامة التبويب **General**، انقر فوق الزر **Change password**.

4. قم بتعيين كلمة مرور جديدة لاتصال المستخدم بـ Kaspersky Security Center.

   لرؤية كلمة المرور التي تم إدخالها، انقر فوق 👁.

5. إذا لزم الأمر، قم بتمكين الخيار **User must change password at first sign-in** لفرض تغيير كلمة المرور عند مصادقة المستخدم التالية.

6. إذا كان حساب المستخدم محميًا ضد التعديل غير المصرح به، فيجب عليك التأكد من امتلاكك للأذونات اللازمة لتغيير هذا الحساب. في النافذة **Account protection**، حدد بيانات اعتماد الحساب الذي يحتوي على حق تعديل قوائم التحكم في الوصول للكائنات في منطقة الوظائف الميزات العامة: أذونات المستخدم.

7. إذا تم تمكين التحقق بخطوتين للحساب الذي استخدمته في الخطوة السابقة، فأدخل رمز الأمان الذي تم إنشاؤه بواسطة تطبيق المصادقة على الجهاز المحمول.

تكوين خيارات تغيير كلمة مرور باستخدام علامات الخادم

يمكنك استخدام الأداة المساعدة klscflag لتكوين تغيير كلمة المرور باستخدام الأوامر التالية:

- تكوين فترة تغيير كلمة المرور (العلامة `LP_SplPwdChangePeriodDays`)

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -
< rotation_period > v
```

  حيث < <rotation_period> > فترة زمنية بالأيام تنتهي بعدها صلاحية كلمة مرور المستخدم. القيم الممكنة: 0–730. إذا كانت قيمة المعلمة 0، فسيتم تعطيل تدوير كلمة المرور.

- تكوين وقت التحذير الأولي بشأن الحاجة إلى تغيير كلمة المرور (العلامة `LP_SplPwdChangeNotificationHours`)

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours
< warning_time > -t d -v
```

  حيث < `warning_time` > فترة زمنية بالساعات قبل انتهاء صلاحية كلمة مرور المستخدم. وخلال هذا الوقت، يتم عرض إشعار حول الحاجة إلى تغيير كلمة المرور. القيم الممكنة: 0–17520. إذا كانت قيمة المعلمة 0، فسيكون وقت التحذير 25 في المائة من فترة تدوير كلمة المرور.

- تحديد القيمة الافتراضية للخيار **User must change password at first sign-in** option (علامة `LP_SplPwdForceChange`)

```
klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v
< value >
```

  حيث القيم الممكنة لعلامة < `value` >:

  `1` - يتم تمكين الخيار **User must change password at first sign-in**.

  `0` - يتم تعطيل الخيار **User must change password at first sign-in**.

لعرض قيمة العلامة الحالية، قم بتشغيل الأمر التالي:

```
t d- < flag > klscflag.exe -fget -pv .core/.independent -s KLLIM -n
```

حيث < flag > هي العلامة LP_SplPwdChangePeriodDays أو LP_SplPwdChangeNotificationHours أو LP_SplPwdForceChange.

إنشاء دور للمستخدم

لإنشاء دور للمستخدم:

1. في القائمة الرئيسية، انتقل إلى **Roles** ← **Users & roles**.
2. انقر على **Add**.
3. في نافذة **New role name** التي تفتح، أدخل اسم الدور الجديد.
4. انقر على **OK** لتطبيق التغييرات.
5. في نافذة خصائص الدور التي تفتح، قم بتغيير إعدادات الدور:
   - في تبويب **General**، قم بتحرير اسم الدور.
     لا يمكنك تحرير اسم دور محدد مسبقًا.
   - في تبويب **Settings**، قم بتحرير نطاق الدور والسياسات وملفات التعريف المرتبطة بالدور.
   - في تبويب **Access rights**، قم بتحرير حقوق الوصول إلى تطبيقات Kaspersky.
6. انقر على **Save**لحفظ التغييرات.

يظهر الدور الجديد في قائمة أدوار المستخدم.

تحرير دور المستخدم

لتحرير دور مستخدم:

1. في القائمة الرئيسية، انتقل إلى **Roles** ← **Users & roles**.
2. انقر على اسم الدور التي ترغب في تحريره.
3. في نافذة خصائص الدور التي تفتح، قم بتغيير إعدادات الدور:
   - في تبويب **General**، قم بتحرير اسم الدور.
     لا يمكنك تحرير اسم دور محدد مسبقًا.
   - في تبويب **Settings**، قم بتحرير نطاق الدور والسياسات وملفات التعريف المرتبطة بالدور.
   - في تبويب **Access rights**، قم بتحرير حقوق الوصول إلى تطبيقات Kaspersky.
4. انقر على **Save**لحفظ التغييرات.

يظهر الدور المحدث في قائمة أدوار المستخدم.

تحرير نطاق دور المستخدم

نطاق دور المستخدم هو مجموعة من المستخدمين ومجموعات الإدارة. لا تنطبق الإعدادات المرتبطة بدور مستخدم إلا على الأجهزة التي تنتمي إلى المستخدمين الذين يملكون هذا الدور، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

لإضافة مستخدمين ومجموعات أمان ومجموعات إدارة إلى نطاق دور المستخدم، يمكنك استخدام إحدى الطرق التالية:

الطريقة الأولى:

1. في القائمة الرئيسية، انتقل الى **Users & groups** ← **Users & roles**، ثم حدد علامة التبويب **Users** أو **Groups**.
2. حدد خانات الاختيار الموجودة بجوار المستخدمين أو مجموعات الأمان التي ترغب في إضافتها إلى نطاق دور المستخدم.
3. انقر على زر **Assign role**.
   سيبدأ معالج تعيين الدور. انتقل عبر المعالج باستخدام زر **Next**.
4. في خطوة **Select role**، حدد دور المستخدم الذي تريد تعيينه.
5. في خطوة **Define scope**، حدد مجموعة الإدارة التي ترغب في إضافتها إلى نطاق دور المستخدم.
6. انقر على الزر **Assign role** لإغلاق النافذة.

تتم إضافة المستخدمين المحددين أو مجموعات الأمان المحددة ومجموعة الإدارة المحددة إلى نطاق دور المستخدم.

الطريقة الثانية:

1. في القائمة الرئيسية، انتقل إلى **Roles** ← **Users & roles**.
2. انقر على اسم الدور الذي ترغب في تحديد نطاقه.
3. في نافذة خصائص السياسة التي تفتح، حدد تبويب **Settings**.
4. في قسم **Role scope**، انقر على **Add**.
   سيبدأ معالج تعيين الدور. انتقل عبر المعالج باستخدام زر **Next**.
5. في خطوة **Define scope**، حدد مجموعة الإدارة التي ترغب في إضافتها إلى نطاق دور المستخدم.
6. في خطوة **Select users**، حدد المستخدمين ومجموعات الأمان التي ترغب في إضافتها إلى نطاق دور المستخدم.
7. انقر على الزر **Assign role** لإغلاق النافذة.
8. انقر على زر **إغلاق** (×) لإغلاق نافذة خصائص الدور.

تتم إضافة المستخدمين المحددين أو مجموعات الأمان المحددة ومجموعة الإدارة المحددة إلى نطاق دور المستخدم.

الطريقة الثالثة:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **Access rights**، حدد خانة الاختيار المجاورة لاسم المستخدم أو مجموعة الأمان التي تريد إضافتها إلى نطاق دور المستخدم، ثم انقر فوق الزر **Roles**.

لا يمكنك تحديد عدة مستخدمين أو مجموعات أمان في الوقت نفسه. وإذا حددت أكثر من عنصر واحد، فسيتم تعطيل الزر **Roles**.

3. في النافذة **Roles**، حدد دور المستخدم الذي تريد تعيينه، ثم طبق واحفظ التغييرات.

تتم إضافة المستخدمين المحددين أو مجموعات الأمان المحددة إلى نطاق دور المستخدم.

حذف دور مستخدم

لحذف دور مستخدم:

1. في القائمة الرئيسية، انتقل إلى **Users & roles** ← **Roles**.

2. حدد خانة الاختيار الموجودة بجوار اسم الدور الذي ترغب في حذفه.

3. انقر على **Delete**.

4. في النافذة التي يتم فتحها، انقر على **OK**.

يتم حذف دور المستخدم.

ربط ملفات تعريف السياسة بأدوار

يمكنك ربط أدوار المستخدم بملفات تعريف السياسة. في هذه الحالة، تستند قاعدة التفعيل لملف تعريف السياسة هذا على الدور: يصبح ملف تعريف السياسة نشطًا لمستخدم له الدور المحدد.

على سبيل المثال: تمنع السياسة تشغيل أي برنامج تحديد الموقع GPS على جميع الأجهزة في مجموعة إدارة. يلزم وجود برنامج تحديد الموقع GPS على جهاز واحد في مجموعة الإدارة "المستخدمين"، وهو الجهاز المملوك لمستخدم يعمل بوظيفة "ساعٍ". يمكنك في هذه الحالة تعيين دور "ساعي" إلى مالكه، وبعدها إنشاء ملف تعريف سياسة يسمح بتشغيل برامج تحديد الموقع GPS فقط على الأجهزة التي تم تخصيص دور "ساعي" إلى مالكيها. يتم الاحتفاظ بجميع إعدادات السياسة الأخرى. لن يتم السماح إلا للمستخدمين بدور "ساعي" أن يقوموا بتشغيل برنامج تحديد الموقع GPS. في حال تخصيص دور "ساعي" لأحد العاملين في وقتٍ لاحق، يمكن للعامل الجديد كذلك تشغيل أي برنامج تحديد الموقع على جهاز المؤسسة لديك. سيستمر حظر تشغيل برنامج تحديد الموقع GPS على الأجهزة الأخرى في مجموعة الإدارة نفسها.

لربط دور بملف تعريف سياسة:

1. في القائمة الرئيسية، انتقل إلى **Users & roles** ← **Roles**.

2. انقر على اسم الدور التي ترغب في رابطه بملف تعريف سياسة.

ستفتح نافذة خصائص الدور مع تحديد تبويب **General**.

3. حدد تبويب **Settings** ثم مرر لأسفل حتى تصل إلى قسم **Policies & profiles**.

4. انقر على **Edit**.

5. لربط الدور مع:

- **ملف تعريف سياسة موجود**: انقر على أيقونة الرتبة العسكرية (⟨) الموجودة بجوار اسم السياسة المطلوب ثم حدد خانة الاختيار الموجودة بجوار الملف الذي ترغب في ربط الدور به.
- **ملف تعريف سياسة جديد**:

a. حدد خانة الاختيار الموجودة بجوار السياسة التي ترغب في إنشاء ملف تعريف لها.

b. انقر على**New policy profile** .

c. حدد اسمًا لملف التعريف الجديد وقم بتكوين إعدادات ملف التعريف.

d. انقر على زر **Save**.

e. حدد خانة الاختيار الموجودة بجوار ملف التعريف الجديد.

6. انقر على **Assign to role** .

بهذا يتم ربط ملف التعريف بالدور ويظهر في خصائص الدور. ينطبق ملف التعريف تلقائيًا بأي جهاز مخصص لمالكه دور.

نشر أدوار المستخدم على خوادم الإدارة الثانوية

بشكلٍ افتراضي، تكون قوائم أدوار المستخدم الخاصة بخوادم الإدارة الأساسية والتابعة مستقلة. يمكنك تكوين التطبيق ليقوم تلقائيًا بنشر أدوار المستخدم التي تم إنشاؤها على خادم الإدارة الرئيسي لجميع خوادم الإدارة الثانوية. يمكن أيضًا نشر أدوار المستخدم من خادم إدارة تابع إلى خوادم الإدارة الثانوية الخاصة به.

قم بما يلي لنشر أدوار المستخدم من خادم الإدارة الرئيسي إلى خوادم الإدارة الثانوية:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

ستفتح نافذة خصائص خادم الإدارة مع تحديد علامة التبويب **General**.

2. انتقل إلى القسم **Hierarchy of Administration Servers**.

3. قم بتمكين خيار **Relay list of roles to secondary Administration Servers**، ثم انقر فوق الزر **Save**.

يقوم التطبيق بنسخ أدوار المستخدم لخادم الإدارة الرئيسي إلى خوادم الإدارة الثانوية.

عندما يتم تمكين الخيار **Relay list of roles to secondary Administration Servers** ويتم نشر أدوار المستخدمين، لا يمكن تحريرها أو حذفها على خوادم الإدارة الثانوية. عند قيامك بإنشاء دور جديد أو تحرير دور موجود بالفعل على خادم الإدارة الرئيسي، يتم نسخ التغييرات تلقائيًا إلى خوادم الإدارة الثانوية. عند قيامك بحذف دور مستخدم على خادم الإدارة الرئيسي، يظل هذا الدور على خوادم الإدارة الثانوية بعد ذلك، ولكن يمكن تحريره أو حذفه.

يتم عرض الأدوار التي يتم نشرها إلى خادم الإدارة الثانوي من الخادم الرئيسي عن طريق علامات اختيار باللون الأخضر (✓). لا يمكنك تحرير هذه الأدوار على خادم الإدارة الثانوي.

إذا قمت بإنشاء دور على خادم الإدارة الرئيسي، وهناك دور بنفس الاسم على خادم الإدارة الثانوي له، فإنه يتم نسخ الدور الجديد إلى خادم الإدارة الثانوي مع إضافة الفهرس إلى اسمه، على سبيل المثال، ~~1، ~~2 (يمكن أن يكون المؤشر عشوائيًا).

إذا قمت بتعطيل الخيار **Relay list of roles to secondary Administration Servers**، فإن جميع أدوار المستخدمين الأخرى تظل موجودة على خوادم الإدارة الثانوية، لكنها تصبح مستقلة عن تلك الأدوار الموجودة على خادم الإدارة الرئيسي. بعد أن تصبح أدوار المستخدم مستقلة، يمكن تحرير أو حذف أدوار المستخدم الموجودة على خوادم الإدارة الثانوية.

تغيير كلمة مرور الحساب

يمكنك تغيير كلمة مرور الحساب المحلي، على سبيل المثال، عندما ينسى المستخدم كلمة مرور الحساب المحلي أو لإجراء تغيير كلمة مرور مجدول.

سيتم تطبيق تغيير كلمة المرور حتى لو لم يقم المستخدم بتسجيل الدخول إلى الحساب. ويمكنك أيضًا تغيير كلمة المرور لحساب الجذر المحلي.

لا يمكن تنفيذ هذه المهمة إلا على أجهزة Linux.

لتغيير كلمة مرور الحساب المحلي على أجهزة محددة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.
2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة.
3. في الحقل **Task type** ، حدد **Change account password (Linux only)**.
4. حدد أحد الخيارات التالية:

   - **Assign task to an administration group**

     يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

     على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

     إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

   - **Specify device addresses manually or import addresses from a list**

     يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

     قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

   - **Assign task to a device selection**

     يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

     على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

   يتم إنشاء مهمة تغيير كلمة مرور الحساب (Linux فقط) للأجهزة المحددة. إذا حددت الخيار **Assign task to an administration group**، فستكون المهمة مجموعة واحدة.
5. في خطوة **Task scope**، حدد مجموعة الإدارة، أو الأجهزة ذات العناوين المحددة ، أو تحديد الجهاز.

   تعتمد الإعدادات المتاحة على الخيار المحدد في الخطوة السابقة.
6. في الخطوة **Enter account name and new password**، حدد الإعدادات التالية:

   - في الحقل **Account name**، حدد اسم الحساب الذي تريد تغيير كلمة المرور الخاصة به.
   - في الحقل **New password**، حدد كلمة المرور التي سيتم تعيينها للحساب المحدد في الحقل السابق.

     لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

- إذا لزم الأمر، حدد خانة الاختيار **Set as a one-time password (the user must change the password after the first login)**.

- **Set as a one-time password (the user must change the password after the first login)**

إذا تم تحديد خانة الاختيار هذه، فستتم مطالبة المستخدم بتعيين كلمة مرور جديدة بعد تسجيل الدخول لأول مرة.

إذا تم مسح خانة الاختيار هذه، فلن يُطلب من المستخدم تعيين كلمة مرور جديدة بعد تسجيل الدخول لأول مرة.

تكون خانة الاختيار غير محددة بشكل افتراضي.

7. في خطوة **إنهاء عملية إنشاء المهمة**، انقر فوق الزر " **إنهاء** " لإنشاء المهمة وإغلاق المعالج.

إذا قمت بتفعيل خيار **Open task details when creation is complete**، ستفتح نافذة إعدادات المهمة. في هذه النافذة، يمكنك التحقق من معلمات المهمة أو تعديلها أو تكوين جدول بدء المهمة، إذا لزم الأمر.

8. في قائمة المهام، حدد المهمة التي قمت بإنشائها، ثم انقر فوق **ابدأ** .

أو بدلاً من ذلك، انتظر حتى تبدأ المهمة وفقًا للجدول الذي حددته في إعدادات المهمة.

عند اكتمال مهمة تغيير كلمة مرور الحساب، سيتم تغيير كلمة المرور للحساب المحلي المحدد على الأجهزة المحددة.

لضمان التشغيل الصحيح لمهام تغيير كلمة مرور الحساب، يجب تعطيل SELinux على جهاز المستخدم.

إلغاء حقوق المسؤول المحلي

يمكنك إلغاء حقوق المسؤول المحلي من الحسابات. ويتيح لك هذا طبقة إضافية من التحكم في حسابات المستخدم. على سبيل المثال، يمكنك إلغاء حقوق المسؤول المحلي بعد اكتمال التعيين لمرة واحدة.

عند تشغيل هذه المهمة، يتم التحقق من الحساب المحلي المحدد لمعرفة ما إذا كان ينتمي إلى مجموعات المسؤولين المحليين. ويتم تعريف هذه المجموعات في إعدادات سياسة عميل الشبكة. ويمكنك تخصيص قائمة مجموعات المسؤولين المحليين في إعدادات سياسة عميل الشبكة. ويمكنك أيضًا التحقق من قائمة حسابات المستخدمين المتميزين باستخدام **الإبلاغ عن مستخدمي الأجهزة المميزة (Linux فقط)**.

لا يمكن تنفيذ هذه المهمة إلا على أجهزة Linux.

لإلغاء حقوق المسؤول المحلي على أجهزة معينة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

سيبدأ معالج المهمة الجديدة.

3. في الحقل **Task type**، حدد **Revoke local administrator rights (Linux only)**.

4. حدد أحد الخيارات التالية:

- **Assign task to an administration group**

يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة. يمكنك تحديد أحد المجموعات الحالية أو إنشاء واحدة جديدة.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة إرسال رسالة للمستخدمين في حال كانت الرسالة محددة للأجهزة المضمنة في مجموعة إدارة محددة.

إذا تم تعيين مهمة إلى مجموعة إدارة، فلن يتم عرض علامة التبويب **الأمان** في نافذة خصائص المهمة لأن مهام المجموعة تخضع لإعدادات الأمان الخاصة بالمجموعات التي تنطبق عليها.

- **Specify device addresses manually or import addresses from a list**

يمكنك تحديد أسماء NetBIOS وأسماء DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.

قد ترغب في استخدام هذا الخيار لتنفيذ مهمة لشبكة فرعية محددة. على سبيل المثال، قد ترغب بتثبيت تطبيق معين على أجهزة المحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

- **Assign task to a device selection**

يتم تعيين المهمة إلى الأجهزة المضمنة في تحديد الجهاز. يمكنك تحديد أحد مجموعات التحديد الحالية.

على سبيل المثال، قد ترغب في استخدام هذا الخيار لتشغيل مهمة على أجهزة باستخدام إصدار نظام تشغيل محدد.

تم إنشاء مهمة إلغاء حقوق المسؤول المحلي (Linux فقط) للأجهزة المحددة. إذا حددت الخيار **Assign task to an administration group**، فستكون المهمة مجموعة واحدة.

5. في خطوة **Task scope**، حدد مجموعة الإدارة، أو الأجهزة ذات العناوين المحددة ، أو تحديد الجهاز.

تعتمد الإعدادات المتاحة على الخيار المحدد في الخطوة السابقة.

6. في هذه الخطوة من المعالج، حدد الإعدادات التالية:

- في مجموعة إعدادات **Operating mode**، حدد وضع التشغيل:

- **Revoke local administrator rights from listed accounts**

إذا تم تحديد هذا الخيار، سيتم إلغاء حقوق المسؤول المحلي من الحسابات المحلية المحددة.

يتم تحديد هذا الخيار افتراضيًا.

- **Exclude listed accounts from local administrator rights revocation**

إذا تم تحديد هذا الخيار، سيتم إلغاء حقوق المسؤول المحلي من جميع الحسابات المحلية، باستثناء الحسابات المحددة.

لا يتم تحديد هذا الخيار افتراضيًا.

- حدد الحسابات المحلية:

- انقر على **Add**.

- في النافذة التي تفتح، نفذ ما يلي:

- في الحقل **Account name**، حدد اسم الحساب المحلي.

- في مجموعة إعدادات **Account action** (متوفر فقط إذا تم تحديد الخيار **Revoke local administrator rights from listed accounts**)، حدد الإجراء.

- **Keep account**

إذا تم تحديد هذا الخيار، فلن يتم حذف الحساب المحلي بعد إلغاء حقوق المسؤول المحلي.

يتم تحديد هذا الخيار افتراضيًا.

- **Delete account**

إذا تم تحديد هذا الخيار، سيتم حذف الحساب المحلي بغض النظر عما إذا كان لديه حقوق المسؤول المحلي أم لا.

لا يتم تحديد هذا الخيار افتراضيًا.

7. في خطوة **إنهاء عملية إنشاء المهمة**، انقر فوق الزر " **إنهاء** " لإنشاء المهمة وإغلاق المعالج.

إذا قمت بتفعيل خيار **Open task details when creation is complete**، ستفتح نافذة إعدادات المهمة. في هذه النافذة، يمكنك التحقق من معلمات المهمة أو تعديلها أو تكوين جدول بدء المهمة، إذا لزم الأمر.

8. في قائمة المهام، حدد المهمة التي قمت بإنشائها، ثم انقر فوق **ابدأ** .

أو بدلاً من ذلك، انتظر حتى تبدأ المهمة وفقًا للجدول الذي حددته في إعدادات المهمة.

عند اكتمال مهمة إلغاء حقوق المسؤول المحلي، سيتم إلغاء حقوق المسؤول المحلي من الحسابات المحلية المحددة على الأجهزة المحددة.

إدارة مراجعات الكائن

يحتوي هذا القسم على معلومات حول إدارة مراجعات الكائنات. يتيح لك Kaspersky Security Center تتبع تعديل الكائن. في كل مرة تحفظ فيها التغييرات التي أُجريت على الكائن، يتم إنشاء مراجعة. لكل مراجعة رقم.

تشتمل كائنات التطبيق التي تدعم إدارة المراجعة على:

- خصائص خادم الإدارة
- السياسات
- المهام
- مجموعات الإدارة
- حسابات المستخدمين
- حزم التثبيت

يمكنك تنفيذ الإجراءات التالية على مراجعات الكائنات:

- عرض مراجعة محددة (متاح فقط للسياسات)
- التراجع عن التغييرات التي أُجريت على كائن في مراجعة محددة
- حفظ المراجعات كملف JSON (متاح فقط للسياسات)

في نافذة خصائص أي كائن يدعم إدارة المراجعة، يعرض القسم **سجل المراجعة** قائمة مراجعات الكائنات تتضمن التفاصيل التالية:

- **Revision** — رقم مراجعة الكائن.
- **Time** — تاريخ ووقت تعديل الكائن.
- **User** — اسم المستخدم الذي قام بتعديل الكائن.
- **User device IP address**—عنوان IP الخاص بالجهاز الذي تم تعديل الكائن منه.
- **Web Console IP address**—عنوان IP لتطبيق Kaspersky Security Center Web Console الذي تم تعديل الكائن باستخدامه.
- **Action** — الإجراء الذي تم تنفيذه على الكائن.
- **Description** — وصف المراجعة ذات الصلة بالتغيير الذي أُتم إجراؤه على إعدادات الكائن.

  تكون خانة وصف مراجعة الكائن فارغة بشكل افتراضي. ولإضافة وصف إلى مراجعة، حدد المراجعة ذات الصلة وانقر فوق الزر **Edit description**. في النافذة التي تفتح، أدخل نصًا لوصف المراجعة.

التراجع عن كائن إلى مراجعة سابقة

وإذا لزم الأمر، يمكنك التراجع عن التغييرات التي تم إجراؤها على الكائن. على سبيل المثال، قد يلزمك إعادة إعدادات سياسة إلى حالتها في تاريخ محدد.

للتراجع عن التغييرات التي تم إجراؤها على أحد الكائنات:

1. في نافذة خصائص الكائن، افتح تبويب **Revision history**.
2. في قائمة مراجعات الكائنات، حدد المراجعة التي ترغب في التراجع عن تغييراتها.
3. انقر على زر **Roll back** .
4. انقر على **OK** لتأكيد العملية.

تمت إعادة الكائن حاليًا إلى المراجعة المحددة. تعرض قائمة مراجعات الكائنات سجلًا بالإجراء الذي تم تنفيذه. يعرض وصف المراجعة معلومات حول رقم المراجعة التي قمت بإعادة الكائن إليها.

عملية التراجع غير متاحة إلا لكائنات السياسة والمهمة.

إضافة وصف للمراجعة

يتيح لك Kaspersky Security Center تتبع تعديل الكائن. في كل مرة تحفظ فيها التغييرات التي أُجريت على الكائن، يتم إنشاء مراجعة. لكل مراجعة رقم.

يمكنك إضافة وصف للمراجعة لتبسيط البحث عن المراجعات في القائمة.

لإضافة وصف لمراجعة:

1. في نافذة خصائص الكائن، افتح علامة التبويب **Revision history**.
2. في قائمة مراجعات الكائنات، حدد المراجعة التي تحتاج إلى إضافة وصف لها.
3. انقر على زر **Edit description**.
   تفتح نافذة **Description**.
4. في النافذة **Description**، أدخل نصًا لوصف المراجعة.
   تكون خانة وصف مراجعة الكائن فارغة بشكل افتراضي.
5. احفظ وصف المراجعة.

يضاف الوصف لمراجعة الكائن.

عرض وحفظ مراجعة سياسة

يتيح لك Kaspersky Security Center عرض التعديلات التي تم إجراؤها على السياسة خلال فترة معينة، بالإضافة إلى حفظ معلومات حول هذه التعديلات في ملف.

يتوفر عرض وحفظ مراجعة السياسة إذا كان البرنامج الإضافي للإدارة على الويب يدعم هذه الوظيفة.

لعرض مراجعة السياسة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. انقر فوق سياسة المراجعة التي تريد عرضها، ثم انتقل إلى قسم **Revision history** .
3. في قائمة مراجعات السياسة، انقر فوق رقم المراجعة التي تريد عرضها.

إذا كان حجم المراجعة أكبر من 10 ميجا بايت، فلن تتمكن من مشاهدتها باستخدام Kaspersky Security Center Web Console. وسيُطلب منك حفظ المراجعة المحددة في ملف JSON.

إذا كان حجم المراجعة لا يتجاوز 10 ميجا بايت، فسيتم عرض تقرير بتنسيق HTML مع إعدادات مراجعة السياسة المحددة. نظرًا لأنه يتم عرض التقرير في نافذة منبثقة، تأكد من السماح بالنوافذ المنبثقة في المستعرض الخاص بك.

لحفظ مراجعة السياسة في ملف JSON،

في قائمة مراجعات السياسة، حدد المراجعة التي تريد حفظها، ثم انقر فوق **حفظ في ملف**.

يتم حفظ المراجعة في ملف JSON.

حذف الكائنات

يوفر هذا القسم معلومات عن حذف الكائنات.

يمكنك حذف الكائنات، بما يشمل الكائنات التالية:

- السياسات
- المهام
- حزم التثبيت
- خوادم الإدارة الافتراضية
- المستخدمين
- مجموعات الأمان
- مجموعات الإدارة

لحذف كائن:

1. افتح القسم المطلوب من Kaspersky Security Center Web Console، ثم حدد الكائن.

2. في شريط الأدوات، انقر فوق الزر **Delete**.

3. في النافذة التي تفتح انقر على زر **OK** لتأكيد اختيارك.

سيتم حذف الكائن المحدد.

عند قيامك بحذف كائن ما، تظل المعلومات حول هذا الكائن في قاعدة البيانات. تكون فترة تخزين المعلومات حول الكائنات المحذوفة هي نفس فترة التخزين لمراجعات الكائن (الفترة الموصى بها هي 90 يومًا). لا يمكنك تغيير مدّة التخزين إلا في حالة حصولك على إذن **التعديل** في نطاق حقوق **الكائنات المحذوفة**.

حول حذف أجهزة العميل

عندما تحذف جهازًا مُدارًا من مجموعة إدارة، ينقل التطبيق الجهاز إلى مجموعة الأجهزة غير المخصصة. بعد حذف الجهاز، تظل تطبيقات Kaspersky المُثبتة - عميل الشبكة وأي تطبيق أمان، مثل Kaspersky Endpoint Security - على الجهاز.

يتعامل Kaspersky Security Center مع الأجهزة الموجودة في مجموعة الأجهزة غير المخصصة وفقًا للقواعد التالية:

- إذا كونت قواعد نقل الجهاز ولبى الجهاز معايير قاعدة النقل، سيتم نقل الجهاز تلقائيًا إلى مجموعة إدارة وفقًا للقاعدة.
- يتم تخزين الجهاز في مجموعة الأجهزة غير المخصصة وإزالته تلقائيًا من المجموعة وفقًا لقواعد الاحتفاظ بالجهاز .

لا تؤثر قواعد الاحتفاظ بالجهاز على الأجهزة التي تحتوي على محرك أقراص واحد أو أكثر مشفر باستخدام تشفير القرص بالكامل. لا يتم حذف هذه الأجهزة تلقائيًا، يمكنك حذفها يدويًا فقط. إذا كنت بحاجة إلى حذف جهاز يحتوي محرك أقراص مشفر، فقم أولاً بفك تشفير محرك الأقراص، ثم احذف الجهاز.

وعند حذف جهاز يحتوي على محرك أقراص مشفر، يتم أيضًا حذف البيانات المطلوبة لفك تشفير محرك الأقراص. إذا حددت خانة الاختيار **أفهم المخاطر وأريد حذف الجهاز المحدد (الأجهزة المحددة)** في نافذة التأكيد التي تفتح عند حذف هذه الأجهزة (إما من مجموعة **Unassigned devices** أو **Managed Devices**)، فهذا يعني أنك على دراية بحذف البيانات اللاحق.

لفك تشفير محرك الأقراص، يجب استيفاء الشروط التالية:

- تمت إعادة توصيل الجهاز بخادم الإدارة لاستعادة البيانات المطلوبة لفك تشفير محرك الأقراص.
- يتذكر مستخدم الجهاز كلمة مرور فك التشفير.
- لا يزال تطبيق الأمان الذي تم استخدامه لتشفير محرك الأقراص، مثل Kaspersky Endpoint Security for Windows، مُثبتًا على الجهاز.

وفي حالة تشفير محرك الأقراص بواسطة تقنية تشفير القرص من Kaspersky، يمكنك أيضًا محاولة استعادة البيانات باستخدام FDERT Restore Utility.

في VDI، إذا كان لديك جهاز يحتوي على محركات أقراص مشفرة، يتم حذف المعلومات الموجودة على محرك الأقراص المشفر بعد حذف الجهاز.

عندما تحذف جهازًا من مجموعة الأجهزة غير المخصصة يدويًا، يزيل التطبيق الجهاز من القائمة. بعد حذف الجهاز، تظل تطبيقات Kaspersky المُثبتة على الجهاز (إن وجدت). بعد ذلك، إذا كان الجهاز لا يزال مرئيًا لخادم الإدارة وكونت استقصاء شبكة منتظم، يكتشف Kaspersky Security Center الجهاز أثناء استقصاء الشبكة ويضيفه مرة أخرى إلى مجموعة الأجهزة غير المخصصة. لذلك، من المعقول حذف الجهاز يدويًا فقط إذا كان الجهاز غير مرئي لخادم الإدارة.

(KSN) Kaspersky Security Network

يصف هذا القسم كيفية استخدام بنية أساسية للخدمات عبر الإنترنت تحمل الاسم Kaspersky Security Network (KSN). يوفر القسم التفاصيل حول KSN، وكذلك تعليمات حول كيفية تمكين KSN، وتكوين الوصول إلى KSN، وعرض إحصائيات استخدام خادم وكيل KSN.

وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية)، بالإضافة إلى وظيفة KSN التي قد لا تكون متاحة في البرنامج في الولايات المتحدة الأمريكية.

حول KSN

تعد Kaspersky Security Network (KSN) بنية أساسية للخدمات عبر الإنترنت والتي توفر الوصول إلى قاعدة معارف Kaspersky عبر الإنترنت، والمتضمنة بدورها معلومات حول سمعة الملفات وموارد الويب والبرامج. ويعد استخدام البيانات من Kaspersky Security Network ضمانًا لسرعة استجابات تطبيقات Kaspersky عند مواجهة تهديدات، كما يعمل ذلك على تحسين أداء بعض مكونات الحماية ويقلل من خطر وقوع الحالات الإيجابية الخاطئة. يتيح KSN لك استخدام قواعد بيانات صيت Kaspersky لاسترداد المعلومات حول التطبيقات المثبتة على الأجهزة المُدارة.

يدعم Kaspersky Security Center حلول البنية التحتية التالية:

- KSN هي حل يسمح لك بتبادل المعلومات مع Kaspersky Security Network. بالمشاركة في KSN، فإنك توافق على إرسال معلومات بشكل تلقائي إلى Kaspersky حول تشغيل تطبيقات Kaspersky المثبتة على أجهزة العميل والأجهزة المُدارة عبر Kaspersky Security Center. يتم نقل المعلومات وفقًا لإعدادات وصول KSN الحالية. بالإضافة إلى ذلك، يقوم محللو Kaspersky بتحليل المعلومات المستلمة وإدراجها في السمات وقواعد البيانات الإحصائية الخاصة بشبكة Kaspersky Security Network. يستخدم Kaspersky Security Center هذا الحل افتراضيًا.

- Kaspersky Private Security Network (KPSN) هي حل يتيح لمستخدمي الأجهزة المثبتة بتطبيقات Kaspersky الوصول إلى قواعد بيانات سمات Kaspersky Security Network والبيانات الإحصائية الأخرى دون إرسال البيانات إلى KSN العالمية من أجهزتهم. تم تصميم KPSN لعملاء الشركة الذين يتعذر عليهم المشاركة في Kaspersky Security Network لأحد الأسباب التالية:

  - أجهزة المستخدم غير متصلة بالإنترنت.

  - يحظر القانون نقل أي بيانات خارج الدولة أو خارج الشبكة المحلية للشركة أو تقيد سياسات أمان الشركة ذلك.

قم بإعداد إعدادات الوصول لشبكة Kaspersky Private Security Network في **KSN Proxy settings** الخاصة بنافذة خصائص خادم الإدارة.

يطالبك التطبيق بالانضمام إلى KSN أثناء تشغيل معالج البدء السريع. يمكنك البدء أو التوقف عن استخدام KSN في أي لحظة عند استخدام التطبيق.

يمكنك استخدام KSN وفق بيان KSN الذي تقرأه وتوافق عليه عندما تقوم بتمكين KSN. إذا تم تحديث بيان KSN، فسيتم عرضه لك عند ترقية إصدار من خادم الإدارة. يمكن قبول بيان KSN المحدث أو رفضه. إذا رفضته ستستمر في استخدام KSN وفق الإصدار السابق لبيان KSN الذي قد قبلته من قبل.

عند تمكين KSN، يتحقق Kaspersky Security Center من إمكانية الوصول إلى خوادم KSN. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة. يعد ذلك ضروريًا للتأكد من الحفاظ على مستوى الأمان للأجهزة المُدارة.

تتفاعل أجهزة العميل المدارة بواسطة خادم الإدارة مع KSN عبر الخادم الوكيل لشبكة KSN. يوفر الخادم الوكيل لشبكة KSN الميزات التالية:

- يمكن للأجهزة العميلة إرسال طلبات إلى KSN، والحصول على معلومات من KSN، ونقل المعلومات إلى KSN حتى لو لم يكن لديهم إمكانية الوصول المباشر إلى الإنترنت.

- يخزن خادم وكيل KSN البيانات المعالجة مؤقتًا، مما يقلل الحمل على القناة الخارجية والفترة الزمنية التي يتم قضاؤها لانتظار المعلومات التي يطلبها جهاز عميل.

يمكنك تكوين الخادم الوكيل لشبكة KSN في القسم **KSN Proxy settings** في نافذة خصائص خادم الإدارة.

تعيين الوصول إلى KSN

يمكنك إعداد الوصول إلى Kaspersky Security Network (KSN) على خادم الإدارة وعلى نقطة توزيع.

لإعداد وصول خادم الإدارة إلى KSN:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **KSN Proxy settings**.

3. قم بتبديل زر التبديل إلى وضع **Enable KSN Proxy on Administration Server Enabled**.

   إذا تم تمكين هذا الخيار، يرسل الخادم الوكيل لشبكة KSN البيانات إلى KSN لزيادة كفاءة مكونات Kaspersky Security Center وتحسين أداء تطبيقات Kaspersky. يتم إرسال البيانات من الأجهزة العميلة إلى KSN وفقًا لسياسة Kaspersky Endpoint Security، والتي تكون نشطة على الأجهزة العميلة تلك. إذا تم إلغاء خانة الاختيار هذه، فلن يتم إرسال أي بيانات إلى KSN من خادم الإدارة ومن الأجهزة العميلة عبر Kaspersky Security Center. ومع ذلك، يمكن للأجهزة العميلة إرسال بيانات إلى KSN مباشرة (عبر تجاوز Kaspersky Security Center)، وفقًا للإعدادات الخاصة بهم. تحدد سياسة Kaspersky Endpoint Security المفعلة على الأجهزة العميلة، البيانات التي سيتم إرسالها بشكل مباشر (عبر تجاوز Kaspersky Security Center) من هذه الأجهزة إلى KSN.

4. بدل زر التبديل إلى وضع **Use Kaspersky Security Network Enabled**.

   إذا تم تحديد هذا الخيار، فسترسل أجهزة العملاء نتائج تثبيت التصحيح إلى Kaspersky. عند تمكين هذا الخيار، تأكد من أنك قد قرأت شروط بيان KSN ووافقت عليها.

   إذا كنت تستخدم شبكة KPSN، بدل زر التبديل إلى وضع **Use Kaspersky Private Security Network Enabled** وانقر على زر **Select file with KSN Proxy settings** لتنزيل إعدادات شبكة KPSN (الملفات بالامتدادين pkcs7 وpem). وعقب تنزيل الإعدادات، تعرض الواجهة اسم المزود وجهات الاتصال، وكذلك تاريخ إنشاء الملف مع إعدادات شبكة KPSN.

> عند تمكين شبكة KPSN، انتبه إلى نقاط التوزيع التي تم تكوينها لإرسال طلبات KSN مباشرةً إلى شبكة KSN السحابية. ستواصل نقاط التوزيع المُثبَّت عليها عميل الشبكة الإصدار 11 (أو إصدار سابق) إرسال طلبات KSN إلى Cloud KSN. إذا أردت إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KPSN، قم بتمكين خيار **Forward KSN requests to Administration Server** لكل نقطة توزيع. يمكنك تمكين هذا الخيار في خصائص نقطة التوزيع أو في سياسة عميل الشبكة.

عند تبديل زر التبديل إلى وضع **Use Kaspersky Private Security Network Enabled**، ستظهر رسالة تحتوي على تفاصيل حول شبكة KPSN.

تدعم تطبيقات Kaspersky التالية شبكة KPSN:

- Kaspersky Security Center
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

في حالة تمكين شبكة KPSN في Kaspersky Security Center، تتلقى هذه التطبيقات معلومات حول دعم شبكة KPSN. وفي نافذة إعدادات التطبيق وفي القسم الفرعي **Kaspersky Security Network** الخاص بالقسم **الحماية المتقدمة من التهديد**، يتم عرض معلومات عن مزود خدمة شبكة KSN موفر شبكة KSN - شبكة KSN أو شبكة KPSN.

إذا كنت تستخدم إصدارات التطبيق الأقدم من Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 أو أقدم من Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent عند تشغيل شبكة KPSN، نوصيك باستخدام خوادم الإدارة الثانوية التي لم يتم تمكين استخدام شبكة KPSN الخاصة لها.

لا يرسل Kaspersky Security Center أي بيانات إحصائية إلى Kaspersky Security Network في حالة تكوين شبكة KPSN في القسم **KSN Proxy settings** الخاص بنافذة خصائص خادم الإدارة.

5. في حالة تكوين إعدادات خادم الوكيل في خصائص خادم الإدارة ولكن بنية الشبكة لديك تتطلب استخدام شبكة KPSN مباشرة، فقم بتمكين الخيار **Ignore proxy server settings when connecting to KPSN**. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المُدارة إلى شبكة KPSN.

6. تكوين اتصال خادم الإدارة بخدمة وكيل KSN:

- ضمن **Connection settings**، بالنسبة إلى **TCP port**، حدد رقم منفذ TCP الذي سيتم استخدامه للاتصال بخادم وكيل KSN. المنفذ الافتراضي للاتصال بخادم وكيل KSN هو 13111.
- إذا كنت تريد أن يتصل خادم الإدارة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار **Use UDP port** وحدد رقم منفذ **UDP port**. بشكل افتراضي، يتم تعطيل هذا الخيار، ويتم استخدام منفذ TCP. إذا تم تمكين هذا الخيار، فإن منفذ UDP الافتراضي للاتصال بخادم وكيل KSN هو 15111.
- إذا كنت تريد أن يتصل خادم الإدارة بخادم وكيل KSN عبر منفذ HTTPS، فقم بتمكين خيار **Use HTTPS** وحدد رقم منفذ للخيار **HTTPS through port**. بشكل افتراضي، يتم تعطيل هذا الخيار، ويتم استخدام منفذ TCP. إذا تم تمكين هذا الخيار، فإن منفذ HTTPS الافتراضي للاتصال بخادم وكيل KSN هو 17111.

7. قم بتبديل زر التبديل إلى وضع **Connect secondary Administration Servers to KSN through the primary Administration Server Enabled**.

إذا تم تحديد هذا الخيار، ستستخدم خوادم الإدارة الثانوية خادم الإدارة الأساسي كخادم وكيل KSN. إذا تم تعطيل هذا الخيار، فستتصل خوادم الإدارة الثانوية بشبكة KSN بنفسهم. وفي هذه الحالة، ستستخدم الأجهزة المدارة خوادم الإدارة الثانوية كخوادم لوكيل KSN

خوادم الإدارة الثانوية تستخدم خادم الإدارة الرئيسي كخادم وكيل إذا كان زر التبديل في الجزء الأيمن بالقسم **KSN Proxy settings** في خصائص خادم الإدارة الثانوي على وضع **Enable KSN Proxy on Administration Server Enabled**.

8. انقر على زر **Save**.

سيتم حفظ إعدادات الوصول إلى KSN.

يمكنك أيضًا إعداد وصول نقطة التوزيع لـ KSN، على سبيل المثال، إذا كنت ترغب في تقليل الحمل على خادم الإدارة. ترسل نقطة التوزيع التي تعمل كخادم عميل لشبكة KSN طلبات KSN من الأجهزة المُدارة إلى Kaspersky مباشرة دون استخدام خادم الإدارة.

لإعداد وصول نقطة التوزيع إلى Kaspersky Security Network (KSN):

1. تأكد من أن نقطة التوزيع معينة يدويًا.

2. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

3. في علامة التبويب **General**، حدد قسم **Distribution points**.

4. انقر على اسم نقطة التوزيع لفتح نافذة خصائصها.

5. في نافذة خصائص نقطة التوزيع، في قسم **KSN Proxy**، قم بتمكين خيار **Enable KSN Proxy on the distribution point side**، ثم قم بتمكين خيار **Access KSN Cloud/KPSN directly over the internet**.

6. انقر على **OK**.

ستعمل نقطة التوزيع كخادم وكيل KSN.

تمكين وتعطيل استخدام KSN

لتمكين استخدام KSN:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **KSN Proxy settings**.

3. قم بتبديل زر التبديل إلى وضع **Enable KSN Proxy on Administration Server Enabled**.

يتم تمكين الخادم الوكيل لشبكة KSN وإرسال البيانات إلى KSN لزيادة كفاءة مكونات Kaspersky Security Center وتحسين أداء تطبيقات Kaspersky.

1. اعتمادًا على حل البنية التحتية لشبكة KSN الذي تستخدمه، قم بتمكين أزرار التبديل المقابلة.

- إذا كنت تستخدم شبكة KSN العامة، قم بتبديل زر التبديل إلى موضع **Use Kaspersky Security Network Enabled**.

  إرسال البيانات إلى شبكة KSN متاح الآن. عند تمكين هذا الخيار، يجب أن تكون قد قرأت شروط بيان KSN ووافقت عليها.

- إذا كنت تستخدم شبكة KPSN، بدل زر التبديل إلى موضع **Use Kaspersky Private Security Network Enabled** ثم انقر على الزر **Select file with KSN Proxy settings** لتنزيل إعدادات شبكة KPSN (الملفات بالامتدادين pkcs7 وpem). وعقب تنزيل الإعدادات، تعرض الواجهة اسم المزود وجهات الاتصال، وكذلك تاريخ إنشاء الملف مع إعدادات شبكة KPSN.

  عند تبديل زر التبديل إلى موضع **Use Kaspersky Private Security Network Enabled**، ستظهر رسالة تحتوي على تفاصيل حول شبكة KPSN.

2. انقر على زر **Save**.

لتعطيل استخدام شبكة KSN:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **KSN Proxy settings**.

3. قم بتبديل زر التبديل إلى موضع **Enable KSN Proxy on Administration Server Disabled** لتعطيل خدمة الخادم الوكيل لشبكة KSN.

4. انقر على زر **Save**.

عرض بيان KSN المقبول

عندما تقوم بتمكين Kaspersky Security Network (KSN)، يجب عليك قراءة بيان KSN وقبوله. يمكنك عرض بيان KSN المقبول في أي وقت.

لعرض بيان KSN المقبول:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **KSN Proxy settings**.

3. انقر على رابط **View Kaspersky Security Network Statement**.

   في النافذة التي تفتح، يمكنك عرض نص بيان KSN المقبول.

قبول بيان KSN محدث

أنت تستخدم KSN وفق بيان KSN الذي تقرأه وتوافق عليه عندما تقوم بتمكين KSN. إذا تم تحديث بيان KSN، فسيتم عرضه لك عند ترقية إصدار من خادم الإدارة. يمكن قبول بيان KSN المحدث أو رفضه. إذا رفضته، ستستمر في استخدام KSN وفقًا لإصدار بيان KSN الذي قبلته مسبقًا.

بعد ترقية إصدار خادم الإدارة، يتم عرض بيان KSN المُحدث تلقائيًا. إذا رفضت بيان KSN المحدث، لا يزال بإمكانك عرضه وقبوله لاحقًا.

لعرض بيان KSN محدث ثم قبوله أو رفضه:

1. انقر على الرابط **View notifications** في الزاوية العلوية اليمنى من نافذة التطبيق الرئيسية.

   ستفتح النافذة **Notifications**.

2. انقر على الرابط **View the updated KSN Statement**.

   ستفتح نافذة **Kaspersky Security Network Statement update**.

3. اقرأ بيان KSN ثم اتخذ قرارك بالنقر على أحد الأزرار التالية:

   - **أقبل بيان KSN المحدث**
   - **استخدم KSN بموجب البيان القديم**

بناءً على اختيارك، تواصل KSN العمل وفقًا لشروط بيان KSN الحالي أو المحدث. يمكنك عرض نص بيان KSN المقبول في خصائص خادم الإدارة في أي وقت.

التحقق مما إذا كانت نقطة التوزيع تعمل كخادم وكيل لشبكة KSN

يمكنك تمكين الخادم الوكيل لشبكة KSN على جهاز مُدار تم تعيينه للعمل كنقطة توزيع. يعمل الجهاز المُدار كخادم وكيل KSN عند تشغيل خدمة ksnproxy على الجهاز. يمكنك التحقق من هذه الخدمة أو تشغيلها أو إيقاف تشغيلها على الجهاز محليًا.

يمكنك تعيين جهاز يعمل بنظام التشغيل Windows أو Linux كنقطة توزيع. وتعتمد طريقة فحص نقطة التوزيع على نظام تشغيل نقطة التوزيع هذه.

للتحقق مما إذا كانت نقطة التوزيع المعتمدة على نظام التشغيل Windows تعمل كخادم وكيل لشبكة KSN:

1. على جهاز نقطة التوزيع، في Windows، افتح **خدمات** (**كل البرامج** ← **الأدوات الإدارية** ← **خدمات**).

2. في قائمة الخدمات، تحقق من تشغيل خدمة ksnproxy.

إذا كانت خدمة ksnproxy قيد التشغيل، فإن عميل الشبكة الموجود على الجهاز يشارك في Kaspersky Security Network ويعمل كخادم وكيل KSN للأجهزة المدارة المضمنة في نطاق نقطة التوزيع.

إذا كنت تريد، يمكنك إيقاف تشغيل خدمة ksnproxy. في هذه الحالة، يتوقف عميل الشبكة لنقطة التوزيع عن المشاركة في Kaspersky Security Network. هذا الأمر يتطلب حقوق المسؤول المحلي.

للتحقق مما إذا كانت نقطة التوزيع المعتمدة على نظام التشغيل Linux تعمل كخادم وكيل لشبكة KSN:

1. على جهاز نقطة التوزيع، اعرض قائمة العمليات الجارية.

2. في قائمة العمليات الجارية، تحقق مما إذا كانت العملية `opt/kaspersky/ksc64/sbin/ksnproxy/` قيد التشغيل.

إذا كانت عملية `opt/kaspersky/ksc64/sbin/ksnproxy/` قيد التشغيل، فإن عميل الشبكة الموجود على الجهاز في Kaspersky Security Network ويعمل كخادم وكيل KSN للأجهزة المدارة المضمنة في نطاق نقطة التوزيع.

سيناريو: ترقية Kaspersky Security Center وتطبيقات الأمان المُدارة

يصف هذا القسم السيناريو الموجز الرئيسي لترقية Kaspersky Security Center وتطبيقات الأمان المُدارة.

Kaspersky Security Center وترقية تطبيقات الأمان المُدارة تتقدم في مراحل:

1. **التحقق من متطلبات الأجهزة والبرامج**

تأكد أن أجهزتك تفي بالمتطلبات وقم بتثبيت التحديثات المطلوبة.

2. **تخطيط الموارد**

تقييم المساحة التي تشغلها قاعدة البيانات لديك على القرص الصلب. تأكد من وجود مساحة كافية على القرص لتخزين النسخة الاحتياطية من إعدادات خادم الإدارة وقاعدة البيانات.

3. **الحصول على ملف المثبِّت لـ Kaspersky Security Center**

احصل على الملف التنفيذي للإصدار الحالي من Kaspersky Security Center واحفظه على الجهاز الذي سيعمل كخادم الإدارة. اقرأ ملاحظات الإصدار الخاصة بإصدار Kaspersky Security Center الذي ترغب في استخدامه.

4. **إنشاء نسخة احتياطية من الإصدار السابق**

استخدم الأداة المساعدة للنسخ الاحتياطي واسترداد البيانات لإنشاء نسخة احتياطية من بيانات خادم الإدارة. ويمكنك أيضًا إنشاء مهمة نسخ احتياطي.

يوصى بتصدير قائمة المكونات الإضافية المُثبتة.

5. **تشغيل المثبِّت**

قم بتشغيل الملف القابل للتنفيذ لأحدث إصدار من Kaspersky Security Center. عند تشغيل ملف، حدد امتلاكك لنسخة احتياطية وحدد موقعها. سيتم استعادة بياناتك من النسخ الاحتياطي.

6. **ترقية التطبيقات المدارة**

يمكنك ترقية التطبيق في حالة وجود إصدار أحدث متاح. اقرأ قائمة تطبيقات Kaspersky المدعومة وتأكد أن إصدارك من Kaspersky Security Center متوافق مع هذا التطبيق. بعد قم بإجراء ترقية التطبيق على النحو الموضح في ملاحظات الإصدار.

النتائج

عند إكمال سيناريو التطبيق، تأكد أن الإصدار الجديد من خادم الإدارة مثبت بنجاح في Microsoft Management Console. انقر على **المساعدة** ← **عن Kaspersky Security Center**. سيتم عرض الإصدار.

للتأكد من أنك تستخدم الإصدار الجديد من خادم الإدارة في Kaspersky Security Center Web Console، انقر في أعلى الشاشة على أيقونة الإعدادات ( ) الموجودة بجوار اسم خادم الإدارة. في نافذة خصائص خادم الإدارة التي تفتح، حدد قسم **General** في تبويب **General**. سيتم عرض الإصدار.

إذا كنت بحاجة إلى استعادة بيانات خادم الإدارة، اتبع الخطوات الموضحة في الموضوع التالي: النسخ الاحتياطي للبيانات واستعادتها في الوضع التفاعلي.

إذا قمت بترقية تطبيق أمن مُدار، تأكد من أنه مثبت بشكل صحيح على الجهاز المُدار/الأجهزة المُدارة. للمزيد من المعلومات، يُرجى الرجوع إلى مستندات هذا التطبيق.

تحديث قواعد بيانات Kaspersky وتطبيقاته

يصف هذا القسم الخطوات الواجب عليك اتخاذها لتحديث ما يلي بانتظام:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج
- تطبيقات Kaspersky المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية)، بالإضافة إلى وظيفة KSN التي قد لا تكون متاحة في البرنامج في الولايات المتحدة الأمريكية.

السيناريو: تحديث منتظم لقواعد بيانات Kaspersky وتطبيقاتها

يوفر هذا القسم سيناريو للتحديث المنتظم لقواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. بعد أن تكمل تكوين سيناريو حماية الشبكة، يجب أن تحافظ على موثوقية نظام الحماية للتأكد أن خوادم الإدارة والأجهزة المُدارة تبقى محمية من مختلف التهديدات، مثل الفيروسات وهجمات الشبكة وهجمات التصيد الاحتيالي.

تبقى حماية الشبكة محدثة بالتحديثات المنتظمة لما يلي:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج
- تطبيقات Kaspersky المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

عند إكمالك لهذا السيناريو، يمكنك التأكد مما يلي:

- شبكتك محمية بأحدث برامج Kaspersky، وهذه تشمل مكونات Kaspersky Security Center وتطبيقات الأمان.
- قواعد بيانات مكافحة الفيروسات وقواعد بيانات Kaspersky الأخرى ضرورية للغاية لأمان الشبكة تبقى محدثة.

المتطلبات الأساسية

يجب أن تكون الأجهزة المُدارة متصلة بخادم الإدارة. إذا كانت غير متصلة، فكر في تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات يدويًا أو مباشرةً من خوادم تحديث Kaspersky.

يجب أن يكون خادم الإدارة متصلاً بالإنترنت.

قبل البدء، تأكد من إجرائك لما يلي:

1. نشرت تطبيقات أمان Kaspersky على الأجهزة المُدارة وفق سيناريو نشر تطبيقات Kaspersky عبر Kaspersky Security Center Web Console.
2. أنشأت وكونت جميع السياسات المطلوبة وملفات تعريف السياسة والمهام وفق سيناريو تكوين حماية الشبكة.
3. خصصت كمية مناسبة من نقاط التوزيع وفق عدد الأجهزة المُدارة ومخطط الشبكة.

تحديث قواعد بيانات Kaspersky وتطبيقاته يسري عبر بضعة مراحل:

1. **اختيار مخطط تحديث**

يوجد عدة مخططات يمكنك استخدامها في تثبيت التحديثات لمكونات Kaspersky Security Center وتطبيقات الأمان. اختر المخطط أو عدة مخططات تلبي متطلبات شبكتك بصورة مثالية.

2. **إنشاء مهمة لتنزيل التحديثات إلى مستودع خادم الإدارة**

يتم إنشاء هذه المهمة تلقائيًا من خلال معالج البدء السريع في Kaspersky Security Center. إذا لم تشغِّل "المعالج"، قم بإنشاء المهمة الآن.

المهمة مطلوبة لتنزيل التحديثات من خوادم تحديث Kaspersky إلى مستودع خادم الإدارة وكذلك لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج لـ Kaspersky Security Center. بعد تنزيل التحديثات، يمكن نشرها على الأجهزة المُدارة.

إذا كانت شبكتك قد خصصت نقاط التوزيع، يتم تنزيل التحديثات تلقائيًا من مستودع خادم الإدارة إلى مستودعات نقاط التوزيع. في هذه الحالة، تقوم الأجهزة المُدارة المضمّنة في نطاق نقطة التوزيع بتنزيل التحديثات من مستودع نقطة التوزيع بدلاً من مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة
- Kaspersky Security Center Web Console: إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة

3. **إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع (اختياري)**

يتم تنزيل التحديثات بشكل افتراضي إلى نقاط التوزيع من خادم الإدارة. يمكنك تكوين Kaspersky Security Center لتنزيل التحديثات إلى نقاط التوزيع مباشرةً من خوادم تحديث Kaspersky. ومن الأفضل التنزيل إلى مستودعات نقاط التوزيع إذا كانت تكلفة حركة المرور بين خادم الإدارة ونقاط التوزيع أكثر من حركة المرور بين نقاط التوزيع وخوادم تحديث Kaspersky أو إذا لم يتمتع خادم الإدارة بإمكانية الوصول إلى الإنترنت.

عند تخصيص شبكتك لنقاط التوزيع وعند إنشاء مهمة Download updates to the repositories of distribution points، تقوم نقاط التوزيع بتنزيل التحديثات من خوادم تحديث Kaspersky وليس من مستودع خادم الإدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع
- Kaspersky Security Center Web Console: إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

4 تكوين نقاط التوزيع

عندما تقوم شبكتك بتخصيص نقاط توزيع، تأكد أن خيار **Deploy updates** مفعل في جميع نقاط التوزيع المطلوبة. عندما يكون هذا الخيار معطلاً لنقطة التوزيع، يتم إدراج الأجهزة في نطاق تنزيل تحديثات نقطة التوزيع من مستودع خادم الإدارة.

إذا كنت ترغب في أن تتلقى الأجهزة المُدارة تحديثات من نقاط التوزيع فقط، قم بتفعيل خيار **Distribute files through distribution points only** في سياسة عميل الشبكة.

5 تحسين عملية التحديث باستخدام النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديث أو ملفات diff (اختياري)

يمكنك تحسين عملية التحديث باستخدام النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات (مفعل بشكل افتراضي) أو باستخدام ملفات diff. لكل قطاع شبكة، عليك اختيار ما ستفعله من هاتين الميزتين لأنهما لا يعملان في الوقت نفسه.

عند تفعيل النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات، يقوم عميل الشبكة بتنزيل التحديثات المطلوبة إلى الجهاز المُدار بمجرد تنزيل التحديثات إلى مستودع خادم الإدارة قبل أن يطلب تطبيق الأمان التحديثات. يعزز هذا من موثوقية عملية التحديث. لاستخدام هذه الميزة، قم بتمكين خيار **Download updates and anti-virus databases from Administration Server in advance (recommended)** في سياسة عميل الشبكة.

إذا لم تستخدم النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات، يمكنك تحسين حركة المرور بين خادم الإدارة والأجهزة المُدارة باستخدام ملفات diff. عند تفعيل هذه الميزة، يقوم خادم الإدارة أو نقطة التوزيع بتنزيل ملفات diff بدلاً من كامل ملفات قواعد بيانات Kaspersky أو الوحدات النمطية للبرامج. يصف ملف diff الاختلافات بين نسختين من ملف قاعدة البيانات أو الوحدة النمطية للبرامج. وبالتالي يشغل ملف diff مساحة أقل من ملف كامل. يتسبب هذا في انخفاض حركة المرور بين خادم الإدارة أو نقاط التوزيع والأجهزة المُدارة. لاستخدام هذه الميزة، قم بتفعيل خيار **Download diff files** في خصائص مهمة Download updates to the Administration Server repository و/أو مهمة Download updates to the repositories of distribution points.

تعليمات للمساعدة:

- استخدام ملفات diff لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج
- وحدة تحكم الإدارة: تمكين النموذج غير المتصل بالإنترنت لتنزيل التحديثات وتعطيله
- Kaspersky Security Center Web Console: تمكين النموذج غير المتصل بالإنترنت لتنزيل التحديثات وتعطيله

6 التحقق من التحديثات المُنزّلة (اختياري)

قبل تثبيت التحديثات التي تم تنزيلها، يمكنك التحقق من صحة التحديث من خلال مهمة تحديث التحقق. تعمل هذه المهمة على تشغيل مهام تحديث الجهاز ثم مهام فحص البرامج الضارة التي تم تكوينها عبر الإعدادات الخاصة بمجموعة محددة من أجهزة الاختبار. عند الحصول على نتائج المهمة، يبدأ خادم الإدارة نشر التحديث إلى الأجهزة الباقية أو يحظره.

يمكن إجراء مهمة التحقق من صحة التحديث كجزء من مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، قم بتمكين الخيار **التحقق من صحة التحديثات قبل التوزيع** في وحدة تحكم الإدارة أو خيار **Run update verification** في Kaspersky Security Center Web Console.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: التحقق من التحديثات المُنزّلة
- Kaspersky Security Center Web Console: التحقق من التحديثات المُنزّلة

7 اعتماد ورفض تحديثات البرنامج

بشكل افتراضي، يكون لتحديثات البرامج التي تم تنزيلها حالة غير محددة. يمكنك تغيير الحالة إلى مقبولة أو مرفوضة. يتم تثبيت التحديثات المقبولة دائمًا. إذا تطلب التحديث مراجعة وقبول شروط اتفاقية ترخيص المستخدم النهائي، أنت بحاجة أولاً إلى قبول الشروط. يمكن بعد ذلك نشر التحديث على الأجهزة المُدارة. لا يمكن تثبيت التحديثات غير المحددة إلا على عميل الشبكة ومكونات Kaspersky Security Center الأخرى وفق إعدادات سياسة عميل الشبكة. لن يتم تثبيت التحديثات التي تحدد لها حالة مرفوضة. في حالة وجود تحديث مرفوض لتطبيق قد تم تثبيته مسبقًا، سيحاول Kaspersky Security Center إلغاء تثبيت ذلك التحديث من جميع الأجهزة.

تتوفر إمكانية الموافقة على التحديثات أو رفضها فقط لعميل الشبكة وتطبيقات Kaspersky المُدارة المثبتة على أجهزة العميل المستندة إلى نظام Windows والمستندة إلى نظام Linux. لا يتم دعم التحديث السلس لخادم الإدارة وKaspersky Security Center Web Console والمكونات الإضافية لإدارة الويب.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: الموافقة على تحديثات البرامج ورفضها
- Kaspersky Security Center Web Console: الموافقة على تحديثات البرامج ورفضها

8 **تكوين التثبيت التلقائي للتحديثات والتصحيحات المخصصة لمكونات Kaspersky Security Center**

يتم تلقائيًا تثبيت التحديثات والتصحيحات المنزلة لعميل الشبكة ومكونات Kaspersky Security Center الأخرى. إذا تركت خيار **Automatically install applicable updates and patches for components that have the Undefined status** مفعلاً في خصائص عميل الشبكة، عندها سيتم جميع التحديثات تلقائيًا بعد أن يتم تنزيلها إلى المستودع (أو عدة مستودعات). إذا تم تعطيل هذا الخيار، فسوف يتم تثبيت تصحيحات Kaspersky التي تم تنزيلها وتعيين الحالة غير محددة لها فقط بعد أن تقوم بتغيير حالتها إلى معتمدة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center
- Kaspersky Security Center Web Console: تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center

9 **تثبيت التحديثات لخادم الإدارة**

تحديثات البرامج لخادم الإدارة لا تعتمد على حالات التحديث. لم يتم تثبيتها تلقائيًا ويجب أن تتم الموافقة عليها بشكل مبدئي من قبل المسؤول في تبويب **المراقبة** في وحدة تحكم الإدارة (**خادم الإدارة** ← **المراقبة**) أو في قسم **Notifications** في Kaspersky Security Center Web Console (**Monitoring & reporting** ← **Notifications**). يجب أن يقوم المدير بعد ذلك بتشغيل تثبيت التحديثات بشكل صريح.

10 **تكوين التثبيت التلقائي لتحديثات تطبيقات الأمان.**

قم بإنشاء مهام التحديث للتطبيقات المُدارة لتوفير التحديثات في الوقت المناسب للتطبيقات والوحدات النمطية للبرامج وقواعد بيانات Kaspersky، بما في ذلك قواعد بيانات مكافحة الفيروسات. لضمان التحديثات في الوقت المناسب، نوصي بتحديد خيار **When new updates are downloaded to the repository** أثناء تكوين جدول المهام.

إذا كانت شبكتك تتضمن أجهزة IPv6 فقط وترغب في تحديث تطبيقات الأمان المثبتة على هذه الأجهزة بانتظام، فتأكد من تثبيت خادم الإدارة (الإصدار الأقدم من 13.2) وعميل الشبكة (الإصدار الأقدم من 13.2) على الإدارة الأجهزة.

بشكل افتراضي، لا يتم تثبيت تحديثات Kaspersky Endpoint Security for Windows وKaspersky Endpoint Security for Linux إلا بعد أن تغير حالة التحديث إلى مقبولة. يمكنك تغيير إعدادات التحديث في مهمة التحديث.

إذا تطلب التحديث مراجعة وقبول شروط اتفاقية ترخيص المستخدم النهائي، أنت بحاجة أولاً إلى قبول الشروط. يمكن بعد ذلك نشر التحديث على الأجهزة المُدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: التثبيت التلقائي لتحديثات Kaspersky Endpoint Security على الأجهزة
- Kaspersky Security Center Web Console: التثبيت التلقائي لتحديثات Kaspersky Endpoint Security على الأجهزة

النتائج

عند إكمال السيناريو، يتم تكوين Kaspersky Security Center لتحديث قواعد بيانات Kaspersky وتطبيقات Kaspersky المثبتة بعد تنزيل التحديثات إلى مستودع خادم الإدارة أو مستودعات نقاط التوزيع. يمكنك بعد ذلك التقدم إلى مراقبة حالة الشبكة.

حول تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات

للتأكد من تحديث حماية خوادم الإدارة والأجهزة المُدارة لديك، يجب عليك توفير تحديثات لما يلي في الوقت المحدد:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج

قبل تنزيل قواعد بيانات Kaspersky ووحدات البرامج النمطية، يتحقق Kaspersky Security Center من إمكانية الوصول إلى خوادم Kaspersky. إذا تعذر الوصول إلى الخوادم باستخدام نظام DNS، فإن التطبيق يستخدم خوادم DNS العامة. يُعد ذلك ضروريًا للتأكد من تحديث قواعد بيانات مكافحة الفيروسات والحفاظ على مستوى الأمان للأجهزة المُدارة.

- تطبيقات Kaspersky المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

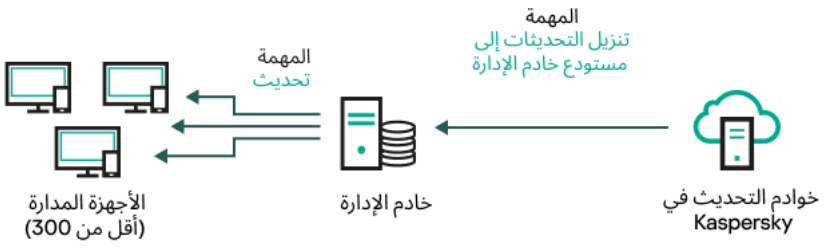
يتيح لك Kaspersky Security Center تحديث عميل الشبكة وتطبيقات Kaspersky المثبتة على أجهزة العميل المستندة إلى Windows وLinux تلقائيًا. لا يتم دعم التحديث السلس لخادم الإدارة وKaspersky Security Center Web Console والمكونات الإضافية لإدارة الويب. لتحديث هذه المكونات، يجب عليك تنزيل أحدث الإصدارات من موقع ويب Kaspersky ، ثم تثبيتها يدويًا.

بناءً على تكوين شبكتك، يمكنك استخدام المخططات التالية الخاصة بتنزيل التحديثات اللازمة وتوزيعها للأجهزة المُدارة:

- باستخدام مهمة واحدة: تنزيل التحديثات إلى مستودع خادم الإدارة
- باستخدام مهمتين:
  - مهمة تنزيل التحديثات إلى مستودع خادم الإدارة
  - مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع
- يدويًا من خلال مجلد محلي أو مجلد مشترك أو خادم FTP
- مباشرة من خوادم تحديث Kaspersky إلى Kaspersky Endpoint Security على الأجهزة المُدارة
- من خلال مجلد محلي أو شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة

في هذا المخطط، يقوم Kaspersky Security Center بتنزيل التحديثات من خلال مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وفي الشبكات الصغيرة التي تحتوي على أقل من 300 جهاز مُدار في مقطع شبكة واحد أو أقل من 10 أجهزة مُدارة في كل مقطع للشبكة، يتم توزيع التحديثات إلى الأجهزة المُدارة مباشرة من مستودع خادم الإدارة (انظر الشكل أدناه).

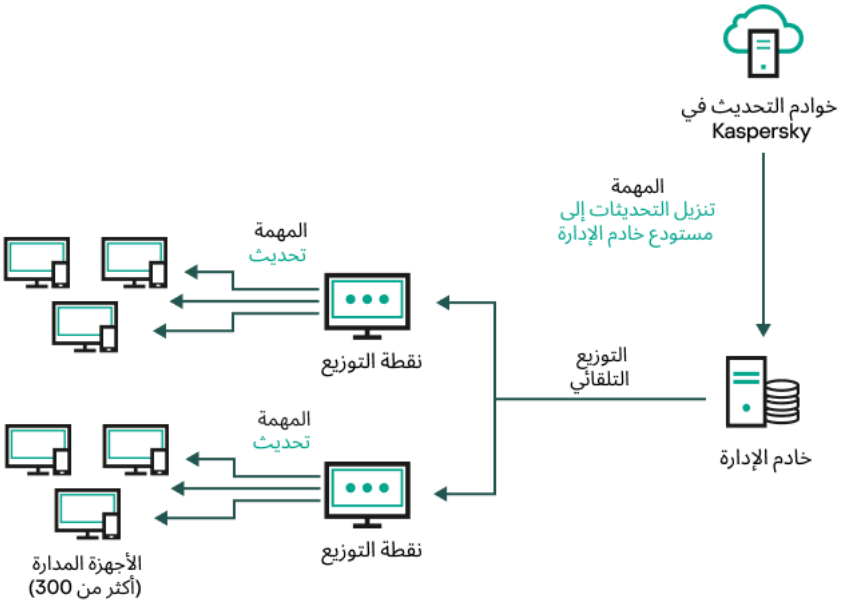


التحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة دون نقاط توزيع

يتصل خادم الإدارة افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة لاستخدام بروتوكول HTTP بدلاً من HTTPS.

إذا كانت شبكتك تحتوي على أكثر من 300 جهاز مُدار في مقطع شبكة واحد أو إذا كانت شبكتك تتكون من مقاطع شبكات متعددة تحتوي على أكثر من 9 أجهزة مُدارة في كل مقطع شبكة، فنوصيك باستخدام نقاط التوزيع لنشر التحديثات إلى الأجهزة المُدارة (انظر الشكل أدناه). وتقلل نقاط التوزيع من التحميل الموجود على خادم الإدارة ويعمل على تحسين حركة المرور بين خادم الإدارة والأجهزة المُدارة. يمكنك حساب عدد نقاط التوزيع لمطلوبة لشبكتك وتكوينها.

وفي هذا المخطط، يتم تنزيل التحديثات تلقائيًا من مستودع خادم الإدارة إلى مستودعات نقاط التوزيع. تقوم الأجهزة المُدارة المضمّنة في نطاق نقطة التوزيع بتنزيل التحديثات من مستودع نقطة التوزيع بدلاً من مستودع خادم الإدارة.



التحديث باستخدام مهمة تنزيل التحديثات إلى مستودع خادم الإدارة مع نقاط توزيع

عند اكتمال المهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يتم تنزيل التحديثات التالية إلى مستودع خادم الإدارة:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج لـ Kaspersky Security Center

  يتم تثبيت هذه التحديثات تلقائيًا.

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج لتطبيقات الأمان على الأجهزة المُدارة

  يتم تثبيت هذه التحديثات من خلال مهمة تحديث لتطبيق Kaspersky Endpoint Security for Windows.

- تحديثات خادم الإدارة

  لا يتم تثبيت هذه التحديثات تلقائيًا. ويجب على المسؤول الموافقة صراحة على تثبيت التحديثات وتشغيلها.

> تلزم حقوق المسؤول المحلي لتثبيت التصحيحات على خادم الإدارة.

- تحديثات مكونات Kaspersky Security Center

  يتم افتراضيًا تثبيت هذه التحديثات تلقائيًا. ويمكنك تغيير الإعدادات في سياسة عميل الشبكة.

- تحديثات تطبيقات الأمن

  بشكل افتراضي، لا يثبت Kaspersky Endpoint Security for Windows إلا التحديثات التي توافق عليها. (يمكنك الموافقة على التحديثات عبر وحدة تحكم الإدارة أو عبر Kaspersky Security Center Web Console). ويتم تثبيت التحديثات من خلال المهمة تحديث ويمكن تكوينها في خصائص هذه المهمة.

> لا تتوفر مهمة تنزيل التحديثات إلى مستودع مهمة خادم الإدارة على خوادم الإدارة الافتراضية. مستودع خادم الإدارة الافتراضي يعرض التحديثات المنزّلة على خادم الإدارة الرئيسي.

ويمكنك تكوين التحديثات للتحقق من التشغيل والأخطاء بمجموعة من الأجهزة الاختبارية. وفي حالة نجاح عملية التحقق، يتم توزيع التحديثات إلى الأجهزة المُدارة الأخرى.

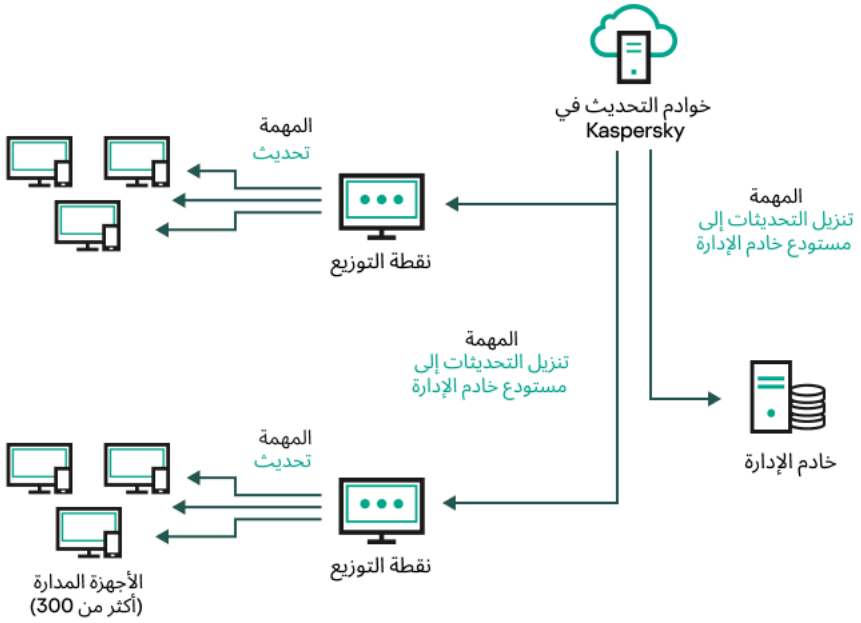
يتطلب كل تطبيق من تطبيقات Kaspersky تحديثات من خادم الإدارة. قام خادم الإدارة بتجميع تلك الطلبات وتنزيل التحديثات التي تم طلبها من قبل التطبيق فقط. يضمن هذا عدم تنزيل نفس التحديثات عدة مرات وعدم تنزيل التحديثات غير الضرورية أبدًا. عند تشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يرسل خادم الإدارة المعلومات التالية إلى خوادم تحديث Kaspersky تلقائيًا لضمان تنزيل إصدارات ذات صلة بقواعد بيانات Kaspersky والوحدات النمطية للبرامج:

- معرف التطبيق وإصداره
- معرف تثبيت التطبيق
- معرف المفتاح المفعل
- معرف تشغيل تنزيل التحديثات إلى مستودع مهمة خادم الإدارة

لا تحتوي أيٌ من المعلومات المنقولة على تفاصيل شخصية أو بيانات سرية أخرى. يحمي AO Kaspersky Lab المعلومات وفقًا للمتطلبات التي ينص عليها القانون.

باستخدام المهمتين: المهمة تنزيل التحديثات إلى مستودع خادم الإدارة والمهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع

يمكنك تنزيل التحديثات إلى مستودعات نقاط التوزيع مباشرة من خوادم تحديث Kaspersky بدلاً من مستودع خادم الإدارة، ثم توزيع التحديثات على الأجهزة المُدارة (انظر الشكل أدناه). ومن الأفضل التنزيل إلى مستودعات نقاط التوزيع إذا كانت تكلفة حركة المرور بين خادم الإدارة ونقاط التوزيع أكثر من حركة المرور بين نقاط التوزيع وخوادم تحديث Kaspersky أو إذا لم يتمتع خادم الإدارة بإمكانية الوصول إلى الإنترنت.



تحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة والمهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع

يتصل خادم الإدارة ونقاط التوزيع افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة و/أو نقاط التوزيع لاستخدام بروتوكول HTTP بدلاً من HTTPS.

لتنفيذ هذا المخطط، قم بإنشاء مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيعبالإضافة إلى مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وبعد ذلك، ستقوم نقاط التوزيع بتنزيل التحديثات من خوادم تحديث Kaspersky وليس من مستودع خادم الإدارة.

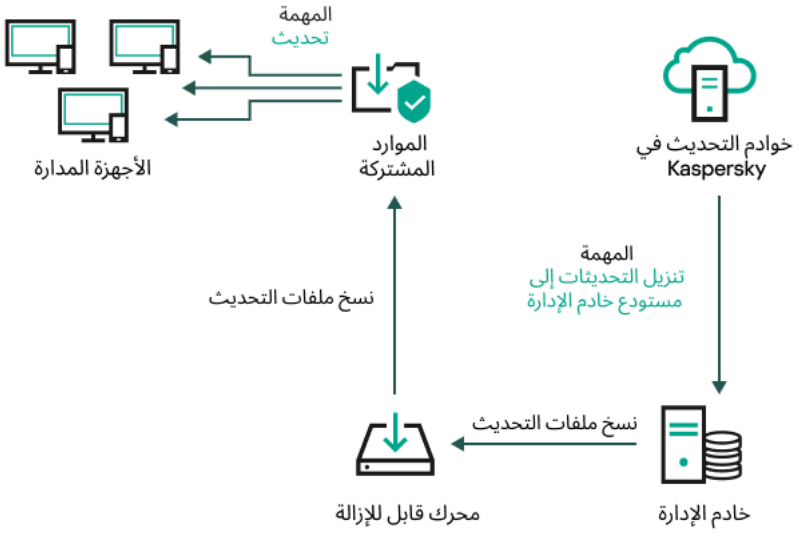
لا يمكن لأجهزة نقاط التوزيع التي تعمل بنظام macOS تنزيل التحديثات من خوادم تحديث Kaspersky.

في حالة وجود جهاز أو أكثر من الأجهزة التي تعمل بنظام macOS داخل نطاق مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع ، تكون المهمة مكتملة مع إظهار حالة فشل ، حتى إذا تم إكمالها بنجاح على جميع أجهزة Windows.

كما يلزم توفير مهمة تنزيل التحديثات إلى مستودع خادم الإدارة في هذا المخطط، نظرًا لاستخدام هذه المهمة في تنزيل قواعد بيانات Kaspersky والوحدات النمطية للبرامج في Kaspersky Security Center.

يدويًا من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

إذا لم تتمتع الأجهزة العميلة باتصال بخادم الإدارة، يمكنك استخدام مجلد محلي أو مورد مشترك كمصدر لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. وفي هذا المخطط، تحتاج إلى نسخ التحديثات اللازمة من مستودع خادم الإدارة إلى محرك الأقراص القابل للإزالة ونسخ التحديثات إلى المجلد المحلي أو المورد المشترك المحدد كمصدر تحديث في إعدادات Kaspersky Endpoint Security (انظر الشكل أدناه).



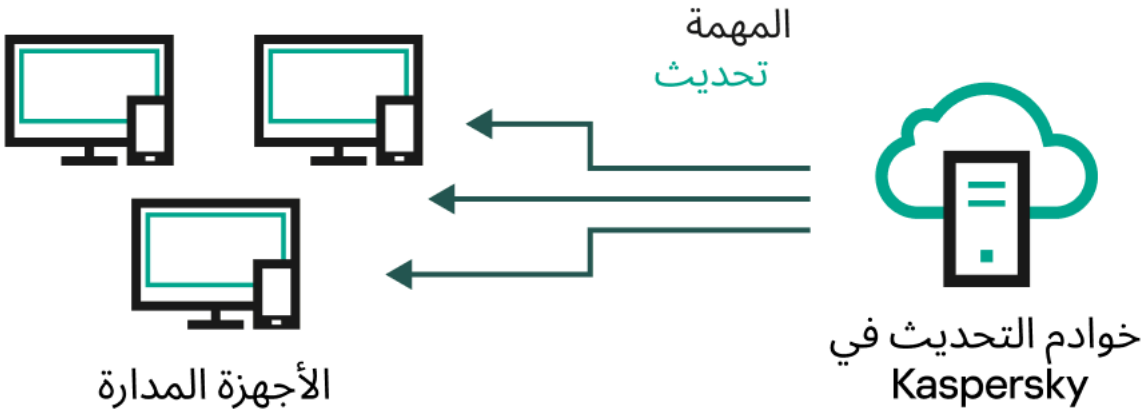
التحديث من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

لمزيد من المعلومات حول مصادر التحديثات في Kaspersky Endpoint Security ، راجع المساعدة التالية:

- تعليمات Kaspersky Endpoint Security for Windows
- دعم Kaspersky Endpoint Security for Linux

مباشرة من خوادم تحديث Kaspersky إلى Kaspersky Endpoint Security على الأجهزة المُدارة

على الأجهزة المُدارة، يمكنك تكوين Kaspersky Endpoint Security لتلقي التحديثات مباشرة من خوادم تحديث Kaspersky (انظر الشكل أدناه).



تحديث تطبيقات الأمن مباشرة من خوادم تحديث Kaspersky

في هذا المخطط، لا يستخدم تطبيق الأمن المستودعات المتوفرة من Kaspersky Security Center. ولتلقي التحديثات مباشرة من خوادم تحديث Kaspersky، حدد خوادم تحديث Kaspersky كمصدر تحديث في واجهة تطبيق الأمان. لمزيد من المعلومات حول هذه الإعدادات، راجع المساعدة التالية:

- تعليمات Kaspersky Endpoint Security for Windows
- دعم Kaspersky Endpoint Security for Linux

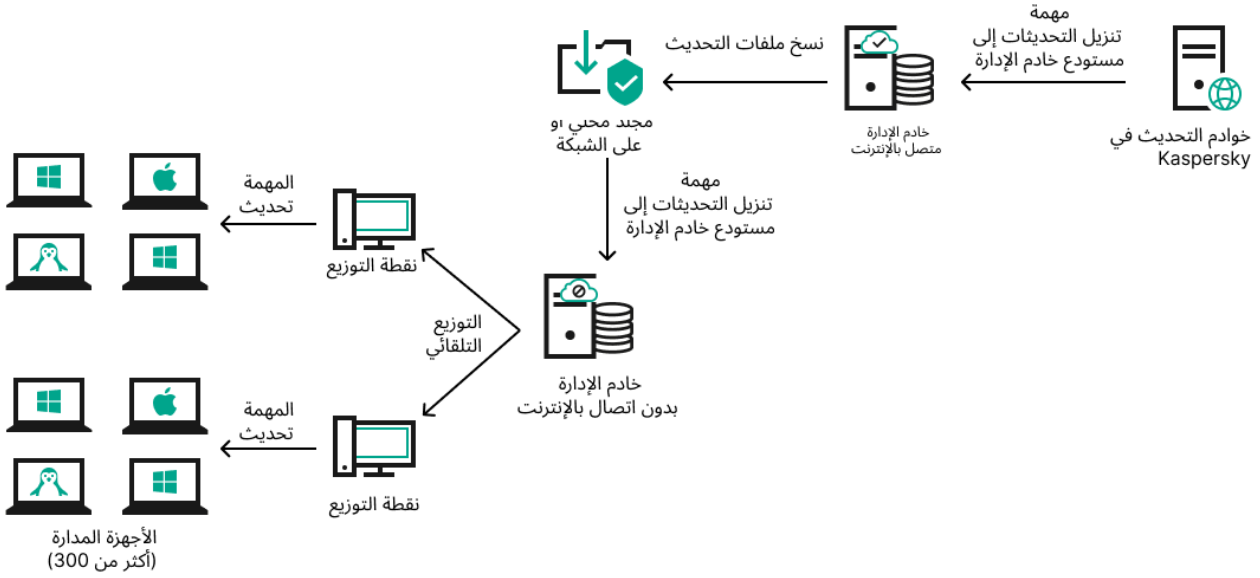
من خلال مجلد محلي أو شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت، فيمكنك تكوين مهمة تنزيل التحديثات إلى مستودع خادم الإدارة لتنزيل التحديثات من مجلد محلي أو مجلد شبكة. في هذه الحالة، يجب عليك نسخ ملفات التحديث المطلوبة إلى المجلد المحدد من وقت لآخر. على سبيل المثال، يمكنك نسخ ملفات التحديث المطلوبة من أحد المصادر التالية:

- خادم الإدارة الذي لديه اتصال بالإنترنت (انظر الشكل أدناه)

  نظرًا لأن خادم الإدارة يقوم بتنزيل التحديثات التي تطلبها تطبيقات الأمان فقط، فيجب أن تتطابق مجموعات تطبيقات الأمان التي تتم إدارتها بواسطة خوادم الإدارة – تلك التي تحتوي على اتصال بالإنترنت وتلك التي لا تحتوي على ذلك –.

إذا كان خادم الإدارة الذي تستخدمه لتنزيل التحديثات يحتوي على الإصدار 13.2 أو إصدار أقدم، فافتح خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، ثم قم بتمكين خيار **تنزيل التحديثات باستخدام النظام القديم** .



التحديث من خلال مجلد محلي أو مجلد شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

- Kaspersky Update Utility

نظرًا لأن هذه الأداة تستخدم النظام القديم لتنزيل التحديثات، افتح خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، ثم قم بتمكين خيار **تنزيل التحديثات باستخدام النظام القديم** .

إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة

يتم إنشاء مهمة Download updates to the Administration Server repository لخادم الإدارة تلقائيًا بواسطة معالج البدء السريع لـ Kaspersky Security Center. لا يمكنك إنشاء إلا مهمة Download updates to the Administration Server repository واحدة. ولهذا السبب، لا يمكنك إنشاء مهمة Download updates to the Administration Server repository إلا إذا تمت إزالة تلك المهمة من قائمة مهام خادم الإدارة.

هذه المهمة مطلوبة لتنزيل التحديثات من خوادم تحديث Kaspersky إلى مستودع خادم الإدارة. قائمة التحديثات تشمل:

- تحديثات قواعد البيانات والوحدات النمطية لخادم الإدارة
- تحديثات قواعد البيانات والوحدات النمطية لتطبيقات أمان Kaspersky
- تحديثات مكونات Kaspersky Security Center
- تحديثات تطبيقات أمان Kaspersky

بعد تنزيل التحديثات، يمكن نشرها على الأجهزة المُدارة.

قبل توزيع التحديثات على الأجهزة المدارة، يمكنك تشغيل المهمة التحقق من التحديث. يمكنك ذلك من التأكد من أن خادم الإدارة سيُثبت التحديثات التي تم تنزيلها بشكل صحيح ولن ينخفض مستوى الأمان بسبب التحديثات. للتحقق منها قبل التوزيع، عليك تكوين الخيار **Run update verification** في إعدادات مهمة Download updates to the Administration Server repository .

لإنشاء مهمة **Download updates to the Administration Server repository**:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع مهمة **Download updates to the Administration Server repository**.

4. حدد اسم المهمة التي ترغب في إنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

5. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

6. انقر على زر **Create**.

   يتم إنشاء المهمة وعرضها في قائمة المهام.

7. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

8. في نافذة خصائص المهمة، حدد الإعدادات التالية في تبويب **Application settings**:

- **Sources of updates**

ويمكن استخدام الموارد التالية كمصدر للتحديثات لخادم الإدارة:

- خوادم تحديث Kaspersky

  خوادم HTTP(S) في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق. يتصل خادم الإدارة افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة لاستخدام بروتوكول HTTP بدلاً من HTTPS.

  يتم تحديده بصورة افتراضية.

- خادم الإدارة الأساسي

  ينطبق هذا المصدر على المهام التي يتم إنشاؤها لخادم الإدارة الثانوي أو الافتراضي.

- المجلد المحلي أو مجلد الشبكة

  مجلد شبكة أو مجلد محلي يحتوي على آخر التحديثات. يمكن أن يكون مجلد الشبكة إما خادم FTP أو خادم HTTP أو مشاركة SMB. إذا تطلب مجلد الشبكة المصادقة، فسيتم دعم بروتوكول SMB فقط. عند تحديد مجلد محلي، يجب عليك تحديد مجلد موجود على الجهاز المُثبت عليه خادم الإدارة.

> يجب أن يحتوي مجلد الشبكة أو خادم FTP أو HTTP المستخدم من قبل مصدر التحديث على بنية مجلدات (مع تحديثات) تتطابق مع البنية التي تم إنشاؤها عند استخدام خوادم تحديث Kaspersky.

في حالة وجود مجلد مشترك يحتوي على تحديثات محميًا بكلمة مرور، قم بتمكين خيار **Specify account for access to shared folder of the update source (if any)** وأدخل بيانات اعتماد الحساب المطلوبة للوصول.

- **Folder for storing updates**

المسار إلى المجلد المحدد لتخزين التحديثات المحفوظة. يمكنك نسخ مسار المجلد المحدد إلى الحافظة. لا يمكنك تغيير المسار إلى مجلد محدد لمهمة جماعية.

- Other settings:

- **Force update of secondary Administration Servers**

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة بتشغيل مهام التحديث على خوادم الإدارة الثانوية بمجرد أن يتم تنزيل التحديثات الجديدة. تبدأ مهام التحديث باستخدام مصدر التحديث الذي تم تكوينه في خصائص المهمة على خوادم الإدارة الثانوية.

إذا تم تعطيل هذا الخيار، فستبدأ مهام التحديث على خوادم الإدارة الثانوية وفقًا لجداولها الزمنية.

يتم تعطيل هذا الخيار افتراضيًا.

- **Copy downloaded updates to additional folders**

بعد تلقي خادم الإدارة للتحديثات، يقوم بنسخها إلى المجلدات المحددة. استخدم هذا الخيار في حال رغبت في إدارة توزيع التحديثات يدويًا على الشبكة الخاصة بك.

على سبيل المثال، قد ترغب في استخدام هذا الخيار في الموقف التالي: تتكون شبكة المؤسسة الخاصة بك من العديد من الشبكات الفرعية المستقلة، ولا تمتلك الأجهزة على كل شبكة فرعية إمكانية الوصول إلى الشبكات الفرعية الأخرى. ومع ذلك فإن جميع الأجهزة في جميع الشبكات الفرعية تمتلك إمكانية الوصول إلى مشاركة الشبكة العامة. في هذه الحالة، قم بتعيين خادم الإدارة في واحدة من الشبكات الفرعية لتنزيل التحديثات من خوادم تحديث Kaspersky، وقم بتمكين هذا الخيار ثم حدد مشاركة الشبكة هذه. من تنزيل التحديثات إلي مستودع المهام لخوادم إدارة أخرى، قم بتحديد نفس مشاركة الشبكة كمصدر تحديث.

إذا حددت نسخ التحديثات التي تم تنزيلها إلى مجلد محلي، فيجب عليك تحديد مجلد على الجهاز الذي تم تثبيت خادم الإدارة عليه. ويعتمد المسار إلى المجلد على نظام تشغيل الجهاز. ونظرًا لوجود المجلد المحلي على خادم الإدارة المستند إلى نظام Linux، فيجب عليك تحديد مسار POSIX، على سبيل المثال: /path/to/dir.

عند تحديد مجلد شبكة موجود على خادم الإدارة المستند إلى نظام Linux، يجب عليك التأكد من إمكانية الوصول إلى مجلد الشبكة مسبقًا من الجهاز المُثبت عليه خادم الإدارة عن طريق تحميل المجلد. ويتم تنفيذ الوصول إلى المجلد باستخدام بروتوكول SMB.

يتم تعطيل هذا الخيار افتراضيًا.

- **Do not force updating of devices and secondary Administration Servers unless copying is complete**

تبدأ مهام تنزيل التحديثات على الأجهزة العميلة وخوادم الإدارة الثانوية فقط بعد نسخ تلك التحديثات من مجلد التحديث الرئيسي إلى مجلدات التحديث الإضافية.

يجب تمكين هذا الخيار إذا كانت الأجهزة العميلة وخوادم الإدارة الثانوية تقوم بتنزيل تحديثات من مجلدات شبكة إضافية.

يتم تعطيل هذا الخيار افتراضيًا.

- **Content of updates**:

- **Download diff files**

يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.

يتم تعطيل هذا الخيار افتراضيًا.

- **Download updates by using the old scheme**

بدءًا من الإصدار 14، يقوم Kaspersky Security Center بتنزيل تحديثات قواعد البيانات ووحدات البرامج باستخدام النظام الجديد. لكي يقوم التطبيق بتنزيل التحديثات باستخدام النظام الجديد، يجب أن يحتوي مصدر التحديث على ملفات تحديث ببيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث ببيانات أولية متوافقة مع النظام القديم فقط، فقم بتمكين الخيار **Download updates by using the old scheme**. خلاف ذلك، ستفشل مهمة تنزيل التحديث.

على سبيل المثال، يجب تمكين هذا الخيار عند تحديد مجلد محلي أو مجلد شبكة كمصدر تحديث، ويتم تنزيل ملفات التحديث الموجودة في هذا المجلد بواسطة أحد التطبيقات التالية:

- Kaspersky Update Utility

تقوم هذه الأداة بتنزيل التحديثات باستخدام النظام القديم.

- Kaspersky Security Center 13.2 أو إصدار سابق

على سبيل المثال، خادم الإدارة 1 ليس به اتصال بالإنترنت. في هذه الحالة، يمكنك تنزيل التحديثات باستخدام خادم الإدارة 2 الذي يحتوي على اتصال بالإنترنت، ثم وضع التحديثات على مجلد محلي أو مجلد شبكة لاستخدامه كمصدر تحديث لخادم الإدارة 1. إذا كان خادم الإدارة 2 يحتوي على الإصدار 13.2 أو إصدار أقدم، فقم بتمكين الخيار **Download updates by using the old scheme** في مهمة خادم الإدارة 1.

يتم تعطيل هذا الخيار افتراضيًا.

- **Run update verification**

سيقوم خادم الإدارة بتنزيل التحديثات من المصدر، وحفظها في مستودع مؤقت، وتشغيل المهمة المحددة في حقل **مهمة التحقق من صحة التحديث**. في حالة اكتمال المهمة بنجاح، يتم نسخ التحديثات من المخزون المؤقت إلى مجلد مشترك على خادم الإدارة ثم توزيعها على جميع الأجهزة التي يعمل عليها خادم الإدارة كمصدر للتحديثات (يتم بدء المهام التي تحتوي على نوع الجدول **عند تنزيل تحديثات جديدة إلى المستودع**). تنتهي مهمة تنزيل التحديثات إلى المستودع فقط بعد اكتمال مهمة التحقق من صحة التحديث.

يتم تعطيل هذا الخيار افتراضيًا.

9. في تبويب **Schedule** من نافذة خصائص المهمة، قم بإنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **Start task:**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **Manually**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **Every N minutes**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **Every N hours**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **Every N days**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **شهريًا**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **تشغيل المهام الفائتة**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **استخدام التأخير العشوائي التلقائي لبدء مهمة**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **Use automatically randomized delay for task starts within an interval of**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

- **Stop the task if it runs longer than**

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائيًا، سواء أكانت مكتملة أم لا.

قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتًا طويلاً للتنفيذ.

يتم تعطيل هذا الخيار افتراضيًا. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

10. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

عندما يجري خادم الإدارة مهمة Download updates to the Administration Server repository، يتم تنزيل تحديثات قواعد البيانات والوحدات النمطية للبرامج من مصدر التحديثات ويتم تخزينها في مجلد خادم الإدارة المشترك. إذا قمت بإنشاء هذه المهمة لإحدى مجموعات الإدارة، فسيتم تطبيقها فقط على عملاء الشبكة المحددين في مجموعة الإدارة المحددة.

يتم توزيع التحديثات على الأجهزة العميلة وخوادم الإدارة الثانوية من المجلد المشترك لخادم الإدارة.

التحقق من التحديثات المُنزّلة

قبل تثبيت التحديثات على الأجهزة المدارة، يمكنك أولاً التحقق من صحة التحديث الخاصة بقابلية التشغيل والأخطاء من خلال مهمة التحقق من صحة التحديث. يتم تنفيذ مهمة التحقق من صحة التحديث تلقائيًا كجزء من مهمة Download updates to the Administration Server repository. يقوم خادم الإدارة بتنزيل التحديثات من المصدر وحفظها في المستودع المؤقت وتشغيل مهمة التحقق من صحة التحديث. إذا اكتملت المهمة بنجاح، سيتم نسخ التحديثات من المستودع المؤقت إلى المجلد المشترك لخادم الإدارة. يتم توزيعها على جميع أجهزة العميل التي يكون فيها خادم الإدارة هو مصدر التحديثات.

إذا، كنتيجة لمهمة التحقق من صحة التحديثات، كانت التحديثات الموجودة في المستودع المؤقت غير صحيحة أو إذا اكتملت مهمة التحقق من صحة التحديث مع وجود خطأ، فلن يتم نسخ هذه التحديثات إلى المجلد المشترك. يحتفظ خادم الإدارة بالمجموعة السابقة من التحديثات. أيضًا لن يتم بدء الهام ذات نوع الجدول **When new updates are downloaded to the repository** بعد. يتم إجراء هذه العمليات في البداية التالية لمهمة Download updates to the Administration Server repository إذا اكتمل فحص التحديثات الجديدة بنجاح.

تعتبر مجموعة التحديثات غير صالحة في حالة الوفاء بأحد الشروط التالية على جهاز اختبار واحد على الأقل:

- حدث خطأ في مهمة تحديث.
- تغيير حالة الحماية في الوقت الحقيقي لتطبيق الأمن بعد تطبيق التحديثات.
- تم اكتشاف كائن مصاب أثناء تشغيل مهمة الفحص عند الطلب.
- حدث خطأ في وقت تشغيل تطبيق Kaspersky.

إذا لم يكن أي من الشروط المدرجة في القائمة صحيحًا لأي جهاز اختبار، فتعتبر مجموعة التحديثات صالحة وتعتبر مهمة التحقق من صحة التحديث مكتملة بنجاح.

قبل أن تبدأ في إنشاء مهمة التحقق من صحة التحديث، نفذ المتطلبات الأساسية:

1. إنشاء مجموعة الإدارة مع العديد من أجهزة الاختبار. ستحتاج إلى هذه المجموعة للتحقق من التحديثات.

نُوصى باستخدام الأجهزة التي تتمتع بحماية موثوقة وتكوين التطبيق الشائع عبر الشبكة. يزيد هذا النهج من جودة واحتمالية اكتشاف الفيروسات أثناء عمليات الفحص، ويقلل من مخاطر الإيجابيات الكاذبة. إذا تم اكتشاف الفيروسات على أجهزة الاختبار، تعتبر مهمة التحقق من صحة التحديث غير ناجحة.

2. أنشئ مهام التحديث وفحص البرامج الضارة لتطبيق مدعوم من Kaspersky Security Center، على سبيل المثال، Kaspersky Endpoint Security for Windows أو Kaspersky Security for Windows Server. وعند إنشاء مهام التحديث وفحص البرامج الضارة، حدد مجموعة الإدارة التي تحتوي على أجهزة الاختبار.

تقوم مهمة التحقق من التحديث بتشغيل مهام التحديث و فحص البرامج الضارة بالتسلسل على أجهزة الاختبار للتحقق من صلاحية جميع التحديثات. بالإضافة إلى ذلك، عند إنشاء مهمة التحقق من التحديث، تحتاج إلى تحديد مهام فحص التحديث والبرامج الضارة

3. إنشاء مهمة Download updates to the Administration Server repository.

لجعل التطبيق Kaspersky Security Center يتحقق من التحديثات التي تم تنزيلها قبل توزيعها إلى الأجهزة العميلة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.

2. انقر على مهمة **Download updates to the Administration Server repository**.

3. في النافذة خصائص المهمة التي تفتح، انتقل إلى علامة التبويب **Application settings**، ومن ثم قم بتمكين الخيار **Run update verification**.

4. إذا كانت مهمة التحقق من صحة التحديث موجودة، فانقر فوق الزر **Select task**. في النافذة التي تفتح، حدد مهمة التحقق من صحة التحديث في مجموعة الإدارة مع أجهزة الاختبار.

5. إذا لم تكن قد أنشأت مهمة التحقق من صحة التحديث مسبقًا، فعليك القيام بما يلي:

   a. انقر على زر **New task**.

   b. في معالج مهمة جديدة الذي يفتح، حدد اسم المهمة إذا كنت تريد تغيير اسم الإعداد المسبق.

   c. حدد مجموعة الإدارة مع أجهزة الاختبار، التي أنشأتها مسبقًا.

   d. أولاً، حدد مهمة تحديث التطبيق المطلوب الذي يدعمه Kaspersky Security Center، ثم حدد مهمة فحص البرامج الضارة.

   بعد ذلك، تظهر الخيارات التالية. نوصي بتركها ممكّنة:

   - **Restart the device after database update**

   بعد تحديث قواعد بيانات مكافحة الفيروسات على الجهاز، نوصي بإعادة تشغيل الجهاز.

   يتم تمكين هذا الخيار بشكل افتراضي.

   - **Check real-time protection status after database update and device restart**

   في حالة تمكين هذا الخيار، فإن مهمة التحقق من صحة التحديث تتحقق مما إذا كانت التحديثات التي تم تنزيلها إلى مستودع خادم الإدارة صالحة أم لا، وما إذا كان مستوى الحماية قد انخفض بعد تحديث قاعدة بيانات مكافحة الفيروسات وإعادة تشغيل الجهاز.

   يتم تمكين هذا الخيار افتراضيًا.

   e. حدد حسابًا سيتم تشغيل مهمة التحقق من صحة التحديث منه. يمكنك استخدام حسابك وترك خيار **Default account** ممكّنًا. أو بدلاً من ذلك، يمكنك تحديد أنه يجب أن يتم تشغيل المهمة ضمن حساب آخر لديه حقوق الوصول الضرورية. وللقيام بذلك، حدد خيار **Specify account**، ثم أدخل بيانات اعتماد هذا الحساب.

6. انقر فوق **Save** لإغلاق نافذة الخصائص الخاصة بالمهمة Download updates to the Administration Server repository.

يتم تفعيل التحقق التلقائي من التحديثات. يمكنك الآن تشغيل مهمة Download updates to the Administration Server repository وستبدأ من التحقق من صحة التحديث.

إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

لا تعمل المهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع إلا على أجهزة نقاط التوزيع التي تعمل بنظام Windows. لا يمكن لأجهزة نقاط التوزيع التي تعمل بنظام Linux أو macOS تنزيل التحديثات من خوادم تحديث Kaspersky. إذا كان هناك جهاز واحد على الأقل يعمل بنظام التشغيل Linux أو macOS ضمن نطاق المهمة، فستكون حالة المهمة هي فشلت. حتى إذا تم إكمال المهمة بنجاح على جميع الأجهزة التي تعمل بنظام Windows، سوف تُرجع خطأً على الأجهزة المتبقية.

يمكنك إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع لمجموعة إدارة. سيتم تشغيل هذه المهمة لنقاط التوزيع المضمنة في مجموعة الإدارة المحددة.

يمكنك استخدام هذه المهمة على سبيل المثال إذا كانت حركة المرور بين خادم الإدارة ونقطة (نقاط) التوزيع أكثر تكلفة من حركة المرور بين نقطة (نقاط) التوزيع وخوادم تحديث Kaspersky أو إذا لم يكن لدى خادم الإدارة الخاص بك اتصال بالإنترنت.

هذه المهمة مطلوبة لتنزيل التحديثات من خوادم تحديث Kaspersky إلى مستودعات نقاط التوزيع. قائمة التحديثات تشمل:

- تحديثات قواعد البيانات والوحدات النمطية لتطبيقات أمان Kaspersky
- تحديثات مكونات Kaspersky Security Center
- تحديثات تطبيقات أمان Kaspersky

بعد تنزيل التحديثات، يمكن نشرها على الأجهزة المُدارة.

إذا كانت نقاط التوزيع تتصل بالإنترنت باستخدام خادم وكيل، فيجب عليك تحديد الإعدادات المقابلة في سياسة عميل الشبكة.

لإنشاء مهمة **Download updates to the repositories of distribution points** لمجموعة إدارة محددة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.
2. انقر على زر **Add**.

   سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.
3. لتطبيق Kaspersky Security Center في حقل **نوع المهمة**، حدد **Download updates to the repositories of distribution points**.
4. حدد اسم المهمة التي ترغب في إنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).
5. حدد زر خيار لتحديد مجموعة الإدارة أو تحديد الجهاز أو الأجهزة التي تنطبق المهمة عليها.
6. في خطوة **Finish task creation**، إذا كنت تريد تعديل إعدادات المهمة الافتراضية، فقم بتمكين **Open task details when creation is complete** اختيار. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.
7. انقر على زر **Create**.

   يتم إنشاء المهمة وعرضها في قائمة المهام.
8. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

9. في تبويب **Application settings** في نافذة خصائص المهمة، حدد الإعدادات التالية:

- **Sources of updates**

يمكن استخدام الموارد التالية كمصدر لتحديثات نقطة التوزيع:

- خوادم تحديث Kaspersky

خوادم (S)HTTP في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق.

ويتم تحديد هذا الخيار بصورة افتراضية.

- المجلد المحلي أو مجلد الشبكة

مجلد شبكة أو مجلد محلي يحتوي على آخر التحديثات. يمكن أن يكون مجلد الشبكة إما خادم FTP أو خادم HTTP أو مشاركة SMB. إذا تطلب مجلد الشبكة المصادقة، فسيتم دعم بروتوكول SMB فقط. عند تحديد مجلد محلي، يجب عليك تحديد مجلد موجود على الجهاز المُثبت عليه خادم الإدارة.

> يجب أن يحتوي مجلد الشبكة أو خادم FTP أو HTTP المستخدم من قبل مصدر التحديث على بنية مجلدات (مع تحديثات) تتطابق مع البنية التي تم إنشاؤها عند استخدام خوادم تحديث Kaspersky.

- **Folder for storing updates**

المسار إلى المجلد المحدد لتخزين التحديثات المحفوظة. يمكنك نسخ مسار المجلد المحدد إلى الحافظة. لا يمكنك تغيير المسار إلى مجلد محدد لمهمة جماعية.

- **Download diff files**

يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.

يتم تعطيل هذا الخيار افتراضيًا.

- **Download updates by using the old scheme**

بدءًا من الإصدار 14، يقوم Kaspersky Security Center بتنزيل تحديثات قواعد البيانات ووحدات البرامج باستخدام النظام الجديد. لكي يقوم التطبيق بتنزيل التحديثات باستخدام النظام الجديد، يجب أن يحتوي مصدر التحديث على ملفات تحديث ببيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث ببيانات أولية متوافقة مع النظام القديم فقط، فقم بتمكين الخيار **Download updates by using the old scheme**. خلاف ذلك، ستفشل مهمة تنزيل التحديث.

على سبيل المثال، يجب تمكين هذا الخيار عند تحديد مجلد محلي أو مجلد شبكة كمصدر تحديث، ويتم تنزيل ملفات التحديث الموجودة في هذا المجلد بواسطة أحد التطبيقات التالية:

- Kaspersky Update Utility

تقوم هذه الأداة بتنزيل التحديثات باستخدام النظام القديم.

- Kaspersky Security Center 13.2 أو إصدار سابق

على سبيل المثال، تم تكوين نقطة توزيع لأخذ التحديثات من مجلد محلي أو مجلد شبكة. في هذه الحالة، يمكنك تنزيل التحديثات باستخدام خادم إدارة متصل بالإنترنت، ثم وضع التحديثات للمجلد المحلي في نقطة التوزيع. إذا كان خادم الإدارة يحتوي على الإصدار 13.2 أو إصدار أقدم ، فقم بتمكين الخيار **Download updates by using the old scheme** في مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع.

يتم تعطيل هذا الخيار افتراضيًا.

10. أنشئ جدولاً لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **Start task**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **Manually**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **Every N minutes**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **Every N hours**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **Every N days**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **By days of week**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 00:00:6 مساءً.

- **Monthly**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **Every month on specified days of selected weeks**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **On virus outbreak**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **On completing another task**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

- **Run missed tasks**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **Use automatically randomized delay for task starts**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **Use automatically randomized delay for task starts within an interval of**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

11. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عند تنفيذ مهمة Download updates to the repositories of distribution points، يتم تنزيل تحديثات قواعد البيانات والوحدات النمطية للبرنامج من مصدر التحديث ويتم تخزينها في المجلد المشترك. سيتم استخدام التحديثات التي تم تنزيلها فقط بواسطة نقاط التوزيع المضمنة في مجموعة الإدارة المحددة وتلك التي لم يتم تعيين مهمة تنزيل تحديث لها بشكل صريح.

تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center.

يمكن تثبيت التحديثات والتصحيحات لخادم الإدارة يدويًا فقط بعد الحصول على موافقة صريحة من المدير.

يتم تمكين التثبيت التلقائي لتحديثات وتصحيحات مكونات Kaspersky Security Center بشكل افتراضي أثناء تثبيت عميل الشبكة على الجهاز. ويمكنك تعطيله أثناء تثبيت عميل الشبكة، أو تعطيله في وقت لاحق باستخدام سياسة.

لتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center أثناء التثبيت المحلي لعميل الشبكة على الجهاز:

1. ابدأ التثبيت المحلي لعميل الشبكة على الجهاز.
2. في الخطوة **الإعدادات المتقدمة**، قم بإلغاء تحديد خانة الاختيار **تثبيت التحديثات والتصحيحات القابلة للتطبيق تلقائيًا للمكونات بالحالة غير محددة**.
3. اتبع إرشادات المعالج.

سيتم تثبيت عميل الشبكة الذي تم تعطيل التثبيت والتصحيح التلقائيين لمكونات Kaspersky Security Center له على الجهاز. يمكنك تمكين التحديث والتصحيح التلقائيين في وقت لاحق باستخدام سياسة.

لتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center أثناء تثبيت عميل الشبكة على الجهاز من خلال حزمة تثبيت:

1. في القائمة الرئيسية، انتقل إلى **Installation packages** ← **Repositories** ← **Operations**.
2. انقر على حزمة **عميل شبكة Kaspersky Security Center <رقم الإصدار>**.
3. في نافذة الخصائص، افتح تبويب **Settings**.
4. أغلق زر التبديل **Automatically install applicable updates and patches for components that have the Undefined status**.

سيتم تثبيت عميل الشبكة الذي تم تعطيل التثبيت والتصحيح التلقائيين لمكونات Kaspersky Security Center له من هذه الحزمة. يمكنك تمكين التحديث والتصحيح التلقائيين في وقت لاحق باستخدام سياسة.

في حالة تحديد خانة الاختيار هذه (أو إلغاء تحديدها) أثناء تثبيت عميل الشبكة على الجهاز، يمكنك بعد ذلك تمكين (أو تعطيل) التحديث التلقائي باستخدام سياسة عميل الشبكة.

لتمكين أو تعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center باستخدام سياسة عميل الشبكة:

1. في القائمة الرئيسية، انتقل إلى **Policies & profiles** ← **Assets (Devices)**.
2. انقر على سياسة عميل الشبكة:

3. في نافذة خصائص السياسة، افتح تبويب **Application settings**.

4. في قسم **Manage patches and updates**، قم بتشغيل أو إيقاف زر التبديل **Automatically install applicable updates and patches for components that have the Undefined status** من أجل تفعيل أو تعطيل التحديثات والتصحيحات والتلقائية على التوالي.

5. عيّن القفل لزر التبديل هذا (🔒).

سيتم تطبيق السياسة على الأجهزة المحددة، وسيتم تمكين (أو تعطيل) التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center على هذه الأجهزة.

التثبيت التلقائي لتحديثات Kaspersky Endpoint Security for Windows

يمكنك تكوين التحديثات التلقائية لقواعد البيانات والوحدات النمطية البرمجية لتطبيق Kaspersky Endpoint Security for Windows على أجهزة العميل.

لتكوين التنزيل والتثبيت التلقائي لتحديثات Kaspersky Endpoint Security for Windows على الأجهزة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على زر **Add**.

سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. لتطبيق Kaspersky Endpoint Security for Windows، حدد **التحديث** كالنوع الفرعي للمهمة.

4. حدد اسم المهمة التي ترغب في إنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

5. اختر نطاق المهمة.

6. حدد مجموعة الإدارة أو تحديد الجهاز أو الأجهزة التي تنطبق المهمة عليها.

7. في خطوة **Finish task creation**، إذا كنت تريد تعديل إعدادات المهمة الافتراضية، فقم بتمكين **Open task details when creation is complete** اختيار. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

8. انقر على زر **Create**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

9. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

10. في تبويب **Application settings** في نافذة خصائص المهمة، حدد إعدادات مهمة التحديث في الوضع المحلي أو وضع الجهاز المحمول:

- **الوضع المحلي**: تم إنشاء الاتصال بين الجهاز وخادم الإدارة.
- **وضع الجهاز المحمول**: لم يتم إنشاء اتصال بين Kaspersky Security Center والجهاز (على سبيل المثال، عندما لا يكون الجهاز متصلاً بالإنترنت).

11. قم بتفعيل مصادر التحديث التي ترغب في استخدامها لتحديث قواعد البيانات والوحدات النمطية للتطبيق لـ Kaspersky Endpoint Security for Windows. يمكنك تغيير أماكن المصادر في القائمة باستخدام زري **Move up** و**Move down** إذا كان ذلك ضروريًا. في حال تفعيل عدة مصادر تحديث، يحاول Kaspersky Endpoint Security for Windows الاتصال بهم واحدًا بعد الآخر بدءًا من أعلى القائمة، ويجري مهمة التحديث باسترداد حزمة التحديث من أول مصدر متوفر.

12. قم بتفعيل خيار **تثبيت تحديثات الوحدة النمطية للتطبيق المقبولة** لتنزيل تحديثات الوحدة النمطية للبرنامج وتثبيتها جنبًا إلى جنب مع قواعد بيانات التطبيق.

في حال تفعيل هذا الخيار، يقوم Kaspersky Endpoint Security for Windows بإخطار المستخدم بتحديثات الوحدة النمطية للبرنامج المتوفرة وتضمين تحديثات الوحدة النمطية للبرنامج في حزمة التحديثات أثناء تشغيل مهمة التحديث. لا يقوم Kaspersky Endpoint Security for Windows بتثبيت إلا التحديثات التي قد خصصتها بحالة مقبولة، وسوف يتم تثبيتهم محليًا من خلال واجهة التطبيق أو من خلال Kaspersky Security Center.

يمكنك كذلك تفعيل خيار **تثبيت التحديثات الحرجة للوحدة النمطية للتطبيق تلقائيًا**. إذا توافرت أي تحديثات للوحدات النمطية للبرنامج، يقوم Kaspersky Endpoint Security for Windows بتثبيت التحديثات التي حالتها حرجة تلقائيًا؛ وسيتم تثبيت التحديثات المتبقية بعد الحصول على موافقتك.

إذا تطلب تحديث الوحدة النمطية للبرنامج مراجعة بنود اتفاقية الترخيص وسياسة الخصوصية والموافقة عليها، فإن التطبيق يقوم بتثبيت التحديثات بعد الموافقة على بنود اتفاقية الترخيص وسياسة الخصوصية من قبل المستخدم.

13. حدد خانة الاختيار **نسخ التحديثات إلى مجلد** لكي يقوم التطبيق بحفظ التحديثات التي تم تنزيلها إلى مجلد، ثم حدد مسار ذلك المجلد.

14. جدول المهمة. لضمان التحديث في الوقت المناسب، ننصحك بتحديد خيار **عند تنزيل تحديثات جديدة إلى المستودع**.

15. انقر على **Save**.

عند تشغيل المهمة **تحديث**، يرسل التطبيق طلبات إلى خوادم تحديث Kaspersky.

تتطلب بعض التحديثات تثبيت أحدث إصدارات مكونات الإدارة الإضافية.

اعتماد ورفض تحديثات البرنامج

قد تتطلب إعدادات مهمة تثبيت تحديث الموافقة على التحديثات المراد تثبيتها. يمكنك الموافقة على التحديثات التي يجب تثبيتها ورفض التحديثات التي لا يتوجب تثبيتها.

على سبيل المثال، قد ترغب أولًا بالتحقق من تثبيت التحديثات في بيئة اختبار والتأكد من عدم تداخلها في عملية تشغيل الأجهزة، وبعد ذلك فقط تسمح بتثبيت تلك التحديثات على الأجهزة العميلة.

تتوفر إمكانية الموافقة على التحديثات أو رفضها فقط لعميل الشبكة والتطبيقات المُدارة المثبتة على أجهزة العميل المستندة إلى نظام Windows. لا يتم دعم التحديث السلس لخادم الإدارة وKaspersky Security Center Web Console والمكونات الإضافية لإدارة الويب. لتحديث هذه المكونات، يجب عليك تنزيل أحدث الإصدارات من موقع ويب Kaspersky ، ثم تثبيتها يدويًا.

قم بما يلي للموافقة على أو رفض تحديث واحد أو عدة تحديثات:

1. في القائمة الرئيسية، انتقل إلى **Operations ← Kaspersky applications ← Seamless updates**.

   ستظهر قائمة بالتحديثات المتاحة.

تحديثات التطبيقات المُدارة قد يتطلب تثبيت إصدار أدنى محدد من Kaspersky Security Center. إذا كان هذا الإصدار أحدث من إصدارك الحالي، يتم عرض هذه التحديثات لكن لا يمكن الموافقة عليها. أيضًا لا يمكن إنشاء حزم تثبيت من هذه التحديثات حتى تقوم بترقية Kaspersky Security Center. سيُطلب منك ترقية مثيلك من Kaspersky Security Center إلى الإصدار الأدنى المطلوب.

2. حدد التحديثات التي ترغب في الموافقة عليها أو رفضها.

3. انقر على **Approve** للموافقة على التحديثات المحددة أو **Decline** لرفض التحديثات المحددة.

   القيمة الافتراضية هي غير محددة.

يتم وضع التحديثات التي تقوم بتعيين حالة مقبولة لها في قائمة انتظار التثبيت.

يتم إلغاء تثبيت التحديثات التي تقوم بتعيين حالة مرفوضة لها من جميع الأجهزة التي تم تثبيتها عليها سابقًا (إن أمكن). لن يتم تثبيتها كذلك على أجهزة أخرى في المستقبل.

لا يمكن إلغاء تثبيت بعض تحديثات تطبيقات Kaspersky. إذا قمت بتعيين الحالة تم رفضه للتحديثات، فلن يقوم Kaspersky Security Center بإلغاء تثبيت هذه التحديثات من الأجهزة التي تم تثبيتها عليها سابقًا. ومع ذلك، لن يتم تثبيت هذه التحديثات أبدًا على أجهزة أخرى في المستقبل.

إذا قمت بتعيين حالة مرفوضة لتحديثات برامج الجهات الخارجية، لن يتم تثبيت هذه التحديثات على الأجهزة التي تم التخطيط لتثبيتها عليها لكنها لم تثبَت بعد. ستظل التحديثات على الأجهزة التي تم تثبيتها عليها بالفعل. إذا كان يتعين عليك حذف التحديثات، يمكنك حذفها يدويًا محليًا.

تحديث خادم الإدارة

يمكنك تثبيت تحديثات خادم الإدارة باستخدام Update Administration Server wizard.

لتثبيت تحديث خادم إدارة:

1. في القائمة الرئيسية، انتقل إلى **Operations** ← **Kaspersky applications** ← **Seamless updates**.
2. قم بتشغيل Update Administration Server wizard بإحدى الطرق التالية:
   - انقر على اسم تحديث خادم الإدارة في قائمة التحديثات، وفي النافذة التي تفتح انقر على رابط **Run Update Administration Server wizard**.
   - انقر على رابط **Run Update Administration Server wizard** في حقل الإخطار في أعلى النافذة.
3. في نافذة Update Administration Server wizard، حدد واحدًا مما يلي لتحديد متى تقوم بتثبيت تحديث:
   - **Install now**. حدد هذا الخيار إذا كنت تريد تثبيت التحديث على الفور.
   - **تأجيل عملية التثبيت**. حدد هذا الخيار إذا كنت تريد تثبيت التحديث لاحقًا. في هذه الحالة سيتم عرض إشعار عن هذا التحديث.
   - **تجاهل التحديث**. حدد هذا الخيار إذا كنت لا تريد تثبيت تحديث ولا ترغب في استقبال إشعارات عن هذا التحديث.
4. حدد خيار **Create backup copy of Administration Server before update installation** إذا كنت ترغب في إنشاء نسخة احتياطية من خادم الإدارة قبل تثبيت التحديث.
5. انقر على زر **OK** لإنهاء المعالج.

في حال انقطاع عملية النسخ الاحتياطي، سيتم تعطيل عملية تثبيت التحديث هي أيضًا.

تمكين النموذج غير متصل بالإنترنت لتنزيل التحديثات وتعطيله

ننصحك بتجنب تعطيل نموذج عدم الاتصال لتنزيل التحديثات. قد يسبب تعطيله إخفاقات في تسليم التحديث إلى الأجهزة. في بعض الحالات، قد ينصحك متخصص الدعم الفني من Kaspersky بتعطيل خيار **تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة بشكل مسبق**. لذلك، سيتعين عليك التأكد من إعداد مهمة استلام التحديثات لتطبيقات Kaspersky.

لتمكين وتعطيل نموذج غير متصل لتنزيل التحديثات لمجموعة إدارة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.

2. انقر على **Groups**.

3. في بنية مجموعة الإدارة، حدد مجموعة الإدارة التي تحتاج إلى تمكين النموذج غير المتصل بالإنترنت الخاص بتنزيل التحديثات من أجلها.

4. انقر على سياسة عميل الشبكة:

   تفتح نافذة الخصائص لسياسة عميل الشبكة.

يتم وراثة إعدادات السياسات الفرعية من السياسات الأصلية بشكل افتراضي، ولا يمكن تعديلهم. إذا كانت السياسة التي ترغب في تعديلها موروثة، ستحتاج أولاً إلى إنشاء سياسة جديدة لعميل الشبكة في مجموعات الإدارة المطلوبة. يمكنك في السياسة التي تم إنشاؤها حديثًا تعديل الإعدادات التي ليست مقفولة في السياسة الأصلية.

5. في تبويب **Application settings**، حدد قسم **Manage patches and updates**.

6. قم بتمكين أو تعطيل الخيار **Download updates and anti-virus databases from Administration Server in advance (recommended)** لتمكين أو تعطيل وضع غير متصل بالإنترنت أو تعطيله على التوالي.

   بشكل افتراضي، يتم تمكين النموذج غير متصل لتنزيل التحديثات.

   سيتم تمكين نموذج غير متصل لتنزيل التحديثات أو تعطيله.

تحديث قواعد بيانات Kaspersky ووحدات البرامج على الأجهزة غير المتصلة بالإنترنت

تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج على الأجهزة المُدارة مهمة ضرورية للمحافظة على حماية الأجهزة من الفيروسات والتهديدات الأخرى. عادةً ما يقوم المديرون بتكوين التحديثات المنتظمة عبر استخدام مستودع خادم الإدارة أو مستودعات نقاط التوزيع.

عندما تحتاج إلى تحديث قواعد البيانات والوحدات النمطية للبرامج على جهاز (أو مجموعة أجهزة) ليست متصلة بخادم الإدارة (الرئيسي أو التابع) أو نقطة توزيع أو الإنترنت، يجب عليك استخدام مصادر تحديثات بديلة، مثل خادم FTP أو مجلد محلي. عليك في هذه الحالة تسليم ملفات التحديثات المطلوبة باستخدام جهاز تخزين كبير المساحة، مثل محرك أقراص فلاش أو محرك قرص ثابت خارجي.

يمكنك نسخ التحديثات المطلوبة من:

- خادم الإدارة.

  للتأكد من احتواء مستودع خادم الإدارة على التحديثات المطلوبة لتطبيق الأمان المثبت على الجهاز غير المتصل، يجب أن يكون على الأقل أحد الأجهزة المتصلة المُدارة مثبت عليه نفس تطبيق الأمان. يجب تكوين هذا التطبيق لاستقبال تحديثات من مستودع خادم الإدارة من خلال مهمة Download updates to the Administration Server repository.

- أي جهاز مثبت عليه نفس تطبيق الأمان ومكون من أجل استلام التحديثات من مستودع خادم الإدارة أو مستودع نقطة توزيع أو مباشرةً من خوادم تحديث Kaspersky.

يوجد أدناه مثال على تكوين تحديثات قواعد بيانات والوحدات النمطية للبرامج عن طريق نسخها من مستودع خادم الإدارة.

لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج على الأجهزة غير المتصلة بالإنترنت:

1. قم بتوصيل محرك الأقراص القابلة للإزالة بالجهاز المثبت عليه خادم الإدارة.

2. انسخ ملفات التحديثات إلى محرك الأقراص القابل للإزالة.

   بشكلِ افتراضي، توجد التحديثات في\\<اسم الخادم>\KLSHARE\Updates.

يمكنك بدلاً من ذلك تكوين Kaspersky Security Center لنسخ التحديثات بانتظام إلى المجلد الذي تحدده. ولهذا الغرض استخدم خيار **Copy downloaded updates to additional folders** في خصائص مهمة Download updates to the Administration Server repository. إذا حددت مجلدًا موجودًا على محرك أقراص فلاش أو محرك أقراص ثابت خارجي كمجلد الوجهة لهذا الخيار، دائمًا ما سيحتوي جهاز التخزين كبير المساحة هذا على أحدث إصدار من التحديثات.

3. قم على الأجهزة غير المتصلة بالإنترنت بتكوين تطبيقات الأمان (مثل Kaspersky Endpoint Security for Windows) لاستقبال التحديثات من مجلد محلي أو مصدر مشترك، مثل خادم FTP أو مجلد مشترك.

4. انسخ ملفات التحديثات من محرك الأقراص القابل للإزالة إلى المجلد المحلي أو المصدر المشترك الذي ترغب في استخدمه كمصدر تحديث.

5. على الجهاز غير المتصل بالإنترنت الذي يتطلب تثبيت التحديث، ابدأ مهمة تحديث Kaspersky Endpoint Security for Windows.

بعد اكتمال مهمة التحديث، تكون قواعد بيانات Kaspersky والوحدات النمطية للبرامج محدثة على الجهاز.

النسخ الاحتياطي واستعادة المكونات الإضافية للويب

يتيح لك Kaspersky Security Center Web Console إجراء نسخ احتياطي للحالة الحالية لمكون ويب إضافي لتتمكن من استعادة الحالة المحفوظة لاحقًا. على سبيل المثال، يمكنك عمل نسخة احتياطية من مكون ويب إضافي قبل تحديثه إلى إصدار أحدث. بعد التحديث، إذا كان الإصدار الأحدث لا يلبي متطلباتك أو توقعاتك، فيمكنك استعادة الإصدار السابق من المكون الإضافي للويب من النسخة الاحتياطية.

لعمل نسخة احتياطية من مكونات الويب الإضافية:

1. في القائمة الرئيسية، انتقل إلى **إعدادات** ← **Web plug-ins**.

2. في القسم **Web plug-ins**، حدد مكونات الويب الإضافية التي تريد نسخها احتياطيًا، ثم انقر على الزر **Create backup copy**.

يتم نسخ مكونات الويب الإضافية المحددة احتياطيًا. يمكنك عرض النسخ الاحتياطية التي تم إنشاؤها في القسم **Backups**.

لاستعادة مكون ويب إضافي من نسخة احتياطية:

1. في القائمة الرئيسية انتقل الى **إعدادات** ← **Backups**.

2. في القسم **Backups**، حدد النسخة الاحتياطية من المكون الإضافي للويب الذي تريد استعادته، ثم انقر على الزر **Restore from backup**.

تمت استعادة المكون الإضافي للويب من النسخة الاحتياطية المحددة.

تعديل نقاط التوزيع وبوابات الاتصال

تُجري بنية مجموعات الإدارة في Kaspersky Security Center الوظائف التالية:

- تعيين نطاق السياسات.

توجد طريقة بديلة لتطبيق مجموعات الإعدادات ذات الصلة على الأجهزة، عن طريق استخدام ملفات تعريف السياسة. في هذه الحالة، يمكنك تعيين نطاق السياسات باستخدام العلامات أو مواقع الجهاز في الوحدات التنظيمية لـ Active Directory والعضوية في مجموعات الأمان الخاصة بـ Active Directory.

- تعيين نطاق المهام الجماعية

يوجد نهج لتحديد نطاق المهام الجماعية غير المستندة إلى التسلسل الهرمي لمجموعات الإدارة: استخدام المهام لتحديدات الأجهزة والمهام لأجهزة محددة.

- تعيين حقوق الوصول إلى الأجهزة وخوادم الإدارة الافتراضية وخوادم الإدارة الثانوية.
- تعيين نقاط التوزيع

عند بناء بنية مجموعات الإدارة، يجب عليك الأخذ في الاعتبار مخطط شبكة المؤسسة للتعيين الأمثل لنقاط التوزيع. يتيح التوزيع المثالي لنقاط التوزيع توفير الحركة على شبكة المؤسسة.

بناءً على المخطط المؤسسي ومخطط الشبكة، يمكن تطبيق التكوينات القياسية التالية على بنية مجموعات الإدارة:

- مكتب واحد
- مكاتب صغيرة متعددة بعيدة

يجب أن تكون الأجهزة التي تعمل كنقاط توزيع محمية، بما في ذلك الحماية الفعلية، وضد أي وصول غير مصرح به.

التكوين القياسي لنقاط التوزيع: مكتب واحد

في التكوين القياسي "مكتب واحد"، تكون كل الأجهزة داخل شبكة المؤسسة ويمكنها "رؤية" بعضها البعض. قد تتكون شبكة المؤسسة من عدد قليل من أجزاء منفصلة (الشبكات أو قطاعات الشبكة) التي ترتبط من خلال قنوات ضيقة.

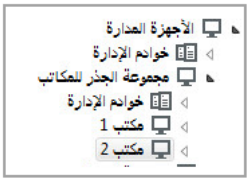
يمكن أن تتوفر الطرق التالية لبناء بنية مجموعات الإدارة:

- بناء بنية مجموعات الإدارة مع الأخذ في الاعتبار مخطط الشبكة. قد لا تعكس بنية مجموعات الإدارة مخطط الشبكة بالدقة المطلقة. قد يكون التطابق بين الأجزاء المنفصلة للشبكة ومجموعات الإدارة المحددة كافيًا. يمكنك استخدام التعيين التلقائي لنقاط التوزيع أو تعيينها يدويًا.
- بناء بنية مجموعات الإدارة دون أخذ مخطط الشبكة في الاعتبار. في هذه الحالة، يجب عليك تعطيل التعيين التلقائي لنقاط التوزيع ثم تعيين جهاز واحد أو عدة أجهزة للعمل كنقاط توزيع لمجموعة إدارة الجذر في كل جزء من الأجزاء المنفصلة للشبكة، على سبيل المثال، لمجموعة **الأجهزة المُدارة**. ستكون جميع نقاط التوزيع عند نفس المستوى وستتميز بنفس النطاق لتغطي جميع الأجهزة في شبكة المؤسسة. في هذه الحالة، سيتصل كل من عميل الشبكة بنقطة التوزيع التي تحتوي على أقصر مسار. يمكن تتبع المسار إلى نقطة توزيع عن طريق الأداة المساعدة tracert.

التكوين القياسي لنقاط التوزيع: مكاتب صغيرة متعددة بعيدة

يقدم هذا التكوين القياسي عدد من المكاتب الصغيرة البعيدة، والتي قد تتصل بالمكتب الرئيسي عبر الإنترنت. كل مكتب بعيد موجود وراء NAT، بمعنى أن الاتصال من مكتب بعيد إلى مكتب آخر غير ممكن لأن الأجهزة معزولة عن بعضها.

يجب أن ينعكس هذا التكوين في بنية مجموعات الإدارة: يجب إنشاء مجموعة إدارة منفصلة لكل مكتب بعيد (المجموعات **المكتب 1** و**المكتب 2** في الشكل الموجود أدناه).



يتم تضمين المكاتب البعيدة في بنية مجموعة الإدارة

يجب تعيين نقطة توزيع واحدة أو عدة نقاط توزيع لكل مجموعة إدارة مقابلة لمكتب ما. يجب أن تكون نقاط التوزيع أجهزة موجودة في المكتب البعيد تحتوي على مساحة قرص خالية كافية. ستتمكن الأجهزة التي تم نشرها في المجموعة **المكتب 1** على سبيل المثال، من الوصول إلى نقاط التوزيع المعينة لمجموعة الإدارة **المكتب 1**.

إذا كان بعض المستخدمين يتنقلون فعليًا بين المكاتب مع أجهزة الكمبيوتر المحمولة الخاصة بهم، فيجب عليك تحديد جهازين أو أكثر (بالإضافة إلى نقاط التوزيع الحاليين) في كل مكتب بعيد وتعيينهم للعمل كنقاط توزيع لمجموعة إدارة من المستوى الأعلى (**المجموعة الجذر للمكاتب** في الشكل الموجود أعلاه).

مثال: جهاز كمبيوتر محمول تم نشره في مجموعة الإدارة **المكتب 1** ثم انتقل فعليًا إلى مكتب مقابل لمجموعة الإدارة **المكتب 2**. بعد انتقال جهاز الكمبيوتر المحمول، يحاول عميل الشبكة الوصول إلى نقاط التوزيع المعينة إلى المجموعة **المكتب 1**، إلا إن هذه النقاط تكون غير متاحة. آنذاك، يحاول عميل الشبكة الوصول إلى نقاط التوزيع التي تم تعيينها إلى **المجموعة الجذر للمكاتب**. ولأن المكاتب البعيدة معزولة عن بعضها، فإن محاولات الوصول إلى نقاط التوزيع المعينة إلى مجموعة الإدارة **المجموعة الجذر للمكاتب** لن تكون ناجحة إلا عند محاولة عميل الشبكة الوصول إلى نقاط التوزيع في مجموعة **المكتب 2**. بمعنى أن جهاز الكمبيوتر المحمول سيظل في مجموعة الإدارة المقابلة للمكتب الأولي، ولكن جهاز الكمبيوتر المحمول سيستخدم نقطة التوزيع الخاصة بالمكتب الذي يوجد فيه فعليًا في الوقت الحالي.

عن تعيين نقاط التوزيع

يمكنك تعيين جهاز مُدار كنقطة توزيع يدويا أو تلقائيا.

إذا قمت بتعيين جهاز مُدار كنقطة توزيع يدويًا، فيمكنك تحديد أي جهاز في شبكتك.

إذا قمت بتعيين نقاط توزيع تلقائيًا، فيمكن لـ Kaspersky Security Center تحديد الجهاز المُدار الذي يستوفي الشروط التالية فقط:

- يحتوي الجهاز على 50 غيغابايت على الأقل من مساحة القرص الخالية.
- الجهاز المُدار متصل بـ Kaspersky Security Center مباشرةً (وليس من خلال البوابة).
- الجهاز المُدار ليس جهاز كمبيوتر محمول.

إذا كانت شبكتك لا تحتوي على أجهزة تستوفي الشروط المحددة، فلن يقوم Kaspersky Security Center بتعيين أي جهاز كنقطة توزيع تلقائيًا.

تعيين نقاط التوزيع تلقائيًا

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. في هذه الحالة، سيحدد Kaspersky Security Center بنفسه الأجهزة التي سيتم تعيين نقاط التوزيع لها.

لا يمكن للأجهزة التي تعمل بنظام التشغيل Microsoft Windows على معالجات Arm العمل كنقاط توزيع.

لتعيين نقاط التوزيع تلقائيًا:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **Distribution points**.
3. حدد خيار **Automatically assign distribution points**.

في حالة تمكين التعيين التلقائي للأجهزة كنقاط توزيع، سيتعذر عليك تكوين نقاط التوزيع يدويًا أو تحرير قائمة نقاط التوزيع.

4. انقر على زر **Save**.

يقوم خادم الإدارة بتعيين نقاط التوزيع وتكوينهم تلقائيًا.

تعيين نقاط التوزيع يدويًا

يتيح لك تطبيق Kaspersky Security Center تعيين أجهزة للعمل كنقاط توزيع.

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. في هذه الحالة، سيحدد Kaspersky Security Center بنفسه الأجهزة التي سيتم تعيين نقاط التوزيع لها. ومع ذلك، إذا اضطررت إلى إلغاء الاشتراك في تعيين نقاط التوزيع تلقائياً لأي سبب (على سبيل المثال، إذا كنت تريد استخدام خوادم مخصصة حصريًا)، يمكنك تعيين نقاط التوزيع يدويًا بعد حساب عدد نقاط التوزيع وتكوينها.

يجب أن تكون الأجهزة التي تعمل كنقاط توزيع محمية، بما في ذلك الحماية الفعلية، وضد أي وصول غير مصرح به.

لا يمكن للأجهزة التي تعمل بنظام التشغيل Microsoft Windows على معالجات Arm العمل كنقاط توزيع.

لتعيين جهاز للعمل كنقطة توزيع يدويًا:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب **General**، حدد قسم **Distribution points**.
3. حدد خيار **Manually assign distribution points**.
4. انقر على زر **Assign**.
5. حدد الجهاز الذي تريد أن تجعل فيه نقطة توزيع.
   عند تحديد جهاز، فيجب مراعاة ميزات تشغيل نقاط التوزيع والمتطلبات المحددة للجهاز الذي يعمل كنقطة توزيع.
6. حدد مجموعة الإدارة التي تريد تضمينها في نطاق نقطة التوزيع المحددة.
7. انقر على زر **OK**.
   سيتم عرض نقطة التوزيع التي أضفتها في قائمة نقاط التوزيع، في القسم **Distribution points**.
8. انقر فوق نقطة التوزيع التي تمت إضافتها مؤخرًا في القائمة لفتح نافذة خصائصه.
9. قم بتكوين نقطة التوزيع في نافذة الخصائص:
   - يحتوي القسم **General** على إعداد تفاعل نقطة التوزيع مع الأجهزة العميلة:
     - **SSL port**

       رقم منفذ SSL للاتصال المشفر بين الأجهزة العميلة ونقطة التوزيع باستخدام SSL.

       يتم استخدام المنفذ 13000 بشكل افتراضي.
     - **Use multicast**

       إذا تم تمكين هذا الخيار، فسوف يتم استخدام البث المتعدد لـ IP في التوزيع التلقائي لحزم التثبيت على أجهزة العميل داخل المجموعة.

       يقلل الإرسال المتعدد لعنوان IP الوقت اللازم لتثبيت تطبيق من حزمة تثبيت على مجموعة من أجهزة العملاء، ولكنه يزيد من وقت التثبيت عند تثبيت تطبيق على جهاز عميل واحد.

- **IP multicast address**

عنوان IP الذي سيتم استخدامه للإرسال المتعدد. يمكنك تحديد عنوان IP في نطاق 224.0.0.0 – 239.255.255.255

بشكل افتراضي، يقوم تطبيق Kaspersky Security Center تلقائيًا بتعيين عنوان IP متعدد الإرسال فريد ضمن النطاق المحدد.

- **IP multicast port number**

رقم منفذ الإرسال المتعدد لعنوان IP.

رقم المنفذ هو 15001 بشكل افتراضي. في حالة تحديد الجهاز المثبت عليه خادم الإدارة كنقطة التوزيع، فسيتم بشكل افتراضي استخدام المنفذ 13001 لاتصال SSL.

- **عنوان نقطة التوزيع للأجهزة البعيدة**

عنوان الشبكة الذي تتصل من خلاله الأجهزة البعيدة بنقطة التوزيع.

- **Deploy updates**

يتم توزيع التحديثات على الأجهزة المدارة من المصادر التالية:

  - نقطة التوزيع هذه، إذا تم تمكين هذا الخيار.
  - نقاط التوزيع الأخرى أو خادم الإدارة أو خوادم تحديث Kaspersky، إذا تم تعطيل هذا الخيار.

إذا كنت تستخدم نقاط التوزيع لنشر التحديثات، فيمكنك حفظ حركة المرور لأنك تقلل عدد التنزيلات. يمكنك أيضًا تخفيف الحمل على خادم الإدارة ونقل الحمل بين نقاط التوزيع. يمكنك حساب عدد نقاط التوزيع لشبكتك لتحسين حركة البيانات والتحميل.

إذا قمت بتعطيل هذا الخيار، فقد يزيد عدد تنزيلات التحديث وتحميلها على خادم الإدارة. يتم تمكين هذا الخيار افتراضيًا.

- **Deploy installation packages**

يتم توزيع حزم التثبيت على الأجهزة المُدارة من المصادر التالية:

  - نقطة التوزيع هذه، إذا تم تمكين هذا الخيار.
  - نقاط التوزيع الأخرى أو خادم الإدارة أو خوادم تحديث Kaspersky، إذا تم تعطيل هذا الخيار.

إذا كنت تستخدم نقاط التوزيع لنشر حزم التثبيت، فيمكنك توفير حركة البيانات لأنك تقلل عدد التنزيلات. يمكنك أيضًا تخفيف الحمل على خادم الإدارة ونقل الحمل بين نقاط التوزيع. يمكنك حساب عدد نقاط التوزيع لشبكتك لتحسين حركة البيانات والتحميل.

إذا قمت بتعطيل هذا الخيار، فقد يزيد عدد تنزيلات حزمة التثبيت وتحميلها على خادم الإدارة. يتم تمكين هذا الخيار افتراضيًا.

- **Run push server**

في Kaspersky Security Center، يمكن أن تعمل نقطة التوزيع كخادم دفع للأجهزة المدارة من خلال بروتوكول الهاتف المحمول وللأجهزة التي يديرها وكيل الشبكة. على سبيل المثال، يجب تمكين خادم الإرسال إذا كنت تريد أن تكون قادرًا على فرض المزامنة لأجهزة KasperskyOS المزودة بخادم الإدارة. خادم الإرسال لديه نفس نطاق الأجهزة المدارة التي تعمل كنقطة التوزيع حيث يتم فيها تمكين خادم الإرسال. إذا كان لديك العديد من نقاط التوزيع المخصصة لمجموعة الإدارة نفسها، فيمكنك تمكين خادم الإرسال في كل نقطة من نقاط التوزيع. في هذه الحالة، يوازن خادم الإدارة التحميل بين نقاط التوزيع.

- **Push server port**

رقم منفذ خادم الإرسال. يمكنك تحديد رقم أي منفذ فارغ.

- في قسم **Scope**، حدد النطاق الذي سيتقوم نقطة التوزيع بتوزيع التحديثات إليه (مجموعات الإدارة و / أو موقع الشبكة).

يمكن للأجهزة التي تعمل بنظام تشغيل Windows فقط تحديد موقع شبكتها. لا يمكن تحديد موقع الشبكة للأجهزة التي تعمل بأنظمة تشغيل أخرى.

- إذا كانت نقطة التوزيع تعمل على جهاز آخر غير خادم الإدارة، في القسم **Source of updates**، يمكنك تحديد مصدر التحديثات لنقطة التوزيع:

- **مصادر التحديثات**

  حدد مصدر تحديثات لنقطة التوزيع:

  - للسماح لنقطة التوزيع بتلقي التحديثات من خادم الإدارة، حدد **Retrieve from Administration Server**.

  - للسماح لنقطة التوزيع بتلقي التحديثات باستخدام مهمة، حدد **Use update download task**، ثم حدد المهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع:

    - إذا كانت هذه المهمة موجودة بالفعل على الجهاز، فحدد المهمة من القائمة.

    - في حالة عدم وجود مثل هذه المهمة حتى الآن على الجهاز، انقر فوق الرابط **Create task** لإنشاء مهمة. سيبدأ معالج المهمة الجديدة. اتبع إرشادات المعالج.

- **Download diff files**

  يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.

  يتم تمكين هذا الخيار افتراضيًا.

- إذا كانت نقاط التوزيع الخاصة بك تستخدم خادمًا وكيلاً عند الاتصال بالإنترنت، ففي القسم الفرعي **إعدادات الاتصال بالإنترنت**، يمكنك تحديد الإعدادات التالية:

- **Use proxy server**

  في حالة تحديد خانة الاختيار هذه، سيتم استخدام خادم وكيل للإنترنت لتوصيل نقاط التوزيع بخوادم التحديث لدى Kaspersky. وفي حقول الإدخال، يمكنك تكوين اتصال الخادم الوكيل.

  تكون خانة الاختيار غير محددة بشكل افتراضي.

- **عنوان الخادم الوكيل**

  عنوان الخادم الوكيل.

- **رقم المنفذ**

  رقم المنفذ المستخدم في الاتصال.

- **Bypass proxy server for local addresses**

  إذا تم تمكين هذا الخيار، فلن يتم استخدام خادم الوكيل للاتصال بالأجهزة على الشبكة المحلية.

  يتم تعطيل هذا الخيار افتراضيًا.

- **Proxy server authentication**

  إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

  تكون خانة الاختيار غير محددة بشكل افتراضي.

- **User name**

  حساب المستخدم الذي من خلاله تم إنشاء اتصال بخادم الوكيل.

- **Password**

  كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

- من القسم **KSN Proxy**، يمكنك تكوين التطبيق لاستخدام نقطة التوزيع لإعادة توجيه طلبات KSN من الأجهزة المدارة:

- **Enable KSN Proxy on the distribution point side**

تعمل خدمة وكيل KSN على الجهاز المستخدم كنقطة توزيع. استخدم هذه الميزة لإعادة توزيع حركة مرور البيانات في الشبكة وتحسينها.

ترسل نقطة التوزيع إحصاءات KSN المُدرجة في بيان Kaspersky Security Network إلى Kaspersky.

يتم تعطيل هذا الخيار افتراضيًا. يسري تمكين هذا الخيار فقط في حالة تمكين الخيارين **Use Administration Server as a proxy server** و**I agree to use Kaspersky Security Network** في نافذة خصائص خادم الإدارة.

يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل خادم KSN على هذه العقدة.

- **Forward KSN requests to Administration Server**

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المدارة إلى خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **Access KSN Cloud/KPSN directly over the internet**

تعيد نقطة التوزيع توجيه طلبات KSN من الأجهزة المُدارة إلى KSN Cloud أو KPSN. يتم أيضًا إرسال طلبات KSN – التي تم إنشاؤها على نقطة التوزيع نفسها – مباشرةً إلى KSN Cloud أو PKSN.

لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى KPSN مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KPSN، فقم بتمكين خيار **توجيه طلبات KSN إلى خادم الإدارة** لكل نقطة توزيع.

لا يمكن لنقاط التوزيع التي لديها الإصدار 12 المثبت من Network Agent (أو إصدار أقدم)، الوصول إلى KPSN مباشرةً.

- **Ignore proxy server settings when connecting to KPSN**

قم بتمكين هذا الخيار، إذا كانت إعدادات الخادم الوكيل مكوّنة في خصائص نقطة التوزيع أو في سياسة عميل الشبكة، لكن كانت بنية شبكتك تتطلب استخدام شبكة KPSN مباشرةً. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المُدارة إلى شبكة KPSN.

يتوفر هذا الخيار إذا حددت الخيار **Access KSN Cloud/KPSN directly over the internet**.

- **المنفذ**

رقم منفذ TCP الذي ستستخدمه الأجهزة المُدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

- **استخدام منفذ UDP**

إذا احتجت لأن تكون الأجهزة المُدارة متصلة بالخادم الوكيل لشبكة KSN عبر منفذ UDP، فقم بتمكين الخيار **استخدام منفذ UDP** وحدد رقم منفذ UDP. يتم تمكين هذا الخيار افتراضيًا.

- **منفذ UDP.**

رقم منفذ UPD الذي ستستخدمه الأجهزة المُدارة للاتصال بخادم وكيل KSN. والمنفذ الافتراضي لـ UDP للاتصال بخادم وكيل KSN هو 15111.

- إذا كانت نقطة التوزيع تعمل على جهاز آخر غير خادم الإدارة، في القسم **بوابة الاتصال**، يمكنك تكوين نقطة التوزيع لتعمل كبوابة للاتصال بين مثيلات عميل الشبكة وخادم الإدارة:

- **Connection gateway**

إذا تعذر إنشاء اتصال مباشر بين خادم الإدارة وعملاء الشبكة بسبب تنظيم شبكتك، يمكنك استخدام نقطة التوزيع للعمل كبوابة اتصال بين خادم الإدارة وعملاء الشبكة.

قم بتمكين هذا الخيار إذا كنت بحاجة لأن تعمل نقطة التوزيع كبوابة اتصال بين عملاء الشبكة وخادم الإدارة. يتم تعطيل هذا الخيار افتراضيًا.

- **Establish connection to gateway from Administration Server (if gateway is in DMZ)**

إذا كان خادم الإدارة موجودًا خارج منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)، على شبكة المنطقة المحلية، لن يتمكن عملاء الشبكة المثبتون على الأجهزة البعيدة من الاتصال بخادم الإدارة. ويمكنك استخدام نقطة توزيع كبوابة اتصال مع اتصال عكسي (ينشئ خادم الإدارة اتصالاً بنقطة التوزيع).

قم بتمكين هذا الخيار إذا كنت بحاجة إلى توصيل خادم الإدارة ببوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

- **Open local port for Kaspersky Security Center Web Console**

قم بتمكين هذا الخيار إذا كنت بحاجة لأن تفتح بوابة الاتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت منفذًا لمكون Web Console الموجودة في المنطقة العازلة أو على الإنترنت. حدد رقم المنفذ الذي سيتم استخدامه للاتصال من Web Console إلى نقطة التوزيع. رقم المنفذ الافتراضي هو 13299.

يتوفر هذا الخيار إذا قمت بتمكين الخيار **Establish connection to gateway from Administration Server (if gateway is in DMZ)**.

عند توصيل الأجهزة المحمولة بخادم الإدارة عبر نقطة التوزيع التي تعمل كبوابة اتصال، يمكنك تمكين الخيارات التالية:

- **Open port for mobile devices (SSL authentication of the Administration Server only)**

قم بتمكين هذا الخيار إذا كنت بحاجة لأن تفتح بوابة الاتصال منفذًا للأجهزة المحمولة وحدد رقم المنفذ الذي ستستخدمه الأجهزة المحمولة للاتصال بنقطة التوزيع. رقم المنفذ الافتراضي هو 13292. وسيتحقق الجهاز المحمول من شهادة خادم الإدارة. عند إنشاء الاتصال، تتم مصادقة خادم الإدارة فقط.

- **Open port for mobile devices (two-way SSL authentication)**

قم بتمكين هذا الخيار إذا كنت بحاجة لأن تفتح بوابة الاتصال منفذًا للمصادقة ثنائية الاتجاه لخادم الإدارة والأجهزة المحمولة. وسيتحقق الجهاز المحمول من شهادة خادم الإدارة، وسيفحص خادم الإدارة شهادة الجهاز المحمول. حدد المعاملات التالية:

- رقم المنفذ الذي ستستخدمه الأجهزة المحمولة للاتصال بنقطة التوزيع. رقم المنفذ الافتراضي هو 13293.

- أسماء مجال DNS لبوابة الاتصال التي ستستخدمها الأجهزة المحمولة. افصل بين أسماء المجال بفواصل. سيتم تضمين أسماء المجال المحددة في شهادة نقطة التوزيع. إذا كانت أسماء المجال التي تستخدمها الأجهزة المحمولة لا تتطابق مع الاسم الشائع في شهادة نقطة التوزيع، فإن الأجهزة المحمولة لا تتصل بنقطة التوزيع.

  اسم مجال DNS الافتراضي هو اسم FQDN لبوابة الاتصال.

في كلتا الحالتين، يتم فحص الشهادات أثناء إنشاء جلسة TLS على نقطة التوزيع فقط. ولا تتم إعادة توجيه الشهادات ليتم فحصها بواسطة خادم الإدارة. وبعد إنشاء جلسة TLS مع الجهاز المحمول، تستخدم نقطة التوزيع شهادة خادم الإدارة لإنشاء قناة للمزامنة بين الجهاز المحمول وخادم الإدارة. وإذا فتحت المنفذ لمصادقة SSL ثنائية الاتجاه، فإن الطريقة الوحيدة لتوزيع شهادة الجهاز المحمول هي عبر حزمة التثبيت.

- قم بتكوين استقصاء مجالات Windows، وActive Directory، ونطاقات IP بواسطة نقطة التوزيع:

- **مجالات Windows**

يمكنك تمكين اكتشاف الأجهزة لمجالات Windows وتعيين الجدول للاكتشاف.

- **وحدات تحكم المجال**

يمكنك تمكين استقصاء الشبكة لـActive Directory وتعيين الجدول للاستقصاء.

إذا كنت تستخدم نقطة توزيع Windows، يمكنك تحديد أحد الخيارات التالية:

- **استقصاء مجال Active Directory الحالي**.

- **استقصاء مجال Active Directory الرئيسي**.

- **استقصاء مجالات Active Directory المحددة فقط**. إذا قمت بتحديد هذا الخيار، فقم بإضافة واحد أو أكثر من مجالات Active Directory إلى هذه القائمة.

إذا كنت تستخدم نقطة توزيع Linux مُثبت عليها الإصدار 15 من عميل الشبكة، يمكنك استقصاء نطاقات Active Directory فقط التي تحدد لها العنوان وبيانات اعتماد المستخدم. لا يتوفر استقصاء مجال Active Directory الحالي ومجال Active Directory الرئيسي.

يمكنك تمكين اكتشاف الأجهزة لوحدات تحكم المجال.

إذا حددت الخيار **Enable domain controller polling**، فيمكنك تحديد وحدات تحكم المجال للاستقصاء وكذلك تحديد جدول الاستقصاء لها.

إذا كنت تستخدم نقطة توزيع نظام Linux، في القسم **Poll specified domains**، انقر فوق **Add**، ثم حدد العنوان وبيانات اعتماد المستخدم لوحدة تحكم المجال.

إذا كنت تستخدم نقطة توزيع Windows، يمكنك تحديد أحد الخيارات التالية:

- **Poll current domain**
- **Poll entire domain forest**
- **Poll specified domains**

- **نطاقات IP**

يمكنك تمكين اكتشاف الجهاز لنطاقات IPv4 وشبكات IPv6.

إذا مكنت خيار **تمكين استقصاء النطاق** ، فيمكنك إضافة نطاقات ممسوحة ضوئيًا وتعيين الجدول الزمني لها. يمكنك إضافة نطاقات IP لقائمة النطاقات التي تم فحصها.

إذا قمت بتمكين الخيار **Use Zeroconf to poll IPv6 networks**، ستقوم نقطة التوزيع تلقائيًا باستقصاء شبكة IPv6 باستخدام شبكات التكوين الصفري (يشار إليها أيضًا باسم شبكة لا تتطلب تكوينًا). في هذه الحالة، يتم تجاهل نطاقات IP المحددة لأن نقطة التوزيع تستقصي الشبكة بالكامل. يتوفر الخيار **Use Zeroconf to poll IPv6 networks** إذا كانت نقطة التوزيع تعمل بنظام Linux. لاستخدام استقصاء IPv6 لشبكة لا تتطلب تكوينًا، يجب عليك تثبيت أداة استعراض avahi على نقطة التوزيع.

- في القسم **خيارات متقدمة**، حدد المجلد الذي يجب أن تستخدمه نقطة التوزيع لتخزين البيانات التي تم توزيعها:

- **استخدام المجلد الافتراضي**

إذا حددت هذا الخيار، سيستخدم التطبيق مجلد تثبيت عميل الشبكة على نقطة التوزيع.

- **استخدام المجلد المعين**

في حالة تحديد هذا الخيار، يمكنك تحديد المسار الخاص بالمجلد في الحقل الموجود أدناه. قد يكون مجلد محلي على نقطة التوزيع أو يمكن أن يكون مجلد على أي جهاز في شبكة الشركة.

يجب أن يمتلك حساب المستخدم الذي يتم استخدامه على نقطة التوزيع لتشغيل عميل الشبكة وصولاً إلى المجلد المحدد للقراءة والكتابة.

10. انقر على زر **OK**.

تعمل الأجهزة المحددة كنقاط توزيع.

تعديل قائمة نقاط التوزيع لمجموعة إدارة

يمكنك عرض قائمة بنقاط التوزيع المخصصة إلى مجموعة إدارة محددة وتعديل القائمة بإضافة نقاط توزيع أو حذفها.

لعرض قائمة نقاط التوزيع المخصصة لمجموعة إدارة وتعديلها:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.
2. في الحقل **Current path** أعلى قائمة الأجهزة المُدارة، انقر فوق ارتباط المسار.
3. في الجزء الأيمن الذي يفتح، حدد مجموعة إدارة ترغب في عرض نقاط التوزيع المعينة لها.
   يؤدي ذلك إلى تمكين عنصر القائمة **Distribution points**.
4. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Distribution points**.

5. لإضافة نقاط توزيع جديدة لمجموعة الإدارة، انقر فوق الزر **Assign** أعلى قائمة الأجهزة المُدارة وحدد الأجهزة من الجزء الذي يفتح.

6. لإزالة نقاط التوزيع المعينة، حدد الأجهزة من القائمة وانقر فوق الزر **Unassign**.

اعتمادًا على التعديلات، يتم إضافة نقاط التوزيع الجديدة إلى القائمة أو يتم إزالة نقاط التوزيع الموجودة من القائمة.

المزامنة المفروضة

على الرغم من أن Kaspersky Security Center يقوم تلقائيًا بمزامنة حالة الأجهزة المُدارة وإعداداتها ومهامها وسياساتها، فقد ترغب في بعض الحالات في تشغيل مزامنة جهاز معين بالقوة. يمكنك تشغيل المزامنة المفروضة للأجهزة التالية:

- الأجهزة المثبت عليها عميل الشبكة
- الأجهزة التي تعمل بنظام KasperskyOS

  قبل تشغيل المزامنة المفروضة لجهاز KasperskyOS، تأكد من تضمين الجهاز في نطاق نقطة التوزيع وتمكين خادم الإرسال على نقطة التوزيع.
- أجهزة iOS
- أجهزة Android

  قبل تشغيل المزامنة المفروضة لجهاز يعمل بنظام Android، يجب عليك تكوين Firebase Cloud Messaging.

مزامنة جهاز واحد

لفرض المزامنة بين خادم الإدارة وجهاز مُدار:

1. في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)**.
2. انقر على اسم الجهاز الذي ترغب في مزامنته مع خادم الإدارة.

   ستفتح نافذة خصائص مع قسم **General** محدد.
3. انقر على زر **Force synchronization** .

   يقوم التطبيق بمزامنة الجهاز المحدد مع خادم الإدارة.

مزامنة عدة أجهزة

لفرض المزامنة بين خادم الإدارة وعدة أجهزة مُدارة:

1. افتح قائمة الجهاز لمجموعة إدارة أو تحديد جهاز:

- في القائمة الرئيسية ، انتقل إلى **Managed devices** ←**Assets (Devices)**، وانقر فوق ارتباط المسار في الحقل **Current path** أعلى قائمة الأجهزة المُدارة، ثم حدد مجموعة الإدارة التي تحتوي على أجهزة لمزامنتها.
- أجر تحديد جهاز لعرض قائمة الجهاز.

2. حدد خانات الاختيار الموجودة بجوار الأجهزة التي ترغب في مزامنتها مع خادم الإدارة.

3. فوق قائمة الأجهزة المدارة ، انقر فوق زر علامة القطع (...) ، ثم انقر فوق الزر **Force synchronization**.

يقوم التطبيق بمزامنة الأجهزة المحددة مع خادم الإدارة.

4. من قائمة الجهاز، تأكد أن وقت آخر اتصال بخادم الإدارة قد تغير للأجهزة المحددة ليصبح الوقت الحالي. إذا لم يتغير الوقت، قم بتحديث محتوى الصفحة بالنقر على زر **Refresh**.

تتم مزامنة الأجهزة المحددة مع خادم الإدارة.

عرض وقت توصيل سياسة

بعد تغيير سياسة لتطبيق Kaspersky على خادم الإدارة، يمكن للمدير التحقق مما إذا قد تم توصيل السياسة التي تم تغييرها إلى جهاز مُدار محدد أم لا. يمكن توصيل سياسة أثناء المزامنة العادية أو المزامنة المفروضة.

لعرض تاريخ ووقت توصيل سياسة تطبيق إلى جهاز مُدار:

1. في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)**.

2. انقر على اسم الجهاز الذي ترغب في مزامنته مع خادم الإدارة.

ستفتح نافذة خصائص مع قسم **General** محدد.

3. حدد علامة التبويب **Applications**.

4. حدد التطبيق الذي ترغب في عرض تاريخ مزامنة السياسة له.

ستفتح نافذة سياسة التطبيق مع تحديد قسم **General** وعرض تاريخ ووقت توصيل السياسة.

تمكين خادم الإرسال

في Kaspersky Security Center، يمكن أن تعمل نقطة التوزيع كخادم دفع للأجهزة المدارة من خلال بروتوكول الهاتف المحمول وللأجهزة التي يديرها عميل الشبكة. على سبيل المثال، يجب تمكين خادم الإرسال إذا كنت تريد أن تكون قادرًا على فرض المزامنة لأجهزة KasperskyOS المزودة بخادم الإدارة. خادم الإرسال لديه نفس نطاق الأجهزة المدارة التي تعمل كنقطة التوزيع حيث يتم فيها تمكين خادم الإرسال. إذا كان لديك العديد من نقاط التوزيع المخصصة لمجموعة الإدارة نفسها، فيمكنك تمكين خادم الإرسال في كل نقطة من نقاط التوزيع. في هذه الحالة، يوازن خادم الإدارة التحميل بين نقاط التوزيع.

قد ترغب في استخدام نقاط التوزيع كخوادم دفع للتأكد من وجود اتصال مستمر بين الجهاز المُدار وخادم الإدارة. يلزم الاتصال المستمر لبعض العمليات، مثل تشغيل المهام المحلية وإيقافها، أو تلقي إحصائيات لتطبيق مُدار، أو إنشاء نفق. إذا كنت تستخدم نقطة توزيع كخادم دفع، فلن تضطر إلى استخدام خيار **عدك قطع الاتصال بخادم الإدارة** على الأجهزة المدارة أو إرسال الحزم إلى منفذ UDP الخاص بوكيل الشبكة.

يدعم خادم الدفع تحميل ما يصل إلى 50 000 اتصال متزامن.

لتمكين خادم الإرسال على نقطة توزيع:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد قسم **Distribution points**.

3. انقر فوق اسم نقطة التوزيع التي تريد تمكين خادم الإرسال عليها.

يتم فتح نافذة خصائص نقطة التوزيع.

4. في قسم **General**، مكّن خيار **Run push server**.

5. في حقل **Push server port**، اكتب رقم المنفذ. يمكنك تحديد رقم أي منفذ فارغ.

6. في حقل **عنوان المضيفين عن بُعد**، حدد عنوان IP أو اسم جهاز نقطة التوزيع.

7. انقر على زر **OK**.

يتم تمكين خادم الإرسال على نقطة التوزيع المحددة.

إدارة تطبيقات الجهات الخارجية على أجهزة العميل

يصف هذا القسم مزايا Kaspersky Security Center المتعلقة بإدارة تطبيقات الأطراف الخارجية المثبتة على أجهزة العميل.

تثبيت تحديثات برامج الجهات الخارجية

يقوم Kaspersky Security Center بتمكينك من إدارة تحديثات برامج الأطراف الخارجية المثبتة على الأجهزة المُدارة وإصلاح الثغرات الأمنية في تطبيقات Microsoft ومنتجات الصناع الآخرين للبرامج من خلال تثبيت التحديثات المطلوبة.

Kaspersky Security Center يبحث عن التحديثات من خلال مهمة Find vulnerabilities and required updates. عند اكتمال هذه المهمة، يتلقى خادم الإدارة قوائم بالثغرات الأمنية المُكتشَفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة. بعد عرض معلومات حول التحديثات المتوفرة، يمكن تثبيتها على الأجهزة.

يقوم Kaspersky Security Center بتحديث بعض التطبيقات عن طريق إزالة الإصدار السابق للتطبيق وتثبيت الإصدار الجديد.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

لأسباب تتعلق بالأمان، يتم تلقائيًا فحص أي تحديثات برامج، تابعة لطرف ثالث، تقوم بتثبيتها باستخدام ميزة إدارة الثغرات الأمنية والتصحيحات بحثًا عن البرامج الضارة بواسطة تقنيات Kaspersky. تُستخدم هذه التقنيات لعمليات فحص الملفات بشكل تلقائي، وتتضمن فحص الفيروسات، وتحليلًا ثابتًا، وتحليلًا ديناميكيًا، وتحليل السلوك في بيئة وضع الحماية والتعلم الآلي.

لا يقوم خبراء Kaspersky بإجراء تحليل يدوي لتحديثات برامج الجهات الخارجية التي يمكن تثبيتها من خلال استخدام ميزة إدارة الثغرات الأمنية والتصحيحات. بالإضافة إلى ذلك، لا يبحث خبراء Kaspersky عن الثغرات الأمنية (المعروفة أو غير المعروفة) أو الميزات غير الموثقة في مثل هذه التحديثات، ولا يجرون أنواعًا أخرى من تحليل التحديثات بخلاف تلك المحددة في الفقرة أعلاه.

مهام تثبيت تحديثات برامج الجهات الخارجية

عند تنزيل بيانات تعريف تحديثات برامج الجهات الخارجية إلى المستودع، يمكنك تثبيت التحديثات على أجهزة العميل باستخدام المهام التالية:

- مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية

  تُستخدم مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية في تثبيت التحديثات لتطبيقات Microsoft، بما في ذلك التحديثات التي توفرها خدمة Windows Update وتحديثات برامج البائعين الآخرين. لاحظ أنه لا يمكن إنشاء هذه المهمة إلا إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات.

  عند اكتمال المهمة، يتم تثبيت التحديثات على الأجهزة المُدارة تلقائيًا. عند تنزيل بيانات تعريف تحديثات جديدة إلى مستودع خادم الإدارة، يتحقق Kaspersky Security Center من استيفاء التحديثات للمعايير المحددة في قواعد التحديث. سوف يتم تنزيل جميع التحديثات الجديدة التي تستوفي المعايير وتثبيتها تلقائيًا عند التشغيل التالي للمهمة.

- مهمة تثبيت تحديثات Windows Update

لا تتطلب مهمة تثبيت تحديثات Windows Update ترخيصًا، ولكن يمكن استخدامها لتثبيت تحديثات Windows Update فقط.

عند اكتمال هذه المهمة، لا يتم تثبيت إلا تلك التحديثات المحددة في خصائص المهمة. في المستقبل إذا أردت تثبيت التحديثات الجديدة التي يتم تنزيلها إلى مستودع خادم الإدارة، يجب أن تضيف التحديثات المطلوبة إلى قائمة التحديثات في المهمة الموجودة أو إنشاء مهمة تثبيت تحديثات Windows Update جديدة.

باستخدام خادم الإدارة كخادم WSUS

يتم تقديم معلومات حول التحديثات المتوفرة لـ Microsoft Windows بواسطة خدمة Windows Update. يمكن استخدام خادم الإدارة كخادم Windows Server Update Services (WSUS). لاستخدام خادم الإدارة كخادم WSUS، قم بإنشاء مهمة إجراء مزامنة Windows Update وحدد خيار **استخدام خادم الإدارة كخادم WSUS** في سياسة عميل الشبكة. بعد تكوين مزامنة البيانات مع Windows Update، يوفر خادم الإدارة تحديثات لخدمات Windows Update على الأجهزة في الوضع المركزي ومع التكرار المضبوط.

السيناريو: تحديث برامج الجهات الخارجية

يوفر هذا القسم سيناريو لتحديث برامج الأطراف الخارجية المثبتة على أجهزة العميل. برنامج الجهة الخارجية يشتمل على تطبيقات من Microsoft وبائعي البرامج الآخرين. يتم توفير تحديثات تطبيقات Microsoft عبر خدمة Windows Update.

المتطلبات الأساسية

يجب أن يكون خادم الإدارة متصلاً بالإنترنت من أجل تثبيت تحديثات تطبيقات الأطراف الخارجية غير تطبيقات Microsoft.

بشكل افتراضي، لا يلزم اتصال خادم الإدارة بالإنترنت لتثبيت تحديثات برامج Microsoft على الأجهزة المدارة. على سبيل المثال، يمكن للأجهزة المدارة تنزيل تحديثات برامج Microsoft مباشرة من خوادم تحديث Microsoft أو من خادم Windows وخدمات تحديث خادم Microsoft Windowsالمنتشرة في شبكة مؤسستك. يجب أن يكون خادم الإدارة متصلاً بالإنترنت عند استخدامك لخادم الإدارة كخادم WSUS.

المراحل

تحديث برامج الجهات الخارجية يسري عبر مراحل:

1. **البحث عن التحديثات المطلوبة**

للعثور على تحديثات برامج الأطراف الخارجية المطلوبة للأجهزة المُدارة، قم بتشغيل مهمة Find vulnerabilities and required updates. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المُكتشَفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

يتم إنشاء مهمة Find vulnerabilities and required updates تلقائيًا بواسطة معالج البدء السريع لخادم الإدارة. إذا لم تشغِّل المعالج، فقم بإنشاء المهمة أو تشغيل معالج البدء السريع الآن.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: فحص التطبيقات بحثًا عن الثغرات الأمنية، وجدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
- Kaspersky Security Center Web Console: إنشاء Find vulnerabilities and required updates المهمة، والبحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة

2 تحليل قائمة التحديثات التي تم العثور عليها

اعرض قائمة **Software updates** وحدد التحديثات التي ترغب في تثبيتها. لعرض معلومات تفصيلية حول كل تحديث، انقر على اسم التحديث في القائمة. لكل تحديث في القائمة، يمكنك أيضًا عرض إحصاءات حول تثبيت التحديث على أجهزة العميل.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: عرض معلومات حول التحديثات المتوفرة
- Kaspersky Security Center Web Console: عرض معلومات حول تحديثات برامج الجهات الخارجية المتوفرة

3 تكوين تثبيت التحديثات

عندما استلم Kaspersky Security Center قائمة تحديثات برامج الأطراف الخارجية، يمكنك تثبيتها على أجهزة العميل باستخدام مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو مهمة تثبيت تحديثات Windows Update. قم بإنشاء إحدى المهام التالية. يمكنك إنشاء هذه المهام في تبويب **Tasks** أو باستخدام قائمة **Software updates**.

تُستخدم مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية في تثبيت التحديثات لتطبيقات Microsoft، بما في ذلك التحديثات التي توفرها خدمة Windows Update وتحديثات برامج البائعين الآخرين. لاحظ أنه لا يمكن إنشاء هذه المهمة إلا إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات.

لا تتطلب مهمة تثبيت تحديثات Windows Update ترخيصًا، ولكن يمكن استخدامها لتثبيت تحديثات Windows Update فقط.

لتثبيت بعض تحديثات البرامج، يجب أن توافق على اتفاقية ترخيص المستخدم النهائي لبرنامج التثبيت. إذا رفضت اتفاقية ترخيص المستخدم النهائي، لن يتم تثبيت تحديث البرنامج.

يمكنك بدء مهمة تثبيت التحديث بالجدول. عند تحديد جدول المهام، تأكد من بدء مهمة تثبيت التحديث بعد اكتمال مهمة Find vulnerabilities and required updates.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إصلاح الثغرات الأمنية في التطبيقات، عرض معلومات حول التحديثات المتوفرة
- Kaspersky Security Center Web Console: إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، إنشاء مهمة تثبيت تحديثات Windows Update، عرض معلومات حول تحديثات برامج الجهات الخارجية المتوفرة

4 جدولة المهام

للتأكد من أن قائمة التحديث مُحدَّثة دائمًا، قم بجدولة مهمة Find vulnerabilities and required updates لتشغيل المهمة تلقائيًا من وقتٍ لآخر. بشكل افتراضي، يتم تحديد مهمة Find vulnerabilities and required updates لكي تبدأ يدويًا.

إذا كنت قد أنشأت مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك جدولتها لتعمل بالتكرار نفسه الذي تعمل به مهمة Find vulnerabilities and required updates أو أقل منه. عند جدولة مهمة تثبيت تحديثات Windows Update، لاحظ أنه من أجل هذه المهمة يجب أن تحدد قائمة التحديثات في كل مرة قبل بدء هذه المهمة.

عند جدولة المهام، تأكد من بدء مهمة تثبيت التحديث بعد اكتمال مهمة Find vulnerabilities and required updates.

5 الموافقة على تحديثات البرامج ورفضها (اختياري)

إذا كنت قد أنشأت مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك تحديد قواعد تثبيت التحديثات في خصائص المهمة. إذا كنت قد أنشأت مهمة تثبيت تحديثات Windows Update، يمكنك تخطي هذه الخطوة.

يمكنك لكل قاعدة تحديد التحديثات المراد تثبيتها اعتمادًا على حالة التحديث: غير محدد أو مقبول أو مرفوض. قد ترغب على سبيل المثال في إنشاء مخمة محددة للخوادم ووضع قاعدة لهذه المهمة من أجل السماح بتثبيت تحديثات Windows Update وفقط التحديثات التي بحالة مقبول. بعدها أنت تقوم يدويًا بتعيين حالة مقبول للتحديثات التي ترغب في تثبيتها. في هذه الحالة، لن يتم تثبيت تحديثات Windows Update التي بحالة غير محدد أو مرفوض على الخوادم التي حددتها في المهمة.

استخدام حالة مقبول لإدارة تثبيت التحديث أمر فعال لعدد صغير من التحديثات. لتثبيت عدة تحديثات، استخدم القواعد التي يمكنك تكوينها في مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. نوصي بتعيين حالة الموافقة لتلك التحديثات المحددة التي لا تفي بالمعايير المحددة في القواعد. عند الموافقة بشكل يدوي على عدد كبير من التحديثات، ينخفض أداء خادم الإدارة مما قد ينتج عنه التحميل الزائد على الخادم.

بشكل افتراضي، يكون لتحديثات البرامج التي تم تنزيلها حالة غير محددة. يمكنك تغيير الحالة إلى مقبول أو مرفوض في قائمة **Software updates** (**Operations** ← **Patch management** ← **Software updates**).

تعليمات للمساعدة:

- وحدة تحكم الإدارة: الموافقة على تحديثات البرامج ورفضها
- Kaspersky Security Center Web Console: الموافقة على تحديثات برامج الأطراف الخارجية ورفضها

6 **تكوين خادم الإدارة للعمل كخادم Windows Server Update Services (WSUS) (اختياري)**

يتم تنزيل تحديثات Windows Update بشكل افتراضي إلى الأجهزة المُدارة من خوادم Microsoft. يمكنك تغيير هذا الإعداد لاستخدام خادم الإدارة كخادم WSUS. يقوم خادم الإدارة في هذه الحالة بمزامنة بيانات التحديث مع Windows Update بالتكرار المحدد ويوفر تحديثات في وضع مركزي إلى Windows Update على الأجهزة المتصلة بالشبكة.

لاستخدام خادم الإدارة كخادم WSUS، قم بإنشاء مهمة إجراء مزامنة Windows Update وحدد خانة الاختيار **استخدام خادم الإدارة كخادم WSUS** في سياسة عميل الشبكة.

تعليمات للمساعدة:

- خادم الإدارة: مزامنة التحديثات من Windows Update مع خادم الإدارة، تكوين تحديثات Windows في سياسة عميل الشبكة.
- Kaspersky Security Center Web Console: إنشاء مهمة إجراء مزامنة Windows Update

7 **تشغيل مهمة تثبيت تحديث**

ابدأ مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو مهمة تثبيت تحديثات Windows Update. عندما تبدأ هذه المهام، يتم تنزيل التحديثات وتثبيتها على الأجهزة المُدارة. بعد اكتمال المهمة، تأكد من أنها بحالة مكتملة بنجاح في قائمة المهام.

8 **أنشئ التقرير حول نتائج تثبيت التحديث لبرنامج جهة خارجية (اختياري)**

لعرض إحصاءات تفصيلية حول تثبيت التحديث، قم بإنشاء **تقرير حول نتائج تثبيت تحديثات برنامج الجهة الخارجية**.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء تقرير وعرضه
- Kaspersky Security Center Web Console: إنشاء تقرير وعرضه

النتائج

إذا قمت بإنشاء وتكوين مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يتم تثبيت التحديثات على الأجهزة المُدارة تلقائيًا. عند تنزيل تحديثات جديدة إلى مستودع خادم الإدارة، يتحقق Kaspersky Security Center من أنها تستوفي المعايير المحددة في قواعد التحديث. سوف يتم تثبيت جميع التحديثات الجديدة التي تستوفي المعايير تلقائيًا عند التشغيل التالي للمهمة.

إذا قمت بإنشاء مهمة تثبيت تحديثات Windows Update، لا يتم تثبيت إلا التحديثات المحددة في خصائص مهمة تثبيت تحديثات Windows Update. في المستقبل إذا أردت تثبيت التحديثات الجديدة التي يتم تنزيلها إلى مستودع خادم الإدارة، يجب أن تضيف التحديثات المطلوبة إلى قائمة التحديثات في المهمة الموجودة أو إنشاء مهمة تثبيت تحديثات Windows Update جديدة.

تثبيت تحديثات برامج الجهات الخارجية

يمكنك تثبيت تحديثات برامج الجهات الخارجية على الأجهزة المُدارة عن طريق إنشاء إحدى المهام التالية وتشغيلها:

- Install required updates and fix vulnerabilities

لا يمكن إنشاء مهمة Install required updates and fix vulnerabilities إلا إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات. ويمكنك استخدام هذه المهمة في تثبيت كلٍ من تحديثات Windows Update التي توفرها Microsoft وتحديثات برامج البائعين الآخرين.

- Install Windows Update updates

يمكنك استخدام مهمة Install Windows Update updates في تثبيت تحديثات Windows Update فقط.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

كخيار متاح، يمكنك إنشاء مهمة لتثبيت التحديثات المطلوبة بالطرق التالية:

- بفتح قائمة التحديث وتحديد التحديثات المراد تثبيتها.

وكنتيجة لذلك، يتم إنشاء مهمة جديدة لتثبيت التحديثات المحددة. كخيار متاح، يمكنك إضافة التحديثات المحددة إلى مهمة موجودة.

- بتشغيل معالج تثبيت التحديث.

لا تتوفر مزايا معالج تثبيت التحديث إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

يقوم المعالج بتبسيط إنشاء مهمة تثبيت التحديث وتكوينها، كما يسمح لك بإزالة إنشاء المهام الزائدة التي تحتوي على نفس التحديثات المراد تثبيتها.

تثبيت تحديثات برامج الجهات الخارجية باستخدام قائمة التحديث

لتثبيت تحديثات برامج الجهات الخارجية باستخدام قائمة التحديثات:

1. افتح أحد قوائم التحديثات:

- لفتح قائمة التحديث العام، في القائمة الرئيسية، انتقل إلى **Software updates** ← **Patch management** ← **Operations**.
- لفتح قائمة التحديث لجهاز مُدار، في القائمة الرئيسة، انتقل إلى **Managed devices** ← **Assets (Devices)** ← <اسم الجهاز> ← **Available updates** ← **Advanced**.
- لفتح قائمة التحديث لتطبيق محدد، في القائمة الرئيسية، انتقل إلى **Applications** ← **Third-party applications** ← **Operations** ← **registry** ← <اسم التطبيق> ← **Available updates**.

ستظهر قائمة بالتحديثات المتاحة.

2. حدد خانات الاختيار الموجودة بجوار التحديثات التي ترغب في تثبيتها.

3. انقر على الزر **Install updates** .

لتثبيت بعض تحديثات البرامج، يجب أن توافق على اتفاقية ترخيص المستخدم النهائي. إذا رفضت اتفاقية ترخيص المستخدم النهائي، لن يتم تثبيت تحديث البرنامج.

4. حدد أحد الخيارات التالية:

- **New task**

سيبدأ معالج المهمة الجديدة. إذا كان لديك ترخيص إدارة الثغرات الأمنية والتصحيحات، يتم تحديد مهمة Install required updates and fix vulnerabilities مسبقًا. إذا لم يكن لديك الترخيص، يتم تحديد مهمة Install Windows Update updates مسبقًا. اتبع خطوات المعالج لإكمال إنشاء المهمة.

- **Install update (add rule to specified task)**

حدد مهمة ترغب في إضافة التحديثات المحددة إليها. إذا كان لديك ترخيص إدارة الثغرات الأمنية والتصحيحات، حدد مهمة Install required updates and fix vulnerabilities. سيتم تلقائيًا إضافة قاعدة جديدة لتثبيت التحديثات المحددة إلى المهمة المحددة. إذا لم يكن لديك الترخيص، حدد مهمة Install Windows Update updates. سيتم إضافة التحديثات إلى خصائص المهمة.

ستفتح نافذة خصائص المهمة. انقر على زر **Save** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، سيتم إنشاء المهمة وعرضها في قائمة المهام في **Tasks** ← **Assets (Devices)**. إذا اخترت إضافة التحديثات إلى مهمة موجودة، يتم حفظ التحديثات في خصائص المهمة.

لتثبيت تحديثات برامج الجهات الخارجية، ابدأ مهمة Install required updates and fix vulnerabilities أو مهمة Install Windows Update updates. يمكنك بدأ أي من هذه المهام يدويًا أو تحديد إعدادات الجدول في خصائص المهمة التي تبدأها. عند تحديد جدول المهام، تأكد من بدء مهمة تثبيت التحديث بعد اكتمال مهمة Find vulnerabilities and required updates.

تثبيت تحديثات برامج الجهات الخارجية باستخدام معالج تثبيت التحديث.

لا تتوفر مزايا معالج تثبيت التحديث إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

لتثبيت مهمة لتثبيت تحديثات برامج الجهات الخارجية باستخدام معالج تثبيت التحديث:

1. في القائمة الرئيسية، انتقل إلى **Software updates** ← **Patch management** ← **Operations**.

ستظهر قائمة بالتحديثات المتاحة.

2. حدد خانة الاختيار الموجودة بجوار التحديث الذي ترغب في تثبيته.

3. انقر على زر **Run Update installation wizard**.

يبدأ تشغيل معالج تثبيت التحديث. صفحة **Select the update installation task** تعرض قائمة بجميع المهام الموجودة من الأنواع التالية:

- Install required updates and fix vulnerabilities
- Install Windows Update updates
- Fix vulnerabilities

لا يمكنك تعديل المهام لآخر نوعين لتثبيت التحديثات الجديدة. لتثبيت التحديثات الجديدة، لا يمكنك استخدام إلا مهام Install required updates and fix vulnerabilities.

4. إذا كنت ترغب في ألا يعرض المعالج إلا المهام التي تثبت التحديث الذي حددته، قم بتفعيل خيار **Show only tasks that install this update**.

5. اختر ما ترغب في فعله:

- لبدء مهمة، حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر **Start**.
- لإضافة قاعدة جديدة إلى مهمة موجودة:

a. حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر **Add rule**.

b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:

- **Installation rule for updates of this importance level**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، لا تقوم التحديثات بإصلاح إلا تلك الثغرات الأمنية التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة لمستوى حدة التحديث المحدد أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **Installation rule for updates of this importance level according to MSRC**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار (متاح فقط لتحديثات Windows Update)، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Microsoft Security Response Center (MSRC) مساويًا للقيمة المحددة في القائمة أو أعلى منها (**منخفض**، أو **متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **Installation rule for updates by this vendor**

هذا الخيار متاح فقط لتحديثات تطبيقات الطرف الثالث. لا يقوم Kaspersky Security Center إلا بتثبيت التحديثات التي تتعلق فقط بالتطبيقات التي قام بها نفس البائع مثل التحديث المحدد. لا يتم تثبيت التحديثات المرفوضة وتحديثات التطبيقات التي أجراها بائعون آخرون.

يتم تعطيل هذا الخيار افتراضيًا.

- **Installation rule for updates of the type**
- **Installation rule for the selected update**
- **Approve selected updates**

سيتم اعتماد التحديث المحدد للتثبيت. تمكين هذا الخيار في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **Automatically install all previous application updates that are required to install the selected updates**

استمر في تمكين هذا الخيار إذا كنت توافق على تثبيت إصدارات التطبيق مؤقتًا عندما يُطلب ذلك لتثبيت التحديثات المحددة.

إذا تم تعطيل هذا الخيار، فإنه يتم تثبيت إصدارات التطبيقات المحددة فقط. قم بتعطيل هذا الخيار إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون محاولة تثبيت إصدارات متتابعة تدريجيًا. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

على سبيل المثال، لديك الإصدار رقم 3 لتطبيق مثبت على أحد الأجهزة وتريد تحديثه إلى الإصدار رقم 5، ولكن الإصدار رقم 5 لهذا التطبيق يمكن تثبيته فوق الإصدار رقم 4 فقط. إذا تم تمكين هذا الخيار، فإن البرنامج يقوم أولاً بتثبيت الإصدار رقم 4، ومن ثم تثبيت الإصدار رقم 5. إذا تم تعطيل هذا الخيار، فإن البرنامج يفشل في تحديث التطبيق.

يتم تمكين هذا الخيار افتراضيًا.

c. انقر على الزر **Add**.

- لإنشاء مهمة:

a. انقر على زر **New task**.

b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:

- **Installation rule for updates of this importance level**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، لا تقوم التحديثات بإصلاح إلا تلك الثغرات الأمنية التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة لمستوى حدة التحديث المحدد أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **Installation rule for updates of this importance level according to MSRC**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار (متاح فقط لتحديثات Windows Update)، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Microsoft Security Response Center (MSRC) مساويًا للقيمة المحددة في القائمة أو أعلى منها (**منخفض**، أو **متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **Installation rule for updates by this vendor**

هذا الخيار متاح فقط لتحديثات تطبيقات الطرف الثالث. لا يقوم Kaspersky Security Center إلا بتثبيت التحديثات التي تتعلق فقط بالتطبيقات التي قام بها نفس البائع مثل التحديث المحدد. لا يتم تثبيت التحديثات المرفوضة وتحديثات التطبيقات التي أجراها بائعون آخرون.

يتم تعطيل هذا الخيار افتراضيًا.

- **Installation rule for updates of the type**

- **Installation rule for the selected update**

- **Approve selected updates**

سيتم اعتماد التحديث المحدد للتثبيت. تمكين هذا الخيار في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **Automatically install all previous application updates that are required to install the selected updates**

استمر في تمكين هذا الخيار إذا كنت توافق على تثبيت إصدارات التطبيق مؤقتًا عندما يُطلب ذلك لتثبيت التحديثات المحددة.

إذا تم تعطيل هذا الخيار، فإنه يتم تثبيت إصدارات التطبيقات المحددة فقط. قم بتعطيل هذا الخيار إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون محاولة تثبيت إصدارات متتابعة تدريجيًا. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

على سبيل المثال، لديك الإصدار رقم 3 لتطبيق مثبت على أحد الأجهزة وتريد تحديثه إلى الإصدار رقم 5، ولكن الإصدار رقم 5 لهذا التطبيق يمكن تثبيته فوق الإصدار رقم 4 فقط. إذا تم تمكين هذا الخيار، فإن البرنامج يقوم أولاً بتثبيت الإصدار رقم 4، ومن ثم تثبيت الإصدار رقم 5. إذا تم تعطيل هذا الخيار، فإن البرنامج يفشل في تحديث التطبيق.

يتم تمكين هذا الخيار افتراضيًا.

c. انقر على الزر **Add**.

إذا اخترت بدء مهمة، يمكنك إغلاق المعالج. سيتم استكمال المهمة في وضع الخلفية. لا يلزم اتخاذ إجراءات إضافية.

إذا اخترت إضافة قاعدة إلى مهمة موجودة، ستفتح نافذة خصائص المهمة. تمت إضافة القاعدة الجديدة بالفعل إلى خصائص المهمة. يمكنك عرض القاعدة أو إعدادات المهمة الأخرى أو تعديلها. انقر على زر **Save** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، ستستمر في إنشاء المهمة في معالج المهمة. المهمة الجديدة التي أضفتها إلى معالج تثبيت التحديث سيتم عرضها في معالج المهمة الجديدة. عندما تكمل المعالج، سيتم إضافة مهمة Install required updates and fix vulnerabilities إلى قائمة المهام.

إنشاء مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة

خلال مهمة Find vulnerabilities and required updates، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المُكتشَفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة المُدارة.

يتم إنشاء مهمة Find vulnerabilities and required updates تلقائيًا عند تشغيل معالج البدء السريع. إذا لم تشغِّل المعالج، يمكنك إنشاء المهمة يدويًا.

لإنشاء مهمة Find vulnerabilities and required updates:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.
2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.
3. لتطبيق Kaspersky Security Center، حدد نوع المهمة **Find vulnerabilities and required updates**.
4. حدد اسم المهمة التي ترغب في إنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).
5. حدد الأجهزة التي سيتم تعيين المهمة إليها:
6. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.
7. انقر على زر **Create**.

   يتم إنشاء المهمة وعرضها في قائمة المهام.
8. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.
9. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة .

10. في تبويب **Application settings**، حدد الإعدادات التالية:

- **Search for vulnerabilities and updates listed by Microsoft**

عند البحث عن الثغرات الأمنية والتحديثات، يستخدم Kaspersky Security Center المعلومات حول تحديثات Microsoft القابلة للتطبيق من مصدر تحديثات Microsoft، المتوفرة في الوقت الحالي.

على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft وتحديثات تطبيقات لجهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

لم يتم إرسال المعلومات المتعلقة بتحديثات Microsoft Windows الاختيارية إلى خادم الإدارة.

- **Connect to the update server to update data**

يتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft. يمكن أن تعمل الخوادم التالية كمصدر لتحديثات Microsoft:

- خادم إدارة Kaspersky Security Center (راجع إعدادات سياسة عميل الشبكة)
- خادم Windows مع خدمات تحديث خادم Microsoft Windows (WSUS) المنشورة في شبكة مؤسستك
- خوادم تحديثات Microsoft

إذا تم تمكين هذا الخيار، فسيتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft لتحديث المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق.

إذا تم تعطيل هذا الخيار، فسيستخدم عميل تحديث Windows على جهاز مُدار المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقتٍ سابق.

يمكن أن يكون الاتصال بمصدر تحديثات Microsoft مستهلكًا للموارد. قد ترغب في تعطيل هذا الخيار، إذا قمت بتعيين اتصال منتظم لمصدر التحديثات هذا في مهمة أخرى أو في خصائص سياسة وكلاء الشبكة في قسم **تحديثات البرنامج والثغرات الأمنية**. إذا كنت لا ترغب في تعطيل هذا الخيار، إذن لتقليل التحميل الزائد على الخادم، يمكنك تكوين جدول المهام لترتيب عملية تأخير بدء المهمة عشوائيًا في غضون 360 دقيقة.

يتم تمكين هذا الخيار افتراضيًا.

يحدد مزيج الخيارات التالية لإعدادات سياسة وكلاء الشبكة طريقة الحصول على التحديثات:

- يتصل عميل Windows Update الموجود على جهاز مُدار بخادم التحديث للحصول على التحديثات فقط في حالة تمكين الخيار **الاتصال بخادم التحديث لتحديث البيانات** في خصائص مهمة Find vulnerabilities and required updates وتم تعيين الخيار **وضع بحث تحديث Windows** على **نشط** في إعدادات سياسة عميل الشبكة.

- إذا لم تكن بحاجة إلى عميل الشبكة لبدء الاتصال بمصدر تحديث Microsoft Windows وتنزيل التحديثات عند إجراء مهمة فحص الثغرات الأمنية، يمكنك ضبط الخيار **وضع بحث تحديث Windows** على **سلبي**، بينما يجب أن يظل الخيار **الاتصال بخادم التحديث لتحديث البيانات** قيد التمكين. ويتيح لك ذلك توفير الموارد واستخدام تحديثات Windows التي تم سبق تلقيها للبحث عن الثغرات الأمنية. ويمكنك استخدام الوضع السلبي إذا كونت تلقي تحديثات Microsoft Windows بطريقة مختلفة. إذا لم يتم تكوين تلقي تحديثات Microsoft Windows بطريقة أخرى، فلا تقم بتعيين الخيار **وضع بحث تحديث Windows** على **سلبي**، لأنه في هذه الحالة، لن يتم تلقي معلومات عن التحديثات مطلقًا.

- بغض النظر عن حالة الخيار **الاتصال بخادم التحديث لتحديث البيانات** (تم تمكينه أو تم تعطيله)، ففي حالة ضبط الخيار **وضع بحث تحديث Windows** على **معطل**، لا يطلب Kaspersky Security Center أي معلومات عن التحديثات.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

في حالة تمكين هذا الخيار، فسيبحث Kaspersky Security Center عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في سجل Windows وفي المجلدات المحددة ضمن **تحديد مسارات للبحث المتقدم للتطبيقات في نظام الملفات**. تدار القائمة الكاملة لتطبيقات الجهة الخارجية المدعومة بواسطة Kaspersky.

إذا تم تعطيل هذا الخيار، فلن يقوم Kaspersky Security Center بالبحث عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية. على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft Windows وتحديثات تطبيقات جهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

- **Specify paths for advanced search of applications across the file system**

المجلدات التي يبحث فيها Kaspersky Security Center عن تطبيقات الجهة الخارجية والتي تتطلب إصلاح الثغرات الأمنية وتثبيت التحديث. يمكنك استخدام متغيرات النظام.

حدد المجلدات التي يتم تثبيت التطبيقات بها. تحتوي القائمة بشكلٍ افتراضي على مجلدات النظام التي يتم تثبيت معظم التطبيقات بها.

- **Enable advanced diagnostics**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **Maximum size, in MB, of advanced diagnostics files**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

11. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

إذا كانت نتائج المهمة تحتوي على تحذير من خطأ 0x80240033 "خطأ عميل Windows Update 80240033 ("تعذر تنزيل شروط الترخيص.")"، يمكنك حل هذه المشكلة من خلال سجل Windows.

البحث عن الثغرات الأمنية والإعدادات المطلوبة لمهمة التحديثات

يتم إنشاء مهمة Find vulnerabilities and required updates تلقائيًا عند تشغيل معالج البدء السريع. إذا لم تشغِّل المعالج، يمكنك إنشاء المهمة يدويًا.

بالإضافة إلى إعدادات المهمة العامة، يمكنك تحديد الإعدادات التالية عند إنشاء مهمة Find vulnerabilities and required updates أو بعد ذلك عند تكوين خصائص المهمة التي تم إنشاؤها:

- **Search for vulnerabilities and updates listed by Microsoft**

عند البحث عن الثغرات الأمنية والتحديثات، يستخدم Kaspersky Security Center المعلومات حول تحديثات Microsoft القابلة للتطبيق من مصدر تحديثات Microsoft، المتوفرة في الوقت الحالي.

على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft وتحديثات تطبيقات لجهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

لم يتم إرسال المعلومات المتعلقة بتحديثات Microsoft Windows الاختيارية إلى خادم الإدارة.

- **Connect to the update server to update data**

يتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft. يمكن أن تعمل الخوادم التالية كمصدر لتحديثات Microsoft:

- خادم إدارة Kaspersky Security Center (راجع إعدادات سياسة عميل الشبكة)
- خادم Windows مع خدمات تحديث خادم Microsoft Windows (WSUS) المنشورة في شبكة مؤسستك
- خوادم تحديثات Microsoft

إذا تم تمكين هذا الخيار، فسيتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft لتحديث المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق.

إذا تم تعطيل هذا الخيار، فسيستخدم عميل تحديث Windows على جهاز مُدار المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقتٍ سابق.

يمكن أن يكون الاتصال بمصدر تحديثات Microsoft مستهلكًا للموارد. قد ترغب في تعطيل هذا الخيار، إذا قمت بتعيين اتصال منتظم لمصدر التحديثات هذا في مهمة أخرى أو في خصائص سياسة وكلاء الشبكة في قسم **تحديثات البرنامج والثغرات الأمنية**. إذا كنت لا ترغب في تعطيل هذا الخيار، إذن لتقليل التحميل الزائد على الخادم، يمكنك تكوين جدول المهام لترتيب عملية تأخير بدء المهمة عشوائيًا في غضون 360 دقيقة.

يتم تمكين هذا الخيار افتراضيًا.

يحدد مزيج الخيارات التالية لإعدادات سياسة وكلاء الشبكة طريقة الحصول على التحديثات:

- يتصل عميل Windows Update الموجود على جهاز مُدار بخادم التحديث للحصول على التحديثات فقط في حالة تمكين الخيار **الاتصال بخادم التحديث لتحديث البيانات** في خصائص مهمة Find vulnerabilities and required updates وتم تعيين الخيار **وضع بحث تحديث Windows** على **نشط** في إعدادات سياسة عميل الشبكة.
- إذا لم تكن بحاجة إلى عميل الشبكة لبدء الاتصال بمصدر تحديث Microsoft Windows وتنزيل التحديثات عند إجراء مهمة فحص الثغرات الأمنية، يمكنك ضبط الخيار **وضع بحث تحديث Windows** على **سلبي**، بينما يجب أن يظل الخيار **الاتصال بخادم التحديث لتحديث البيانات** قيد التمكين. ويتيح لك ذلك توفير الموارد واستخدام تحديثات Windows التي تم سبق تلقيها للبحث عن الثغرات الأمنية. ويمكنك استخدام الوضع السلبي إذا كونت تلقي تحديثات Microsoft Windows بطريقة مختلفة. إذا لم يتم تكوين تلقي تحديثات Microsoft Windows بطريقة أخرى، فلا تقم بتعيين الخيار **وضع بحث تحديث Windows** على **سلبي**، لأنه في هذه الحالة، لن يتم تلقي معلومات عن التحديثات مطلقًا.
- بغض النظر عن حالة الخيار **الاتصال بخادم التحديث لتحديث البيانات** (تم تمكينه أو تم تعطيله)، ففي حالة ضبط الخيار **وضع بحث تحديث Windows** على **معطل**، لا يطلب Kaspersky Security Center أي معلومات عن التحديثات.

- **Search for third-party vulnerabilities and updates listed by Kaspersky**

في حالة تمكين هذا الخيار، فسيبحث Kaspersky Security Center عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في سجل Windows وفي المجلدات المحددة ضمن **تحديد مسارات للبحث المتقدم للتطبيقات في نظام الملفات**. تدار القائمة الكاملة لتطبيقات الجهة الخارجية المدعومة بواسطة Kaspersky.

إذا تم تعطيل هذا الخيار، فلن يقوم Kaspersky Security Center بالبحث عن الثغرات الأمنية والتحديثات المطلوبة لتطبيقات الجهات الخارجية. على سبيل المثال، قد ترغب في تعطيل هذا الخيار إذا كانت لديك مهام مختلفة ذات إعدادات مختلفة لتحديثات Microsoft Windows وتحديثات تطبيقات جهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

- **Specify paths for advanced search of applications across the file system**

المجلدات التي يبحث فيها Kaspersky Security Center عن تطبيقات الجهة الخارجية والتي تتطلب إصلاح الثغرات الأمنية وتثبيت التحديث. يمكنك استخدام متغيرات النظام.

حدد المجلدات التي يتم تثبيت التطبيقات بها. تحتوي القائمة بشكلٍ افتراضي على مجلدات النظام التي يتم تثبيت معظم التطبيقات بها.

- **Enable advanced diagnostics**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **Maximum size, in MB, of advanced diagnostics files**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

التوصيات عن جدول المهمة

عند جدولة مهمة Find vulnerabilities and required updates، تأكد من تفعيل خياري**Run missed tasks** و**Use automatically randomized delay for task starts**.

بشكل افتراضي، يتم تحديد مهمة Find vulnerabilities and required updates لكي تبدأ يدويًا. إذا كانت قواعد مكان العمل الخاصة بالمؤسسة تعمل على إيقاف تشغيل جميع الأجهزة في هذا الوقت، سيتم تشغيل مهمة Find vulnerabilities and required updates بعد تشغيل الأجهزة مرة أخرى، أي في صباح اليوم التالي. قد يكون مثل هذا النشاط غير مرغوب فيه لأن عملية فحص الثغرات لأمنية قد تزيد من الحمل على وحدات المعالجة المركزية والأنظمة الفرعية للقرص. يجب عليك إعداد الجدول الأكثر ملاءمةً للمهمة بناءً على قواعد مكان العمل التي تتبناها المؤسسة.

إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية

لا تتوفر مهمة Install required updates and fix vulnerabilities إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

تُستخدَم المهمة Install required updates and fix vulnerabilities لتحديث وإصلاح الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها، بما في ذلك برامج Microsoft المثبتة على الأجهزة المُدارة. تتيح لك هذه المهمة تثبيت تحديثات متعددة وإصلاح ثغرات أمنية متعددة وفقًا لقواعد معينة.

لتثبيت التحديثات أو إصلاح الثغرات الأمنية باستخدام مهمة Install required updates and fix vulnerabilities، يمكنك القيام بأي مما يلي:

- تشغيل معالج تثبيت التحديث أو معالج إصلاح الثغرات الأمنية.
- إنشاء مهمة Install required updates and fix vulnerabilities.
- أضف قاعدة لتثبيت التحديث إلى مهمة Install required updates and fix vulnerabilities موجودة.

لإنشاء مهمة Install required updates and fix vulnerabilities:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة **Install required updates and fix vulnerabilities**.

   إذا لم يتم عرض المهمة، فتحقق مما إذا كان حسابك لديه **حقوق القراءة** و **التعديل** و التنفيذ للمجال **الوظيفي**: **لإدارة الثغرات الأمنية والتصحيحات** لا يمكنك إنشاء وتكوين مهمة قم بتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية بدون حقوق الوصول هذه.

4. حدد اسم المهمة التي ترغب في إنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

5. حدد الأجهزة التي سيتم تعيين المهمة إليها:

6. حدد قواعد تثبيت التحديث، وبعدها حدد الإعدادات التالية:

- **Start installation at device restart or shutdown**

إذا تم تمكين هذا الخيار، فسيتم تثبيت التحديثات عند إعادة تشغيل الجهاز أو إغلاقه. بخلاف ذلك، يتم تثبيت التحديثات وفقًا لجدول زمني.

استخدم هذا الخيار في حال كان تنزيل التحديثات قد يؤثر على أداء الجهاز.

يتم تعطيل هذا الخيار افتراضيًا.

- **Install the required general system components**

إذا تم تمكين هذا الخيار، قبل تثبيت التحديث، يقوم التطبيق تلقائيًا بتثبيت كافة مكونات النظام العامة (المتطلبات الأساسية) اللازمة لتثبيت التحديث. على سبيل المثال، يمكن أن تكون تلك المتطلبات الأساسية عبارة عن تحديثات نظام التشغيل.

إذا تم تعطيل هذا الخيار، فقط يتعين عليك تثبيت المتطلبات الأساسية يدويًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **Allow installation of new application versions during updates**

إذا تم تمكين هذا الخيار، سيتم السماح بالتحديثات التي تؤدي إلى تثبيت إصدار جديد من تطبيق البرنامج.

إذا تم تعطيل هذا الخيار، فلن تتم ترقية البرنامج. بعد ذلك يمكنك تثبيت إصدارات البرنامج الجديدة يدويًا أو من خلال مهمة أخرى. على سبيل المثال، قد تستخدم هذا الخيار في حال كانت البنية الأساسية الخاصة بشركتك غير مدعومة بواسطة إصدار جديد للبرنامج أو في حال رغبت في التحقق من ترقية في اختبار البنية الأساسية.

يتم تمكين هذا الخيار افتراضيًا.

> قد تؤدي ترقية التطبيق إلى حدوث خلل في التطبيقات التابعة المثبتة على أجهزة عميلة.

- **Download updates to the device without installing them**

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بتنزيل التحديثات على الجهاز ولكن لن يقوم بتنزيلها تلقائيًا. بعد ذلك يمكنك تثبيت التحديثات التي تم تنزيلها يدويًا.

تم تنزيل تحديثات Microsoft إلى مخزن Windows في النظام. يتم تنزيل تحديثات تطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في المجلد المحدد في حقل **تنزيل التحديثات إلى**.

إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائيًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **Download updates to**

يتم استخدام هذا المجلد لتنزيل تحديثات خاصة بتطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky وMicrosoft).

- **Enable advanced diagnostics**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **Maximum size, in MB, of advanced diagnostics files**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

7. حدد إعدادات إعادة تشغيل نظام التشغيل:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **فترة الانتظار قبل فرض إغلاق التطبيقات في الجلسات المحجوبة (بالدقائق)**

  يتم غلق التطبيقات إجباريًا عند قفل جهاز المستخدم (تلقائيًا عقب فترة زمنية محددة من عدم النشاط، أو يدويًا)

  إذا تم تمكين هذا الخيار، فسيتم فرض غلق التطبيقات على الجهاز المقفل عند انتهاء الفترة الزمنية المحددة في حقل الإدخال.

  إذا تم تعطيل هذا الخيار، فلن يتم غلق التطبيقات على الجهاز المقفل.

  يتم تعطيل هذا الخيار افتراضيًا.

8. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

9. انقر على زر **Finish**.

   يتم إنشاء المهمة وعرضها في قائمة المهام.

10. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

11. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك.

12. انقر على زر **Save**.

    سيتم إنشاء المهمة وتكوينها.

إذا كانت نتائج المهمة تحتوي على تحذير من خطأ 0x80240033 "خطأ عميل Windows Update 80240033 ("تعذر تنزيل شروط الترخيص.")"، يمكنك حل هذه المشكلة من خلال سجل Windows.

حدد قواعد لتثبيت التحديثات

هذه الميزة غير متاحة إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

عند تثبيت تحديثات برامج أو إصلاح ثغرات أمنية في برنامج باستخدام مهمة Install required updates and fix vulnerabilities، يجب عليك تحديد قواعد تثبيت التحديث. تحدد هذه القواعد التحديثات المراد تثبيتها والثغرات الأمنية المراد إصلاحها.

تعتمد نفس الإعدادات عما إذا كنت تقوم بإنشاء قاعدة لتحديثات تطبيقات Microsoft، أو تطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky وMicrosoft) أو لجميع التطبيقات. عند إنشاء قاعدة لتطبيقات Microsoft أو تطبيقات الجهات الخارجية، يمكنك تحديد تطبيقات وإصدارات تطبيق معينة ترغب في تثبيت التحديثات من أجلها. عند إنشاء قاعدة لجميع التطبيقات، يمكنك تحديد تحديثات معينة ترغب في تثبيتها وثغرات أمنية ترغب في إصلاحها عن طريق تثبيت التحديثات.

يمكنك إضافة قاعدة لتثبيت التحديث بالطرق التالية:

- بإضافة قاعدة أثناء إنشاء مهمة Install required updates and fix vulnerabilities جديدة.
- عن طريق إضافة قاعدة في تبويب **إعدادات التطبيق** في نافذة الخصائص للمهمة Install required updates and fix vulnerabilities الموجودة.
- من خلال معالج تثبيت التحديث أو معالج إصلاح الثغرات الأمنية.

لإضافة قاعدة جديدة لجميع التحديثات:

1. انقر على الزر **إضافة**.

   يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

2. في صفحة **نوع القاعدة**، حدد**قاعدة لجميع التحديثات**.

3. في صفحة **المعايير العامة**، استخدم القوائم المنسدلة لتحديد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في صفحة **التحديثات**، حدد التحديثات المراد تثبيتها:

- **تثبيت جميع التحديثات المناسبة**

تثبيت جميع تحديثات البرامج التي تتوافق مع المعايير المحددة في صفحة **معايير عامة** الخاصة بالمعالج. يتم تحديده بصورة افتراضية.

- **تثبيت التحديثات من القائمة فقط**

قم بتثبيت تحديثات البرامج التي تحددها يدويًا فقط من القائمة. تحتوي القائمة على جميع تحديثات البرامج المتاحة.

على سبيل المثال، قد ترغب في تحديد تحديثات معينة في الحالات التالية: للتحقق من إجراءات تثبيتها في بيئة اختبارية، أو لتحديث التطبيقات المهمة فقط، أو لتحديث التطبيقات المعينة فقط.

- **تثبيت كل تحديثات التطبيق السابقة المطلوبة لتثبيت التحديثات المحددة تلقائيًا**

استمر في تمكين هذا الخيار إذا كنت توافق على تثبيت إصدارات التطبيق مؤقتًا عندما يُطلب ذلك لتثبيت التحديثات المحددة.

إذا تم تعطيل هذا الخيار، فإنه يتم تثبيت إصدارات التطبيقات المحددة فقط. قم بتعطيل هذا الخيار إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون محاولة تثبيت إصدارات متتابعة تدريجيًا. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

على سبيل المثال، لديك الإصدار رقم 3 لتطبيق مثبت على أحد الأجهزة وتريد تحديثه إلى الإصدار رقم 5، ولكن الإصدار رقم 5 لهذا التطبيق يمكن تثبيته فوق الإصدار رقم 4 فقط. إذا تم تمكين هذا الخيار، فإن البرنامج يقوم أولاً بتثبيت الإصدار رقم 4، ومن ثم تثبيت الإصدار رقم 5. إذا تم تعطيل هذا الخيار، فإن البرنامج يفشل في تحديث التطبيق.

يتم تمكين هذا الخيار افتراضيًا.

5. في صفحة **الثغرات الأمنية**، حدد الثغرات الأمنية التي سيتم إصلاحها عن طريق تثبيت التحديثات المحددة:

- **إصلاح جميع الثغرات الأمنية التي تطابق المعايير الأخرى**

إصلاح جميع الثغرات الأمنية التي تتوافق مع المعايير المحددة في صفحة **معايير عامة** في المعالج. يتم تحديده بصورة افتراضية.

- **إصلاح الثغرات الأمنية من القائمة فقط**

قم بإصلاح الثغرات الأمنية التي تحددها يدويًا فقط من القائمة. تحتوي هذه القائمة على جميع الثغرات الأمنية التي تم اكتشافها.

على سبيل المثال، قد ترغب في تحديد ثغرات أمنية معينة في الحالات التالية: للتحقق من إجراءات إصلاحها في بيئة اختبارية، أو لإصلاح الثغرات الأمنية في التطبيقات المهمة فقط، أو لإصلاح الثغرات الأمنية في تطبيقات معينة فقط.

6. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإضافتها. يمكنك بعد ذلك تغيير هذا الاسم في قسم **الإعدادات** من نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد استكمال معالج إنشاء القاعدة لعملياته، يتم إضافة القاعدة الجديدة وعرضها في قائمة القاعدة في معالج المهمة الجديدة أو في خصائص المهمة.

لإضافة قاعدة جديدة إلى تحديثات Windows Update:

1. انقر على الزر **إضافة**.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

2. في صفحة **نوع القاعدة**، حدد **قاعدة تحديث Windows**.

3. في صفحة **المعايير العامة**، حدد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **قم بإصلاح الثغرات الأمنية ذات مستوى الخطورة MSRC الذي يساوي أو أعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Microsoft Security Response Center (MSRC) مساويًا للقيمة المحددة في القائمة أو أعلى منها (**منخفض**، أو **متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضيًا.

5. في الصفحة **فئات التحديثات**، حدد فئات التحديثات المطلوب تثبيتها. هذه الفئات هي نفس الفئات الموجودة في Microsoft Update Catalog. يتم تحديد جميع الفئات افتراضيًا.

6. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإضافتها. يمكنك بعد ذلك تغيير هذا الاسم في قسم **الإعدادات** من نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد استكمال معالج إنشاء القاعدة لعملياته، يتم إضافة القاعدة الجديدة وعرضها في قائمة القاعدة في معالج المهمة الجديدة أو في خصائص المهمة.

لإضافة قاعدة جديدة لتحديثات تطبيقات الجهات الخارجية:

1. انقر على الزر **إضافة**.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

2. في صفحة **نوع القاعدة**، حدد**قاعدة تحديثات الأطراف الخارجية**.

3. في صفحة **المعايير العامة**، حدد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضيًا.

5. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإضافتها. يمكنك بعد ذلك تغيير هذا الاسم في قسم الإعدادات في نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد استكمال معالج إنشاء القاعدة لعملياته، يتم إضافة القاعدة الجديدة وعرضها في قائمة القاعدة في معالج المهمة الجديدة أو في خصائص المهمة.

إنشاء مهمة تثبيت تحديثات Windows Update

تتيح لك مهمة Install Windows Update updates تثبيت تحديثات البرامج التي توفرها خدمة Windows Update على الأجهزة المُدارة.

إذا لم يكن لديك ترخيص إدارة الثغرات الأمنية والتصحيحات، لا يمكنك إنشاء مهام جديدة لنوع Install Windows Update updates. لتثبيت التحديثات الجديدة، يمكنك إضافتها إلى مهمة Install Windows Update updates موجودة. نوصي باستخدام مهمة Install required updates and fix vulnerabilities بدلاً من مهمة Install Windows Update updates. تمكنك مهمة Install required updates and fix vulnerabilities من تثبيت تحديثات متعددة وإصلاح العديد من الثغرات الأمنية تلقائيًا وفقًا للقواعد التي تحددها. بالإضافة إلى ذلك، تمكنك هذه المهمة من تثبيت التحديثات من بائعي برامج غير Microsoft.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

لإنشاء مهمة تثبيت تحديثات Windows Update:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Tasks**.

2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة **Install Windows Update updates**.

4. حدد اسم المهمة التي ترغب في إنشائها.

   لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

5. حدد الأجهزة التي سيتم تعيين المهمة إليها:

6. انقر على زر **Add**.

   ستفتح قائمة التحديثات.

7. حدد تحديثات Windows Update التي ترغب في تثبيتها ثم انقر على **OK**.

8. حدد إعدادات إعادة تشغيل نظام التشغيل:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **Force closure of applications in blocked sessions**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

9. حدد الإعدادات التالية:

- **Default account**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.

يتم تحديد هذا الخيار افتراضيًا.

- **Specify account**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **Account**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **Password**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

10. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

11. انقر على زر **Finish**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

12. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

13. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك.

14. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

عرض معلومات حول تحديثات برامج الجهات الخارجية المتوفرة

يمكنك عرض قائمة التحديثات المتوفرة لبرامج الجهات الخارجية، بما في ذلك برامج Microsoft، المثبتة على أجهزة العميل.

لعرض قائمة بالتحديثات المتوفرة لتطبيقات الجهات الخارجية المثبتة على أجهزة العميل،

في القائمة الرئيسية، انتقل إلى **Software updates** ← **Patch management** ← **Operations**.

ستظهر قائمة بالتحديثات المتاحة.

يمكنك تحديد عامل تصفية لعرض قائمة تحديثات البرنامج. انقر على أيقونة **Filter** (⚟) في أعلى يمين قائمة تحديثات البرنامج لإدارة عامل التصفية. يمكنك كذلك تحديد أحد عوامل التصفية المعدة مسبقًا من القائمة المنسدلة **Preset filters** أعلى قائمة الثغرات الأمنية في البرنامج.

لعرض خصائص تحديث:

1. انقر على اسم تحديث البرنامج المطلوب.

2. يتم فتح نافذة خصائص التحديث حيث تعرض معلومات مجمعة عن علامات التبويب التالية:

- **General**

يعرض هذا التبويب تفاصيل عامة عن التحديث المحدد:

- حالة الموافقة على التحديث (يمكن تغييرها يدويًا عبر تحديد حالة جديدة في القائمة المنسدلة)
- فئة Windows Server Update Services التي ينتمي التحديث إليها
- تاريخ ووقت تسجيل التحديث
- تاريخ ووقت إنشاء التحديث
- مستوى أهمية التحديث
- متطلبات التثبيت التي يتطلبها التحديث
- عائلة التطبيق التي ينتمي إليها التحديث
- التطبيق الذي ينطبق عليه التحديث
- رقم مراجعة التحديث

- **Attributes**

يعرض هذا التبويب مجموعة من السمات التي يمكنك استخدامها للحصول على المزيد من المعلومات عن التحديث المحدد. تختلف هذه المجموعة اعتمادًا على ما إذا كان التحديث من نشر Microsoft أم بائع طرف ثالث.

يعرض هذا التبويب المعلومات التالية عن تحديث Microsoft:

- مستوى أهمية التحديث وفق مركز استجابة خبراء الأمان من Microsoft (MSRC).
- رابط المقال في قاعدة معارف Microsoft الذي يصف التحديث
- رابط المقال في نشرة أمان Microsoft الذي يصف التحديث
- معرف التحديث (ID)

يعرض هذا التبويب المعلومات التالية عن تحديث الطرف الخارجي:

- سواء كان التحديث تصحيحًا أو حزمة توزيع كاملة
- لغة ترجمة التحديث
- إذا ما كان التحديث مثبت تلقائيًا أو يدويًا
- إذا ما قد تم رفض التحديث بعد تطبيقه
- رابط تنزيل التحديث

- **Devices**

يعرض هذا التبويب قائمة بالأجهزة التي تم تثبيت التحديث المحدد عليها.

- **Fixed vulnerabilities**

يعرض هذا التبويب قائمة بالثغرات الأمنية التي يمكن للتحديث المحدد إصلاحها.

- **Crossover of updates**

يعرض هذا التبويب التقاطعات المحتملة بين عدة تحديثات منشورة للتطبيق نفسه، أي إذا ما كان التحديث المحدد يمكنه أن يحل محل التحديثات الأخرى أو العكس، يمكن استبداله بتحديثات أخرى (متوفرة لتحديثات Microsoft فقط).

- **Tasks to install this update**

يعرض هذا التبويب قائمة بالمهام التي يشمل نطاقها تثبيت التحديث المحدد. يمكنك هذا التبويب كذلك من إنشاء مهمة تثبيت عن بُعد للتحديث.

لعرض إحصاءات تثبيت التحديث:

1. حدد خانة الاختيار الموجودة بجوار تحديث البرنامج المطلوب.

2. انقر على زر **Statistics of update installation statuses**.

يتم عرض مخطط حالات تثبيت التحديث. النقر على حالة يؤدي إلى فتح قائمة بالأجهزة التي تحتوي على التحديث ذي الحالة المحددة.

يمكنك عرض معلومات عن تحديثات البرامج المتوفرة لبرامج الجهات الخارجية، بما في ذلك برامج Microsoft، المثبتة على الجهاز المُدار المحدد بنظام التشغيل Windows.

لعرض قائمة بالتحديثات المتوفرة لبرامج الجهات الخارجية المثبتة على الجهاز المُدار المحدد:

1. في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)**.

يتم عرض قائمة الأجهزة المُدارة.

2. في قائمة الأجهزة المُدارة، انقر على رابط اسم الجهاز الذي ترغب في عرض تحديثات برامج الجهات الخارجية له.

يتم عرض نافذة خصائص الجهاز المحدد.

3. في نافذة الخصائص للجهاز المحدد، حدد تبويب **Advanced**.

4. في الجزء الأيسر، حدد قسم **Available updates**. إذا كنت ترغب في عرض التحديثات المثبتة فقط، قم بتفعيل خيار **Show installed updates**.

يتم عرض قائمة بتحديثات برامج الجهات الخارجية المتوفرة للجهاز المحدد.

تصدير قائمة تحديثات البرامج المتوفرة إلى ملف

يمكنك تصدير قائمة تحديثات برامج الجهات الخارجية، بما في ذلك برامج Microsoft، المعروضة في تلك اللحظة إلى ملف بامتداد CSV أو TXT. يمكنك استخدام هذه الملفات، على سبيل المثال، لإرسالها إلى مدير أمن المعلومات الخاص بك أو لتخزينها لأغراض الإحصائيات.

لتصدير قائمة بالتحديثات المتوفرة لبرامج الجهات الخارجية المثبتة على جميع الأجهزة المُدارة المحددة إلى ملف نصي:

1. في القائمة الرئيسية، انتقل إلى **Software updates** ← **Patch management** ← **Operations**.

   لعرض الصفحة قائمة بالتحديثات المتوفرة لبرامج الجهات الخارجية المثبتة على جميع الأجهزة المُدارة.

2. انقر على زر **Export to TXT** أو **Export to CSV**، حسب التنسيق الذي تفضله للتصدير.

يتم تنزيل الملف الذي يحتوي على قائمة بالتحديثات المتوفرة لبرامج الجهات الخارجية، بما في ذلك برامج Microsoft، إلى الجهاز الذي تستخدمه في تلك اللحظة.

لتصدير قائمة بالتحديثات المتوفرة لبرامج الجهات الخارجية المثبتة على الجهاز المُدار المحدد إلى ملف نصي:

1. افتح قائمة تحديثات برامج الجهات الخارجية المتوفرة على الجهاز المُدار المحدد.

2. حدد تحديثات البرامج التي ترغب في تصديرها.

   يمكن تخطي هذه الخطوة إذا كنت ترغب في تصدير قائمة كاملة بتحديثات البرامج.

   إذا كنت ترغب في تصدير قائمة كاملة بتحديثات البرامج، لن يتم تصدير إلا التحديثات المعروضة على الصفحة الحالية.

   إذا كنت ترغب في تصدير التحديثات المثبتة فقط، حدد خانة الاختيار **Show installed updates**.

3. انقر على زر **Export to TXT** أو **Export to CSV**، حسب التنسيق الذي تفضله للتصدير.

يتم تنزيل الملف الذي يحتوي على قائمة بتحديثات برامج الجهات الخارجية، بما في ذلك برامج Microsoft، والمثبتة على الجهاز المُدار المحدد إلى الجهاز الذي تستخدمه في تلك اللحظة.

الموافقة على تحديثات برامج الجهات الخارجية ورفضها

عندما تقوم بتكوين مهمة تثبيت Install required updates and fix vulnerabilities، يمكنك إنشاء قاعدة تتطلب حالة محددة للتحديثات التي سيتم تثبيتها. على سبيل المثال: يمكن لقاعدة تحديث السماح بتثبيت ما يلي:

- التحديثات المقبولة فقط
- التحديثات المقبولة وغير المحددة فقط
- جميع التحديثات بغض النظر على حالات التحديث

يمكنك الموافقة على التحديثات التي يجب تثبيتها ورفض التحديثات التي لا يتوجب تثبيتها.

استخدام حالة مقبول لإدارة تثبيت التحديث أمر فعال لعدد صغير من التحديثات. لتثبيت عدة تحديثات، استخدم القواعد التي يمكنك تكوينها في مهمة Install required updates and fix vulnerabilities. نوصي بتعيين حالة الموافقة لتلك التحديثات المحددة التي لا تفي بالمعايير المحددة في القواعد. عند الموافقة بشكل يدوي على عدد كبير من التحديثات، ينخفض أداء خادم الإدارة مما قد ينتج عنه التحميل الزائد على الخادم.

قم بما يلي للموافقة على أو رفض تحديث واحد أو عدة تحديثات:

1. في القائمة الرئيسية، انتقل إلى **Software updates** ← **Patch management** ← **Operations**.

   ستظهر قائمة بالتحديثات المتاحة.

2. حدد التحديثات التي ترغب في الموافقة عليها أو رفضها.

3. انقر على **Approve** للموافقة على التحديثات المحددة أو **Decline** لرفض التحديثات المحددة.

   القيمة الافتراضية هي غير محددة.

   التحديدات المحددة لها الحالات التي وضعتها.

كخيار متاح، يمكنك تغيير حالة الموافقة في خصائص تحديث محدد.

للموافقة على تحديث أو رفضه في خصائصه:

1. في القائمة الرئيسية، انتقل إلى **Software updates** ← **Patch management** ← **Operations**.
ستظهر قائمة بالتحديثات المتاحة.

2. انقر على اسم التحديث الثي ترغب في الموافقة عليه أو رفضه.
ستفتح نافذة خصائص التحديث.

3. في قسم **General**، حدد حالة للتحديث بتغيير خيار **Update approval status**. يمكنك تحديد حالة Approved أو Declined أو Undefined

4. انقر على زر **Save** لحفظ التغييرات.

يكون للتحديث المحدد الحالة التي عرفتها.

إذا قمت بتعيين حالة **مرفوضة** لتحديثات برامج الجهات الخارجية، لن يتم تثبيت هذه التحديثات على الأجهزة التي تم التخطيط لتثبيتها عليها لكنها لم تثبَت بعد. ستظل التحديثات على الأجهزة التي تم تثبيتها عليها بالفعل. إذا كان يتعين عليك حذفها، فيمكنك حذفها يدويًا محليًا.

إنشاء مهمة إجراء مزامنة Windows Update.

لا تتوفر مهمة إجراء مزامنة Windows Update إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

مهمة إجراء مزامنة Windows Update مطلوبة إذا كنت ترغب في استخدام خادم الإدارة كخادم WSUS. يقوم خادم الإدارة في هذه الحالة بتنزيل تحديثات Windows إلى قاعدة البيانات ويوفر التحديثات إلى Windows Update على أجهزة العميل في الوضع المركزي من خلال عملاء الشبكة. إذا لم تستخدم الشبكة خادم WSUS، فسيقوم كل جهاز عميل بتنزيل تحديثات Microsoft من خوادم خارجية بشكل مستقل.

تقوم المهمة إجراء مزامنة Windows Update بتنزيل البيانات الوصفية فقط من خوادم Microsoft. يقوم Kaspersky Security Center بتنزيل التحديثات عندما تقوم بتشغيل مهمة تثبيت تحديث وفقط تلك التحديثات التي تحددها للتثبيت.

عند تشغيل مهمة **إجراء مزامنة Windows Update**، يتلقى التطبيق قائمة بالتحديثات الحالية من خادم تحديث Microsoft. بعد ذلك، يقوم Kaspersky Security Center بتجميع قائمة بالتحديثات التي أصبحت قديمة. عند التشغيل التالي لمهمة **بحث عن الثغرات الأمنية والتحديثات المطلوبة**، يضع Kaspersky Security Center علامات على كل التحديثات القديمة ويحدد وقت حذفها. عند التشغيل التالي لمهمة **إجراء مزامنة Windows Update**، يتم حذف كل التحديثات التي تحمل علامة للحذف منذ 30 يومًا. كما يتحقق Kaspersky Security Center من التحديثات القديمة التي تم وضع علامة عليها للحذف منذ أكثر من 180 يومًا، ثم يحذف هذه التحديثات الأقدم.

عند اكتمال المهمة **إجراء مزامنة Windows Update** وحذف التحديثات القديمة، قد تظل قاعدة البيانات تحتوي على رموز تجزئة متعلقة بملفات التحديثات المحذوفة، بالإضافة إلى الملفات المقابلة في ملفات Application\%AllUsersProfile% wusfiles\working.\1093\adminkit\KasperskyLab\Data (إذا كان قد تم تنزيلها من قبل). يمكنك تشغيل المهمة **صيانة خادم الإدارة** لحذف هذه السجلات القديمة من قاعدة البيانات والملفات المقابلة.

إنشاء مهمة إجراء مزامنة Windows Update.

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.
سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة **Perform Windows Update synchronization**.

4. حدد اسم المهمة التي ترغب في إنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

5. قم بتفعيل خيار **Download express installation files** إذا كنت ترغب في تنزيل ملفات التحديث السريع عند تشغيل المهمة.

عندما يقوم Kaspersky Security Center بمزامنة التحديثات مع خوادم Microsoft Windows Update، سيتم حفظ المعلومات حول جميع الملفات في قاعدة بيانات خادم الإدارة. يتم أيضًا تنزيل جميع الملفات اللازمة للتحديث على محرك الأقراص أثناء التفاعل مع وكيل تحديث Windows. على وجه الخصوص، يقوم Kaspersky Security Center بحفظ المعلومات حول ملفات التحديث السريع على قاعدة البيانات وتنزيلها عند اللزوم. يؤدي تنزيل ملفات التحديث السريع إلى تقليل المساحة الفارغة على محرك الأقراص.

لتجنب تقليل حجم القرص وللحد من حركة المرور، قم بتعطيل خيار **Download express installation files**.

6. حدد التطبيق الذي ترغب في تنزيل التحديثات له.

إذا تم تحديد خانة الاختيار **All applications**، فسيتم تنزيل تحديثات لجميع التطبيقات الموجودة، ولجميع التطبيقات التي قد يتم إطلاقها في المستقبل.

7. حدد فئات التحديثات الذي ترغب في تنزيلها إلى خادم الإدارة.

إذا تم تحديد خانة الاختيار **All categories**، فسيتم تنزيل تحديثات لجميع فئات التحديثات الموجودة، ولجميع الفئات التي قد تظهر في المستقبل.

8. حدد لغات الترجمة للتحديثات اليي ترغب في تنزيلها إلى خادم الإدارة. حدد أحد الخيارات التالية:

- **Download all languages, including new ones**

إذا تم تحديد هذا الخيار، فسيتم تنزيل جميع لغات ترجمة التحديثات المتوفرة على خادم الإدارة. يتم تحديد هذا الخيار افتراضيًا.

- **Download selected languages**

إذا تم تحديد هذا الخيار، فيمكنك تحديد من قائمة لغات ترجمة التحديثات اللغة التي يجب تنزيلها على خادم الإدارة.

9. حدد الحساب الذي ستستخدمه عند تشغيل المهمة. حدد أحد الخيارات التالية:

- **الحساب الافتراضي**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.

يتم تحديد هذا الخيار افتراضيًا.

- **تحديد حساب**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

10. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

11. انقر على زر **Finish**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

12. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

13. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك.

14. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

تحديث تطبيقات الجهات الخارجية تلقائيًا

يمكن تحديث بعض تطبيقات الجهات الخارجية تلقائيًا. بائع التطبيق يحدد ما إذا كان التطبيق يدعم ميزة التحديث التلقائي أم لا. في حال تثبيت تطبيق جهة خارجية على جهاز مُدار يدعم التحديث التلقائي، يمكنك تحديد إعداد التحديث التلقائي في خصائص التطبيق. بعد أن تقوم بتغيير إعداد التحديث التلقائي، يطبق عميل الشبكة الإعداد الجديد على كل جهاز مُدار المثبت عليه التطبيق.

إعداد التحديث التلقائي مستقل عن الكائنات الأخرى وإعدادات ميزة إدارة الثغرات الأمنية والتصحيحات. على سبيل المثال: لا يعتمد هذا الإعداد على حالة الموافقة على التحديث أو مهام تثبيت الحديث، مثل Install required updates and fix vulnerabilities وInstall Windows Update updates وFix vulnerabilities.

لتكوين إعداد التحديث التلقائي لتطبيق جهة خارجية:

1. في القائمة الرئيسية، انتقل إلى **Applications registry** ← **Third-party applications** ← **Operations**.
2. انقر على اسم التطبيق الذي ترغب في تغيير إعداد التحديث التلقائي له.

   لتبسيط البحث، يمكنك تصفية القائمة بعمود **Automatic Updates status**.

   ستفتح نافذة خصائص التطبيق.
3. في قسم **General**، حدد قيمة للإعداد التالي:

   Automatic Updates status

   حدد أحد الخيارات التالية:

   - **Undefined**

     يتم تعطيل ميزة التحديث التلقائي. يقوم Kaspersky Security Center بتثبيت تحديثات تطبيقات الجهات الخارجية باستخدام المهام:Install required updates and fix vulnerabilities وInstall Windows Update updates وFix vulnerabilities .
   - **Allowed**

     بعد أن يصدر البائع تحديثًا للتطبيق، يتم تثبيت ذلك التحديث على الأجهزة المُدارة تلقائيًا. لا يلزم اتخاذ أي إجراءات إضافية.
   - **Blocked**

     لا يتم تثبيت تحديثات التطبيق تلقائيًا. يقوم Kaspersky Security Center بتثبيت تحديثات تطبيقات الجهات الخارجية باستخدام المهام:Install required updates and fix vulnerabilities وInstall Windows Update updates وFix vulnerabilities .
4. انقر على زر **Save** لحفظ التغييرات.

   يتم تطبيق إعداد التحديث التلقائي إلى التطبيق المحدد.

إصلاح الثغرات الأمنية ببرامج الجهات الخارجية

يصف هذا القسم ميزات Kaspersky Security Center المتعلقة بإصلاح الثغرات الأمنية في البرامج المثبتة على الأجهزة المُدارة.

السيناريو: البحث عن الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها

يوفر هذا القسم سيناريو للعثور على الثغرات الأمنية وإصلاحها على الأجهزة المُدارة التي تشغل Windows. يمكنك العثور على الثغرات الأمنية بالبرامج وإصلاحها في نظام التشغيل وفي برامج الجهات الخارجية، بما في ذلك برامج Microsoft.

المتطلبات الأساسية

- يتم نشر Kaspersky Security Center في مؤسستك.
- هناك أجهزة مُدارة تشغل نظام Windows في مؤسستك.
- يلزم اتصال خادم الإدارة بالإنترنت للقيام بالمهام التالية:
  - لعمل قائمة بالإصلاحات الموصى بها بشأن الثغرات الأمنية في برنامج Microsoft. يقوم المتخصصون من Kaspersky بإنشاء القائمة وتحديثها بانتظام.
  - لإصلاح الثغرات الأمنية في برامج الطرف الثالث بدلاً من برامج Microsoft.

المراحل

يستمر البحث عن ثغرات البرامج وإصلاحها على مراحل:

1. **البحث عن الثغرات الأمنية في البرنامج المثبتة على الأجهزة المُدارة**

للعثور على الثغرات المنية الموجودة في البرامج المثبت على الأجهزة المُدارة، قم بتشغيل المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المُكتشَفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

تم إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا بواسطة معالج البدء السريع لـ Kaspersky Security Center. إذا لم تشغِّل المعالج، ابدأ تشغيله الآن أو أنشئ المهمة يدويًا.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: فحص التطبيقات بحثًا عن الثغرات الأمنية، وجدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة
- Kaspersky Security Center Web Console: إنشاء بحث عن الثغرات الأمنية والتحديثات المطلوبة المهمة، والبحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة

2. **تحليل قائمة الثغرات الأمنية المكتشَفة بالبرامج**

اعرض القائمة **الثغرات الأمنية بالبرنامج** وحدد الثغرات الأمنية التي يجب إصلاحها. لعرض معلومات تفصيلية حول كل ثغرة أمنية، انقر فوق اسم الثغرة الأمنية في القائمة. لكل ثغرة أمنية في القائمة، يمكنك أيضًا عرض الإحصاءات حول الثغرة الأمنية في الأجهزة المُدارة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: عرض معلومات حول الثغرات الأمنية في البرامج، وعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة
- Kaspersky Security Center Web Console: عرض معلومات حول ثغرات البرامج، وعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة

3. **تكوين إصلاح الثغرات الأمنية**

عند اكتشاف الثغرات الأمنية بالبرامج، يمكنك إصلاح الثغرات الأمنية بالبرامج على الأجهزة المُدَارة باستخدام المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو المهمة إصلاح الثغرات الأمنية.

تُستخدَم المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية لتحديث وإصلاح الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها، بما في ذلك برامج Microsoft المثبتة على الأجهزة المُدارة. تتيح لك هذه المهمة تثبيت تحديثات متعددة وإصلاح ثغرات أمنية متعددة وفقًا لقواعد معينة. لاحظ أنه لا يمكن إنشاء هذه المهمة إلا إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات. لإصلاح الثغرات الأمنية بالبرامج تستخدم المهمةتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية تحديثات البرامج الموصى بها.

لا تتطلب مهمة إصلاح الثغرات الأمنية وجود خيار الترخيص لميزة إدارة الثغرات الأمنية والتصحيحات. لاستخدام هذه المهمة، يجب عليك تحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية المدرجة في إعدادات المهام تحديدًا يدويًا. تستخدم المهمة إصلاح الثغرات الأمنية الإصلاحات الموصى بها لبرامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية.

يمكنك بدء تشغيل معالج إصلاح الثغرات الأمنية الذي ينشئ إحدى هذه المهام تلقائيًا، أو يمكنك إنشاء واحدة من هذه المهام يدويًا.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية، إصلاح الثغرات الأمنية في التطبيقات
- Kaspersky Security Center Web Console: تحديد إصلاحات المستخدم للثغرات الأمنية في برنامج الجهة الخارجية، وإصلاح الثغرات الأمنية في برامج الجهات الخارجية، وإنشاء تثبيت التحديثات المطلوبة وإصلاح مهمة الثغرات الأمنية

4 **جدولة المهام**

للتأكد من أن قائمة الثغرات الأمنية مُحدَّثة دائمًا، قم بجدولة المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة لتشغيلها تلقائيًا من وقتٍ لآخر. متوسط التكرار الموصى به هو مرة واحدة في الأسبوع.

إذا كنت قد أنشأت المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، فيمكنك جدولتها لتعمل مع نفس تردد المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة أو أقل غالبًا. عند وضع جدول إصلاح الثغرات الأمنية للمهمة، لاحظ أنه يجب تحديد إصلاحات لبرامج Microsoft أو تحديد إصلاحات المستخدم لبرامج الطرف الثالث في كل مرة قبل بدء المهمة.

عند جدولة المهام، تأكد من أن مهمة إصلاح الثغرات الأمنية تبدأ بعد استكمال المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة.

5 **تجاهل الثغرات الأمنية في البرامج (اختياري)**

إذا كنت تريد، فيمكنك تجاهل الثغرات الأمنية بالبرامج التي يلزم إصلاحها على جميع الأجهزة المُدارة أو على الأجهزة المُدارة المحددة فحسب.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تجاهل الثغرات الأمنية بالبرامج
- Kaspersky Security Center Web Console: تجاهل الثغرات الأمنية في البرامج

6 **تشغيل مهمة إصلاح الثغرات الأمنية**

ابدأ المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو المهمة إصلاح الثغرات الأمنية. عند اكتمال المهمة، تأكد من وجود الحالة مكتمل بنجاح في قائمة المهام.

7 **إنشاء تقرير حول نتائج إصلاح الثغرات الأمنية في البرامج (اختياري)**

لعرض إحصاءات تفصيلية حول إصلاح الثغرات الأمنية، قم بإنشاء تقرير الثغرات الأمنية. يعرض التقرير معلومات حول الثغرات الأمنية بالبرامج التي لم يتم إصلاحها. وبالتالي، يمكن أن يكون لديك فكرة عن العثور على ثغرات أمنية وإصلاحها في برامج الجهات الخارجية، بما في ذلك برامج Microsoft، في مؤسستك.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء تقرير وعرضه
- Kaspersky Security Center Web Console: إنشاء تقرير وعرضه

8 **التحقق من تكوين البحث عن الثغرات الامنية وإصلاحها في برامج الجهات الخارجية**

تأكد من أنك قد قمت بما يلي:

- تم الحصول على الثغرات الأمنية بالبرامج ومراجعتها على الأجهزة المُدارة
- تجاهل الثغرات الأمنية في البرامج إذا أردت
- تم تكوين المهمة لإصلاح الثغرات الأمنية

- جدولة المهام للعثور على الثغرات الأمنية للبرامج وإصلاحها حتى تبدأ بالتتابع
- تم التحقق من تشغيل مهمة إصلاح الثغرات الأمنية في البرامج

النتائج

إذا أنشأت المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وكوَّنتها، يتم إصلاح الثغرات الأمنية على الأجهزة المُدارة تلقائيًا. عند تشغيل المهمة، فإنها تربط قائمة تحديثات البرامج المتاحة بالقواعد المحددة في إعدادات المهمة. سيتم تنزيل جميع تحديثات البرامج التي تفي بالمعايير الواردة في القواعد على مستودع خادم الإدارة وسيتم تثبيتها لإصلاح الثغرات الأمنية بالبرامج.

إذا كنت قد أنشأت المهمة إصلاح الثغرات الأمنية، فسيتم إصلاح الثغرات الأمنية في البرامج فقط في برامج Microsoft.

حول البحث عن الثغرات الأمنية بالبرامج وإصلاحها

يكتشف Kaspersky Security Center ويصلح الثغرات الأمنية على الأجهزة المُدارة التي تعمل بأنظمة تشغيل عائلات Microsoft Windows. تم الكشف عن الثغرات الأمنية في نظام التشغيل وفي برامج الجهات الخارجية، بما فيها برامج Microsoft.

وظيفة التحديثات (بما في ذلك توفير تحديثات توقيع مكافحة الفيروسات وتحديثات قاعدة التعليمات البرمجية)، بالإضافة إلى وظيفة KSN التي قد لا تكون متاحة في البرنامج في الولايات المتحدة الأمريكية.

العثور على الثغرات الأمنية بالبرامج

للعثور على الثغرات الأمنية بالبرامج، يستخدم Kaspersky Security Center الخصائص من قاعدة بيانات الثغرات الأمنية المعروفة. يتم إنشاء قاعدة البيانات هذه بواسطة أخصائيين في Kaspersky. يحتوي على معلومات حول الثغرات الأمنية، مثل وصفها وتاريخ اكتشافها ومستوى شدتها. يمكنك العثور على تفاصيل الثغرات الأمنية بالبرامج على موقع ويب Kaspersky.

يستخدم Kaspersky Security Center المهمةبحث عن الثغرات الأمنية والتحديثات المطلوبة للعثور على الثغرات الأمنية بالبرامج.

في بعض الحالات، يمكن إصلاح الثغرات الأمنية المكتشفة في نظام التشغيل Microsoft Windows باستخدام أي من الطرق التالية:

- تثبيت تحديث لنظام التشغيل.
- ترقية نظام التشغيل إلى إصدار أحدث (على سبيل المثال، من Windows 10 إلى Windows 11).

في هذا السيناريو، يعرض Kaspersky Security Center إدخالين للثغرة الأمنية نفسها.

إصلاح الثغرات الأمنية في البرامج

لإصلاح الثغرات الأمنية بالبرامج، يستخدم Kaspersky Security Center تحديثات البرامج الصادرة عن بائعي البرامج. يتم تنزيل بيانات تعريف تحديثات البرامج إلى مستودع خادم الإدارة نتيجة تشغيل المهام التالية:

- تنزيل التحديثات إلى مستودع خادم الإدارة. تهدف هذه المهمة إلى تنزيل بيانات التعريف الخاصة بالتحديثات لـ Kaspersky وبرامج الجهات الخارجية. يتم إنشاء هذه المهمة تلقائيًا من خلال معالج البدء السريع في Kaspersky Security Center. يمكنك إنشاء تحديثات التنزيل لمهمة مستودع خادم الإدارة يدويًا.

- إجراء مزامنة Windows Update. تهدف هذه المهمة إلى تنزيل بيانات التعريف الخاصة بالتحديثات لبرامج Microsoft.

يمكن تمثيل تحديثات البرامج لإصلاح الثغرات الأمنية كحزم توزيع كاملة أو تصحيحات. تحديثات البرنامج التي تعمل على إصلاح الثغرات الأمنية بالبرامج تُسمى إصلاحات. الإصلاحات الموصى بها هي تلك الموصى بها للتثبيت بواسطة أخصائيين في Kaspersky. إصلاحات المستخدم هي التحديثات التي تُحدَّد يدويًا للتثبيت من خلال المستخدمين. لتثبيت إصلاح مستخدم، يجب عليك إنشاء حزمة تثبيت تحتوي على هذا الإصلاح.

إذا كان لديك ترخيص Kaspersky Security Center مع ميزة إدارة الثغرات الأمنية والتصحيحات، فيمكنك لإصلاح ثغرات البرامج التي يمكنك استخدام المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. تعمل هذه المهمة تلقائيًا على إصلاح ثغرات أمنية متعددة تقوم بتثبيت الإصلاحات الموصى بها. لهذه المهمة، يمكنك تكوين قواعد معينة يدويًا لإصلاح ثغرات أمنية متعددة.

إذا لم يكن لديك ترخيص Kaspersky Security Center مع ميزة إدارة الثغرات الأمنية والتصحيحات، لإصلاح الثغرات الأمنية في البرامج، فيمكنك استخدام المهمة إصلاح الثغرات الأمنية. عن طريق هذه المهمة، يمكنك إصلاح الثغرات الأمنية عن طريق تثبيت الإصلاحات الموصى بها لبرامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية.

لأسباب تتعلق بالأمان، يتم تلقائيًا فحص أي تحديثات برامج، تابعة لطرف ثالث، تقوم بتثبيتها باستخدام ميزة إدارة الثغرات الأمنية والتصحيحات بحثًا عن البرامج الضارة بواسطة تقنيات Kaspersky. تُستخدم هذه التقنيات لعمليات فحص الملفات بشكل تلقائي، وتتضمن فحص الفيروسات، وتحليلًا ثابتًا، وتحليلًا ديناميكيًا، وتحليل السلوك في بيئة وضع الحماية والتعلم الآلي.

لا يقوم خبراء Kaspersky بإجراء تحليل يدوي لتحديثات برامج الجهات الخارجية التي يمكن تثبيتها من خلال استخدام ميزة إدارة الثغرات الأمنية والتصحيحات. بالإضافة إلى ذلك، لا يبحث خبراء Kaspersky عن الثغرات الأمنية (المعروفة أو غير المعروفة) أو الميزات غير الموثقة في مثل هذه التحديثات، ولا يجرون أنواعًا أخرى من تحليل التحديثات بخلاف تلك المحددة في الفقرة أعلاه.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

لإصلاح بعض الثغرات الأمنية في البرامج، يجب عليك قبول اتفاقية ترخيص المستخدم النهائي لتثبيت البرنامج إذا كانت الموافقة على اتفاقية ترخيص المستخدم النهائي مطلوبة. إذا رفضت اتفاقية ترخيص المستخدم النهائي، فلا يتم إصلاح الثغرات الأمنية بالبرامج.

إصلاح الثغرات الأمنية ببرامج الجهات الخارجية

بعد أن تحصل على قائمة الثغرات الأمنية بالبرنامج، يمكنك إصلاح الثغرات الأمنية في البرنامج على الأجهزة المُدارة التي تعمل بنظام Windows. يمكنك إصلاح الثغرات الأمنية في البرنامج في نظام التشغيل وفي برامج الجهات الخارجية، بما في ذلك برامج Microsoft، عن طريق إنشاء مهمة Fix vulnerabilities وتشغيلها أو مهمة Install required updates and fix vulnerabilities.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

كخيار متاح، يمكنك إنشاء مهمة لإصلاح الثغرات الأمنية في البرنامج بالطرق التالية:

- عن طريق فتح قائمة الثغرات الأمنية وتحديد الثغرات الأمنية المراد إصلاحها.

  وكنتيجة لذلك، يتم إنشاء مهمة جديدة لإصلاح الثغرات الأمنية في البرنامج. كخيار متاح، يمكنك إضافة الثغرات الأمنية المحددة إلى مهمة موجودة.

- عن طريق تشغيل معالج إصلاح الثغرات الأمنية.

> لا يتوفر معالج إصلاح الثغرات الأمنية إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

يقوم المعالج بتبسيط إنشاء مهمة إصلاح الثغرات الأمنية وتكوينها، كما يسمح لك بإزالة إنشاء المهام الزائدة التي تحتوي على نفس التحديثات المراد تثبيتها.

إصلاح الثغرات الأمنية في البرامج عن طريق استخدام قائمة الثغرات الأمنية

لإصلاح الثغرات الأمنية في البرامج:

1. افتح إحدى قوائم الثغرات الأمنية:

- لفتح قائمة الثغرات الأمنية العامة، في القائمة الرئيسية، انتقل إلى **Software** ← **Patch management** ← **Operations** ← **vulnerabilities**.
- لفتح قائمة الثغرات الأمنية لجهاز مُدار، في القائمة الرئيسية، انتقل إلى <device name> ← **Managed devices** ← **Assets (Devices)** ← **Software vulnerabilities** ← **Advanced** ←.
- لفتح قائمة الثغرات الأمنية لتطبيق محدد، في القائمة الرئيسة، انتقل إلى **Applications** ← **Third-party applications** ← **Operations** ← **Vulnerabilities** ← <application name> ← **registry**.

سيتم عرض صفحة بها قائمة الثغرات الأمنية في برنامج الجهة الخارجية.

2. حدد ثغرة أمنية أو أكثر في القائمة ثم انقر على زر **Fix vulnerability**.

   في غياب تحديث برنامج موصى به لإصلاح إحدى الثغرات الأمنية المحددة، سيتم عرض رسالة تفيد ذلك.

   لإصلاح بعض الثغرات الأمنية في البرامج، يجب عليك قبول اتفاقية ترخيص المستخدم النهائي لتثبيت البرنامج إذا كانت الموافقة على اتفاقية ترخيص المستخدم النهائي مطلوبة. إذا رفضت اتفاقية ترخيص المستخدم النهائي، فلا يتم إصلاح الثغرات الأمنية بالبرامج.

3. حدد أحد الخيارات التالية:

- **New task**

  سيبدأ معالج المهمة الجديدة. إذا كان لديك ترخيص إدارة الثغرات الأمنية والتصحيحات، يتم تحديد مهمة Install required updates and fix vulnerabilities مسبقًا. إذا لم يكن لديك الترخيص، يتم تحديد مهمة Fix vulnerabilities مسبقًا. اتبع خطوات المعالج لإكمال إنشاء المهمة.

- **Fix vulnerability (add rule to specified task)**

  حدد مهمة ترغب في إضافة الثغرات الأمنية المحددة إليها. إذا كان لديك ترخيص إدارة الثغرات الأمنية والتصحيحات، حدد مهمة Install required updates and fix vulnerabilities. سيتم تلقائيًا إضافة قاعدة جديدة لإصلاح الثغرات الأمنية المحددة إلى المهمة المحددة. إذا لم يكن لديك الترخيص، حدد مهمة Fix vulnerabilities. سيتم إضافة الثغرات الأمنية إلى خصائص المهمة.

  ستفتح نافذة خصائص المهمة. انقر على زر **Save** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، سيتم إنشاء المهمة وعرضها في قائمة المهام في **Tasks** ← **Assets (Devices)**. إذا اخترت إضافة الثغرات الأمنية إلى مهمة موجودة، يتم حفظ الثغرات الأمنية في خصائص المهمة.

لإصلاح الثغرات الأمنية لبرامج الجهات الخارجية، ابدأ مهمة Install required updates and fix vulnerabilities أو مهمة Fix vulnerabilities. إذا كنت قد أنشأت مهمة Fix vulnerabilities، يجب عليك تحديد تحديثات البرامج يدويًا لإصلاح الثغرات الأمنية في البرامج المدرجة في إعدادات المهمة.

إصلاح الثغرات الأمنية في البرامج عن طريق استخدام معالج إصلاح الثغرات الأمنية

لا يتوفر معالج إصلاح الثغرات الأمنية إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

لإصلاح الثغرات الأمنية في البرامج عن طريق استخدام معالج إصلاح الثغرات الأمنية:

1. في القائمة الرئيسية ، انتقل إلى **Software vulnerabilities** ← **Patch management** ← **Operations**.
   سيتم عرض صفحة بها قائمة الثغرات الأمنية في برنامج الجهة الخارجية المثبتة على الأجهزة المُدارة.
2. حدد خانة الاختيار الموجودة بجوار الثغرة الأمنية التي ترغب في إصلاحها.
3. انقر على زر **Run Vulnerability fix wizard**.
   يبدأ معالج إصلاح الثغرات الأمنية. تعرض صفحة **Select the vulnerability fix task** قائمة بجميع المهام الموجودة من الأنواع التالية:
   - Install required updates and fix vulnerabilities
   - Install Windows Update updates
   - Fix vulnerabilities

   لا يمكنك تعديل آخر نوعين من المهام لتثبيت التحديثات الجديدة. لتثبيت التحديثات الجديدة، لا يمكنك استخدام إلا مهمة Install required updates and fix vulnerabilities.
4. إذا كنت ترغب في ألا يعرض المعالج إلا المهام التي تصلح الثغرة الأمنية التي حددتها، قم بتفعيل خيار **Show only tasks that fix this vulnerability**.
5. اختر ما ترغب في فعله:
   - لبدء مهمة، حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر **Start**.
   - لإضافة قاعدة جديدة إلى مهمة موجودة:
     a. حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر **Add rule**.
     b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:
     - **Rule for fixing vulnerabilities of this severity level**

       قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

       إذا تم تمكين هذا الخيار، لا تقوم التحديثات بإصلاح إلا تلك الثغرات الأمنية التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة لمستوى حدة التحديث المحدد أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

       إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

       يتم تعطيل هذا الخيار افتراضيًا.

- **قاعدة لإصلاح الثغرات الأمنية عن طريق تحديثات من نفس نوع التحديث المحدد على النحو الموصى به للثغرة الأمنية المحددة** (غير متاح إلا لثغرات برامج Microsoft)

- **Rule for fixing vulnerabilities in applications from the selected vendor** (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

- **Rule for fixing a vulnerability in all versions of the selected application** (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

- **Rule for fixing the selected vulnerability**

- **Approve updates that fix this vulnerability**

سيتم اعتماد التحديث المحدد للتثبيت. تمكين هذا الخيار في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها فقط.

يتم تعطيل هذا الخيار افتراضيًا.

c. انقر على الزر **Add**.

- لإنشاء مهمة:

a. انقر على زر **New task**.

b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:

- **Rule for fixing vulnerabilities of this severity level**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، لا تقوم التحديثات بإصلاح إلا تلك الثغرات الأمنية التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة لمستوى حدة التحديث المحدد أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **قاعدة لإصلاح الثغرات الأمنية عن طريق تحديثات من نفس نوع التحديث المحدد على النحو الموصى به للثغرة الأمنية المحددة** (غير متاح إلا لثغرات برامج Microsoft)

- **Rule for fixing vulnerabilities in applications from the selected vendor** (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

- **Rule for fixing a vulnerability in all versions of the selected application** (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

- **Rule for fixing the selected vulnerability**

- **Approve updates that fix this vulnerability**

سيتم اعتماد التحديث المحدد للتثبيت. تمكين هذا الخيار في حالة سماح بعض القواعد المطبقة الخاصة بتثبيت التحديث بتثبيت تحديثات مصدق عليها فقط.

يتم تعطيل هذا الخيار افتراضيًا.

c. انقر على الزر **Add**.

إذا اخترت بدء مهمة، يمكنك إغلاق المعالج. سيتم استكمال المهمة في وضع الخلفية. لا يلزم اتخاذ إجراءات إضافية.

إذا اخترت إضافة قاعدة إلى مهمة موجودة، ستفتح نافذة خصائص المهمة. تمت إضافة القاعدة الجديدة بالفعل إلى خصائص المهمة. يمكنك عرض القاعدة أو إعدادات المهمة الأخرى أو تعديلها. انقر على زر **Save** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، ستستمر في إنشاء المهمة في معالج المهمة. القاعدة الجديدة التي أضفتها إلى معالج إصلاح الثغرات الأمنية سيتم عرضها في معالج المهمة الجديدة. عندما تكمل المعالج، سيتم إضافة مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية إلى قائمة المهام.

إنشاء مهمة إصلاح الثغرات الأمنية.

مهمة Fix vulnerabilities تتيح لك إصلاح الثغرات الأمنية في البرامج على الأجهزة المُدارة التي تعمل بنظام Windows. يمكنك إصلاح الثغرات الأمنية في برامج الجهات الخارجية، بما في ذلك برامج Microsoft.

إذا لم يكن لديك ترخيص إدارة الثغرات الأمنية والتصحيحات، فلن تتمكن من إنشاء مهام جديدة لنوع Fix vulnerabilities. لإصلاح الثغرات الأمنية الجديدة، يمكنك إضافتها إلى مهمة Fix vulnerabilities موجودة. نوصي باستخدام مهمة Install required updates and fix vulnerabilities بدلاً من مهمة Fix vulnerabilities. تمكنك مهمة Install required updates and fix vulnerabilities من تثبيت تحديثات متعددة وإصلاح العديد من الثغرات الأمنية تلقائيًا وفقًا للقواعد التي تحددها.

قد يكون تفاعل المستخدم مطلوبًا عند تحديث تطبيق تابع لجهة خارجية أو إصلاح ثغرة أمنية في تطبيق تابع لجهة خارجية على جهاز مُدار. على سبيل المثال، قد يُطلب من المستخدم إغلاق تطبيق الجهة الخارجية إذا كان مفتوحًا حاليًا.

لإنشاء مهمة Fix vulnerabilities.

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.
2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.
3. لتطبيق Kaspersky Security Center، حدد نوع المهمة **Fix vulnerabilities**.
4. حدد اسم المهمة التي ترغب في إنشائها.

   لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).
5. حدد الأجهزة التي سيتم تعيين المهمة إليها:
6. انقر على زر **Add**.

   ستفتح قائمة الثغرات الأمنية.
7. حدد الثغرات الأمنية التي ترغب في إصلاحها ثم انقر على **OK**.

   الثغرات الأمنية في برامج Microsoft عادةً ما يكون لها إصلاحات موصى بها. لا يلزم اتخاذ أي إجراءات إضافية لها. للثغرات الأمنية في البرامج من البائعين الآخرين، ستحتاج أولاً إلى تحديد إصلاح مستخدم لكل ثغرة أمنية ترغب في إصلاحها. ستقدر بعد ذلك على إضافة تلك الثغرات الأمنية إلى مهمة Fix vulnerabilities.
8. حدد إعدادات إعادة تشغيل نظام التشغيل:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **Force closure of applications in blocked sessions**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

9. حدد الإعدادات التالية:

- **Default account**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه.

يتم تحديد هذا الخيار افتراضيًا.

- **Specify account**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **Account**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **Password**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

10. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

11. انقر على زر **Finish**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

12. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

13. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك.

14. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية

لا تتوفر مهمة Install required updates and fix vulnerabilities إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

تُستخدَم المهمة Install required updates and fix vulnerabilities لتحديث وإصلاح الثغرات الأمنية في برامج الجهات الخارجية وإصلاحها، بما في ذلك برامج Microsoft المثبتة على الأجهزة المُدارة. تتيح لك هذه المهمة تثبيت تحديثات متعددة وإصلاح ثغرات أمنية متعددة وفقًا لقواعد معينة.

لتثبيت التحديثات أو إصلاح الثغرات الأمنية باستخدام مهمة Install required updates and fix vulnerabilities، يمكنك القيام بأي مما يلي:

- تشغيل معالج تثبيت التحديث أو معالج إصلاح الثغرات الأمنية.
- إنشاء مهمة Install required updates and fix vulnerabilities.
- أضف قاعدة لتثبيت التحديث إلى مهمة Install required updates and fix vulnerabilities موجودة.

لإنشاء مهمة Install required updates and fix vulnerabilities:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة **Install required updates and fix vulnerabilities**.

إذا لم يتم عرض المهمة، فتحقق مما إذا كان حسابك لديه **حقوق القراءة** و **التعديل** و التنفيذ للمجال **الوظيفي**: **لإدارة الثغرات الأمنية والتصحيحات** لا يمكنك إنشاء وتكوين مهمة قم بتثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية بدون حقوق الوصول هذه.

4. حدد اسم المهمة التي ترغب في إنشائها. لا يمكن أن يحتوي اسم المهمة على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة ("*<>?\:|).

5. حدد الأجهزة التي سيتم تعيين المهمة إليها:

6. حدد قواعد تثبيت التحديث، وبعدها حدد الإعدادات التالية:

- **Start installation at device restart or shutdown**

إذا تم تمكين هذا الخيار، فسيتم تثبيت التحديثات عند إعادة تشغيل الجهاز أو إغلاقه. بخلاف ذلك، يتم تثبيت التحديثات وفقًا لجدول زمني.

استخدم هذا الخيار في حال كان تنزيل التحديثات قد يؤثر على أداء الجهاز.

يتم تعطيل هذا الخيار افتراضيًا.

- **Install the required general system components**

إذا تم تمكين هذا الخيار، قبل تثبيت التحديث، يقوم التطبيق تلقائيًا بتثبيت كافة مكونات النظام العامة (المتطلبات الأساسية) اللازمة لتثبيت التحديث. على سبيل المثال، يمكن أن تكون تلك المتطلبات الأساسية عبارة عن تحديثات نظام التشغيل.

إذا تم تعطيل هذا الخيار، فقط يتعين عليك تثبيت المتطلبات الأساسية يدويًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **Allow installation of new application versions during updates**

إذا تم تمكين هذا الخيار، سيتم السماح بالتحديثات التي تؤدي إلى تثبيت إصدار جديد من تطبيق البرنامج.

إذا تم تعطيل هذا الخيار، فلن تتم ترقية البرنامج. بعد ذلك يمكنك تثبيت إصدارات البرنامج الجديدة يدويًا أو من خلال مهمة أخرى. على سبيل المثال، قد تستخدم هذا الخيار في حال كانت البنية الأساسية الخاصة بشركتك غير مدعومة بواسطة إصدار جديد للبرنامج أو في حال رغبت في التحقق من ترقية في اختبار البنية الأساسية.

يتم تمكين هذا الخيار افتراضيًا.

قد تؤدي ترقية التطبيق إلى حدوث خلل في التطبيقات التابعة المثبتة على أجهزة عميلة.

- **Download updates to the device without installing them**

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بتنزيل التحديثات على الجهاز ولكن لن يقوم بتنزيلها تلقائيًا. بعد ذلك يمكنك تثبيت التحديثات التي تم تنزيلها يدويًا.

تم تنزيل تحديثات Microsoft إلى مخزن Windows في النظام. يتم تنزيل تحديثات تطبيقات الجهات الخارجية (تطبيقات تم صنعها من قبل موردي برامج آخرين غير Kaspersky وMicrosoft) في المجلد المحدد في حقل **تنزيل التحديثات إلى**.

إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائيًا.

يتم تعطيل هذا الخيار افتراضيًا.

- **Download updates to**

يتم استخدام هذا المجلد لتنزيل تحديثات خاصة بتطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky وMicrosoft).

- **Enable advanced diagnostics**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة ملفات التتبع حتى إذا كانت كتابة ملفات التتبع معطلة لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الأخر؛ ويتم تحديد الحجم الإجمالي لكلا الملفين من خلال القيمة **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**. عندما يصبح كلا الملفين مكتملين، يبدأ عميل الشبكة في الكتابة بهم مرة أخرى. يتم تخزين الملفات ذات عمليات التتبع في مجلد %WINDIR%\Temp. يمكن الوصول لهذه الملفات في أداة التشخيصات المساعدة عن بُعد، حيث يمكنك تنزيلهم أو حذفهم.

إذا تم تعطيل هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع وفقًا للإعدادات في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. لا يتم كتابة عمليات تتبع إضافية.

عند إنشاء مهمة، لا يتوجب عليك تمكين التشخيصات المتقدمة. قد تحتاج لاستخدام هذه الميزة لاحقًا إذا فشل على سبيل المثال تشغيل مهمة على بعض الأجهزة، وكنت ترغب في الحصول على معلومات إضافية أثناء تشغيل مهمة أخرى.

يتم تعطيل هذا الخيار افتراضيًا.

- **Maximum size, in MB, of advanced diagnostics files**

القيمة الافتراضية هي 100 ميجابايت، وتتراوح القيم المتوفرة بين 1 ميجابايت و2 048 ميجابايت. قد يطلب منك أخصائيو الدعم الفني لـ Kaspersky تغيير القيمة الافتراضية عندما لا تكون المعلومات المتواجدة في ملفات التشخيص المتقدمة التي قمت بإرسالها كافية لاستكشاف المشكلة وإصلاحها.

7. حدد إعدادات إعادة تشغيل نظام التشغيل:

- **Do not restart the device**

لم تتم إعادة تشغيل أجهزة العميل تلقائيًا بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). يتم حفظ المعلومات حول إعادة التشغيل المطلوب في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب للمهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل أمرًا بالغ الأهمية.

- **Restart the device**

يتم إعادة تشغيل الأجهزة العميلة تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **Prompt user for action**

سيتم عرض تذكير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمةً لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

يتم تحديد هذا الخيار افتراضيًا.

- **Repeat prompt every (min)**

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد.

يتم تمكين هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو 5 دقائق. القيم المتوفرة بين 1 و1440 دقيقة.

إذا تم تعطيل هذا الخيار، فسيتم عرض المطالبة مرة واحدة فقط.

- **Restart after (min)**

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد.

يتم تمكين هذا الخيار افتراضيًا. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

- **فترة الانتظار قبل فرض إغلاق التطبيقات في الجلسات المحجوبة (بالدقائق)**

يتم غلق التطبيقات إجباريًا عند قفل جهاز المستخدم (تلقائيًا عقب فترة زمنية محددة من عدم النشاط، أو يدويًا)

إذا تم تمكين هذا الخيار، فسيتم فرض غلق التطبيقات على الجهاز المقفل عند انتهاء الفترة الزمنية المحددة في حقل الإدخال.

إذا تم تعطيل هذا الخيار، فلن يتم غلق التطبيقات على الجهاز المقفل.

يتم تعطيل هذا الخيار افتراضيًا.

8. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **Open task details when creation is complete** في صفحة **Finish task creation**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

9. انقر على زر **Finish**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

10. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

11. في نافذة خصائص المهمة، حدد إعدادات المهمة العامة وفقًا لاحتياجاتك.

12. انقر على زر **Save**.

سيتم إنشاء المهمة وتكوينها.

إذا كانت نتائج المهمة تحتوي على تحذير من خطأ 0x80240033 "خطأ عميل Windows Update 80240033 ("تعذر تنزيل شروط الترخيص.")"، يمكنك حل هذه المشكلة من خلال سجل Windows.

حدد قواعد لتثبيت التحديثات

هذه الميزة غير متاحة إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

عند تثبيت تحديثات برامج أو إصلاح ثغرات أمنية في برنامج باستخدام مهمة Install required updates and fix vulnerabilities، يجب عليك تحديد قواعد تثبيت التحديث. تحدد هذه القواعد التحديثات المراد تثبيتها والثغرات الأمنية المراد إصلاحها.

تعتمد نفس الإعدادات عما إذا كنت تقوم بإنشاء قاعدة لتحديثات تطبيقات Microsoft، أو تطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky وMicrosoft) أو لجميع التطبيقات. عند إنشاء قاعدة لتطبيقات Microsoft أو تطبيقات الجهات الخارجية، يمكنك تحديد تطبيقات وإصدارات تطبيق معينة ترغب في تثبيت التحديثات من أجلها. عند إنشاء قاعدة لجميع التطبيقات، يمكنك تحديد تحديثات معينة ترغب في تثبيتها وثغرات أمنية ترغب في إصلاحها عن طريق تثبيت التحديثات.

يمكنك إضافة قاعدة لتثبيت التحديث بالطرق التالية:

- بإضافة قاعدة أثناء إنشاء مهمة Install required updates and fix vulnerabilities جديدة.
- عن طريق إضافة قاعدة في تبويب **إعدادات التطبيق** في نافذة الخصائص للمهمة Install required updates and fix vulnerabilities الموجودة.
- من خلال معالج تثبيت التحديث أو معالج إصلاح الثغرات الأمنية.

لإضافة قاعدة جديدة لجميع التحديثات:

1. انقر على الزر **إضافة**.

   يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

2. في صفحة **نوع القاعدة**، حدد**قاعدة لجميع التحديثات**.

3. في صفحة **المعايير العامة**، استخدم القوائم المنسدلة لتحديد الإعدادات التالية:

   - **مجموعة التحديثات المراد تثبيتها**

     حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

     - **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
     - **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
     - **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

   - **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

     قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

     إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

     إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

     يتم تعطيل هذا الخيار افتراضيًا.

4. في صفحة **التحديثات**، حدد التحديثات المراد تثبيتها:

- **تثبيت جميع التحديثات المناسبة**

تثبيت جميع تحديثات البرامج التي تتوافق مع المعايير المحددة في صفحة **معايير عامة** الخاصة بالمعالج. يتم تحديده بصورة افتراضية.

- **تثبيت التحديثات من القائمة فقط**

قم بتثبيت تحديثات البرامج التي تحددها يدويًا فقط من القائمة. تحتوي القائمة على جميع تحديثات البرامج المتاحة.

على سبيل المثال، قد ترغب في تحديد تحديثات معينة في الحالات التالية: للتحقق من إجراءات تثبيتها في بيئة اختبارية، أو لتحديث التطبيقات المهمة فقط، أو لتحديث التطبيقات المعينة فقط.

- **تثبيت كل تحديثات التطبيق السابقة المطلوبة لتثبيت التحديثات المحددة تلقائيًا**

استمر في تمكين هذا الخيار إذا كنت توافق على تثبيت إصدارات التطبيق مؤقتًا عندما يُطلب ذلك لتثبيت التحديثات المحددة.

إذا تم تعطيل هذا الخيار، فإنه يتم تثبيت إصدارات التطبيقات المحددة فقط. قم بتعطيل هذا الخيار إذا كنت تريد تحديث التطبيقات بطريقة مباشرة، دون محاولة تثبيت إصدارات متتابعة تدريجيًا. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، فسيفشل تحديث التطبيق.

على سبيل المثال، لديك الإصدار رقم 3 لتطبيق مثبت على أحد الأجهزة وتريد تحديثه إلى الإصدار رقم 5، ولكن الإصدار رقم 5 لهذا التطبيق يمكن تثبيته فوق الإصدار رقم 4 فقط. إذا تم تمكين هذا الخيار، فإن البرنامج يقوم أولاً بتثبيت الإصدار رقم 4، ومن ثم تثبيت الإصدار رقم 5. إذا تم تعطيل هذا الخيار، فإن البرنامج يفشل في تحديث التطبيق.

يتم تمكين هذا الخيار افتراضيًا.

5. في صفحة **الثغرات الأمنية**، حدد الثغرات الأمنية التي سيتم إصلاحها عن طريق تثبيت التحديثات المحددة:

- **إصلاح جميع الثغرات الأمنية التي تطابق المعايير الأخرى**

إصلاح جميع الثغرات الأمنية التي تتوافق مع المعايير المحددة في صفحة **معايير عامة** في المعالج. يتم تحديده بصورة افتراضية.

- **إصلاح الثغرات الأمنية من القائمة فقط**

قم بإصلاح الثغرات الأمنية التي تحددها يدويًا فقط من القائمة. تحتوي هذه القائمة على جميع الثغرات الأمنية التي تم اكتشافها.

على سبيل المثال، قد ترغب في تحديد ثغرات أمنية معينة في الحالات التالية: للتحقق من إجراءات إصلاحها في بيئة اختبارية، أو لإصلاح الثغرات الأمنية في التطبيقات المهمة فقط، أو لإصلاح الثغرات الأمنية في تطبيقات معينة فقط.

6. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإضافتها. يمكنك بعد ذلك تغيير هذا الاسم في قسم **الإعدادات** من نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد استكمال معالج إنشاء القاعدة لعملياته، يتم إضافة القاعدة الجديدة وعرضها في قائمة القاعدة في معالج المهمة الجديدة أو في خصائص المهمة.

لإضافة قاعدة جديدة إلى تحديثات Windows Update:

1. انقر على الزر **إضافة**.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

2. في صفحة **نوع القاعدة**، حدد **قاعدة تحديث Windows**.

3. في صفحة **المعايير العامة**، حدد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

- **قم بإصلاح الثغرات الأمنية ذات مستوى الخطورة MSRC الذي يساوي أو أعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Microsoft Security Response Center (MSRC) مساويًا للقيمة المحددة في القائمة أو أعلى منها (**منخفض**، أو **متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضيًا.

5. في الصفحة **فئات التحديثات**، حدد فئات التحديثات المطلوب تثبيتها. هذه الفئات هي نفس الفئات الموجودة في Microsoft Update Catalog. يتم تحديد جميع الفئات افتراضيًا.

6. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإضافتها. يمكنك بعد ذلك تغيير هذا الاسم في قسم **الإعدادات** من نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد استكمال معالج إنشاء القاعدة لعملياته، يتم إضافة القاعدة الجديدة وعرضها في قائمة القاعدة في معالج المهمة الجديدة أو في خصائص المهمة.

لإضافة قاعدة جديدة لتحديثات تطبيقات الجهات الخارجية:

1. انقر على الزر **إضافة**.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

2. في صفحة **نوع القاعدة**، حدد**قاعدة تحديثات الأطراف الخارجية**.

3. في صفحة **المعايير العامة**، حدد الإعدادات التالية:

- **مجموعة التحديثات المراد تثبيتها**

حدد التحديثات التي يجب تثبيتها على الأجهزة العميلة:

- **تثبيت التحديثات المعتمدة فقط**. يقوم هذا الأمر بتثبيت التحديثات المعتمدة فقط.
- **تثبيت جميع التحديثات (ما عدا المرفوضة)**. يقوم هذا الأمر بتثبيت التحديثات التي تتمتع بحالة الموافقة المعتمدة أو غير المحددة.
- **تثبيت جميع التحديثات (بما في ذلك المرفوضة)**. يقوم هذا الأمر بتثبيت جميع التحديثات، بغض النظر عن حالة الموافقة التي تتمتع بها. حدد هذا الخيار بحذر. على سبيل المثال، استخدم هذا الخيار إذا كنت ترغب في التحقق من تثبيت بعض التحديثات المرفوضة في بنية تحتية اختبارية.

- **إصلاح الثغرات الأمنية ذات مستوى الخطورة المساوي لـ أو الأعلى من**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبيًا على تجربة المستخدم مع البرامج. في مثل هذه الحالات، يمكنك اتخاذ القرار بتثبيت تلك التحديثات المهمة فقط لتشغيل البرامج وتخطي تحديثات أخرى.

إذا تم تمكين هذا الخيار، فإن التحديثات تقوم بإصلاح تلك الثغرات الأمنية فقط التي يكون مستوى الخطورة الذي تم ضبطه من أجلها من جانب Kaspersky مساويًا للقيمة المحددة في القائمة أو أعلى منها (**متوسط**، أو **مرتفع**، أو **حرج**). لا يتم إصلاح الثغرات الأمنية التي لديها مستوى خطورة أقل من القيمة المحددة.

إذا تم تعطيل هذا الخيار، فإن التحديثات تقوم بإصلاح جميع الثغرات الأمنية بغض النظر عن مستوى خطورتها.

يتم تعطيل هذا الخيار افتراضيًا.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضيًا.

5. في صفحة **الاسم**، حدد اسم القاعدة التي تقوم بإضافتها. يمكنك بعد ذلك تغيير هذا الاسم في قسم الإعدادات في نافذة الخصائص للمهمة التي تم إنشاؤها.

بعد استكمال معالج إنشاء القاعدة لعملياته، يتم إضافة القاعدة الجديدة وعرضها في قائمة القاعدة في معالج المهمة الجديدة أو في خصائص المهمة.

تحديد إصلاحات المستخدم للثغرات الأمنية في برامج الجهات الخارجية

لاستخدام المهمة إصلاح الثغرات الأمنية، يجب عليك تحديد تحديثات البرامج يدويًا لإصلاح الثغرات الأمنية الموجودة في برامج الجهات الخارجية المدرجة في إعدادات المهمة. تستخدم المهمة إصلاح الثغرات الأمنية الإصلاحات الموصى بها لبرامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية الأخرى. إصلاحات المستخدم هي تحديثات للبرامج لإصلاح الثغرات الأمنية التي يحددها المسؤول يدويًا للتثبيت.

لتحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية:

1. في القائمة الرئيسية ، انتقل إلى **Operations ← Patch management ← Software vulnerabilities**.

تعرض الصفحة قائمة الثغرات الأمنية في البرامج التي تم اكتشافها على أجهزة العميل.

2. في قائمة الثغرات الأمنية في البرامج، انقر على رابط اسم الثغرة الأمنية في البرنامج الذي ترغب في تحديد إصلاح مستخدم له.

ستفتح نافذة خصائص الثغرة الأمنية.

3. في الجزء الأيمن، حدد القسم **User fixes and other fixes**.

سيتم عرض قائمة بإصلاحات المستخدم للثغرة الأمنية في البرنامج المحدد.

4. انقر فوق **إضافة**.

يتم عرض قائمة حزم التثبيت المتاحة. تتوافق قائمة حزم التثبيت المعروضة مع قائمة **Operations ← Repositories ← Installation packages** إذا لم تقم بإنشاء حزمة تثبيت تحتوي على إصلاح مستخدم لثغرة أمنية محددة، فيمكنك إنشاء الحزمة الآن عن طريق بدء معالج حزمة جديدة.

5. حدد حزمة (أو حزم) تثبيت تحتوي على إصلاح مستخدم (أو إصلاحات مستخدم) لثغرة أمنية في برنامج تابع لجهة خارجية.

6. انقر فوق **حفظ**.

يتم تحديد حزم التثبيت التي تحتوي على إصلاحات للمستخدم للثغرات الأمنية في البرامج. عند بدء المهمة إصلاح الثغرات الأمنية، سيتم تثبيت حزمة التثبيت وإصلاح الثغرات الأمنية في البرامج.

عرض معلومات حول ثغرات البرامج المكتشفة على جميع الأجهزة المدارة

بعد أن تكون قد فحصت البرامج على الأجهزة المُدارة بحثًا عن الثغرات الأمنية، يمكنك عرض قائمة الثغرات الأمنية في البرامج التي تم اكتشافها على جميع الأجهزة المُدارة. إذا قمت بتشغيل مهمة التسلسل الهرمي لخوادم الإدارة، فيمكنك عرض قائمة بالأجهزة المدارة التي تحتوي على ثغرات أمنية مكتشفة فقط لخادم الإدارة المحدد.

لعرض قائمة الثغرات الأمنية في البرامج المكتشفة على جميع الأجهزة المُدارة،

في القائمة الرئيسية ، انتقل إلى **Software vulnerabilities** ← **Patch management** ← **Operations**.

تعرض الصفحة قائمة الثغرات الأمنية في البرامج التي تم اكتشافها على أجهزة العميل.

يمكنك أيضًا إنشاء وعرض تقرير حول الثغرات الأمنية.

يمكنك تحديد عامل تصفية لعرض قائمة الثغرات الأمنية في البرامج. انقر على أيقونة **Filter** ( ) في أعلى يمين قائمة الثغرات الأمنية في البرنامج لإدارة عامل التصفية. يمكنك كذلك تحديد أحد عوامل التصفية المعدة مسبقًا من القائمة المنسدلة **Preset filters** أعلى قائمة الثغرات الأمنية في البرنامج.

يمكنك الحصول على معلومات تفصيلية عن أي ثغرة أمنية من القائمة.

للحصول على معلومات حول ثغرة أمنية في برنامج:

في قائمة الثغرات الأمنية في البرنامج، انقر على الرابط الذي يحمل اسم الثغرة الأمنية.

ستفتح نافذة خصائص الثغرة الأمنية للبرنامج.

عرض معلومات حول ثغرات البرامج المكتشفة على الجهاز المُدار المحدد

يمكنك عرض معلومات حول ثغرات البرامج المكتشفة على الجهاز المُدار المحدد ويعمل بنظام Windows.

لعرض قائمة الثغرات الأمنية في البرامج المكتشفة على الجهاز المُدار المحدد:

1. في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)**.
   يتم عرض قائمة الأجهزة المُدارة.

2. في قائمة الأجهزة المُدارة، انقر على رابط اسم الجهاز الذي ترغب في عرض الثغرات الأمنية المكتشفة عليه.
   يتم عرض نافذة خصائص الجهاز المحدد.

3. في نافذة خصائص الجهاز المحدد، حدد علامة التبويب **Advanced**.

4. في الجزء الأيمن، حدد القسم **Software vulnerabilities**.

سيتم عرض قائمة الثغرات الأمنية في البرامج المكتشفة على الجهاز المُدار المحدد.

لعرض خصائص الثغرة الأمنية في البرنامج المحددة،

انقر على رابط اسم الثغرة الأمنية في البرنامج في قائمة الثغرات الأمنية في البرنامج.

يتم عرض نافذة الخصائص الثغرة الأمنية في البرنامج المحددة.

عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة

يمكنك عرض إحصائيات لكل ثغرة أمنية في البرامج على الأجهزة المُدارة. تُمثَّل الإحصاءات في شكل مخطط. يعرض المخطط عدد الأجهزة بالحالات التالية:

- تم تجاهله على: <عدد الأجهزة>. يتم تعيين هذه الحالة إذا عيَّنت يدويًا، في خصائص الثغرة الأمنية، الخيار لتجاهل الثغرات الأمنية.
- مثبت على: <عدد الأجهزة>. يتم تعيين هذه الحالة إذا تم إكمال مهمة إصلاح الثغرات الأمنية بنجاح.
- الإصلاح مقرر في: <عدد الأجهزة> . يتم تعيين هذه الحالة إذا كنت قد أنشأت المهمة لإصلاح الثغرات الأمنية لكن لم يتم تنفيذ المهمة بعد.
- التصحيح المطبق على: <عدد الأجهزة>. يتم تعيين هذه الحالة إذا حددت تحديث برنامج يدويًا لإصلاح الثغرات الأمنية لكن تحديث البرنامج هذا لم يحل الثغرات الأمنية.
- الإصلاح مطلوب في: <عدد الأجهزة>. يتم تعيين هذه الحالة في حالة إصلاح الثغرة الأمنية على بعض الأجهزة المُدارة فقط، وكان من المطلوب إصلاح الثغرة الأمنية على المزيد من الأجهزة المُدارة.

لعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة:

1. في القائمة الرئيسية ، انتقل إلى **Software vulnerabilities** ← **Patch management** ← **Operations**.
   تعرض الصفحة قائمة بالثغرات الأمنية في التطبيقات المكتشفة على الأجهزة المُدارة.
2. حدد خانة الاختيار الموجودة بجوار الثغرة الأمنية المطلوبة.
3. انقر على زر **Statistics of vulnerability on devices**.

يتم عرض مخطط بحالات الثغرات الأمنية. يؤدي النقر فوق إحدى الحالات إلى فتح قائمة بالأجهزة التي تحتوي على الثغرة الأمنية للحالة المحددة.

تصدير قائمة بأحداث التشفير إلى ملف نص

يمكنك تصدير القائمة المعروضة للثغرات الأمنية إلى ملف بامتداد CSV أو TXT. يمكنك استخدام هذه الملفات، على سبيل المثال، لإرسالها إلى مدير أمن المعلومات الخاص بك أو لتخزينها لأغراض الإحصائيات.

لتصدير قائمة الثغرات الأمنية في البرامج المكتشفة على جميع الأجهزة المُدارة إلى ملف نصي:

1. في القائمة الرئيسية ، انتقل إلى **Software vulnerabilities** ← **Patch management** ← **Operations**.
   تعرض الصفحة قائمة بالثغرات الأمنية في التطبيقات المكتشفة على الأجهزة المُدارة.
2. انقر على زر **Export to TXT** أو **Export to CSV**، حسب التنسيق الذي تفضله للتصدير.

يتم تنزيل الملف الذي يحتوي على قائمة الثغرات الأمنية في البرامج إلى الجهاز الذي تستخدمه في تلك اللحظة.

لتصدير قائمة الثغرات الأمنية في البرامج المكتشفة على الجهاز المُدار المحدد إلى ملف نصي:

1. افتح قائمة الثغرات الأمنية في البرامج المكتشفة على الجهاز المُدار المحدد.

2. حدد الثغرات الأمنية في البرامج التي ترغب في تصديرها.

يمكن تخطي هذه الخطوة إذا كنت ترغب في تصدير قائمة كاملة من الثغرات الأمنية في البرامج المكتشفة على الجهاز المُدار.

إذا كنت ترغب في تصدير قائمة كاملة بالثغرات الأمنية في البرامج المكتشفة على الجهاز المُدار، لن يتم تصدير إلا الثغرات الأمنية المعروضة على الصفحة الحالية.

3. انقر على زر **Export to TXT** أو **Export to CSV**، حسب التنسيق الذي تفضله للتصدير.

يتم تنزيل الملف الذي يحتوي على قائمة الثغرات الأمنية في البرامج التي تم اكتشافها على الجهاز المُدار المحدد إلى الجهاز الذي تستخدمه في تلك اللحظة.

تجاهل الثغرات الأمنية في البرامج

يمكنك تجاهل إصلاح الثغرات الأمنية بالبرامج. قد تكون أسباب تجاهل الثغرات الأمنية للبرامج، على سبيل المثال، ما يلي:

- لا تعتبر ثغرة أمنية في البرنامج مشكلة حرجة لمؤسستك.
- تدرك أن إصلاح الثغرات الأمنية بالبرامج يمكن أن يتلف البيانات المتعلقة بالبرامج التي تطلبت إصلاح الثغرات الأمنية.
- تتأكد من أن الثغرة الأمنية بالبرنامج ليست خطيرة على شبكة مؤسستك لأنك تستخدم تدابير أخرى لحماية أجهزتك المُدارة.

يمكنك تجاهل ثغرة أمنية في البرامج على جميع الأجهزة المُدارة أو على الأجهزة المدارة المحددة فقط.

لتجاهل ثغرة أمنية في البرامج على جميع الأجهزة المُدارة:

1. في القائمة الرئيسية ، انتقل إلى **Software vulnerabilities** ← **Patch management** ← **Operations**.

تعرض الصفحة قائمة الثغرات الأمنية في البرامج التي تم اكتشافها على الأجهزة المُدارة.

2. في قائمة الثغرات الأمنية في البرامج، انقر على رابط اسم الثغرة الأمنية في البرنامج التي ترغب في تجاهلها.

ستفتح نافذة خصائص الثغرة الأمنية في البرنامج.

3. في تبويب **General**، قم بتفعيل خيار **Ignore vulnerability**.

4. انقر على زر **Save**.

ستغلق نافذة خصائص الثغرات الأمنية بالبرامج.

يتم تجاهل الثغرات الأمنية بالبرامج على جميع الأجهزة المُدارة.

لتجاهل ثغرة أمنية في البرامج على الجهاز المُدار المحدد:

1. في القائمة الرئيسية، انتقل إلى **Managed devices** ← **Assets (Devices)**.

يتم عرض قائمة الأجهزة المُدارة.

2. في قائمة الأجهزة المُدارة، انقر على رابط اسم الجهاز الذي ترغب في تجاهل ثغرة أمنية في برنامج مكتشفة عليه.

ستفتح نافذة خصائص الجهاز.

3. في نافذة خصائص الجهاز، حدد تبويب **Advanced**.

4. في الجزء الأيمن، حدد القسم **Software vulnerabilities**.

سيتم عرض قائمة الثغرات الأمنية في البرامج المكتشفة على الجهاز.

5. في قائمة الثغرات الأمنية في البرامج، حدد الثغرة الأمنية التي ترغب في تجاهلها على الجهاز المحدد.

ستفتح نافذة خصائص الثغرة الأمنية في البرنامج.

6. في نافذة خصائص الثغرة الأمنية في البرنامج، في تبويب **General**، قم بتفعيل خيار **Ignore vulnerability**.

7. انقر على زر **Save**.

ستغلق نافذة خصائص الثغرات الأمنية بالبرامج.

8. أغلق نافذة خصائص الجهاز.

يتم تجاهل الثغرات الأمنية بالبرامج على الجهاز المُحدَّد.

لن يتم إصلاح الثغرات الأمنية للبرامج التي تم تجاهلها بعد الانتهاء من المهمة إصلاح الثغرات الأمنية أو المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. يمكنك استثناء الثغرات الأمنية للبرامج التي تم تجاهلها من قائمة الثغرات الأمنية باستخدام عامل تصفية.

إدارة التطبيقات المشغلة على أجهزة العميل

يصف هذا القسم مزايا Kaspersky Security Center المتعلقة بإدارة التطبيقات التي تعمل على أجهزة العميل.

استخدام التحكم في التطبيقات لإدارة الملفات القابلة للتنفيذ

يمكنك استخدام مكون التحكم في التطبيق للسماح ببدء تشغيل الملفات القابلة للتنفيذ أو منعه على أجهزة المستخدم. ويدعم مكون التحكم في التطبيقات أنظمة التشغيل المستندة إلى Windows وLinux.

بالنسبة لأنظمة التشغيل المستندة إلى Linux، يتوفر مكون التحكم في التطبيقات بدءًا من Kaspersky Endpoint Security 11.2 لنظام Linux.
ويتوفر المكون لتطبيق Kaspersky Embedded Systems Security for Windows 3.0 أو أحدث.

المتطلبات الأساسية

- يتم نشر Kaspersky Security Center في مؤسستك.
- تم إنشاء سياسة Kaspersky Endpoint Security for Windows أو Kaspersky Endpoint Security for Linux وهي نشطة.
- تم إنشاء سياسة Kaspersky Embedded Systems Security for Windows أو Kaspersky Embedded Systems Security وهي نشطة.

المراحل

يسير سيناريو استخدام التحكم في التطبيقات في مراحل:

1. **تشكيل قائمة الملفات التنفيذية على أجهزة العميل وعرضها**

تساعدك هذه المرحلة في معرفة الملفات التنفيذية الموجودة على الأجهزة المُدارة. اعرض قائمة الملفات التنفيذية وقارنها بقوائم الملفات التنفيذية المسموح بها والمحظورة. يمكن أن تكون القيود المفروضة على استخدام الملفات التنفيذية متعلقة بسياسات أمان المعلومات في مؤسستك.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: مخزون الملفات التنفيذية
- Kaspersky Security Center Web Console: الحصول على قائمة الملفات التنفيذية المخزنة على أجهزة العميل وعرضها

2. **إنشاء فئات للملفات القابلة للتنفيذ المستخدمة في مؤسستك**

قم بتحليل قوائم الملفات التنفيذية المخزنة على الأجهزة المُدارة. استنادًا إلى التحليل، أنشئ فئات للملفات القابلة للتنفيذ. ومن الموصى به إنشاء فئة "تطبيقات العمل" التي تغطي المجموعة القياسية من الملفات القابلة للتنفيذ في مؤسستك. إذا كانت مجموعات الأمان المختلفة تستخدم مجموعاتها الخاصة من الملفات القابلة للتنفيذ في عملها، فيمكن إنشاء فئة منفصلة لكل مجموعة أمان.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا، إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة، إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد.
- Kaspersky Security Center Web Console: إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا، إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة، إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من مجلد محدد.

3. **تكوين التحكم في التطبيق في سياسة Kaspersky Endpoint Security**

قم بتكوين مكون التحكم في التطبيق في سياسة Kaspersky Endpoint Security باستخدام الفئات التي قمت بإنشائها في المرحلة السابقة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: تكوين إدارة بدء تشغيل التطبيق على أجهزة العميل
- Kaspersky Security Center Web Console: تكوين التحكم في التطبيق في سياسة Kaspersky Endpoint Security for Windows

4. **تكوين التحكم في التطبيقات في سياسة تطبيق Kaspersky Embedded Systems Security**

قم بتكوين مكون التحكم في التطبيقات في سياسة Kaspersky Embedded Systems Security for Windows باستخدام الفئات التي أنشأتها. للمزيد من المعلومات عن مكون التحكم في التطبيقات، ارجع إلى تعليمات Kaspersky Embedded Systems Security for Windows أو تعليمات Kaspersky Embedded Systems Security for Linux.

إذا كنت تستخدم عددًا كبيرًا من القواعد، فقد يحدث خطأ عند تحميل السياسة. ويمكنك زيادة الحد الأقصى لحجم الطلب بالبايت باستخدام الأوامر التالية:

- لطلب JSON:

```
s KLLIM -n- "core/.independent." klscflag -fset -pv
t d- <max_request_size> LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v
```

- لطلب HTTP:

```
s KLLIM -n- "core/.independent." klscflag -fset -pv
t d- <max_request_size> LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v
```

حيث `<max_request_size>` هو الحد الأقصى لحجم الطلب بالبايت (على سبيل المثال، `200000000`).

5. **تشغيل مكون التحكم في التطبيقات في وضع الاختبار**

للتأكد من أن قواعد التحكم في التطبيقات لا تحظر الملفات القابلة للتنفيذ المطلوبة لعمل المستخدم، يوصى بتمكين اختبار قواعد التحكم في التطبيقات وتحليل عملها بعد إنشاء قواعد جديدة. وعند تمكين الاختبار، لن يحظر Kaspersky Endpoint Security for Windows أو Kaspersky Embedded Systems Security الملفات التنفيذية التي يحظر بدء تشغيلها بموجب قواعد التحكم في التطبيقات، لكنه بدلاً من ذلك سيرسل إخطارات حول بدء التشغيل إلى خادم الإدارة.

عند اختبار قواعد التحكم في التطبيقات، يُنصح باتخاذ الإجراءات التالية:

- تحديد فترة الاختبار. يمكن أن تتنوع فترة الاختبار من عدة أيام إلى شهرين.
- فحص الأحداث الناتجة عن اختبار عملية التحكم في التطبيقات.

تعليمات إرشادات Kaspersky Security Center Web Console: تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows. اتبع هذه التعليمات وقم بتفعيل خيار **وضع الاختبار** في عملية التكوين.

6 **تغيير إعدادات الفئات لمكون التحكم في التطبيقات**

أجر تغييرات في إعدادات التحكم في التطبيقات عند الضرورة. استنادًا إلى نتائج الاختبار، يمكنك إضافة ملفات قابلة للتنفيذ تتعلق بأحداث مكون التحكم في التطبيق إلى فئة مع إضافة المحتوى يدويًا.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق
- Kaspersky Security Center Web Console: إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق

7 **تطبيق قواعد التحكم في التطبيقات في وضع التشغيل**

بعد اختبار قواعد التحكم في التطبيقات واكتمال تكوين الفئات، يمكنك تطبيق قواعد التحكم في التطبيقات في وضع التشغيل.

تعليمات إرشادات Kaspersky Security Center Web Console: تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security لـ Windows. اتبع هذه التعليمات وقم بتعطيل خيار **وضع الاختبار** في عملية التكوين.

8 **التحقق من تكوين التحكم في التطبيقات**

تأكد من أنك قد قمت بما يلي:

- إنشاء فئات للملفات القابلة للتنفيذ.
- تكوين التحكم في التطبيقات باستخدام الفئات.
- قد طبقت قواعد التحكم في التطبيقات في وضع التشغيل.

النتائج

عند اكتمال السيناريو، يتم التحكم في بدء تشغيل الملفات القابلة للتنفيذ على الأجهزة المُدارة. يمكن للمستخدمين تشغيل الملفات القابلة للتنفيذ المسموح بها في مؤسستك فقط، ولا يمكنهم تشغيل الملفات القابلة للتنفيذ المحظورة في مؤسستك.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent

- تعليمات Kaspersky Embedded Systems Security for Windows
- تعليمات Kaspersky Embedded Systems Security for Linux

أوضاع وفئات التحكم في التطبيق

يراقب مكون التحكم في التطبيقات محاولات المستخدمين لبدء تشغيل الملفات القابلة للتنفيذ. ويمكنك استخدام قواعد التحكم في التطبيقات للتحكم في بدء تشغيل الملفات القابلة للتنفيذ.

يتوفر مكون التحكم في التطبيقات لتطبيق Kaspersky Endpoint Security for Windows و Kaspersky Endpoint Security 11.2 for Linux والإصدارات الأحدث ولأجل Kaspersky Security for Virtualization Light Agent. جميع التعليمات الواردة في هذا القسم تصف تكوين التحكم في التطبيقات لتطبيق Kaspersky Endpoint Security for Windows.

يتم تنظيم بدء تشغيل الملفات القابلة للتنفيذ التي لا تطابق إعداداتها أي من قواعد التحكم في التطبيقات عبر وضع التشغيل المحدد للمكون:

- قائمة الرفض. يُستخدم الوضع إذا كنت تريد السماح ببدء تشغيل جميع الملفات القابلة للتنفيذ باستثناء تلك المحددة في قواعد الحظر. يتم تحديد هذا الوضع بصورة افتراضية.
- قائمة السماح. يُستخدم الوضع إذا كنت تريد حظر بدء تشغيل جميع الملفات القابلة للتنفيذ باستثناء تلك المحددة في قواعد السماح.

يتم تنفيذ قواعد التحكم في التطبيقات من خلال فئات الملفات القابلة للتنفيذ. يوجد في Kaspersky Security Center ثلاثة أنواع من الفئات:

- الفئة المضاف إليها المحتوى يدويًا. أنت تضع الشروط، مثل بيانات تعريف الملف وكود التجزئة للملف وشهادة الملف وفئة KL ومسار الملف كي تشمل الملفات التنفيذية في الفئة.
- الفئة التي تتضمن ملفات تنفيذية من أجهزة محددة. أنت تحدد جهازًا يتم تضمين الملفات التنفيذية الخاصة به تلقائيًا في الفئة.
- الفئة التي تتضمن ملفات تنفيذية من مجلد محدد. أنت تحدد مجلدًا يتم منه تضمين الملفات التنفيذية في الفئة المحددة تلقائيًا.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent
- تعليمات Kaspersky Embedded Systems Security for Windows
- تعليمات Kaspersky Embedded Systems Security for Linux

الحصول على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل وعرضها

يمكنك الحصول على قائمة الملفات التنفيذية المخزنة على أجهزة العميل بإحدى الطرق التالية:

- تمكين الإخطارات عن بدء التشغيل في سياسة Kaspersky Endpoint Security.
- إنشاء مهمة جرد.

تمكين الإخطارات عن بدء التشغيل في سياسة Kaspersky Endpoint Security

لتمكين الإخطارات حول بدء تشغيل التطبيقات:

1. افتح إعدادات سياسة Kaspersky Endpoint Security، وانتقل إلى **General settings** ← **Reports and Storage**.

2. في مجموعة الإعدادات **Data transfer to Administration Server**، حدد خانة الاختيار **About started applications**، واحفظ التغييرات.

عندما يحاول المستخدم بدء ملفات تنفيذية، تتم إضافة معلومات عن هذه الملفات إلى قائمة الملفات التنفيذية على جهاز عميل. ويرسل Kaspersky Endpoint Security هذه المعلومات إلى عميل الشبكة، ثم يرسلها عميل الشبكة إلى خادم الإدارة.

إنشاء مهمة جرد

ميزة جرد الملفات القابلة للتنفيذ متاحة للتطبيقات التالية:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux version 11.2 وأحدث
- Kaspersky Security for Virtualization 4.0 Light Agent والإصدارات الأحدث

يمكنك تقليل الحمل على قاعدة البيانات أثناء الحصول على معلومات عن التطبيقات المثبتة. لتوفير مساحة قاعدة البيانات، قم بتشغيل مهمة جرد على الأجهزة المرجعية التي تم تثبيت مجموعة قياسية من البرامج عليها. والعدد المفضل للأجهزة هو 3-1.

نوصي بشدة بعدم تشغيل مهمة الجرد عند استخدام قواعد البيانات التالية: MySQL وPostgreSQL وSQL Server Express Edition وMariaDB (جميع الإصدارات).

لإنشاء مهمة مخزون للملفات التنفيذية على الأجهزة العميلة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

يتم عرض قائمة المهام.

2. انقر على الزر **Add**.

سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. في صفحة **New task settings** في قائمة **Application** المنسدلة ، حدد Kaspersky Endpoint Security لنظام التشغيل Windows أو Kaspersky Endpoint Security لنظام التشغيل Linux، بناءً على نوع نظام التشغيل لأجهزة العميل.

4. من القائمة المنسدلة **Task type**، حدد **Inventory**.

5. في صفحة " **Finish task creation**، انقر على زر **Finish**.

بعد انتهاء معالج المهمة الجديدة، يتم إنشاء مهمة **Inventory** وتكوينها. يمكنك إذا كنت ترغب أن تقوم بتغيير إعدادات المهمة التي تم إنشاؤها. يتم عرض المهمة التيتم إنشاؤها في قائمة المهام.

للحصول على وصف تفصيلي لمهمة الجرد، راجع المساعدة التالية:

- تعليمات Kaspersky Endpoint Security for Windows
- دعم Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

بعد إجراء مهمة **Inventory**، يتم تشكيل قائمة الملفات التنفيذية المخزنة على الأجهزة المُدارة، ويمكنك عرض القائمة.

أثناء عملية الجرد، يمكن اكتشاف الملفات التنفيذية بالتنسيقات التالية (اعتمادًا على الخيار الذي تحدده في خصائص مهمة الجرد): MZ وCOM وPE وNE وSYS وCMD وBAT وPS1 وJS وVBS وREG وMSI وCPL وDLL وJAR وHTML.

عرض قائمة الملفات التنفيذية المخزنة على الأجهزة المُدارة

لعرض قائمة الملفات التنفيذية المخزنة على أجهزة العميل:

في القائمة الرئيسية، انتقل إلى **Executable files** ← **Third-party applications** ← **Operations**.

تعرض الصفحة قائمة الملفات التنفيذية المخزنة على أجهزة العميل.

إذا لزم الأمر ، يمكنك إرسال الملف التنفيذي للجهاز المدار إلى الجهاز حيث يتم فتح Kaspersky Security Center Web Console.

لإرسال ملف تنفيذي:

1. في القائمة الرئيسية، انتقل إلى **Executable files** ← **Third-party applications** ← **Operations**.
2. انقر على رابط الملف التنفيذي الذي تريد إرساله.
3. في النافذة التي تفتح، انتقل إلى القسم **Devices**، ثم حدد خانة الاختيار الخاصة بالجهاز المُدار الذي تريد إرسال الملف القابل للتنفيذ منه.

قبل إرسال الملف التنفيذي تأكد من أن الجهاز المُدار لديه اتصال مباشر بخادم الإدارة، عن طريق تحديد خانة الاختيار **Do not disconnect from the Administration Server**.

4. انقر على الزر **Send**.

يتم تنزيل الملف التنفيذي المحدد لإرساله لاحقًا إلى الجهاز حيث يتم فتح Kaspersky Security Center Web Console.

إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا

يمكنك تحديد مجموعة من المعايير كقالب للملفات التنفيذية التي ترغب في السماح ببدئها أو حظرها في مؤسستك. على أساس الملفات التنفيذية التي تستوفي المعايير، يمكنك إنشاء فئة تطبيق واستخدامها في تكوين مكون التحكم في التطبيقات.

لإنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا:

1. في القائمة الرئيسية، انتقل إلى **Application categories** ← **Third-party applications** ← **Operations**.

يتم عرض صفحة بقائمة فئات التطبيقات.

2. انقر على الزر **Add**.

يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج باستخدام زر **Next**.

3. في صفحة **Select category creation method**، حدد خيار **Category with content added manually. Data of executable files is manually added to the category**.

4. في خطوة **Conditions**، انقر على الزر **Add** لإضافة معيار شرط لإدراج الملفات في فئة الإنشاء.

5. في خطوة **Condition criteria**، حدد نوع قاعدة لإنشاء فئة من القائمة:

- **From KL category**

إذا تم تحديد هذا الخيار، يمكنك تحديد فئة تطبيق Kaspersky كشرط لإضافة تطبيقات إلى فئة المستخدم. ستتم إضافة التطبيقات من فئة Kaspersky المحددة إلى فئة تطبيقات المستخدم.

- **Select certificate from repository**

إذا تم تحديد هذا الخيار، فيمكنك تحديد الشهادات من المستودع. يتطابق شرط الفئة فقط مع الملفات التنفيذية الموقعة بواسطة الشهادة المحددة.

يتم إضافة الشهادات إلى المستودع إذا أنشأت مهمة جرد وبدأتها أو حددت خانة الاختيار **عن التطبيقات التي تم بدء تشغيلها** في سياسة Kaspersky Endpoint Security. ويمكنك تنفيذ كلا الإجراءين.

لا يمكن استخراج المعلومات عن الشهادات إلا من الملفات القابلة للتنفيذ بتنسيق PE (.exe، .dll، .sys).

- **Specify path to application (masks supported)**

إذا تم تحديد هذا الخيار، فيمكنك تحديد المسار المؤدي إلى الملف أو المجلد الموجود على الجهاز العميل الذي يحتوي على الملفات التنفيذية المراد إضافتها إلى فئة تطبيقات المستخدم. يمكنك استخدام التعبيرات العادية مثل C:\path_to_exe*، على سبيل المثال: C:\Program Files\Internet\Explorer*.

- **Removable drive**

إذا تم تحديد هذا الخيار، يمكنك تحديد نوع الوسيط (أي جهاز أو جهاز قابل للإزالة) الذي يعمل عليه التطبيق. تتم إضافة التطبيقات التي تم تشغيلها على نوع محرك الأقراص المحدد إلى فئة تطبيقات المستخدم.

- **Hash, metadata, or certificate:**

  - **Select from list of executable files**

إذا تم تحديد هذا الخيار، فيمكنك استخدام قائمة الملفات التنفيذية على الجهاز العميل لتحديد التطبيقات وإضافتها إلى الفئة.

  - **Select from applications registry**

في حال تحديد هذا الخيار، يتم عرض سجل التطبيقات. بعد تحديد تطبيق من السجل، تفتح النافذة مع المعلمات المملوءة بالبيانات الوصفية من التطبيق الذي حددته:

- اسم الملف.
- نسخة الملف. يمكنك تحديد قيمة دقيقة للإصدار أو وصف شرط. على سبيل المثال: "أكبر من 5.0".
- اسم التطبيق.
- إصدار التطبيق يمكنك تحديد قيمة دقيقة للإصدار أو وصف شرط. على سبيل المثال: "أكبر من 5.0".
- البائع.

لاحظ أنه يتم حظر تشغيل الملفات التنفيذية التي تلبي المعلمات المحددة فقط، وليس تشغيل التطبيق الذي تحدده. إذا كانت بيانات التعريف الخاصة بالتطبيق المحدد تتطابق مع بيانات التعريف الخاصة بالملف التنفيذي الذي يتم تشغيله عند تشغيل التطبيق، فيمكنك المتابعة إلى الخطوة التالية. وإلا، فيجب عليك تغيير القيم يدويًا لتتوافق مع بيانات التعريف للملف التنفيذي.

- **Specify manually**

إذا تم تحديد هذا الخيار، يجب عليك تحديد تجزئة الملف أو بيانات تعريفه أو شهادته كشرط لإضافة تطبيقات إلى فئة المستخدم.

File Hash

بناءً على رقم إصدار تطبيق الأمان المثبت على الأجهزة الموجودة على شبكتك، يجب عليك تحديد خوارزمية لحساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في هذه الفئة. يتم تخزين المعلومات عن قيم التجزئة المحسوبة بواسطة وظائف التجزئة في قاعدة بيانات خادم الإدارة.

SHA256 هي وظيفة تجزئة التشفير: لم يتم العثور على ثغرات أمنية في الخوارزميات الخاصة بها، فهي تعتبر وظيفة التشفير الأكثر موثوقية في الوقت الحاضر. يدعم Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث حساب SHA256. حساب وظيفة تجزئة MD5 مدعوم من جميع الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

حدد أيًا من خيارات حساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في الفئة:

- إذا كانت جميع مثيلات تطبيقات الأمان المثبتة على شبكتك هي Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows أو الإصدارات الأحدث، فحدد خانة الاختيار **SHA256** . لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA256 لملف تنفيذي للإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows. قد يتسبب ذلك في حدوث عمليات فشل في تشغيل تطبيق الأمان. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير MD5 لملفات الفئة.

- إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows على شبكتك، فحدد ملف **MD5 hash**. لا يمكنك إضافة فئة تم إنشاؤها بناءً على معيار مجموع تجزئة MD5 لملف تنفيذي لـ Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو الإصدارات الأحدث. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير SHA256 لملفات الفئة.

- إذا كانت الأجهزة المختلفة الموجودة على شبكتك تستخدم كلاً من الإصدارات السابقة والإصدارات الأحدث من Kaspersky Endpoint Security 10، فحدد خانة الاختيار **SHA256** وخانة اختيار **MD5 hash**.

Metadata

في حال تحديد هذا الخيار، يمكنك تحديد بيانات تعريف الملف مثل اسم الملف وإصدار الملف والبائع. يتطابق شرط الفئة فقط مع الملفات التنفيذية التي تحتوي على نفس بيانات التعريف.

Certificate

إذا تم تحديد هذا الخيار، فيمكنك تحديد الشهادات من المستودع. يتطابق شرط الفئة فقط مع الملفات التنفيذية الموقعة بواسطة الشهادة المحددة.

يتم إضافة الشهادات إلى المستودع إذا أنشأت مهمة جرد وبدأتها أو حددت خانة الاختيار **عن التطبيقات التي تم بدء تشغيلها** في سياسة Kaspersky Endpoint Security. ويمكنك تنفيذ كلا الإجراءين.

- **From file or from MSI package/archived folder**

إذا تم تحديد هذا الخيار، يمكنك تحديد ملف مثبّت MSI كشرط لإضافة تطبيقات إلى فئة المستخدم. وسيتم إرسال البيانات الوصفية لمثبّت التطبيق إلى خادم الإدارة. تتم إضافة التطبيقات التي تشبه فيها البيانات الوصفية للمثبت مثبت MSI المحدد إلى فئة تطبيقات المستخدم.

يتم إضافة المعيار المحدد إلى قائمة الشروط.

يمكنك إضافة أي عدد من المعايير لإنشاء فئة التطبيق كما تحتاج.

6. في خطوة **Exclusions** ، انقر على الزر **Add** لإضافة معيار شرط حصري لاستثناء الملفات من الفئة التي تم إنشاؤها.

7. في خطوة **Condition criteria**، حدد نوع قاعدة من القائمة بنفس الطريقة التي حددت بها نوع قاعدة لإنشاء الفئة.

بعد انتهاء المعالج، يتم إنشاء فئة تطبيق مخصصة. يتم عرضه في قائمة فئات التطبيق. يمكنك استخدام فئة التطبيق التي تم إنشاؤها عند تكوين التحكم في التطبيقات.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent
- تعليمات Kaspersky Embedded Systems Security for Windows
- تعلميات Kaspersky Embedded Systems Security for Linux

إنشاء فئة تطبيق تتضمن ملفات قابلة للتنفيذ من أجهزة محددة

يمكنك استخدام الملفات التنفيذية من الأجهزة المحددة كقوالب للملفات التنفيذية التي ترغب في السماح لها أو حظرها. على أساس الملفات القابلة للتنفيذ من الأجهزة المحددة، يمكنك إنشاء فئة واستخدامها في تكوين مكون التحكم في التطبيقات.

لاسترداد قائمة الملفات التنفيذية من الأجهزة:

1. تأكد من إنشاء سياسة Kaspersky Endpoint Security for Windows أو Kaspersky Endpoint Security for Linux وأنها نشطة. قم بتمكين مكون التحكم في التطبيقات في السياسة.
2. احصل على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل

لإنشاء فئة تتضمن ملفات قابلة للتنفيذ من أجهزة محددة:

1. في القائمة الرئيسية، انتقل إلى **Application categories** ← **Third-party applications** ← **Operations**.

   يتم عرض صفحة بقائمة الفئات.
2. انقر على الزر **Add**.

   يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.
3. في خطوة **Select category creation method**، حدد اسم الفئة وحدد الخيار **Category that includes executable files from selected devices. These executable files are processed automatically and their metrics are added to the category**.
4. انقر على **Add**.
5. في النافذة التي تفتح، حدد جهازًا أو أجهزة سيتم استخدام ملفاتها القابلة للتنفيذ في إنشاء الفئة.
6. حدد الإعدادات التالية:

   - **خوارزمية الحساب لقيمة التجزئة**

     بناءً على رقم إصدار تطبيق الأمان المثبت على الأجهزة الموجودة على شبكتك، يجب عليك تحديد خوارزمية لحساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في هذه الفئة. يتم تخزين المعلومات عن قيم التجزئة المحسوبة بواسطة وظائف التجزئة في قاعدة بيانات خادم الإدارة.

     SHA256 هي وظيفة تجزئة التشفير: لم يتم العثور على ثغرات أمنية في الخوارزميات الخاصة بها، فهي تعتبر وظيفة التشفير الأكثر موثوقية في الوقت الحاضر. يدعم Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث حساب SHA256. حساب وظيفة تجزئة MD5 مدعوم من جميع الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

حدد أيًا من خيارات حساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في الفئة:

- إذا كانت جميع مثيلات تطبيقات الأمان المثبتة على شبكتك هي Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows أو الإصدارات الأحدث، فحدد خانة الاختيار **SHA256** . لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA256 لملف تنفيذي للإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows. قد يتسبب ذلك في حدوث عمليات فشل في تشغيل تطبيق الأمان. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير MD5 لملفات الفئة.

- إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows على شبكتك، فحدد ملف **MD5 hash**. لا يمكنك إضافة فئة تم إنشاؤها بناءً على معيار مجموع تجزئة MD5 لملف تنفيذي لـ Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو الإصدارات الأحدث. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير SHA256 لملفات الفئة.

إذا كانت الأجهزة المختلفة الموجودة على شبكتك تستخدم كلاً من الإصدارات السابقة والإصدارات الأحدث من Kaspersky Endpoint Security 10، فحدد خانة الاختيار **SHA256** وخانة اختيار **MD5 hash**.

يتم تحديد خانة الاختيار **حساب SHA256 للملفات في هذه الفئة (المدعومة من Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو أي إصدارات أحدث)** بشكل افتراضي.

يتم إلغاء تحديد خانة الاختيار **حساب MD5 للملفات في هذه الفئة (المدعومة بواسطة الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** بشكل افتراضي.

- **Synchronize data with Administration Server repository**

حدد هذا الخيار إذا كنت ترغب في أن يقوم خادم الإدارة بالتحقق من التغييرات في المجلد المحدد (المجلدات المحددة) كل فترة.

يتم تعطيل هذا الخيار افتراضيًا.

إذا قمت بتفعيل هذا الخيار، حدد الفترة (بالساعات) للتحقق من التغييرات في المجلد المحدد (المجلدات المحددة). بشكل افتراضي، الفاصل الزمني للفحص هو 24 ساعة.

- **File type**

يمكنك في هذا القسم تحديد نوع الملف المستخدم في إنشاء فئة التطبيق.

All files. يتم أخذ جميع الملفات في الاعتبار عند إنشاء الفئة. يتم تحديد هذا الخيار افتراضيًا.

Only files outside the application categories. لا يتم الأخذ في الاعتبار عند إنشاء الفئة إلا الملفات خارج فئات التطبيقات.

- **Folders**

يمكنك في هذا القسم تحديد المجلدات من الجهاز المحدد (الأجهزة المحددة) التي تحتوي على ملفات مستخدمة لإنشاء فئة التطبيق.

All folders. يتم أخذ جميع المجلدات في الاعتبار لإنشاء الفئة. يتم تحديد هذا الخيار افتراضيًا.

Specified folder. لا يتم أخذ في الاعتبار لإنشاء الفئة إلا المجلد المحدد. في حالة تحديدك لهذا الخيار، يجب أن تحدد المسار الخاص بالمجلد.

عند انتهاء المعالج، يتم إنشاء فئة للملفات القابلة للتنفيذ. ويتم عرضه في قائمة الفئات. ويمكنك استخدام الفئة التي تم إنشاؤها عند تكوين التحكم في التطبيقات.

إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد

يمكنك استخدام الملفات التنفيذية من مجلد محدد كمقياس للملفات التنفيذية التي ترغب في السماح لها أو حظرها في مؤسستك. على أساس الملفات التنفيذية من المجلد المحدد، يمكنك إنشاء فئة تطبيق واستخدامها في تكوين مكون التحكم في التطبيقات.

لإنشاء فئة تتضمن ملفات قابلة للتنفيذ من المجلد المحدد:

1. في القائمة الرئيسية، انتقل إلى **Application categories** ← **Third-party applications** ← **Operations**.

   يتم عرض صفحة بقائمة الفئات.

2. انقر على الزر **Add**.

   يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. في خطوة **Select category creation method**، حدد اسم الفئة وحدد الخيار **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**.

4. حدد المجلد الذي سيتم استخدام الملفات القابلة للتنفيذ الموجودة فيه لإنشاء الفئة.

5. حدد الإعدادات التالية:

- **Include dynamic-link libraries (DLL) in this category**

تشمل فئة التطبيق مكتبات الروابط الديناميكية (ملفات بتنسيق DLL)، ويسجّل مكون التحكم في التطبيقات الإجراءات التي تقوم هذه المكتبات بتشغيلها في النظام. قد يؤدي تضمين ملفات DLL في الفئة إلى خفض أداء Kaspersky Security Center.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **Include script data in this category**

تشمل فئة التطبيق البيانات الموجودة على البرامج النصية ولا يتم حظر البرامج النصية بواسطة "الحماية من تهديدات الويب". قد يؤدي تضمين بيانات البرنامج النصي في الفئة إلى خفض أداء Kaspersky Security Center.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **خوارزمية حساب قيمة التجزئة: 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)**

بناءً على رقم إصدار تطبيق الأمان المثبت على الأجهزة الموجودة على شبكتك، يجب عليك تحديد خوارزمية لحساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في هذه الفئة. يتم تخزين المعلومات عن قيم التجزئة المحسوبة بواسطة وظائف التجزئة في قاعدة بيانات خادم الإدارة.

SHA256 هي وظيفة تجزئة التشفير: لم يتم العثور على ثغرات أمنية في الخوارزميات الخاصة بها، فهي تعتبر وظيفة التشفير الأكثر موثوقية في الوقت الحاضر. يدعم Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث حساب SHA256. حساب وظيفة تجزئة MD5 مدعوم من جميع الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

حدد أيًا من خيارات حساب قيمة التجزئة بواسطة Kaspersky Security Center للملفات الموجودة في الفئة:

- إذا كانت جميع مثيلات تطبيقات الأمان المثبتة على شبكتك هي Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows أو الإصدارات الأحدث، فحدد خانة الاختيار **SHA256** . لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA256 لملف تنفيذي للإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows. قد يتسبب ذلك في حدوث عمليات فشل في تشغيل تطبيق الأمان. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير MD5 لملفات الفئة.

- إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 لنظام التشغيل Windows على شبكتك، فحدد ملف **MD5 hash**. لا يمكنك إضافة فئة تم إنشاؤها بناءً على معيار مجموع تجزئة MD5 لملف تنفيذي لـ Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو الإصدارات الأحدث. في هذه الحالة، يمكنك استخدام وظيفة تجزئة التشفير SHA256 لملفات الفئة.

إذا كانت الأجهزة المختلفة الموجودة على شبكتك تستخدم كلاً من الإصدارات السابقة والإصدارات الأحدث من Kaspersky Endpoint Security 10، فحدد خانة الاختيار **SHA256** وخانة اختيار **MD5 hash**.

يتم تحديد خانة الاختيار **حساب SHA256 للملفات في هذه الفئة (المدعومة من Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو أي إصدارات أحدث)** بشكل افتراضي.

يتم إلغاء تحديد خانة الاختيار **حساب MD5 للملفات في هذه الفئة (المدعومة بواسطة الإصدارات الأقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** بشكل افتراضي.

- **Force folder scan for changes**

إذا تم تمكين هذا الخيار، فسيبحث التطبيق بشكل منتظم عن مجلد إضافة محتوى الفئة لإجراء التغييرات. يمكنك تحديد تكرار الفحوصات (بالساعات) في حقل الإدخال بجوار خانة الاختيار. وبشكل افتراضي، يكون الفاصل الزمني بين الفحوصات الإجبارية هو 24 ساعة.

إذا تم تعطيل هذا الخيار، فلن يفرض التطبيق أي تحققات من المجلد. يحاول الخادم الوصول إلى الملفات إذا تم تعديلها أو إضافتها أو حذفها.

يتم تعطيل هذا الخيار افتراضيًا.

عند انتهاء المعالج، يتم إنشاء فئة الملفات القابلة للتنفيذ. ويتم عرضه في قائمة الفئات. ويمكنك استخدام الفئة في تكوين التحكم في التطبيقات.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent
- تعليمات Kaspersky Embedded Systems Security for Windows
- تعلميات Kaspersky Embedded Systems Security for Linux

عرض قائمة فئات التطبيق

يمكنك عرض قائمة الفئات التي تم تكويتها للملفات القابلة للتنفيذ وإعدادات كل فئة.

لعرض قائمة فئات التطبيقات،

في القائمة الرئيسية، انتقل إلى **Application categories** ← **Third-party applications** ← **Operations**.

يتم عرض صفحة بقائمة الفئات.

لعرض خصائص فئة تطبيق،

انقر على اسم الفئة.

يتم عرض نافذة خصائص الفئة. يتم تجميع الخصائص في عدة علامات تبويب.

إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق

بعد أن تقوم بتكوين التحكم في التطبيقات في سياسات Kaspersky Endpoint Security for Windows، سيتم عرض الأحداث التالية في قائمة الأحداث:

- **تم حظر بدء التطبيق** (حدث حرج). يتم عرض هذا الحدث إذا قمت بتكوين التحكم في التطبيقات لتطبيق القواعد.
- **تم حظر بدء التطبيق في وضع الاختبار**(حدث معلومات). يتم عرض هذا الحدث إذا قمت بتكوين التحكم في التطبيقات لاختبار القواعد.
- **رسالة إلى المسؤول عن حظر بدء تشغيل التطبيق** (حدث تحذير). يتم عرض هذا الحدث إذا قمت بتكوين التحكم في التطبيقات لتطبيق القواعد وطلب مستخدم الوصول إلى التطبيق المحظور بدء تشغيله.

يُنصح بإنشاء تحديدات الحدث لعرض الأحداث المتعلقة بعمل التحكم في التطبيقات.

يمكنك إضافة ملفات تنفيذية متعلقة بأحداث التحكم في التطبيقات إلى فئة تطبيق موجودة أو إلى فئة تطبيق جديدة. لا يمكنك إضافة الملفات التنفيذية إلا إلى فئة تطبيق مضاف إليها المحتوى يدويًا.

لإضافة ملفات تنفيذية ذات صلة بأحداث التحكم في التطبيقات إلى فئة تطبيق:

1. في القائمة الرئيسية، انتقل إلى **Event selections** ← **Monitoring & reporting**.
   يتم عرض قائمة تحديدات الأحداث.
2. حدد تحديد الحدث لعرض الأحداث المتعلقة بالتحكم في التطبيقات وبدء تحديد الحدث هذا.

إذا لم تقم بإنشاء تحديد الحدث المتعلق بالتحكم في التطبيقات، يمكنك اختيار تحديد محدد مسبقًا وبدئه، مثل **الأحداث الأخيرة**.

يتم عرض قائمة الأحداث.

3. حدد الأحداث التي ترغب في إضافة الملفات التنفيذية المرتبطة بها إلى فئة التطبيق، ثم انقر على زر **Assign to category**.

يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

4. في صفحة المعالج، حدد الإعدادات ذات الصلة:

- في الصفحة **Action on executable file related to the event**، حدد أحد الخيارات التالية:

  - **Add to a new application category**

  حدد هذا الخيار إذا كنت ترغب في إنشاء فئة تطبيق جديدة بناءً على الملفات التنفيذية ذات الصلة بالحدث.

  يتم تحديد هذا الخيار افتراضيًا.

  إذا كنت قد حددت هذا الخيار، حدد اسم فئة جديدة.

  - **Add to an existing application category**

  حدد هذا الخيار إذا كنت ترغب في إضافة ملفات تنفيذية متعلقة بالحدث إلى فئة تطبيق موجودة.

  لا يتم تحديد هذا الخيار افتراضيًا.

  إذا كنت قد حددت هذا الخيار، حدد فئة التطبيق المضاف إليها المحتوى يدويًا الت ترغب في إضافة ملفات تنفيذية إليها.

- في قسم **Rule type**، حدد أحد الخيارات التالية:

  - **Rules for adding to inclusions**

  - **Rules for adding to exclusions**

- في قسم **Parameter used as a condition**، حدد أحد الخيارات التالية:

  - **Certificate details (or SHA256 hashes for files without a certificate)**

  قد يتم توقيع الملفات باستخدام شهادة. قد يتم توقيع ملفات متعددة باستخدام الشهادة ذاتها. على سبيل المثال، قد يتم توقيع الإصدارات المختلفة للتطبيق ذاته باستخدام الشهادة ذاتها أو العديد من التطبيقات المختلفة من البائع ذاته باستخدام الشهادة ذاتها. عند تحديد شهادة ما، قد تنتهي العديد من إصدارات تطبيق ما أو تطبيقات مختلفة من البائع ذاته إلى الفئة.

  كل ملف لديه وظيفة تجزئة SHA256 فريدة خاصة به. عندما تحديد وظيفة تجزئة SHA256 ، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة.

  حدد هذا الخيار إذا كنت ترغب بإضافة تفاصيل الشهادة الخاصة بملف تنفيذي إلى قواعد الفئة (أو وظيفة تجزئة SHA256 للملفات بدون شهادة).

  يتم تحديد هذا الخيار افتراضيًا.

  - **Certificate details (files without a certificate will be skipped)**

  قد يتم توقيع الملفات باستخدام شهادة. قد يتم توقيع ملفات متعددة باستخدام الشهادة ذاتها. على سبيل المثال، قد يتم توقيع الإصدارات المختلفة للتطبيق ذاته باستخدام الشهادة ذاتها أو العديد من التطبيقات المختلفة من البائع ذاته باستخدام الشهادة ذاتها. عند تحديد شهادة ما، قد تنتهي العديد من إصدارات تطبيق ما أو تطبيقات مختلفة من البائع ذاته إلى الفئة.

  حدد هذا الخيار إذا كنت ترغب بإضافة تفاصيل الشهادة الخاصة بملف تنفيذي لقواعد الفئة. إن لم يكن الملف التنفيذي يحتوي على شهادة، فسيتم تخطي هذا الملف. لم يتم إضافة معلومات حول هذا الملف إلى الفئة.

  - **Only SHA256 (files without a hash will be skipped)**

  كل ملف لديه وظيفة تجزئة SHA256 فريدة خاصة به. عندما تحديد وظيفة تجزئة SHA256 ، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة.

  حدد هذا الخيار إذا كنت ترغب بإضافة فقط تفاصيل وظيفة تجزئة SHA256 الخاصة بالملف التنفيذي.

- **Only MD5 (discontinued mode, only for Kaspersky Endpoint Security 10 Service Pack 1 version)**

  كل ملف لديه وظيفة تجزئة MD5 فريدة خاصة به. عندما تحديد وظيفة تجزئة MD5 ، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة.

  حدد هذا الخيار إذا كنت ترغب بإضافة فقط تفاصيل وظيفة تجزئة MD5 الخاصة بالملف التنفيذي. حساب وظيفة تجزئة MD5 مدعومة من Kaspersky Endpoint Security 10 Service Pack 1 for Windows وكل الإصدارات الأقدم.

5. انقر على **OK**.

عند انتهاء المعالج، يتم إضافة الملفات التنفيذية المتعلقة بأحداث التحكم في التطبيقات إلى فئة التطبيق الموجودة أو إلى فئة تطبيق جديدة. يمكنك عرض إعدادات فئة التطبيق التي قد عدلتها أو أنشأتها.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent
- تعليمات Kaspersky Embedded Systems Security for Windows
- تعليمات Kaspersky Embedded Systems Security for Linux

تكوين التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows

بعد إنشاء فئات التحكم في التطبيقات، يمكنك استخدامها في تكوين التحكم في التطبيقات في سياسات Kaspersky Endpoint Security for Windows.

لتكوين التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.

   سيتم عرض صفحة بقائمة السياسات.

2. انقر على سياسة **Kaspersky Endpoint Security for Windows**.

   ستفتح نافذة إعدادات السياسة.

3. انتقل إلى **Application settings** ← **ضوابط الأمن** ← **التحكم في التطبيق**.

   يتم عرض نافذة **التحكم في التطبيقات** التي تتضمن إعدادات التحكم في التطبيقات.

4. يتم تمكين خيار **التحكم في التطبيق** افتراضيًا. تأكد من **تعطيل زر التحكم في التطبيق** إلى وضع التعطيل.

5. في إعدادات حظر **إعدادات التحكم في التطبيق**، قم بتمكين وضع التشغيل لتطبيق قواعد التحكم في التطبيق والسماح لـ Kaspersky Endpoint Security for Windows بحظر بدء تشغيل التطبيقات.

   إذا كنت ترغب في اختبار قواعد التحكم في التطبيق، في قسم **إعدادات التحكم في التطبيق**، قم بتمكين وضع الاختبار. في وضع الاختبار، لا يمنع Kaspersky Endpoint Security for Windows بدء تشغيل التطبيقات، ولكنه يسجل معلومات حول القواعد المشغلة في التقرير. انقر على **عرض التقرير** رابط لعرض هذه المعلومات.

6. يرجى تفعيل الخيار **التحكم في تحميل وحدات DLL** إذا كنت تريد أن يراقب Kaspersky Endpoint Security for Windows تحميل وحدات DLL عند بدء المستخدمين للتطبيقات.

   سيتم حفظ معلومات حول الوحدة النمطية والتطبيق الذي قد حمل الوحدة النمطية إلى تقرير.

لا يراقب Kaspersky Endpoint Security for Windows إلا وحدات DLL ومحركات الأقراص المحملة بعد تحديد خيار **التحكم في تحميل وحدات DLL**. أعد تشغيل الجهاز بعد تحديد خيار **التحكم في تحميل وحدات DLL** إذا كنت ترغب في أن يراقب Kaspersky Endpoint Security for Windows جميع وحدات DLL ومحركات الأقراص، بما في ذلك تلك المحملة قبل بدء تشغيل Kaspersky Endpoint Security for Windows.

7. (اختياري) في **قوالب الرسائل** للحظر، قم بتغيير قالب الرسالة التي يتم عرضها عند حظر عند حظر تطبيق من البدء وقالب رسالة البريد الإلكتروني التي يتم إرسالها إليك.

8. في إعدادات قسم **وضع التحكم في التطبيقات**، حدد وضع **قائمة الرفض** أو **قائمة السماح**.

يتم تحديد وضع **قائمة الرفض** افتراضيًا.

9. انقر على رابط **إعدادات قوائم القواعد**.

ستفتح نافذة **قوائم الرفض وقوائم السماح** كي تتيح لك إضافة فئة تطبيق. يكون تبويب **قائمة الرفض** محددًا إذا كان وضع **قائمة الرفض** محددًا، ويكون تبويب **قائمة السماح** محددًا إذا كان وضع **قائمة السماح** محددًا.

10. في نافذة **قوائم الرفض وقوائم السماح**، انقر على زر **Add**.

يتم فتح نافذة **قاعدة التحكم في التطبيقات**.

11. انقر على الرابط **يُرجى اختيار فئة**.

ستفتح نافذة **فئة التطبيقات**.

12. أضف فئة التطبيق (أو الفئات) التي قد أنشأتها قبل ذلك.

يمكنك تعديل إعدادات فئة تم إنشاؤها بالنقر على زر **تعديل**.

يمكنك إنشاء فئة جديدة بالنقر على زر **إضافة**.

يمكنك حذف فئة من القائمة عن طريق النقر على زر **حذف**.

13. بعد اكتمال قائمة فئات التطبيقات، انقر على زر **OK**.

ستغلق نافذة **فئة التطبيقات**.

14. في نافذة قاعدة **التحكم في التطبيقات**، في قسم **المواضيع وحقوقها**، أنشئ قائمة مستخدمين ومجموعات المستخدمين لتطبيق قاعدة التحكم في التطبيقات.

15. انقر على زر **OK** لحفظ الإعدادات ولإغلاق نافذة **قاعدة التحكم في التطبيقات**.

16. انقر على زر **OK** لحفظ الإعدادات ولإغلاق نافذة **قوائم الرفض وقوائم السماح**.

17. انقر على زر **OK** لحفظ الإعدادات ولإغلاق نافذة **التحكم في التطبيقات**.

18. أغلق النافذة باستخدام إعدادات سياسة Kaspersky Endpoint Security for Windows.

يتم تكوين التحكم في التطبيقات. بعد نشر السياسة إلى أجهزة العميل، يتم إدارة بدء تشغيل الملفات التنفيذية.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent
- تعليمات Kaspersky Embedded Systems Security for Windows
- تعليمات Kaspersky Embedded Systems Security for Linux

الحصول على قائمة بالتطبيقات المثبتة على أجهزة العميل وعرضها

يسجل Kaspersky Security Center مخزون جميع البرامج المثبتة على الأجهزة العميلة المُدارة التي تعمل بنظام Linux و Windows.

يقوم عميل الشبكة بإعداد قائمة بالتطبيقات المثبتة على جهاز، ثم يرسل هذه القائمة إلى خادم الإدارة. يستغرق عميل الشبكة حوالي 15-10 دقيقة لتحديث قائمة التطبيقات.

بالنسبة للأجهزة العميلة المستندة إلى Windows، يتلقى عميل الشبكة معظم المعلومات حول التطبيقات المثبتة من سجل Windows. بالنسبة للأجهزة العميلة المستندة إلى Linux، يوفر مديرو الحزم معلومات حول التطبيقات المثبتة إلى عميل الشبكة.

وفي حالة اكتشاف تطبيق من القسم **سجل التطبيقات** على جهاز Linux، فإن خصائص التطبيق لا تحتوي على معلومات حول الملفات القابلة للتنفيذ ذات الصلة.

لعرض قائمة التطبيقات المثبتة على الأجهزة المُدارة:

1. في القائمة الرئيسية، انتقل إلى **Applications registry** ← **Third-party applications** ← **Operations**.

تعرض الصفحة جدولاً بالتطبيقات المثبتة على الأجهزة المدارة. حدد التطبيق لعرض خصائصه، على سبيل المثال اسم البائع أو رقم الإصدار أو قائمة الملفات التنفيذية أو قائمة الأجهزة المثبت عليها التطبيق أو قائمة تحديثات البرنامج وقائمة الثغرات الأمنية المكتشفة في البرنامج.

2. يمكنك تجميع بيانات الجدول وتصفيتها مع التطبيقات المثبتة على النحو التالي:

- انقر على أيقونة الإعدادات ( ) في الزاوية العلوية اليمنى من الجدول.

في قائمة **Columns settings** التي تم استدعاؤها، حدد الأعمدة المراد عرضها في الجدول. لعرض نوع نظام التشغيل للأجهزة العميلة التي تم تثبيت التطبيق عليها، حدد عمود **Operating system type**.

- انقر على أيقونة عامل التصفية ( ) في الزاوية العلوية اليمنى من الجدول، ثم حدد معيار عامل التصفية وطبقه في القائمة التي تم استدعاؤها.

يتم عرض الجدول التطبيقات المثبتة الذي تم تصفيته.

لعرض قائمة التطبيقات المثبتة على جهاز مُدار محدد،

في القائمة الرئيسية، انتقل إلى**الأجهزة** ← **Applications registry** ← **Advanced** ← **<device name>** ← **Managed devices**. في هذه القائمة يمكنك تصدير قائمة برامج التشغيل المشفرة إلى ملف CSV أو TXT.

للحصول على معلومات مفصلة حول التحكم في التطبيق، راجع موضوعات التعليمات التالية:

- دعم Kaspersky Endpoint Security for Windows عبر الإنترنت
- دعم Kaspersky Endpoint Security for Linux عبر الإنترنت
- Kaspersky Security for Virtualization Light Agent
- تعليمات Kaspersky Embedded Systems Security for Windows
- تعليمات Kaspersky Embedded Systems Security for Linux

إنشاء حزمة تثبيت لتطبيق جهة خارجية من قاعدة بيانات Kaspersky

Kaspersky Security Center Web Console يتيح لك إجراء التثبيت عن بُعد لتطبيقات الجهات الخارجية باستخدام حزم التثبيت. تطبيقات الجهات الخارجية هذه تكون ضمن قاعدة بيانات Kaspersky مخصصة. يتم إنشاء قاعدة البيانات هذه تلقائيًا عند تقوم بتشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة لأول مرة.

لإنشاء حزمة تثبيت لتطبيق جهة خارجية من قاعدة بيانات Kaspersky:

1. في القائمة الرئيسية، انتقل إلى **Installation packages** ← **Deployment & assignment** ← **Discovery & deployment**.
2. انقر على الزر **Add**.
3. في صفحة معالج الحزمة الجديدة التي تفتح، حدد خيار **تحديد تطبيق من قاعدة بيانات Kaspersky لإنشاء حزمة تثبيت** ثم انقر على **Next**.
4. في قائمة التطبيقات التي تفتح، حدد التطبيق ذي الصلة ثم انقر على **Next**.
5. حدد لغة الترجمة ذات الصلة في القائمة المنسدلة ثم انقر على **Next**.

لا يتم عرض هذه الخطوة إلا إذا كان التطبيق يعرض خيارات عدة لغات.

6. إذا طُلب منك الموافقة على اتفاقية ترخيص للتثبيت، في صفحة **End User License Agreement** التي تفتح، انقر على الرابط لقراءة اتفاقية الترخيص على الموقع الإلكتروني للبائع ثم حدد خانة الاختيار **I confirm that I have fully read, understand, and accept the terms and conditions of this End User License Agreement**.
7. في صفحة **Name of the new installation package** التي تفتح، في حقل **Package name**، أدخل اسم حزمة التثبيت ثم انقر على **Next**.

انتظر حتى يتم رفع حزمة التثبيت التي تم إنشاؤها حديثًا إلى خادم الإدارة. عندما يعرض معالج الحزمة الجديدة الرسالة التي تخبرك بنجاح عملية إنشاء الحزمة، انقر على **Finish**.

تظهر حزمة التثبيت التي تم إنشاؤها حديثًا في قائمة حزم التثبيت. يمكنك تحديد هذه الحزمة عند إنشاء مهمة تثبيت التطبيق عن بُعد

عرض وتعديل إعدادات حزمة تثبيت لتطبيق جهة خارجية من قاعدة بيانات Kaspersky

إذا كنت قد أنشأت أي حزم تثبيت لتطبيقات جهات خارجية مدرجة في قاعدة بيانات Kaspersky، يمكنك بالتالي عرض إعدادات هذه الحزم وتعديلها.

تعديل إعدادات حزمة تثبيت تطبيق جهة خارجية من قاعدة بيانات Kaspersky غير متوفر إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

لعرض وتعديل إعدادات حزمة تثبيت لتطبيق جهة خارجية من قاعدة بيانات Kaspersky:

1. في القائمة الرئيسية، انتقل إلى **Installation packages** ← **Deployment & assignment** ← **Discovery & deployment**.
2. في قائمة حزم التثبيت التي تفتح، انقر على اسم الحزمة ذات الصلة.
3. في صفحة الخصائص التي تفتح، قم بتعديل الإعدادات إذا كان ذلك ضروريًا.
4. انقر على زر **Save**.

يتم حفظ الإعدادات التي عدلتها.

إعدادات حزمة تثبيت تطبيق جهة خارجية من قاعدة بيانات Kaspersky

إعدادات حزمة تثبيت لتطبيق جهة خارجية يتم تجميعها في علامات التبويب التالية:

لا يتم عرض إلا جزء من الإعدادات المدرجة بالأسفل بشكل افتراضي حتى يمكنك إضافة الأعمدة المقابلة عن طريق النقر على زر **Filter** وتحديد أسماء الأعمدة ذات الصلة من القائمة.

- تبويب **General**:
  - حقل الإدخال الذي يحتوي على اسم حزمة التثبيت الذي يمكن تحريره يدويًا
  - **Application**

    اسم تطبيق الجهة الخارجية الذي تم إنشاء حزمة التثبيت له.
  - **Version**

    رقم إصدار تطبيق الجهة الخارجية الذي تم إنشاء حزمة التثبيت له.
  - **Size**

    حجم حزمة تثبيت الجهة الخارجية (بالكيلو بايت).
  - **Created**

    تاريخ ووقت إنشاء حزمة تثبيت الجهة الخارجية.
  - **Path**

    مسار مجلد الشبكة الذي يوجد فيه حزمة تثبيت الجهة الخارجية.
- تبويب **Installation procedure**:
  - **Install the required general system components**

    إذا تم تمكين هذا الخيار، قبل تثبيت التحديث، يقوم التطبيق تلقائيًا بتثبيت كافة مكونات النظام العامة (المتطلبات الأساسية) اللازمة لتثبيت التحديث. على سبيل المثال، يمكن أن تكون تلك المتطلبات الأساسية عبارة عن تحديثات نظام التشغيل.

    إذا تم تعطيل هذا الخيار، فقط يتعين عليك تثبيت المتطلبات الأساسية يدويًا.

    يتم تعطيل هذا الخيار افتراضيًا.
  - جدول يعرض خصائص التحديث ويحتوي على الأعمدة التالية:
    - **Name**

      اسم الشبكة الفرعية.
    - **Description**

      وصف التحديث.

- **Source**

مصدر التحديث، أي ما إذا كان قد تم إصداره بواسطة Microsoft أو بواسطة مطور آخر تابع لجهة خارجية.

- **Type**

نوع التحديث، أي ما إذا كان مخصصًا لبرنامج تشغيل أو تطبيق.

- **Category**

يتم عرض فئة Windows Server Update Services (WSUS) لتحديثات Microsoft (التحديثات المهمة أو تحديثات التعريف أو برامج التشغيل أو حزم الميزات أو تحديثات الأمان أو حزم الخدمة أو الأدوات أو مجموعات التحديثات أو التحديثات أو الترقية).

- **Importance level according to MSRC**

مستوى أهمية التحديث المحدد في مركز استجابة خبراء الأمان من Microsoft (MSRC).

- **Importance level**

مستوى أهمية التحديث كما تحدده Kaspersky.

- **Patch importance level**

مستوى أهمية التصحيح إذا كان مخصصًا لتطبيق Kaspersky.

- **Article**

معرف المقالة في "قاعدة المعارف" التي تصف التحديث.

- **Bulletin**

معرف نشرة الأمان التي تصف التحديث.

- **Not assigned for installation (new version)**

يعرض ما إذا كان التحديث بحالة "غير مخصص للتثبيت" أم لا.

- **To be installed**

يعرض ما إذا كان التحديث بحالة "للتثبيت" أم لا.

- **Installing**

يعرض ما إذا كان التحديث بحالة "جاري التثبيت" أم لا.

- **Installed**

يعرض ما إذا كان التحديث بحالة "مثبت" أم لا.

- **Failed**

يعرض ما إذا كان التحديث بحالة "تعذر" أم لا.

- **Restart is required**

يعرض ما إذا كان التحديث بحالة "إعادة التشغيل مطلوبة" أم لا.

- **Registered**

يعرض تاريخ ووقت تسجيل التحديث.

- **Installed in interactive mode**

  يعرض ما إذا كان التحديث يتطلب التفاعل مع المستخدم أثناء التثبيت.

- **Revoked**

  يعرض التاريخ والوقت اللذين تم فيهما إبطال التحديث.

- **Update approval status**

  يعرض ما إذا قد تمت الموافقة على التحديث للتثبيت أم لا.

- **Revision**

  يعرض رقم المراجعة الحالي للتحديث.

- **Update ID**

  يعرض معرّف التحديث.

- **Application version**

  يعرض رقم الإصدار الذي سيتم تحديث التطبيق إليه.

- **Superseded**

  يعرض التحديثات الأخرى التي يمكن أن تحل محل التحديث.

- **Superseding**

  يعرض التحديثات الأخرى التي يمكن أن يحل محلها التحديث.

- **You must accept the terms of the License Agreement**

  يعرض ما إذا كان التحديث يتطلب قبول شروط اتفاقية ترخيص المستخدم النهائي أم لا.

- **Description URL**

  يعرض اسم بائع التحديث.

- **Application family**

  يعرض اسم عائلة التطبيقات التي ينتمي إليها التحديث.

- **Application**

  يعرض اسم التطبيق الذي ينتمي إليه التحديث.

- **Localization language**

  يعرض لغة ترجمة التحديث.

- **Not assigned for installation (new version)**

  يعرض ما إذا كان التحديث بحالة "غير مخصص للتثبيت (إصدار جديد)".

- **Requires prerequisites installation**

  يعرض ما إذا كان التحديث بحالة "يتطلب متطلبات أساسية للتثبيت".

- **Download mode**

  يعرض وضع تنزيل التحديث.

- **Is a patch**

  يعرض ما إذا كان التحديث عبارة عن تصحيح أم لا.

- **Not installed**

  يعرض ما إذا كان التحديث بحالة "غير مثبت" أم لا.

- علامة تبويب **Settings** تعرض إعدادات حزمة التثبيت - مع عرض أسمائها وأوصافها وقيمها - والمستخدمة كمعلمات في سطر الأوامر أثناء التثبيت. إذا كانت الحزمة لا توفر تلك الإعدادات، يتم عرض الرسالة المقابلة. يمكنك تعديل قيم هذه الإعدادات.

- علامة تبويب **Revision history** تعرض مراجعات حزمة التثبيت وتحتوي على الأعمدة التالية:

  - **Revision** - رقم مراجعة حزم التثبيت.
  - **Time** - تاريخ ووقت تعديل إعدادات حزمة التثبيت.
  - **User** — اسم المستخدم الذي أجر التعديل على إعدادات حزمة التثبيت.
  - **Action** — الإجراء الذي تم اتخاذه على حزمة التثبيت في المراجعة.
  - **Description** — وصف المراجعة ذات الصلة بالتغيير الذي تم إجراؤه على إعدادات حزمة التثبيت.

  تكون خانة وصف المراجعة فارغة بشكل افتراضي. ولإضافة وصف إلى مراجعة، حدد المراجعة ذات الصلة وانقر فوق الزر **Edit description**. في النافذة التي تفتح، أدخل نصًا لوصف المراجعة.

علامات التطبيقات

يتيح لك Kaspersky Security Center تمييز التطبيقات من سجل التطبيقات. العلامة هي ملصق تطبيق يمكن استخدامها لتجميع التطبيقات أو العثور عليها. يمكن للعلامة المخصصة لتطبيقات أن تكون بمثابة شرط في تحديدات الأجهزة.

يمكنك على سبيل المثال إنشاء علامة [للمتصفحات] وتخصيصها لجميع المتصفحات (مثل Microsoft Internet Explorer وGoogle Chrome وMozilla Firefox. وغيرها).

إنشاء علامة تطبيق

إنشاء علامة تطبيق:

1. في القائمة الرئيسية، انتقل إلى **Application tags** ← **Third-party applications** ← **Operations**.
2. انقر على **Add**.

   ستفتح نافذة علامة جديدة.
3. أدخل اسم العلامة.
4. انقر فوق **OK** لحفظ التغييرات.

تظهر العلامة الجديدة في قائمة علامات التطبيقات.

إعادة تسمية علامة تطبيق

لإعادة تسمية علامة تطبيق:

1. في القائمة الرئيسية، انتقل إلى **Application tags** ← **Third-party applications** ← **Operations**.

2. حدد خانة الاختيار الموجودة بجوار العلامة التي ترغب في إعادة تسميتها ثم انقر على **Edit**.

   ستفتح نافذة الخصائص.

3. قم بتغيير اسم العلامة.

4. انقر فوق **OK** لحفظ التغييرات.

   تظهر العلامة المحدثة في قائمة علامات التطبيقات.

تعيين علامات لتطبيق

لتخصيص علامة أو عدة علامات لتطبيق:

1. في القائمة الرئيسية، انتقل إلى **Applications registry** ← **Third-party applications** ← **Operations**.

2. انقر على اسم التطبيق الذي ترغب في تخصيص العلامات له.

3. حدد علامة التبويب **Tags**.

   تعرض علامة التبويب جميع علامات التطبيق الموجودة على خادم الإدارة. بالنسبة للعلامات المخصصة للتطبيق المحدد، يتم تحديد خانة الاختيار في عمود **Tag assigned**.

4. بالنسبة للعلامات التي ترغب في تخصيصها، حدد خانات الاختيار في عمود **Tag assigned**.

5. انقر على **Save**لحفظ التغييرات.

   يتم تخصيص العلامات للتطبيق.

إزالة علامات معينة من تطبيق

لإزالة علامة أو عدة علامات من تطبيق:

1. في القائمة الرئيسية، انتقل إلى **Applications registry** ← **Third-party applications** ← **Operations**.

2. انقر على اسم التطبيق الذي ترغب في إزالة العلامات منه.

3. حدد علامة التبويب **Tags**.

   تعرض علامة التبويب جميع علامات التطبيق الموجودة على خادم الإدارة. بالنسبة للعلامات المخصصة للتطبيق المحدد، يتم تحديد خانة الاختيار في عمود **Tag assigned**.

4. بالنسبة للعلامات التي ترغب في إزالتها، حدد خانات الاختيار في عمود **Tag assigned**.

5. انقر على **Save** لحفظ التغييرات.

يتم إزالة العلامات من التطبيق.

لا يتم حذف علامات التطبيق التي تمت إزالتها. يمكنك، إذا كنت ترغب، حذفها يدويًا.

حذف علامة تطبيق

لحذف علامة تطبيق:

1. في القائمة الرئيسية، انتقل إلى **Application tags** ← **Third-party applications** ← **Operations**.

2. من القائمة، حدد علامة التطبيق التي ترغب في حذفها.

3. انقر على زر **Delete**.

4. في النافذة التي يتم فتحها، انقر على **OK**.

سيتم حذف علامة التطبيق. يتم إزالة العلامة المحذوفة بشكل تلقائي من جميع التطبيقات التي تخصيصها إليها.

المراقبة وإعداد التقارير

يبين هذا القسم إمكانيات المراقبة وإعداد التقارير في Kaspersky Security Center. تمنحك هذه الإمكانيات نظرة عامة على البنية الأساسية الخاصة بك وحالات الحماية والإحصائيات.

بعد نشر Kaspersky Security Center أو أثناء العملية، يمكنك تكوين مزايا المراقبة وإعداد التقارير لتتناسب مع احتياجاتك بشكل أفضل.

السيناريو: المراقبة وإعداد التقارير

يعرض هذا القسم سيناريو لتكوين ميزة المراقبة وإعداد التقارير في Kaspersky Security Center.

المتطلبات الأساسية

بعد أن تنشر Kaspersky Security Center في شبكة مؤسسة، يمكنك بدء مراقبته وإنشاء تقارير عن عمله.

المراقبة وإعداد التقارير في شبكة مؤسسة تسير في مراحل:

1. **تكوين تبديل حالات الجهاز**

تعرَّف على إعدادات حالات الجهاز اعتمادًا على الظروف. يمكنك عن طريق تغيير هذه الإعدادات تغيير عدد الأحداث ذات مستويات الأهمية حرج أو تحذيري. عند تكوين تبديل حالات الجهاز، تأكد مما يلي:

- الإعدادات الجديدة لا تخالف سياسات أمان المعلومات لمؤسستك.
- أنت تقدر على التفاعل مع أحداث الأمان المهمة في شبكة مؤسستك في الوقت المناسب.

2 **تكوين إخطارات الأحداث التي تحدث على أجهزة العميل:**

تعليمات للمساعدة:

قم بتكوين الإخطار (عن طريق البريد الإلكتروني أو الرسائل النصية القصيرة أو عن طريق تشغيل ملف تنفيذي) للأحداث على أجهزة العميل.

3 **تغيير استجابة شبكة أمانك لحدث Virus outbreak.**

يمكنك تغيير الحدود المحددة في خصائص خادم الإدارة. يمكنك كذلك إنشاء سياسة أكثر صرامة يتم تفعيلها أو إنشاء مهمة سيتم تشغيلها عند وقوع هذا الحدث.

4 **اتخاذ الإجراءات الموصى بها للإخطارات الحرجة والتحذيرية**

تعليمات للمساعدة:

اتخاذ الإجراءات الموصى بها لشبكة مؤسستك

5 **مراجعة حالة الأمان لشبكة مؤسستك**

تعليمات للمساعدة:

- راجع عنصر الواجهة Protection status
- قم بإنشاء ومراجعة Report on protection status
- قم بإنشاء ومراجعة Report on errors

6 **تحديد مواقع أجهزة العميل غير المحمية**

تعليمات للمساعدة:

- مراجعة عنصر واجهة المستخدمNew devices
- قم بإنشاء ومراجعة Report on protection deployment

7 **التحقق من حماية أجهزة العميل**

تعليمات للمساعدة:

- إنشاء التقارير ومراجعتها من فئتي Protection status وThreat statistics
- بدء تحديد الحدث Critical ومراجعته

8 **تقييم وتقييد تحميل الحدث على قاعدة البيانات**

يتم نقل المعلومات حول الأحداث التي تحدث أثناء تشغيل التطبيقات المُدارة من جهاز عميل ويتم تسجيلها بقاعدة بيانات خادم الإدارة. لتقييد التحميل على خادم الإدارة، قم بتقييم وتقليل أقصى عدد من الأحداث التي يمكن تخزينها في قاعدة البيانات.

تعليمات للمساعدة:

- حساب مساحة قاعدة البيانات
- وضع حد للعدد الأقصى من الأحداث

9 **مراجعة معلومات الترخيص**

تعليمات للمساعدة:

- أضف عنصر الواجهة License key usage إلى جزء المعلومات وراجعه.
- قم بإنشاء ومراجعة Report on usage of license keys

النتائج

عند إكمال السيناريو، سيتم إعلامك بحماية شبكة مؤسستك وبالتالي يمكنك التخطيط لإجراءات للمزيد من الحماية.

حول أنواع المراقبة وإعداد التقارير

يتم تخزين المعلومات الخاصة بأحداث الأمان في شبكة المؤسسة في قاعدة بيانات خادم الإدارة. استنادًا إلى الأحداث، توفر Kaspersky Security Center Web Console الأنواع التالية من المراقبة وإعداد التقارير في شبكة مؤسستك:

- لوحة القيادة
- تقارير
- مجموعات الأحداث المحددة
- الإشعارات

لوحة القيادة

يتيح لك جزء المعلومات مراقبة اتجاهات الأمان في شبكة مؤسستك من خلال تزويدك بعرض رسومي للمعلومات.

تقارير

تسمح لك ميزة التقارير بالحصول على معلومات رقمية تفصيلية حول أمان شبكة مؤسستك وحفظ هذه المعلومات إلى أحد الملفات وإرسالها بالبريد الإلكتروني وطباعتها.

مجموعات الأحداث المحددة

توفر تحديدات الأحداث عرضًا على الشاشة يتضمن مجموعات الأحداث المُسمَّاة المحددة من قاعدة بيانات خادم الإدارة. يتم تجميع مجموعات الأحداث هذه وفقًا للفئات التالية:

- حسب مستوى الأهمية—**أحداث حرجة**، و**حالات الخلل الوظيفي**، و**تحذيرات**، و**معلومات عن الأحداث**
- حسب الوقت—**الأحداث الأخيرة**
- حسب النوع—**طلبات المستخدم** و**أحداث التدقيق**

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center Web Console.

الإشعارات

تنبهك الإشعارات بشأن الأحداث، وتساعدك على تسريع استجاباتك لهذه الأحداث من خلال تنفيذ الإجراءات الموصى بها أو التي تراها مناسبة.

لوحة القيادة والبرامج المصغرة

يحتوي هذا القسم على معلومات حول لوحة المعلومات والبرامج المصغرة التي توفرها لوحة المعلومات. يتضمن القسم إرشادات حول كيفية إدارة عناصر واجهة المستخدم وتكوين إعدادات البرامج المصغرة.

باستخدام لوحة القيادة

يتيح لك جزء المعلومات مراقبة اتجاهات الأمان في شبكة مؤسستك من خلال تزويدك بعرض رسومي للمعلومات.

تتوفر لوحة المعلومات في Kaspersky Security Center Web Console في قسم **Monitoring & reporting** عن طريق النقر على **Dashboard**.

جزء المعلومات يوفر عناصر واجهة يمكن تخصيصها. يمكنك اختيار عدد كبير من عناصر الواجهة المختلفة التي يتم عرضها في مخطط دائري أو مخطط دائرة مجوف أو جداول أو رسومات بيانية أو مخطط شريطي أو قوائم. يتم تحديث المعلومات المعروضة في الأدوات تلقائيًا، وتتراوح فترة التحديث من دقيقة إلى دقيقتين. يختلف الفاصل الزمني بين التحديثات باختلاف عنصر الواجهة. يمكنك تحديث البيانات في عنصر الواجهة يدويًا في أي وقت عن طريق قائمة الإعدادات.

بشكل افتراضي، عناصر الواجهة تشمل معلومات عن الأحداث المخزنة في قاعدة بيانات خادم الإدارة.

Kaspersky Security Center Web Console به مجموعة افتراضية من عناصر الواجهة للفئات التالية:

- **Protection status**
- **Deployment**
- **Updating**
- **Threat statistics**
- **Other**

بعض عناصر الواجهة بها معلومات نصية ذات روابط. يمكنك عرض معلومات تفصيلية عن طريق النقر على رابط.

عند تكوين جزء المعلومات، يمكنك إضافة عناصر الواجهة التي تحتاج إليها أو إخفاء عناصر الواجهة التي لا تحتاج إليها أو تغيير حجم أو مظهر عناصر الواجهة أو نقل عناصر الواجهة أو تغيير إعداداتها.

إضافة عناصر واجهة إلى جزء المعلومات

لإضافة عناصر واجهة إلى جزء المعلومات:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
2. انقر على زر **Add or restore web widget**.
3. في قائمة عناصر الواجهة المتوفرة، حدد عناصر الواجهة التي ترغب في إضافتها إلى جزء المعلومات.

   يتم تجميع عناصر الواجهة بالفئة. لعرض قائمة بعناصر الأمان المدرجة في فئة، انقر على أيقونة الرتبة العسكرية (>) الموجود بجوار اسم الفئة.
4. انقر على الزر **Add**.

   يتم إضافة عناصر الواجهة المحددة إلى نهاية جزء المعلومات.

   يمكنك الآن تعديل تمثيل عناصر الواجهة المضافة ومعلماتها.

إخفاء عنصر واجهة من لوحة القيادة

لإخفاء عنصر واجهة معروض من جزء المعلومات:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
2. انقر على أيقونة الإعدادات (⚙) الموجود بجوار عنصر الواجهة الذي ترغب في إخفائه.
3. حدد **Hide web widget** .
4. في النافذة **Warning** التي تفتح، انقر فوق **OK**.

   يتم إخفاء عنصر الواجهة المحدد. يمكنك لاحقًا إضافة عنصر الواجهة هذا إلى جزء المعلومات مرة أخرى.

تحريك عنصر واجهة مستخدم على لوحة القيادة

لنقل عنصر واجهة إلى جزء المعلومات:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
2. انقر على أيقونة الإعدادات (⚙) الموجود بجوار عنصر الواجهة الذي ترغب في نقله.
3. حدد **Move**.
4. انقر على المكان الذي ترغب في نقل عنصر الواجهة إليه. يمكنك تحديد عنصر واجهة آخر فقط.

   يتم تبديل مكاني عنصري الواجهة المحددين.

تغيير حجم عنصر الواجهة أو مظهره

لعناصر الواجهة التي تعرض رسمًا بيانيًا، يمكنك تغيير تمثيلها إلى مخطط شريطي أو مخطط خطي. يمكنك لبعض عناصر الواجهة تغيير حجمها: صغير أو متوسط أو كبير.

لتغير تمثيل عنصر الواجهة:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
2. انقر على أيقونة الإعدادات (⚙) الموجود بجوار عنصر الواجهة الذي ترغب في تحريره.
3. قم بأحد الإجراءات التالية:
   - لعرض عنصر الواجهة كمخطط شريطي، حدد **Chart type: Bars**.
   - لعرض عنصر الواجهة كمخطط خطي، حدد **Chart type: Lines**.
   - لتغيير المنطقة التي يشغلها التطبيق المصغر، حدد إحدى القيم:
     - **Compact**
     - **Compact (bar only)**
     - **Medium (donut chart)**
     - **Medium (bar chart)**
     - **Maximum**

يتم تغيير تمثيل عنصر الواجهة المحدد.

تغيير إعدادات عنصر الواجهة

لتغيير إعدادات عنصر واجهة:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
2. انقر على أيقونة الإعدادات (⚙) الموجود بجوار عنصر الواجهة الذي ترغب في تغييره.
3. حدد **Show settings**.
4. في نافذة إعدادات عنصر الواجهة التي تفتح، قم بتغيير إعدادات عنصر الواجهة كما هو مطلوب.
5. انقر على **Save**لحفظ التغييرات.

يتم تغيير إعدادات عنصر الواجهة المحدد.

تعتمد مجموعة الإعدادات على عنصر الواجهة المعين. يوجد أدناه بعض الإعدادات الشائعة:

- **Web widget scope** (مجموعة الكائنات التي يعرض عنصر الواجهة معلومات لها)، مثل مجموعة الإدارة أو تحديد جهاز.
- **Select task** (المهمة التي يعرض عنصر الواجهة معلومات لها).
- **Time interval** (الفاصل الزمني الذي يتم عرض المعلومات خلاله في عنصر الواجهة) بين التاريخين المحددين أو من التاريخ المحدد إلى اليوم الحالي أو من اليوم الحالي إلا عدد الأيام المحدد إلى اليوم الحالي.
- **Set to Critical if these are specified** و**Set to Warning if these are specified** (القواعد التي تحدد لون إشارة حركة المرور).

بعد تغيير إعدادات الأداة، يمكنك تحديث البيانات على الأداة يدويًا.

لتحديث البيانات في أداة:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
2. انقر على أيقونة الإعدادات (⚙) الموجود بجوار الأداة التي ترغب في نقلها.
3. حدد **Refresh**.

يتم تحديث البيانات الموجودة في الأداة.

حول وضع لوحة القيادة فقط

يمكنك تكوين وضع لوحة المعلومات فقط للموظفين الذين لا يديرون الشبكة ولكنهم يرغبون في الاطلاع على إحصائيات حماية الشبكة في Kaspersky Security Center (على سبيل المثال، أحد كبار المديرين). عندما يقوم المستخدم بتمكين هذا الوضع، تُعرض لوحة معلومات تتضمن مجموعة محددة مسبقًا من التطبيقات المصغرة للمستخدم فقط. وبالتالي، يمكنه مراقبة الإحصائيات المحددة في التطبيقات المصغرة، على سبيل المثال، حالة الحماية لجميع الأجهزة المدارة، أو عدد التهديدات المكتشفة مؤخرًا، أو قائمة التهديدات الأكثر شيوعًا في الشبكة.

عندما يعمل المستخدم في وضع لوحة المعلومات فقط، تُطبق القيود التالية:

- لا تُعرض القائمة الرئيسية للمستخدم، لذا لا يمكنه تغيير إعدادات حماية الشبكة.
- لا يمكن للمستخدم تنفيذ أي إجراءات باستخدام التطبيقات المصغرة، على سبيل المثال، إضافتها أو إخفاؤها. لذلك، تحتاج إلى وضع جميع التطبيقات المصغرة المطلوبة للمستخدم في لوحة المعلومات وتكوينها، على سبيل المثال، يمكنك تعيين قاعدة حساب العناصر أو تحديد الفاصل الزمني.

لا يمكنك تعيين وضع لوحة التحكم فقط لنفسك. إذا كنت ترغب في العمل في هذا الوضع، فاتصل بمسؤول النظام أو موفر الخدمة المُدارة (MSP) أو مستخدم لديه حق **تعديل كائن ACL** في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.

جارٍ تكوين وضع لوحة المعلومات فقط

قبل بدء تكوين وضع لوحة المعلومات فقط، تأكد من استيفاء المتطلبات الأساسية التالية:

- لديك حق **تعديل قوائم التحكم في الوصول للكائن** مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**. إذا لم يكن لديك هذا الحق، فستكون علامة التبويب الخاصة بتكوين الوضع مخفية.
- يكون للمستخدم حق **القراءة** في المجال الوظيفي **الميزات العامة: الوظائف الأساسية**.

في حالة ترتيب تسلسل هرمي لخوادم الإدارة في شبكتك، لتكوين وضع لوحة المعلومات فقط، انتقل إلى الخادم حيث يتوفر حساب المستخدم في علامة التبويب **Users** في القسم **Users & groups ← Users & roles** يمكن أن يكون خادمًا أساسيًا أو خادمًا ثانويًا فعليًا. لا يمكن ضبط الوضع على خادم افتراضي.

لتكوين وضع لوحة المعلومات فقط:

1. في القائمة الرئيسية، انتقل الى **Users & groups ← Users & roles**، ثم حدد علامة التبويب **Users**.
2. انقر على اسم حساب المستخدم الذي تريد ضبط لوحة المعلومات مع التطبيقات المصغرة له.
3. في نافذة إعدادات الحساب التي تفتح، حدد علامة التبويب **لوحة المعلومات**.

   في علامة التبويب التي تفتح، تُعرض لوحة المعلومات نفسها كما تظهر للمستخدم.
4. في حالة تمكين الخيار **عرض وحدة التحكم في وضع لوحة المعلومات فقط**، اضغط على زر التبديل لتعطيله.

   عند تمكين هذا الخيار، لا يمكنك أيضًا تغيير لوحة المعلومات. بعد تعطيل الخيار، يمكنك إدارة التطبيقات المصغرة.
5. تكوين مظهر لوحة المعلومات. مجموعة التطبيقات المصغرة المعدة في علامة التبويب **لوحة المعلومات** متاحة للمستخدم الذي لديه حساب قابل للتخصيص. لا يمكنه تغيير أي إعدادات أو تغيير حجم التطبيقات المصغرة أو إضافتها أو حذفها من لوحة التحكم. لذلك، عليك تعديلها لتناسب المستخدم، حتى يتمكن من عرض إحصائيات حماية الشبكة. لهذا الغرض، في علامة تبويب **لوحة المعلومات**، يمكنك تنفيذ الإجراءات نفسها باستخدام التطبيقات المصغرة كما في القسم **Monitoring & reporting ← Dashboard**:
   - إضافة برامج مصغرة جديدة إلى لوحة المعلومات.
   - إخفاء البرامج المصغرة التي لا يحتاجها المستخدم.
   - نقل البرامج المصغرة في ترتيب معين.
   - تغيير حجم أو مظهر البرامج المصغرة.
   - تغيير إعدادات البرامج المصغرة.
6. بدل زر التبديل من أجل تفعيل خيار **عرض وحدة التحكم في وضع لوحة المعلومات فقط**.

   بعد ذلك، تتوفر لوحة المعلومات فقط للمستخدم. يمكنه مراقبة الإحصائيات ولكن لا يمكنه تغيير إعدادات حماية الشبكة ومظهر لوحة المعلومات. بينما تُعرض لوحة المعلومات نفسها كما تظهر للمستخدم، لن تتمكن أيضًا من تغيير لوحة المعلومات.

   إذا أبقيت الخيار معطلاً، فستُعرض القائمة الرئيسية للمستخدم، حتى يتمكن من تنفيذ إجراءات مختلفة في Kaspersky Security Center، بما في ذلك تغيير إعدادات الأمان والتطبيقات المصغرة.
7. انقر فوق الزر **حفظ** عند الانتهاء من تكوين وضع لوحة المعلومات فقط. وبعد ذلك ستُعرض فقط لوحة المعلومات المعدة مسبقًا للمستخدم.
8. إذا أراد المستخدم عرض إحصائيات تطبيقات Kaspersky المدعومة ويحتاج إلى حقوق الوصول للقيام بذلك، عليك تكوين حقوق الوصول للمستخدم. بعد ذلك، تُعرض بيانات تطبيقات Kaspersky للمستخدم في التطبيقات المصغرة هذه.

يمكن الآن للمستخدم تسجيل الدخول إلى Kaspersky Security Center ضمن الحساب المخصص ومراقبة إحصائيات حماية الشبكة في وضع لوحة المعلومات فقط.

تقارير الإدارة والحماية

يصف هذا القسم كيفية استخدام التقارير وإدارة قوالب التقارير المخصصة واستخدام قوالب التقارير لإنشاء تقارير جديدة وإنشاء مهام تسليم التقارير.

استخدام التقارير

تسمح لك ميزة التقارير بالحصول على معلومات رقمية تفصيلية حول أمان شبكة مؤسستك وحفظ هذه المعلومات إلى أحد الملفات وإرسالها بالبريد الإلكتروني وطباعتها.

تتوفر التقارير في Kaspersky Security Center Web Console في قسم **Monitoring & reporting** عن طريق النقر على **Reports**.

بشكل افتراضي، التقارير تشمل معلومات لآخر 30 يومًا.

Kaspersky Security Center به مجموعة افتراضية من التقارير للفئات التالية:

- **Protection status**
- **Deployment**
- **Updating**
- **Threat statistics**
- **Other**

يمكنك إنشاء قوالب تقارير مخصصة وتحرير قوالب التقارير وحذفها.

يمكنك إنشاء التقارير المبنية على قوالب موجودة وتصدير التقارير إلى الملفات وإنشاء المهام لتقديم التقارير.

إنشاء قالب تقرير

لإنشاء قالب تقرير:

1. في القائمة الرئيسية، انتقل إلى**Monitoring & reporting** ← **Reports**
2. انقر على **Add**.

   يبدأ معالج قالب التقرير الجديد. انتقل عبر المعالج باستخدام زر **Next**.
3. أدخل اسم التقرير وحدد نوع التقرير.
4. في خطوة **Scope** في المعالج، حدد مجموعة أجهزة العميل (مجموعة الإدارة أو تحديد الجهاز أو الأجهزة المحددة أو جميع أجهزة الشبكة) التي سيتم عرض بياناتها في التقارير المبنية على قالب التقرير هذا.

5. في خطوة **Reporting period** في المعالج، حدد فترة التقرير. القيم المتاحة هي كما يلي:

- بين تاريخين محددين
- من التاريخ المحدد إلى تاريخ إنشاء التقرير
- من تاريخ إنشاء التقرير، ناقص العدد المحدد من الأيام، إلى تاريخ إنشاء التقرير

قد لا تظهر هذه الصفحة لبعض التقارير.

6. انقر على **OK** لإغلاق المعالج.

7. قم بأحد الإجراءات التالية:

- انقر على زر **Save and run** لحفظ قالب التقرير الجديد ولتشغيل تقرير بناءً عليه.
  يتم حفظ قالب التقرير. يتم إنشاء التقرير.
- انقر على زر **Save** لحفظ قالب التقرير الجديد.
  يتم حفظ قالب التقرير.

يمكنك استخدام القالب الجديد في إنشاء التقارير وعرضها.

عرض وتحرير خصائص قالب التقرير

يمكنك عرض وتحرير الخصائص الأساسية لقالب تقرير، على سبيل المثال، اسم قالب التقرير أو الحقول المعروضة في التقرير.

لعرض وتحرير خصائص قالب التقرير:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Reports**.

2. حدد خانة الاختيار الموجودة بجوار قالب التقارير التي ترغب في عرض خصائصه وتحريرها.
   كحل بديل، يمكنك أولاً إنشاء التقرير ثم النقر على زر **Edit**.

3. انقر على زر **فتح خصائص قالب التقرير** .
   ستفتح نافذة **تحرير التقرير <اسم التقرير>** مع تحديد تبويب **General**.

4. قم بتحرير خصائص قالب التقرير:

- تبويب **General**:
  - اسم قالب التقرير
  - **Maximum number of entries to display**

إذا تم تمكين هذا الخيار، فإن عدد الإدخالات المعروضة في الجدول مع بيانات التقرير التفصيلية لا يزيد عن القيمة المحددة.

يتم أولاً فرز إدخالات التقرير وفقًا للقواعد المحددة في القسم **الحقول** ← **حقول التفاصيل** في خصائص قالب التقرير، وبعد ذلك يتم الاحتفاظ فقط بالإدخالات الأولى الناتجة. يعرض عنوان الجدول المزود ببيانات تقرير مفصلة العدد المعروض من الإدخالات وإجمالي عدد الإدخالات المتاح الذي يطابق إعدادات قالب التقرير الآخر.

إذا تم تعطيل هذا الخيار، فإن الجدول المزود ببيانات التقرير التفصيلية يعرض جميع الإدخالات المتوفرة. لا نوصيك بتعطيل هذا الخيار. إن تقليل عدد إدخالات التقرير المعروضة يقلل من الحمل على نظام إدارة قواعد البيانات (DBMS) ويقلل الوقت اللازم لإنشاء وتصدير التقرير. تحتوي بعض التقارير على عدد كبير جدًا من الإدخالات. إذا كانت هذه هي الحالة، فقد تجد صعوبة في قراءتها وتحليلها جميعًا. وقد تنفذ مساحة الذاكرة في جهازك أيضًا أثناء إنشاء مثل هذا التقرير، وبالتالي لن تتمكن من عرض التقرير.

يتم تمكين هذا الخيار افتراضيًا. القيمة الافتراضية هي 1000.

- **Group**

انقر على زر **Settings** لتغيير مجموعة أجهزة العميل التي تم إنشاء التقرير من أجلها. قد لا يكون هذا الزر متاحًا لبعض أنواع التقارير. الإعدادات الفعلية تعتمد على الإعدادات المحددة أثناء إنشاء قالب القرير.

- **Time interval**

انقر على زر **Settings** لتعديل فترة التقرير. قد لا يكون هذا الزر متاحًا لبعض أنواع التقارير. القيم المتاحة هي كما يلي:

  - بين تاريخين محددين
  - من التاريخ المحدد إلى تاريخ إنشاء التقرير
  - من تاريخ إنشاء التقرير، ناقص العدد المحدد من الأيام، إلى تاريخ إنشاء التقرير

- **Include data from secondary and virtual Administration Servers**

إذا تم تمكين هذا الخيار، فإن التقرير يقوم بتضمين معلومات من خوادم الإدارة الثانوية والظاهرية التابعة الخاضعة لخادم الإدارة الذي يتم إنشاء قالب التقرير له.

قم بتعطيل هذا الخيار إذا كنت ترغب في عرض البيانات فقط من خادم الإدارة الحالي.

يتم تمكين هذا الخيار افتراضيًا.

- **Up to nesting level**

يتضمن التقرير بيانات من خوادم الإدارة الثانوية والظاهرية الموجودة ضمن خادم الإدارة الحالي على مستوى تداخل أقل من أو يساوي القيمة المحددة.

القيمة الافتراضية هي 1. قد ترغب في تغيير هذه القيمة إذا كان عليك استعادة المعلومات من خوادم الإدارة الثانوية الموجودة في المستويات الأدنى في الشجرة.

- **Data wait interval (min)**

قبل إنشاء التقرير، ينتظر خادم الإدارة الذي يتم إنشاء قالب التقرير له البيانات من خوادم الإدارة الثانوية خلال العدد المحدد من الدقائق. إذا لم يتم تلقي أي بيانات من خادم الإدارة الثانوي في نهاية هذه الفترة، فسيتم تشغيل التقرير على أي حال. بدلاً من البيانات الفعلية، يظهر التقرير البيانات المأخوذة من ذاكرة التخزين المؤقت (إذا تم تمكين خيار **Cache data from secondary Administration Servers**)، أو **لا يوجد** (غير متوفر) بخلاف ذلك.

القيمة الافتراضية هي 5 (ثوانٍ).

- **Cache data from secondary Administration Servers**

تقوم خوادم الإدارة الثانوية بنقل البيانات إلى خادم الإدارة الذي يتم من أجله إنشاء قالب التقرير بانتظام. وهناك يتم تخزين البيانات المنقولة في ذاكرة التخزين المؤقت.

إذا لم يتمكن خادم الإدارة الحالي من تلقي البيانات من خادم الإدارة الثانوي أثناء إنشاء التقرير، فسيعرض التقرير البيانات المأخوذة من ذاكرة التخزين المؤقت. يتم أيضًا عرض التاريخ الذي تم فيه نقل البيانات إلى ذاكرة التخزين المؤقت.

يتيح لك تمكين هذا الخيار عرض المعلومات من خوادم الإدارة الثانوية حتى إذا تعذر استرجاع البيانات الحديثة. ومع ذلك، يمكن أن تكون البيانات المعروضة قديمة.

يتم تعطيل هذا الخيار افتراضيًا.

- **Cache update frequency (h)**

تقوم خوادم الإدارة الثانوية بنقل البيانات إلى خادم الإدارة الذي يتم من أجله إنشاء قالب التقرير على فترات منتظمة. يمكنك تحديد هذه الفترة بالساعات. إذا حددت 0 ساعات، لا يتم نقل البيانات إلا عند إنشاء التقرير.

القيمة الافتراضية هي 0.

- **Transfer detailed information from secondary Administration Servers**

في التقرير الذي يتم إنشاؤه، يشتمل الجدول المزود ببيانات التقرير التفصيلية على بيانات من خوادم الإدارة الثانوية لخادم الإدارة الذي يتم من أجله إنشاء قالب التقرير.

يؤدي تمكين هذا الخيار إلى إبطاء إنشاء التقرير وزيادة حركة المرور بين خوادم الإدارة. ومع ذلك، يمكنك عرض جميع البيانات في تقرير واحد.

بدلاً من تمكين هذا الخيار، قد تحتاج إلى تحليل بيانات التقرير التفصيلية للكشف عن خادم إدارة تابع معيب، ثم إنشاء نفس التقرير فقط لخادم الإدارة المعيب هذا.

يتم تعطيل هذا الخيار افتراضيًا.

- تبويب **Fields**

حدد الحقول التي سيتم عرضها في التقرير، واستخدم زر **Move up** وزر **Move down** لتغيير ترتيب هذه الحقول. استخدم زر **Add** أو زر **Edit** في تحديد إذا ما كانت المعلومات في التقرير يجب أن تبقى مرتبة ومفلترة لكل من الحقول.

في قسم **Filters of Details fields**، يمكنك أيضًا النقر على زر **Convert filters** لبدء استخدام تنسيق التصفية الممتد. هذا التنسيق يمكّنك من دمج شروط التصفية المحددة في مختلف الحقول باستخدام عملية OR المنطقية. بعد أن تنقر على الزر، ستفتح لوحة **Convert filters** على اليمين. انقر على زر **Convert filters** لتأكيد التحويل. يمكنك الآن تحديد عامل تصفية محوّل بشروط من قسم **Details fields** والتي يتم تطبيقها باستخدام عملية OR المنطقية.

> تحويل تقرير إلى التنسيق الذي يدعم شروط التصفية المعقدة سيؤدي إلى جعل التقرير غير متوافق مع الإصدارات السابقة من Kaspersky Security Center (11 والإصدارات الأقدم). أيضًا لن يحتوي التقرير المحول على أي بيانات من خوادم الإدارة الثانوية التي تقوم بتشغيل مثل هذه الإصدارات غير المتوافقة.

5. انقر على **Save**لحفظ التغييرات.

6. أغلق نافذة **تحرير التقرير <Report name>** .

يظهر قالب التقارير المحدث في قائمة قوالب التقارير.

تصدير تقرير إلى ملف

يمكنك تصدير تقرير إلى ملف بامتداد XML أو HTML أو PDF.

لتصدير تقرير إلى ملف:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Reports**.

2. حدد خانة الاختيار الموجودة بجوار التقرير الذي ترغب في تصديره إلى ملف.

3. انقر على الزر **Export report**.

4. في النافذة التي تفتح، قم بتغيير اسم ملف التقرير في حقل **Name**. بشكل افتراضي، يتوافق اسم الملف مع اسم قالب التقرير المحدد.

5. حدد نوع ملف التقرير: XML أو HTML أو PDF.

6. انقر على الزر **Export report**.

سيتم تنزيل التقرير بالتنسيق المحدد إلى جهازك (إلى المجلد الافتراضي على جهازك) أو ستفتح نافذة **حفظ باسم** في مستعرضك كي تتيح لك حفظ الملف في المكان الذي تريده.

يتم حفظ التقرير إلى الملف.

إنشاء تقرير وعرضه

لإنشاء تقرير وعرضه:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Reports**.
2. انقر على اسم قالب التقرير الذي ترغب في استخدامه لإنشاء تقرير.

   يتم إنشاء وعرض تقرير باستخدام القالب المحدد.

يتم عرض بيانات التقرير وفقًا لمجموعة الترجمة لخادم الإدارة.

ويعرض التقرير البيانات التالية:

- في تبويب **Summary**:
  - اسم ونوع التقرير، ووصف مختصر له، وفترة التقرير بالإضافة إلى معلومات حول مجموعة الأجهزة التي تم إنشاء التقرير لها.
  - مخطط رسم بياني يوضح بيانات التقرير الأكثر تمثيلًا.
  - جدول موحد يحتوي على مؤشرات التقرير المعدودة.
- في تبويب **Details**، يتم عرض جدول يحتوي على بيانات التقرير التفصيلية.

إنشاء مهمة تسليم تقرير

يمكنك إنشاء مهمة ستسلم التقارير المحددة.

لإنشاء مهمة تسليم تقرير:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Reports**.
2. حدد خانات الاختيار الموجودة بجوار قوالب التقارير التي ترغب في إنشاء مهمة تسليم تقرير لها.
3. انقر فوق الزر **Create delivery task**.

   سيبدأ معالج المهمة الجديدة. انتقل عبر المعالج باستخدام زر **Next**.
4. في خطوة **New task settings** في المعالج، أدخل اسم المهمة.

   يكون الاسم الافتراضي هو **Deliver reports**. وإذا كانت هناك مهمة بهذا الاسم موجودة بالفعل، فسيتم عرض رقم تسلسلي (<N>) تمت إضافته إلى اسم المهمة.
5. في خطوة **Report configuration** في المعالج، حدد الإعدادات التالية:
   a. قوالب التقارير التي سيتم تسليمها بالمهمة.
   b. تنسيق التقرير HTML أو XLS أو PDF.

   أداة wkhtmltopdf مطلوبة لتحويل تقرير إلى PDF. عند تحديد خيار صيغة PDF، يتحقق خادم الإدارة من تثبيت أداة wkhtmltopdf على الجهاز. إذا لم يتم تثبيت الأداة، فسيعرض التطبيق رسالة حول ضرورة تثبيت الأداة على جهاز خادم الإدارة. ثبّت الأداة يدويًا، ثم انتقل إلى الخطوة التالية.

c. سواء كان سيتم إرسال التقارير عبر البريد الإلكتروني أو مع إعدادات الإخطار بالبريد الإلكتروني.

يمكنك تحديد ما يصل إلى 20 عنوان بريد إلكتروني. لفصل عناوين البريد الإلكتروني، اضغط على **Enter** . ويمكنك أيضًا لصق قائمة مفصولة بفاصلة من عناوين البريد الإلكتروني، ثم الضغط على **Enter**.

d. سواء كان سيتم حفظ التقارير إلى مجلد، وسواء إذا ما كان سيتم استبدال تقارير محفوظة مسبقًا في هذا المجلد، وسواء إذا ما كان سيتم استخدام حساب معين للوصول إلى المجلد (لمجلد مشترك).

6. في خطوة **تكوين جدول المهمة** في المعالج، حدد جدول بدء المهمة.

تتوفر خيارات جدول المهام التالية:

- **Manually**

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.

يتم تحديد هذا الخيار افتراضيًا.

- **Every N minutes**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **Every N hours**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 6 ساعات، بداية من التاريخ والوقت الحاليين للنظام.

- **Every N days**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. بالإضافة إلى ذلك، يمكنك تحديد تاريخ تشغيل المهمة الأولى ووقته. تصبح هذه الخيارات الإضافية متاحة، إذا كانت مدعومة من خلال التطبيق الذي تنشئ المهمة من أجله.

بشكل افتراضي، تعمل المهمة كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- **Every N weeks**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **Monthly**

تعمل المهمة بشكل منتظم، في اليوم المحدد من الشهر وفي الوقت المحدد.

في الأشهر التي تفتقد إلى اليوم المحدد، تعمل المهمة في اليوم الأخير.

بشكل افتراضي، تعمل المهمة في اليوم الأول من كل شهر، في الوقت الحالي للنظام.

- **On specified days**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكل افتراضي، يكون وقت البدء هو الساعة 00:18، ولا يتم تحديد أي أيام من الشهر.

> لاحظ أنك لا تحدد تاريخًا محددًا في الشهر، ولا رقم الأسبوع (الأسبوع الأول، الأسبوع الثاني من الشهر)، لكنك تحدد الرقم التسلسلي ليوم الأسبوع خلال الشهر. على سبيل المثال، إذا وضعت المؤشر في الخلية **Tu** للصف **First**، فهذا يعني أنه سيتم تشغيل المهمة كل يوم ثلاثاء أول من كل شهر جديد.

يمكنك تحديد عدة أيام في الأسبوع.

- **On virus outbreak**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوافر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع عن المحيط الخارجي
- مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة اعتمادًا على نوع تطبيق الأمان الذي يُبلغ عن تفشي فيروس. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

- **On completing another task**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يعمل هذا الخيار فقط إذا تم تعيين كلتا المهمتين للأجهزة نفسها. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، تقوم بتشغيل مهمة فحص الفيروسات كمهمة تشغيل.

يجب عليك تحديد مهمة التشغيل من الجدول والحالة التي يجب أن تكتمل بها هذه المهمة (**Completed successfully** أو **Failed**).

إذا لزم الأمر، يمكنك البحث عن المهام وفرزها وتصفيتها في الجدول على النحو التالي:

- أدخل اسم المهمة في حقل البحث، للبحث عن المهمة حسب اسمها.
- انقر فوق أيقونة الفرز لفرز المهام حسب الاسم.

  بشكل افتراضي، يتم فرز المهام بترتيب أبجدي تصاعدي.
- انقر فوق أيقونة عامل التصفية، وفي النافذة التي تفتح، قم بتصفية المهام حسب المجموعة ، ثم انقر فوق الزر **Apply**.

7. في هذه الخطوة من المعالج، كوّن إعدادات جدول المهام الأخرى:

- في قسم **Task schedule**، تتحقق من الجدول المحدد مسبقًا أو أعد تكوينه وقم بتعيين الفاصل الزمني وأيام الشهر أو الأسبوع، أو تعيين حالة تفشي الفيروس أو إكمال مهمة أخرى كمحفز لبدء المهمة. ويمكن أيضًا تحديد وقت البدء في هذا القسم إذا تم تحديد جدول زمني قابل للتطبيق.
- في القسم **Additional settings**، حدد الإعدادات التالية:

- **Run missed tasks**

يحدد هذا الخيار سلوك مهمة في حالة كان الجهاز العميل غير مرئي على الشبكة عندما تكون المهمة على وشك البدء.

إذا تم تمكين هذا الخيار، فسيحاول النظام بدء تشغيل المهمة في المرة التالية التي يتم فيها تشغيل تطبيق Kaspersky على الجهاز العميل. إذا تم تعيين جدول المهمة على **يدويًا** أو **مرة** أو **فورًا**، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فلن يتم تشغيل سوى المهام المجدولة على الأجهزة العميلة. للجدول الزمني **يدويًا** و**مرة** و**فورًا** ، تعمل المهام فقط على الأجهزة العميلة المرئية على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تعطيل هذا الخيار افتراضيًا.

- **Use automatically randomized delay for task starts**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال فاصل زمني محدد، وهو، بداية المهمة الموزعة. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **Use automatically randomized delay for task starts within an interval of**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

- **Stop the task if it runs longer than**

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائيًا، سواء أكانت مكتملة أم لا.

قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتًا طويلاً للتنفيذ.

يتم تعطيل هذا الخيار افتراضيًا. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

8. في خطوة **Selecting an account to run the task** في المعالج، حدد بيانات اعتماد حساب المستخدم المستخدم لتشغيل المهمة.

9. إذا كنت تريد تعديل إعدادات المهام الأخرى بعد إنشاء المهمة، في خطوة **Finish task creation** في المعالج، قم بتمكين الخيار **Open task details when creation is complete** (بشكل افتراضي، يتم تمكين هذا الخيار).

10. انقر على الزر **إنهاء** لإنشاء المهمة وإغلاق المعالج.

يتم إنشاء مهمة تسليم التقرير. إذا قمت بتمكين الخيار **Open task details when creation is complete**، ستفتح نافذة إعدادات المهمة.

حذف قوالب التقارير

لحذف قالب أو عدة قوالب تقارير:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Reports**.

2. حدد خانات الاختيار الموجودة بجوار قوالب التقارير التي ترغب في حذفها.

3. انقر على زر **Delete**.

4. في النافذة التي تفتح انقر على زر **OK** لتأكيد اختيارك.

يتم حذف وقالب التقارير المحددة. إذا كانت قوالب التقارير هذه مدرجة في مهام تسليم التقارير، سيتم إزالتها كذلك من المهام.

الفعاليات واختيارات الفعالية

يوفر هذا القسم معلومات حول تحديدات الفعاليات واختيارات الفعالية، وحول أنواع الفعاليات التي تحدث في مكونات Kaspersky Security Center، وحول إدارة حظر الفعاليات المتكررة.

عن أحداث Kaspersky Security Center

يتيح لك Kaspersky Security Center تلقي معلومات عن الأحداث التي تقع أثناء تشغيل خادم الإدارة وتطبيقات Kaspersky المثبتة على الأجهزة المُدارة. يتم حفظ المعلومات حول الأحداث في قاعدة بيانات خادم الإدارة.

أنواع الأحداث

يتوفر في Kaspersky Security Center الأنواع التالية من الأحداث:

- الأحداث العامة. تحدث هذه الأحداث في جميع تطبيقات Kaspersky المدارة. مثال على حدث عام هو انتشار الفيروسات. لقد حددت الأحداث العامة بناء الجملة والدلالات بدقة. يتم استخدام الأحداث العامة على سبيل المثال، في التقارير ولوحات المعلومات.
- أحداث خاصة بتطبيقات Kaspersky المدارة. يحتوي كل تطبيق من تطبيقات Kaspersky المدارة على مجموعة من الأحداث الخاصة به.

مصادر الحدث

يمكن إنشاء الأحداث من خلال التطبيقات التالية:

- مكونات Kaspersky Security Center:
  - خادم الإدارة
  - عميل الشبكة
  - خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM
  - خادم الأجهزة المحمولة Exchange
- تطبيقات Kaspersky المُدارة

  للحصول على تفاصيل حول الأحداث التي تم إنشاؤها بواسطة تطبيقات Kaspersky المُدارة، يُرجى الرجوع إلى وثائق التطبيق المقابل.

يمكنك عرض القائمة الكاملة للأحداث التي يمكن إنشاؤها بواسطة تطبيق ما في علامة التبويب **Event configuration**. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث في خصائص خادم الإدارة.

مستوى خطورة الأحداث

يحتوي كل حدث على مستوى الأهمية الخاص به. بناء على شروط الحدوث، يمكن تعيين مستويات أهمية مختلفة لأي حدث. توجد أربعة مستويات للأهمية للأحداث:

- حدث حرج هو حدث يشير إلى تكرار مشكلة حرجة قد تؤدي إلى فقدان البيانات أو خلل في التشغيل أو خطأ حرج.
- خلل وظيفي هو حدث يشير إلى تكرار مشكلة خطيرة أو خطأ أو خلل حدث أثناء تشغيل التطبيق أو عند تنفيذ الإجراء.
- تحذير هو حدث ليس خطيرًا بالضرورة، غير أنه يشير إلى مشكلة محتملة في المستقبل. يتم تعيين معظم الأحداث كتحذيرات إذا كان من الممكن استعادة التطبيق بدون فقدان البيانات أو الإمكانيات الوظيفية بعد حدوث هذه الأحداث.
- حدث معلومات هو حدث يحدث لأغراض الإخبار عن إكمال التشغيل بنجاح، أو التشغيل الصحيح للتطبيق، أو إكمال الإجراء.

لكل حدث مدّة تخزين محددة، يمكنك خلالها عرضه في Kaspersky Security Center أو تعديله. لا يتم حفظ بعض البيانات في قاعدة بيانات خادم الإدارة بشكل افتراضي لأن مدّة التخزين المحددة هي صفر. يمكن تصدير الأحداث التي سيتم تخزينها في قاعدة بيانات خادم الإدارة فقط لمدة يوم واحد على الأقل إلى الأنظمة الخارجية.

استخدام تحديدات الحدث

توفر تحديدات الأحداث عرضًا على الشاشة يتضمن مجموعات الأحداث المُسمَّاة المحددة من قاعدة بيانات خادم الإدارة. يتم تجميع مجموعات الأحداث هذه وفقًا للفئات التالية:

- حسب مستوى الأهمية—**أحداث حرجة**، و**حالات الخلل الوظيفي**، و**تحذيرات**، و**معلومات عن الأحداث**
- حسب الوقت—**الأحداث الأخيرة**
- حسب النوع—**طلبات المستخدم** و**أحداث التدقيق**

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center Web Console.

تتوفر تحديدات الأحدث في Kaspersky Security Center Web Console في قسم **Monitoring & reporting** عن طريق النقر على **Event selections**.

بشكل افتراضي، تحديدات الأحداث تشمل معلومات لآخر سبعة أيام.

Kaspersky Security Center به مجموعة افتراضية من تحديدات الأحداث (المحددة مسبقًا):

- أحداث ذات مستويات أهمية مختلفة:
  - **أحداث حرجة**
  - **حالات الخلل الوظيفي**
  - **تحذيرات**
  - **معلومات عن الأحداث**
- **طلبات المستخدمين** (أحداث التطبيقات المُدارة)
- **الأحداث الأخيرة** (في آخر أسبوع)
- **أحداث التدقيق**.

يمكنك كذلك إنشاء وتكوين تحديدات إضافية من تعريف المستخدم. في التحديدات من تعريف المستخدم، يمكنك تصفية الأحداث بخصائص الأجهزة التي تنشأ منها (أسماء الأجهزة ونطاقات IP ومجموعات الإدارة) بأنواع الأحداث ومستويات الخطورة، وبالتطبيق واسم المكون، وبالفاصل الزمني. من الممكن كذلك إدراج نتائج المهمة في نطاق البحث. يمكنك كذلك استخدام حقل بحث بسيط يمكن فيه كتابة كلمة أو بضعة كلمات. يتم عرض جميع الأحداث التي تحتوي على أي من الكلمات المكتوبة في أي مكان في سماتها (مثل اسم حدث أو وصف حدث أو اسم مكون).

لكلٍ من التحديثات المحددة مسبقًا والتي يحددها المستخدم، يمكنك وضع حدٍ لعدد الأحداث المعروضة أو عدد السجلات التي سيتم البحث عنها. يؤثر الخياران على الوقت الذي يستغرقه Kaspersky Security Center في عرض الأحداث. كلما كبرت قاعدة البيانات، كلما ارتفعت إمكانية زيادة الوقت الذي تستغرقه العملية.

يمكنك القيام بما يلي:

- تحرير خصائص اختيارات الحدث
- إنشاء تحديدات الحدث
- عرض تفاصيل اختيارات الحدث

- حذف اختيارات الحدث
- حذف الأحداث من قاعدة بيانات خادم الإدارة

إنشاء تحديد حدث

لإنشاء تحديد حدث:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Event selections**.
2. انقر على **Add**.
3. في نافذة **New event selection** التي تفتح، حدد إعدادات تحديد الحدث الجديد. افعل هذا في قسم أو أكثر من الأقسام في النافذة.
4. انقر على **Save**لحفظ التغييرات.
   ستفتح نافذة التأكيد.
5. لعرض نتيجة تحديد الحدث، أبق على خانة الاختيار **Go to selection result** محددة.
6. انقر على **Save** لتأكيد إنشاء تحديد الحدث.

إذا احتفظت بخانة الاختيار **Go to selection result** محددة، سيتم عرض نتيجة تحديد الحدث. بخلاف ذلك، سيظهر تحديد الحدث الجديد في قائمة تحديدات الحدث.

إنشاء تحديد حدث

لتحرير تحديد حدث:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Event selections**.
2. حدد خانة الاختيار الموجودة بجوار تحديد الحدث الذي ترغب في تحريره.
3. انقر على زر **Properties**.
   ستفتح نافذة إعدادات تحديد حدث.
4. قم بتحرير خصائص تحديد الحدث.

> لتحديدات الأحداث المحددة مسبقًا، لا يمكنك إلا تحرير خصائص علامات التبويب التالية: 0 **General**باستثناء اسم التحديد) و**Time** و**Access rights**.

للتحديدات التي يحددها المستخدم، يمكنك تحرير جميع الخصائص.

5. انقر على **Save**لحفظ التغييرات.

يظهر تحديد الحدث الذي تم تحريره في القائمة.

عرض قائمة تحديد الحدث

لعرض تحديد حدث:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Event selections**.
2. حدد خانة الاختيار الموجودة بجوار تحديد الحدث الذي ترغب في بدئه.
3. قم بأحد الإجراءات التالية:
   - إذا كنت ترغب في تكوين الفرز في نتيجة تحديد الحدث، افعل ما يلي:
     a. انقر على زر **Reconfigure sorting and start**.
     b. في نافذة **Reconfigure sorting for event selection** المعروضة، حدد إعدادات الفرز.
     c. انقر على اسم التحديد.
   - بخلاف ذلك، إذا كنت ترغب في عرض قائمة الأحداث كما يتم فرزها في خادم الإدارة، انقر على اسم التحديد.

يتم عرض نتيجة تحديد الحدث.

تصدير مجموعة حدث

يتيح لك Kaspersky Security Center حفظ مجموعة حدث وإعداداته في ملف KLO. يمكنك استخدام ملف KLO هذا لاستيراد مجموعة الحدث المحفوظة إلى كل من Kaspersky Security Center Windows وKaspersky Security Center Linux.

> لاحظ أنه يمكنك تصدير مجموعات الأحداث المحددة من قبل المستخدم فقط. ولا يمكن حفظ مجموعات الأحداث من المجموعة الافتراضية لتطبيق Kaspersky Security Center (المجموعات المحددة مسبقًا) في ملف.

لتصدير مجموعة حدث:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Event selections**
2. حدد خانة الاختيار الموجودة بجوار مجموعة الحدث التي تريد تصديرها.

   لا يمكنك تصدير مجموعات أحداث متعددة في الوقت نفسه. إذا قمت بتحديد أكثر من مجموعة واحدة، فسيتم تعطيل الزر **Export**.
3. انقر على الزر **Export**.
4. في نافذة **حفظ باسم** المفتوحة، حدد اسم ومسار ملف مجموعة الحدث، ثم انقر فوق الزر **حفظ**.

   يتم عرض نافذة **حفظ باسم** فقط إذا كنت تستخدم Google Chrome أو Microsoft Edge أو Opera. إذا كنت تستخدم مستعرضًا آخر، فسيتم حفظ ملف مجموعة الحدث تلقائيًا في مجلد **التنزيلات**.

استيراد مجموعة حدث

يتيح لك Kaspersky Security Center استيراد مجموعة حدث من ملف KLO. يحتوي ملف KLO على مجموعة الأحداث التي تم تصديرها وإعداداتها.

لتحرير مجموعة حدث:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Event selections**

2. انقر فوق الزر **Import**، ثم اختر ملف مجموعة الحدث الذي تريد استيراده.

3. في النافذة المفتوحة، حدد المسار إلى ملف KLO، ثم انقر على الزر **فتح**. لاحظ أنه يمكنك تحديد ملف مجموعة حدث واحد فقط.
   تبدأ معالجة مجموعة الحدث.

يُظهر الإشعار نتائج الاستيراد. إذا تم استيراد مجموعة الحدث بنجاح، فيمكنك النقر على الرابط **عرض تفاصيل الاستيراد** لعرض خصائص مجموعة الحدث.

بعد نجاح الاستيراد، يتم عرض مجموعة الحدث في قائمة المجموعة. يتم أيضًا استيراد إعدادات مجموعة الحدث.

إذا كانت مجموعة الحدث المستوردة حديثًا لها اسم مطابق لاسم مجموعة حدث موجودة، فسيتم توسيع اسم المجموعة المستوردة بامتداد فهرس **(<next sequence number>)**، على سبيل المثال: **(1)** و**(2)**.

عرض تفاصيل حدث

لعرض تفاصيل حدث:

1. ابدأ تحديد حدث.

2. انقر على وقت الحدث المطلوب.
   تفتح نافذة **Event properties**.

3. يمكنك فعل ما يلي في النافذة المعروضة:

- عرض معلومات عن الحدث المحدد.
- الانتقال إلى الحدث التالي والحدث السابق في نتيجة تحديد الحدث.
- انتقل إلى الجهاز الذي وقع عليه الحدث.
- انتقل إلى مجموعة الإدارة التي تشمل الجهاز الذي وقع عليه الحدث.
- انتقل إلى خصائص المهمة في حالات المهمة المتعلقة بحدث.

تصدير الأحداث إلى ملف

يتيح لك Kaspersky Security Center حفظ الأحداث من حدث محدد في ملف TXT.

لتصدير الأحداث إلى ملف:

1. ابدأ تحديد حدث.

2. حدد خانة الاختيار الموجودة بجوار الحدث المطلوب.
يمكنك أيضًا تحديد عدة أحداث أو تحديد الحدث بأكمله.

3. انقر على زر **Export to file**.

يتم تصدير الحدث المحدد إلى ملف TXT.

عرض تاريخ كائن من حدث

من حدث إنشاء أو تعديل كائن يدعم إدارة المراجعة، يمكنك التبديل إلى تاريخ مراجعة الكائن.

لعرض تاريخ كائن من حدث:

1. ابدأ تحديد حدث.

2. حدد خانة الاختيار الموجودة بجوار الحدث المطلوب.

3. انقر على زر **Revision history** .

يتم فتح تاريخ مراجعة الكائن.

حذف الأحداث

لحذف حدث أو عدة أحداث:

1. ابدأ تحديد حدث.

2. حدد خانات الاختيار الموجودة بجوار الأحداث المطلوبة.

3. انقر على زر **Delete**.

يتم حذف الأحداث المحددة ولا يمكن استردادها.

حذف تحديدات الحدث

لا يمكنك حذف إلا تحديدات الأحداث من تحديد المستخدم. لا يمكن حذف تحديدات الأحداث المحددة مسبقًا.

لحذف تحديد حدث أو عدة تحديدات:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Event selections**.

2. حدد خانات الاختيار الموجودة بجوار تحديدات الحدث التي ترغب في حذفها.

3. انقر على **Delete**.

4. في النافذة التي يتم فتحها، انقر على **OK**.

يتم حذف تحديد الحدث.

تعيين مدة التخزين لحدث

يتيح لك Kaspersky Security Center تلقي معلومات عن الأحداث التي تقع أثناء تشغيل خادم الإدارة وتطبيقات Kaspersky المثبتة على الأجهزة المُدارة. يتم حفظ المعلومات حول الأحداث في قاعدة بيانات خادم الإدارة. قد تحتاج إلى تخزين بعض الأحداث لفترة أطول أو أقصر من تلك التي حددتها القيم الافتراضية. يمكنك تغيير الإعدادات الافتراضية لمدّة التخزين لحدث.

إذا لم تكن مهتمًا بتخزين بعض الأحداث في قاعدة بيانات خادم الإدارة، يمكنك تعطيل الإعداد المسؤول عن ذلك في سياسة خادم الإدارة وسياسة تطبيق Kaspersky أو في خصائص خادم الإدارة (لأحداث خادم الإدارة فقط). سيقلل هذا من عدد أنواع الأحداث في قاعدة البيانات.

لكما زادت مدة تخزين حدث، زادت سرعة وصول قاعدة البيانات إلى أقصى سعة لها. رغم ذلك، تتيح لك فترة التخزين الطويلة لحدث إجراء مهام المراقبة وإعداد التقارير لفترة أطول.

لتحديد فترة التخزين لحدث في قاعدة بيانات خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.

2. انقر على اسم السياسة المطلوبة.

يمكنك تحديد سياسة لتطبيق Kaspersky مُدار أو عميل شبكة اتصال أو خادم إدارة. وبالنسبة لخادم الإدارة، يمكنك أيضًا تكوين مدة تخزين الأحداث من خلال النقر على أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

3. حدد علامة تبويب **Event configuration** .

يتم عرض قائمة بأنواع الأحداث ذات الصلة بقسم **Critical**. وإذا لزم الأمر، يمكنك الانتقال إلى قسم **Functional failure** أو **Warning** أو **Info**.

4. في قائمة أنواع الأحداث في الجزء الأيمن، انقر على رابط الحدث الذي ترغب في تغيير فترة تخزينه.

في قسم **Event registration** في النافذة التي تفتح، يتم تفعيل زر التبديل **Store in the Administration Server database for (days)**.

5. في خانة التحرير أسفل زر التبديل هذا، أدخل عدد أيام تخزين الحدث.

6. إذا كنت لا ترغب في تخزين حدث في قاعدة بيانات خادم الإدارة، قم بتعطيل خيار **Store in the Administration Server database for (days)**.

> إذا قمت بتكوين أحداث خادم الإدارة في نافذة خصائص خادم الإدارة، وإذا كانت إعدادات الحدث مقفولة في سياسة خادم إدارة Kaspersky Security Center، لا يمكنك إعادة تحديد قيمة فترة التخزين لحدث.

7. انقر فوق **OK**، ثم بعد إغلاق الجزء الأيسر، انقر فوق الزر **حفظ**.

يتم إغلاق نافذة خصائص السياسة.

من الآن فصاعدًا، عندما يتلقى خادم الإدارة الأحداث من النوع المحدد ويخزنها، سيكون لديهم مدة التخزين المتغيرة. لا يغير خادم الإدارة مدة التخزين للأحداث المتلقاة مسبقًا.

أحداث مكونات Kaspersky Security Center

يحتوي كل مكون من مكونات Kaspersky Security Center على مجموعة من أنواع الأحداث خاصة به. يقوم هذا القسم بإدراج أنواع الأحداث التي تقع في خادم إدارة Kaspersky Security Center، وفي عميل الشبكة، وخادم iOS MDM. أنواع الأحداث التي تظهر في تطبيقات Kaspersky غير مدرجة في هذا القسم.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

بنية البيانات لوصف نوع الحدث

بالنسبة لكل أنواع الأحداث، يتوفر اسم العرض والمعرف (ID) والرمز بالحروف الأبجدية والوصف ومدة التخزين الافتراضية.

- **اسم العرض لنوع الحدث**. يتم عرض هذا النص في Kaspersky Security Center عند قيامك بتكوين الأحداث وعند حدوثها.
- **مُعرّف نوع الحدث**. يتم استخدام هذا الرمز الرقمي عند قيامك بمعالجة الأحداث باستخدام أدوات تابعة لجهات خارجية لتحليل الأحداث.
- **نوع الحدث** (رمز بالحروف الأبجدية). يتم استخدام هذا الرمز عند قيامك باستعراض ومعالجة الأحداث باستخدام طرق العرض العامة المتوفرة في قاعدة بيانات Kaspersky Security Center وعندما يتم تصدير الأحداث إلى نظام SIEM.
- **الوصف**. يحتوي هذا النص على المواقف التي يحدث فيها الحدث وما يمكنك القيام به في مثل هذه الحالة.
- **مدة التخزين الافتراضية**. هذا هو عدد الأيام التي يتم خلالها تخزين الحدث في قاعدة بيانات خادم الإدارة ويتم عرضه في قائمة الأحداث على خادم الإدارة. بعد انقضاء هذه الفترة، يتم حذف الحدث. إذا كانت قيمة وقت تخزين الحدث هي عدم التخزين، فإنه يتم اكتشاف هذه الأحداث ولكن لا يتم عرضها في قائمة الأحداث على خادم الإدارة. إذا قمت بتكوين الإعدادات الخاصة بك لحفظ مثل هذه الأحداث في سجل أحداث نظام التشغيل، فيمكنك العثور عليها هناك.

  يمكنك تغيير مدّة التخزين للأحداث:

  - وحدة تحكم الإدارة: تعيين مدة التخزين لحدث
  - Kaspersky Security Center Web Console: تعيين مدة تخزين حدث

قد تتضمن البيانات الأخرى الحقول التالية:

- **event_id**: رقم فريد للحدث في قاعدة البيانات يتم إنشاؤه وتخصيصه تلقائيًا؛ لا يجب الخلط بينه وبين **معرف نوع الحدث**.
- **task_id**: معرّف المهمة التي تسببت في الحدث (إن وجد)
- **الخطورة**: أحد مستويات الخطورة التالية (بترتيب تصاعدي للخطورة):

  0) مستوى خطورة غير صالح

  1) معلومات

  2) تحذير

  3) خطأ

  4) خطير

أحداث خادم الإدارة

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بخادم الإدارة.

الأحداث الحرجة لخادم الإدارة

يوضح الجدول أدناه أنواع أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **حرج**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

إذا حددت المنفذ في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة، فإن **Kaspersky Security Center ينشر مقاييسه** والأحداث المهمة التي سيحصل عليها نظام Prometheus، وهو نظام للمراقبة والتنبيه. ويحصل نظام Prometheus على المقاييس والأحداث الحرجة، ثم ينشئ تنبيهات لكل حدث.

// Kaspersky Security Center common counters—KL.KSC.Common

"klserver errors" ,"counter" ,"xdr_klserver_errors"

"klserver api calls time" ,"counter" ,"xdr_klserver_api_calls_time"

// Transport counters set—KL.KSC.Transport

"number of all connections" ,"counter" ,"ksc_Transport__Number_of_all_connections"

"number of all Network Agent connection" ,"counter" ,"ksc_Transport__Number_of_all_nagent_connection"

number of controlled Network Agent" ,"counter" ,"ksc_Transport__Number_of_controlled_nagent_connections" "connections

"total active devices count" ,"gauge" ,"ksc_Transport__Total_active_hosts_count"

"number of pings processed" ,"counter" ,"ksc_Transport__Number_of_pings_processed"

"number of pings rejected" ,"counter" ,"ksc_Transport__Number_of_pings_rejected"

"number of ping processing errors" ,"counter" ,"ksc_Transport__Number_of_ping_processing_errors"

"number of TCP connections accepted" ,"counter" ,"ksc_Transport__Number_of_TCP_connections_accepted"

"number of failed TCP connections" ,"counter" ,"ksc_Transport__Number_of_failed_TCP_connections"

"bytes sent by TCP" ,"counter" ,"ksc_Transport__Bytes_sent_by_TCP"

"bytes received by TCP" ,"counter" ,"ksc_Transport__Bytes_received_by_TCP"

"number of GetNextFileChunk requests" ,"counter" ,"ksc_Transport__Number_of_GetNextFileChunk_requests"

"number of GetNextFileChunk rejected" ,"counter" ,"ksc_Transport__Number_of_GetNextFileChunk_rejected"

bytes transmitted through" ,"counter" ,"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk" "GetNextFileChunk

// Events delivery counters set—KL.KSC.Events

"number of event bulks processed" ,"counter" ,"ksc_Events__Number_of_event_bulks_processed"

"number of event bulks rejected" ,"counter" ,"ksc_Events__Number_of_event_bulks_rejected"

"number of event bulks processing errors" ,"counter" ,"ksc_Events__Number_of_event_bulks_processing_errors"

number of event bulks processing just" ,"gauge" ,"ksc_Events__Number_of_event_bulks_processing_just_now" "now

"number of events processed" ,"counter" ,"ksc_Events__Number_of_events_processed"

"number of events rejected" ,"counter" ,"ksc_Events__Number_of_events_rejected"

"number of events processing errors" ,"counter" ,"ksc_Events__Number_of_events_processing_errors"

"number of events processing just now" ,"gauge" ,"ksc_Events__Number_of_events_processing_just_now"

Kaspersky Security Center resources usage—KL.KSC.Resources //

"CPU time in user mode" ,"counter" ,"ksc_Resources__CPU_time_in_user_mode"

"CPU time in kernel mode" ,"counter" ,"ksc_Resources__CPU_time_in_kernel_mode"

"process ID of klserver" ,"gauge" ,"ksc_Resources__PID_of_klserver_process"

"process ID of klnagent" ,"gauge" ,"ksc_Resources__PID_of_klnagent_process"

"available disk user quota for server data" ,"gauge" ,"ksc_Resources__Available_disk_user_quota_for_server_data"

"available disk user quota for packages" ,"gauge" ,"ksc_Resources__Available_disk_user_quota_for_packages"

"current OpenAPI threads count" ,"counter" ,"ksc_Resources__Current_OpenAPI_threads_count"

"maximum OpenAPI threads count" ,"counter" ,"ksc_Resources__Maximum_OpenAPI_threads_count"

KL.KSC.NLST //

List of server transactions—KL.KSC.NLST.Trans.Common //

"current transactions count" ,"gauge" ,"ksc_NLST__Common__Current_transactions_count"

"transactions queue full" ,"gauge" ,"ksc_NLST__Common__Transactions_queue_ful"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Common__Transactions_queue_near_to_ful"

Application Control link—KL.KSC.NLST.InvAppCtrlLink //

"items changed" ,"gauge" ,"ksc_NLST__Application_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Application_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Application_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Application_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_in_queue"

Software Inventory—KL.KSC.NLST.InvSoft //

"items changed" ,"gauge" ,"ksc_NLST__Software_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Software_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Software_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Software_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Software_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Software_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Software_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Software_inventory__transactions_in_queue"

Hardware Inventory—KL.KSC.NLST.InvHard //

"items changed" ,"gauge" ,"ksc_NLST__Hardware_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Hardware_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Hardware_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Hardware_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Hardware_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Hardware_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Hardware_inventory__transactions_in_queue"

Device Control—KL.KSC.NLST.DevCtrl //

"items changed" ,"gauge" ,"ksc_NLST__Device_control__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Device_control__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Device_control__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Device_control__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Device_control__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Device_control__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Device_control__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Device_control__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Device_control__transactions_in_queue"

Mobile Device Management—KL.KSC.NLST.MDM //

"items changed" ,"gauge" ,"ksc_NLST__Mobile_device_management__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Mobile_device_management__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Mobile_device_management__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Mobile_device_management__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Mobile_device_management__transactions_queue_full"

transactions queue near" ,"gauge" ,"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full" "to full

"list is pending" ,"gauge" ,"ksc_NLST__Mobile_device_management__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Mobile_device_management__transactions_in_queue"

Device management emails—KL.KSC.NLST.MDMmails //

"items changed" ,"gauge" ,"ksc_NLST__Device_management_emails__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Device_management_emails__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Device_management_emails__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Device_management_emails__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Device_management_emails__transactions_queue_full"

transactions queue near" ,"gauge" ,"ksc_NLST__Device_management_emails__transactions_queue_near_to_full" "to full

"list is pending" ,"gauge" ,"ksc_NLST__Device_management_emails__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Device_management_emails__transactions_in_queue"

Application Control—KL.KSC.NLST.AppCtrl //

"items changed" ,"gauge" ,"ksc_NLST__Application_control__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Application_control__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Application_control__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Application_control__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Application_control__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Application_control__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Application_control__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Application_control__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Application_control__transactions_in_queue"

"items changed" ,"gauge" ,"ksc_NLST__Application_inventory__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Application_inventory__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Application_inventory__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Application_inventory__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Application_inventory__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Application_inventory__transactions_in_queue"

Data protection errors—KL.KSC.NLST.DPEErrors //

"items changed" ,"gauge" ,"ksc_NLST__Data_protection_errors__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Data_protection_errors__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Data_protection_errors__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Data_protection_errors__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Data_protection_errors__transactions_queue_full"

transactions queue near to" ,"gauge" ,"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full" "full

"list is pending" ,"gauge" ,"ksc_NLST__Data_protection_errors__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Data_protection_errors__transactions_in_queue"

iOS Mobile Device Management—KL.KSC.NLST.iOsMDM //

"items changed" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__change_item_operations"

list is disabled due" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize"
"to oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__transactions_queue_full"

transactions queue" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full"
"near to full

"list is pending" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__iOS_mobile_device_management__transactions_in_queue"

Vulnerability assessment and patch management—KL.KSC.NLST.Vapm //

"items changed" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items"

change" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations"
"item operations

list" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize"
"is disabled due to oversize

,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full"
"transactions queue full"

,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full"
"transactions queue near to full"

"list is pending" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending"

transactions" ,"gauge" ,"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue"
"in queue

Vulnerability assessment—KL.KSC.NLST.Va //

"items changed" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__transactions_queue_full"

transactions queue near to" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full" "full

"list is pending" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Vulnerability_assesment__transactions_in_queue"

Virtual machines—KL.KSC.NLST.VM //

"items changed" ,"gauge" ,"ksc_NLST__Virtual_machines__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Virtual_machines__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Virtual_machines__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Virtual_machines__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Virtual_machines__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Virtual_machines__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Virtual_machines__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Virtual_machines__transactions_in_queue"

Windows Update—KL.KSC.NLST.WUS //

"items changed" ,"gauge" ,"ksc_NLST__Windows_update__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Windows_update__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Windows_update__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Windows_update__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Windows_update__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Windows_update__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Windows_update__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Windows_update__transactions_in_queue"

CIP PLC—KL.KSC.NLST.CIP_PLC //

"items changed" ,"gauge" ,"ksc_NLST__CIP_PLC__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__CIP_PLC__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__CIP_PLC__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__CIP_PLC__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__CIP_PLC__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__CIP_PLC__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__CIP_PLC__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__CIP_PLC__transactions_in_queue"

Network Agent Network Scan—KL.KSC.NLST.NagentNetScan //

"items changed" ,"gauge" ,"ksc_NLST__Network_scan__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Network_scan__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Network_scan__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Network_scan__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Network_scan__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Network_scan__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Network_scan__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Network_scan__transactions_in_queue"

Adaptive Security—KL.KSC.NLST.AS //

"items changed" ,"gauge" ,"ksc_NLST__Adaptive_security__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Adaptive_security__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Adaptive_security__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Adaptive_security__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Adaptive_security__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Adaptive_security__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Adaptive_security__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Adaptive_security__transactions_in_queue"

Adaptive Security State—KL.KSC.NLST.ASS //

"items changed" ,"gauge" ,"ksc_NLST__Adaptive_security_state__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Adaptive_security_state__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Adaptive_security_state__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Adaptive_security_state__change_item_operations"

list is disabled due to" ,"gauge" ,"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize" "oversize

"transactions queue full" ,"gauge" ,"ksc_NLST__Adaptive_security_state__transactions_queue_full"

transactions queue near to" ,"gauge" ,"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full" "full

"list is pending" ,"gauge" ,"ksc_NLST__Adaptive_security_state__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Adaptive_security_state__transactions_in_queue"

Kill Chain—KL.KSC.NLST.KillChain //

"items changed" ,"gauge" ,"ksc_NLST__Kill_chain__items_changed"

"items deleted" ,"gauge" ,"ksc_NLST__Kill_chain__items_deleted"

"items ()DeleteAll" ,"gauge" ,"ksc_NLST__Kill_chain__DeleteAll_items"

"change item operations" ,"gauge" ,"ksc_NLST__Kill_chain__change_item_operations"

"list is disabled due to oversize" ,"gauge" ,"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize"

"transactions queue full" ,"gauge" ,"ksc_NLST__Kill_chain__transactions_queue_full"

"transactions queue near to full" ,"gauge" ,"ksc_NLST__Kill_chain__transactions_queue_near_to_full"

"list is pending" ,"gauge" ,"ksc_NLST__Kill_chain__list_is_pending"

"transactions in queue" ,"gauge" ,"ksc_NLST__Kill_chain__transactions_in_queue"

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تم تجاوز حد الترخيص	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	يتحقق Kaspersky Security Center مرة واحدة يوميًا من تجاوز حد الترخيص. تحدث الأحداث من هذا النوع عند اكتشاف خادم الإدارة حدوث تجاوز لبعض قيود الترخيص بواسطة تطبيقات Kaspersky المثبتة على الأجهزة العميلة وكذلك في حال تجاوز عدد وحدات الترخيص المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد لنسبة 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص. حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). يحدد Kaspersky Security Center القواعد المُستخدمة لإنشاء أحداث عند تجاوز حد الترخيص.	180 يومًا
انتشار الفيروسات	26 (للحماية من تهديدات الملفات)	GNRL_EV_VIRUS_OUTBREAK	تقع الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة قصيرة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة اليتي سيتم تشغيلها عند وقوع هذا الحدث.	180 يومًا
انتشار الفيروسات	27 (للحماية من تهديدات البريد)	GNRL_EV_VIRUS_OUTBREAK	تقع الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة قصيرة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة اليتي سيتم تشغيلها عند وقوع هذا الحدث.	180 يومًا
انتشار الفيروسات	28 (لجدار الحماية)	GNRL_EV_VIRUS_OUTBREAK	تقع الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة قصيرة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة اليتي سيتم تشغيلها عند وقوع هذا الحدث.	180 يومًا
أصبح الجهاز غير مُدار	4111	KLSRV_HOST_OUT_CONTROL	تقع الأحداث من هذا النوع في حالة وجود أي جهاز مُدار مرئيًا على الشبكة، ولكنه غير متصل بخادم الإدارة لفترة محددة. تعرف على ما يمنع التشغيل السليم لعميل الشبكة على الجهاز. تتضمن الأسباب المحتملة حدوث مشكلات في الشبكة وإزالة عميل الشبكة من الجهاز.	180 يومًا
حالة الجهاز حرج	4113	KLSRV_HOST_STATUS_CRITICAL	تحدث الأحداث من هذا النوع عندما يتم تعيين أي جهاز مُدار للحالة حرج. يمكنك تكوين الشروط التي يتم من خلالها تغيير حالة الجهاز إلى حرجة.	180 يومًا
تمت إضافة ملف المفتاح إلى قائمة الرفض	4124	KLSRV_LICENSE_BLACKLISTED	تقع الأحداث من هذا النوع عندما يضيف برنامج Kaspersky رمز التفعيل أو ملف المفتاح الذي تستخدمه في قائمة الرفض. تواصل مع الدعم الفني للحصول على المزيد من التفاصيل.	180 يومًا
وضع الوظائف المحدودة	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	تحدث الأحداث من هذا النوع عند قيام Kaspersky Security Center ببدء التشغيل باستخدام الوظائف الأساسية، دون إدارة الثغرات الأمنية والتصحيحات وكذلك دون مزايا إدارة الجهاز المحمول. في ما يلي أسباب وقوع الحدث والاستجابات المناسبة له: • لقد انتهت فترة الترخيص. يقدم ترخيص لاستخدام وضع الوظائف الكاملة لـ Kaspersky Security Center (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). • يقوم خادم الإدارة بإدارة عدد أجهزة أكبر من المحدد من قبل حد الترخيص. قم بنقل الأجهزة من مجموعات الإدارة الخاصة بخادم الإدارة إلى تلك الخاصة بخادم إدارة آخر (إذا سمح حد الترخيص الخاص بخادم الإدارة الأخر).	180 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
ستنتهي فترة صلاحية الترخيص قريبًا	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	تحدث أحداث من هذا النوع عندما يقترب تاريخ انتهاء صلاحية الترخيص التجاري. يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز تاريخ انتهاء صلاحية الترخيص أم لا بمعدل مرة يوميًا. يتم نشر أحداث من هذا النوع قبل 30 يوم و15يوم و 5 أيام ويوم واحد من تاريخ انتهاء صلاحية الترخيص. لا يمكنك تغيير عدد الأيام. إذا تم إيقاف تشغيل خادم الإدارة في اليوم المحدد قبل تاريخ انتهاء صلاحية الترخيص، فلن يتم نشر الحدث حتى اليوم التالي. عند انتهاء صلاحية الترخيص التجاري، يوفر Kaspersky Security Center الوظائف الأساسية فقط. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تأكد من إضافة مفتاح ترخيص احتياطي إلى خادم الإدارة. • إذا كنت تستخدم اشتراكًا، فتأكد من تجديده. يتم تجديد الاشتراك غير المحدود تلقائيًا في حالة الدفع المسبق لموفر الخدمة في المواعيد المحددة.	180 يومًا
انتهت صلاحية الشهادة	4132	KLSRV_CERTIFICATE_EXPIRED	تقع الأحداث من هذا النوع عند انتهاء صلاحية شهادة العميل على الأجهزة المحمولة.	180 يومًا
انتهت صلاحية شهادة خادم الإدارة.	6129	ServerCertificateExpired	تقع الأحداث من هذا النوع عند انتهاء صلاحية شهادات خادم الإدارة للأجهزة المحمولة وأجهزة UEFI. تحتاج إلى تحديث الشهادة منتهية الصلاحية.	180 يومًا
تم إبطال تحديثات الوحدات النمطية لتطبيق Kaspersky	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	تحدث الأحداث من هذا النوع في حالة إبطال التحديثات المستمرة (يتم عرض حالة الإبطال لتلك التحديثات) بواسطة متخصصين فنيين في Kaspersky؛ لأنه على سبيل المثال يلزم تحديثها إلى إصدار أحدث. يتعلق الحدث بتصحيحات Kaspersky Security Center ولا يتعلق بالوحدات النمطية الخاصة بتطبيقات Kaspersky المُدارة. يقدم الحدث السبب الذي يؤدي إلى عدم تثبيت التحديثات المستمرة.	180 يومًا
Audit: Export to SIEM failed	5130	KLAUD_EV_SIEM_EXPORT_ERROR	تحدث أحداث من هذا النوع عند فشل تصدير الأحداث إلى نظام SIEM بسبب خطأ في الاتصال بنظام SIEM.	180 يومًا

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

يوضح الجدول أدناه أنواع أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **خلل وظيفي**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
حدث خطأ وقت التشغيل	4125	KLSRV_RUNTIME_ERROR	تحدث الأحداث من هذا النوع بسبب حدوث مشكلات غير معروفة. وفي الغالب ما تكون عبارة عن مشكلات DBMS، ومشكلات في الشبكة، ومشكلات أخرى في البرامج والأجهزة. يمكن العثور على تفاصيل الحدث في وصف الحدث.	180 يومًا
تم تجاوز حد عمليات تثبيت إحدى مجموعات التطبيقات المرخصة	4126	KLSRV_INVLICPROD_EXCEDED	ينشئ خادم الإدارة أحداث من هذا النوع بشكل دوري (كل ساعة). تحدث الأحداث من هذا النوع في حالة قيامك بإدارة مفاتيح الترخيص لتطبيقات تابعة لجهات خارجية في Kaspersky Security Center وكذلك إذا تجاوز عدد عمليات التثبيت الحد الذي تم تعيينه بواسطة مفتاح الترخيص التابع لجهة خارجية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. قم بحذف التطبيق التابع لجهة خارجية من الأجهزة التي لا يستخدم عليها التطبيق. • قم باستخدام ترخيص تابع لجهة خارجية لعدد أجهزة أكثر. يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة. تشتمل مجموعة التطبيقات المرخصة على التطبيقات التي تفي بالمعايير المحددة بواسطتك.	180 يومًا
فشل استقصاء قطاع السحابة	4143	KLSRV_KLCLOUD_SCAN_ERROR	تحدث الأحداث من هذا النوع عندما يفشل خادم الإدارة في استقصاء مقطع شبكة في بيئة سحابية . اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقًا لذلك.	غير مخزنة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
فشل نسخ التحديثات إلى المجلد المحدد	4123	KLSRV_UPD_REPL_FAIL	تحدث الأحداث من هذا النوع عند القيام بنسخ تحديثات البرنامج إلى مجلد (مجلدات) إضافية مشتركة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا كان يحتوي حساب المستخدم المخصص للحصول على إمكانية الوصول إلى المجلد (المجلدات) على أذن كتابي أم لا. • تحقق مما إذا تم تغيير اسم المستخدم و / أو كلمة المرور الخاصة بالمجلد أم لا. • تحقق من الاتصال بالإنترنت لأنه قد يكون السبب في حدوث هذا الحدث. اتبع التعليمات للقيام بتحديث قواعد البيانات والوحدات النمطية للبرامج.	180 يومًا
لا توجد مساحة فارغة على القرص	4107	KLSRV_DISK_FULL	تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة. قم بتحرير مساحة القرص على الجهاز.	180 يومًا
المجلد المشترك غير متاح	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	تحدث الأحداث من هذا النوع في حال عدم توافر المجلد المشترك لخادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا تم تشغيل خادم الإدارة وتوافره (حيث يوجد المجلد المشترك) أم لا. • تحقق مما إذا تم تغيير اسم المستخدم و / أو كلمة المرور الخاصة بالمجلد أم لا. • تحقق من الاتصال بالشبكة.	180 يومًا
قاعدة بيانات خادم الإدارة غير متوفرة	4109	KLSRV_DATABASE_UNAVAILABLE	تحدث الأحداث من هذا النوع في حال أصبحت قاعدة بيانات خادم الإدارة غير متاحة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا كان الخادم البعيد الذي يحتوي على خادم SQL المثبت متاحًا أم لا. • اعرض سجلات DBMS لمعرفة سبب عدم توافر قاعدة بيانات خادم الإدارة. على سبيل المثال، بسبب الصيانة الوقائية قد يكون الخادم البعيد الذي يحتوي على خادم SQL غير متاح.	180 يومًا
لا توجد مساحة فارغة في قاعدة بيانات خادم الإدارة	4110	KLSRV_DATABASE_FULL	تحدث الأحداث من هذا النوع في حالة عدم توافر مساحة فارغة في قاعدة بيانات خادم الإدارة. لا يقوم خادم الإدارة بإداء وظيفته عند وصول قاعدة البيانات الخاصة به إلى سعته وكذلك عند استحالة إجراء المزيد من التسجيلات في قاعدة البيانات. فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـDBMS التي تستخدمها، والاستجابات المناسبة للحدث: • إنك تستخدم خادم SQL Server Express Edition DBMS: في وثيقة SQL Server Express، قم بفحص حد حجم قاعدة البيانات للإصدار الذي تستخدمه. من المحتمل أنه قد تجاوزت قاعدة بيانات خادم الإدارة الخاصة بك حد حجم قاعدة البيانات. يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. في قاعدة بيانات خادم الإدارة، توجد أحداث تجاوز عددها الحد الأقصى أرسلها مكون التحكم في التطبيقات. يمكنك تغيير إعدادات سياسة Kaspersky Endpoint Security for Windows المتعلقة بتخزين حدث التحكم في التطبيقات في قاعدة بيانات خادم الإدارة. • إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition: لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. استعرض المعلومات عند تحديد DBMS.	180 يومًا

أحداث التحذير لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **تحذير**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تم اكتشاف حدث متكرر		KLSRV_EVENT_SPAM_EVENTS_DETECTED	تقع الأحداث من هذا النوع عندما يكتشف خادم الإدارة حدثًا متكررًا على جهاز مُدار. راجع القسم التالي للحصول على التفاصيل: منع الأحداث المتكررة.	90 يومًا
تم تجاوز حد الترخيص	4098	KLSRV_EV_LICENSE_CHECK_100_110	يتحقق Kaspersky Security Center مرة واحدة يوميًا من تجاوز حد الترخيص. تحدث الأحداث من هذا النوع عند اكتشاف خادم الإدارة حدوث تجاوز لبعض قيود الترخيص بواسطة تطبيقات Kaspersky المثبتة على الأجهزة العميلة وكذلك في حال كان عدد وحدات الترخيص المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد يشكل من 100% إلى 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص. حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). يحدد Kaspersky Security Center القواعد المُستخدمة لإنشاء أحداث عند تجاوز حد الترخيص.	90 يومًا
ظل الجهاز غير نشط على الشبكة لوقت طويل	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	تحدث الأحداث من هذا النوع عندما يظهر الجهاز المُدار عدم النشاط لبعض الوقت. يحدث هذا غالبًا عند إيقاف تشغيل الجهاز المُدار. يمكنك الاستجابة للحدث من خلال الطرق التالية: • إزالة الجهاز من قائمة الأجهزة المدارة تلقائيًا. • حدد الفاصل الزمني الذي يتم بعده إنشاء الحدث **ظل الجهاز غير نشط على الشبكة لوقت طويل** باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center Web Console. • حدد الفاصل الزمني الذي يتم بعده إزالة الجهاز تلقائيًا من المجموعة باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center Web Console.	90 يومًا
تعارض في أسماء الجهاز	4102	KLSRV_EVENT_HOSTS_CONFLICT	تحدث الأحداث من هذا النوع عندما يعتبر خادم الإدارة جهازين مُدارين أو أكثر كجهاز واحد. يحدث هذا غالبًا عند استخدام محرك أقراص ثابت مستنسخ لنشر البرامج على الأجهزة المُدارة وبدون تحويل عميل الشبكة إلى وضع استنساخ القرص المخصص على جهاز مرجعي. لتجنب هذه المشكلة، قم بتبديل عميل الشبكة إلى وضع استنساخ القرص على جهاز مرجعي قبل استنساخ محرك الأقراص الثابتة لهذا الجهاز.	90 يومًا
حالة الجهاز 'تحذير'	4114	KLSRV_HOST_STATUS_WARNING	تحدث الأحداث من هذا النوع عندما يتم تعيين الحالة تحذير للجهاز المُدار. يمكنك تكوين الشروط التي يتم من خلالها تغيير حالة الجهاز إلى تحذير.	90 يومًا
سيتم تجاوز حد عمليات التثبيت لإحدى مجموعات التطبيقات المرخصة قريبًا	4127	KLSRV_INVLICPROD_FILLED	تحدث الأحداث من هذا النوع عندما يصل عدد عمليات التثبيت لتطبيقات الطرف الثالث المضمنة في مجموعة التطبيقات المرخصة إلى 90% من الحد الأقصى للقيمة المسموح بها المحددة في خصائص مفتاح الترخيص. يمكنك الاستجابة للحدث من خلال الطرق التالية: • إذا لم يكن تطبيق الطرف الثالث قيد الاستخدام على بعض الأجهزة المدارة، فاحذف التطبيق من هذه الأجهزة. • إذا كنت تتوقع أن يتجاوز عدد عمليات التثبيت لتطبيق الطرف الثالث الحد الأقصى المسموح به في المستقبل القريب، ففكر في الحصول على ترخيص جهة خارجية لعدد أكبر من الأجهزة مقدمًا. يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة.	90 يومًا
تم طلب شهادة	4133	KLSRV_CERTIFICATE_REQUESTED	تحدث الأحداث من هذا النوع عندما تفشل إعادة إصدار شهادة إدارة الأجهزة المحمولة تلقائيًا. قد تكون الأسباب والردود المناسبة على الحدث فيما يلي: • تم بدء إعادة الإصدار التلقائي للشهادة التي تم تعطيل خيار **إعادة إصدار الشهادة تلقائيًا إن أمكن**. قد يكون هذا بسبب حدوث خطأ أثناء إنشاء الشهادة. قد يلزم إعادة إصدار الشهادة يدويًا. • إذا كنت تستخدم تكاملاً مع بنية تحتية للمفتاح العام، فقد يكون السبب هو عدم وجود سمة SAM-Account-Name للحساب المستخدم للتكامل مع PKI ولإصدار الشهادة. راجع خصائص الحساب.	90 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تمت إزالة الشهادة	4134	KLSRV_CERTIFICATE_REMOVED	تحدث الأحداث من هذا النوع عندما يزيل المسؤول أي نوع من الشهادات (عامة، بريد، VPN) لإدارة جهاز المحمول. بعد إزالة الشهادة، ستفشل الأجهزة المحمولة المتصلة عبر هذه الشهادة في الاتصال بخادم الإدارة. قد يكون هذا الحدث مفيدًا عند التحقيق في الأعطال المرتبطة بإدارة الأجهزة المحمولة.	90 يومًا
تنتهي صلاحية الشهادة	6128	ServerCertificateExpiresSoon	تقع الأحداث من هذا النوع عند انتهاء صلاحية شهادات خادم الإدارة للأجهزة المحمولة وأجهزة UEFI. تحتاج إلى تحديث الشهادة منتهية الصلاحية.	90 يومًا
انتهت صلاحية شهادة أسماء نقاط الوصول	4135	KLSRV_APN_CERTIFICATE_EXPIRED	تحدث الأحداث من هذا النوع عند انتهاء صلاحية شهادة APN. تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.	غير مخزنة
ستنتهي صلاحية شهادة أسماء نقاط الوصول قريبًا	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	تحدث الأحداث من هذا النوع عندما يتبقى أقل من 14 يومًا قبل انتهاء صلاحية شهادة APN. عند انتهاء صلاحية شهادة APN، تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. نوصيك بجدولة تجديد شهادة أسماء نقاط الوصول (APNs) قبل تاريخ انتهاء الصلاحية.	غير مخزنة
فشل إرسال رسالة FCM إلى الجهاز المحمول	4138	KLSRV_GCM_DEVICE_ERROR	تقع الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Firebase Cloud Messaging (FMC) للاتصال بأجهزة الجوال المدارة بنظام تشغيل Android ويفشل خادم FMC في التعامل مع بعض الطلبات الواردة من خادم الإدارة. هذا يعني أن بعض الأجهزة المحمولة المدارة لن تتلقى إشعارًا فوريًا. اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقًا لذلك. لمزيد من المعلومات حول رموز HTTP المستلمة من خادم FMC والأخطاء ذات الصلة، يُرجى الرجوع إلى وثائق خدمة Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات").	90 يومًا
حدث خطأ في HTTP أثناء إرسال رسالة FCM إلى خادم FCM	4139	KLSRV_GCM_HTTP_ERROR	تقع الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Firebase Cloud Messaging (FMC) لتوصيل الأجهزة المحمولة المدارة بنظام التشغيل Android ويعود خادم FMC إلى طلب خادم الإدارة برمز HTTP غير 200 (موافق). قد تكون الأسباب والردود المناسبة على الحدث فيما يلي: • مشكلات من جانب خادم FMC. اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقًا لذلك. لمزيد من المعلومات حول رموز HTTP المستلمة من خادم FMC والأخطاء ذات الصلة، يُرجى الرجوع إلى وثائق خدمة Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات"). • مشاكل من جانب الخادم الوكيل (إذا كنت تستخدم خادمًا وكيلاً). اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقًا لذلك.	90 يومًا
فشل إرسال رسالة FCM إلى خادم FCM	4140	KLSRV_GCM_GENERAL_ERROR	تحدث الأحداث من هذا النوع بسبب أخطاء غير متوقعة من جانب خادم الإدارة عند العمل مع بروتوكول Firebase Cloud Messaging HTTP. اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقًا لذلك. إذا لم تتمكن من إيجاد حل لمشكلة ما بنفسك، فنوصيك بالاتصال بالدعم الفني لـ Kaspersky.	90 يومًا
توجد مساحة فارغة قليلة على القرص الصلب	4105	KLSRV_NO_SPACE_ON_VOLUMES	تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة. قم بتحرير مساحة القرص على الجهاز.	90 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
توجد مساحة فارغة قليلة في قاعدة بيانات خادم الإدارة	4106	KLSRV_NO_SPACE_IN_DATABASE	تحدث الأحداث من هذا النوع في حال أصبحت مساحة قاعدة بيانات خادم الإدارة محدودة للغاية. إذا لم يتم إصلاح الوضع، فستصل قاعدة بيانات خادم الإدارة إلى سعتها ولن يقوم خادم الإدارة بأداء وظيفته قريبًا. فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـ DBMS التي تستخدمها، والاستجابات المناسبة للحدث. إنك تستخدم خادم SQL Server Express Edition DBMS: • في وثيقة SQL Server Express، قم بفحص حد حجم قاعدة البيانات للإصدار الذي تستخدمه. من المحتمل أن قاعدة بيانات خادم الإدارة الخاصة بك على وشك الوصول إلى حد حجم قاعدة البيانات. • يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • في قاعدة بيانات خادم الإدارة، توجد أحداث تجاوز عددها الحد الأقصى أرسلها مكون التحكم في التطبيقات. يمكنك تغيير إعدادات سياسة Kaspersky Endpoint Security for Windows المتعلقة بتخزين حدث التحكم في التطبيقات في قاعدة بيانات خادم الإدارة. إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition: • لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. استعرض المعلومات عند تحديد DBMS.	90 يومًا
تمت مقاطعة الاتصال بخادم الإدارة الثانوي	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي. اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الثانوي واستجب وفقًا لذلك.	90 يومًا
تم قطع الاتصال بخادم الإدارة الأساسي	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي. اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الرئيسي واستجب وفقًا لذلك.	90 يومًا
تم تسجيل تحديثات جديدة للوحدات النمطية لتطبيق Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	تحدث أحداث من هذا النوع عندما يسجل خادم الإدارة تحديثات جديدة لبرنامج Kaspersky المثبت على الأجهزة المدارة التي تتطلب الموافقة ليتم تثبيتها. وافق على التحديثات أو ارفضها باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center Web Console.	90 يومًا
تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وبدأت عملية حذف الأحداث	4145	KLSRV_EVP_DB_TRUNCATING	تحدث الأحداث من هذا النوع عند بدء حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد الوصول إلى سعة قاعدة بيانات خادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.	غير مخزنة
تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وتم حذف الأحداث	4146	KLSRV_EVP_DB_TRUNCATED	تحدث الأحداث من هذا النوع عند حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد الوصول إلى سعة قاعدة بيانات خادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • قم بتغيير الحد الأقصى المسموح به لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.	غير مخزنة
التدقيق (فشل اختبار الاتصال بخادم SIEM)	5120	KLAUD_EV_SIEM_TEST_FAILED	تحدث الأحداث من هذا النوع عند فشل اتصال اختبار خادم SIEM.	30 يومًا
فشل إصدار الشهادة تلقائيا		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	يحدث هذا الحدث في حالة حدوث خطأ أثناء إنشاء شهادة عميل لجهاز محمول (جهاز يعمل بموجب بروتوكول محمول).	90 يومًا

الأحداث المعلوماتية لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية **معلومات**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث وتكوينها في خصائص خادم الإدارة. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.	ملاحظات
تم استنفاد أكثر من 90% من هذا المفتاح	4097	KLSRV_EV_LICENSE_CHECK_90	30 يومًا	
تم اكتشاف جهاز جديد	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 يومًا	
تمت إضافة جهاز إلى المجموعة تلقائيًا	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 يومًا	
Device has been automatically moved according to a rule	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 يومًا	
تمت إزالة الجهاز من المجموعة: غير نشط على الشبكة لمدة طويلة	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 يومًا	
سيتم تجاوز حد عمليات التثبيت قريبًا (تم استهلاك أكثر من 95%) لأحدى مجموعات التطبيقات المرخصة	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 يومًا	
تم العثور على ملفات ستُترسل إلى Kaspersky للتحليل	4131	KLSRV_APS_FILE_APPEARED	30 يومًا	
تم تغيير معرف مثيل FCM على هذا الجهاز المحمول	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 يومًا	
تم نسخ التحديثات بنجاح إلى المجلد المحدد	4122	KLSRV_UPD_REPL_OK	30 يومًا	
تم إنشاء الاتصال بخادم الإدارة الثانوي	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 يومًا	
تم إنشاء الاتصال بخادم الإدارة الأساسي	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 يومًا	
تم تحديث قواعد البيانات	4144	KLSRV_UPD_BASES_UPDATED	30 يومًا	
تدقيق: تم إنشاء اتصال بخادم الإدارة	4147	KLAUD_EV_SERVERCONNECT	30 يومًا	تقع الأحداث من هذا النوع عندما يتصل المستخدم بخادم الإدارة باستخدام وحدة تحكم الإدارة أو Kaspersky Security Center Web Console. وتتضمن هذه الأحداث معلومات عن عنوان IP للجهاز الذي تم تثبيت وحدة تحكم الإدارة المستندة إلى MMC أو خادم Kaspersky Security Center Web Console عليه.
تدقيق: تم تعديل الكائن	4148	KLAUD_EV_OBJECTMODIFY	30 يومًا	يتتبع هذا الحدث التغييرات في العناصر التالية: • مجموعة الإدارة • مجموعة الأمان • المستخدم • الحزمة • المهمة • سياسة • الخادم • الخادم الافتراضي
تدقيق: تم تغيير حالة الكائن	4150	KLAUD_EV_TASK_STATE_CHANGED	30 يومًا	على سبيل المثال، يقع هذا الحدث عندما تفشل مهمة مع وجود خطأ.
تدقيق: تم تعديل إعدادات المجموعة	4149	KLAUD_EV_ADMGROUP_CHANGED	30 يومًا	
Audit: Connection to Administration Server has been terminated	4151	KLAUD_EV_SERVERDISCONNECT	30 يومًا	

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.	ملاحظات
Audit: Object properties have been modified	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 يومًا	يتتبع هذا الحدث التغييرات في الخصائص التالية: • المستخدم • الترخيص • الخادم • الخادم الافتراضي
Audit: User permissions have been modified	4153	KLAUD_EV_OBJECTACLMODIFIED	30 يومًا	
تدقيق: تم استيراد مفاتيح التشفير أو تصديرها من خادم الإدارة	5100	KLAUD_EV_DPEKEYSEXPORT	30 يومًا	
Audit: Test connection to SIEM server succeeded	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 يومًا	يحدث هذا الحدث عندما ينجح اتصال اختبار خادم SIEM.
تم إنشاء الشهادة الاحتياطية		ServerReserveCertificateCreated	30 يومًا	يقع هذا الحدث عندما يتم إنشاء شهادة خادم الإدارة.
تجديد الشهادة		ServerCertificateRenewed	30 يومًا	يقع هذا الحدث عند تجديد شهادة خادم الإدارة.

يتم نشر حدثي **تم إنشاء الشهادة الاحتياطية** و**تجديد الشهادة** تلقائيًا بواسطة خادم الإدارة ويتم عرضهما في وحدة تحكم الإدارة فقط عند تنفيذ العمليات المقابلة لهذين الحدثين لشهادات خادم الإدارة للأجهزة المحمولة وأجهزة UEFI.

أحداث عميل الشبكة

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بعميل الشبكة.

أحداث الخلل الوظيفي لعميل الشبكة

يوضح الجدول أدناه أنواع حدث عميل شبكة Kaspersky Security Center التي تندرج ضمن مستوى خطورة **خلل وظيفي**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث الخلل الوظيفي لعميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
خطأ في تثبيت التحديث	7702	KLNAG_EV_PATCH_INSTALL_ERROR	تحديث الأحداث من هذا النوع في حالة عدم نجاح التحديث والتصحيح التلقائي لمكونات Kaspersky Security Center. لا يتعلق الحدث بعمليات تحديث تطبيقات Kaspersky المُدارة. اقرأ وصف الحدث. قد يرجع ظهور هذا الحدث إلى حدوث مشكلة في Windows على خادم الإدارة. إذا ذكر الوصف أي مشكلة تتعلق بتكوين Windows، فقم بحل هذه المشكلة.	30 يومًا
فشل تثبيت تحديث برامج الجهة الخارجية	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	تحدث الأحداث من هذا النوع في حالة استخدام مزايا إدارة الثغرات الأمنية والتصحيحات وإدارة جهاز المحمول وإذا لم ينجح تحديث البرامج التابعة لجهة خارجية. تحقق من صحة الرابط الخاص بالبرامج التابعة لجهة خارجية. اقرأ وصف الحدث.	30 يومًا
فشل تثبيت تحديثات Windows	7717	KLNAG_EV_WUA_INSTALL_ERROR	تحدث الأحداث من هذا النوع في حالة عدم نجاح تحديثات Windows. يمكنك تكوين تحديثات Windows في سياسة عميل الشبكة. اقرأ وصف الحدث. ابحث عن الخطأ في قاعدة معارف Microsoft. واتصل بالدعم الفني لـ Microsoft إذا تعذر عليك حل المشكلة بنفسك.	30 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
User management: errors	7723	KLNAG_EV_USR_MNG_ERR	حدث تحذير عام.	30 يومًا
Failed to restore sudoers file to reference value	7726	KLNAG_EV_SUDOER_RESTORED_ERR	يحتوي الحدث على وصف لخطأ استبدال ملف sudoers.	30 يومًا
Failed to install root certificates	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	يحتوي الحدث على وصف خطأ تثبيت الشهادات.	30 يومًا
Failed to remove root certificates	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	يحتوي الحدث على وصف لخطأ إزالة الشهادات.	30 يومًا

أحداث تحذير عميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تندرج ضمن مستوى خطورة **تحذير**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث تحذير عميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
ظهر تحذير أثناء تثبيت تحديث الوحدة النمطية للبرامج	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 يومًا
اكتمل تثبيت تحديث برامج الجهة الخارجية مع وجود تحذير	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 يومًا
تم تأجيل تثبيت تحديث برامج الجهة الخارجية	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 يومًا
حدثت مشكلة أمنية	549	GNRL_EV_APP_INCIDENT_OCCURED	30 يومًا
بدأ وكيل KSN. فشل فحص مدى توفر KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 يومًا
User management: warnings	7722	KLNAG_EV_USR_MNG_WRN	30 يومًا
Sudoers file found doesn't match reference value	7724	KLNAG_EV_SUDOER_DIFFERENT	30 يومًا

الأحداث المعلوماتية لعميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تندرج ضمن مستوى خطورة **معلومات**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

الأحداث المعلوماتية لعميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم تثبيت تحديث الوحدات النمطية للبرامج بنجاح	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 يومًا
بدأ تثبيت تحديث الوحدة النمطية للبرامج	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 يومًا
تم تثبيت التطبيق	7703	KLNAG_EV_INV_APP_INSTALLED	30 يومًا
تم إلغاء تثبيت التطبيق	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 يومًا
تم تثبيت التطبيق المراقب	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 يومًا
تم إلغاء تثبيت التطبيق المراقب	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 يومًا
تم تثبيت التطبيق التابع لجهة خارجية	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 يومًا
تمت إضافة جهاز جديد	7708	KLNAG_EV_DEVICE_ARRIVAL	30 يومًا
تمت إزالة الجهاز	7709	KLNAG_EV_DEVICE_REMOVE	30 يومًا
تم اكتشاف جهاز جديد	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 يومًا
تم اعتماد الجهاز	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 يومًا
مشاركة سطح المكتب لـ Windows: تمت قراءة الملف	7712	KLUSRLOG_EV_FILE_READ	30 يومًا
مشاركة سطح المكتب لـ Windows: تم تعديل الملف	7713	KLUSRLOG_EV_FILE_MODIFIED	30 يومًا

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
مشاركة سطح المكتب لـ Windows: تم بدء التطبيق	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 يومًا
مشاركة سطح المكتب لـ Windows: تم البدء	7715	KLUSRLOG_EV_WDS_BEGIN	30 يومًا
مشاركة سطح المكتب لـ Windows: تم الإيقاف	7716	KLUSRLOG_EV_WDS_END	30 يومًا
تم تثبيت تحديث برامج الجهات الخارجية بنجاح	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 يومًا
تم بدء تثبيت تحديث برامج الجهة الخارجية	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 يومًا
بدأ وكيل KSN. اكتمل فحص مدى توفر KSN بنجاح	7719	KSNPROXY_STARTED_CON_CHK_OK	30 يومًا
توقف وكيل شبكة KSN	7720	KSNPROXY_STOPPED	30 يومًا

أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لـ Kaspersky Security Center التي تندرج ضمن مستوى الخطورة **خلل وظيفي**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
فشل في طلب قائمة ملفات التعريف	PROFILELIST_COMMAND_FAILED	30 يومًا
فشل في تثبيت ملف التعريف	INSTALLPROFILE_COMMAND_FAILED	30 يومًا
فشل في إزالة ملف التعريف	REMOVEPROFILE_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة ملفات تعريف التزويد	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 يومًا
فشل في تثبيت ملف تعريف التزويد	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 يومًا
فشل في إزالة ملف تعريف التزويد	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة الشهادات الرقمية	CERTIFICATELIST_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة التطبيقات المثبتة	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 يومًا
فشل في طلب المعلومات العامة بشأن الجهاز المحمول	DEVICEINFORMATION_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة معلومات الأمان	SECURITYINFO_COMMAND_FAILED	30 يومًا
فشل في قفل الجهاز المحمول	DEVICELOCK_COMMAND_FAILED	30 يومًا
فشل في إعادة تعيين كلمة المرور	CLEARPASSCODE_COMMAND_FAILED	30 يومًا
فشل في مسح البيانات من الجهاز المحمول	ERASEDEVICE_COMMAND_FAILED	30 يومًا
فشل في تثبيت التطبيق	INSTALLAPPLICATION_COMMAND_FAILED	30 يومًا
فشل في تعيين رمز الاسترداد للتطبيق	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 يومًا
فشل في طلب قائمة التطبيقات المُدارة	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 يومًا
فشل في إزالة التطبيق المُدار	REMOVEAPPLICATION_COMMAND_FAILED	30 يومًا
تم رفض إعدادات التجوال	SETROAMINGSETTINGS_COMMAND_FAILED	30 يومًا
حدث خطأ في تشغيل التطبيق	PRODUCT_FAILURE	30 يومًا
تحتوي نتيجة الأمر على بيانات غير صالحة	MALFORMED_COMMAND	30 يومًا
فشل في إرسال إشعار الدفع	SEND_PUSH_NOTIFICATION_FAILED	30 يومًا

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
فشل في إرسال الأمر	SEND_COMMAND_FAILED	30 يومًا
لم يتم العثور على الجهاز	DEVICE_NOT_FOUND	30 يومًا

أحداث التحذير لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لـ Kaspersky Security Center التي تندرج ضمن مستوى خطورة **تحذير**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

أحداث التحذير لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم اكتشاف محاولة توصيل جهاز محمول مقفل	INACTICE_DEVICE_TRY_CONNECTED	30 يومًا
تم إزالة ملف التعريف	MDM_PROFILE_WAS_REMOVED	30 يومًا
تم اكتشاف محاولة إعادة استخدام شهادة عميل.	CLIENT_CERT_ALREADY_IN_USE	30 يومًا
تم اكتشاف جهاز غير مفعل.	FOUND_INACTIVE_DEVICE	30 يومًا
رمز الاسترداد مطلوب.	NEED_REDEMPTION_CODE	30 يومًا
تم تضمين ملف التعريف في سياسة تمت إزالتها من الجهاز.	UMDM_PROFILE_WAS_REMOVED	30 يومًا

الأحداث المعلوماتية لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM لـ Kaspersky Security Center التي تندرج ضمن مستوى خطورة **معلومات**.

لكل حدث يمكن إنشاؤه بواسطة أحد التطبيقات، يمكنك تحديد إعدادات الإخطار وإعدادات التخزين في علامة التبويب **Event configuration** في سياسة التطبيق. إذا كنت ترغب في تكوين إعدادات الإخطار لجميع الأحداث مرة واحدة، يمكنك تكوين إعدادات الإخطار العامة في خصائص خادم الإدارة.

الأحداث المعلوماتية لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم توصيل جهاز محمول جديد.	NEW_DEVICE_CONNECTED	30 يومًا
تم طلب قائمة بملفات التعريف بنجاح.	PROFILELIST_COMMAND_SUCCESSFULL	30 يومًا
تم تثبيت ملف التعريف بنجاح.	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تمت إزالة ملف التعريف بنجاح.	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة بملفات تعريف التزويد بنجاح.	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 يومًا
تم تثبيت ملف تعريف التزويد بنجاح.	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تم إزالة ملف تعريف التزويد بنجاح.	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة بالشهادات الرقمية بنجاح.	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة بالتطبيقات المثبتة بنجاح.	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 يومًا
تم طلب المعلومات العامة بشأن الجهاز المحمول بنجاح.	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 يومًا
تم طلب معلومات الأمان بنجاح.	SECURITYINFO_COMMAND_SUCCESSFULL	30 يومًا
تم قفل الجهاز المحمول بنجاح.	DEVICELOCK_COMMAND_SUCCESSFULL	30 يومًا
تمت إعادة تعيين كلمة المرور بنجاح.	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 يومًا
تم مسح البيانات من الجهاز المحمول.	ERASEDEVICE_COMMAND_SUCCESSFULL	30 يومًا
تم تثبيت التطبيق بنجاح.	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 يومًا
تم تعيين رمز الاسترداد الخاص بالتطبيق بنجاح.	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 يومًا
تم طلب قائمة التطبيقات المُدارة بنجاح.	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 يومًا

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تمت إزالة التطبيق المدار بنجاح.	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 يومًا
تم تطبيق إعدادات التجوال بنجاح.	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 يومًا

حظر الأحداث المتكررة

يوفر هذا القسم معلومات عن إدارة حظر الأحداث المتكررة وحول إزالة حظر الأحداث المتكررة.

حول حظر الأحداث المتكررة

التطبيق المُدار، على سبيل المثال، Kaspersky Endpoint Security for Windows، المثبت على جهاز مدار واحد أو عدة أجهزة مُدارة يمكنه إرسال الكثير من الأحداث من نفس النوع إلى خادم الإدارة. تلقي أحداث متكررة قد يؤدي إلى زيادة التحميل على قاعدة بيانات خادم الإدارة والكتابة فوق أحداث أخرى. يبدأ خادم الإدارة في حظر الأحداث الجماعية عندما يتجاوز مقدار كل الأحداث المستلمة الحد المحدد لقاعدة البيانات.

يحظر خادم الإدارة الأحداث المتكررة من الاستلام تلقائيًا. لا يمكنك حظر الأحداث المتكررة بنفسك، أو اختر الأحداث التي ترغب في حظرها.

إذا كنت ترغب في معرفة ما إذا تم حظر حدث أم لا، يمكنك عرض قائمة الإخطارات أو يمكنك معرفة ما إذا كان هذا الحدث موجودًا في قسم **حظر الأحداث المتكررة** في خصائص خادم الإدارة. في النافذة، يمكنك إجراء ما يلي:

- إذا كنت ترغب في منع الكتابة فوق قاعدة البيانات، يمكنك ذلك الاستمرار في حظر استلام مثل هذا النوع من الأحداث.
- إذا كنت ترغب، على سبيل المثال، في معرفة سبب إرسال الأحداث المتكررة إلى خادم الإدارة، يمكنك رفع الحظر عن الأحداث المتكررة والاستمرار في استقبال أحداث من هذا النوع على أي حال.
- إذا كنت ترغب في الاستمرار في تلقي الأحداث المتكررة حتى يتم حظرها مرة أخرى، يمكنك رفع الحظر عن الأحداث المتكررة.

إدارة حظر الأحداث المتكررة

يقوم خادم الإدارة بحظر التلقي التلقائي للأحداث المتكررة، ولكن يمكنك إلغاء الحظر والاستمرار في تلقي الأحداث المتكررة. يمكنك كذلك حظر تلقي الأحداث المتكررة التي قمت بإلغاء حظرها من قبل.

لإدارة منع الأحداث المتكررة:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد القسم **Blocking frequent events**.
3. في قسم **Blocking frequent events**:
   - إذا كنت ترغب في إلغاء حظر تلقي الأحداث المتكررة:
     a. حدد الأحداث المتكررة التي تريد إلغاء حظرها، ثم انقر فوق زر **Exclude**.
     b. انقر على زر **Save**.

- إذا كنت ترغب في حظر تلقي أحداث متكررة:

  a. حدد الأحداث المتكررة التي تريد حظرها، ثم انقر فوق زر **Block**.

  b. انقر على زر **Save**.

خادم الإدارة يستلم الأحداث المتكررة غير المحظورة ولا يستلم الأحداث المتكررة المحظورة.

إزالة حظر الأحداث المتكررة

يمكنك إزالة حظر الأحداث الجماعية والبدء في الاستلام حتى يقوم خادم الإدارة بحظر هذه الأحداث الجماعية مرة أخرى.

لإزالة حظر الأحداث المتكررة:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب **General**، حدد القسم **Blocking frequent events**.
3. في قسم **Blocking frequent events** حدد أنواع الأحداث المتكررة التي تريد إزالة الحظر لها.
4. انقر على الزر **Remove from blocking**.

بهذا تم حذف الحدث المتكرر من قائمة الأحداث الجماعية. سيستلم خادم الإدارة أحداثًا من هذا النوع.

الإخطارات وحالات الجهاز

يحتوي هذا القسم على معلومات حول كيفية عرض الإخطارات وتهيئة تسليم الإخطارات واستخدام حالات الجهاز وتمكين تغيير حالات الجهاز.

استخدام الإخطارات

تنبهك الإشعارات بشأن الأحداث، وتساعدك على تسريع استجاباتك لهذه الأحداث من خلال تنفيذ الإجراءات الموصى بها أو التي تراها مناسبة.

اعتمادًا على طريقة الإخطار المختارة، تتوفر أنواع الإخطارات التالية:

- إخطارات على الشاشة
- إخطارات عبر رسائل نصية قصيرة
- إخطارات عبر البريد الإلكتروني
- إخطارات عن طريق ملف تنفيذي أو نص

إخطارات على الشاشة

الإخطارات على الشاشة تحذرك من أحداث يجمعها مستويات الأهمية (حرجة وتحذير ومعلومات).

يمكن أن يكون للإخطارات على الشاشة إحدى هاتين الحالتين:

- تم مراجعته. هذه الحالة تعني أنك قد اتخذت الإجراءات الموصى بها للإخطار، أو قد خصصت هذه الحالة للإخطار يدويًا.
- لم يتم مراجعته. هذه الحالة تعني أنك لم تتخذ الإجراءات الموصى بها للإخطار، أو لم تخصص هذه الحالة للإخطار يدويًا.

بشكل افتراضي، قائمة الإخطارات تشمل الإخطارات بحالة لم يتم مراجعتها.

يمكنك مراقبة شبكة مؤسستك بعرض الإخطارات على الشاشة والاستجابة لها على الفور.

الإخطارات عبر البريد الإلكتروني أو الرسائل النصية القصيرة أو ملف تنفيذي أو نص

يوفر Kaspersky Security Center القدرة على مراقبة شبكة مؤسستك عن طريق إرسال إخطارات عن أي حدث تعتبره مهمًا. لأي حدث، يمكنك تكوين الإخطارات عبر البريد الإلكتروني أو الرسائل النصية القصيرة أو عن طريق تشغيل ملف تنفيذي أو نص.

عند استلام الإخطارات عبر البريد الإلكتروني أو الرسائل النصية القصيرة، يمكنك أخذ قرار في الاستجابة إلى حدث. يجب أن تكون هذه الاستجابة هي الأنسب لشبكة مؤسستك. بتشغيل ملف تنفيذي أو نص، أنت تحدد الاستجابة لحدث مسبقًا. يمكنك كذلك التفكير في تشغيل ملف تنفيذي أو نص كطريقة الاستجابة الرئيسية لحدث. بعد تشغيل الملف التنفيذي، يمكنك اتخاذ خطوات أخرى للاستجابة إلى الحدث.

عرض الإخطارات التي تظهر على الشاشة

يمكنك عرض الإخطارات على الشاشة بثلاث طرق:

- في **Monitoring & reporting** ← قسم **Notifications**. يمكنك هنا عرض الإخطارات المتعلقة بالفئات المحددة مسبقًا.
- في نافذة منفصلة يمكن فتحها مهما كان القسم الذي تستخدمه في تلك اللحظة. يمكنك في هذه الحالة وضع علامة على الإخطارات بأنها تمت مراجعتها.
- في عنصر الواجهة **Notifications by selected severity level** في **Monitoring & reporting** ← قسم **Dashboard**. يمكنك في عنصر الواجهة عرض إخطارات الأحداث المحدد لها مستويات الأهمية حرج أو تحذير.

يمكنك تنفيذ إجراءات، مثل أن يمكنك الاستجابة إلى حدث.

لعرض إخطارات من الفئات المحددة مسبقًا:

1. في القائمة الرئيسية، انتقل إلى **Notifications** ← **Monitoring & reporting**.

   يتم تحديد فئة **All notifications** في الجزء الأيسر، ويتم عرض جميع الإخطارات في الجزء الأيسر.

2. حدد إحدى الفئات في الجزء الأيسر:

   - **Deployment**
   - **Devices**
   - **Protection**
   - **Updates** (يشمل هذا الإخطارات عن تطبيقات Kaspersky المتوفرة للتنزيل والإخطارات عن تحديثات قاعدة بيانات مكافحة الفيروسات التي تم تنزيلها).
   - **Exploit Prevention**

- **Administration Server** (يشمل هذا الأحداث التي تتعلق بخادم الإدارة فقط)

- **Useful links** يشمل هذا روابط إلى موارد Kaspersky، مثل الدعم الفني من Kaspersky ومنتدى Kaspersky وصفحة تجديد الترخيص وموسوعة تكنولوجيا المعلومات من Kaspersky)

يتم عرض قائمة بإخطارات الفئة المحددة. تحتوي القائمة على ما يلي:

- الأيقونة المتعلقة بموضوع الإخطار: النشر ( )، الحماية ( )، التحديثات ( )، إدارة الجهاز ( )، منع الاستغلال ( )، خادم الإدارة ( ).

- مستوى أهمية الإشعار. يتم عرض إخطارات مستويات الأهمية التالية: **Critical notifications** ( )، و**Warning notifications** ( )، و**Info notifications**. يتم تجميع الإخطارات في القائمة بمستويات الأهمية.

- **Notification**. يحتوي هذا على وصف الإخطار.

- **Action** . يحتوي هذا على رابط لإجراء سريع ننصح باتخاذه. يمكنك على سبيل المثال بالنقر على هذا الرابط التقدم إلى المستودع وتثبيت تطبيقات الأمان على الأجهزة أو عرض قائمة بالأجهزة أو قائمة بالأحداث. بعد اتخاذ الإجراء الموصى به للإخطار، يتم تخصيص حالة تم مراجعته إلى هذا الإخطار.

- **Status registered** . يحتوي هذا على عدد الأيام أو الساعات التي مرت منذ لحظة تسجيل الإخطار على خادم الإدارة.

لعرض الإخطارات على الشاشة في نافذة منفصلة بمستوى الأهمية:

1. في أعلى الزاوية اليمنى من Kaspersky Security Center Web Console، انقر على أيقونة العلم ( ).

إذا كان أيقونة العلم به نقطة حمراء، يوجد إخطارات لم يتم مراجعتها.

ستفتح نافذة تسرد الإخطارات. بشكل افتراضي، يكون تبويب **All notifications** محددًا ويتم تجميع الإخطارات بمستوى الأهمية: حرج أو تحذير أو معلومات.

2. حدد تبويب**System**.

يتم عرض قائمة إخطارات مستويات الأهمية حرج ( ) وتحذير ( ). قائمة الإخطارات تشمل ما يلي:

- تحديد بالألوان. الإخطارات الحرجة تكون باللون الأحمر. الإخطارات التحذيرية تكون باللون الأصفر.

- الأيقونة التي تشير إلى موضوع الإخطار: النشر ( )، الحماية ( )، التحديثات ( )، إدارة الجهاز ( )، منع الاستغلال ( )، خادم الإدارة ( ).

- وصف الإخطار.

- أيقونة العلم. يكون أيقونة العلم باللون الرمادي إلى كان قد تم تخصيص حالة لم يتم مراجعته إلى الإخطارات. عندما تحدد أيقونة العلم الرمادي وتخسس حالة تم مراجعته إلى إخطار، يتغير لون الأيقونة إلى الأبيض.

- رابط الإجراء الموصى به. عندما تتخذ الإجراء الموصى به بعد النقر على الرابط، يتم تخصيص حالة تم مراجعته إلى الإخطار.

- عدد الأيام التي مرت منذ لحظة تسجيل الإخطار على خادم الإدارة.

3. حدد تبويب **More**.

يتم عرض قائمة إخطارات مستويات الأهمية معلومات.

تنظيم القائمة هو نفسه للقائمة في تبويب **System** (راجع الوصف أعلاه). الاختلاف الوحيد هو غياب تحديد الألوان.

يمكنك تصفية الإخطارات بالفاصل الزمني للتاريخ عند تسجيلها على خادم الإدارة. استخدم خانة الاختيار **Show filter** لإدارة عامل التصفية.

لعرض الإخطارات على الشاشة في عنصر الواجهة:

1. في قسم **Dashboard**، حدد **Add or restore web widget**.

2. في النافذة التي تفتح، انقر على فئة **Other** وحدد عنصر الواجهة **Notifications by selected severity level** ثم انقر على إضافة.

   سيظهر عنصر الواجهة الآن في تبويب **Dashboard**. بشكل افتراضي، يتم عرض إخطارات مستوى الأهمية حرج في عنصر الواجهة.

   يمكنك النقر على زر **الإعدادات** في عنصر الواجهة ثم تغيير إعدادات عنصر الواجهة لعرض إخطارات مستوى الأهمية تحذير. أو يمكنك إضافة عنصر واجهة آخر: **الإخطارات بمستوى الأهمية المحدد** مع مستوى الخطورة تحذير.

   يتم تحديد قائمة الإخطارات في عنصر الواجهة بحجمها، وتشمل إخطارين. هذا الإخطاران يتعلقان بآخر الأحداث.

قائمة الإخطارات في عنصر الواجهة تشمل ما يلي:

- الأيقونة المتعلقة بموضوع الإخطار: النشر ( )، الحماية ( )، التحديثات ( )، إدارة الجهاز ( )، منع الاستغلال ( )، خادم الإدارة ( ).
- وصف الإخطار مع رابط إلى الإجراء الموصى به. عندما تتخذ إجراء الموصى به بعد النقر على الرابط، يتم تخصيص حالة تم مراجعته إلى الإخطار.
- عدد الأيام أو عدد الساعات التي مرت منذ لحظة تسجيل الإخطار على خادم الإدارة.
- رابط الإخطارات الأخرى. عند النقر على هذا الرابط، يتم نقلك إلى عرض الإخطارات في قسم **Notifications** لقسم **Monitoring & reporting**.

حول حالات الجهاز

يخصص Kaspersky Security Center حالة لكل جهاز مُدار. تعتمد الحالة الخاصة على ما إذا كانت الشروط التي حددها المستخدم قد استوفيت أم لا. في بعض الحالات، عند تعيين حالة لجهازٍ ما، يأخذ Kaspersky Security Center في الاعتبار علامة رؤية الجهاز على الشبكة (انظر الجدول أدناه). على سبيل المثال: إذا تم تعيين الحالة حرج إلى جهاز مُدار بسبب عدم استيفاء شرط Databases are outdated ثم بعد ذلك تم تعيين علامة الرؤية للجهاز، يتم تعيين حالة موافق إلى الجهاز. إذا لم يعثر Kaspersky Security Center على جهاز على الشبكة في غضون ساعتين، سيتم تعيين علامة رؤية الجهاز إلى غير مرئي.

الحالات كما يلي:

- حرج أو حرج/مرئي
- تحذير أو تحذير/مرئي
- موافق أو موافق/مرئي

يسرد الجدول أدناه الشروط الافتراضية التي يجب استيفائها لتعيين الحالة حرج أو تحذير إلى جهاز، مع جميع القيم المحتملة.

شروط تعيين الحالة إلى الجهاز

الشرط	وصف الشرط	القيم المتوفرة
Security application is not installed	عميل الشبكة مثبّت على الجهاز، إلا أن تطبيق الأمان غير مثبّت.	• زر التبديل قيد التشغيل. • زر التبديل متوقف.
Too many viruses detected	تم العثور على بعض الفيروسات على الجهاز عن طريق تنفيذ إحدى مهام اكتشاف الفيروسات، على سبيل المثال مهمة فحص البرامج الضارة، ويتجاوز عدد الفيروسات التي تم العثور عليها القيمة المحددة.	أكثر من 0.
Real-time protection level differs from the level set by the Administrator	الجهاز مرئي على الشبكة، إلا أن مستوى الحماية في الوقت الحقيقي يختلف عن المستوى الذي حدده المسؤول (في الشرط) لحالة الجهاز.	• متوقف. • متوقف مؤقتًا. • قيد التشغيل.
Malware scan has not been performed in a long time	يكون الجهاز مرئيًا على الشبكة ويتم تثبيت تطبيق أمان على الجهاز، لكن لا يتم تشغيل أي من مهمة فحص البرامج الضارة ولا مهمة فحص محلية خلال الفاصل الزمني المحدد. لا ينطبق الشرط إلا على الأجهزة التي تمت إضافتها إلى قاعدة بيانات خادم الإدارة قبل 7 أيام أو أكثر.	أكثر من يوم واحد.
Databases are outdated	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لم يتم تحديث قواعد بيانات مكافحة الفيروسات على هذا الجهاز خلال الفاصل الزمني المحدد. لا ينطبق الشرط إلا على الأجهزة التي تمت إضافتها إلى قاعدة بيانات خادم الإدارة قبل يوم واحد أو أكثر.	أكثر من يوم واحد.

الشرط	وصف الشرط	القيم المتوفرة
Not connected in a long time	يتم تثبيت عميل الشبكة على الجهاز، ولكن لم يتم اتصال الجهاز بخادم الإدارة خلال الفاصل الزمني المحدد نظرًا لإيقاف تشغيل الجهاز.	أكثر من يوم واحد.
Active threats are detected	يتجاوز عدد الكائنات التي لم تتم معالجتها في المجلد **Active threats** القيمة المحددة.	أكثر من 0 عناصر.
Restart is required	الجهاز مرئي على الشبكة، إلا إن أحد التطبيقات يتطلب إعادة تشغيل الجهاز لمدة أطول من الفاصل الزمني المحدد ولأحد الأسباب المحددة.	أكثر من 0 دقائق.
Incompatible applications are installed	الجهاز مرئي على الشبكة، إلا إن مخزون البرنامج المنفَّذ عبر عميل الشبكة قد اكتشف تطبيقات غير متوافقة مثبتة على الجهاز.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Software vulnerabilities have been detected	الجهاز مرئي على الشبكة وعميل الشبكة مثبت على الجهاز، إلا أن مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة قد اكتشفت وجود ثغرات أمنية بمستوى الخطورة المحدد في التطبيقات المثبّتة على الجهاز.	• حرج. • مرتفع. • متوسط. • تجاهل إذا تعذر إصلاح الثغرات الأمنية. • تجاهل إذا تم تعيين تحديث للتثبيت.
License expired	الجهاز مرئي على الشبكة، إلا إن الترخيص قد انتهى.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
License expires soon	الجهاز مرئي على الشبكة، إلا أن الترخيص سينتهي على الجهاز خلال فترة أقل من عدد الأيام المحدد.	أقل من 0 يوم.
Check for Windows Update updates has not been performed in a long time	الجهاز مرئي على الشبكة، لكن لم يتم تشغيل مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة خلال الفاصل الزمني المحدد.	أكثر من يوم واحد.
Invalid encryption status	عميل الشبكة مثبت على الجهاز، إلا إن نتيجة تشفير الجهاز مساوية للقيمة المحددة.	• لا تتفق مع السياسة بسبب رفض المستخدم (بالنسبة للأجهزة الخارجية فقط). • لا تتوافق مع السياسة بسبب وجود خطأ. • إعادة التشغيل مطلوبة عند تطبيق السياسة. • لم يتم تحديد سياسة تشفير. • غير مدعوم • عند تطبيق السياسة.
Mobile device settings do not comply with the policy	إعدادات الجهاز المحمول تختلف عن الإعدادات المحددة في سياسة Kaspersky Endpoint Security for Android أثناء التحقق من قواعد الامتثال.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Unprocessed security issues detected	تم العثور على بعض مشكلات الأمان التي لم تتم معالجتها على الجهاز. يمكن إنشاء مشاكل الأمان إما تلقائيًا من خلال تطبيقات Kaspersky المُدارة المثبتة على الجهاز العميل أو يدويًا من قبل المسؤول.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Device status defined by application	تم تحديد حالة الجهاز بواسطة التطبيق المدار. يمكن أن يكون للأجهزة المدارة حالة محددة بواسطة التطبيقات المدارة بغض النظر عن إعدادات Kaspersky Security Center. بعد أن تعيد هذه الحالة إحدى الحالات المحددة بواسطة Kaspersky Security Center، يُعين خادم الإدارة الحالة الأكثر أهمية للجهاز الذي تتم إدارته بواسطة التطبيق المُدار والتي يتم تعيينها بواسطة خادم الإدارة. وتمتلك الحالات المحددة بواسطة التطبيقات المدارة أوصافًا تنقلها التطبيقات المدارة. ويمكنك عرض الأوصاف في قائمة الأجهزة المدارة، في العمود **Status description**.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
Device is out of disk space	مساحة القرص الشاغرة على الجهاز أقل من القيمة المحددة أو أنه يتعذر مزامنة الجهاز مع خادم الإدارة. يتم تغيير الحالة حرج أو تحذير إلى الحالة جيد عند مزامنة الجهاز بنجاح مع خادم الإدارة وتكون المساحة الفارغة على الجهاز أكبر من أو تساوي القيمة المحددة.	أكثر من 0 ميجابايت
Device has become unmanaged	أثناء اكتشاف الأجهزة، تم التعرف على الجهاز بأنه مرئي على الشبكة، لكن فشلت أكثر من ثلاث محاولات للمزامنة مع خادم الإدارة.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.

الشرط	وصف الشرط	القيم المتوفرة
Protection is disabled	الجهاز مرئي على الشبكة، إلا إنه قد تم تعطيل تطبيق الأمان على الجهاز لمدة أطول من الفاصل الزمني المحدد. في هذه الحالة، تكون حالة تطبيق الأمان متوقف أو فشل، ويختلف عما يلي: جارٍ البدء أو قيد التشغيل أو معلق.	أكثر من 0 دقائق.
Security application is not running	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لا يعمل.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.

يسمح لك Kaspersky Security Center بإعداد التبديل التلقائي لحالة الجهاز في مجموعة إدارة عند استيفاء الشروط المحددة. عند استيفاء الشروط المحددة، يتم تعيين الجهاز العميل إلى إحدى الحالات التالية: حرج أو تحذير. عند عدم استيفاء الشروط المحددة، يتم تعيين حالة الجهاز العميل على موافق .

يمكن وجود حالات مختلفة لقيم مختلفة لنفس الشرط. على سبيل المثال: إذا كان الشرط **Databases are outdated** له قيمة **أكثر من 3 أيام** بشكل افتراضي، سيتم تعيين حالة تحذير إلى الجهاز العميل؛ أما إذا كان بقيمة **أكثر من 7 يومًا**، سيتم تعيين حالة حرج إلى الجهاز.

إذا قمت بترقية Kaspersky Security Center من الإصدار السابق، قيم شرط **Databases are outdated** لتخصيص الحالة تتغير إلى حرجة أو تحذير أو لا تتغير.

تكوين تبديل حالات الجهاز

يمكنك تغيير الشروط لتعيين الحالة حرجة أو تحذير لجهازٍ ما.

لتمكين تغيير حالة الجهاز إلى حرجة:

1. في القائمة الرئيسية، انتقل إلى **Hierarchy of groups** ← **Assets (Devices)**.
2. في قائمة المجموعات التي تفتح، انقر على الرابط الذي يحمل اسم المجموعة التي ترغب في تغييرها بتبديل حالات الجهاز.
3. في نافذة الخصائص التي تفتح، حدد تبويب **Device status**.
4. في الجزء الأيسر، حدد **Critical**.
5. في الجزء الأيمن في قسم **Set to Critical if these are specified**، قم بتفعيل الشرط لتبديل جهاز إلى حالة حرج.

لا يمكنك تغيير سوى الإعدادات غير المقفلة في السياسة الأصلية.

6. حدد زر الراديو الموجود بجوار الشرط في القائمة.
7. في الزاوية العلوية اليسرى من القائمة، انقر على زر **Edit**.
8. حدد القيمة المطلوبة للحالة المحددة.
   لا يمكن تعيين القيم لكل حالة.
9. انقر على **OK**.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار عى حرج .

لتمكين تغيير حالة الجهاز إلى تحذير:

1. في القائمة الرئيسية، انتقل إلى **Hierarchy of groups** ← **Assets (Devices)**.
2. في قائمة المجموعات التي تفتح، انقر على الرابط الذي يحمل اسم المجموعة التي ترغب في تغييرها بتبديل حالات الجهاز.
3. في نافذة الخصائص التي تفتح، حدد تبويب **Device status**.

4. في الجزء الأيمن، حدد **Warning**.

5. في الجزء الأيمن في قسم **Set to Warning if these are specified**، قم بتفعيل الشرط لتبديل جهاز إلى حالة تحذير.

لا يمكنك تغيير سوى الإعدادات غير المقفلة في السياسة الأصلية.

6. حدد زر الراديو الموجود بجوار الشرط في القائمة.

7. في الزاوية العلوية اليسرى من القائمة، انقر على زر **Edit**.

8. حدد القيمة المطلوبة للحالة المحددة.

   لا يمكن تعيين القيم لكل حالة.

9. انقر على **OK**.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار عى تحذير .

تكوين تسليم الإخطار

يمكنك تكوين إخطار عن الأحداث التي تقع في Kaspersky Security Center. اعتمادًا على طريقة الإخطار المختارة، تتوفر أنواع الإخطارات التالية:

- البريد الإلكتروني: عند وقوع حدثٍ ما، يرسل Kaspersky Security Center إخطارًا إلى لعناوين البريد الإلكتروني المحددة.
- الرسائل النصية القصيرة: عند وقوع حدثٍ ما، يرسل Kaspersky Security Center إخطارًا إلى أرقام الهواتف المحددة.
- الملف التنفيذي: عند وقوع حدثٍ ما، يعمل الملف التنفيذي على خادم الإدارة.

لتكوين تسليم الإخطار للأحداث التي تقع في Kaspersky Security Center:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   ستفتح نافذة خصائص خادم الإدارة مع تحديد علامة التبويب **General**.

2. انقر على قسم **Notification**، وفي الجزء الأيمن حدد تبويب طريقة الإخطار التي تريدها:

- **Email**

تبويب **Email** يتيح لك تكوين إخطار الحدث عبر البريد الإلكتروني.

في حقل **Recipients (email addresses)**، حدد عناوين البريد الإلكتروني التي سيرسل التطبيق الإخطارات إليها. يمكنك تحديد عدة عناوين في هذا الحقل بالفصل بينهم بفواصل منقوطة.

في حقل **SMTP servers**، حدد عناوين خادم البريد، مع الفصل بينهم بفواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

في حقل **SMTP server port**، حدد رقم منفذ اتصال خادم SMTP. رقم المنفذ الافتراضي هو 25.

إذا قمت بتمكين خيار **Use DNS MX lookup**، فيمكنك استخدام عدة سجلات من MX لعناوين IP الخاصة بنفس اسم منطقة DNS في خادم SMTP. قد يكون لاسم DNS نفسه عدة سجلات من MX بقيم مختلفة لتلقي رسائل البريد الإلكتروني ذو الأولوية. يحاول خادم الإدارة إرسال إشعارات البريد الإلكتروني إلى خادم SMTP بترتيب تصاعدي لسجلات MX ذات الأولوية.

إذا قمت بتمكين خيار **Use DNS MX lookup**، ولم تقم بتمكين استخدام إعدادات TLS، فإننا نوصي باستخدام إعدادات DNSSEC على جهاز الخادم الخاص بك كإجراء إضافي للحماية لإرسال إعلامات البريد الإلكتروني.

في حال تمكين خيار **استخدام مصادقة ESMTP**، يمكنك تحديد إعدادات مصادقة ESMTP في **User name** و**Password**. يكون هذا الخيار معطلاً بشكل افتراضي، وتكون إعدادات مصادقة ESMTP غير متوفرة

يمكنك تحديد إعدادات TLS للاتصال بخادم SMTP:

- **Do not use TLS**

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

- **Use TLS if supported by the SMTP server**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام اتصال TLS مع خادم SMTP. إذا كان خادم SMTP لا يدعم TLS، فإن خادم الإدارة يتصل بخادم SMTP بدون استخدام TLS.

- **Always use TLS, check server certificate validity**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام إعدادات مصادقة TLS. إذا كان خادم SMTP لا يدعم TLS، فلن يتمكن خادم الإدارة من توصيل خادم SMTP.

نوصي باستخدام هذا الخيار لتوفير حماية أفضل للاتصال بخادم SMTP. إذا قمت بتحديد هذا الخيار، فيمكنك تعيين إعدادات المصادقة لاتصال TLS.

إذا قمت بتحديد قيمة **Always use TLS, check server certificate validity** فيمكنك تحديد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال من خلال أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. يمكنك أيضًا تحديد شهادة لمصادقة العميل على خادم SMTP.

يمكنك تحديد شهادات لاتصال TLS بالنقر فوق رابط **Specify certificates** :

- تصفح للوصول إلى ملف شهادة خادم SMTP:

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

- تصفح للوصول إلى ملف شهادة العميل:

يمكنك استخدام شهادة استلمتها من أي مصدر، على سبيل المثال، من أي جهة إصدار موثوقة. يجب تحديد الشهادة ومفتاحها الخاص باستخدام أحد أنواع الشهادات التالية:

- شهادة X-509:

يجب تحديد ملف مع الشهادة وملف مع المفتاح الخاص. كلا الملفين لا يعتمدان على بعضهما البعض وترتيب تحميل الملفات ليس مهمًا. عند تحميل كلا الملفين، يجب تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- الحاوية pkcs12:

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك بعد ذلك تحديد كلمة المرور لفك تشفير المفتاح الخاص. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

في حقل **Subject**، حدد موضوع البريد الإلكتروني. يمكنك ترك هذا الحقل فارغًا.

في القائمة المنسدلة **Subject template**، حدد قالب موضوعك. متغير يحدده القالب المحدد يُوضع تلقائيًا في حقل **Subject**. يمكنك إنشاء موضوع بريد إلكتروني باختيار عدة قوالب للموضوع.

في حقل **Sender email address**، حدد عنوان البريد الإلكتروني للمرسل. إذا تركت هذا الحقل فارغًا، سيتم استخدام عنوان المستلم افتراضيًا. لا يُنصح باستخدام عناوين بريد إلكتروني وهمية.

يحتوي حقل **Notification message** على نص قياسي يحتوي على معلومات حول الحدث الذي يرسله التطبيق عند وقوع حدث. يتضمن هذا النص معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة عن طريق إضافة بعض المعلمات البديلة الأخرى مع تفاصيل ذات صلة أكثر بالحدث.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

النقر على رابط **Configure numeric limit of notifications** يتيح لك تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مُدار الفاصل الزمني المحدد.

النقر على زر **Send test message** يتيح لك التحقق مما إذا قمت بتكوين الإخطارات بطريقة صحيحة: يرسل التطبيق إخطار اختبار إلى عناوين البريد الإلكتروني التي حددتها.

- **SMS**

تبويب **SMS** يتيح لك تكوين إرسال إخطارات بمختلف الأحداث عبر رسالة نصية قصيرة إلى هاتف محمول. يتم إرسال الرسائل النصية القصيرة عبر بوابة بريد.

في حقل **SMTP servers**، حدد عناوين خادم البريد، مع الفصل بينهم بفواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6
- اسم شبكة Windows (اسم NetBIOS) للجهاز
- اسم DNS لخادم SMTP.

في حقل **SMTP server port**، حدد رقم منفذ اتصال خادم SMTP. رقم المنفذ الافتراضي هو 25.

في حال تمكين خيار **استخدام مصادقة ESMTP**، يمكنك تحديد إعدادات مصادقة ESMTP في حقل **User name** و **Password**. يكون هذا الخيار معطلاً بشكل افتراضي، وتكون إعدادات مصادقة ESMTP غير متوفرة

يمكنك تحديد إعدادات TLS للاتصال بخادم SMTP:

- **Do not use TLS**

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

- **Use TLS if supported by the SMTP server**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام اتصال TLS مع خادم SMTP. إذا كان خادم SMTP لا يدعم TLS، فإن خادم الإدارة يتصل بخادم SMTP بدون استخدام TLS.

- **Always use TLS, check server certificate validity**

يمكنك تحديد هذا الخيار إذا كنت تريد استخدام إعدادات مصادقة TLS. إذا كان خادم SMTP لا يدعم TLS، فلن يتمكن خادم الإدارة من توصيل خادم SMTP.

نوصي باستخدام هذا الخيار لتوفير حماية أفضل للاتصال بخادم SMTP. إذا قمت بتحديد هذا الخيار، فيمكنك تعيين إعدادات المصادقة لاتصال TLS.

إذا قمت بتحديد قيمة **Always use TLS, check server certificate validity** فيمكنك تحديد شهادة لمصادقة خادم SMTP واختيار ما إذا كنت تريد تمكين الاتصال من خلال أي إصدار من TLS أو فقط من خلال TLS 1.2 أو الإصدارات الأحدث. يمكنك أيضًا تحديد شهادة لمصادقة العميل على خادم SMTP.

يمكنك تحديد ملف شهادة خادم SMTP بالنقر فوق رابط **Specify certificates** :

يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center الاتصال بخادم SMTP إذا لم يتم استلام شهادة خادم SMTP من جهات إصدار موثوقة.

في حقل **Recipients (email addresses)**، حدد عناوين البريد الإلكتروني التي سيرسل التطبيق الإخطارات إليها. يمكنك تحديد عدة عناوين في هذا الحقل بالفصل بينهم بفواصل منقوطة. سيتم إرسال الإخطارات إلى أرقام الهواتف المرتبطة بعناوين البريد الإلكتروني المحددة.

في حقل **Subject**، حدد موضوع البريد الإلكتروني.

في القائمة المنسدلة **Subject template**، حدد قالب موضوعك. متغير وفق القالب المحدد يُوضع في حقل **Subject**. يمكنك إنشاء موضوع بريد إلكتروني باختيار عدة قوالب للموضوع.

في حقل **Sender email address: If this setting is not specified, the recipient address will be used instead. Warning: We do not recommend using a fictitious email address**، حدد عنوان البريد الإلكتروني للمرسل. إذا تركت هذا الحقل فارغًا، سيتم استخدام عنوان المستلم افتراضيًا. لا يُنصح باستخدام عناوين بريد إلكتروني وهمية.

في حقل **Phone numbers of SMS message recipients**، حدد أرقام الهواتف المحمولة لمستلمي إشعار SMS.

في حقل **Notification message**، حدد نصًا يحتوي على معلومات حول الحدث الذي يرسله التطبيق عند وقوع حدث. يمكن أن يشمل هذا النص معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

انقر فوق رابط **Configure numeric limit of notifications** لتحديد الحد الأقصى لعدد الإشعارات التي يمكن للتطبيق إرسالها خلال الفترة الزمنية المحددة.

انقر فوق زر **Send test message** للتحقق مما إذا كنت قد قمت بتكوين الإشعارات بشكل صحيح: يرسل التطبيق إشعارا تجريبيًا إلى المستلم الذي حددته.

- **Executable file to be run**

إذا تم تحديد أسلوب الإخطار هذا، ففي حقل الإدخال يمكنك تحديد التطبيق الذي سيتم بدء تشغيله عند وقوع حدث ما.

في حقل **Executable file to be run on the Administration Server when an event occurs**، حدد المجلد واسم الملف الذي سيتم تشغيله. قبل تحديد الملف، قم بإعداد الملف وحدد العناصر النائبة التي تحدد تفاصيل الحدث التي سيتم إرسالها في رسالة الإشعار. يجب أن يكون المجلد والملف اللذين تحددهما موجودين على خادم الإدارة.

النقر على رابط **Configure numeric limit of notifications** يتيح لك تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مُدار الفاصل الزمني المحدد.

3. حدد إعدادات الإخطار في التبويب.

4. انقر فوق الزر **OK** لإغلاق النافذة خصائص خادم الإدارة.

يتم تطبيق إعدادات تسليم الإخطار المحفوظة على جميع الأحداث التي تقع في Kaspersky Security Center.

يمكنك تجاوز إعدادات تسليم الإخطار لبعض الأحداث المعينة في قسم **Event configuration** في إعدادات قسم خادم الإدارة أو في إعدادات سياسة أو في إعدادات تطبيق.

إخطارات الحدث التي يتم عرضها بواسطة الملف التنفيذي

بإمكان Kaspersky Security Center إخطار المسؤول بشأن الأحداث على الأجهزة العميلة عبر تشغيل الملف التنفيذي. يجب أن يحتوي الملف التنفيذي على ملف تنفيذي آخر مع العناصر النائبة للحدث ليتم ترحيله إلى المسؤول (انظر الجدول أدناه).

العناصر النائبة لوصف حدث

عنصر نائب	وصف عنصر نائب
%الخطورة%	خطورة الحدث. القيم الممكنة: • Info • Warning • خطأ • Critical
%الكمبيوتر%	اسم الجهاز الذي وقع عليه الحدث. الحد الأقصى لطول اسم الجهاز هو 256 حرفًا.
%المجال%	اسم المجال للجهاز الذي وقع عليه الحدث.

عنصر نائب	وصف عنصر نائب
%الحدث%	اسم نوع الحدث. الحد الأقصى لطول اسم نوع الحدث هو 50 حرفًا.
%DESCR%	وصف الحدث. الحد الأقصى لطول اسم الجهاز هو 1000 حرفًا.
%RISE_TIME%	وقت إنشاء الحدث.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	اسم المهمة. الحد الأقصى لطول اسم المهمة هو 100 حرف.
%KL_PRODUCT%	اسم التطبيق.
%KL_VERSION%	رقم إصدار التطبيق.
%KLCSAK_EVENT_SEVERITY_NUM%	رقم خطورة الحدث. القيم الممكنة: • **Info**—1 • **Warning**—2 • **Error**—3 • **Critical**—4
%HOST_IP%	عنوان IP للجهاز الذي وقع عليه الحدث.
%HOST_CONN_IP%	عنوان IP للاتصال بالجهاز الذي وقع عليه الحدث.

مثال:
يتم إرسال إشعارات الحدث بواسطة ملف تنفيذي (مثل script1.bat) الذي يوجد بداخله ملف تنفيذي آخر (مثل script2.bat) مع تشغيل العنصر النائب %COMPUTER%. عند وقوع حدث ما، سيتم تشغيل الملف script1.bat على جهاز المسؤول والذي بدوره يشغّل الملف script2.bat مع العنصر النائب %COMPUTER%. يتلقى المسؤول اسم الجهاز حيث وقع الحدث.

إعلامات Kaspersky

يصف هذا القسم كيفية استخدام إعلانات Kaspersky وتكوينها وتعطيلها.

حول أخبار Kaspersky

قسم أخبار Kaspersky (**Monitoring & reporting** ← **أخبار Kaspersky**) يبقيك على اطلاع من خلال توفير المعلومات المتعلقة بإصدار Kaspersky Security Center لديك والتطبيقات المدارة المثبتة على الأجهزة المدارة. يقوم Kaspersky Security Center بتحديث المعلومات الواردة في القسم بشكل دوري عن طريق إزالة الأخبار القديمة وإضافة معلومات جديدة.

يعرض Kaspersky Security Center إعلانات Kaspersky التي تتعلق بخادم الإدارة المتصل حاليًا وتطبيقات Kaspersky المثبتة على الأجهزة المدارة لخادم الإدارة هذا. يتم عرض الإعلانات بشكل فردي لأي نوع من خوادم الإدارة سواء كام—أساسي أم ثانوي أم افتراضي.

يجب أن يكون خادم الإدارة متصلاً بالإنترنت لتلقي أخبار Kaspersky.

الأخبار تتضمن معلومات من الأنواع التالية:

- الأخبار المتعلقة بالأمان

تهدف الأخبار المتعلقة بالأمان إلى إبقاء تطبيقات Kaspersky المثبتة في شبكتك محدثة وتعمل بكامل طاقتها. الأخبار قد تتضمن معلومات حول التحديثات المهمة لتطبيقات Kaspersky وإصلاحات الثغرات الأمنية التي تم العثور عليها وطرق إصلاح المشكلات الأخرى في تطبيقات Kaspersky. يتم تمكين الأخبار المتعلقة بالأمان بشكل افتراضي. إذا كنت لا ترغب في تلقي الأخبار، يمكنك تعطيل هذه الميزة.

لتظهر لك المعلومات التي تتوافق مع تكوين حماية شبكتك، Kaspersky Security Center يرسل البيانات إلى خوادم Kaspersky السحابية ولا يتلقى إلا الأخبار المتعلقة بتطبيقات Kaspersky المثبتة في شبكتك. البيانات التي يمكن إرسالها إلى الخوادم موصوفة في اتفاقية ترخيص المستخدم النهائي التي توافق عليها عند تثبيت خادم إدارة Kaspersky Security Center.

- الأخبار التسويقية

الأخبار التسويقية تتضمن معلومات حول العروض الخاصة لتطبيقاتك من Kaspersky والإعلانات والأخبار من Kaspersky. يتم تعطيل الأخبار التسويقية افتراضيًا. أنت لا تتلقى هذا النوع من الأخبار إلا إذا قمت بتمكين Kaspersky Security Network (KSN). يمكنك تعطيل الأخبار التسويقية عن طريق تعطيل KSN.

كي لا يظهر لك إلا المعلومات ذات الصلة التي قد تكون مفيدة في حماية أجهزة شبكتك وفي مهامك اليومية، Kaspersky Security Center يرسل البيانات إلى خوادم Kaspersky السحابية ويتلقى الأخبار المناسبة. مجموعة البيانات التي يمكن إرسالها إلى الخوادم موصوفة في قسم البيانات المعالجة في بيان KSN.

يتم تقسيم المعلومات الجديدة إلى الفئات التالية حسب الأهمية:

1. معلومات مهمة
2. أخبار مهمة
3. تحذير
4. معلومات

عندما تظهر معلومات جديدة في قسم أخبار Kaspersky، Kaspersky Security Center Web Console يعرض ملصق إخطار يتوافق مع مستوى أهمية الأخبار. يمكنك النقر على الملصق لعرض هذا الخبر في قسم أخبار Kaspersky.

يمكنك تحديد إعدادات أخبار Kaspersky، بما في ذلك فئات الأخبار التي ترغب في عرضها ومكان عرض ملصق الإخطار.

تحديد إعدادات أخبار Kaspersky

في قسم أخبار Kaspersky، يمكنك تحديد إعدادات أخبار Kaspersky، بما في ذلك فئات الأخبار التي ترغب في عرضها ومكان عرض ملصق الإخطار.

لتكوين إعلانات Kaspersky:

1. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Kaspersky announcements**.
2. انقر على رابط **الإعدادات**.

   تفتح نافذة إعدادات أخبار Kaspersky.
3. حدد الإعدادات التالية:
   - حدد مستوى الأهمية للأخبار التي ترغب في عرضها. لن يتم عرض الأخبار من الفئات الأخرى.
   - حدد المكان الذي ترغب في رؤية ملصق الإخطار فيه. يمكن عرض الملصق في جميع أقسام وحدة التحكم أو في قسم **Monitoring & reporting** وأقسامه الفرعية.
4. انقر على زر **موافق**.

   بهذا تم تحديد إعدادات أخبار Kaspersky.

تعطيل أخبار Kaspersky

قسم أخبار Kaspersky (**Monitoring & reporting** ← **أخبار Kaspersky**)يبقيك على اطلاع من خلال توفير المعلومات المتعلقة بإصدار Kaspersky Security Center لديك والتطبيقات المدارة المثبتة على الأجهزة المدارة. إذا كنت لا ترغب في تلقي أخبار Kaspersky، يمكنك تعطيل هذه الميزة.

أخبار Kaspersky تشمل نوعين من المعلومات: الأخبار المتعلقة بالأمان والأخبار التسويقية. يمكنك تعطيل الأخبار من كل نوع على حدة.

لتعطيل الأخبار المتعلقة بالأمان:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب **General**، حدد القسم **Kaspersky announcements**.
3. بدل زر التبديل إلى وضع **Security-related announcements Disabled**.
4. انقر على زر **Save**.
   بهذا تم تعطيل أخبار Kaspersky.

يتم تعطيل الأخبار التسويقية افتراضيًا. أنت لا تتلقى أخبار تسويقية إلا إذا قمت بتمكين Kaspersky Security Network (KSN). يمكنك تعطيل هذا النوع من الأخبار عن طريق تعطيل KSN.

لتعطيل الأخبار التسويقية:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب **General**، حدد قسم **إعدادات وكيل KSN**.
3. قم بتعطيل خيار **Use Kaspersky Security Network Enabled**.
4. انقر على زر **Save**.
   بهذا تم تعطيل الأخبار التسويقية.

عرض معلومات حول اكتشافات التهديدات

يمكنك تمكين أو تعطيل عرض المعلومات حول التنبيهات.

لتمكين أو تعطيل عرض قسم **Alerts** في القائمة الرئيسية:

1. في القائمة الرئيسية، انتقل إلى إعدادات حسابك ثم حدد **Interface options**.
2. في نافذة **خيارات الواجهة** التي تفتح، قم بتمكين خيار **Show EDR alerts** أو تعطيله.
3. انقر فوق **حفظ**.

تعرض الوحدة القسم الفرعي **Alerts** في القسم **Monitoring & reporting** من القائمة الرئيسية. في القسم الفرعي **Alerts**، يمكنك عرض معلومات حول اكتشاف التهديدات على أجهزة نقطة النهاية. إذا أضفت مفتاح ترخيص لـ EDR الأمثل ، فسيعرض Kaspersky Security Center Web Console القسم الفرعي **Alerts** تلقائيًا في القسم **Monitoring & reporting** من القائمة الرئيسية. يمكنك أيضًا إضافة تطبيق مصغر يعرض معلومات حول التنبيهات.

يتم عرض القسم الفرعي **Alerts** تلقائيًا فقط إذا أضفت مفتاح الترخيص لتطبيق EDR Optimum قبل تمكين خيار **Show EDR alerts**EDR. وإذا أضفت مفتاح الترخيص بعد تمكين خيار **Show EDR alerts**، فسيتم عرض القسم الفرعي **Alerts** فقط بعد إعادة تمكين هذا الخيار.

لعرض معلومات تفصيلية عن التهديدات المكتشفة في بطاقة التنبيه بشكل صحيح، يجب عليك أيضًا تثبيت المكون الإضافي لتطبيق Kaspersky Endpoint Agent والإصدار المتوافق من المكون الإضافي لتطبيق Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 أو أحدث، أو Kaspersky Endpoint Security for Mac 12.1 أو أحدث، أو Kaspersky Endpoint Security for Windows 12.6 أو أحدث).

استخدم قائمة **التصفية** لتصفية التنبيهات حسب التاريخ وقيم الحقل.

يحتوي الحقل **نوع الكائن** على القيم التالية:

- Unknown
- Phishing link
- Virus
- Trojan
- Malicious tool
- Backdoor
- Worm
- Other application
- Adware
- Pornware
- Dangerous packed program
- Dangerous behavior

يحتوي الحقل **الاستجابة التلقائية** على القيم التالية:

- Malicious object detected
- Object deleted
- Object disinfected
- Object failed to disinfect
- Object moved to Quarantine

- Password-protected archive detected
- Virus detected

اكتشاف السحابة

يتيح لك Kaspersky Security Center مراقبة استخدام الخدمات السحابية على الأجهزة المُدارة التي تعمل بنظام التشغيل Windows ومنع الوصول إلى الخدمات السحابية التي تعتبرها غير مرغوب فيها. يتتبع Cloud Discovery محاولات المستخدم للوصول إلى هذه الخدمات من خلال المستعرضات وتطبيقات سطح المكتب. ويتتبع كذلك محاولات المستخدم للوصول إلى الخدمات السحابية عبر اتصالات غير مشفرة (على سبيل المثال، باستخدام بروتوكول HTTP). وتساعدك هذه الميزة على اكتشاف وإيقاف استخدام الخدمات السحابية بواسطة الأدوات المُثبتة دون موافقة قسم تكنولوجيا المعلومات.

تتوفر إمكانية الحظر فقط إذا قمت بتفعيل Kaspersky Security Center بموجب ترخيص Kaspersky Next EDR Optimum أو Kaspersky Next XDR Expert license.

تتوفر إمكانية الحظر فقط إذا كنت تستخدم Kaspersky Endpoint Security 11.2 for Windows أو أحدث. وتسمح لك الإصدارات السابقة من تطبيق الأمان فقط بمراقبة استخدام الخدمات السحابية.

يمكنك تمكين ميزة Cloud Discovery وتحديد سياسات الأمان أو ملفات التعريف التي تريد تمكين الميزة لها. ويمكنك أيضًا تمكين الميزة أو تعطيلها بشكل منفصل في كل سياسة أمان أو ملف تعريف. ويمكنك حظر الوصول إلى الخدمات السحابية التي لا تريد أن يصل إليها المستخدمون.

لتتمكن من حظر الوصول إلى الخدمات السحابية غير المرغوب فيها، تأكد من استيفاء المتطلبات الأساسية التالية:

- يمكنك استخدام Kaspersky Endpoint Security 11.2 for Windows أو أحدث. وتسمح لك الإصدارات السابقة من تطبيق الأمان فقط بمراقبة استخدام الخدمات السحابية.
- اشتريت طبقة ترخيص Kaspersky Next التي تتضمن القدرة على حظر الوصول إلى الخدمات السحابية غير المرغوب فيها. للحصول على التفاصيل، ارجع إلى تعليمات Kaspersky Next.

تعرض أداة Cloud Discovery وتقارير Cloud Discovery معلومات عن المحاولات الناجحة والمحظورة للوصول إلى الخدمات السحابية. وتعرض الأداة أيضًا مستوى الخطر لكل خدمة سحابية. يحصل Kaspersky Security Center على معلومات عن استخدام الخدمات السحابية من جميع الأجهزة المدارة المحمية فقط من خلال سياسات أو ملفات تعريف الأمان التي تم تمكين هذه الميزة فيها.

تمكين Cloud Discovery باستخدام الأداة

تسمح لك ميزة Cloud Discovery بالحصول على معلومات عن استخدام الخدمات السحابية من جميع الأجهزة المدارة المحمية فقط من خلال سياسات الأمان التي تم تمكين هذه الميزة فيها. ويمكنك تمكين أو تعطيل Cloud Discovery لسياسة Kaspersky Endpoint Security for Windows فقط.

هناك طريقتان لتمكين ميزة Cloud Discovery:

- باستخدام أداة Cloud Discovery.
- في خصائص سياسة Kaspersky Endpoint Security for Windows.

للحصول على تفاصيل عن كيفية تمكين ميزة Cloud Discovery في خصائص سياسة Kaspersky Endpoint Security for Windows، راجع قسم Cloud Discovery في تعليمات Kaspersky Endpoint Security for Windows.

لاحظ أنه يمكنك تعطيل ميزة Cloud Discovery في معلمات سياسة Kaspersky Endpoint Security for Windows فقط.

لتمكين Cloud Discovery، يجب أن يكون لديك حق **كتابة** في المنطقة الوظيفية **الميزات العامة: الوظائف الأساسية**.

لتمكين ميزة Cloud Discovery باستخدام أداة Cloud Discovery:

1. انتقل إلى Kaspersky Security Center.
2. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
3. في أداة **Cloud Discovery**، انقر فوق الزر **تمكين**.

إذا كان لديك الإصدار 12.4 من Kaspersky Endpoint Security for Windows مثبتًا، فقم بتمكين ميزة Cloud Discovery في خصائص سياسة Kaspersky Endpoint Security for Windows. للحصول على التفاصيل، ارجع إلى قسم Cloud Discovery في تعليمات Kaspersky Endpoint Security for Windows.

إذا كان لديك Kaspersky Endpoint Security for Windows أقدم من الإصدار 12.4، فقم بتحديث المكون الإضافي Kaspersky Endpoint Security for Windows إلى الإصدار 12.5.

4. في النافذة **Enable Cloud Discovery** التي تفتح، حدد سياسات الأمان التي تريد تمكين الميزة لها، ثم انقر فوق الزر **تمكين**.

سيتم تمكين إعدادات السياسة التالية تلقائيًا: **إدخال برنامج نصي في حركة مرور الويب للتفاعل مع صفحات الويب** و**مراقب جلسة الويب** و**فحص الاتصالات المشفرة**.

يتم تمكين ميزة Cloud Discovery وتتم إضافة الأداة إلى لوحة المعلومات.

إضافة أداة Cloud Discovery إلى لوحة المعلومات

يمكنك إضافة أداة **Cloud Discovery** إلى لوحة المعلومات لمراقبة استخدام الخدمات السحابية على الأجهزة المدارة.

لإضافة أداة Cloud Discovery إلى لوحة المعلومات، يجب أن تمتلك حق **كتابة** في المنطقة الوظيفية **الميزات العامة: الوظائف الأساسية**.

لإضافة أداة Cloud Discovery إلى لوحة المعلومات:

1. انتقل إلى Kaspersky Security Center.
2. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.
3. انقر فوق الزر **Add or restore web widget**.
4. في قائمة الأدوات المتاحة ، انقر فوق أيقونة الشريط (>) بجوار الفئة **غير ذلك**.
5. حدد أداة **Cloud Discovery**، ثم انقر على الزر **Add**.

إذا تم تعطيل ميزة Cloud Discovery، فاتبع الإرشادات الموجودة في قسم تمكين Cloud Discovery باستخدام الأداة.

يتم إضافة الأداة المحددة إلى نهاية لوحة المعلومات.

عرض معلومات عن استخدام الخدمات السحابية

يمكنك عرض أداة **Cloud Discovery** التي تعرض معلومات عن محاولات الوصول إلى الخدمات السحابية. وتعرض الأداة أيضًا مستوى الخطر لكل خدمة سحابية. يحصل Kaspersky Security Center على معلومات عن استخدام الخدمات السحابية من جميع الأجهزة المدارة المحمية فقط من خلال ملفات تعريف الأمان التي تم تمكين هذه الميزة فيها.

قبل العرض تأكد من التالي:

- تتم إضافة أداة Cloud Discovery إلى لوحة المعلومات.
- تم تمكين ميزة Cloud Discovery.
- تمتلك حق **Read** في منطقة الوظائف **الميزات العامة: الوظائف الأساسية** .

لعرض أداة Cloud Discovery:

1. انتقل إلى Kaspersky Security Center.
2. في القائمة الرئيسية، انتقل إلى **Monitoring & reporting** ← **Dashboard**.

   يتم عرض أداة **Cloud Discovery** في لوحة المعلومات.
3. على الجانب الأيمن من أداة **Cloud Discovery**، حدد فئة الخدمات السحابية.

   يعرض الجدول الموجود على الجانب الأيسر من الأداة ما يصل إلى خمس خدمات من الفئة المحددة، التي يحاول المستخدمون في أغلب الأحيان الوصول إليها. يتم احتساب كل من المحاولات الناجحة والمحظورة.
4. على الجانب الأيسر من الأداة، حدد خدمة معينة.

   يعرض الجدول أدناه ما يصل إلى عشرة أجهزة تحاول غالبًا الوصول إلى الخدمة. في هذا الجدول، يمكنك إنشاء نوعين من التقارير: تقرير حول محاولات الوصول الناجحة وإعداد تقرير حول محاولات الوصول الممنوعة.

   بالإضافة إلى ذلك، يمكنك في هذا الجدول منع الوصول إلى الخدمة السحابية لجهاز معين.

   تعرض الأداة المعلومات المطلوبة.

يمكنك فعل ما يلي من الأداة المعروضة:

- الانتقال إلى قسم **Reports** ← **Monitoring & reporting**، لعرض تقارير Cloud Discovery.
- حظر أو السماح بالوصول إلى الخدمة السحابية المحددة.

تتوفر إمكانية الحظر فقط إذا قمت بتفعيل Kaspersky Security Center بموجب ترخيص Kaspersky Next EDR Optimum أو Kaspersky Next XDR Expert license.

تتوفر إمكانية الحظر فقط إذا كنت تستخدم Kaspersky Endpoint Security 11.2 for Windows أو أحدث. وتسمح لك الإصدارات السابقة من تطبيق الأمان فقط بمراقبة استخدام الخدمات السحابية.

مستوى خطر خدمة سحابية

لكل خدمة سحابية، توفر لك Cloud Discovery مستوى مخاطرة. يساعدك مستوى المخاطرة في تحديد الخدمات التي لا تناسب متطلبات الأمان الخاصة بمؤسستك. على سبيل المثال، قد ترغب في أخذ مستوى المخاطرة في الاعتبار عند تحديد ما إذا كنت تريد منع الوصول إلى خدمة معينة أم لا.

مستوى المخاطرة هو مؤشر تقديري ولا يذكر أي شيء عن جودة الخدمة السحابية أو الشركة المصنعة للخدمة. مستوى المخاطر هو مجرد توصية من خبراء Kaspersky.

يتم عرض مستويات مخاطر الخدمات السحابية في أداة Cloud Discovery وفي قائمة جميع الخدمات السحابية الخاضعة للمراقبة.

حظر الوصول إلى الخدمات السحابية غير المرغوب فيها

ويمكنك حظر الوصول إلى الخدمات السحابية التي لا تريد أن يصل إليها المستخدمون. ويمكنك أيضًا السماح بالوصول إلى الخدمات السحابية التي تم حظرها مسبقًا.

من بين الاعتبارات الأخرى، قد ترغب في أخذ مستوى المخاطرة في الاعتبار عند اتخاذ قرار بشأن حظر الوصول إلى خدمة معينة.

يمكنك حظر أو السماح بالوصول إلى الخدمات السحابية لسياسة أو ملف تعريف أمان.

هناك طريقتان لمنع الوصول إلى الخدمات السحابية غير المرغوب فيها:

- باستخدام أداة Cloud Discovery.

  في هذه الحالة، يمكنك منع الوصول إلى الخدمات واحدة تلو الأخرى.

- في خصائص سياسة Kaspersky Endpoint Security for Windows.

  في هذه الحالة، يمكنك منع الوصول إلى الخدمات واحدة تلو الأخرى أو منع فئة كاملة مرة واحدة.

  للحصول على تفاصيل عن كيفية تمكين ميزة Cloud Discovery في خصائص سياسة Kaspersky Endpoint Security for Windows، راجع قسم Cloud Discovery في تعليمات Kaspersky Endpoint Security for Windows.

لمنع الوصول إلى خدمة سحابية أو السماح به باستخدام الأداة:

1. افتح أداة Cloud Discovery، ثم حدد الخدمة السحابية المطلوبة.
2. في القسم **Top 10 devices that use the service**، ابحث عن سياسة الأمان أو ملف التعريف الذي تريد منع الخدمة أو السماح بها لأجله.
3. في السطر المطلوب، في العمود **Access status in policy or profile**، نفذ أيًا مما يلي:
   - لمنع الخدمة، حدد **Blocked** في القائمة المنسدلة.
   - للسماح بالخدمة، حدد **مسموح به** في القائمة المنسدلة.
4. انقر على زر **حفظ**.

يتم حظر الوصول إلى الخدمة المحددة أو السماح به لسياسة الأمان أو ملف التعريف.

تسجيل نشاط Kaspersky Security Center Web Console

تسجيل نشاط Kaspersky Security Center Web Console يمكن أن يساعد في تقصي أسباب خلل برنامج. عند الاتصال بالدعم الفني في Kaspersky بشأن عطل في Kaspersky Security Center Web Console، يستطيع متخصصو الدعم الفني في Kaspersky طلب ملفات سجل Kaspersky Security Center Web Console منك. تُخزن ملفات سجل Kaspersky Security Center Web Console في المجلد logs/<Kaspersky Security Center Web Console installation folder> طوال الوقت الذي تستخدم فيه التطبيق. لا يتم إرسال ملفات السجل إلى أخصائي الدعم الفني من Kaspersky تلقائيًا.

لتفعيل تسجيل نشاط Kaspersky Security Center Web Console،

حدد خانة اختيار **Enable logging of Kaspersky Security Center Web Console activities** في النافذة **Kaspersky Security Center Web Console connection settings** في معالج إعداد Kaspersky Security Center 14 Web Console.

تكون ملفات السجل في تنسيق نصي.

أسماء ملفات السجل بالتنسيق التالي: سجلات-<اسم المكون>.<اسم الجهاز>-<رقم مراجعة الملف>.عام-شهر-يوم، حيث

- <component name> هو اسم مكون Kaspersky Security Center أو اسم مكون الإدارة الإضافي لـ Kaspersky Security Center Web Console.
- <اسم الجهاز> هو اسم الجهاز الذي يعمل عليه <اسم المكون>.
- <رقم مراجعة الملف> هو رقم ملف السجل الذي تم إنشاؤه ل<اسم المكون> الذي يعمل على <اسم الجهاز>. يمكن إنشاء عدة ملفات سجلات لنفس <اسم المكون> و<اسم الجهاز> خلال يوم واحد. أقصى حجم لملف السجل هو 50 ميجا بايت. يتم إنشاء مل سجل جديد عند الوصول إلى أقص حجم. يتم وضع الرقم 1 في نهاية <رقم مراجعة الملف> لملف السجل.
- YYYY وMM وDD هم العام والشهر واليوم بالترتيب بتاريخ أول إنشاء للسجل. عند يبدأ يوم جديد، يتم إنشاء ملف سجل جديد.

التكامل بين Kaspersky Security Center والحلول الأخرى

يصف هذا القسم كيفية تكوين الوصول من Kaspersky Security Center Web Console إلى تطبيق آخر من Kaspersky، مثل Kaspersky Managed Detection and Response. يصف هذا القسم أيضًا كيفية تكوين التصدير إلى أنظمة إدارة معلومات الأمان والأحداث (SIEM).

جارٍ إنشاء اتصال في الخلفية

لتمكين Kaspersky Security Center Web Console من أداء مهامها في الخلفية، فيجب عليك إنشاء اتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة. يمكنك إنشاء هذا الاتصال فقط إذا كان حسابك له حق تعديل **قوائم التحكم في الوصول للكائن** مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.

إذا قمت بتثبيت المكون الإضافي لبرنامج Kaspersky Endpoint Security for Windows 12.6، أو إذا قمت بتحديث المكوّن الإضافي Kaspersky Endpoint Security for Windows من إصدار أقدم من 11.7 ولم يتم إنشاء اتصال في الخلفية بعد، فسيُعرض إشعار بأنك أنشأت اتصالاً في الخلفية. سيتعين عليك أيضًا منح حساب الخدمة حقوق المنطقة الوظيفية **الميزات العامة: العمليات على خادم الإدارة**.

لإنشاء اتصال في الخلفية:

1. في القائمة الرئيسية انتقل الى **إعدادات** ← **Integration**.

2. في القسم **Integration**، قم بتشغيل زر التبديل لإنشاء اتصال في الخلفية إلى الموضع: **Background connection for integration Enabled**.

3. في قسم **Enable a background connection** المفتوح، انقر على زر **OK**.

تم إنشاء الاتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة. خادم الإدارة ينشئ حسابًا للاتصال في الخلفية، ويتم استخدام هذا الحساب كحساب خدمة للحفاظ على التفاعل بين Kaspersky Security Center وتطبيق أو حل آخر من Kaspersky. اسم حساب الخدمة هذا يضم البادئة NWCSvcUser.

يقوم خادم الإدارة تلقائيًا بتغيير كلمة مرور حساب الخدمة مرة واحدة كل 30 يومًا لأسباب أمنية. لا يمكنك حذف حساب الخدمة يدويًا. خادم الإدارة يحذف هذا الحساب تلقائيًا عند تعطيل اتصال عبر الخدمات. خادم الإدارة ينشئ حساب خدمة واحد لكل وحدة تحكم في الإدارة ويعيّن جميع حسابات الخدمة لمجموعة الأمان التي تحمل الاسم ServiceNwcGroup. خادم الإدارة ينشئ مجموعة الأمان هذه تلقائيًا أثناء عملية تثبيت Kaspersky Security Center. لا يمكنك حذف مجموعة الأمان هذه يدويًا.

تصدير الأحداث إلى أنظمة SIEM

يصف هذا القسم كيفية تكوين تصدير الأحداث إلى أنظمة SIEM.

تكوين تصدير الحدث إلى أنظمة SIEM

يسمح Kaspersky Security Center بالتكوين بإحدى الطرق التالية: التصدير إلى أي نظام SIEM يستخدم تنسيق Syslog أو التصدير إلى أنظمة QRadar وSplunk وArcSight SIEM التي تستخدم تنسيقات LEEF وCEF أو تصدير الأحداث إلى أنظمة SIEM مباشرةً من قاعدة بيانات Kaspersky Security Center. عند إكمال هذا السيناريو، يرسل خادم الإدارة الأحداث إلى نظام SIEM تلقائيًا.

المتطلبات الأساسية

قبل أن تبدأ في تصدير تكوين الأحداث في Kaspersky Security Center:

- تعرف على المزيد حول طرق تصدير الحدث.
- تأكد من أن لديك قيم إعدادات النظام.

يمكنك تنفيذ خطوات هذا السيناريو بأي ترتيب.

تتكون عملية تصدير الأحداث إلى نظام SIEM من الخطوات التالية:

- **تكوين نظام SIEM لاستقبال الأحداث من Kaspersky Security Center**

  تعليمات للمساعدة: تكوين تصدير الحدث في نظام SIEM

- **تحديد الأحداث التي تريد تصديرها إلى نظام SIEM:**

تعليمات للمساعدة:

- وحدة تحكم الإدارة: وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog، ووضع علامة على الأحداث العامة للتصدير بتنسيق Syslog
- Kaspersky Security Center Web Console: تمييز أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog وتمييز الأحداث العامة للتصدير بتنسيق Syslog

- **قم بتكوين تصدير الأحداث إلى نظام SIEM باستخدام إحدى الطرق التالية:**
  - استخدم TCP أو UDP أو TLS عبر بروتوكولات TCP.

    تعليمات للمساعدة:

    - وحدة تحكم الإدارة: تكوين تصدير الأحداث إلى أنظمة SIEM
    - Kaspersky Security Center Web Console: تكوين تصدير الأحداث إلى أنظمة SIEM
  - استخدام تصدير الأحداث بشكل مباشر من قاعدة بيانات Kaspersky Security Center (يتم توفير مجموعة من طرق العرض العامة في قاعدة بيانات Kaspersky Security Center؛ ويمكنك العثور على وصف لهذه العروض العامة في المستند klakdb.chm).

النتائج

بعد تكوين تصدير الأحداث إلى نظام SIEM يمكنك عرض نتائج التصدير إذا قمت بتحديد الأحداث التي تريد تصديرها.

قبل البدء

عند إعداد التصدير التلقائي للأحداث في Kaspersky Security Center، يجب عليك تحديد بعض إعدادات نظام SIEM. يوصى بأن تتحقق من هذه الإعدادات مسبقًا للتحضير لإعداد Kaspersky Security Center.

لتكوين الإرسال التلقائي للأحداث إلى نظام SIEM، يجب أن تكون على علم بالإعدادات التالية:

- **عنوان خادم نظام SIEM**

  عنوان IP للخادم المستخدم حاليًا الذي تم تثبيت نظام SIEM عليه. تحقق من هذه القيمة في إعدادات نظام SIEM لديك.

- **منفذ خادم نظام SIEM**

  رقم المنفذ المستخدم لإنشاء اتصال بين Kaspersky Security Center وخادم نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center وفي إعدادات المستلم لنظام SIEM الخاص بك.

- **البروتوكول**

  البروتوكول المستخدم لنقل الرسائل من Kaspersky Security Center إلى نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center وفي إعدادات المستلم لنظام SIEM الخاص بك.

حول الأحداث في Kaspersky Security Center

يتيح لك Kaspersky Security Center تلقي معلومات عن الأحداث التي تقع أثناء تشغيل خادم الإدارة وتطبيقات Kaspersky المثبتة على الأجهزة المُدارة. يتم حفظ المعلومات حول الأحداث في قاعدة بيانات خادم الإدارة. يمكنك تصدير هذه المعلومات إلى أنظمة SIEM الخارجية. يسمح تصدير معلومات الأحداث إلى أنظمة SIEM لمسؤولي أنظمة SIEM بالاستجابة السريعة لأحداث نظام الأمان التي تحدث في الأجهزة المدارة أو مجموعات الإدارة.

أنواع الأحداث

يتوفر في Kaspersky Security Center الأنواع التالية من الأحداث:

- الأحداث العامة. تحدث هذه الأحداث في جميع تطبيقات Kaspersky المدارة. مثال على حدث عام هو انتشار الفيروسات. لقد حددت الأحداث العامة بناء الجملة والدلالات بدقة. يتم استخدام الأحداث العامة على سبيل المثال، في التقارير ولوحات المعلومات.
- أحداث خاصة بتطبيقات Kaspersky المدارة. يحتوي كل تطبيق من تطبيقات Kaspersky المدارة على مجموعة من الأحداث الخاصة به.

مصادر الحدث

يمكن إنشاء الأحداث من خلال التطبيقات التالية:

- مكونات Kaspersky Security Center:
  - خادم الإدارة
  - عميل الشبكة
  - خادم الأجهزة المحمولة التي تعمل بنظام iOS
- تطبيقات Kaspersky المُدارة

للحصول على تفاصيل حول الأحداث التي تم إنشاؤها بواسطة تطبيقات Kaspersky المُدارة، يُرجى الرجوع إلى وثائق التطبيق المقابل.

يمكنك عرض القائمة الكاملة للأحداث التي يمكن إنشاؤها بواسطة تطبيق ما في علامة التبويب **Event configuration**. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث في خصائص خادم الإدارة.

مستوى خطورة الأحداث

يحتوي كل حدث على مستوى الأهمية الخاص به. بناء على شروط الحدوث، يمكن تعيين مستويات أهمية مختلفة لأي حدث. توجد أربعة مستويات للأهمية للأحداث:

- حدث حرج هو حدث يشير إلى تكرار مشكلة حرجة قد تؤدي إلى فقدان البيانات أو خلل في التشغيل أو خطأ حرج.
- خلل وظيفي هو حدث يشير إلى تكرار مشكلة خطيرة أو خطأ أو خلل حدث أثناء تشغيل التطبيق أو عند تنفيذ الإجراء.
- تحذير هو حدث ليس خطيرًا بالضرورة، غير أنه يشير إلى مشكلة محتملة في المستقبل. يتم تعيين معظم الأحداث كتحذيرات إذا كان من الممكن استعادة التطبيق بدون فقدان البيانات أو الإمكانيات الوظيفية بعد حدوث هذه الأحداث.
- حدث معلومات هو حدث يحدث لأغراض الإخبار عن إكمال التشغيل بنجاح، أو التشغيل الصحيح للتطبيق، أو إكمال الإجراء.

لكل حدث مدّة تخزين محددة، يمكنك خلالها عرضه في Kaspersky Security Center أو تعديله. لا يتم حفظ بعض البيانات في قاعدة بيانات خادم الإدارة بشكل افتراضي لأن مدّة التخزين المحددة هي صفر. يمكن تصدير الأحداث التي سيتم تخزينها في قاعدة بيانات خادم الإدارة فقط لمدة يوم واحد على الأقل إلى الأنظمة الخارجية.

حول تصدير الحدث

يمكن استخدام تصدير الحدث في الأنظمة المركزية التي تتعامل مع مشكلات الأمان على المستوى التنظيمي والتقني، والتي توفر خدمات مراقبة الأمان، وتجمع المعلومات من الحلول المختلفة. وهذه هي أنظمة SIEM التي توفر التحليل الفوري لتحذيرات الأمان والأحداث التي تنشئها أجهزة الشبكة والتطبيقات، أو مراكز تشغيل الأمان (SOC).

يمكن لهذه الأنظمة استلام البيانات من العديد من المصادر، بما فيها الشبكات والأمان والخوادم وقواعد البيانات والتطبيقات. توفر أنظمة SIEM أيضًا وظيفة تجميع البيانات التي تم رصدها لمساعدتك في تجنب فقدان الأحداث الحرجة. إضافة إلى ذلك، تُجري الأنظمة تحليلاً تلقائيًا للأحداث والتحذيرات المترابطة لإخطار المسؤولين بمشاكل الأمان العاجلة. يمكن تنفيذ التحذير من خلال لوحة معلومات ويمكن إرسالها من خلال قنوات لجهات خارجية مثل البريد الإلكتروني.

تشتمل عملية تصدير الأحداث من Kaspersky Security Center إلى أنظمة SIEM الخارجية على طرفين: Kaspersky Security Center ومستلم الحدث – نظام SIEM. لتصدير حدث بنجاح، يجب عليك تكوين هذا الحدث في نظام SIEM وفي وحدة تحكم إدارة Kaspersky Security Center. لا يهم ما الطرف الذي تقوم بتكوينه أولاً. يمكنك تكوين نقل الأحداث في Kaspersky Security Center ثم تكوين مستلم الأحداث بواسطة نظام SIEM أو العكس.

طرق إرسال الأحداث من Kaspersky Security Center

توجد ثلاث طرق لإرسال الأحداث من Kaspersky Security Center إلى الأنظمة الخارجية:

- إرسال الأحداث من خلال بروتوكول Syslog إلى أي نظام من أنظمة SIEM.

  باستخدام بروتوكول Syslog، يمكنك ترحيل أي من الأحداث التي تحدث في خادم إدارة Kaspersky Security Center وفي تطبيقات Kaspersky المثبتة على الأجهزة المدارة. بروتوكول Syslog هو بروتوكول قياسي لتسجيل الرسائل. يمكنك استخدامه لتصدير الأحداث إلى أي نظام SIEM.

  لهذا الغرض، تحتاج إلى تحديد الأحداث التي تريد ترحيلها إلى نظام SIEM. يمكنك وضع علامة على الأحداث في وحدة تحكم الإدارة أو Kaspersky Security Center Web Console. سيتم ترحيل الأحداث التي تم وضع علامة عليها فقط إلى نظام SIEM. إذا لم تضع علامة على أي شيء، فلن يتم ترحيل أي أحداث.

- إرسال الأحداث من خلال بروتوكولات CEF وLEEF إلى أنظمة QRadar وSplunk وArcSight.

  يمكنك استخدام بروتوكولي CEF وLEEF لتصدير الأحداث العامة . عند تصدير الأحداث عبر بروتوكولات CEF وLEEF، فلن يكون لديك إمكانية تحديد أحداث محددة لتصديرها. وبدلاً من ذلك، يتم تصدير جميع الأحداث العامة. لتحويل أحداث Kaspersky Security Center إلى أحداث بتنسيقي CEF وLEEF، تحتاج إلى استخدام ملف siem_conversion_rules.xml. ويحتوي هذا الملف على قائمة بسمات أحداث Kaspersky Security Center والسمات المقابلة للأحداث بتنسيقي CEF وLEEF. ويحتوي ملف siem_conversion_rules.xml أيضًا على القواعد اللازمة لإنشاء الرسائل المقابلة للأحداث. يتم تضمين هذا الملف في مجموعة توزيع Kaspersky Security Center.

  خلافًا لبروتوكول Syslog، لا تعتبر البروتوكولات CEF وLEEF بروتوكولات عامة. تكون البروتوكولات CEF وLEEF مخصصة لأنظمة SIEM المناسبة (QRadar وSplunk وArcSight). لذا، عند اختيارك لتصدير الأحداث عبر واحد من هذه البروتوكولات، فستستخدم المحلل المطلوب في نظام SIEM.

- بشكل مباشر من قاعدة بيانات Kaspersky Security Center إلى نظام SIEM.

  يمكن استخدام هذه الوسيلة الخاصة بتصدير الأحداث لاستلام الأحداث مباشرةً من طرق العرض العامة لقاعدة البيانات باستخدام استعلامات SQL. يتم حفظ نتائج الاستعلام على ملف XML يمكن استخدامه كبيانات إدخال لنظام خارجي. يمكن تصدير الأحداث المتاحة فقط في الرؤى العامة مباشرة من قاعدة البيانات.

استلام الأحداث بواسطة نظام SIEM

يجب أن يستلم نظام SIEM الأحداث المحللة بشكل صحيح والمستلمة من Kaspersky Security Center. لهذه الأغراض يجب عليك تكوين نظام SIEM على النحو الصحيح. يعتمد التكوين على نظام SIEM المحدد الذي تم استخدامه. ومع ذلك، يوجد عدد من الخطوات العامة في تكوين جميع أنظمة SIEM، مثل تكوين المستلم والمحلل.

حول تكوين تصدير الحدث في نظام SIEM

تشتمل عملية تصدير الأحداث من Kaspersky Security Center إلى أنظمة SIEM الخارجية على طرفين: Kaspersky Security Center ومستلم الحدث – نظام SIEM. يجب عليك تكوين عملية تصدير الأحداث في نظام SIEM الخاص بك وفي Kaspersky Security Center.

تعتمد الإعدادات التي تحددها في نظام SIEM على النظام المحدد الذي تستخدمه. بوجه عام، بالنسبة إلى جميع الأجهزة يتعين عليك إعداد المستلم، ولك الخيار، في إعداد محلل الرسالة لتحليل الأحداث المستلمة.

إعداد المستلم

لاستلام الأحداث التي يرسلها Kaspersky Security Center، يجب عليك إعداد المستلم في نظام SIEM الخاص بك. بوجه عام، يجب تحديد الإعدادات التالية في نظام SIEM.

- **تصدير بروتوكول أو نوع إدخال**

  إنه بروتوكول نقل الرسائل، على سبيل المثال، UDP. يجب أن يكون البروتوكول مطابقًا لما حددته في Kaspersky Security Center.

- **المنفذ**

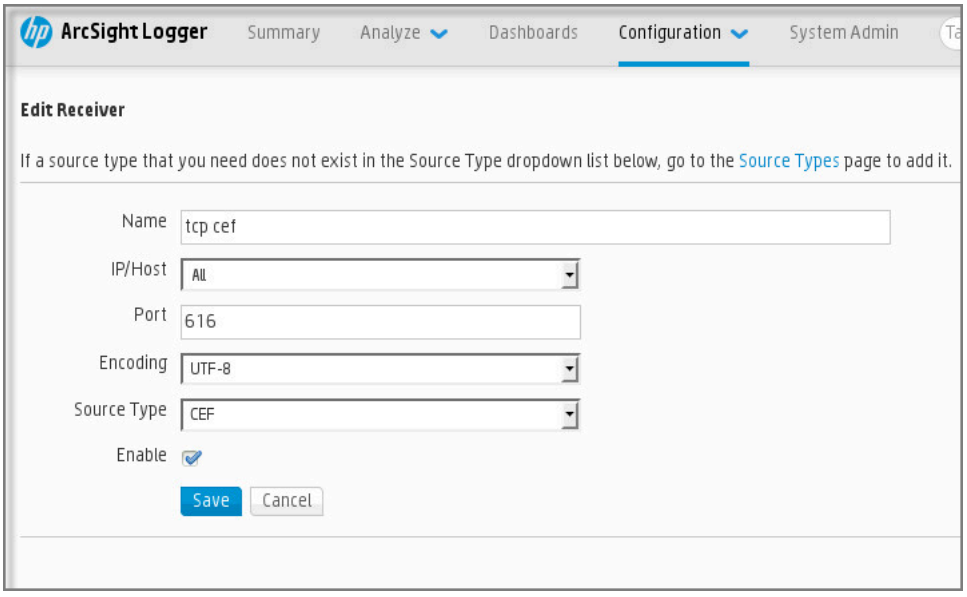
  رقم المنفذ للاتصال بـ Kaspersky Security Center. يجب أن يكون هذا المنفذ مطابقًا لما حددته في Kaspersky Security Center.

- **بروتوكول الرسالة أو نوع المصدر**

  البروتوكول المستخدم لتصدير الأحداث إلى نظام SIEM. يمكن أن يكون أحد البروتوكولات القياسية: Syslog أو CEF أو LEEF. يحدد نظام SIEM محلل الرسالة وفقًا للبروتوكول الذي تحدده.

بناءً على نظام SIEM الذي تستخدمه، قد يتعين عليك تحديد بعض الإعدادات الإضافية للمستلم.

يوضح الشكل أدناه شاشة إعداد جهاز الاستقبال في ArcSight.



إعداد المستلم في ArcSight

محلل الرسالة

يتم تمرير الأحداث التي تم تصديرها إلى أنظمة SIEM كرسائل. يجب تحليل هذه الرسائل على النحو الصحيح حتى يتسنى استخدام معلومات الأحداث بواسطة نظام SIEM. تمثل محللات الرسالة جزءًا من نظام SIEM، إذ تُستخدم لتجزئة محتويات الرسالة في الحقول ذات الصلة، مثل معرف الحدث والخطورة والوصف والمعلمات. يتيح هذا الإجراء لنظام SIEM معالجة الأحداث المستلمة من Kaspersky Security Center حتى يمكن تخزينها في قاعدة بيانات نظام SIEM.

وضع علامة على الأحداث للتصدير إلى أنظمة SIEM بتنسيق Syslog

بعد تمكين التصدير التلقائي للأحداث، يجب عليك تحديد الأحداث التي سيتم تصديرها إلى نظام SIEM الخارجي.

يمكنك تكوين تصدير الأحداث بتنسيق Syslog إلى نظام خارجي وفقًا لأحد الشروط التالية:

- وضع علامة على الأحداث العامة. إذا وضعت علامة على الأحداث التي تريد تصديرها في سياسة، فسيتلقى نظام SIEM الأحداث المحددة التي حدثت في جميع التطبيقات المُدارة من جانب السياسة المحددة. إذا تم تحديد الأحداث التي تم تصديرها في السياسة، فلن تتمكن من إعادة تحديدها لتطبيق فردي مدار بواسطة هذه السياسة.
- وضع علامة على أحداث تطبيق مُدار. إذا قمت بوضع علامة على أحداث تريد تصديرها إلى تطبيق مُدار على جهاز مُدار، فسيتلقى نظام SIEM فقط الأحداث التي حدثت في هذا التطبيق.

حول وضع علامة على الأحداث لتصديرها إلى نظام SIEM بتنسيق Syslog

بعد تمكين التصدير التلقائي للأحداث، يجب عليك تحديد الأحداث التي سيتم تصديرها إلى نظام SIEM الخارجي.

يمكنك تكوين تصدير الأحداث بتنسيق Syslog إلى نظام خارجي وفقًا لأحد الشروط التالية:

- وضع علامة على الأحداث العامة. إذا وضعت علامة على الأحداث التي تريد تصديرها في سياسة، فسيتلقى نظام SIEM الأحداث المحددة التي حدثت في جميع التطبيقات المُدارة من جانب السياسة المحددة. إذا تم تحديد الأحداث التي تم تصديرها في السياسة، فلن تتمكن من إعادة تحديدها لتطبيق فردي مدار بواسطة هذه السياسة.
- وضع علامة على أحداث تطبيق مُدار. إذا قمت بوضع علامة على أحداث تريد تصديرها إلى تطبيق مُدار على جهاز مُدار، فسيتلقى نظام SIEM فقط الأحداث التي حدثت في هذا التطبيق.

وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog

إذا كنت تريد تصدير الأحداث التي حدثت في تطبيق مُدار محدد مثبت على الأجهزة المُدارة، فقم بتمييز الأحداث للتصدير في سياسة التطبيق. في هذه الحالة، يتم تصدير الأحداث المميزة من كل الأجهزة المتضمنة في نطاق السياسة.

لتحديد الأحداث التي تريد تصديرها لتطبيق فردي مُدار:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Policies & profiles**.
2. انقر على سياسة التطبيق الذي تريد تحديد الأحداث الخاصة به.

   ستفتح نافذة إعدادات السياسة.
3. انتقل إلى قسم **Event configuration**.
4. حدد خانات الاختيار الموجودة بجوار الأحداث التي ترغب في تصديرها إلى نظام SIEM.

5. انقر على الزر **Mark for export to SIEM system by using Syslog**.

> يمكنك أيضًا تحديد حدث للتصدير إلى نظام SIEM في القسم، **Event registration** والذي يفتح بالنقر على رابط الحدث.

6. تظهر علامة الاختيار (✓)في العمود **Syslog** من الحدث أو الأحداث التي حددتها للتصدير إلى نظام SIEM.

7. انقر على زر **Save**.

الأحداث المحددة من التطبيق المُدار جاهزة للتصدير إلى نظام SIEM.

يمكنك تحديد الأحداث المراد تصديرها إلى نظام SIEM لجهاز معين مُدار. إذا تم تحديد الأحداث التي تم تصديرها مسبقًا في سياسة التطبيق، فلن تتمكن من إعادة تعريف الأحداث المحددة لجهاز مُدار.

لتحديد الأحداث التي تريد تصديرها لجهاز مُدار:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.

   يتم عرض قائمة الأجهزة المُدارة.

2. انقر فوق الرابط الذي يحمل اسم الجهاز المطلوب في قائمة الأجهزة المُدارة.

   يتم عرض نافذة خصائص الجهاز المحدد.

3. انتقل إلى قسم **Applications**.

4. انقر فوق الرابط الذي يحمل اسم التطبيق المطلوب في قائمة التطبيقات.

5. انتقل إلى قسم **Event configuration**.

6. حدد خانات الاختيار الموجودة بجوار الأحداث التي ترغب في تصديرها إلى SIEM.

7. انقر على الزر **Mark for export to SIEM system by using Syslog**.

> ويمكنك أيضا وضع علامة على حدث للتصدير إلى نظام SIEM في القسم **Event registration** الذي يفتح بالنقر فوق رابط الحدث.

8. تظهر علامة الاختيار (✓)في العمود **Syslog** من الحدث أو الأحداث التي حددتها للتصدير إلى نظام SIEM.

من الآن فصاعدًا، يرسل خادم الإدارة الأحداث المحددة إلى نظام SIEM إذا تم تكوين التصدير إلى نظام SIEM.

وضع علامة على الأحداث العامة للتصدير بتنسيق Syslog

يمكنك وضع علامة على الأحداث العامة التي سيصدرها خادم الإدارة إلى أنظمة SIEM باستخدام تنسيق Syslog.

وضع علامة على الأحداث العامة للتصدير إلى نظام SIEM:

1. قم بأحد الإجراءات التالية:

   - في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   - انتقل إلى **Assets (Devices)** ← **Policies & profiles**، ثم انقر فوق رابط السياسة.

2. في النافذة التي تفتح، انقر فوق علامة التبويب **Event configuration**.

3. انقر على **Mark for export to SIEM system by using Syslog**.

ويمكنك أيضا وضع علامة على حدث للتصدير إلى نظام SIEM في القسم **Event registration**، الذي يفتح بالنقر فوق رابط الحدث.

4. تظهر علامة الاختيار (✓)في العمود **Syslog** من الحدث أو الأحداث التي حددتها للتصدير إلى نظام SIEM.

من الآن فصاعدًا، يرسل خادم الإدارة الأحداث المحددة إلى نظام SIEM إذا تم تكوين التصدير إلى نظام SIEM.

تصدير الأحداث باستخدام تنسيقات CEF وLEEF

يمكنك استخدام تنسيقات CEF وLEEF لتصدير الأحداث العامة إلى أنظمة SIEM، وكذلك الأحداث التي تنقلها تطبيقات Kaspersky إلى خادم الإدارة. تم تحديد مجموعة تصدير الأحداث مسبقًا، ولا يمكنك تحديد أحداث لتصديرها. وقبل إرسال الأحداث إلى نظام SIEM (QRadar أو ArcSight أو Splunk)، من الضروري تفسير أحداث Kaspersky Security Center إلى أحداث بتنسيقي CEF وLEEF باستخدام القواعد المحددة في ملف siem_conversion_rules.xml.

حدد تنسيق التصدير بناءً على نظام SIEM المستخدم. يوضح الجدول أدناه أنظمة SIEM وتنسيقات التصدير المطابقة.

تنسيقات تصدير الحدث إلى نظام SIEM

نظام SIEM	تنسيق التصدير
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (التنسيق الموسع لحدث السجل)— هو تنسيق حدث مخصص لـ IBM Security QRadar SIEM. بحيث يمكن لـ QRadar دمج وتحديد ومعالجة أحداث LEEF. يجب أن تستخدم أحداث LEEF ترميز أحرف UTF-8. يمكنك العثور على المعلومات المفصلة حول بروتوكول LEEF في مركز معرفة IBM.

- CEF (تنسيق الحدث العام)—مقياس لإدارة سجل مفتوح يعمل على تحسين إمكانية التشغيل التفاعلي للمعلومات المرتبطة بالأمان من مختلف أجهزة الشبكة وتطبيقات الأمان. يتيح لك تنسيق CEF استخدام تنسيق تسجيل حدث عام حتى تتمكن من تضمين البيانات بسهولة لتحليلها بواسطة نظام إدارة المؤسسة. يجب أن تستخدم أحداث CEF ترميز أحرف UTF-8.

يمثل التصدير التلقائي إرسال Kaspersky Security Center الأحداث العامة إلى نظام SIEM. يبدأ التصدير التلقائي للأحداث بعد تمكينك له على الفور. يشرح هذا القسم بالتفصيل كيفية تمكين التصدير التلقائي للحدث.

تحويل الأحداث إلى تنسيق CEF أو LEEF

وقبل إرسال الأحداث إلى نظام SIEM (QRadar أو ArcSight أو Splunk)، من الضروري تفسير أحداث Kaspersky Security Center إلى أحداث بتنسيقي CEF وLEEF باستخدام القواعد المحددة في ملف siem_conversion_rules.xml. يتم تضمين هذا الملف في مجموعة توزيع Kaspersky Security Center.

ويحتوي ملف siem_conversion_rules.xml على قواعد التفسير المحددة مسبقًا لتحويل الأحداث إلى تنسيقي CEF وLEEF. وإذا كنت تريد استخدام قواعد تفسير الأحداث الإضافية، فيمكنك إضافتها إلى الملف يدويًا.

يتضمن ملف siem_conversion_rules.xml الأقسام التالية:

- `<"IBM"=vendor "SP_QRADAR"=product name>`

  ويحتوي هذا القسم على قواعد لإنشاء الأحداث بتنسيق LEEF، والتي يمكن تصديرها إلى نظام QRadar SIEM.

- <"HP"=vendor "SP_ARCSIGHT"=product name>.

ويحتوي هذا القسم على قواعد لإنشاء الأحداث بتنسيق CEF، والتي يمكن تصديرها إلى نظام ArcSight أو Splunk SIEM.

يحتوي كل قسم على القسم الفرعي <common>، حيث توجد سمات أحداث Kaspersky Security Center وسمات الأحداث المقابلة لها بتنسيق LEEF. وتُستخدم هذه السمات المشتركة لجميع أنواع الأحداث التي يمكن تصديرها.

لدى كل قسم أيضًا أقسام فرعية باسم <event>. ويحتوي كل قسم فرعي باسم <event> على سمات إضافية تمت إضافتها إلى تلك المدرجة في قسم <common>.

يمكنك إضافة قاعدة جديدة لإنشاء حدث إلى ملف siem_conversion_rules.xml يدويًا.

لإضافة قاعدة جديدة لإنشاء حدث:

1. أضف قسمًا فرعيًا جديدًا باسم <event> إلى قسم <"IBM"=vendor "SP_QRADAR"=product name> أو <"HP"=vendor "SP_ARCSIGHT"=name product>، ثم حدد سمات الحدث الإضافية، إذا لزم الأمر.

2. إذا كان الحدث يتكون فقط من السمات المشتركة، فسيكون القسم الفرعي <event> فارغًا.

siem_conversion_rules.xml

```
<conversion_rules>
<"IBM"=vendor "SP_QRADAR"=product name>
-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --!> <common>
<
<"STRING_T"=type "KLSPLG_HOST_DISP_NAME"=param name>
</"255"=limit "AT_STRING"=type "EVC_EV_DISP_HOST_NAME"=attr name>
<param/>
...
<common/>
Generation rule for the GNRL_EV_VIRUS_FOUND event with additional --!> <"GNRL_EV_VIRUS_FOUND"=event id>
<-- attributes
<"STRING_T"=type "GNRL_EA_PARAM_1"=param name>
</"255"=limit "AT_STRING"=type "EVC_EV_SHA256"=attr name>
<param/>
...
<event/>
...
<product/>
<"HP"=vendor "SP_ARCSIGHT"=product name>
-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --!> <common>
<
<"STRING_T"=type "KLSPLG_HOST_DISP_NAME"=param name>
</"1023"=limit "AT_STRING"=type "dhost"=attr name>
<param/>
...
<common/>
<"GNRL_EV_VIRUS_FOUND"=event id>
<"STRING_T"=type "GNRL_EA_PARAM_1"=param name>
</"255"=limit "AT_STRING"=type "cs4"=attr name>
</"SHA256"=val "AT_STRING"=type "cs4Label"=attr name>
<param/>
...
<product/>
<conversion_rules/>
```

حول تصدير الأحداث باستخدام تنسيق Syslog

يمكنك استخدام بروتوكول Syslog لتصدير الأحداث التي حدثت في خادم الإدارة وغيره من تطبيقات Kaspersky المثبتة على الأجهزة المُدارة إلى أنظمة SIEM.

Syslog هو البروتوكول القياسي لتسجيل الرسائل. ويسمح بفصل البرامج التي تنشيئ الرسائل والنظام الذي يخزنها والبرامج التي تبلغ بها وتحللها. يتم تمييز كل رسالة برمز منشأة، للإشارة إلى نوع البرنامج الذي ينشئ الرسالة ويتم تخصيص مستوى خطورة لها.

يتم تحديد بروتوكول Syslog بواسطة مستندات طلب التعليقات (RFC) التي ينشرها فريق مهام هندسة الإنترنت (معايير الإنترنت). يُستخدم معيار RFC 5424 لتصدير الأحداث من Kaspersky Security Center إلى الأنظمة الخارجية.

في Kaspersky Security Center، يمكنك تكوين تصدير الأحداث إلى الأنظمة الخارجية باستخدام تنسيق Syslog.

تتألف عملية التصدير من خطوتين:

1. تمكين التصدير التلقائي للأحداث. في هذه الخطوة، يتم تكوين Kaspersky Security Center ليرسل الأحداث إلى نظام SIEM. يبدأ Kaspersky Security Center إرسال الأحداث على الفور بعد أن تقوم بتمكين التصدير التلقائي.

2. تحديد الأحداث لتصديرها إلى النظام الخارجي. في هذه الخطوة، تحدد الحدث لتصديره إلى نظام SIEM.

تكوين Kaspersky Security Center لتصدير الأحداث إلى نظام SIEM

لتصدير الأحداث إلى نظام SIEM، يتعين عليك تكوين عملية التصدير في Kaspersky Security Center Web Console.

وقبل إرسال الأحداث إلى نظام SIEM (QRadar أو ArcSight أو Splunk)، من الضروري تفسير أحداث Kaspersky Security Center إلى أحداث بتنسيقي CEF وLEEF باستخدام القواعد المحددة في ملف siem_conversion_rules.xml.

لتكوين التصدير إلى أنظمة SIEM في Kaspersky Security Center Web Console:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.

   تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **General**، حدد القسم **Export to SIEM**.

3. انقر على الرابط **Settings**.

   يفتح قسم **Export settings**.

4. قم بتحديد الإعدادات التالية في القسم **Export settings**:

   - **SIEM system server address**

     عنوان IP للخادم المستخدم حاليًا الذي تم تثبيت نظام SIEM عليه. تحقق من هذه القيمة في إعدادات نظام SIEM لديك.

   - **SIEM system port**

     رقم المنفذ المستخدم لإنشاء اتصال بين Kaspersky Security Center وخادم نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center وفي إعدادات المستلم لنظام SIEM الخاص بك.

   - **Protocol**

     حدد البروتوكول الذي سيُستخدم لنقل الرسائل إلى نظام SIEM. يمكنك تحديد TCP أو UDP أو TLS عبر بروتوكول TCP.

     حدد إعدادات TLS التالية إذا قمت بتحديد TLS عبر بروتوكول TCP:

   - **Server authentication**

في حقل **Server authentication**، يمكنك تحديد قيم **الشهادات الموثوق بها** أو **بصمات أصابع SHA**:

- **شهادات موثوقة**. يمكنك الحصول على سلسلة شهادات كاملة (بما في ذلك شهادة الجذر) من مرجع اعتماد موثوق (CA) وتحميل الملف إلى Kaspersky Security Center. يتحقق Kaspersky Security Center مما إذا كانت سلسلة شهادة خادم نظام SIEM موقعة أيضًا من قِبل مرجع اعتماد موثوق أم لا.

  لإضافة شهادة موثوقة، انقر فوق الزر **تصفح ملف شهادات CA**، ثم قم بتحميل الشهادة.

- **بصمات SHA**. يمكنك تحديد بصمات SHA1 لسلسلة الشهادات الكاملة لنظام SIEM (بما في ذلك شهادة الجذر) في Kaspersky Security Center. لإضافة بصمة SHA1، أدخلها في الحقل **Thumbprints**، ثم انقر فوق الزر **Add**.

باستخدام إعداد **Add client authentication**، يمكنك إنشاء شهادة لمصادقة Kaspersky Security Center. وبالتالي، ستستخدم شهادة موقعة ذاتيًا صادرة عن Kaspersky Security Center. في هذه الحالة، يمكنك استخدام شهادة موثوقة وبصمة SHA لمصادقة خادم نظام SIEM.

- **Add Subject name/Subject alternative name**

اسم الموضوع هو اسم المجال الذي تم استلام الشهادة من أجله. لا يمكن لـ Kaspersky Security Center الاتصال بخادم نظام SIEM إذا كان اسم المجال لخادم نظام SIEM لا يتطابق مع اسم موضوع شهادة خادم نظام SIEM. ومع ذلك، يمكن لخادم نظام SIEM تغيير اسم المجال الخاص به إذا تم تغيير الاسم في الشهادة. في هذه الحالة، يمكنك تحديد أسماء الموضوعات في الحقل **Add Subject name/Subject alternative name**. إذا تطابق أيٍ من أسماء الموضوعات المحددة مع اسم موضوع شهادة نظام SIEM، فسيتحقق Kaspersky Security Center من صحة شهادة خادم نظام SIEM.

- **Add client authentication**

لمصادقة العميل، يمكنك إدخال شهادتك أو إنشائها في Kaspersky Security Center.

- **Insert certificate**. يمكنك استخدام شهادة استلمتها من أي مصدر، على سبيل المثال، من أي جهة إصدار موثوقة. يجب تحديد الشهادة ومفتاحها الخاص باستخدام أحد أنواع الشهادات التالية:

  - **X.509 certificate PEM**. قم بتحميل ملف بشهادة في الحقل **File with certificate**، وملف بمفتاح خاص في الحقل **File with key**. كلا الملفين لا يعتمدان على بعضهما البعض وترتيب تحميل الملفات ليس مهمًا. عند تحميل كلا الملفين، حدد كلمة المرور لفك تشفير المفتاح الخاص في حقل **Password or certificate verification**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

  - **X.509 certificate PKCS12** قم بتحميل ملف واحد يحتوي على شهادة ومفتاحها الخاص في الحقل **File with certificate**. عند تحميل الملف، حدد كلمة المرور لفك تشفير المفتاح الخاص في حقل **Password or certificate verification**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- **Generate key**. يمكنك إنشاء شهادة موقعة ذاتيًا في Kaspersky Security Center. نتيجة لذلك، يخزن Kaspersky Security Center الشهادة الموقعة ذاتيًا التي تم إنشاؤها، ويمكنك تمرير الجزء العام من الشهادة أو بصمة SHA1 إلى نظام SIEM.

- **Data format**

يمكنك تحديد تنسيقات سجل Kaspersky SIEM أو IBM QRadar SIEM أو ArcSight أو Splunk أو System، وفقًا لمتطلبات نظام SIEM.

إذا قمت بتحديد تنسيق بيانات سجل النظام، فيجب عليك تحديد:

- **Maximum message size, in bytes**

حدد أقصى حجم للرسالة (بالبايت) التي يتم ترحيلها إلى نظام SIEM. يتم ترحيل كل حدث في رسالة واحدة. إذا تجاوز الطول الفعلي للرسالة القيمة المحددة، فقد يتم اقتطاع الرسالة أو فقد البيانات. الحجم الافتراضي هو 2048 بايت. لا يتوفر هذا الحقل إلا إذا قمت بتحديد تنسيق سجل النظام في حقل **البروتوكول**.

5. إذا أردت، يمكنك تصدير الأحداث المؤرشفة من قاعدة بيانات خادم الإدارة وتعيين تاريخ البدء الذي تريد بدء تصدير الأحداث المؤرشفة منه:

a. انقر فوق الرابط **Set the export start date**.

b. في القسم الذي يفتح، حدد تاريخ البدء في حقل **Start date of system events export**.

c. انقر على زر **OK**.

6. عليك تبديل الخيار إلى الوضع **Automatically export events to SIEM system database Enabled**.

7. للتحقق من تكوين اتصال نظام SIEM، انقر فوق الزر **Check connection**.

تم إنشاء الاتصال مع خادم نظام SIEM، وتم إرسال حدث اختبار. سيتم عرض حالة الاتصال.

يتم إجراء الفحص لبروتوكولات TCP وTLS عبر TCP فقط.

8. انقر على زر **Save**.

يتم تكوين التصدير إلى نظام SIEM.

تصدير الأحداث مباشرة من قاعدة البيانات

يمكنك استعادة الأحداث مباشرة من قاعدة بيانات Kaspersky Security Center دون استخدام واجهة Kaspersky Security Center. يمكنك إما الاستعلام عن الآراء العامة مباشرة واستعادة بيانات الحدث أو إنشاء الآراء الخاصة بك بناءً على الآراء العامة الموجودة وتناولها لجمع البيانات التي تحتاج إليها.

الآراء العامة

لتسهيل الأمر عليك، يتم توفير مجموعة من الآراء العامة في قاعدة بيانات Kaspersky Security Center. يمكنك العثور على وصف طرق العرض العامة هذه في المستند klakdb.chm.

يشتمل الرأي العام v_akpub_ev_event على مجموعة حقول تمثل معلمات الحدث في قاعدة البيانات. في الوثيقة klakdb.chm يمكنك أيضًا العثور على معلومات حول الآراء العامة المطابقة لكيانات Kaspersky Security Center الأخرى، على سبيل المثال، الأجهزة أو التطبيقات أو المستخدمين. يمكنك استخدام هذه المعلومات في استعلاماتك.

يحتوي هذا القسم على تعليمات لتنفيذ استعلام SQL بواسطة أداة klsql2 المساعدة ومثال الاستعلام.

لإنشاء استعلامات SQL أو آراء قاعدة البيانات، يمكنك أيضًا استخدام أي برنامج آخر للتعامل مع قوعد البيانات. يتم ذكر معلومات حول كيفية عرض المعلمات للاتصال بقاعدة بيانات Kaspersky Security Center، مثل اسم المثيل واسم قاعدة البيانات، في القسم المقابل.

تنفيذ استعلام SQL باستخدام أداة klsql2 المساعدة

توضح هذه المقالة كيفية تنزيل أداة klsql2 المساعدة واستخدامها، وكيفية تنفيذ استعلام SQL باستخدام هذه الأداة المساعدة.

لاستخدام أداة klsql2 المساعدة:

1. حدد موقع الأداة المساعدة klsql2 في مجلد تثبيت Kaspersky Security Center. مسار التثبيت الافتراضي هو Program Files\:<Disk>\(x86) Kaspersky Security Center\Kaspersky Lab. لا تستخدم إصدارات الأداة المساعدة klsql2 المخصصة لإصدارات Kaspersky Security Center الأقدم.

2. أنشئ ملفًا بملحق .sql في أي محرر نصوص وضع الملف في المجلد نفسه باستخدام الأداة المساعدة.

3. في ملف .sql الذي تم إنشاؤه، اكتب الاستعلام الذي تريده، ثم احفظ الملف.

4. في الجهاز المثبت عليه خادم إدارة Kaspersky Security Center، في سطر الأوامر، اكتب الأمر التالي لتنفيذ استعلام SQL من الملف .sql واحفظ النتائج على الملف result.xml:

```
o result.xml- < password > p- < username > klsql2 -i src.sql -u
```

حيث < username > و < password > هما بيانات اعتماد حساب المستخدم الذي يمتلك حق الوصول إلى قاعدة البيانات.

5. وإذا لزم الأمر، أدخل معلومات تسجيل الدخول وكلمة المرور لحساب المستخدم الذي يمكنه الوصول إلى قاعدة البيانات.

6. افتح ملفات result.xml التي تم إنشاؤها حديثًا لعرض نتائج استعلام SQL.

يمكنك تحرير الملف .sql وإنشاء أي استعلام SQL للعروض العامة. بعد ذلك، من سطر الأوامر، قم بتنفيذ استعلام SQL واحفظ النتائج في ملف.

مثال لاستعلام SQL في أداة klsql2 المساعدة

يعرض هذا القسم مثالاً لاستعلام SQL، الذي يتم تنفيذه بواسطة أداة klsql2 المساعدة.

توضح الأمثلة التالية استعادة الأحداث التي حدثت في الأجهزة خلال السبعة أيام الماضية، وعرضًا للأحداث التي طُلبت وقت حدوثها، ويتم عرض الأحداث الأخيرة أولاً. ويتم عرض الأحداث الأخيرة أولاً.

مثال لبرنامج Microsoft SQL Server:

```
SELECT
/* معرف الحدث */
,e.nId

/* الوقت الذي وقع فيه الحدث */
,e.tmRiseTime

/* الاسم الداخلي لنوع الحدث */
,e.strEventType

/* الاسم المعروض للحدث */
,e.wstrEventTypeDisplayName

/* الوصف المعروض للحدث */
,e.wstrDescription

/* اسم المجموعة حيث يوجد الجهاز */
,e.wstrGroupName

/* الاسم المعروض للجهاز الذي وقع عليه الحدث */
,h.wstrDisplayName
+ '.' + ((4)AS varchar (255 & (h.nIp / 16777216)))CAST
+ '.' + ((4)AS varchar (255 & (h.nIp / 65536)))CAST
+ '.' + ((4)AS varchar (255 & (h.nIp / 256)))CAST

/* عنوان IP للجهاز الذي وقع عليه الحدث */
as strIp ((4)AS varchar (255 & (h.nIp)))CAST
FROM v_akpub_ev_event e
e.nHostId=INNER JOIN v_akpub_host h ON h.nId
(()GETUTCDATE ,7- ,Day)DATEADD=<WHERE e.tmRiseTime
ORDER BY e.tmRiseTime DESC
```

مثال لبرنامج PostgreSQL:

```
SELECT
/* معرف الحدث */
"nId"."e",

/* الوقت الذي وقع فيه الحدث */
"tmRiseTime"."e",

/* الاسم الداخلي لنوع الحدث */
"strEventType"."e",

/* الاسم المعروض للحدث*/
"wstrEventTypeDisplayName"."e",

/* الوصف المعروض للحدث */
"wstrDescription"."e",

/* الوصف المعروض للحدث */
"wstrGroupName"."e",

/* الاسم المعروض للجهاز الذي وقع عليه الحدث */
"wstrDisplayName"."h",
)
||  '.' ||  ((4)AS VARCHAR ( 255 &( 16777216 / "nIp"."h")))CAST
||  '.' ||  ((4)AS VARCHAR ( 255 &( 65536 / "nIp"."h")))CAST
||  '.' ||  ((4)AS VARCHAR ( 255 &( 256 / "nIp"."h")))CAST

/* عنوان IP للجهاز الذي وقع عليه الحدث */
((4)AS VARCHAR ( 255 &( "nIp"."h")))CAST
"strIp" AS  (
"e" AS  "v_akpub_ev_event" FROM
"nHostId"."e" = "nId"."h" ON "h" AS  "v_akpub_host"  INNER JOIN
((7  AS INT-)CAST <= days)make_interval +  'utc' AT TIME ZONE ()NOW =< "tmRiseTime"."e" WHERE
; DESC "tmRiseTime"."e" ORDER BY
```

مثال لبرنامج MySQL أو MariaDB:

```
SELECT

/* معرف الحدث */
`nId`.`e`,

/* الوقت الذي وقع فيه الحدث */
`tmRiseTime`.`e`,

/* الاسم الداخلي لنوع الحدث */
`strEventType`.`e`,

/* الاسم المعروض للحدث */
`wstrEventTypeDisplayName`.`e`,

/* الوصف المعروض للحدث */
`wstrDescription`.`e`,

/* اسم مجموعة الأجهزة */
`wstrGroupName`.`e`,

/* الاسم المعروض للجهاز الذي وقع عليه الحدث */
`wstrDisplayName`.`h`,
)CONCAT
,'.' ,(4 ,(AS CHAR (255 & (DIV  1677721  `nIp`.`h`)))CAST)LEFT
,'.' ,(4 ,(AS CHAR (255 & (DIV  65536  `nIp`.`h`)))CAST)LEFT
,'.' ,(4 ,(AS CHAR (255 & (DIV  256  `nIp`.`h`)))CAST)LEFT

/* عنوان IP للجهاز الذي وقع عليه الحدث */
(4 ,(AS CHAR (255 & (`nIp`.`h`)))CAST)LEFT
`strIp` AS  (
`e` AS  `v_akpub_ev_event` FROM
`nHostId`.`e` = `nId`.`h` ON `h` AS  `v_akpub_host`  INNER JOIN
(INTERVAL -7  DAY , ( )UTC_TIMESTAMP )ADDDATE =< `tmRiseTime`.`e` WHERE
; DESC `tmRiseTime`.`e` ORDER BY
```

عرض اسم قاعدة بيانات Kaspersky Security Center

إذا كنت ترغب في الوصول إلى قاعدة بيانات Kaspersky Security Center بواسطة خادم SQL Server أو أدوات إدارة قاعدة بيانات MariaDB، فيتعين عليك معرفة اسم قاعدة البيانات للاتصال بها من محرر البرنامج النصي SQL الخاص بك.

لعرض اسم قاعدة بيانات Kaspersky Security Center:

1. في القائمة الرئيسية، انقر فوق أيقونة الإعدادات ( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب **General**، حدد القسم **Details of current database**.

يتم تحديد اسم قاعدة البيانات في حقل **Database name**. استخدام اسم قاعدة البيانات لمعالجة قاعدة البيانات في استعلامات SQL الخاصة بك.

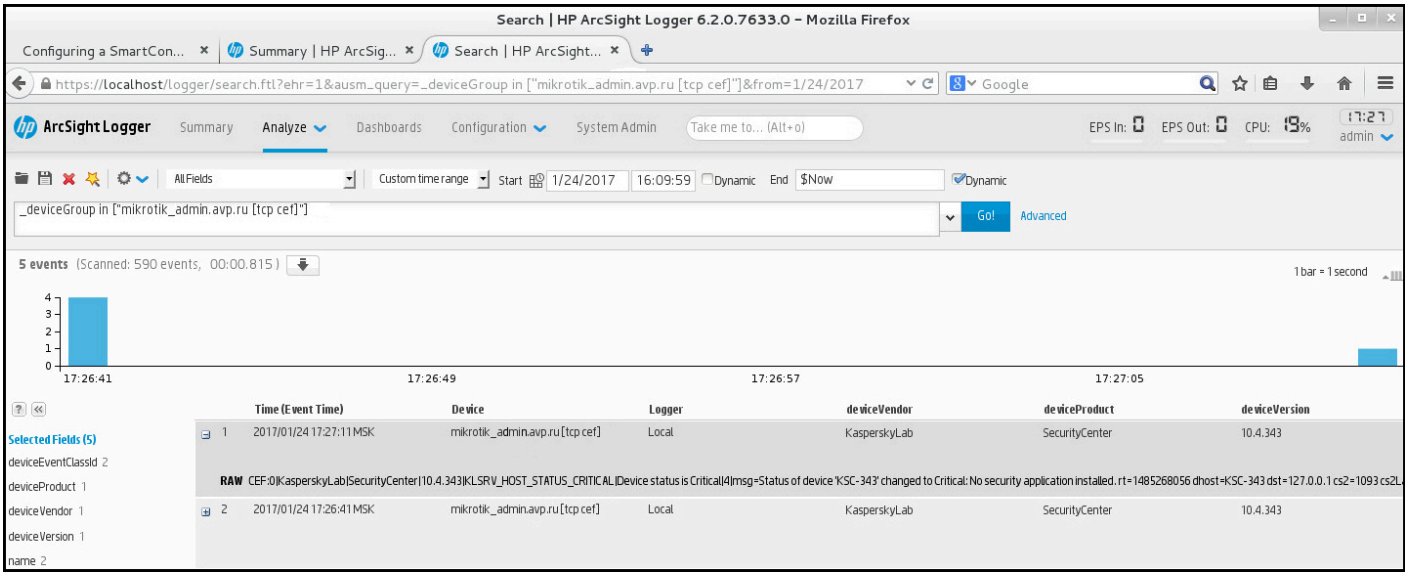
عرض نتائج التصدير

يمكنك التحكم في إكمال إجراء تصدير الحدث بنجاح. وللقيام بهذا الإجراء، تحقق من استلام نظام SIEM الخاص بك للرسائل المشتملة على أحداث التصدير

إذا تم استلام الأحداث المرسلة من Kaspersky Security Center وتحليلها على النحو الصحيح بواسطة نظام SIEM الخاص بك، فسيتم تنفيذ التكوين بشكل صحيح على كلا الجانبين. في الجانب الآخر، تحقق من أن الإعدادات التي حددتها في Kaspersky Security Center مقابلة للتكوين في نظام SIEM الخاص بك.

يوضح الشكل أدناه الأحداث التي تم تصديرها إلى ArcSight. على سبيل المثال، يعتبر الحدث الأول حدثًا مهمًا لخادم الإدارة: "حالة الجهاز حرجة".

يتباين تمثيل أحداث التصدير في نظام SIEM بحسب نظام SIEM الذي تستخدمه.



مثال للأحداث

العمل باستخدام Kaspersky Security Center Web Console في بيئة السحابة

يوفر هذا القسم معلومات حول ميزة Kaspersky Security Center Web Console المتعلقة بنشر Kaspersky Security Center وصيانته في بيئات السحابة، مثل Amazon Web Services أو Microsoft Azure أو Google Cloud.

للعمل في بيئة سحابة، أنت بحاجة إلى ترخيص خاص. إذا لم يكن لديك ذلك الترخيص، لن يتم عرض عناصر الواجهة ذات الصلة بالأجهزة السحابية.

تكوين بيئة السحابة في Kaspersky Security Center Web Console

لتكوين Kaspersky Security Center باستخدام هذه البيئة، يجب أن تمتلك ما يلي:

- بيانات اعتماد محددة لبيئة السحابة:
  - دور IAM الذي تم منحه حق استقصاء قطاع السحابة أو حساب مستخدم IAM الذي تم منحه حق استقصاء قطاع السحابة (للعمل مع Amazon Web Services)
  - معرف تطبيق Azure، وكلمة المرور، والاشتراك (للعمل في بيئة السحابة لـ Microsoft Azure)
  - البريد الإلكتروني لعميل Google ومعرف المشروع والمفتاح الخاص (للعمل مع Google Cloud)
- حزم التثبيت:
  - عميل الشبكة لنظام التشغيل Windows
  - عميل الشبكة لنظام التشغيل Linux
  - Kaspersky Endpoint Security for Linux
- المكون الإضافي للويب لـ Kaspersky Endpoint Security for Linux
- أحد ما يلي على الأقل:
  - حزمة التثبيت ومكوّن الويب الإضافي لتطبيق Kaspersky Endpoint Security for Windows (موصى به)
  - حزمة التثبيت ومكوّن الويب الإضافي لبرنامج Kaspersky Security لخادم Windows

سيبدأ تشغيل تكوين بيئة السحابة تلقائيًا في أول اتصال بخادم الإدارة من خلال وحدة تحكم الإدارة إذا نشرت Kaspersky Security Center من صورة جاهزة للاستخدام. يمكنك أيضًا بدء تشغيل المعالج في أي وقت.

لبدء تشغيل معالج تكوين بيئة السحابة يدويًا،

في القائمة الرئيسية، انتقل إلى **Configure cloud environment** ← **Deployment & assignment** ← **Discovery & deployment**.

سيبدأ المعالج.

تستغرق جلسة العمل المتوسطة لتكوين بيئة السحابة 15 دقيقة تقريبًا.

الخطوة 1. تحقق من حزم التثبيت والمكونات الإضافية

لا يتم عرض هذه الخطوة إذا كان لديك كل البرامج الإضافية المطلوبة للويب وحزم التثبيت المدرجة أدناه.

لتكوين بيئة سحابية، يجب أن يكون لديك المكونات التالية:

- حزم التثبيت:
  - عميل الشبكة لنظام التشغيل Windows
  - عميل الشبكة لنظام التشغيل Linux
  - Kaspersky Endpoint Security for Linux
- المكون الإضافي للويب لـ Kaspersky Endpoint Security for Linux
- أحد ما يلي على الأقل:
  - حزمة التثبيت ومكوّن الويب الإضافي لتطبيق Kaspersky Endpoint Security for Windows (موصى به)
  - حزمة التثبيت ومكوّن الويب الإضافي لبرنامج Kaspersky Security لخادم Windows

  نوصي باستخدام Kaspersky Endpoint Security for Windows بدلاً من Kaspersky Security for Windows Server.

يكتشف Kaspersky Security Center تلقائيًا المكونات التي لديك بالفعل ويسرد فقط المكونات المفقودة. قم بتنزيل المكونات المدرجة عن طريق النقر على زر **حدد التطبيقات المراد تنزيلها**، ثم تحديد المكونات الإضافية وحزم التثبيت المطلوبة. بعد تنزيل أحد المكونات، يمكنك استخدام زر **ينعش** لتحديث قائمة المكونات المفقودة.

الخطوة 2. ترخيص التطبيق

لا يتم عرض هذه الخطوة إلا إذا كنت تستخدم BYOL AMI وقد قمت بتفعيل التطبيق باستخدام ترخيص Kaspersky Security for Virtualization أو ترخيص Kaspersky Hybrid Cloud Security.

حدد مفتاح الترخيص ثم انقر على **Next** للمتابعة.

يتم إضافة مفتاح الترخيص إلى تخزين خادم الإدارة.

إذا قمت بتشغيل المعالج مرة أخرى، لن يتم عرض هذه الخطوة.

الخطوة 3. تحديد بيئة السحابة والمصادقة

يوضح هذا القسم الميزات التي تنطبق فقط على تطبيق Kaspersky Security Center 12.1 Web Console أو الإصدار الأحدث.

حدد الإعدادات التالية:

- **Cloud environment**

حدد بيئة السحابة التي تقوم فيها بنشر Kaspersky Security Center: AWS أو Azure.

إذا كنت تخطط للعمل مع أكثر من بيئة سحابية واحدة، حدد بيئة واحدة ثم قم بتشغيل المعالج مرة أخرى.

- **Connection name**

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google".

أدخل بيانات الاعتماد الخاصة بك لاستلام التصديق في بيئة السحابة التي حددتها.

AWS

إذا حددت AWS لتكون نوع قطاع السحابة، أنت بحاجة إلى دور IAM أو مفتاح وصول AWS IAM لإجراء المزيد من الاستقصاءات على قطاع السحابة:

- **AWS IAM role assigned to an EC2 instance**

حدد هذا الخيار إذا كان لديك دور IAM بالحقوق المطلوبة لخادم الإدارة.

- **AWS IAM user**

حدد هذا الخيار إذا كان لديم مفتاح وصول AWS IAM. أدخل بيانات مفتاحك:

- **Access key ID**

يكون معرف مفتاح وصول IAM عبارة عن تسلسل من الحروف الأبجدية الرقمية. لقد تلقيت معرف مفتاح عند إنشائك حساب مستخدم IAM.

هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

- **Secret key**

المفتاح السري الذي تلقيته مع معرف مفتاح الوصول عند إنشائك حساب مستخدم IAM.

تظهر حروف المفتاح السري في صورة علامة النجمة. بعد أن تبدأ في إدخال المفتاح السري، سيظهر الزر **إظهار** . انقر مع الاستمرار فوق هذا الزر لتحديد الفترة الزمنية اللازمة لإظهار الحروف التي أدخلتها.

هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

Azure

إذا قمت بتحديد Azure لتكون نوع قطاع السحابة، حدد الإعدادات التالية للاتصال الذي سيتم استخدامه لاستقصاء قطاع السحابة بعد ذلك:

- **Azure Application ID**

لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

- **Azure Subscription ID**

لقد قمت بإنشاء الاشتراك على مدخل Azure.

- **Azure Application password**

لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

- **اسم حساب تخزين Azure**

لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

- **مفتاح وصول تخزين Azure**

لقد حصلت على كلمة المرور (المفتاح) عند إنشائك لحساب تخزين Azure لاستخدام Kaspersky Security Center.

يكون المفتاح متاحًا في القسم "نظرة عامة على حساب تخزين Azure"، في القسم الفرعي "المفاتيح".

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

Google Cloud

إذا حددت Google Cloud ليكون نوع قطاع السحابة، حدد الإعدادات التالية للاتصال الذي سيتم استخدامه لاستقصاء قطاع السحابة بعد ذلك:

- **Client email address**

البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

- **Project ID**

معرف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

- **Private key**

المفتاح الخاص هو تسلسل الأحرف التي استلمتها كمفتاح خاص عند تسجيل مشروعك في Google Cloud. قد ترغب في نسخ هذا التسلسل ولصقه لتجنب الأخطاء.

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

يتم حفظ الاتصال الذي حددته في إعدادات التطبيق.

يسمح لك معالج تكوين بيئة السحابة بتحديد قطاع واحد فقط. يمكنك بعد ذلك تحديد المزيد من الاتصالات لإدارة قطاعات السحابة الأخرى.

انقر على **Next**للمضي قدما.

الخطوة 4. استقصاء القطاع، تكوين المزامنة مع السحابة واختيار إجراءات إضافية

في هذه الخطوة، سيبدأ استقصاء قطاع السحابة وسيتم إنشاء مجموعة إدارة خاصة للمثيلات لأجهزة السحابة تلقائيًا. تم وضع الأجهزة التي تم العثور عليها أثناء الاستقصاء في هذه المجموعة. يتم تكوين الجدول الزمني لاستقصاء قطاع السحابة (كل 5 دقائق بشكل افتراضي؛ يمكنك تغيير هذا الإعداد لاحقًا).

سيتم أيضًا إنشاء قاعدة النقل التلقائي **المزامنة مع السحابة**. بالنسبة إلى كل عملية فحص تالية لشبكة السحابة، سيتم نقل الأجهزة الظاهرية التي تم اكتشافها إلى المجموعة الفرعية المقابلة في المجموعة **الأجهزة المُدارة/السحابة**.

حدد الإعدادات التالية:

- **Synchronize administration groups with cloud structure**

إذا تم تمكين هذا الخيار، سيتم إنشاء مجموعة **السحابة** تلقائيًا في مجموعة **الأجهزة المُدارة** وسيتم بدء اكتشاف أجهزة السحابة. يتم وضع الأجهزة الظاهرية والمثيلات التي تم اكتشافها أثناء كل عملية فحص لشبكة السحابة في مجموعة السحابة. تتوافق بنية المجموعات الفرعية للإدارة الموجودة ضمن هذه المجموعة مع بنية قطاع السحابة الخاص بك (في AWS، لا يتم تمثيل مناطق التوفر ومجموعات تعيين الموضع في البنية؛ في Azure، لا يتم تمثيل الشبكات الفرعية في البنية). توجد الأجهزة التي لم يتم تحديدها كمثيلات في بيئة السحابة في مجموعة **الأجهزة غير المخصصة**. تسمح لك بنية المجموعة هذه باستخدام مهام التثبيت الجماعية، لتثبيت تطبيقات مكافحة الفيروسات على المثيلات وإعداد سياسات مختلفة للمجموعات المختلفة.

إذا تم تعطيل هذا الخيار، فسيتم أيضًا إنشاء مجموعة **السحابة** وبدء تشغيل اكتشاف أجهزة السحابة كذلك؛ إلا إنه لن يتم إنشاء المجموعات الفرعية التي تتوافق مع بنية قطاع السحابة ضمن المجموعة. توجد جميع المثيلات المكتشفة في مجموعة إدارة **السحابة** ولذلك يتم عرضها في قائمة واحدة. إذا كان استخدامك لـ Kaspersky Security Center يتطلب إجراء مزامنة، فيمكنك تعديل خصائص قاعدة **المزامنة مع السحابة** وفرضها. يؤدي فرض هذه القاعدة إلى حدوث تغيير في بنية المجموعات الفرعية في مجموعة السحابة لكي تتطابق مع بنية قطاع السحابة الخاص بك.

يتم تعطيل هذا الخيار افتراضيًا.

- **Deploy protection**

إذا تم تحديد هذا الخيار، فسينشئ المعالج مهمة لتثبيت تطبيقات الأمان على المثيلات. بعد انتهاء المعالج، سيبدأ تشغيل معالج نشر الحماية تلقائيًا على الأجهزة في قطاعات السحابة الخاصة بك، وستتمكن من تثبيت عميل الشبكة وتطبيقات الأمان على هذه الأجهزة.

يستطيع Kaspersky Security Center القيام بالنشر باستخدام أدواته الأصلية. إذا لم تكن تمتلك أذونات لتثبيت التطبيقات على مثيلات EC2 أو على الأجهزة الظاهرية لـ Azure، يمكنك تكوين مهمة **التثبيت عن بُعد** يدويًا وتحديد حساب يمتلك الأذونات المطلوبة. في هذه الحالة، لن يعمل التثبيت عن بُعد مع الأجهزة التي تم اكتشافها بواسطة AWS API أو Azure. ستعمل هذه المهمة فقط مع الأجهزة المكتشفة باستخدام استقصاء Active Directory، أو استقصاء مجالات Windows، أو استقصاء نطاق IP.

إذا تم إلغاء تحديد هذا الخيار، فلن يبدأ تشغيل معالج نشر الحماية ولن يتم إنشاء مهام تثبيت تطبيقات الأمان على المثيلات. يمكنك تنفيذ كلا الإجراءين يدويًا في وقت لاحق.

إذا قمت بتحديد خيار Deploy protection، سيصبح قسم **Restarting devices** متاحًا. في هذا القسم، يجب عليك اختيار ما ستفعله عندما يتوجب إعادة تشغيل نظام التشغيل في جهاز الهدف. حدد ما إذا كان سيتم إعادة تشغيل المثيلات إذا كان من الضروري إعادة تشغيل نظام التشغيل الخاص بالجهاز أثناء تثبيت التطبيقات:

- **Do not restart**

في حالة تحديد هذا الخيار، لن يتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

- **Restart**

في حالة تحديد هذا الخيار، فستتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

انقر على **Next**للمضي قدما.

بالنسبة إلى Google Cloud، يمكنك فقط إجراء النشر باستخدام الأدوات الأصلية لـ Kaspersky Security Center. إذا قمت بتحديد Google Cloud، فلا يكون الخيار **Deploy protection** غير متوفر.

الخطوة 5. اختيار تطبيق لإنشاء سياسة ومهام لـ

يتم عرض هذه الخطوة فقط إذا كانت لديك حزم تثبيت ومكونات إضافية لكل من Kaspersky Endpoint Security for Windows و Kaspersky Security for Windows Server. إذا كان لديك مكون إضافي وحزمة تثبيت لواحد فقط من هذه التطبيقات، فسيتم تخطي هذه الخطوة ويقوم Kaspersky Security Center بإنشاء سياسة ومهام للتطبيق الحالي.

حدد التطبيق الذي تريد إنشاء سياسة ومهام له:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

الخطوة 6. تكوين Kaspersky Security Network لأجل Kaspersky Security Center

حدد إعدادات ترحيل المعلومات حول عمليات Kaspersky Security Center إلى قاعدة معارف Kaspersky Security Network (KSN). حدد أحد الخيارات التالية:

- **I agree to use Kaspersky Security Network**

  سيقوم Kaspersky Security Center والتطبيقات المدارة المثبتة على الأجهزة العميلة بنقل تفاصيل عملياته تلقائيًا إلى Kaspersky Security Network. تضمن المشاركة في Kaspersky Security Network التحديثات السريعة لقواعد البيانات التي تشتمل على معلومات حول الفيروسات وغيرها من التهديدات، مما يضمن الاستجابة السريعة للتهديدات الأمنية الطارئة.

- **I do not agree to use Kaspersky Security Network**

  لن يوفر Kaspersky Security Center والتطبيقات المدارة أية معلومات إلى Kaspersky Security Network.

  إذا قمت بتحديد هذا الخيار، فسيتم تعطيل استخدام Kaspersky Security Network.

توصي Kaspersky بالمشاركة في Kaspersky Security Network.

يمكن كذلك عرض اتفاقيات KSN للتطبيقات المُدارة. إذا وافقت على استخدام Kaspersky Security Network، سيرسل التطبيق المُدار البيانات إلى Kaspersky. إذا لم توافق على المشاركة في Kaspersky Security Network، لن يرسل التطبيق المُدار بيانات إلى Kaspersky (يمكنك تغيير هذا الإعداد لاحقًا في سياسة التطبيق).

انقر على **Next**للمضي قدما.

الخطوة 7. إنشاء تكوين أولي للحماية

يمكنك التحقق من قائمة بالسياسات والمهام التي تم إنشاؤها.

انتظر حتى يكتمل إنشاء السياسات والمهام ثم انقر على **Next** للمتابعة. في آخر صفحة من المعالج، انقر على الزر **Finish** للخروج.

استقصاء مقطع الشبكة عبر Kaspersky Security Center Web Console

يتم استلام معلومات حول بنية الشبكة (والأجهزة فيها) عن طريق خادم الإدارة من خلال الاستقصاء العادي لقطاعات السحابة باستخدام أدوات AWS API أو Azure API أو Google API. Kaspersky Security Center يستخدم هذه المعلومات لتحديث محتويات مجلدات الأجهزة غير المخصصة والأجهزة المُدارة. إذا قمت بتكوين الأجهزة التي سيتم نقلها إلى مجموعات الإدارة تلقائيًا، سيتم تضمين الأجهزة التي تم اكتشافها في مجموعات الإدارة.

للسماح لخادم الإدارة باستقصاء قطاعات السحابة، يجب أن يكون لديك الحقوق المطلوبة المقدمة مع دور IAM أو حساب مستخدم IAM (في AWS) أو مع معرف التطبيق وكلمة المرور (في Azure) أو مع بريد العميل الإلكتروني على جوجل ومعرف مشروع جوجل والمفتاح الخاص (في Google Cloud).

يمكنك إضافة الاتصالات وحذفها، بالإضافة إلى ضبط جدول الاستقصاء لكل قطاع سحابة.

إضافة اتصالات لاستقصاء قطاع السحابة

لإضافة اتصال لاستقصاء قطاع السحابة لقائمة الاتصالات المتاحة:

1. في القائمة الرئيسية، انتقل إلى **Cloud** ← **Discovery** ← **Discovery & deployment**.

2. في النافذة التي تفتح، انقر على **Properties**.

3. في نافذة **Settings** التي تفتح، انقر على **Add**.

   ستفتح نافذة **Cloud segment settings**.

4. حدد اسم بيئة السحابة للاتصال الذي سيتم استخدامه لإجراء المزيد من الاستقصاءات على قطاع السحابة:

   - **Cloud environment**

     حدد بيئة السحابة التي تقوم فيها بنشر Kaspersky Security Center: AWS أو Azure.

     إذا كنت تخطط للعمل مع أكثر من بيئة سحابية واحدة، حدد بيئة واحدة ثم قم بتشغيل المعالج مرة أخرى.

   - **Connection name**

     أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفًا. لا يُسمح إلا بحروف Unicode

     كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة.

     إذا كنت تخطط للعمل مع أكثر من بيئة سحابة واحدة، فقد ترغب في تضمين اسم البيئة في اسم الاتصال، على سبيل المثال، "قطاع Azure" أو "قطاع AWS" أو "قطاع Google".

5. أدخل بيانات الاعتماد الخاصة بك لاستلام التصديق في بيئة السحابة التي حددتها.

   - إذا حددت AWS، فحدد الإعدادات التالية:

     - **Use AWS IAM role**

       حدد هذا الخيار إذا قمت بالفعل بإنشاء دور IAM لخادم الإدارة ليستخدم خدمات AWS.

     - **AWS IAM user account credentials**

       حدد هذا الخيار إذا كان لديك حساب مستخدم IAM لديه الأذونات المطلوبة ويمكنك إدخال معرّف مفتاح والمفتاح السري.

       إذا حددت أنك تملك AWS IAM user account credentials، حدد ما يلي:

       - **Access key ID**

         يكون معرف مفتاح وصول IAM عبارة عن تسلسل من الحروف الأبجدية الرقمية. لقد تلقيت معرف مفتاح عند إنشائك حساب مستخدم IAM.

         هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

       - **Secret key**

         المفتاح السري الذي تلقيته مع معرف مفتاح الوصول عند إنشائك حساب مستخدم IAM.

         تظهر حروف المفتاح السري في صورة علامة النجمة. بعد أن تبدأ في إدخال المفتاح السري، سيظهر الزر **إظهار** . انقر مع الاستمرار فوق هذا الزر لتحديد الفترة الزمنية اللازمة لإظهار الحروف التي أدخلتها.

         هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

     لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

- إذا حددت Azure، فحدد الإعدادات التالية:

  - **Azure Application ID**

    لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

    يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

  - **Azure Subscription ID**

    لقد قمت بإنشاء الاشتراك على مدخل Azure.

  - **Azure Application password**

    لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

    تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

    لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

  - **Azure storage account name**

    لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

  - **Azure storage access key**

    لقد حصلت على كلمة المرور (المفتاح) عند إنشائك لحساب تخزين Azure لاستخدام Kaspersky Security Center.

    يكون المفتاح متاحًا في القسم "نظرة عامة على حساب تخزين Azure"، في القسم الفرعي "المفاتيح".

    لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

- إذا حددت Google Cloud، فحدد الإعدادات التالية:

  - **Client email address**

    البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

  - **Project ID**

    معرف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

  - **Private key**

    المفتاح الخاص هو تسلسل الأحرف التي استلمتها كمفتاح خاص عند تسجيل مشروعك في Google Cloud. قد ترغب في نسخ هذا التسلسل ولصقه لتجنب الأخطاء.

    لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **Show**.

6. يمكنك إذا كنت ترغب النقر على **Set polling schedule** ثم تغيير الإعدادات الافتراضية.

   يتم حفظ الاتصال في إعدادات التطبيق.

بعد استقصاء قطاع السحابة الجديد لأول مرة، تظهر المجموعة الفرعية المقابلة لذلك القطاع في مجموعة الإدارة **الأجهزة المُدارة/السحابة**.

إذا قمت بتحديد بيانات اعتماد غير صحيحة، فلن تجد أي مثيلات أثناء استقصاء قطاع السحابة، ولن تظهر مجموعة فرعية جديدة في مجموعة الإدارة **الأجهزة المُدارة/السحابة**.

حذف اتصال خاص باستقصاء قطاع السحابة

إذا لم يعد من الضروري استقصاء قطاع سحابة محدد، يمكنك حذف الاتصال المطابق لذلك القطاع من قائمة الاتصالات المتاحة. يمكنك أيضًا حذف اتصال، على سبيل المثال إذا كانت أذونات استقصاء قطاع سحابة قد تم نقلها إلى مستخدم آخر يملك بيانات اعتماد مختلفة.

لحذف اتصال:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Discovery** ← **Cloud**.
2. في النافذة التي تفتح، انقر على **Properties**.
3. في نافذة **Settings** التي تفتح، انقر على اسم القطاع الذي ترغب في حذفه.
4. انقر على **Delete**.
5. في النافذة التي تفتح انقر على زر **OK** لتأكيد اختيارك.

يتم حذف الاتصال. الأجهزة في قطاع السحابة المطابقة لهذا الاتصال يتم حذفها من مجموعات الإدارة تلقائيًا.

تكوين جدول الاستقصاء عبر Kaspersky Security Center Web Console

يتم تنفيذ استقصاء قطاع السحابة وفقًا لجدول. يمكنك إعداد تكرار الاستقصاء.

يتم إعداد تكرار التحقق من إرسال البيانات تلقائيًا في غضون 5 دقائق في إعدادات تكوين بيئة السحابة. يمكنك تغيير هذه القيمة في أي وقت وإعداد جدول آخر. ومع ذلك، لا يوصى بتكوين الاستقصاء ليتم تشغيله بصورة متكررة بعد أقل من 5 دقائق لأن ذلك قد يؤدي إلى ظهور أخطاء في تشغيل API.

لتكوين جدول استقصاء قطاع السحابة:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Discovery** ← **Cloud**.
2. في النافذة التي تفتح، انقر على **Properties**.
3. في نافذة **Settings** التي تفتخ، انقر على اسم القطاع الذي ترغب في تكوين جدول استقصاء له.
   سيفتح هذا نافذة **Cloud segment settings**.
4. في النافذة **Cloud segment settings**، انقر على زر **Set polling schedule**.
   يؤدي ذلك إلى فتح نافذة **Schedule**.
5. في نافذة **Schedule**، حدد الإعدادات التالية:
   - **Scheduled start**
     خيارات جدول الاستقصاء:
   - **Every N days**

     يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين.

     بشكل افتراضي، يعمل الاستقصاء كل يوم، بداية من التاريخ والوقت الحاليين للنظام.

- Every N minutes

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل خمس دقائق، بداية من الوقت الحالي للنظام.

- By days of week

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 00:00:6 مساءً.

- Every month on specified days of selected weeks

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

بشكلٍ افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 00:00:6 مساءً.

- **موعد البدء**

حدد قيمة ن (لدقائق أو أيام).

- **Starting from**

حدد متى يبدأ أول استقصاء.

- **Run missed tasks**

إذا كان خادم الإدارة مغلقًا أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فورًا بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فورًا بعد تشغيله.

إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها.

يتم تمكين هذا الخيار افتراضيًا.

6. احفظ التغييرات.

يتم تكوين جدول الاستقصاء للقطاع وحفظه.

عرض نتائج استقصاء قطاع السحابة عبر Kaspersky Security Center Web Console

يمكنك عرض نتائج استقصاء قطاع السحابة، أي عرض قائمة أجهزة السحابة التي يديرها خادم الإدارة.

لعرض نتائج استقصاء قطاع السحابة،

في القائمة الرئيسية، انتقل إلى **Cloud** ← **Discovery** ← **Discovery & deployment**.

يعرض هذا قطاعات السحابة المتوفرة للاستقصاء.

عرض خصائص الأجهزة السحابية عبر Kaspersky Security Center Web Console

يمكنك عرض خصائص كل جهاز سحابة.

لعرض خصائص جهاز السحابة:

1. في القائمة الرئيسية، انتقل إلى **Assets (Devices)** ← **Managed devices**.

2. انقر على اسم الجهاز الذي ترغب في عرض خصائصه.
   ستفتح نافذة خصائص مع قسم **General** محدد.

3. إذا كنت ترغب في عرض الخصائص المحددة لأجهزة السحابة، حدد قسم **System** في نافذة الخصائص.
   يتم عرض الخصائص اعتمادًا على منصة السحابة للجهاز.
   للأجهزة في AWS، يتم عرض الخصائص التالية:

- **الجهاز المكتشف باستخدام API** (القيمة: **AWS**)
- **منطقة السحابة**
- **Cloud VPC**
- **منطقة توافر السحابة**
- **الشبكة الفرعية السحابية**
- **مجموعة وضع السحابة** (يتم عرض هذه الوحدة فقط إذا كان المثيل ينتمي إلى مجموعة الوضع؛ وإلا فلن يتم عرضه)

للأجهزة في Azure، يتم عرض الخصائص التالية:

- **الجهاز المكتشف باستخدام API** (القيمة: **Microsoft Azure**)
- **منطقة السحابة**
- **الشبكة الفرعية السحابية**

للأجهزة في Google Cloud، يتم عرض الخصائص التالية:

- **الجهاز المكتشف باستخدام API** (القيمة: **Google Cloud**)
- **منطقة السحابة**
- **Cloud VPC**
- **منطقة توافر السحابة**
- **الشبكة الفرعية السحابية**

التزامن مع السحابة: تكوين قاعدة النقل

أثناء عملية تكوين بيئة السحابة، سيتم إنشاء القاعدة المزامنة مع السحابة تلقائيًا. تسمح لك هذه القاعدة بنقل الأجهزة التي تم اكتشافها في كل استقصاء تلقائيًا من مجموعة الأجهزة غير المخصصة إلى مجموعة الأجهزة المُدارة\أجهزة السحابة لتوفير هذه الأجهزة للإدارة المركزية. بشكل افتراضي، ستكون القاعدة نشطة بعد إنشائها. يمكنك تعطيل القاعدة أو تعديلها أو فرضها في أي وقت.

لتحرير خصائص قاعدة المزامنة مع السحابة و/أو فرض القاعدة:

1. في القائمة الرئيسية، انتقل إلى **Discovery & deployment** ← **Deployment & assignment** ← **Moving rules**.

يفتح هذا قائمة بقواعد النقل.

2. في قائمة قواعد النقل، حدد **Synchronize with cloud**.

يفتح هذا نافذة خصائص القاعدة.

3. يمكنك عند الضرورة تحديد الإعدادات التالية في تبويب **Rule conditions** في تبويب**Cloud segments**:

- **Device is in a cloud segment**

لا تنطبق القاعدة إلا على الأجهزة الموجودة في قطاع السحابة المحدد. خلافًا لذلك، فستطبق القاعدة على جميع الأجهزة التي تم اكتشافها.

يتم تحديد هذا الخيار افتراضيًا.

- **Include child objects**

تطبق القاعدة على جميع الأجهزة الموجودة في القطاع المحدد وفي جميع الأقسام الفرعية السحابية المتداخلة. خلافًا لذلك، فستطبق القاعدة فقط على الأجهزة الموجودة قطاع الجذر.

يتم تحديد هذا الخيار افتراضيًا.

- **Move devices from nested objects to corresponding subgroups**

إذا تم تمكين هذا الخيار، فستنتقل الأجهزة من الكائنات المتداخلة تلقائيًا إلى المجموعات الفرعية التي تتوافق مع بنيتها.

إذا تم تعطيل هذا الخيار، سيتم نقل الأجهزة من الكائنات المتداخلة تلقائيًا إلى جذر المجموعة الفرعية للسحابة دون أي تفريع لاحق.

يتم تمكين هذا الخيار افتراضيًا.

- **Create subgroups corresponding to containers of newly detected devices**

إذا تم تمكين هذا الخيار، في حالة عدم اشتمال بنية مجموعة **الأجهزة المُدارة/السحابة** على مجموعات فرعية تتوافق مع القسم الذي يحتوي على الجهاز، فسيقوم Kaspersky Security Center بإنشاء هذه المجموعات الفرعية. على سبيل المثال، إذا تم اكتشاف شبكة فرعية جديدة أثناء اكتشاف الأجهزة، سيتم إنشاء مجموعة جديدة تحمل نفس الاسم ضمن المجموعة **الأجهزة المدارة/السحابة**.

إذا تم تعطيل هذا الخيار، فلن يقوم Kaspersky Security Center بإنشاء أي مجموعات فرعية جديدة. على سبيل المثال، إذا تم اكتشاف شبكة فرعية جديدة أثناء استقصاء الشبكة، فلن يتم إنشاء مجموعة جديدة تحمل نفس الاسم ضمن المجموعة **الأجهزة المُدارة/السحابة**، وسيتم نقل الأجهزة الموجودة في هذه الشبكة الفرعية إلى المجموعة **الأجهزة المُدارة/السحابة**.

يتم تمكين هذا الخيار افتراضيًا.

- **Delete subgroups for which no match is found in the cloud segments**

إذا تم تمكين هذا الخيار، فسيحذف التطبيق من مجموعة السحابة جميع المجموعات الفرعية التي لا تطابق أي من كائنات السحابة الموجودة.

إذا تم تعطيل هذا الخيار، فسيتم الاحتفاظ بالمجموعات الفرعية التي لا تطابق أي من كائنات السحابة الموجودة.

يتم تمكين هذا الخيار افتراضيًا.

إذا قمت بتمكين الخيار **Synchronize administration groups with cloud structure** عند استخدام تكوين بيئة السحابة، يتم إنشاء القاعدة **Synchronize with cloud devices** مع تمكين الخيارين **Create subgroups corresponding to containers of newly detected devices** و**Delete subgroups for which no match is found in the cloud segments**.

إذا لم تقم بتفعيل خيار **Synchronize administration groups with cloud structure**، سيتم إنشاء قاعدة **Synchronize with cloud** بحيث تكون هذه الخيارات معطلة (تم إلغاء تحديدها). إذا كان استخدامك لتطبيق Kaspersky Security Center يتطلب أن تتوافق بنية المجموعات الفرعية في المجموعة الفرعية **الأجهزة المُدارة\السحابة** مع بنية قطاعات السحابة، فقم بتمكين الخيارين **Create subgroups corresponding to containers of newly detected devices** و**Delete subgroups for which no match is found in the cloud segments** في خصائص القاعدة، ثم افرض القاعدة.

4. في القائمة المنسدلة **Device discovered by using the API**، حدد إحدى القيم التالية:

- **No**. لا يمكن اكتشاف الجهاز باستخدام AWS أو Azure أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة لكن لا يمكن اكتشافه باستخدام واجهة برمجة التطبيق (API) لسبب ما.
- **AWS**. يتم اكتشاف الجهاز باستخدام AWS API، أي أن الجهاز يوجد بالفعل في بيئة سحابة AWS.
- **Azure**. يتم اكتشاف الجهاز باستخدام Azure API، أي أن الجهاز يوجد بالفعل في بيئة سحابة Azure.
- **Google Cloud**. يتم اكتشاف الجهاز باستخدام Google API، آي أن الجهاز موجود بالفعل في بيئة Google cloud.
- دون قيمة. يتعذر تطبيق هذا المعيار.

5. إن لزم الأمر، قم بإعداد خصائص قاعدة أخرى في الأقسام الأخرى.

تم تكوين قاعدة النقل.

التثبيت عن بُعد للتطبيقات لأجهزة Azure الافتراضية

يجب أن تمتلك ترخيصًا ساري المفعول لتثبيت التطبيقات على أجهزة Microsoft Azure الظاهرية.

يدعم Kaspersky Security Center السيناريوهات التالية:

- اكتشاف جهاز عميل بواسطة Azure API؛ وإجراء التثبيت بواسطة API. يعني استخدام Azure API أنه يمكنك فقط تثبيت التطبيقات التالية:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- تم اكتشاف جهاز عميل عن طريق Azure API؛ يتم تنفيذ التثبيت عن طريق نقطة توزيع أو يدويًا باستخدام حزم التثبيت المستقلة في حالة عدم وجود نقاط توزيع. يمكنك تثبيت أي تطبيق يدعمه Kaspersky Security Center بهذه الطريقة.

لإنشاء مهمة للتثبيت عن بُعد لأحد التطبيقات على أجهزة Azure الظاهرية:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.
2. انقر على **Add**.

   سيبدأ معالج المهمة الجديدة.
3. اتبع إرشادات المعالج:
   a. حدد **Install application remotely** كنوع المهمة.
   b. على ال **Installation packages** الصفحة، حدد **Remote installation by Microsoft Azure API**.
   c. عند تحديد الحساب للوصول إلى الأجهزة، استخدم حساب Azure الحالي، أو انقر فوق **Add** وأدخل بيانات اعتماد حساب Azure الخاص بك:
      - **Azure Account Name**

        أدخل أي اسم لبيانات الاعتماد التي تحددها. سيتم عرض هذا الاسم في قائمة الحسابات لتشغيل المهمة.

- **Azure Application ID**

لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

- **Azure Application password**

لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

d. حدد الأجهزة ذات الصلة من مجموعة **الأجهزة المدارة\السحابة**.

بعد انتهاء المعالج، تظهر مهمة التثبيت عن بُعد للتطبيق في قائمة المهام.

إنشاء نسخة احتياطية من مهمة بيانات خادم الإدارة باستخدام سحابة DBMS

مهام النسخ الاحتياطي من مهام خادم الإدارة. يمكنك إنشاء مهمة نسخ احتياطي إذا كنت تريد استخدام DBMS موجود في بيئة سحابة (AWS أو Azure).

لإنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **Tasks** ← **Assets (Devices)**.

2. انقر على **Add**.

سيبدأ معالج المهمة الجديدة.

3. في الصفحة الأولى من المعالج في قائمة **Application**، حدد **Kaspersky Security Center 15**، وفي قائمة **Task type** حدد **Backup of Administration Server data**.

4. في الصفحة المقابلة في المعالج، حدد المعلومات التالية:

- إذا كنت تعمل مع قاعدة بيانات في AWS:

- **اسم مستودع S3**

اسم مستودع S3 الذي قمت بإنشائه للنسخ الاحتياطي.

- **معرف مفتاح الوصول**

لقد تلقيت معرف المفتاح (عبارة عن تسلسل من الحروف الأبجدية الرقمية) عند إنشائك حساب مستخدم IAM للتعامل مع مثيل تخزين مستودع S3.

يكون الحقل متاحًا في حالة تحديد قاعدة بيانات RDS على مستودع S3.

- **المفتاح السري**

المفتاح السري الذي تلقيته مع معرف مفتاح الوصول عند إنشائك حساب مستخدم IAM.

تظهر حروف المفتاح السري في صورة علامة النجمة. بعد أن تبدأ في إدخال المفتاح السري، سيظهر الزر **إظهار** . انقر مع الاستمرار فوق هذا الزر لتحديد الفترة الزمنية اللازمة لإظهار الحروف التي أدخلتها.

هذا الحقل متاح في حالة تحديد مفتاح وصول AWS IAM للتخويل بدلاً من دور IAM.

- إذا كنت تعمل مع قاعدة بيانات في Microsoft Azure:

  - **اسم حساب تخزين Azure**

    لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

  - **معرف اشتراك Azure**

    لقد قمت بإنشاء الاشتراك على مدخل Azure.

  - **كلمة مرور Azure**

    لقد تلقيت كلمة مرور معرف التطبيق عند قيامك بإنشاء معرف التطبيق.

    تظهر حروف كلمة المرور في صورة علامة النجمة. بعد أن تبدأ في إدخال كلمة المرور، سيصبح الزر **إظهار** متاحًا. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

  - **معرف تطبيق Azure**

    لقد قمت بإنشاء معرف التطبيق هذا على مدخل Azure.

    يمكنك فقط تقديم معرف تطبيق Azure واحد للاستقصاء وللأغراض الأخرى. إذا كنت ترغب في استقصاء قطاع Azure آخر، فيجب عليك أن تقوم أولًا بحذف اتصال Azure الموجود.

  - **اسم خادم Azure SQL Server**

    يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

  - **مجموعة مورد خادم Azure SQL Server**

    يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

  - **مفتاح وصول تخزين Azure**

    يكون متاحًا في خصائص حساب التخزين الخاص بك، في قسم مفاتيح الوصول. يمكنك استخدام أي من المفاتيح (المفتاح1 أو المفتاح2).

يتم إنشاء المهمة وعرضها في قائمة المهام. إذا كنت تفعل خيار **Open task details when creation is complete**، فيمكنك تعديل إعدادات المهمة الافتراضية على الفور بعد إنشاء المهمة. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

التشخيصات عن بُعد لأجهزة العميل

يمكنك استخدام التشخيص عن بعد للتنفيذ عن بعد للعمليات التالية على الأجهزة العميلة التي تعمل بنظامي التشغيل Windows وLinux:

- تمكين وتعطيل التتبع، وتغيير مستوى التتبع، وتنزيل ملف التتبع.
- تنزيل معلومات النظام وإعدادات التطبيق.
- تنزيل سجلات الأحداث
- إنشاء ملف تفريغ لتطبيق.
- بدء التشخيصات وتنزيل تقاريرها.
- تشغيل التطبيقات وإيقافها وإعادة تشغيلها

يمكنك استخدام سجلات الأحداث وتقارير التشخيصات التي تم تنزيلها من جهاز عميل لاستكشاف المشكلات وإصلاحها بنفسك. أيضًا عند تواصلك مع أخصائي دعم من Kaspersky، قد يطالبك أخصائي الدعم الفني بتنزيل ملفات التتبع وملفات التفريغ وسجلات الأحداث وتقارير التشخيصات من جهاز عميل لإجراء المزيد من التحليلات في Kaspersky.

فتح نافذة التشخيص عن بُعد

لإجراء التشخيص عن بعد على الأجهزة العميلة التي تعمل بنظامي التشغيل Windows وLinux، يتعين عليك أولاً فتح نافذة التشخيص عن بعد.

لفتح نافذة التشخيص عن بُعد:

1. لتحديد الجهاز الذي ترغب في فتح نافذة التشخيص عن بُعد له، اتخذ أحد الإجراءات التالية:
   - إذا كان الجهاز ينتمي إلى مجموعة إدارة، انتقل إلى **Assets (Devices)** ← **Managed devices**.
   - إذا كان الجهاز ينتمي إلى مجموعة الأجهزة غير المخصصة، انتقل إلى **Discovery & deployment** ← **Unassigned devices**.
2. انقر على اسم الجهاز المطلوب.
3. في نافذة خصائص الجهاز التي تفتح، حدد تبويب **Advanced**.
4. في النافذة التي تفتح، انقر على **Remote diagnostics**.

   يؤدي هذا إلى فتح نافذة **Remote diagnostics** لجهاز عميل. إذا لم يتم إنشاء اتصال بين خادم الإدارة والجهاز العميل، يتم عرض رسالة الخطأ.

بدلاً من ذلك، إذا كنت بحاجة إلى الحصول على جميع معلومات التشخيص عن جهاز عميل يستند إلى Linux في وقت واحد، فيمكنك تشغيل البرنامج النصي collect.sh على هذا الجهاز.

تمكين التتبع للتطبيقات وتعطيله

يمكنك تمكين التتبع للتطبيقات وتعطيله، بما في ذلك تتبع Xperf.

تمكين التتبع وتعطيله

لتمكين التتبع أو تعطيله على جهاز بعيد:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.
2. في نافذة التشخيصات عن بُعد، حدد علامة تبويب **Kaspersky applications**.

   في القسم **Application management**، يتم عرض قائمة بتطبيقات Kaspersky المثبتة على الجهاز.
3. في قائمة التطبيقات، حدد التطبيق الذي ترغب في تمكين التتبع أو تعطيله له.

   تفتح قائمة خيارات التشخيص عن بُعد.

4. إذا كنت ترغب في تفعيل التتبع:

a. في القسم **Tracing**، انقر على **Enable tracing**.

b. في النافذة **Modify tracing level** التي تفتح، نوصي بإبقاء القيم الافتراضية للإعدادات. عند الضرورة، سيقوم أخصائي الدعم الفني بإرشادك خلال عملية التكوين. تتوفر الإعدادات التالية:

- **Tracing level**

  يحدد مستوى التتبع مقدار التفاصيل التي يحتويها ملف التتبع.

- **Rotation-based tracing**

  يقوم التطبيق باستبدال معلومات التتبع لمنع الزيادة المفرطة في حجم ملف التتبع. حدد العدد الأقصى للملفات التي سيتم استخدامها لتخزين معلومات التتبع، وأقصى حجم لكل ملف. في حالة كتابة العدد الأقصى لملفات التتبع ذات الحد الأقصى للحجم، يتم حذف ملف التتبع القديم حتى يتسنى كتابة ملف التتبع الجديد.

  هذا الإعداد متوفر لـ Kaspersky Endpoint Security فقط.

c. انقر على **Save**.

يتم تفعيل التتبع للتطبيق المحدد. في بعض الحالات، يجب إعادة تشغيل تطبيق الأمان والمهمة التابعة له ليتم تمكين التتبع.

على الأجهزة العميلة التي تعمل بنظام التشغيل Linux، يتم تنظيم تتبع مكون محدث عميل الشبكة بواسطة إعدادات عميل الشبكة. لذلك، يتم تعطيل خياري **Enable tracing** و**Modify tracing level** لهذا المكون على الأجهزة العميلة التي تعمل بنظام التشغيل Linux.

5. إذا كنت ترغب في تعطيل التتبع للتطبيق المحدد، انقر على الزر **Disable tracing**.

   يتم تعطيل التتبع للتطبيق المحدد.

تمكين تتبع Xperf

في حالة Kaspersky Endpoint Security For، قد يطالبك أخصائي الدعم الفني بتمكين تتبع Xperf للحصول على معلومات حول أداء النظام.

لتمكين وتكوين تتبع Xperf أو تعطيله:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.

2. في نافذة التشخيصات عن بُعد، حدد علامة تبويب **Kaspersky applications**.

   في القسم **Application management**، يتم عرض قائمة بتطبيقات Kaspersky المثبتة على الجهاز.

3. في قائمة التطبيقات، حدد Kaspersky Endpoint Security for Windows.

   يتم عرض قائمة خيارات التشخيص عن بُعد لتطبيق Kaspersky Endpoint Security for Windows.

4. في القسم **Xperf tracing**، انقر على **Enable Xperf tracing**.

   إذا كان تتبع Xperf ممكنًا بالفعل/ يتم عرض زر **Disable Xperf tracing** بدلاً من ذلك. انقر فوق هذا الزر إذا كنت تريد تعطيل تتبع Xperf لتطبيق Kaspersky Endpoint Security for Windows.

5. في نافذة **Change Xperf tracing level** التي تفتح، واستنادًا إلى طلب أخصائي الدعم الفني، افعل أحد الإجراءات التالية:

a. حدد أحد مستويات التتبع التالية:

- **Light level**

يحتوي ملف التتبع من هذا النوع على الحد الأدنى لمقدار المعلومات حول النظام.

يتم تحديد هذا الخيار افتراضيًا.

- **Deep level**

يحتوي ملف التتبع من هذا النوع على معلومات مفصلة مقارنة بملفات التتبع من النوع البسيط، وقد يطالبك أخصائي الدعم الفني بتحديده عندما لا يكون ملف التتبع من النوع البسيط كافيًا لتقييم الأداء. يحتوي ملف التتبع العميق على معلومات تقنية حول النظام والتي تشتمل على معلومات حول الجهاز ونظام التشغيل وقائمة بالتطبيقات والعمليات التي تم بدؤها وإنهاؤها والأحداث المستخدمة في تقييم الأداء والأحداث من أداة تقييم نظام Windows.

b. حدد أحد أنواع تتبع Xperf التالية:

- **Basic type**

يتم استقبال معلومات التتبع أثناء تشغيل تطبيق Kaspersky Endpoint Security.

يتم تحديد هذا الخيار افتراضيًا.

- **On-restart type**

يتم استقبال معلومات التتبع عند بدء تشغيل نظام التشغيل على الجهاز المُدار. يكون نوع التتبع هذا فعالًا عند حدوث المشكلة التي تؤثر على أداء النظام بعد تشغيل الجهاز وقبل بدء تشغيل Kaspersky Endpoint Security.

قد تتم مطالبتك أيضًا بتمكين الخيار **Rotation file size, in MB** لمنع الزيادة المفرطة في حجم ملف التتبع. ثم حدد الحد الأقصى لحجم ملف التتبع. عند وصول الملف للحد الأقصى للحجم، يتم استبدال معلومات التتبع القديمة بالمعلومات الجديدة.

c. حدد حجم ملف التدوير.

d. انقر على **Save**.

تم تمكين تتبع Xperf وتكوينه.

6. إذا كنت تريد تعطيل تتبع Xperf لتطبيق Kaspersky Endpoint Security for Windows، فانقر فوق **Disable Xperf tracing** في القسم **Xperf tracing**.

تم تعطيل تتبع Xperf.

تنزيل ملفات التتبع لتطبيق

لتنزيل ملف التتبع لتطبيق:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.

2. في نافذة التشخيصات عن بُعد، حدد علامة تبويب **Kaspersky applications**.

في القسم **Application management**، يتم عرض قائمة بتطبيقات Kaspersky المثبتة على الجهاز.

3. في قائمة التطبيقات، حدد التطبيق الذي تريد تنزيل ملف التتبع له.

4. في قسم **Tracing**، انقر على زر **Trace files**.

يفتح هذا نافذة **Device tracing logs** حيث يتم عرض قائمة بملفات التتبع.

5. في قائمة ملفات التتبع، حدد الملف الذي تريد تنزيله.

6. قم بأحد الإجراءات التالية:

- قم بتنزيل الملف المحدد عن طريق النقر فوق **Download**. يمكنك تحديد ملف واحد أو عدة ملفات لتنزيلها.
- قم بتنزيل جزء من الملف المحدد:

a. انقر فوق **Download a portion**.

لا يمكنك تنزيل أجزاء من عدة ملفات في الوقت نفسه. وإذا حددت أكثر من ملف تتبع واحد، فسيتم تعطيل الزر **Download a portion**.

b. في النافذة التي تفتح، حدد الاسم وجزء الملف المراد تنزيله، وفقًا لاحتياجاتك.

بالنسبة للأجهزة التي تعمل بنظام التشغيل Linux، لا يتوفر تحرير اسم جزء الملف.

c. انقر فوق **Download**.

يتم تنزيل الملف المحدد أو جزئه إلى الموقع الذي تحدده.

حذف ملفات التتبع

يمكنك حذف ملفات التتبع التي لم تعد بحاجة إليها.

لحذف ملف تتبع:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.

2. في نافذة التشخيصات عن بعد التي تفتح، حدد علامة التبويب **Event logs**.

3. في قسم **Trace files**، انقر على **Windows Update logs** أو **Remote installation logs**، اعتمادًا على ملفات التتبع التي ترغب في حذفها.

يتوفر الرابط **Windows Update logs** للأجهزة العميلة التي تعمل بنظام التشغيل Windows.

يفتح هذا نافذة **Device tracing logs** حيث يتم عرض قائمة بملفات التتبع.

4. في قائمة ملفات التتبع، حدد ملفًا واحدًا أو عدة ملفات تريد حذفها.

5. انقر على الزر **Remove**.

يتم حذف ملفات التتبع المحددة.

تنزيل إعدادات التطبيق

لتنزيل إعدادات تطبيق من جهاز عميل:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.
2. في نافذة التشخيصات عن بُعد، حدد علامة تبويب **Kaspersky applications**.
3. في القسم **Application settings**، انقر على زر **Download** لتنزيل معلومات عن إعدادات التطبيقات المثبتة على الجهاز العميل.

يتم تنزيل أرشيف ZIP الذي يحتوي على المعلومات إلى الموقع المحدد.

تنزيل سجلات الأحداث

لتنزيل سجل الأحداث من جهاز بعيد:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.
2. في نافذة التشخيصات عن بُعد، في علامة التبويب **Event logs**، انقر فوق **All device logs**.
3. في النافذة **All device logs**، حدد سجلاً واحدًا أو أكثر ذي صلة:
4. قم بأحد الإجراءات التالية:
   - قم بتنزيل السجل المحدد عن طريق النقر على **Download entire file**.
   - قم بتنزيل جزء من السجل المحدد:

     a. انقر على **Download a portion**.

     لا يمكنك تنزيل أجزاء من عدة سجلات في الوقت نفسه. وإذا حددت أكثر من سجل أحداث واحد، فسيتم تعطيل الزر **Download a portion**.

     b. في النافذة التي تفتح، حدد الاسم وجزء السجل المراد تنزيله، وفقًا لاحتياجاتك.

     بالنسبة للأجهزة التي تعمل بنظام التشغيل Linux، لا يتوفر تحرير اسم جزء السجل.

     c. انقر فوق **Download**.

يتم تنزيل سجل الأحداث المحدد أو جزء منه إلى الموقع المحدد.

بدء التطبيق وإيقافه وإعادة تشغيله

يمكنك تشغيل التطبيقات وإيقافها وإعادة تشغيلها على جهاز عميل.

لتشغيل أحد التطبيقات وإيقافه وإعادة تشغيله:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.

2. في نافذة التشخيصات عن بُعد، حدد علامة تبويب **Kaspersky applications**.
في القسم **Application management**، يتم عرض قائمة بتطبيقات Kaspersky المثبتة على الجهاز.

3. في قائمة التطبيقات، حدد التطبيق الذي ترغب في بدئه أو إيقافه أو إعادة تشغيله.

4. حدد إجراءً بالنقر على أحد الأزرار التالية:

- **Stop application**
لا يتوفر هذا الزر إلا إذا كان التطبيق قيد التشغيل حاليًا.

- **Restart application**
لا يتوفر هذا الزر إلا إذا كان التطبيق قيد التشغيل حاليًا.

- **Start application**
لا يكون هذا الزر متوفرًا إلا إذا كان التطبيق ليس قيد التشغيل حاليًا.

بناءً على الإجراء الذي حددته، يتم تشغيل التطبيق المحدد أو إيقافه أو إعادة تشغيله على الجهاز العميل.

إذا أعدت تشغيل عميل الشبكة، يتم عرض سالة تفيد أنه سيتم فقد الاتصال الحالي للجهاز بخادم الإدارة.

تشغيل التشخيصات عن بُعد لعميل شبكة Kaspersky Security Center وتنزيل النتائج

لبدء تشخيصات عميل شبكة Kaspersky Security Center على جهاز بعيد وتنزيل النتائج:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.

2. في نافذة التشخيصات عن بُعد، حدد علامة تبويب **Kaspersky applications**.
في القسم **Application management**، يتم عرض قائمة بتطبيقات Kaspersky المثبتة على الجهاز.

3. في قائمة التطبيقات، حدد **عميل شبكة Kaspersky Security Center**.
تفتح قائمة خيارات التشخيص عن بُعد.

4. في القسم **Diagnostics report**، انقر فوق الزر **Run diagnostics**.
يؤدي هذا إلى بدء عملية التشخيص عن بُعد وينشئ تقريرًا عن التشخيص. عندما تكتمل عملية التشخيص، يتوفر زر **Download diagnostics report**.

5. انقر فوق الزر **Download diagnostics report** لتنزيل التقرير.

يتم تنزيل التقرير إلى الموقع المحدد.

تشغيل تطبيق على جهاز عميل

قد تضطر إلى تشغيل تطبيق على الجهاز العميل إذا طلب منك أخصائي الدعم الفني في Kaspersky هذا. لا يتعين عليك تثبيت التطبيق على ذلك الجهاز.

تشغيل تطبيق على الجهاز العميل:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.
2. في نافذة التشخيصات عن بُعد، حدد علامة التبويب **Running a remote application**.
3. في القسم **Application files**، انقر فوق الزر **Browse** لتحديد أرشيف مضغوط يحتوي على التطبيق الذي تريد تشغيله على الجهاز العميل.

يجب أن يتضمن أرشيف ZIP مجلد الأداة المساعدة. ويحتوي هذا المجلد على الملف القابل للتنفيذ الذي سيتم تشغيله على جهاز بعيد.

يمكنك تحديد اسم الملف القابل للتنفيذ ووسائط سطر الأوامر، إذا لزم الأمر. ولفعل ذلك، املأ **الملف القابل للتنفيذ في أرشيف ليتم تشغيله على جهاز بعيد** وحقول **Command-line arguments**.

4. انقر فوق الزر **Upload and run** لتشغيل التطبيق المحدد على جهاز عميل.
5. اتبع تعليمات متخصص الدعم في Kaspersky.

إنشاء ملف تفريغ لتطبيق.

يتيح لك ملف تفريغ التطبيق عرض معلمات التطبيق الذي يتم تشغيله على جهاز عميل في وقت معين. ويحتوي هذا الملف أيضًا على معلومات عن الوحدات النمطية التي تم تحميلها لأحد التطبيقات.

لا يتم دعم الحصول على ملفات التفريغ من الأجهزة المستندة إلى Linux.

للحصول على ملفات التفريغ من خلال التشخيص عن بعد، يتم استخدام الأداة المساعدة kldumper. وتم تصميم هذه الأداة للحصول على ملفات تفريغ عمليات تطبيقات Kaspersky بناءً على طلب متخصصي الدعم الفني. تتوفر معلومات تفصيلية عن متطلبات استخدام الأداة المساعدة kldumper في قاعدة معارف Kaspersky Security Center.

لإنشاء ملف تفريغ لتطبيق:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.
2. في نافذة التشخيصات عن بُعد، حدد علامة التبويب **Running a remote application**.
3. في القسم **Generating the process dump file**، حدد الملف القابل للتنفيذ للتطبيق الذي تريد إنشاء ملف تفريغ له.
4. انقر فوق الزر **Download dump file**.

   يتم تنزيل أرشيف يحتوي على ملف التفريغ للتطبيق المحدد.

   إذا كان التطبيق المحدد لا يعمل على الجهاز العميل، فسيكون مجلد "النتيجة" الموجود في الأرشيف الذي تم تنزيله فارغًا.

   إذا كان التطبيق المحدد قيد التشغيل، ولكن فشل التنزيل بسبب خطأ أو كان مجلد "النتيجة" الموجود في الأرشيف الذي تم تنزيله فارغًا، فارجع إلى قاعدة معارف Kaspersky Security Center.

تشغيل التشخيصات عن بُعد على جهاز عميل يعمل بنظام التشغيل Linux

يتيح لك Kaspersky Security Center تنزيل معلومات التشخيص الأساسية من جهاز عميل. بدلاً من ذلك، يمكنك الحصول على معلومات التشخيص حول جهاز يعمل بنظام التشغيل Linux باستخدام البرنامج النصي collection.sh بواسطة Kaspersky. ويتم تشغيل هذا البرنامج النصي على الجهاز العميل الذي يعمل بنظام Linux الذي يحتاج إلى التشخيص، ثم ينشئ ملفًا يحتوي على معلومات التشخيص، ومعلومات النظام عن هذا الجهاز، وملفات تتبع التطبيقات، وسجلات الجهاز، وملف تفريغ للطوارئ- التطبيقات المنتهية.

نوصي باستخدام البرنامج النصي collect.sh للحصول على جميع المعلومات التشخيصية حول الجهاز العميل الذي يعمل بنظام Linux مرة واحدة. إذا قمت بتنزيل معلومات التشخيص عن بُعد من خلال Kaspersky Security Center، فستحتاج إلى استعراض جميع أقسام واجهة التشخيص عن بُعد. ومن المحتمل كذلك ألا يتم الحصول على معلومات التشخيص الخاصة بجهاز يعمل بنظام Linux بشكل كامل.

إذا كنت بحاجة إلى إرسال الملف الذي تم إنشاؤه مع معلومات التشخيص إلى الدعم الفني في Kaspersky، فاحذف جميع المعلومات السرية قبل إرسال الملف.

لتنزيل معلومات التشخيص من جهاز عميل يعمل بنظام Linux باستخدام البرنامج النصي collect.sh:

1. قم بتنزيل البرنامج النصي collect.sh الموجود داخل أرشيف collect.tar.gz.
2. انسخ الأرشيف الذي تم تنزيله إلى جهاز العميل الذي يعمل بنظام Linux الذي يحتاج إلى التشخيص.
3. قم بتشغيل الأمر التالي لفك ضغط أرشيف collect.tar.gz:

```
tar -xzf collect.tar.gz #
```

4. قم بتشغيل الأمر التالي لتحديد حقوق تنفيذ البرنامج النصي:

```
chmod +x collect.sh #
```

5. قم بتشغيل البرنامج النصي collect.sh باستخدام حساب يمتلك حقوق المسؤول:

```
collect.sh/. #
```

يتم إنشاء ملف يحتوي على معلومات التشخيص وحفظه في المجلد /tmp/$HOST_NAME-collect.tar.gz.

تنزيل وحذف الملفات من العزل وBackup

يقدم هذا القسم معلومات حول كيفية التنزيل وكيفية حذف الملفات من العزل وBackup في Kaspersky Security Center Web Console.

تنزيل الملفات من العزل والنسخ الاحتياطي

لا يمكنك تنزيل الملفات من العزل والنسخ الاحتياطي إلا إذا تم استيفاء أحد الشرطين: إما تمكين الخيار **عدم قطع الاتصال عن خادم الإدارة** في إعدادات الجهاز، أو أن بوابة الاتصال قيد الاستخدام. بخلاف ذلك، فإن التنزيل غير ممكن.

لحفظ نسخة من الملف من العزل أو Backup إلى محرك الأقراص الثابتة:

1. قم بأحد الإجراءات التالية:

- إذا كنت تريد حفظ نسخة من الملف من العزل، في القائمة الرئيسية، انتقل إلى **Operations** ← **Repositories** ← **Quarantine**.
- إذا كنت تريد حفظ نسخة من الملف من النسخ الاحتياطي، في القائمة الرئيسية، انتقل إلى **Operations** ← **Repositories** ← **Backup**.

2. في النافذة التي تفتح، حدد الملف الذي تريد تنزيله وانقر فوق **Download**.

سيبدأ التنزيل. يتم حفظ نسخة من الملف الذي تم وضعه في العزل على جهاز العميل في المجلد المحدد.

تغيير لغة واجهة Kaspersky Security Center Web Console

يمكنك تحديد لغة واجهة Kaspersky Security Center Web Console.

لتغيير لغة الواجهة:

1. في القائمة الرئيسية، انتقل إلى **Settings** ← **Language**.
2. حدد إحدى لغات الترجمة المدعومة.

الدليل المرجعي لـ API

تم تصميم هذا الدليل المرجعي من Kaspersky Security Center OpenAPI للمساعدة في المهام التالية:

- الأتمتة والتخصيص. أنت تستطيع أتمتة المهام التي قد لا ترغب في معالجتها يدويًا باستخدام وحدة تحكم الإدارة. يمكنك كذلك تنفيذ سيناريوهات مخصصة غير مدعومة حتى الآن في وحدة تحكم الإدارة. على سبيل المثال، يمكنك بصفتك مشرفًا استخدام Kaspersky Security Center OpenAPI لإنشاء وتشغيل البرامج النصية التي من شأنها تسهيل تطوير بنية مجموعات الإدارة والحفاظ على تحديث الهيكل.
- التنمية المخصصة. يمكنك على سبيل المثال تطوير وحدة تحكم إدارية بديلة قائمة على MMC لعملائك، والتي تسمح بمجموعة محدودة من الإجراءات.

في الدليل المرجعي OpenAPI، يمكنك استخدام حقل البحث في الجزء الأيسر من الشاشة لتحديد المعلومات التي تحتاجها.

الدليل المرجعي لـ OPENAPI

نماذج من البرامج النصية

يحتوي الدليل المرجعي OpenAPI على نماذج من برامج Python النصية المدرجة في الجدول أدناه. توضح العينات كيف يمكنك استدعاء أساليب OpenAPI وإنجاز المهام المختلفة تلقائيًا لحماية شبكتك، على سبيل المثال، إنشاء تسلسل هرمي "أساسي/ثانوي"، أو تشغيل المهام في Kaspersky Security Center، أو تعيين نقاط التوزيع . يمكنك تشغيل النماذج كما هي أو إنشاء البرامج النصية الخاصة بك بناءً على النماذج.

لاستدعاء أساليب OpenAPI وتشغيل البرامج النصية:

1. قم بتنزيل أرشيف KlAkOAPI.tar.gz . يتضمن هذا الأرشيف حزمة ونماذج KlAkOAPI (يمكنك نسخها من الأرشيف أو الدليل المرجعي OpenAPI). يوجد أرشيف KlAkOAPI.tar.gz أيضًا في مجلد تثبيت Kaspersky Security Center.
2. قم بتثبيت حزمة KlAkOAPI من أرشيف KlAkOAPI.tar.gz على جهاز مثبت عليه خادم الإدارة.

يمكنك استدعاء أساليب OpenAPI وتشغيل النماذج والبرامج النصية الخاصة بك فقط على الأجهزة حيث تم تثبيت خادم الإدارة وحزمة KlAkOAPI.

المطابقة بين سيناريوهات المستخدمين وعينات من أساليب Kaspersky Security Center OpenAPI

عينة	الغرض من العينة	سيناريو
سجل KlAkParams	يمكنك استخلاص البيانات ومعالجتها وجمعها باستخدام هيكل بيانات `KlAkParams`. يوضح النموذج كيفية العمل مع هيكل البيانات هذا. قد يكون إخراج النموذج موجودًا بطرق مختلفة. يمكنك الحصول على البيانات لإرسال طريقة HTTP أو استخدامها في التعليمات البرمجية الخاصة بك.	المراقبة وإعداد التقارير
إنشاء وحذف تسلسل هرمي"رئيسي/ثانوي"	يمكنك إضافة خادم إدارة كخادم إدارة ثانوي، والذي يقوم بإنشاء تسلسل هرمي "رئيسي/ثانوي". بالتناوب، يمكنك فصل خادم الإدارة الثانوي من التسلسل الهرمي.	• إنشاء تسلسل هرمي من خوادم الإدارة: إضافة خادم إدارة تابع • حذف تسلسل هرمي لخوادم الإدارة
إنشاء التسلسل الهرمي للمجموعة مع هيكل يستند إلى وحدة Active Directory	يمكنك الاستقصاء عن وحدة Active Directory وتشكيل تسلسل هرمي لمجموعات الأجهزة المكتشفة.	إنشاء مجموعات إدارة
إنشاء التسلسل الهرمي للمجموعة مع هيكل يستند إلى وحدة Active Directory المكخزنة مؤقتًا	يمكنك تكوين تسلسل هرمي لمجموعات الأجهزة المُدارة بناءً على وحدة Active Directory التي تم استقصاؤها مسبقًا. إذا ظهرت أجهزة جديدة في Active Directory بعد الاستقصاء الأخير، فلن تتم إضافتها إلى المجموعة لأنها ليست في نتائج الاستقصاء المحفوظة.	إنشاء مجموعات إدارة
تنزيل ملفات قائمة الشبكة عبر بوابة الاتصال للجهاز المحدد	يمكنك الاتصال بعميل الشبكة على الجهاز المطلوب عن طريق استخدام بوابة اتصال، وبعدها قم بتنزيل ملف بقائمة الشبكات على جهازك.	تعديل نقاط التوزيع وبوابات الاتصال
قم بتثبيت مفتاح ترخيص مخزن في مستودع خادم الإدارة الرئيسي على خوادم الإدارة الثانوية	يمكنك الاتصال بخادم الإدارة الرئيسي، وتنزيل مفتاح الترخيص المطلوب منه، ونقل هذا المفتاح إلى جميع خوادم الإدارة الثانوية المضمنة في التسلسل الهرمي.	ترخيص التطبيقات المُدارة

عينة	الغرض من العينة	سيناريو
إنشاء تقرير بحقوق المستخدم النشطة	تستطيع إنشاء تقارير مختلفة . يمكنك على سبيل المثال إنشاء تقرير عن حقوق المستخدم النشطة باستخدام هذا النموذج. يصف هذا التقرير الحقوق التي يمتلكها المستخدم اعتمادًا على مجموعته ودوره. يمكنك تنزيل التقرير بصيغة HTML أو PDF أو Excel.	إنشاء تقرير وعرضه
ابدأ مهمة لجهاز	يمكنك الاتصال بعميل الشبكة على الجهاز المطلوب عن طريق استخدام بوابة اتصال ثم تشغيل المهمة المطلوبة.	بدء مهمة يدويًا
إنشاء شبكات IP فرعية استنادًا إلى موقع وخدمات Active Directory	يمكنك إنشاء شبكة IP فرعية استنادًا إلى وحدة Active Directory التي تستخدمها. يقوم النموذج بتشغيل استقصاء نطاق IP المحدد ويحذف الشبكات الفرعية المكتشفة لتجنب تعارضها مع شبكة فرعية جديدة. لذلك، لا تقم بتشغيل هذا النموذج في الشبكة حيث من المهم الاحتفاظ بالشبكات الفرعية. بعد الاستقصاء، يشير النموذج إلى Active Directory ويفحص كل جهاز فيه وينشئ شبكة IP الفرعية. لفعل ذلك، يستخدم النموذج أقنعة وعناوين IP لجميع الأجهزة.	تكوين حماية الشبكة
تسجيل نقاط التوزيع للأجهزة في مجموعة	يمكنك تعيين الأجهزة المُدارة كنقاط توزيع (كانت معروفة سابقًا باسم وكلاء التحديث).	تحديث قواعد بيانات Kaspersky وتطبيقاته
عد كل المجموعات	يمكنك تنفيذ العديد من الإجراءات على مجموعات الإدارة. يوضح النموذج كيفية فعل ذلك: • احصل على معرّف لمجموعة الجذر "الأجهزة المُدارة" • تنقل عبر التسلسل الهرمي للمجموعة • استرجع التسلسل الهرمي الكامل والموسع للمجموعات، جنبًا إلى جنب مع أسمائها وتداخلها	تكوين خادم الإدارة
عد المهام والاستعلام عن إحصائيات المهام وتشغيل مهمة	يمكنك معرفة المعلومات التالية: • تاريخ تقدم المهمة • حالة المهمة الحالية • عدد المهام في حالات مختلفة يمكنك أيضًا تشغيل مهمة. بشكل افتراضي، يقوم النموذج بتشغيل مهمة بعد إخراج الإحصائيات.	مراقبة تنفيذ المهمة
إنشاء وتشغيل مهمة	يمكنك إنشاء مهمة. حدد معلمات المهمة التالية في النموذج: • النوع • طريقة التشغيل • الاسم • مجموعة الأجهزة التي سيتم استخدام المهمة لها بشكل افتراضي، يقوم النموذج بإنشاء مهمة من النوع "إظهار الرسالة". يمكنك تشغيل هذه المهمة لجميع الأجهزة المدارة لخادم الإدارة. يمكنك إذا لزم الأمر تحديد معلمات المهمة الخاصة بك.	إنشاء مهمة
عد مفاتيح الترخيص	يمكنك الحصول على قائمة بجميع مفاتيح الترخيص النشطة لتطبيقات Kaspersky المثبتة على الأجهزة المُدارة لخادم الإدارة. تحتوي القائمة على بيانات مفصلة حول كل مفتاح ترخيص، مثل الاسم أو النوع أو تاريخ انتهاء الصلاحية.	عرض معلومات حول مفاتيح التراخيص قيد الاستخدام
إنشاء والعثور على مستخدم داخلي	يمكنك إنشاء حساب لمزيد من العمل.	تحديد الحساب لتشغيل خادم الإدارة
إنشاء فئة مخصصة	يمكنك إنشاء فئة التطبيق بالمعلمات المطلوبة.	إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا
عد المستخدمين باستخدام SrvView	يمكنك استخدام الفئة SrvView لطلب معلومات مفصلة من خادم الإدارة. يمكنك على سبيل المثال الحصول على قائمة المستخدمين عن طريق استخدام هذا النموذج.	إدارة حسابات المستخدمين

التطبيقات التي تتفاعل مع Kaspersky Security Center عبر OpenAPI

تتفاعل بعض التطبيقات مع Kaspersky Security Center عبر OpenAPI. تشمل هذه التطبيقات على سبيل المثال، Kaspersky Anti Targeted Attack Platform أو Kaspersky Security for Virtualization. يمكن أن يكون هذا أيضًا تطبيق عميل مخصص تم تطويره من خلالك بناءً على OpenAPI.

التطبيقات التي تتفاعل مع Kaspersky Security Center عبر OpenAPI تتصل بخادم الإدارة. في حالة تكوين ملف قائمة السماح لعناوين IP للاتصال بخادم الإدارة، فأضف عناوين IP للأجهزة حيث يتم تثبيت التطبيقات التي تستخدم Kaspersky Security Center OpenAPI. لمعرفة ما إذا كان التطبيق الذي تستخدمه يعمل بواسطة OpenAPI، راجع تعليمات هذا التطبيق.

أفضل ممارسات موفري الخدمات

يوفر هذا القسم معلومات حول كيفية تكوين Kaspersky Security Center واستخدامه.

يحتوي هذا القسم على توصيات حول كيفية نشر التطبيق وتكوينه واستخدامه، بالإضافة إلى شرح طرق حل المشكلات النمطية عند تشغيل التطبيق.

التخطيط لنشر Kaspersky Security Center

عند التخطيط لنشر مكونات Kaspersky Security Center على شبكة المؤسسة، يجب عليك أخذ حجم المشروع ونطاقه في الاعتبار؛ وبخاصةٍ العوامل التالية:

- إجمالي عدد الأجهزة
- عدد عملاء MSP

يمكن لخادم إدارة واحد دعم 100 000 جهاز بحد أقصى. إذا كان إجمالي عدد الأجهزة في شبكة مؤسسة ما يتخطى 100 000 جهاز، فيجب نشر خوادم إدارة متعددة على جانب مزود الخدمة وجمعها في تسلسل هرمي للحصول على إدارة مركزية ملائمة.

يمكن إنشاء عدد يصل إلى 500 خادم ظاهري على خادم إدارة واحد، ولذلك يلزم توفر خادم إدارة واحد لكل 500 عميل من عملاء MSP.

في مرحلة التخطيط للنشر، يجب وضع تعيين شهادة X.509 الخاصة لخادم الإدارة في الاعتبار. قد يكون تعيين شهادة X.509 لخادم الإدارة مفيدًا في الحالات التالية (قائمة جزئية):

- فحص حركة مرور طبقة مآخذ التوصيل الآمنة (SSL) بواسطة وكيل إنهاء SSL
- تحديد القيم المطلوبة في حقول الشهادة
- تقديم قوة التشفير المطلوبة لشهادة ما

توفير الوصول عبر الإنترنت إلى خادم الإدارة

للسماح للأجهزة الموجودة في شبكة العميل بالوصول إلى خادم الإدارة عبر الإنترنت، يتعين عليك توفير منافذ خادم الإدارة التالية:

- TCP 13000—منفذ TLS لخادم الإدارة لاتصال عملاء الشبكة الذين تم نشرهم في شبكة العميل
- منفذ TCP 8061—HTTPS لنشر الحزم المستقلة باستخدام أدوات وحدة تحكم الإدارة
- منفذ TCP 8060—HTTP لنشر الحزم المستقلة باستخدام أدوات وحدة تحكم الإدارة
- منفذ TCP 13292—TLS المطلوب فقط عند وجود أجهزة محمولة تلزم إدارتها

إذا كنت بحاجة إلى تزويد العملاء بالخيارات الأساسية لإدارة الشبكة من خلال Kaspersky Security Center Web Console، يجب عليك أيضًا فتح منفذ Kaspersky Security Center Web Console رقم TCP 8080 (منفذ HTTPS).

التكوين القياسي لـ Kaspersky Security Center

يمكن نشر خادم إدارة واحد أو خوادم إدارة متعددة على خوادم MSPs. يمكن تحديد عدد خوادم الإدارة إما بناءً على المكون المادي المتوفر، أو على العدد الإجمالي لعملاء MSP المزوَّدين بالخدمات أو العدد الإجمالي للأجهزة المُدارة.

يمكن لخادم إدارة واحد دعم ما يصل إلى 100 000 جهاز. يجب عليك وضع احتمالية زيادة عدد الأجهزة المدارة في المستقبل القريب في الاعتبار: قد يكون من المفيد توصيل عدد أقل قليلاً من الأجهزة بخادم إدارة واحد.

يمكن إنشاء عدد يصل إلى 500 خادم ظاهري على خادم إدارة واحد، ولذلك يلزم توفر خادم إدارة واحد لكل 500 عميل من عملاء MSP.

في حالة استخدام خوادم متعددة، فمن المستحسن الجمع بينها في ترتيب هرمي. يتيح لك استخدام الترتيب الهرمي لخوادم الإدارة تجنب السياسات والمهام المسمّاة والتعامل مع مجموعة الأجهزة المُدارة بالكامل كما لو أنها تتم إداراتها بواسطة خادم إدارة واحد: مثل البحث عن أجهزة، وبناء تحديدات الأجهزة، وإنشاء التقارير.

في كل خادم افتراضي يطابق عميل MSP، يجب عليك تعيين نقطة توزيع أو عدة نقاط توزيع. في حالة ارتباط عملاء MSP وخادم الإدارة عبر الإنترنت، فقد يكون من المفيد إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع لنقاط التوزيع، حتى يكون بإمكانهم تنزيل التحديثات مباشرةً من خوادم Kaspersky، وليس من خادم الإدارة.

إذا كانت بعض الأجهزة الموجودة في شبكة عميل MSP لا تمتلك وصولاً مباشرًا إلى الإنترنت، فيتعين عليك تحويل نقاط التوزيع إلى وضع بوابة الاتصال. في هذه الحالة، سيكون عملاء الشبكة الموجودون في شبكة عميل MSP متصلين بخادم الإدارة – للحصول على مزيد من المزامنة – ولكن عبر البوابة وليس بشكل مباشر.

ولأن خادم الإدارة على الأرجح لن يتمكن من استقصاء شبكة عميل MSP، فقد يكون من المفيد تحويل هذه الوظيفة إلى نقطة التوزيع.

سيتعذر على خادم الإدارة إرسال إخطارات إلى المنفذ 15000 UDP الموجود على الأجهزة المُدارة الموجودة خارج نطاق NAT في شبكة عميل MSP. لحل هذه المشكلة، قد يكون من المفيد تمكين وضع الاتصال المستمر بخادم الإدارة من خصائص الأجهزة التي تعمل كنقاط توزيع وتعمل في وضع بوابة الاتصال (خانة اختيار **عدم قطع الاتصال عن خادم الإدارة**). يكون وضع الاتصال المستمر متاحًا إذا كان عدد نقاط التوزيع الإجمالي لا يتعدى 300 نقطة.

حول نقاط التوزيع

يمكن استخدام عميل الشبكة كنقطة توزيع. في هذا الوضع، يمكن أن يؤدي عميل الشبكة الوظائف التالية:

- نقل الملفات إلى أجهزة العميل، بما في ذلك:
  - تحديثات قواعد بيانات Kaspersky والوحدات النمطية للبرنامج

    يمكن استرداد التحديثات إما من خادم الإدارة أو من خوادم Kaspersky. في الحالة الأخيرة، يجب إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع للجهاز الذي يعمل كنقطة توزيع.
  - تحديثات برامج الجهات الخارجية
  - حزم التثبيت
  - تحديثات Windows عندما تستخدم خادم الإدارة كخادم WSUS
- تثبيت البرنامج (بما في ذلك عملية النشر الأولي لعملاء الشبكة) على أجهزة أخرى.
- قم باستقصاء الشبكة لاكتشاف الأجهزة الجديدة وتحديث المعلومات حول الأجهزة الموجودة بالفعل. يمكن لنقطة التوزيع تطبيق نفس وسائل اكتشاف الأجهزة كخادم الإدارة.

تحقق عملية نشر نقاط التوزيع على شبكة المؤسسة الأهداف التالية:

- تخفيف الحمل على خادم الإدارة إذا كان يعمل كمصدر تحديث.
- تحسين حركة الإنترنت لأنه، في هذه الحالة، لا يمتلك كل جهاز في شبكة عميل MSP الوصول إلى خوادم Kaspersky أو خادم الإدارة للتحديثات.
- توفير الوصول إلى خادم الإدارة للأجهزة التي تقع وراء نطاق NAT (فيما يتعلق بخادم الإدارة) لشبكة عميل MSP، مما يسمح لخادم الإدارة بتنفيذ الإجراءات التالية:
  - أرسل إشعارات إلى الأجهزة عبر UDP على شبكة IPv4 أو IPv6
  - استطلع رأي شبكة IPv4 أو IPv6
  - إجراء نشر أولي
  - العمل ك خادم إرسال

يتم تعيين نقطة توزيع لمجموعة إدارة. في هذه الحالة، يشمل نطاق نقطة التوزيع كل الأجهزة الموجودة في مجموعة الإدارة وكل المجموعات الفرعية التابعة لها. ولكن لا يتوجب تضمين الجهاز الذي يعمل كنقطة توزيع في مجموعة الإدارة التي تم تعيينه لها.

يمكنك تعيين وظيفة نقطة توزيع كبوابة اتصال. وفي هذه الحالة، ستكون الأجهزة الموجودة في نطاق نقطة التوزيع هذه متصلة بخادم الإدارة عبر البوابة وليس مباشرةً. يمكنك استخدام هذا الوضع في السيناريوهات التي لا تسمح بتأسيس اتصال مباشر بين الأجهزة باستخدام عميل شبكة وخادم إدارة.

يجب أن تكون الأجهزة التي تعمل كنقاط توزيع محمية، بما في ذلك الحماية الفعلية، وضد أي وصول غير مصرح به.

التسلسل الهرمي لخوادم الإدارة

قد تقوم مؤسسة MSP ما بتشغيل العديد من خوادم الإدارة. ويمكن أن يكون من الشاق إدارة العديد من خوادم الإدارة المنفصلة، وبذلك يمكن استخدام ترتيب هرمي. يمكن للتكوين الرئيسي/التابع لاثنين من خوادم الإدارة توفير الخيارات التالية:

- يرث خادم الإدارة الثانوي السياسات والمهام من خادم الإدارة الرئيسي، وهذا يمنع تكرار الإعدادات.
- يمكن أن يشمل تحديد أجهزة على خادم الإدارة الرئيسي أجهزة من خوادم الإدارة الثانوية.
- يمكن أن تحتوي التقارير الموجودة على خادم الإدارة الرئيسي على بيانات (تشمل معلومات تفصيلية) من خوادم الإدارة الثانوية.

يتلقى خادم الإدارة الأساسي البيانات فقط من خوادم الإدارة الثانوية غير الافتراضية ضمن نطاق الخيارات المذكورة أعلاه. لا ينطبق هذا القيد على خوادم الإدارة الافتراضية، التي تشارك قاعدة البيانات مع خادم الإدارة الأساسي الخاص بها.

خوادم الإدارة الافتراضية

بالاستناد إلى خادم الإدارة الفعلي، يمكن إنشاء خوادم إدارة افتراضية متعددة، والتي ستكون مشابهة لخوادم الإدارة الثانوية. بالمقارنة بطراز الوصول الاختياري، الذي يستند إلى قوائم التحكم في الوصول (ACL)، يُعتبر طراز خادم الإدارة الافتراضي أكثر وظيفية ويوفر درجة أكبر من العزل. بالإضافة إلى الهيكل المحدد لمجموعات الإدارة للأجهزة المخصصة ذات السياسات والمهام، يتميز كل خادم إدارة افتراضي بمجموعته الخاصة من الأجهزة غير المخصصة، ومجموعات التقارير الخاصة، والأجهزة والأحداث المحددة، وحزم التثبيت، وقواعد النقل، وما إلى ذلك. لأقصى عزل متبادل بين عملاء MSP، ننصحك باختيار خادم إدارة افتراضي حتى يتم استخدام الخاصية. بالإضافة إلى ذلك، يسمح لك خادم الإدارة الافتراضي الخاص بكل عميل MSP بتزويد العملاء بالخيارات الرئيسية لإدارة الشبكة من خلال Kaspersky Security Center Web Console.

خوادم الإدارة الافتراضية تشبه إلى حدٍ كبير خوادم الإدارة الثانوية، ولكن مع الفروق التالية:

- يفتقد خادم الإدارة الافتراضي لأغلب الإعدادات العمومية ومنافذ TCP الخاصة به.
- لا يحتوي خادم الإدارة الافتراضي على خوادم إدارة ثانوية.
- لا يحتوي خادم الإدارة الافتراضي على خوادم إدارة افتراضية أخرى.
- يمكن لخادم الإدارة الفعلي عرض الأجهزة والمجموعات والأحداث والكائنات الموجودة على الأجهزة المدارة (العناصر الموجودة في العزل وسجل التطبيقات وما إلى ذلك) الخاصة بكل خوادم الإدارة الافتراضية الخاصة به.
- لا يمكن لخادم الإدارة الافتراضي فحص الشبكة إلا مع اتصال نقاط التوزيع.

إدارة الأجهزة المحمولة باستخدام Kaspersky Endpoint Security for Android

تتم إدارة الأجهزة المحمولة المثبّت عليها Kaspersky Endpoint Security for Android™ (يُشار إليها فيما بعد باسم أجهزة KES) بواسطة خادم الإدارة. يدعم Kaspersky Security Center الميزات التالية لإدارة أجهزة KES:

- التعامل مع الأجهزة المحمولة كأجهزة عميلة:
  - عضوية في مجموعات الإدارة
  - المراقبة، مثل عرض الحالات والأحداث والتقارير
  - تعديل الإعدادات المحلية وتعيين السياسات لـ Kaspersky Endpoint Security for Android
- إرسال الأوامر في الوضع المركزي
- تثبيت حزم تطبيقات الأجهزة المحمولة عن بُعد.

خادم الإدارة يدير أجهزة KES من خلال TLS، منفذ TCP 13292.

النشر والإعداد الأولي

يُعتبر Kaspersky Security Center تطبيقًا موزَّعًا. يشمل Kaspersky Security Center التطبيقات التالية:

- خادم الإدارة—وهو المكوّن الرئيسي، تم تصميمه لإدارة أجهزة إحدى المؤسسات وتخزين البيانات في نظام إدارة قواعد البيانات.
- وحدة تحكم الإدارة—الأداة الأساسية للمسؤول. يتم شحن وحدة تحكم الإدارة مع خادم الإدارة، ولكن يمكن تثبيتها بشكل فردي على جهاز واحد أو أجهزة متعددة يشغّلها المسؤول.
- Kaspersky Security Center Web Console—واجهة ويب لخادم الإدارة مصممة لعمليات التشغيل الرئيسية. يمكنك تثبيت هذا المكون على أي جهاز يفي بمتطلبات الأجهزة والبرامج.
- عميل الشبكة – مصمم لإدارة تطبيق الأمان المثبت على أحد الأجهزة، بالإضافة إلى الحصول على معلومات حول هذا الجهاز. يتم تثبيت عملاء الشبكة على أجهزة مؤسسة ما.

يتم القيام بنشر Kaspersky Security Center على شبكة المؤسسة كما يلي:

- تثبيت خادم الإدارة
- تثبيت Kaspersky Security Center Web Console
- تثبيت وحدة تحكم الإدارة على جهاز المسؤول
- تثبيت عميل الشبكة وتطبيق الأمان على أجهزة المؤسسة

توصيات حول تثبيت خادم الإدارة

يحتوي هذا القسم على توصيات حول كيفية تثبيت خادم الإدارة. يقدّم هذا القسم أيضًا سيناريوهات استخدام مجلد مشترك موجود على جهاز خادم الإدارة لنشر عميل الشبكة على أجهزة عميلة.

إنشاء حسابات لخدمات خادم الإدارة على مجموعة تجاوز الفشل.

بشكل افتراضي، يقوم المثبّت تلقائيًا بإنشاء حسابات غير مميزة لخدمات خادم الإدارة. هذا السلوك هو الأكثر ملاءمةً لتثبيت خادم الإدارة على جهاز عادي.

على الرغم من ذلك، يتطلب تثبيت خادم الإدارة على مجموعة تجاوز الفشل سيناريو مختلفًا:

1. قم بإنشاء حسابات مجال غير مميزة لخدمات خادم الإدارة وأعطها العضوية في مجموعة أمان المجال العمومي المسمّى KLAdmins
2. في مثبّت خادم الإدارة، حدد حسابات المجال التي تم إنشاؤها للخدمات.

تحديد نظام إدارة قواعد البيانات

عند اختيار نظام إدارة قواعد البيانات (DBMS) الذي سيستخدمه خادم الإدارة، يجب عليك الأخذ في الاعتبار عدد الأجهزة التي يغطيها خادم الإدارة.

يسرد الجدول التالي خيارات نظام إدارة قاعدة البيانات الصالحة، بالإضافة إلى توصيات وقيود استخدامها.

التوصيات والقيود حول نظام إدارة قواعد البيانات

نظام إدارة قاعدة البيانات	التوصيات والقيود
إصدار SQL Server Express Edition 2016 أو الإصدار الأحدث.	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 10000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يمكنك تحديد الحد الأقصى لعدد الأحداث في مخزن الأحداث لمنع تجاوز قاعدة البيانات. يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات. يُحظر تمامًا الاستخدام المتزامن لنظام إدارة قواعد البيانات الخاص بـ SQL Server Express Edition DBMS بواسطة خادم الإدارة وتطبيق آخر. لا يتم دعم قاعدة بيانات Microsoft SQL Express لمهمة **إجراء مزامنة Windows Update**.
إصدار 2016 أو الإصدارات الأحدث من خادم SQL Server المحلي، غير الإصدار Express.	بلا قيود.
إصدار 2016 من SQL Server البعيد، غير الإصدار Express، أو الإصدار الأحدث.	صالح فقط في حالة وجود الجهازين في مجال Windows® نفسه؛ وفي حالة اختلاف المجالات، يجب إنشاء علاقة ثقة ثنائية بينهم.

نظام إدارة قاعدة البيانات	التوصيات والقيود
إصدارات MySQL 5.5 أو 5.6 أو 5.7 المحلية أو البعيدة (لم تعد إصدارات MySQL 5.5.1 و5.5.2 و5.5.3 و5.5.4 و5.5.5 مدعومة)	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 10000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.
MySQL 8.0.20 محلي أو عن بُعد أو إصدار أحدث	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 50000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.
MariaDB محلي أو بعيد (انظر الإصدارات المدعومة)	استخدم نظام إدارة قاعدة البيانات (DBMS) هذا إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 20000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.
PostgreSQL، Postgres Pro (انظر الإصدارات المدعومة)	استخدم أحد نظم إدارة قواعد البيانات هذه إذا كنت تنوي تشغيل خادم إدارة واحد لأقل من 50000 جهاز. يوصى بتعطيل مهمة مخزون البرامج وتعطيل إخطارات خادم الإدارة عند بدء تشغيل التطبيقات (في إعدادات سياسة Kaspersky Endpoint Security). يرجى الرجوع إلى الموضوع التالي للحصول على التفاصيل: حساب مساحة قاعدة البيانات.

إذا حددت MSSQL 2019، فيجب عليك استخدام التصحيح التراكمي CU12 أو إصدار أحدث. ويتيح لك ذلك تجنب الأخطاء والعبء الزائد على النظام الذي قد يحدث.

إذا كنت تستخدم PostgreSQL أو MariaDB أو MySQL DBMS، فإن علامة التبويب **الأحداث** قد تعرض قائمة غير كاملة بالأحداث للجهاز العميل المحدد. ويحدث هذا عندما يخزن نظام إدارة قواعد البيانات (DBMS) قدرًا كبيرًا جدًا من الأحداث. ويمكنك زيادة عدد الأحداث المعروضة عن طريق تنفيذ أي مما يلي:

- إزالة الأحداث غير الضرورية.
- تقليل مدة التخزين للأحداث غير الضرورية.

للاطلاع على قائمة كاملة بالأحداث التي تم تسجيلها على خادم الإدارة للجهاز، استخدم التقارير.

تحديد عنوان خادم الإدارة

عند تثبيت خادم الإدارة، يجب عليك تحديد العنوان الخارجي لخادم الإدارة. سيتم استخدام هذا العنوان كعنوان افتراضي عند إنشاء حزمة التثبيت الخاصة بعميل الشبكة. وبعد ذلك، سيكون بإمكانك تغيير عنوان مضيف خادم الإدارة باستخدام أدوات وحدة تحكم الإدارة، ولن يتغير العنوان تلقائيًا في حزم تثبيت عميل الشبكة التي تم إنشاؤها بالفعل.

تكوين الحماية في شبكة المؤسسة العميلة

بعد اكتمال تثبيت خادم الإدارة، يتم تشغيل وحدة تحكم الإدارة ويطلب منك إجراء الإعداد الأولي من خلال المعالج ذي الصلة. عند تشغيل معالج البدء السريع، يتم إنشاء السياسات والمهام التالية في مجموعة إدارة الجذر:

- سياسة Kaspersky Endpoint Security
- مهمة جماعية لتحديث Kaspersky Endpoint Security
- مهمة جماعية لفحص جهاز باستخدام Kaspersky Endpoint Security
- سياسة عميل الشبكة

- مهمة فحص الثغرات الأمنية (مهمة عميل الشبكة)
- مهمة تثبيت التحديثات وإصلاح الثغرات الأمنية (مهمة عميل الشبكة).

يتم إنشاء السياسات والمهام بالإعدادات الافتراضية، والتي قد يتبين أنها دون المستوى الأمثل أو حتى غير مقبولة للمؤسسة. لذلك، يجب عليك التحقق من خصائص الكائنات التي تم إنشاؤها والقيام بتعديلها يدويًا، إذا لزم الأمر.

يحتوي هذا القسم على معلومات حول تكوين السياسات والمهام والإعدادات الأخرى لخادم الإدارة يدويًا ومعلومات حول نقطة التوزيع وبناء بنية مجموعة إدارة والتسلسل الهرمي للمهام والإعدادات الأخرى.

الإعداد اليدوي لسياسة Kaspersky Endpoint Security

يقدم هذا القسم اقتراحات حول كيفية تكوين سياسة Kaspersky Endpoint Security، التي يتم إنشاؤها بواسطة معالج البدء السريع. يمكنك إجراء الإعداد في نافذة خصائص السياسة.

عند تحرير إعداد ما، ضع في الاعتبار أنه يجب عليك النقر على أيقونة القفل فوق الإعداد ذي الصلة للسماح باستخدام القيمة الخاصة به على محطة عمل.

تكوين السياسة في قسم الحماية من التهديدات المتقدمة

للحصول على وصف كامل للإعدادات الموجودة في هذا القسم، فبرجاء الرجوع إلى وثائق Kaspersky Endpoint Security for Windows.

في قسم **الحماية من التهديدات المتقدمة**، يمكنك تكوين استخدام Kaspersky Security Network لتطبيق Kaspersky Endpoint Security for Windows. كما يمكنك تكوين وحدات Kaspersky Endpoint Security for Windows النمطية، مثل اكتشاف السلوك ومنع الاستغلال ومنع اختراق المضيف ومحرك المعالجة.

في القسم الفرعي **Kaspersky Security Network**، نوصيك بتمكين الخيار **Kaspersky Security Network**. يساعد استخدام هذا الخيار في إعادة توزيع وتحسين حركة المرور على الشبكة. إذا كان خيار **Kaspersky Security Network** معطلاً، فيمكنك تمكين استخدام خوادم KSN مباشرةً.

تكوين السياسة في قسم الحماية من التهديدات الأساسية

للحصول على وصف كامل للإعدادات الموجودة في هذا القسم، فبرجاء الرجوع إلى وثائق Kaspersky Endpoint Security for Windows.

في قسم **الحماية من التهديدات الأساسية** في نافذة خصائص السياسة، نوصي بتحديد إعدادات إضافية في القسمين الفرعيين **جدار الحماية** و**الحماية من تهديدات الملفات**.

يحتوي القسم الفرعي **جدار الحماية** على إعدادات تسمح لك بالتحكم في نشاط الشبكة للتطبيقات على أجهزة العميل. يستخدم جهاز العميل شبكة تم تعيين إحدى الحالات التالية لها: عامة أو محلية أو موثوقة. اعتمادًا على حالة الشبكة، يمكن أن يسمح Kaspersky Endpoint Security بنشاط الشبكة على الجهاز أو يرفضه. عند إضافة شبكة جديدة إلى مؤسستك، يجب عليك تعيين حالة شبكة مناسبة لها. على سبيل المثال، إذا كان جهاز العميل عبارة عن كمبيوتر محمول ، فإننا نوصي بأن يستخدم هذا الجهاز الشبكة العامة أو الموثوقة، لأن الكمبيوتر المحمول غير متصل دائمًا بالشبكة المحلية. في القسم الفرعي **جدار الحماية**، يمكنك التحقق مما إذا كنت قد قمت بتعيين الحالات بشكل صحيح للشبكات المستخدمة في مؤسستك.

للتحقق من قائمة الشبكات:

1. في نافذة خصائص السياسة، انتقل إلى **الحماية من التهديدات الأساسية** ← **جدار الحماية**.

2. في قسم **الشبكات المتاحة**، انقر فوق الزر **الإعدادات**.

3. في نافذة **جدار الحماية** التي تفتح، انتقل إلى علامة التبويب **شبكات الاتصال** لعرض قائمة الشبكات.

في القسم الفرعي **الحماية من تهديدات الملفات**، يمكنك تعطيل فحص محركات أقراص الشبكة. من الممكن يتسبب فحص محركات أقراص الشبكة إلى تطبيق حمل كبير على محركات أقراص الشبكة. إجراء فحص غير مباشر على خوادم الملفات هو السلوك الأكثر ملاءمة.

لتعطيل فحص محركات أقراص الشبكة:

1. في خصائص السياسة، انتقل إلى **الحماية من التهديدات الأساسية** ← **الحماية من تهديدات الملفات**.

2. قي قسم **مستوى الأمان**، انقر فوق الزر **الإعدادات**.

3. في النافذة **الحماية من تهديدات الملفات** التي تفتح، في علامة التبويب **عام** امسح خانة الاختيار **كل محركات أقراص الشبكة**.

تكوين السياسة في قسم الإعدادات العامة

للحصول على الوصف الكامل للإعدادات الموجودة في هذا القسم، فبرجاء الرجوع إلى وثائق Kaspersky Endpoint Security.

موضّح أدناه إجراءات الإعداد المتقدمة، والتي ننصحك بإجرائها في نافذة خصائص السياسة لأجل Kaspersky Endpoint Security، في قسم **الإعدادات العامة**.

قسم الإعدادات العامة، القسم الفرعي التقارير وعمليات التخزين

في القسم **نقل البيانات إلى خادم الإدارة**، يرجى ملاحظة خانة الاختيار **حول التطبيقات التي تم تشغيلها**. عند حالة تحديد خانة الاختيار هذه، تحفظ قاعدة بيانات خادم الإدارة معلومات حول جميع إصدارات كل الوحدات النمطية للبرنامج على الأجهزة المتصلة بالشبكة. قد تتطلب هذه المعلومات مساحة كبيرة من مساحة القرص في قاعدة بيانات Kaspersky Security Center (عشرات الجيجابايت). لذلك، إذا كانت خانة اختيار **حول التطبيقات التي تم بدؤها** ما زالت محددة في سياسة المستوى الأعلى، يجب إزالة تحديدها.

قسم الإعدادات العامة، القسم الفرعي الواجهة

إذا كان من الضروري إدارة الحماية من التهديدات في شبكة المؤسسة في الوضع المركزي من خلال وحدة تحكم الإدارة، فيجب عليك تعطيل عرض واجهة مستخدم Kaspersky Endpoint Security على محطات العمل (عن طريق مسح **عرض واجهة التطبيق** خانة الاختيار في القسم **التفاعل مع المستخدم**)، وقم بتمكين الحماية بكلمة مرور (عن طريق تحديد خانة الاختيار **تمكين الحماية بكلمة مرور** في القسم **حماية بكلمة مرور**).

تكوين السياسة في القسم تكوين الحدث

في القسم **تكوين الحدث**، ينبغي عليك تعطيل حفظ أي أحداث على خادم الإدارة ماعدا الأحداث التالية:

- في علامة التبويب **حرج**:
  - تم تعطيل التشغيل التلقائي للتطبيق
  - تم رفض الوصول
  - تم حظر بدء تشغيل التطبيق

- يتعذر التنظيف
- تم انتهاك اتفاقية ترخيص المستخدم النهائي
- تعذر تحميل وحدة التشفير النمطية
- تعذر بدء مهمتين في نفس الوقت
- تم اكتشاف تهديد نشط. يجب بدء التنظيف المتقدم
- تم اكتشاف هجوم عبر الشبكة
- لم يتم تحديث كافة المكونات
- خطأ في التفعيل
- خطأ في تمكين الوضع المحمول
- حدث خطأ في التفاعل مع Kaspersky Security Center
- خطأ في تعطيل الوضع المحمول
- حدث خطأ في تغيير مكونات التطبيق
- خطأ في تطبيق قواعد تشفير / فك تشفير الملفات
- لا يمكن تطبيق السياسة
- تم إنهاء العملية
- تم منع نشاط الشبكة

- في علامة التبويب **خلل وظيفي**: إعدادات غير صالحة للمهمة. لم يتم تطبيق الإعدادات
- في علامة التبويب **تحذير**:
  - تم تعطيل الدفاع الذاتي
  - المفتاح الاحتياطي غير صحيح
  - انسحب المستخدم من سياسة التشفير
- في علامة التبويب **معلومات**: تم حظر بدء تشغيل التطبيق في وضع الاختبار

الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security

إذا كان خادم الإدارة يعمل كمصدر التحديث، فخيار الجدولة الأمثل والموصى به لإصدارات Kaspersky Endpoint Security هو **عند تنزيل تحديثات جديدة إلى المستودع** مع تحديد خانة الاختيار **استخدام التأخير العشوائي التلقائي لعمليات بدء تشغيل المهمة**.

إذا تم إنشاء مهمة محلية لتنزيل تحديثات من خوادم Kaspersky إلى المستودع على كل نقطة توزيع، فستكون الجدولة الدورية هي الخيار المثالي والموصى به لمهمة تحديث مجموعة Kaspersky Endpoint Security. وفي هذه الحالة، ينبغي تعيين قيمة الفاصل الزمني العشوائي إلى ساعة واحدة.

الإعداد اليدوي للمهمة الجماعية لفحص جهاز باستخدام Kaspersky Endpoint Security

ينشئ معالج البدء السريع مهمة جماعية لفحص جهاز. بشكل افتراضي، يتم تعيين الجدول **تشغيل في أيام الجمعة الساعة 00:7 م** للمهمة بعشوائية تلقائية، مع إلغاء تحديد خانة الاختيار **تشغيل المهام الفائتة**.

وهذا يعني أنه في حالة إيقاف تشغيل الأجهزة الموجودة في مؤسسة ما في أيام الجمعة على سبيل المثال في 30:6 م، فلن يتم تشغيل مهمة فحص الجهاز أبدًا. يجب عليك إعداد الجدول الأكثر ملاءمةً لهذه المهمة بناءً على قواعد مكان العمل التي تتبناها المؤسسة.

جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة

ينشئ معالج البدء السريع مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة لعميل الشبكة. بشكل افتراضي، يتم تعيين الجدول **تشغيل في أيام الثلاثاء الساعة 00:7 م** للمهمة بعشوائية تلقائية، مع تحديد خانة الاختيار **تشغيل المهام الفائتة**.

إذا كانت قواعد مكان العمل الخاصة بالمؤسسة تعمل على إيقاف تشغيل جميع الأجهزة في هذا الوقت، سيتم تشغيل مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة بعد تشغيل الأجهزة مرة أخرى، وسيكون هذا في صباح يوم الأربعاء. قد يكون مثل هذا النشاط غير مرغوب فيه لأن عملية فحص الثغرات لأمنية قد تزيد من الحمل على وحدات المعالجة المركزية والأنظمة الفرعية للقرص. يجب عليك إعداد الجدول الأكثر ملاءمةً للمهمة بناءً على قواعد مكان العمل التي تتبناها المؤسسة.

الإعداد اليدوي للمهمة الجماعية لتثبيت التحديثات وإصلاح الثغرات الأمنية

ينشئ معالج البدء السريع مهمة جماعية لتثبيت التحديثات وإصلاح الثغرات الأمنية لعميل الشبكة. بشكل افتراضي، يتم إعداد المهمة للتشغيل كل يوم الساعة 00:01 ص، بعشوائية تلقائية، مع إلغاء تمكين خيار **تشغيل المهام الفائتة**.

إذا كانت قواعد مكان العمل الخاصة بالمؤسسة تعمل على إيقاف تشغيل الأجهزة أثناء الليل، فلن يتم تشغيل تثبيت التحديثات أبدًا. يجب عليك إعداد الجدول الأكثر ملاءمةً لمهمة فحص الثغرات الأمنية بناءً على قواعد مكان العمل التي تتبناها المؤسسة. من المهم أيضًا أن تضع في اعتبارك أن تثبيت التحديثات قد يتطلب إعادة تشغيل الجهاز.

بناء بنية مجموعات الإدارة وتعيين نقاط التوزيع

تُجري بنية مجموعات الإدارة في Kaspersky Security Center الوظائف التالية:

- تعيين نطاق السياسات.

  توجد طريقة بديلة لتطبيق مجموعات الإعدادات ذات الصلة على الأجهزة، عن طريق استخدام ملفات تعريف السياسة. في هذه الحالة، يتم تعيين نطاق السياسات، على سبيل المثال، باستخدام العلامات ومواقع الجهاز في الوحدات التنظيمية لبرنامج Active Directory والعضوية في مجموعات أمان Active Directory.

- تعيين نطاق المهام الجماعية.

  يوجد نهج لتحديد نطاق المهام الجماعية غير المستندة إلى التسلسل الهرمي لمجموعات الإدارة: استخدام المهام لتحديدات الأجهزة والمهام لأجهزة محددة.

- تعيين حقوق الوصول إلى الأجهزة وخوادم الإدارة الافتراضية وخوادم الإدارة الثانوية.

- يقوم بتعيين نقاط التوزيع.

عند بناء بنية مجموعات الإدارة، يجب عليك الأخذ في الاعتبار مخطط شبكة المؤسسة للتعيين الأمثل لنقاط التوزيع. يتيح التوزيع المثالي لنقاط التوزيع توفير الحركة على شبكة المؤسسة.

بناءً على المخطط التنظيمي للمؤسسة ومخطط الشبكة المعتمد من عميل MSP، يمكن تطبيق التكوينات القياسية التالية على بنية مجموعات الإدارة.

- مكتب واحد
- مكاتب صغيرة متعددة منفصلة

التكوين القياسي لعميل MSP: مكتب واحد

في التكوين القياسي "مكتب واحد"، تكون كل الأجهزة داخل شبكة المؤسسة ويمكنها "رؤية" بعضها البعض. قد تتكون شبكة المؤسسة من عدد قليل من أجزاء منفصلة (الشبكات أو قطاعات الشبكة) التي ترتبط من خلال قنوات ضيقة.

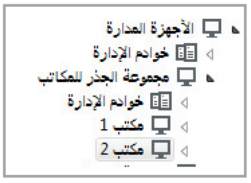
يمكن أن تتوفر الطرق التالية لبناء بنية مجموعات الإدارة:

- بناء بنية مجموعات الإدارة مع الأخذ في الاعتبار مخطط الشبكة. قد لا تعكس بنية مجموعات الإدارة مخطط الشبكة بالدقة المطلقة. قد يكون التطابق بين الأجزاء المنفصلة للشبكة ومجموعات الإدارة المحددة كافيًا. يمكنك استخدام التعيين التلقائي لنقاط التوزيع أو تعيينها يدويًا.
- بناء بنية مجموعات الإدارة دون أخذ مخطط الشبكة في الاعتبار. في هذه الحالة، يجب عليك تعطيل التعيين التلقائي لنقاط التوزيع ثم تعيين جهاز واحد أو عدة أجهزة للعمل كنقاط توزيع لمجموعة إدارة الجذر في كل جزء من الأجزاء المنفصلة للشبكة، على سبيل المثال، لمجموعة **الأجهزة المدارة**. ستكون جميع نقاط التوزيع عند نفس المستوى وستتميز بنفس النطاق لتغطي جميع الأجهزة في شبكة المؤسسة. في هذه الحالة، سيتصل كل من وكلاء الشبكة بنقطة التوزيع التي تحتوي على أقصر مسار. يمكن تتبع المسار إلى نقطة توزيع عن طريق الأداة المساعدة tracert.

التكوين القياسي لعميل MSP: مكاتب صغيرة متعددة بعيدة

يعمل هذا التكوين القياسي على عدد من المكاتب الصغيرة البعيدة، والتي قد تكون متصلة بالمكتب الرئيسي عبر الإنترنت. كل مكتب بعيد موجود وراء NAT، بمعنى أن الاتصال من مكتب بعيد إلى مكتب آخر غير ممكن لأن الأجهزة معزولة عن بعضها.

يجب أن ينعكس هذا التكوين في بنية مجموعات الإدارة: يجب إنشاء مجموعة إدارة منفصلة لكل مكتب بعيد (المجموعات **المكتب 1** و**المكتب 2** في الشكل الموجود أدناه).



يتم تضمين المكاتب البعيدة في بنية مجموعة الإدارة

يجب تعيين نقطة توزيع واحدة أو عدة نقاط توزيع لكل مجموعة إدارة مقابلة لمكتب ما. يجب أن تكون نقاط التوزيع أجهزة موجودة في المكتب البعيد تحتوي على مساحة قرص خالية كافية. ستتمكن الأجهزة التي تم نشرها في المجموعة **المكتب 1** على سبيل المثال، من الوصول إلى نقاط التوزيع المعينة لمجموعة الإدارة **المكتب 1**.

إذا كان بعض المستخدمين يتنقلون فعليًا بين المكاتب مع أجهزة الكمبيوتر المحمولة الخاصة بهم، فيجب عليك تحديد جهازين أو أكثر (بالإضافة إلى نقاط التوزيع الحاليين) في كل مكتب بعيد وتعيينهم للعمل كنقاط توزيع لمجموعة إدارة من المستوى الأعلى (**المجموعة الجذر للمكاتب** في الشكل الموجود أعلاه).

مثال: جهاز كمبيوتر محمول تم نشره في مجموعة الإدارة **المكتب 1** ثم انتقل فعليًا إلى مكتب مقابل لمجموعة الإدارة **المكتب 2**. بعد انتقال جهاز الكمبيوتر المحمول، يحاول عميل الشبكة الوصول إلى نقاط التوزيع المعينة إلى المجموعة **المكتب 1**، إلا إن هذه النقاط تكون غير متاحة. آنذاك، يحاول عميل الشبكة الوصول إلى نقاط التوزيع التي تم تعيينها إلى **المجموعة الجذر للمكاتب**. ولأن المكاتب البعيدة معزولة عن بعضها، فإن محاولات الوصول إلى نقاط التوزيع المعينة إلى مجموعة الإدارة **المجموعة الجذر للمكاتب** لن تكون ناجحة إلا عند محاولة عميل الشبكة الوصول إلى نقاط التوزيع في مجموعة **المكتب 2**. بمعنى أن جهاز الكمبيوتر المحمول سيظل في مجموعة الإدارة المقابلة للمكتب الأولي، ولكن جهاز الكمبيوتر المحمول سيستخدم نقطة التوزيع الخاصة بالمكتب الذي يوجد فيه فعليًا في الوقت الحالي.

التسلسل الهرمي للسياسات، واستخدام ملفات تعريف السياسة

يُقدم هذا القسم معلومات حول كيفية تطبيق السياسات على الأجهزة في مجموعات الإدارة. يوفر هذا القسم أيضًا معلومات حول ملفات تعريف السياسة.

التسلسل الهرمي للسياسات

في Kaspersky Security Center، أنت تستخدم سياسات لتحديد مجموعة فردية من الإعدادات لأجهزة متعددة. على سبيل المثال، نطاق السياسة للتطبيق P المحددة لمجموعة الإدارة G يتضمن أجهزة مدارة مثبت عليها التطبيق P الذي تم نشره في المجموعة G وكل مجموعاتها الفرعية، باستثناء المجموعات الفرعية التي تم إلغاء تحديد خانة الاختيار **توريث من المجموعة الأصلية** في خصائصها.

تتميز السياسة عن أي إعداد محلي بوجود رموز قفل (🔒) بجانب إعداداتها. في حالة قفل إعداد ما (أو مجموعة إعدادات) في خصائص السياسة، يجب عليك أولاً استخدام هذا الإعداد (أو مجموعة الإعدادات) عند إنشاء إعدادات فعالة، وثانيًا يجب كتابة الإعدادات أو مجموعة الإعدادات في سياسة انتقال البيانات من الخادم.

يمكن وصف إنشاء الإعدادات الفعالة على جهاز ما كما يلي: يتم الحصول على قيم كل الإعدادات التي لم يتم قفلها من السياسة، ثم يتم الكتابة عليها باستخدام قيم الإعدادات المحلية، ثم يتم الكتابة على المجموعة الناتجة باستخدام قيم الإعدادات التي تم قفلها والتي تم الحصول عليها من السياسة.

تؤثر السياسات الخاصة بالتطبيق نفسه على بعضها البعض عبر من خلال الترتيب الهرمي لمجموعات الإدارة: الإعدادات التي تم قفلها من سياسة انتقال البيانات إلى الخادم تقوم بالكتابة فوق الإعدادات نفسها من سياسة انتقال البيانات من الخادم.

توجد سياسة خاصة للمستخدمين خارج المكتب. تسري هذه السياسة على الجهاز عندما يتحول إلى وضع الوجود خارج المكتب. لا تؤثر سياسات خارج المكتب على السياسات الأخرى من خلال الترتيب الهرمي لمجموعات الإدارة.

ملفات تعريف السياسة

قد يكون تطبيق السياسات على الأجهزة من خلال الترتيب الهرمي لمجموعات الإدارة فقط غير ملائم في كثير من الحالات. قد يكون من الضروري إنشاء مثيلات متعددة لسياسة واحدة ما تختلف بإعداد واحد أو اثنين لمجموعات إدارة مختلفة، ومزامنة المحتويات الخاصة بهذه السياسات في المستقبل.

لمساعدتك في تجنب مثل هذه المشاكل، يدعم Kaspersky Security Center ملفات تعريف السياسة. ملف تعريف السياسة هو مجموعة فرعية مسمّاة لإعدادات السياسة. يتم توزيع هذه المجموعة الفرعية على الأجهزة المستهدفة بالإضافة إلى السياسة، وتلحقها في حالة خاصة تُسمى شرط تفعيل ملف التعريف. تحتوي ملفات التعريف فقط على الإعدادات التي تختلف عن السياسة "الأساسية" والتي تكون نشطة على الجهاز العميل (كمبيوتر أو جهاز محمول). يؤدي تنشيط ملف التعريف إلى تعديل إعدادات السياسة التي كانت نشطة على الجهاز قبل أن يتم تنشيط ملف التعريف. هذه الإعدادات تأخذ القيم التي تم تحديدها في ملف التعريف.

يتم فرض القيود التالية حاليًا على ملفات تعريف السياسة:

- يمكن أن تتضمن سياسة ما على 100 ملف تعريف بحد أقصى.
- لا يمكن أن يحتوي ملف تعريف سياسة على ملفات تعريف أخرى
- لا يمكن أن يحتوي ملف تعريف السياسة على إعدادات الإخطار.

محتويات ملف التعريف

يحتوي ملف تعريف السياسة على الأجزاء التأسيسية التالية:

- الاسم. تؤثر ملفات التعريف ذات الأسماء المتشابهة على بعضها البعض عبر الترتيب الهرمي لمجموعات الإدارة ذات القواعد المشتركة.
- مجموعة فرعية من إعدادات السياسة. على عكس السياسة، التي تحتوي على كل الإعدادات، يحتوي ملف التعريف على الإعدادات المطلوبة فعليًا فقط (الإعدادات المقفولة).

- شرط التعريف هو تعبير منطقي باستخدام خصائص الجهاز. يكون ملف التعريف نشطًا (يلحق بالسياسة) فقط عندما يتحقق شرط تنشيط ملف التعريف. في كل الحالات الأخرى، يكون ملف التعريف غير نشط ويتم تجاهله. يمكن تضمين خصائص الجهاز التالية في هذا التعبير المنطقي:
  - حالة وضع الوجود خارج المكتب.
  - خصائص بيئة الشبكة—اسم القاعدة المفعلة لـ اتصال عميل الشبكة.
  - وجود أو غياب علامات محددة على الجهاز
  - موقع الجهاز في وحدة Active Directory: بشكل صريح (يوجد الجهاز في الوحدة التنظيمية المحددة) أو ضمنيًا (يوجد الجهاز في وحدة تنظيمية ما، والذي يوجد ضمن الوحدة التنظيمية المحددة على أي مستوى من التداخل)
  - عضوية الجهاز في مجموعة أمن Active Directory (بشكل صريح أو ضمني)
  - عضوية مالك الجهاز في مجموعة أمن Active Directory (بشكل صريح أو ضمني)
- خانة اختيار تعطيل ملف التعريف. دائمًا ما يتم تجاهل ملفات التعريف المعطلة ولا يتم التحقق من شروط التنشيط الخاصة بها.
- أولوية ملف التعريف. شروط التنشيط الخاصة بملفات التعريف المختلفة مستقلة، وبذلك يمكن تنشيط العديد من ملفات التعريف في الوقت نفسه. إذا كانت ملفات التعريف المفعلة لا تحتوي على مجموعات إعدادات متداخلة، فلن تحدث أي مشكلة. ولكن، إذا كان ملفا تعريف نشطان يحتويان على قيم مختلفة للإعداد نفسه، فسيحدث التباس. يمكن تجنب هذا الالتباس عبر خصائص ملف التعريف: سيتم الحصول على قيمة المتغير الملتبسة من ملف التعريف الذي يملك الأولوية الأعلى (وهو الملف ذي التصنيف الأعلى في قائمة ملفات التعريف).

سلوك ملفات التعريف عندما تؤثر السياسات على بعضها البعض عبر الترتيب الهرمي

يتم دمج ملفات التعريف التي لها الاسم نفسه طبقًا لقواعد الدمج الخاصة بالسياسة. تملك ملفات التعريف الخاصة بسياسة نقل البيانات إلى الخادم أولوية أعلى من ملفات تعريف سياسة نقل البيانات من الخادم. في حالة حظر إعدادات التحرير في سياسة نقل البيانات إلى الخادم (تم قفلها)، تستخدم سياسة نقل البيانات من الخادم شروط تفعيل ملف التعريف من سياسة نقل البيانات إلى الخادم. في حالة السماح بإعدادات التحرير في سياسة نقل البيانات إلى الخادم، يتم استخدام شروط تنشيط ملف التعريف من سياسة نقل البيانات من الخادم.

حيث إن ملف تعريف السياسة قد يحتوي على الخاصية **الجهاز غير متصل** في شرط التنشيط الخاص به، فإن ملفات التعريف تستبدل تمامًا ميزة السياسات للمستخدمين خارج المكتب، والتي لن تعد مدعومة.

قد تحتوي سياسة خاصة بالمستخدمين خارج المكتب على ملفات تعريف، ولكن يمكن تنشيط ملفات تعريفها فقط بعدما يتحول الجهاز إلى وضع الوجود خارج المكتب.

المهام

يقوم Kaspersky Security Center بإدارة تطبيقات Kaspersky security المثبتة على الأجهزة عن طريق إنشاء المهام وتشغيلها. يلزم وجود المهام من أجل تثبيت التطبيقات، وبدء تشغيلها، وإيقافها، وفحص الملفات، وتحديث قواعد البيانات والوحدات النمطية للبرامج، واتخاذ إجراءات أخرى بشأن التطبيقات.

يمكن إنشاء مهام لتطبيق محدد فقط في حالة تثبيت مكونات الإدارة لهذا التطبيق.

يمكن إجراء المهام على خادم الإدارة وعلى الأجهزة.

يتم إجراء المهام التالية على خادم الإدارة:

- التوزيع التلقائي للتقارير
- تنزيل التحديثات إلى مستودع خادم الإدارة
- النسخ الاحتياطي لبيانات خادم الإدارة

- صيانة قاعدة البيانات
- مزامنة Windows Update
- إنشاء حزمة تثبيت بناءً على صورة نظام التشغيل (OS) للجهاز المرجعي

يتم إجراء أنواع المهام التالية على الأجهزة:

- المهام المحلية—هي المهام التي يتم إجراؤها على جهاز محدد

  يمكن تعديل المهام المحلية إما بواسطة المسؤول باستخدام أدوات وحدة تحكم الإدارة أو بواسطة مستخدم جهاز بعيد (على سبيل المثال، عبر واجهة تطبيق الأمان). في حالة تعديل مهمة محلية بواسطة المسؤول ومستخدم الجهاز المُدار في الوقت نفسه، فستسري التغييرات التي يقوم بها المسؤول حيث أنه يملك أولوية أعلى.

- المهام الجماعية—هي المهام التي يتم إجرائها على كافة الأجهزة الخاصة بمجموعة محددة

  ما لم يتم تحديد خلاف ذلك في خصائص المهمة، تؤثر أيضًا المهمة الجماعية على كافة المجموعات الفرعية الخاصة بالمجموعة المحددة. كما تؤثر المهام الجماعية (بشكل اختياري) على الأجهزة المتصلة بخوادم الإدارة الثانوية والافتراضية التي تم نشرها في هذه المجموعة أو أيٍ من مجموعاتها الفرعية.

- المهام العالمية—هي المهام التي تنفذ على مجموعة من الأجهزة محددة بصرف النظر عما إذا كانت مضمنة في أية مجموعة إدارة أم لا

يمكنك إنشاء أي عدد من المهام الجماعية أو المهام العالمية أو المهام المحلية، وذلك لكل تطبيق.

ويمكنك إجراء تغييرات على إعدادات المهام، وعرض مستوى تقدمها، ونسخها، وتصديرها، واستيرادها، وحذفها.

لا يتم بدء تشغيل المهمة على جهاز إلا إذا كان التطبيق الذي تم إنشاء المهمة له قيد التشغيل.

يتم حفظ نتائج المهام في سجل أحداث Microsoft Windows وسجل أحداث Kaspersky Security Center، بشكل مركزي على حد سواء على خادم الإدارة ومحليًا على كل جهاز.

لا تقم بتضمين بيانات خاصة في إعدادات المهمة. على سبيل المثال، تجنّب تخصيص كلمة مرور مسؤول المجال.

قواعد نقل الجهاز

نوصيك بإجراء التخصيص التلقائي للأجهزة إلى مجموعات الإدارة على الخادم الافتراضي الذي يطابق عميل MSP، باستخدام قواعد نقل الجهاز. تتكون قاعدة نقل جهاز ما من ثلاثة أجزاء رئيسية: اسم وشرط التنفيذ (التعبير المنطقي باستخدام سمات الجهاز) ومجموعة إدارة مستهدفة. تقوم قاعدة ما بنقل جهاز ما إلى مجموعة الإدارة الهدف إذا توافقت سمات الجهاز مع شرط تنفيذ القاعدة.

كل قواعد نقل الأجهزة تحتوي على أولويات. يتحقق خادم الإدارة من سمات الجهاز وهل تتوافق هذه السمات مع شرط تنفيذ كل قاعدة أو لا، بترتيب تصاعدي للأولويات. إذا توافقت سمات الجهاز مع شرط تنفيذ قاعدة ما، يتم نقل الجهاز إلى المجموعة الهدف، وبذلك تكتمل معالجة القاعدة لهذا الجهاز. إذا توافقت سمات الجهاز مع شروط قواعد متعددة، يتم نقل الجهاز إلى المجموعة الهدف الخاصة بالقاعدة ذات الأولوية الأعلى (أي التي لها أعلى رتبة في قائمة القواعد).

يمكن إنشاء قواعد نقل الجهاز ضمنيًا. على سبيل المثال، في خصائص حزمة تثبيت ما أو مهمة تثبيت عن بُعد، يمكنك تحديد مجموعة الإدارة التي يجب نقل الجهاز إليها بعد تثبيت عميل الشبكة عليه. كما يمكن إنشاء قواعد نقل الجهاز بشكل صريح بواسطة مسؤول Kaspersky Security Center، في قائمة قواعد النقل. توجد القائمة في وحدة تحكم الإدارة، في خصائص مجموعة **الأجهزة غير المخصصة**.

بشكل افتراضي، تكون قاعدة نقل جهاز مصممة للتخصيص الأولي للأجهزة إلى مجموعات الإدارة لمرة واحدة. تنقل القاعدة الأجهزة من مجموعة **الأجهزة غير المخصصة** مرة واحدة فقط. في حالة نقل جهاز مرة واحدة بواسطة هذه القاعدة، فلن تنقله القاعدة مرة أخرى أبدًا، حتى وإن قمت بإعادة الجهاز إلى مجموعة **الأجهزة غير المخصصة** يدويًا. هذه هي الطريقة المستحسنة لتطبيق قواعد النقل.

يمكنك نقل الأجهزة التي تم تخصيصها بالفعل لبعض مجموعات الإدارة. للقيام بذلك، من خصائص القاعدة، قم بإلغاء تحديد خانة الاختيار **نقل الأجهزة التي لا تنتمي لأي من مجموعات إدارة فقط**.

يؤدي تطبيق قواعد النقل على الأجهزة التي تم تخصيصها بالفعل لبعض مجموعات الإدارة إلى زيادة الحمل بشكل كبير على خادم الإدارة.

يمكنك إنشاء قاعدة نقل من شأنها التأثير على جهاز واحد بشكل متكرر.

ننصح بشدة أن تتجنب نقل جهاز واحد من مجموعة إلى أخرى بشكل متكرر (على سبيل المثال، لتطبيق سياسة محددة على هذا الجهاز، قم بتشغيل مهمة جماعية محددة أو قم بتحديث الجهاز عبر نقطة توزيع محددة).

مثل هذا السيناريو غير مدعوم، لأنه يزيد الحمل على خادم الإدارة وحركة مرور الشبكة إلى الدرجة القصوى. تتعارض هذه السيناريوهات أيضًا مع مبادئ تشغيل Kaspersky Security Center (وبخاصةً في مناطق حقوق الوصول والأحداث والتقارير). يجب العثور على حل أخر، على سبيل المثال، من خلال استخدام ملفات تعريف السياسة، والمهام الخاصة بـ تحديدات الأجهزة، وتعيين عملاء الشبكة حسب السيناريو القياسي، وما إلى ذلك.

تصنيف البرنامج

الأداة الرئيسية لتشغيل التطبيقات هي فئات Kaspersky (يُشار إليها فيما بعد باسم فئات KL). تساعد فئات KL مسؤولي Kaspersky Security Center في تبسيط دعم تصنيف البرامج وتقليل حركة المرور المتوجهة إلى الأجهزة المدارة لأدنى حد.

يجب إنشاء فئات المستخدم فقط للتطبيقات التي لا يمكن تصنيفها في أي من فئات KL (على سبيل المثال البرامج المعدّة حسب الطلب). يتم إنشاء فئات المستخدم على أساس حزمة التثبيت الخاصة بتطبيق ما (MSI) أو مجلد يحتوي على حزمة التثبيت.

في حالة توفر مجموعة كبيرة من البرامج، والتي لم يتم تصنيفها عبر فئات KL، فقد يكون من المفيد إنشاء فئة يتم تحديثها تلقائيًا. ستتم إضافة المجاميع الاختبارية للملفات التنفيذية إلى هذه الفئة عند كل تعديل للمجلد الذي يحتوي على حزم التوزيع.

لا تنشئ فئات برامج محدثة تلقائيًا للمجلدات My Documents و%windir% و%ProgramFiles% و%ProgramFiles(x86)%. تخضع مجموعة الملفات الموجودة في هذه المجلدات لتغييرات متكررة، والتي تؤدي إلى حمل زائد على خادم الإدارة وحركة مرور الشبكة. يجب عليك إنشاء مجلد مخصص لمجموعة البرامج وإضافة عناصر جديدة إليه بشكل دوري.

معلومات عن التطبيقات متعددة المستأجرين

يمكّن Kaspersky Security Center مسؤولي مزودي الخدمة ومسؤولي المستأجر من استخدام تطبيقات Kaspersky التي تتمتع بدعم التشغيل المتعدد. بعد تثبيت تطبيق Kaspersky متعدد المستأجرين في البنية التحتية لمزود خدمة، يمكن للمستأجرين بدء استخدام التطبيق.

لتمييز المهام والسياسات المتعلقة بأي من المستأجرين، يلزم إنشاء خادم إدارة افتراضي مخصص في Kaspersky Security Center لكل مستأجر. يلزم إنشاء جميع المهام والسياسات للتطبيقات متعددة المستأجرين التي يتم تعيينها لمستأجر ما لمجموعة إدارة الأجهزة المدارة لخادم الإدارة الافتراضي المطابق لهذا المستأجر. لا تؤثر المهام التي تم إنشاؤها لمجموعات الإدارة المتعلقة بخادم الإدارة الرئيسي في أجهزة المستأجرين.

وعلى عكس مسؤولي مزود الخدمة، يمكن لمسؤول المستأجر إنشاء مهام وسياسات التطبيق وعرضها فقط لأجهزة المستأجر المطابق. تكون مجموعات إعدادات المهام والسياسات المتاحة لمسؤولي مزود الخدمة ومسؤولي المستأجر مختلفة. تكون بعض إعدادات المهام والسياسة غير متاحة لمسؤولي المستأجر.

ضمن البنية الهرمية للمستأجر، يتم توريث السياسات التي تم إنشاؤها للتطبيقات متعددة المستأجرين في مجموعات الإدارة منخفضة المستوى وكذلك في مجموعات الإدارة ذات المستوى الأعلى: يتم نشر السياسة على جميع الأجهزة العميلة التي تنتمي إلى المستأجر.

النسخ الاحتياطي والاستعادة لإعدادات خادم الإدارة

النسخ الاحتياطي لإعدادات خادم الإدارة وقاعدة البيانات الخاصة به عبر مهمة النسخ الاحتياطي والأداة المساعدة klbackup. تتضمن النسخة الاحتياطية جميع الإعدادات والكائنات الرئيسية المتعلقة بخادم الإدارة، مثل الشهادات، والمفاتيح الأساسية لتشفير محركات الأقراص على الأجهزة المُدارة، ومفاتيح التراخيص المختلفة، وهيكل مجموعات الإدارة بكل محتوياتها، ومهامها، وسياساتها، إلخ. . باستخدام نسخة احتياطية، يمكنك استعادة تشغيل خادم الإدارة في أسرع وقت ممكن، حيث تستغرق من اثنتي عشرة دقيقة إلى بضع ساعات في ذلك.

في حالة عدم توفر نسخة احتياطية، قد يؤدي العطل إلى خسارة نهائية للشهادات وكل إعدادات خادم الإدارة. وسيستلزم هذا إعادة تكوين Kaspersky Security Center من البداية، وإجراء النشر الأولي لعميل الشبكة على شبكة الشركة مرة أخرى. كما ستفقد أيضًا كل المفاتيح الرئيسية لتشفير محركات الأقراص الموجودة على الأجهزة المدارة، مما يعرضك لمجازفة الفقد النهائي لكل البيانات المشفرة الموجودة على الأجهزة المثبت عليها Kaspersky Endpoint Security. وبالتالي، لا تغفل عن عمليات النسخ الاحتياطي لخادم الإدارة باستخدام مهمة النسخ الاحتياطي القياسية.

ينشئ معالج البدء السريع مهمة النسخ الاحتياطي لإعدادات خادم الإدارة ويضبطها كي تعمل يوميًا الساعة 00:4 صباحًا. يتم حفظ النسخ الاحتياطية افتراضيًا في المجلد %ALLUSERSPROFILE\Application Data\KasperskySC.

في حالة تثبيت مثيل لخادم Microsoft SQL Server على جهاز آخر يُستخدم كنظام إدارة قواعد البيانات، فيجب عليك تعديل مهمة النسخ الاحتياطي عن طريق تحديد مسار UNC، المتوفر للكتابة بواسطة كلاً من خدمة خادم الإدارة وخدمة خادم SQL Server، كمجلد لتخزين النسخ الاحتياطية. هذا المتطلب مشتق من ميزة خاصة للنسخ الاحتياطي في نظام إدارة قواعد البيانات الخاص بخادم Microsoft SQL Server.

في حالة استخدام مثيل محلي لخادم Microsoft SQL Server كنظام إدارة قواعد بيانات، ننصح كذلك بحفظ النسخ الاحتياطية على وسيط مخصص لتأمينها ضد التلف بالإضافة إلى خادم الإدارة.

لأن النسخة الاحتياطية تحتوي على بيانات مهمة، فإن مهمة النسخ الاحتياطي والأداة المساعدة klbackup يعملان على حماية النسخ احتياطية باستخدام كلمة مرور. بشكل افتراضي، يتم إنشاء مهمة النسخ الاحتياطي بكلمة مرور فارغة. يجب عليك تعيين كلمة مرور في خصائص مهمة النسخ الاحتياطي. يتسبب تجاهل هذا الطلب في أن تظل كل مفاتيح شهادات خادم الإدارة ومفاتيح التراخيص والمفاتيح الرئيسية لتشفير كل محركات الأقراص الموجودة على الأجهزة المدارة غير مشفرة.

بالإضافة إلى إجراء النسخ الاحتياطي بانتظام، يجب عليك أيضًا إنشاء نسخة احتياطية قبل كل تغيير مهم، بما في ذلك تثبيت خادم الإدارة وترقياته وتصحيحاته.

إذا كنت تستخدم Microsoft SQL Server باعتباره DBMS، فيمكنك تصغير حجم النسخ الاحتياطية. للقيام بذلك، قم بتمكين **ضغط النسخ الاحتياطي** الخيار في إعدادات خادم SQL.

تتم الاستعادة من نسخة احتياطية باستخدام الأداة المساعدة klbackup على مثيل قابل للتشغيل لخادم الإدارة الذي تم تثبيته للتو وله نفس الإصدار (أو أحدث) الذي تم إنشاء النسخة الاحتياطية له.

يجب أن يقوم مثيل خادم الإدارة الذي ستتم عملية الاستعادة عليه باستخدام نظام إدارة قواعد بيانات من النوع نفسه (على سبيل المثال، SQL Server أو MariaDB نفسه) والإصدار نفسه أو إصدار أحدث. يمكن أن يكون إصدار خادم الإدارة هو نفسه (بتصحيح مشابه أو أحدث) أو إصدار أحدث.

يوضح هذا القسم السيناريوهات القياسية لإعدادات الاستعادة وكائنات خادم الإدارة.

تعذر تشغيل جهاز يحتوي على خادم الإدارة

في حالة تعذر تشغيل جهاز يحتوي على خادم الإدارة نتيجة لعطل ما، فمن المستحسن أن تقوم بالإجراءات التالية:

- يجب تعيين خادم الإدارة الجديد إلى العنوان نفسه: اسم NetBIOS أو FQDN أو IP ثابت (بناءً على ما تم تعيينه منهم عند نشر عملاء الشبكة).
- تثبيت خادم إدارة من الإصدار نفسه (أو أحدث) باستخدام نظام إدارة قواعد بيانات من نفس النوع. يمكنك تثبيت الإصدار نفسه من الخادم بالتصحيح نفسه (أو أحدث) أو إصدار أحدث من الخادم. بعد التثبيت، لا تقم بإعداد أولي من خلال المعالج.
- من قائمة **ابدأ** قم بتشغيل الأداة المساعدة klbackup وتنفيذ الاستعادة.

إعدادات خادم الإدارة أو قاعدة البيانات تالفة

إذا تعذر تشغيل خادم الإدارة نتيجة لتلف الإعدادات أو قاعدة البيانات (على سبيل المثال، بعد حدوث تغير مفاجئ في الطاقة)، فمن المستحسن أن تستخدم سيناريو الاستعادة التالي:

1. فحص نظام الملفات الموجود على الجهاز التالف.
2. إلغاء تثبيت الإصدار غير القابل للتشغيل من خادم الإدارة.
3. إعادة تثبيت خادم الإدارة، باستخدام نظام إدارة قواعد بيانات من النوع نفسه ومن الإصدار نفسه (أو أحدث). يمكنك تثبيت الإصدار نفسه من الخادم بالتصحيح نفسه (أو أحدث) أو إصدار أحدث من الخادم. بعد التثبيت، لا تقم بإعداد أولي من خلال المعالج.
4. من القائمة **بدء**، قم بتشغيل الأداة المساعدة klbackup وإجراء الاستعادة.

يُحظر استعادة خادم الإدارة بأي طريقة إلا من خلال الأداة المساعدة klbackup.

أية محاولات لاستعادة خادم الإدارة من خلال برنامج تابع لجهة خارجية ستؤدي حتمًا إلى عدم مزامنة البيانات على عُقَد تطبيق Kaspersky Security Center الموزّع، وبالتالي عمل التطبيق بطريقة غير صحيحة.

نشر عميل الشبكة وتطبيق الأمان

لإدارة أجهزة في مؤسسة ما، يجب عليك تثبيت عميل الشبكة على كلٍ منها. تبدأ عملية نشر Kaspersky Security Center الموزّع على أجهزة المؤسسة عادةً بتثبيت عميل الشبكة عليها.

في Microsoft Windows XP، قد لا يُجري عميل الشبكة العمليات التالية بشكل صحيح: تنزيل التحديثات مباشرة من خوادم Kaspersky (كنقطة توزيع) والعمل كخادم وكيل لشبكة KSN (كنقطة توزيع) واكتشاف الثغرات الأمنية لجهة خارجية (في حالة استخدام إدارة الثغرات الأمنية والتصحيحات).

النشر الأولي

إذا تم تثبيت عميل الشبكة بالفعل على جهاز ما، فيتم إجراء تثبيت التطبيقات عن بُعد على هذا الجهاز عبر عميل الشبكة هذا. يتم نقل حزمة التوزيع الخاصة بتطبيق ما المراد تثبيتها عبر قنوات الاتصال بين عملاء الشبكة وخادم الإدارة، بالإضافة إلى إعدادات التثبيت المحددة بواسطة المسؤول. لنقل حزمة التوزيع ، يمكنك استخدام عقد توزيع الترحيل، أي نقاط التوزيع، وتسليم البث المتعدد، وما إلى ذلك. لمزيد من التفاصيل حول كيفية تثبيت التطبيقات على الأجهزة المُدارة مع تثبيت عميل الشبكة بالفعل، انظر أدناه في هذا القسم.

يمكنك إجراء تثبيت أولي لعميل الشبكة على الأجهزة التي تعمل بنظام تشغيل Windows، باستخدام طريقة من الطرق التالية:

- باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد.
- باستخدام سياسات المجموعة من Windows: باستخدام أدوات الإدارة القياسية من Windows لسياسات المجموعة.
- في الوضع الإجباري، استخدام خيارات خاصة في مهمة التثبيت عن بُعد لـ Kaspersky Security Center.
- عن طريق إرسال روابط الحزم المستقلة التي يتم إنشاؤها بواسطة Kaspersky Security Center إلى مستخدمي الجهاز. الحزم المستقلة هي وحدات نمطية تنفيذية تحتوي على حزم التوزيع الخاصة بالتطبيقات المحددة مع تحديد إعداداتها.
- يدويًا، عن طريق تشغيل مثبّتات التطبيق على الأجهزة.

في المنصات بخلاف Microsoft Windows، يتعين عليك تنفيذ التثبيت الأولي لعميل الشبكة على الأجهزة المدارة إما من خلال أدوات الجهات الخارجية الموجودة، أو يدويًا، أو بإرسال أرشيف به حزمة توزيع تم تكوينها مسبقًا إلى المستخدمين. يمكنك ترقية عميل الشبكة إلى إصدار جديد أو تثبيت تطبيقات Kaspersky الأخرى على الأنظمة الأساسية غير Windows، باستخدام عملاء شبكة (مثبتين بالفعل على الأجهزة) لإجراء مهام تثبيت عن بُعد. في هذه الحالة، يكون التثبيت مطابق للتثبيت الموجود على أجهزة تعمل بنظام التشغيل Microsoft Windows.

عند تحديد طريقة واستراتيجية لنشر التطبيقات في شبكة مُدارة، يجب عليك وضع عدد من العوامل في الاعتبار (قائمة جزئية):

- تكوين شبكة المؤسسة
- إجمالي عدد الأجهزة
- وجود مجالات Windows في الشبكة المُدارة، احتمالية تعديل سياسات مجموعة Active Directory في تلك المجالات
- التعرف على حساب (حسابات) المستخدم الذي لديه حقوق المسؤول المحلي على الأجهزة التي تم التخطيط للنشر الأولي لتطبيقات Kasperskyعليها (أي: توفير حساب المستخدم للمجال الذي لديه حقوق المسؤول المحلي أو وجود حسابات مستخدمين محليين موحدة التي لديها حقوق مسؤول على تلك الأجهزة)
- نوع الاتصال والنطاق الترددي لقنوات الشبكة بين خادم الإدارة وشبكات عميل MSP، وكذلك النطاق الترددي للقنوات داخل تلك الشبكات
- إعدادات الأمان المطبقة على الأجهزة البعيدة عند بداية النشر (مثل استخدام UAC ووضع مشاركة الملفات البسيطة)

تكوين أدوات التثبيت

قبل البدء في نشر تطبيقات Kaspersky على شبكة ما، يجب عليك تحديد إعدادات التثبيت، أي هذه التي يتم تحديدها أثناء تثبيت التطبيق. عند تثبيت عميل الشبكة، يجب عليك تحديد عنوان، واحد على الأقل، للاتصال بخادم الإدارة وإعدادات الوكيل؛ كما يمكن أن تكون بعض الإعدادات المتقدمة مطلوبة. بناءً على طريقة التثبيت التي حددتها، يمكنك تحديد الإعدادات بطرق مختلفة. في الحالات الأكثر بساطة (تثبيت تفاعلي يدوي على جهاز محدد)، يمكن تحديد كل الإعدادات ذات الصلة من خلال واجهة المستخدم الخاصة بالمثبّت، ولذلك، في بعض الحالات، يمكن أيضًا تنفيذ النشر الأولي عن طريق إرسال رابط حزمة توزيع عميل الشبكة إلى المستخدمين إلى جانب الإعدادات (عنوان خادم الإدارة، وما إلى ذلك) الذي يجب على المستخدم إدخاله في واجهة المثبّت.

لا يوصى باستخدام هذه الطريقة لأنها لا تناسب المستخدمين، وتنطوي على مخاطر كبيرة بحدوث الأخطاء عند تحديد الإعدادات يدويًا، ولا يمكن استخدامها أيضًا مع التثبيت الصامت للتطبيقات على مجموعات الأجهزة. بشكل عام، يجب على المسؤول تحديد قيم للإعدادات في الوضع المركزي؛ ويمكن استخدام هذه القيم لاحقًا لإنشاء الحزم المستقلة. الحزم المستقلة هي أرشيفات ذاتية الاستخراج تحتوي على حزم توزيع إلى جانب الإعدادات التي حددها المسؤول. يمكن أن توجد حزم التوزيع المستقلة على الموارد التي تسمح بالتنزيل عن طريق المستخدمين النهائيين (على سبيل المثال، على Kaspersky Security Center Web Server) والتثبيت الصامت على الأجهزة المحددة المتصلة بالشبكة.

حزم التثبيت

الطريقة الأولى والرئيسية لتحديد إعدادات التثبيت الخاصة بالتطبيقات تتميز بأنها متعددة الأغراض وبذلك فهي مناسبة لكل طرق التثبيت، باستخدام كلاً من أدوات Kaspersky Security Center وأغلب أدوات الجهة الخارجية. تتكون هذه الطريقة من إنشاء حزم تثبيت للتطبيقات في Kaspersky Security Center.

يتم إنشاء حزم التثبيت باستخدام الطرق التالية:

- تلقائيًا: من حزم توزيع محددة، على أساس أدوات الوصف المضمنة (ملفات بامتداد kud. والتي تحتوي على قواعد للتثبيت وتحليل النتائج ومعلومات أخرى)
- من الملفات التنفيذية الخاصة بالمثبت أو من المثبتات الموجودة في تنسيق Microsoft Windows Installer (MSI) للتطبيقات القياسية أو المدعومة.

حزم التثبيت التي تم إنشاؤها مرتبة ترتيبًا هرميًا كمجلدات بها مجلدات فرعية وملفات. بالإضافة إلى حزمة التوزيع الأصلية، تحتوي حزمة التثبيت على إعدادات قابلة للتحرير (تتضمن إعدادات المثبت وقواعد معالجة حالات مثل ضرورة إعادة تشغيل نظام التشغيل لإكمال التثبيت) بالإضافة إلى الوحدات النمطية الإضافية الثانوية.

يمكن تحديد قيم إعدادات التثبيت المخصصة لتطبيق محدد سيتم دعمه في واجهة مستخدم وحدة تحكم الإدارة عند إنشاء حزمة تثبيت (يمكن العثور على المزيد من الإعدادات في خصائص حزمة التثبيت التي تم إنشائها بالفعل). عند إجراء تثبيت التطبيقات عن بُعد باستخدام أدوات Kaspersky Security Center tools، يتم تسليم حزم التثبيت إلى الأجهزة الهدف يمكن أن يؤدي تشغيل مثبّت تطبيق ما إلى جعل كل الإعدادات المحددة للمسؤول متوفرة له. عند استخدام أدوات جهة خارجية لتثبيت تطبيقات Kaspersky، يجب عليك التأكد من توفر حزمة التثبيت بالكامل على الجهاز الهدف، أي توفر حزمة التوزيع وإعداداتها. يتم إنشاء حزم التثبيت وتخزينها بواسطة Kaspersky Security Center في مجلد فرعي مخصص في مجلد البيانات المشترك.

لا تقم بتحديد أي من التفاصيل للحسابات المميزة في معلمات حزم التثبيت.

للحصول على إرشادات حول استخدام وسيلة التكوين هذه لتطبيقات Kaspersky قبل نشرها باستخدام أدوات تابعة لجهة خارجية، راجع قسم "النشر باستخدام سياسات المجموعة الخاصة بـ Microsoft Windows".

مباشرةً بعد تثبيت Kaspersky Security Center، يتم إنشاء عدد قليل من حزم التثبيت تلقائيًا؛ والتي تكون جاهزة للتثبيت وتشمل حزم عميل الشبكة وحزم تطبيقات الأمان الخاصة بـ Microsoft Windows.

في بعض الحالات، يتضمن استخدام حزم التثبيت لنشر التطبيقات في شبكة عميل MSP ضرورة إنشاء حزم التثبيت على الخوادم الافتراضية التي تطابق عملاء MSP. يسمح إنشاء حزم التثبيت على الخوادم الافتراضية باستخدام إعدادات التثبيت المختلفة لعملاء MSP المختلفين. في الحالة الأولى، يعد هذا الإجراء نافعًا عند التعامل مع حزم تثبيت شبكة العميل لأن عملاء الشبكة يتم نشرهم في شبكات عملاء MSP المختلفين الذين يستخدمون عناوين مختلفة للاتصال بخادم الإدارة. في الواقع، يحدد عنوان الاتصال الخادم الذي يتصل به عميل الشبكة.

بالإضافة إلى إمكانية إنشاء حزم تثبيت جديدة على أي خادم إدارة افتراضي بشكل مباشر، يكون وضع التشغيل الرئيسي لحزم التثبيت على خوادم الإدارة الافتراضية هو "توزيع" حزم التثبيت من خوادم الإدارة الأساسية إلى خوادم الإدارة الافتراضية. يمكنك توزيع حزم التثبيت المحددة (أو جميع الحزم) إلى خوادم الإدارة الافتراضية المحددة (بما في ذلك جميع الخوادم الموجودة في مجموعة الإدارة المحددة) باستخدام مهمة خادم الإدارة المطابقة. يمكنك أيضًا تحديد قائمة بحزم تثبيت خادم الإدارة الرئيسي عند إنشاء خادم إدارة افتراضي جديد. سيتم توزيع الحزم التي حددتها على الفور إلى خادم الإدارة الافتراضي الذي تم إنشائه حديثًا.

عند توزيع حزمة تثبيت، لا يتم نسخ محتوياتها بالكامل. يقوم مستودع الملفات على أي خادم إدارة افتراضي، الذي يطابق حزمة التثبيت التي يتم توزيعها، فقط بتخزين ملفات الإعدادات الخاصة بالخادم الافتراضي هذا. لا يحدث أي تغيير للجزء الرئيسي من حزمة التثبيت (بما في ذلك حزمة توزيع التطبيق التي يتم تثبيتها)؛ ويتم تخزينه في مستودع خادم الإدارة الرئيسي فقط. ويسمح لك ذلك برفع أداء النظام بدرجة كبيرة وتقليل حجم القرص المطلوب. عند التعامل مع حزم التثبيت التي يتم توزيعها على خوادم الإدارة الافتراضية (أي عند تشغيل مهام التثبيت عن بُعد أو إنشاء حزم تثبيت مستقلة)، يتم "دمج" البيانات من حزمة التثبيت الأصلية بخادم الإدارة الرئيسي مع ملفات الإعدادات، التي تطابق الحزمة التي تم توزيعها على خادم الإدارة الافتراضي.

على الرغم من إمكانية تعيين مفتاح الترخيص لتطبيق ما في خصائص حزمة التثبيت، يُنصح بتجنب طريقة توزيع الترخيص هذه لأن فيها يكون من السهل الحصول على وصول قراءة للملفات الموجودة في الملف عن طريق الخطأ. ينبغي عليك استخدام مفاتيح الترخيص الموزعة تلقائيًا أو مهام تثبيت لمفاتيح الترخيص.

خصائص MSI وملفات التحويل

طريقة أخرى لتكوين تثبيت على النظام الأساسي Windows هي تحديد خصائص MSI وملفات التحويل. يمكن استخدام هذه الطريقة عند تنفيذ التثبيت من خلال أدوات الجهات الخارجية المخصصة لتنسيق المثبتات في Microsoft وعند تنفيذ التثبيت من خلال سياسات مجموعة Windows باستخدام أدوات Microsoft القياسية أو الأدوات الأخرى للجهات الخارجية المصممة للتعامل مع سياسات مجموعة Windows.

النشر باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد.

عند توفر أي أدوات لتثبيت التطبيقات عن بُعد في مؤسسة ما (مثل Microsoft System Center)، فمن الملائم إجراء نشر أولي باستخدام هذه الأدوات.

يجب القيام بالإجراءات التالية:

- تحديد طريقة تكوين التثبيت الأنسب لأداة النشر المستخدمة.
- تحديد آلية المزامنة بين تعديل إعدادات حزم التثبيت (عبر واجهة وحدة تحكم الإدارة) وعمل أدوات الجهة الخارجية المحددة المستخدمة في نشر التطبيقات من بيانات حزمة التثبيت.

معلومات عامة حول مهام التثبيت عن بُعد في Kaspersky Security Center

يوفر Kaspersky Security Center نطاقًا عريضًا من طرق تثبيت التطبيقات عن بُعد، والتي تنفَّذ كمهام تثبيت عن بُعد. يمكنك إنشاء مهمة تثبيت عن بُعد لمجموعة إدارة محددة ولأجهزة محددة أو مجموعة من الأجهزة (يتم عرض تلك المهام في وحدة تحكم الإدارة، في مجلد **المهام**). عند إنشاء مهمة، يمكنك تحديد حزم التثبيت (الخاصة بعميل الشبكة و/ أو تطبيق آخر) التي سيتم تثبيتها في هذه المهمة، بالإضافة إلى تحديد إعدادات خاصة تحدد طريقة التثبيت عن بُعد.

تؤثر مهام مجموعات الإدارة على كلٍ من الأجهزة المضمنة في مجموعة محددة وكل الأجهزة الموجودة في كل المجموعات الفرعية داخل مجموعة الإدارة هذه. تغطي المهمة أجهزة خوادم الإدارة المضمنة في مجموعة ما أو أي من مجموعاتها الفرعية في حالة تمكين الإعداد المقابل في المهمة.

تحدّث المهام الأجهزة المحددة قائمة الأجهزة العميلة عند كل تشغيل وفقًا لمحتويات التحديد عند بدء تشغيل المهمة. إذا احتوي تحديد ما على أجهزة تم توصيلها بخوادم الإدارة الثانوية، ستعمل المهمة على هذه الأجهزة أيضًا.

لضمان نجاح تشغيل مهمة تثبيت عن بُعد على أجهزة متصلة بخوادم الإدارة الثانوية، يجب عليك استخدام مهمة التوزيع في توزيع حزم التثبيت التي استخدمتها المهمة الخاصة بك إلى خوادم الإدارة الثانوية المقابلة مقدمًا.

النشر باستخدام سياسات المجموعة الخاصة بـ Microsoft Windows

من المستحسن إجراء النشر الأولي لعملاء الشبكة عبر سياسات مجموعة Microsoft Windows في حالة الوفاء بالشروط التالية:

- أن يكون هذا الجهاز عضوًا في مجال Active Directory
- يُمنح الوصول إلى وحدة التحكم بالمجال من خلال حقوق المسؤول، مما يسمح لك بإنشاء سياسات مجموعة Active Directory وتعديلها.
- يمكن نقل حزمة التثبيت التي تم تكوينها إلى الشبكة التي تستضيف الأجهزة الهدف المدارة (إلى مجلد مشترك متاح للقراءة بواسطة جميع الأجهزة الهدف).
- يتيح لك نظام النشر الانتظار لإعادة التشغيل الروتيني التالي للأجهزة الهدف قبل بدء نشر عملاء الشبكة عليها (أو يمكنك إجبار تطبيق سياسة مجموعة Windows على هذه الأجهزة.)

يتكون نظام النشر هذا مما يلي:

- توجد حزمة توزيع التطبيق بتنسيق مثبّت Microsoft (حزمة MSI) في مجلد مشترك (هو المجلد الذي تحتوي فيه حسابات LocalSystem الخاصة بالأجهزة الهدف على أذونات قراءة).
- في سياسة مجموعة Active Directory، يتم إنشاء كائن تثبيت لحزمة التوزيع.

- يتم تعيين نطاق التثبيت عن طريق تحديد الوحدة التنظيمية (OU) و/أو مجموعة الأمان التي تحتوي على الأجهزة الهدف.

- في المرة القادمة التي يتم فيها تسجيل دخول جهاز هدف إلى المجال (قبل دخول مستخدمي الجهاز إلى النظام)، يتم التحقق من كل التطبيقات المثبتة بحثًا عن التطبيق المطلوب. في حالة عدم العثور على التطبيق، يتم تنزيل حزمة التوزيع من المورد المحدد في السياسة ثم يتم تثبيتها.

يتميز نظام النشر هذا بأن التطبيقات المعيّنة يتم تثبيتها على الأجهزة الهدف أثناء تحميل نظام التشغيل، أي حتى قبل دخول المستخدم إلى النظام. حتى وإن قام شخص يملك الحقوق الكافية بإزالة التطبيق، فسيتم إعادة تثبيته عند بدء التشغيل التالي لنظام التشغيل. نقطة ضعف نظام النشر هذا هي أن التغييرات التي يقوم بها المسؤول على سياسة المجموعة لن تسري حتى تتم إعادة تشغيل الأجهزة (في حالة عدم تضمين أدوات إضافية).

يمكنك استخدام سياسات المجموعة لتثبيت كلاً من عميل الشبكة والتطبيقات الأخرى إذا كانت المثبتات الخاصة بها بتنسيق مثبّت Windows.

لا يمكن تثبيت عميل الشبكة من حزمة MSI إلا في الوضع الصامت، ولا يتم دعم التثبيت التفاعلي من حزمة MSI.

بالإضافة إلى ذلك، عند تحديد طريقة النشر هذه، يجب عليك أيضًا تقييم الحمل على مورد الملف الذي سيتم نسخ الملفات منه إلى الأجهزة الهدف بعد تطبيق سياسة مجموعة Windows. يتعين عليك أيضًا اختيار طريقة تسليم حزمة التثبيت التي تم تكوينها إلى ذلك المورد، وطريقة مزامنة التغييرات ذات الصلة في إعداداته.

التعامل مع سياسات Microsoft Windows عبر مهمة التثبيت عن بُعد الخاصة بـ Kaspersky Security Center

لا تتوفر طريقة النشر إلا إذا كانت هناك إمكانية للوصول إلى وحدة التحكم بالمجال، والتي تحتوي على الأجهزة الهدف، من خادم الإدارة، بينما يمكن الوصول المجلد المشترك لخادم الإدارة (المجلد الذي يقوم بتخزين حزم التثبيت) للقراءة من الأجهزة الهدف. ونظرًا للأسباب السالف ذكرها، لا يتم عرض طريقة النشر على أنها تنطبق على MSP.

تثبيت التطبيقات بدون مساعدة عبر سياسات Microsoft Windows

يمكن للمسؤول إنشاء كائنات مطلوبة للتثبيت في سياسة مجموعة Windows بشكل مستقل. وفي هذه الحالة، يتعين عليك تحميل الحزم على خادم ملفات مستقل وتزويدها برابط.

سيناريوهات التثبيت التالية ممكنة:

- يقوم المسؤول بإنشاء حزمة تثبيت وإعداد خصائصها في وحدة تحكم الإدارة. وبعدها يقوم المسؤول بنسخ المجلد الفرعي EXEC بكامله الخاص بهذه الحزمة من المجلد المشترك الخاص بـ Kaspersky Security Center إلى مجلد موجود على مورد ملفات محدد خاص بالمؤسسة. يوفر كائن سياسة المجموعة رابط إلى ملف MSI الخاص بهذه الحزمة المخزنة في مجلد فرعي على مورد ملفات مخصص خاص بالمؤسسة.

- يقوم المسؤول بتنزيل حزمة توزيع التطبيق (بما في ذلك الخاصة بعميل الشبكة) من الإنترنت وتحميلها إلى مورد الملفات المخصص الخاص بالمؤسسة. يوفر كائن سياسة المجموعة رابط إلى ملف MSI الخاص بهذه الحزمة المخزنة في مجلد فرعي على مورد ملفات مخصص خاص بالمؤسسة. يتم تحديد إعدادات التثبيت عن طريق تكوين خصائص MSI أو عن طريق تكوين ملفات تحويل MST.

النشر الإجباري عبر مهمة تثبيت عن بُعد من Kaspersky Security Center

لإجراء النشر الأولي لعميل الشبكة أو التطبيقات الأخرى، يمكنك فرض تثبيت حزم التثبيت المحددة باستخدام مهمة التثبيت عن بُعد في Kaspersky Security Center - شريطة أن يكون لكل جهاز حساب (حسابات) مستخدم يتمتع بحقوق المسؤول المحلي.

يمكن تطبيق التثبيت الإجباري أيضًا إذا تعذر الوصول المباشر إلى الأجهزة بواسطة خادم الإدارة: على سبيل المثال، تتواجد الأجهزة في شبكات معزولة أو في شبكة محلية بينما يوجد عنصر خادم الإدارة في منطقة الأجهزة الموصلة مباشرة بالإنترنت.

في حالة النشر الأولي، لن يتم تثبيت عميل الشبكة. لذلك، في إعدادات مهمة التثبيت عن بعد، لا يمكنك تحديد توزيع الملفات المطلوبة لتثبيت التطبيق باستخدام عميل الشبكة. ويمكنك فقط اختيار توزيع الملفات باستخدام موارد نظام التشغيل عبر خادم الإدارة أو نقاط التوزيع.

يجب تشغيل خدمة خادم الإدارة تحت حساب يتمتع بامتيازات إدارية على الأجهزة المستهدفة. وبدلاً من ذلك، يمكنك تحديد حساب لديه حق الوصول إلى مشاركة admin$ في إعدادات مهمة التثبيت عن بُعد.

بشكل افتراضي، تتصل مهمة التثبيت عن بعد بالأجهزة باستخدام بيانات اعتماد الحساب الذي يعمل تحته خادم الإدارة، أي الحساب الخاص بالوصول إلى مشاركة admin$. ويجب عليك تحديد هذا الحساب في إعدادات مهمة التثبيت عن بُعد فقط في حالة عدم تثبيت عميل الشبكة على الأجهزة المستهدفة.
عند إنشاء مهمة التثبيت عن بُعد لتشغيل الأجهزة التي تعمل بنظام التشغيل Linux، يجب عليك دائمًا تحديد حساب لإنشاء اتصال SSH.

يمكنك تحديد أجهزة مستهدفة إما بشكل صريح (باستخدام قائمة) أو عن طريق تحديد مجموعة الإدارة الخاصة بـ Kaspersky Security Center التي ينتمون لها، أو عن طريق إنشاء مجموعة من الأجهزة بالاستناد إلى معيار محدد. يتم تحديد وقت بدء التثبيت بواسطة جدول المهمة. في حالة تمكين إعداد **Run missed tasks** في خصائص المهمة، فيمكن تشغيل المهمة إما فورًا أو بعد تشغيل الأجهزة المستهدفة أو عند نقلها إلى مجموعة الإدارة المستهدفة.

يتألف التثبيت الإجباري من تسليم حزم التثبيت إلى الأجهزة المستهدفة، والنسخ التالي للملفات إلى مورد admin$ على كل جهاز من الأجهزة المستهدفة، والتسجيل عن بُعد لخدمات الدعم على تلك الأجهزة. يتم تنفيذ تسليم حزم التثبيت إلى الأجهزة المستهدفة من خلال ميزة Kaspersky Security Center التي تضمن تفاعل الشبكة. يجب الوفاء بالشروط التالية في هذه الحالة:

- يمكن الوصول إلى الأجهزة المستهدفة من جانب خادم الإدارة أو من جانب نقطة التوزيع.
- يعمل تحليل الاسم للأجهزة الهدف بشكل صحيح على الشبكة.
- تظل المشاركات الإدارية (admin $) ممكّنة على الأجهزة الهدف.
- يتم تشغيل خدمات النظام التالية على الأجهزة المستهدفة:
  - الخادم (LanmanServer)
    بشكل افتراضي، يتم تشغيل هذه الخدمة.
  - مشغل عملية خادم DCOM (DcomLaunch)
  - مُعيّن نقطة نهاية RPC (RpcEptMapper)
  - استدعاء الإجراء عن بعد (RpcSs)
- تم فتح منفذ TCP 445 على الأجهزة المستهدفة لتمكين الوصول عن بعد من خلال أدوات Windows.

يتم استخدام منافذ TCP 139 و UDP 137 و UDP 138 بواسطة البروتوكولات القديمة ولم تعد ضرورية للتطبيقات الحالية.

يجب السماح بمنافذ الوصول الخارجي الديناميكية على جدار الحماية للاتصالات من خادم الإدارة ونقاط التوزيع إلى الأجهزة المستهدفة.

- يُسمح لإعدادات أمان سياسة مجال Active Directory بتوفير تشغيل بروتوكول NTLM أثناء نشر عميل الشبكة.
- يتم تعطيل وضع مشاركة الملفات البسيطة على الأجهزة المستهدفة التي تعمل بنظام التشغيل Microsoft Windows XP.
- على الأجهزة المستهدفة، يتم تعيين نموذج مشاركة الوصول والأمان على كلاسيكي - يتحقق المستخدمون المحليون من هوياتهم بأنفسهم. ولا يمكن بأي حال من الأحوال أن يكون مخصصًا للضيوف فقط - يتم التحقق من صحة المستخدمين المحليين كضيوف.
- يجب أن تكون الأجهزة الهدف أعضاءً في المجال، أو يجب إنشاء حسابات موحدة باستخدام حقوق المسؤول على الأجهزة الهدف مقدمًا.

لنشر عميل الشبكة أو التطبيقات الأخرى بنجاح على جهاز غير منضم إلى Windows Server 2003 أو مجال Active Directory أحدث، يجب عليك تعطيل التحكم في حساب المستخدم (UAC) عن بُعد على هذا الجهاز. ويعد التحكم في حساب المستخدم (UAC) عن بُعد أحد الأسباب التي تمنع الحسابات الإدارية المحلية من الوصول إلى admin$، وهو أمر ضروري للنشر الإجباري لعميل الشبكة أو التطبيقات الأخرى. ولا يؤثر تعطيل التحكم في حساب المستخدم عن بُعد على التحكم في حساب المستخدم المحلي.

أثناء التثبيت على أجهزة جديدة لم يتم تخصيصها بعد إلى أي من مجموعات إدارة Kaspersky Security Center، يمكنك فتح خصائص مهمة التثبيت عن بُعد وتحديد مجموعات الإدارة التي تريد نقل الأجهزة إليها بعد تثبيت عميل الشبكة.

عند إنشاء مهمة جماعية، ضع في اعتبارك أن كل مهمة جماعية تؤثر على كل الأجهزة الموجودة في كل المجموعات المتداخلة ضمن مجموعة محددة. لذلك، يجب عليك تجنب تكرار مهام التثبيت في المجموعات الفرعية.

يعد التثبيت التلقائي طريقة مبسطة لإنشاء مهام التثبيت الإجباري للتطبيقات. ولفعل ذلك، يجب عليك فتح خصائص مجموعة الإدارة، وفتح قائمة حزم التثبيت، ثم تحديد تلك التي يجب تثبيتها على الأجهزة في هذه المجموعة. وكنتيجة لذلك، سيتم تثبيت حزم التثبيت المحددة تلقائيًا على كل الأجهزة في هذه المجموعة وكل مجموعاتها الفرعية. الفاصل الزمني الذي سيتم تثبيت الحزم عبره يعتمد على معدل نقل الشبكة وإجمالي عدد الأجهزة المتصلة بالشبكة.

لتقليل الحمل على خادم الإدارة أثناء تسليم حزم التثبيت إلى الأجهزة المستهدفة، يمكنك تحديد التثبيت عبر نقاط التوزيع في مهمة التثبيت. لاحظ أن طريقة التثبيت هذه تضع حملاً كبيرًا على الأجهزة التي تعمل كنقاط توزيع. ولذلك، يوصى بتحديد الأجهزة التي تلبي متطلبات نقاط التوزيع. وإذا كنت تستخدم نقاط التوزيع، فيجب عليك التأكد من وجودها في كل من الشبكات الفرعية المعزولة التي تستضيف الأجهزة المستهدفة.

قد يكون استخدام نقاط التوزيع كمراكز تثبيت محلية مفيدًا عند القيام بالتثبيت على أجهزة في الشبكات الفرعية التي تتصل بخادم الإدارة عبر قناة منخفضة السعة في حين تتاح قناة أوسع بين الأجهزة في نفس الشبكة الفرعية.

علاوة على ذلك، يجب أن تتجاوز مساحة القرص الخالية في القسم الذي يحتوي على المجلد %ALLUSERSPROFILE%\Application adminkit\KasperskyLab\Data، بعدة مرات، الحجم الإجمالي لحزم توزيع التطبيقات المثبتة.

تشغيل الحزم المستقلة التي أنشأها Kaspersky Security Center

لا يمكن تطبيق الطرق الموضحة أعلاه للنشر الأولي لعميل الشبكة والتطبيقات الأخرى دائمًا بسبب تعذر تحقق كل الشروط القابلة للتطبيق. في مثل هذه الحالات، يمكنك إنشاء ملف تنفيذي مشترك يُسمى حزمة تثبيت مستقلة من خلال Kaspersky Security Center، باستخدام حزمة التثبيت ذات إعدادات التثبيت ذات الصلة التي تم إعدادها بواسطة المسؤول. يمكن نشر حزمة تثبيت مستقلة إما على خادم ويب داخلي (مضمَن في Kaspersky Security Center) إذا كان يُعتبر مقبولاً (الوصول الخارجي إلى خادم الويب الذي تم تكوينه لمستخدمي الجهاز الهدف)، أو على خادم ويب تم نشره حصريًا مضمَن في Kaspersky Security Center Web Console. يمكنك أيضًا نسخ الحزم المستقلة إلى خادم ويب آخر.

يمكنك استخدام Kaspersky Security Center لإرسال رسالة بريد إلكتروني إلى المستخدمين المحددين تحتوي على رابط ملف الحزمة المستقلة على خادم الويب المستخدَم حاليًا، مطالبًا إياهم بتشغيل الملف (إما في الوضع التفاعلي أو باستخدام المفتاح "-s" للتثبيت الصامت). يمكنك إرفاق حزمة تثبيت مستقلة برسالة بريد إلكتروني ثم إرسالها إلى مستخدمي الأجهزة التي لا يتوفر لها وصول إلى خادم الويب. يمكن للمسؤول أيضًا نسخ الحزمة المستقلة إلى جهاز خارجي، وتسليمه إلى جهاز ذي صلة ثم تشغيله فيما بعد.

يمكنك إنشاء حزمة مستقلة من حزمة عميل شبكة أو حزمة تطبيق آخر (على سبيل المثال، تطبيق الأمان) أو كليهما. إذا تم إنشاء حزمة مستقلة من عميل شبكة وتطبيق آخر، يبدأ التثبيت بعميل الشبكة.

عند إنشاء حزمة مستقلة باستخدام عميل الشبكة، يمكنك تحديد مجموعة الإدارة التي سيتم نقل الأجهزة الجديدة إليها (الأجهزة التي لم يتم تخصيصها لأي مجموعات إدارة) عند اكتمال تثبيت عميل الشبكة عليها.

يمكن تشغيل الحزم المستقلة في الوضع التفاعلي (بشكل افتراضي)، وعرض نتائج تثبيت التطبيقات التي تحتوي عليها أو يمكن تشغيلها في الوضع الصامت (عند التشغيل باستخدام المفتاح "-s"). يمكن استخدام الوضع الصامت للتثبيت من البرامج النصية، على سبيل المثال، من البرامج النصية التي تم تكوينها للتشغيل بعد نشر صورة نظام التشغيل. يتم تحديد نتيجة التثبيت في الوضع الصامت عن طريق رمز الإرجاع الخاص بالعملية.

خيارات التثبيت اليدوي للتطبيقات

يمكن للمسؤولين أو المستخدمين ذوي الخبرة تثبيت التطبيقات يدويًا في الوضع التفاعلي. يمكنهم استخدام إما حزم التوزيع الأصلية أو حزم التثبيت التي تم إنشاؤها منها وتخزينها في المجلد المشترك الخاص بـ Kaspersky Security Center. بشكل افتراضي، يتم تشغيل أدوات التثبيت في الوضع التفاعلي وتطالب المستخدمين بكل القيم المطلوبة. ولكن عند تشغيل العملية setup.exe من جذر حزمة تثبيت باستخدام المفتاح "-s"، سيعمل المثبت في الوضع الصامت وبالإعدادات التي تم تحديدها عند تكوين حزمة التثبيت.

عند تشغيل setup.exe من جذر حزمة تثبيت، سيتم نسخ الحزمة أولاً إلى مجلد محلي مؤقت، ثم سيتم تشغيل مثبّت التطبيق من المجلد المحلي.

تثبيت التطبيقات عن بُعد على الأجهزة المثبت عليها عميل الشبكة.

في حالة إن كان عميل شبكة قابل للتشغيل ومتصل بخادم الإدارة الرئيسي (أو متصل بأي من الخوادم التابعة له) مثبتًا على جهاز ما، فيمكنك ترقية عميل الشبكة على هذا الجهاز، بالإضافة إلى تثبيت أي تطبيقات مدعومة أو ترقيتها أو إزالتها من خلال عميل الشبكة.

يمكنك تمكين هذا الخيار عن طريق تحديد خانة اختيار **استخدام عميل الشبكة** في خصائص مهمة التثبيت عن بُعد.

في حالة تحديد خانة الاختيار هذه، سيتم نقل حزم التثبيت التي تم تحديد إعدادات التثبيت بها من قِبل المسؤول إلى الأجهزة الهدف عبر قنوات الاتصال بين عميل الشبكة وخادم الإدارة.

لتحسين التحميل على خادم الإدارة وتقليل الحركة بين خادم الإدارة والأجهزة، من المفيد تعيين نقاط توزيع في كل شبكة عن بُعد أو في كل مجال بث (انظر القسم "حول نقاط التوزيع" و"إنشاء بنية مجموعات الإدارة وتعيين نقاط التوزيع"). في هذه الحالة، يتم توزيع حزم التثبيت وإعدادات المثبت من خادم الإدارة إلى الأجهزة الهدف عبر نقاط التوزيع.

علاوةً على ذلك، يمكنك استخدام نقاط التوزيع لبث تسليم (متعدد الإرسال) لحزم التثبيت، مما يسمح بتقليل حركة مرور الشبكة بشكل كبير عند نشر التطبيقات.

عند نقل حزم التثبيت إلى الأجهزة الهدف عبر قنوات اتصال بين عملاء الشبكة وخادم الإدارة، كل حزم التثبيت التي تم تحضيرها للنقل سيتم تخزينها مؤقتًا في المجلد %ALLUSERSPROFILE\Application Data\KasperskyLab\adminkit\1093\working.\FTServer. عند استخدام حزم تثبيت كبيرة متعددة من أنواع مختلفة وتضمين عدد كبير من نقاط التوزيع، قد يزداد حجم هذا المجلد بشكل كبير.

لا يمكن حذف الملفات من مجلد FTServer يدويًا. عند حذف حزم التثبيت الأصلية، سيتم حذف البيانات المقابلة لها تلقائيًا من المجلد FTServer.

يتم تخزين كل البيانات التي يتم استلامها في جهة نقاط التوزيع في المجلد %ALLUSERSPROFILE\Application Data\KasperskyLab\adminkit\1103\FTClTmp$.

لا يمكن حذف الملفات من المجلد FTClTmp$ يدويًا. عند اكتمال المهام التي تستخدم بيانات من هذا المجلد، سيتم حذف محتويات هذا المجلد تلقائيًا.

ولأن حزم التثبيت يتم توزيعها عبر قنوات اتصال بين خادم الإدارة وعملاء الشبكة من مستودع وسيط بتنسيق محسّن لعمليات النقل عبر الشبكة، فلا يتم السماح بإحداث تغييرات في حزم التثبيت المخزنة في المجلد الأصلي لكل حزمة تثبيت. لن يتم تسجيل هذه التغييرات تلقائيًا بواسطة خادم الإدارة. إذا احتجت لتعديل ملفات حزم التثبيت يدويًا (على الرغم من أنه من المستحسن تجنب هذا السيناريو)، يجب عليك تحرير أيٍ من إعدادات حزمة التثبيت في وحدة تحكم الإدارة. يؤدي تحرير إعدادات حزمة تثبيت في وحدة تحكم الإدارة إلى قيام خادم الإدارة بتحديث صورة الحزمة في ذاكرة التخزين المؤقتة التي تم تحضيرها للنقل إلى الأجهزة الهدف.

إدارة عمليات إعادة تشغيل الجهاز في مهمة التثبيت عن بُعد

غالبًا ما تحتاج الأجهزة لإعادة التشغيل لإكمال تثبيت التطبيقات عن بُعد (بخاصةً في Windows).

في حالة استخدام مهمة التثبيت عن بُعد من Kaspersky Security Center، في معالج المهمة الجديدة أو في نافذة خصائص المهمة التي تم إنشاؤها (قسم **إعادة تشغيل نظام التشغيل**)، يمكنك تحديد الإجراء الذي سيتم اتخاذه عندما يتطلب جهاز Windows إعادة تشغيله:

- **عدم إعادة تشغيل الجهاز**. في هذه الحالة، لن يتم إجراء إعادة تشغيل تلقائي. لإكمال التثبيت، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدويًا أو عبر مهمة إدارة الجهاز). سيتم حفظ المعلومات حول إعادة التشغيل المطلوبة في نتائج المهمة وحالة الجهاز. هذا الخيار مناسب لتثبيت المهام على الخوادم والأجهزة الأخرى حيث يكون التشغيل المتواصل مهمًا.

- **إعادة تشغيل الجهاز**. في هذه الحالة، تتم إعادة تشغيل الجهاز تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال التثبيت. هذا الخيار مفيد لمهام التثبيت على أجهزة تعمل على عمليات إيقاف مؤقتة منتظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

- **مطالبة المستخدم باتخاذ إجراء**. في هذه الحالة، سيتم عرض تذكير إعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدويًا. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفاصل الزمني الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد الخيار **مطالبة المستخدم باتخاذ إجراء** هو الخيار الأكثر ملاءمةً لمحطات العمل حيث يحتاج المستخدمون لإمكانية تحديد الوقت الأكثر ملاءمةً لإعادة التشغيل.

ملاءمة تحديث قواعد البيانات في حزمة تثبيت ما خاصة بتطبيق مكافحة الفيروسات

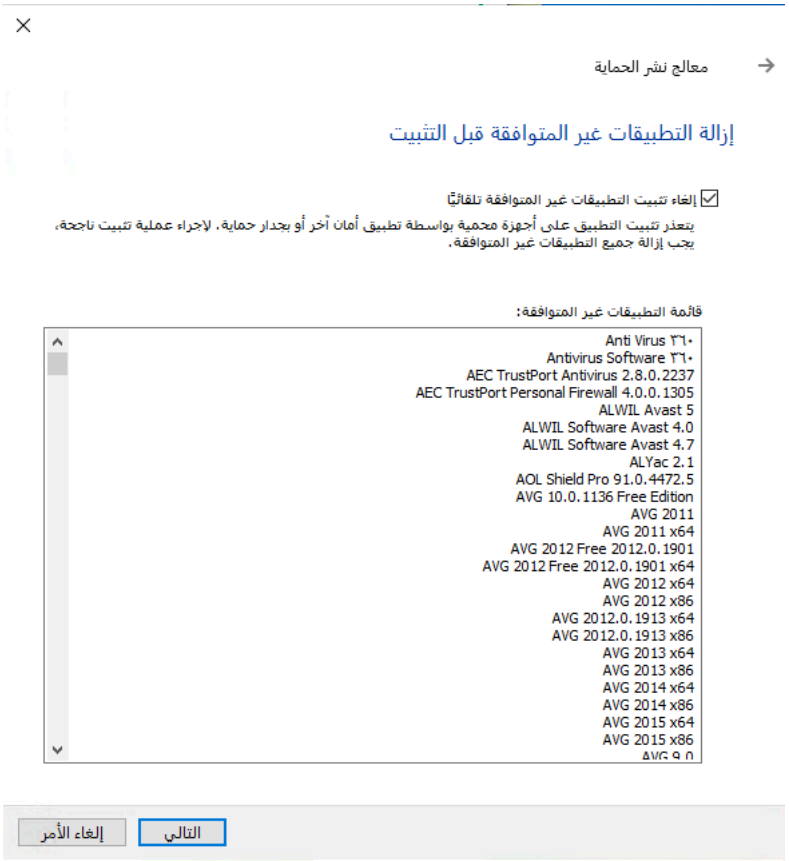
قبل بدء نشر الحماية، يجب عليك أن تضع في اعتبارك إمكانية تحديث قواعد بيانات مكافحة الفيروسات (بما في ذلك الوحدات النمطية للتصحيحات التلقائية) التي يتم شحنها مع حزمة التوزيع الخاصة بتطبيق الأمان. من المفيد تحديث قواعد البيانات الموجودة في حزمة تثبيت التطبيق قبل البدء في النشر (على سبيل المثال، باستخدام الأمر المقابل من قائمة السياق الخاصة بحزم التثبيت المحددة). سيقلل هذا من عدد عمليات إعادة التشغيل المطلوبة لإكمال نشر الحماية على الأجهزة الهدف. إذا كان يتضمن التثبيت عن بُعد حزم التثبيت التي تم نقلها إلى الخوادم الافتراضية من خادم الإدارة الرئيسي، سيتعين عليك فقط تحديث قواعد البيانات في الحزمة الأصلية على خادم الإدارة. وفي هذه الحالة، لا يتعين عليك تحديث قواعد البيانات في الحزم التي تم نقلها على الخوادم الافتراضية.

استبدال تطبيقات الأمان من جهة خارجية غير المتوافقة

قد يتطلب تثبيت تطبيقات الأمان الخاصة بـ Kaspersky عبر Kaspersky Security Center إزالة برنامج الجهة الخارجية غير المتوافق مع التطبيق الذي يتم تثبيته. توجد طريقتان رئيسيتان لإزالة تطبيقات الجهات الخارجية.

الإزالة التلقائية للتطبيقات غير المتوافقة باستخدام المثبّت

عند تشغيل برنامج التثبيت، فإنه يعرض قائمة بالتطبيقات غير المتوافقة مع تطبيق Kaspersky:



قائمة التطبيقات غير المتوافقة التي يتم عرضها في معالج التثبيت عن بعد

يكتشف Kaspersky Security Center البرامج غير المتوافقة. وفقًا لذلك، يمكنك تحديد خانة الاختيار **إلغاء تثبيت التطبيقات غير المتوافقة تلقائيًا** لمتابعة التثبيت. إذا قمت بإلغاء تحديد خانة الاختيار هذه ولم تقم بإلغاء تثبيت البرنامج غير المتوافق، فسيحدث الخطأ ولن يتم تثبيت تطبيق Kaspersky.

يتم دعم الإزالة التلقائية للتطبيقات غير المتوافقة من خلال أنواع مختلفة من التثبيت.

إزالة التطبيقات غير المتوافقة من خلال مهمة محددة

لإزالة تطبيقات غير متوافقة، استخدم المهمة Uninstall application remotely. يجب أن تعمل هذه المهمة على الأجهزة قبل مهمة تثبيت تطبيق الأمان. على سبيل المثال، في مهمة التثبيت، يمكنك تحديد **On completing another task** كنوع الجدول حيث تكون المهمة الأخرى هي Uninstall application remotely.

طريقة إلغاء التثبيت هذه مفيدة عند عدم تمكّن مثبت تطبيق الأمان من إزالة التطبيق غير متوافق بشكل صحيح.

إزالة عميل الشبكة المحمي بكلمة مرور باستخدام موجه الأوامر

لإلغاء تثبيت عميل الشبكة عن بُعد الذي قمت بتعيين كلمة مرور إلغاء التثبيت له، يمكنك استخدام موجه الأوامر.

إذا فقدت أو نسيت كلمة المرور لعميل الشبكة المحمي بكلمة مرور والمثبت على الجهاز الذي لم يعد تحت إدارة Kaspersky Security Center، فلن تتمكن من إزالة عميل الشبكة باستخدام أداة klmover أو أداة Cleaner (cleaner.exe) أو موجه الأوامر. في هذه الحالة، يتعين عليك إعادة تثبيت نظام التشغيل على الجهاز المثبت عليه عميل الشبكة المحمي بكلمة مرور.

لإلغاء تثبيت عميل الشبكة عبر موجه الأوامر:

1. حوّل كلمة مرور إلغاء التثبيت إلى رمز سداسي عشري.

استخدم مورد إنترنت أو بيئة برمجة أو محرر نصوص أو أداة أخرى مناسبة لتحويل كلمة مرورك إلى رمز سداسي عشري.

تأكد من تعيين محدد الإخراج المستخدم لفصل الرمز السداسي العشري الذي تم إنشاؤه إلى أجزاء على `00`. على سبيل المثال، الرمز السداسي `51 79 74 72 65 77` غير صحيح، والرمز السداسي .صحيح `510077006500720074007900`

2. أدخل الأمر التالي في موجه الأوامر، ثم اضغط على **ENTER**:

```
hex code of your uninstallation>=qn KLUNINSTPASSWD/ {<product code>}msiexec.exe /x
<password
```

يمكنك العثور على رمز المنتج الخاص بعميل الشبكة الخاص بك في الجدول أدناه.

رموز منتج عميل الشبكة

الترجمة	رمز المنتج
العربية	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
البلغارية	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
التشيكية	{478A6A0B-D177-4402-B703-808C05C56B13}
الإنجليزية	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
الفرنسية	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
الألمانية	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
المجرية	{8899A4D4-D678-49F8-AD96-0B784F58D355}
الإيطالية	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
اليابانية	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
الكورية	{70812A40-973B-4DA1-96B9-C2011280CD99}
البولندية	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
البرتغالية	{0F05E4E5-5A89-482C-9A62-47CC58643788}
روماني	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
الروسية	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
الصينية المبسطة	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
الإسبانية	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
الإسبانية - المكسيك	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
الصينية التقليدية	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
التركية	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

استخدام الأدوات لتثبيت التطبيقات عن بُعد في Kaspersky Security Center لتشغيل الملفات التنفيذية ذات الصلة على الأجهزة المدارة

باستخدام معالج الحزمة الجديدة، يمكنك تحديد أي ملف تنفيذي وتحديد إعدادات سطر الأوامر الخاص به. للقيام بذلك، يمكنك إضافة إما الملف المحدد نفسه أو المجلد بالكامل المخزّن فيه هذا الملف لحزمة التثبيت. بعد ذلك، يجب عليك إنشاء مهمة التثبيت عن بُعد وتحديد حزمة التثبيت التي تم إنشاؤها.

عندما تكون المهمة قيد التشغيل، سيتم تشغيل الملف التنفيذي المحدد مع الإعدادات المحددة لموجه الأوامر على الأجهزة الهدف.

إذا كنت تستخدم مثبتات بتنسيق Microsoft Windows Installer (MSI)، يقوم Kaspersky Security Center بتحليل نتائج التثبيت بواسطة الأدوات القياسية.

في حالة توفر ترخيص إدارة الثغرات الأمنية والتصحيحات، يستخدم Kaspersky Security Center (عند إنشاء حزمة تثبيت لأي تطبيق مدعوم في بيئة الشركة) أيضًا قواعد التثبيت وتحليل نتائج التثبيت التي توجد في قاعدة البيانات القابلة للتحديث الخاص به.

وإلا، ستنتظر المهمة الافتراضية للملفات التنفيذية اكتمال العملية قيد التشغيل وكل عملياتها الفرعية. بعد اكتمال كل العمليات قيد التشغيل، ستكتمل المهمة بنجاح بعض النظر عن رمز الإرجاع الخاص بالعملية الأولية. لتغيير مثل هذا السلوك في هذه المهمة، قبل إنشاء المهمة، عليك تعديل الملفات ذات التنسيق .kpd يدويًا والتي أنشأها Kaspersky Security Center في مجلد حزمة التثبيت المنشأة حديثًا ومجلداتها الفرعية.

تستخدم ملفات .kpd ترميز ASCII. وتستخدم ملفات .kud ترميز Unicode.

لجعل المهمة لا تنتظر اكتمال العملية قيد التشغيل، قم بتعيين قيم إعداد الانتظار إلى 0 في القسم [SetupProcessResult]:

```
[SetupProcessResult]
0=Wait
```

لجعل المهمة تنتظر اكتمال العملية قيد التشغيل فقط على Windows، وليس اكتمال كل العمليات الفرعية، قم بتعيين قيمة إعداد WaitJob إلى 0 في القسم [SetupProcessResult]، على سبيل المثال:

```
[SetupProcessResult]
0=WaitJob
```

لكي تكتمل المهمة بنجاح أو ترجع خطأً بناءً على رمز الإرجاع لعملية التشغيل، أنشئ الملف التنفيذي .bat الذي يحفظ رمز الخطأ في ملف، على سبيل المثال:

```
setup.log < [ResponseResult] echo
setup.log << 2=echo ResultCode
exit 0
```

ثم قم بتعديل ملفات .kud التي تم إنشاؤها بواسطة Kaspersky Security Center في مجلد حزمة التثبيت التي تم إنشاؤه حديثًا:

```
[SetupMainResult]
setup.log=File
ResponseResult=Section
ResultCode=Value
[SetupMainResult_SuccessCodes]
.Installation completed successfully=0
[SetupMainResult_ErrorCodes]
Installation script error=1
Custom error=2
```

في هذه الحالة، أي رمز غير تلك المدرجة سيؤدي إلى إرجاع خطأ.

لعرض سلسلة تحتوي على تعليق عند اكتمال المهمة بنجاح أو عند حدوث خطأ في نتائج المهمة، قم بإدخال أوصاف مختصرة للأخطاء المقابلة لرموز الإرجاع الخاصة بالعملية في الأقسام [SetupProcessResult_SuccessCodes] و[SetupProcessResult_ErrorCodes] على سبيل المثال:

```
[SetupProcessResult_SuccessCodes]
Installation completed successfully =0
A restart is required to complete the installation=3010
[SetupProcessResult_ErrorCodes]
Installation canceled by the user=1602
Fatal error during installation=1603
```

لاستخدام أدوات Kaspersky Security Center لإدارة إعادة تشغيل الجهاز (إذا كانت إعادة التشغيل مطلوبة لإكمال عملية ما)، قم بإدراج رموز الإرجاع الخاصة بالعملية التي تشير إلى أنه يجب القيام بإعادة التشغيل، في القسم [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
=3010
```

مراقبة النشر

لمراقبة نشر Kaspersky Security Center وللتأكد من أن تطبيق الأمان وعميل الشبكة تم تثبيتهما على الأجهزة المدارة، يجب عليك التحقق من إشارة حركة المرور في القسم **النشر**. توجد إشارة المرور هذه في مساحة عمل عقدة خادم الإدارة في النافذة الرئيسية لوحدة تحكم الإدارة. تعكس إشارة حركة المرور حالة النشر الحالية. يتم عرض عدد الأجهزة المثبّت عليها عميل الشبكة وتطبيقات الأمان بجوار إشارة حركة المرور. عندما تكون أي مهام تثبيت قيد التشغيل، يمكنك مراقبة تقدمها هنا. في حالة حدوث أخطاء في التثبيت، يتم عرض عدد الأخطاء هنا. يمكنك عرض تفاصيل أي خطأ عن طريق النقر فوق الرابط.

يمكنك أيضًا استخدام مخطط النشر في مساحة العمل الخاصة بالمجلد **الأجهزة المُدارة** من علامة التبويب **المجموعات**. يعكس المخطط عملية النشر، ويوضح عدد الأجهزة التي لا تحتوي على عميل شبكة أو تحتوي على عميل شبكة أو تحتوي على عميل شبكة وتطبيق أمان.

للحصول على مزيد من المعلومات حول تقدم النشر (أو عمل مهمة تثبيت محددة) افتح نافذة النتائج الخاصة بمهمة التثبيت عن بُعد ذات الصلة: انقر بزر الماوس الأيمن فوق المهمة وحدد **النتائج** في قائمة السياق. تعرض النافذة قائمتين: العليا تحتوي على حالات المهمة على الأجهزة، بينما تحتوي السفلى على أحداث المهمة على الجهاز المحدد حاليًا في القائمة العليا.

تتم إضافة معلومات حول أخطاء النشر إلى سجل أحداث Kaspersky على خادم الإدارة. تتوفر أيضًا المعلومات حول الأخطاء في تحديد الأحداث المقابل في مجلد **التقارير والإخطارات**، والمجلد الفرعي **الأحداث**.

تكوين أدوات التثبيت

يقدم هذا القسم معلومات حول ملفات أدوات تثبيت Kaspersky Security Center وإعدادات التثبيت، بالإضافة إلى توصيات حول كيفية تثبيت خادم الإدارة وعميل الشبكة في الوضع الصامت.

معلومات عامة

أدوات تثبيت مكونات Kaspersky Security Center 15.1 (خادم الإدارة، وعميل الشبكة، ووحدة تحكم الإدارة) مضمنة في تقنية مثبّت Windows Installer. حزمة MSI هي أساس أداة التثبيت. يتيح تنسيق الحزمة استخدام كل الميزات التي يقدمها Windows Installer: وهي قابلية التوسع وتوفر نظام التصحيح ونظام التحويل والتثبيت المركزي من خلال حلول الجهة الخارجية والتسجيل الشفاف باستخدام نظام التشغيل.

التثبيت في الوضع الصامت (مع ملف الاستجابة)

تحتوي أدوات تثبيت خادم الإدارة وعميل الشبكة على ميزة العمل باستخدام ملف الاستجابة (ss_install.xml)، عندما تكون معلمات التثبيت في الوضع الصامت دون تضمين مشاركة المستخدم. يوجد الملف ss_install.xml في المجلد نفسه الذي توجد فيه الحزمة MSI، ويُستخدم تلقائيًا أثناء التثبيت في الوضع الصامت. يمكنك تمكين وضع التثبيت الصامت باستخدام مفتاح سطر الأوامر "/s".

نظرة عامة على تشغيل مثال كما يلي:

```
setup.exe /s
```

قبل بدء المُثبت في الوضع الصامت، اقرأ اتفاقية ترخيص المستخدم النهائي (EULA). إذا لم تتضمن مجموعة توزيع Kaspersky Security Center ملف TXT يحتوي على نصل اتفاقية ترخيص المستخدم النهائي، يمكنك تنزيل الملف من موقع ويب Kaspersky.

الملف ss_install.xml هو مثيل للتنسيق الداخلي لمعلمات مثبّت Kaspersky Security Center. تحتوي حزمة التوزيع على الملف ss_install.xml مع المعلمات الافتراضية.

يرجى عدم تعديل ملف ss_install.xml يدويًا. يمكن تعديل هذا الملف عبر أدوات Kaspersky Security Center عند تحرير معلمات حزم التثبيت في وحدة تحكم الإدارة.

لتعديل ملف الاستجابة لتثبيت خادم الإدارة:

1. افتح حزمة توزيع Kaspersky Security Center. إذا كنت تستخدم ملف EXE حزمة كاملة، قم بفك ضغطه.

2. من مجلد الخادم، افتح سطر الأوامر، ثم قم بتشغيل الأمر التالي:

```
setup.exe /r ss_install.xml
```

يبدأ مُثبّت Kaspersky Security Center.

3. اتبع خطوات المعالج لتكوين تثبيت Kaspersky Security Center.

عند إكمال المعالج، يتم تعديل ملف الاستجابة تلقائيًا وفقًا للإعدادات الجديدة التي حددتها.

تثبيت عميل الشبكة في الوضع الصامت (دون ملف استجابة)

يمكنك تثبيت عميل الشبكة باستخدام حزمة msi واحدة، مع تحديد قيم خصائص MSI بالطريقة القياسية. يتيح هذا السيناريو تثبيت عميل الشبكة باستخدام سياسات المجموعة.

لا تقم بإعادة تسمية حزمة التثبيت Kaspersky Network Agent.msi. وقد يؤدي إعادة تسمية هذه الحزمة إلى حدوث أخطاء في التثبيت أثناء التحديثات المستقبلية لعميل الشبكة.

لتجنب التعارض بين المعلمات المحددة عبر خصائص MSI والمعلمات المحددة في ملف الاستجابة، يمكنك تعطيل ملف الاستجابة عن طريق تعيين الخاصية 1=DONT_USE_ANSWER_FILE. يقع ملف MSI. في حزمة توزيع Kaspersky Security Center، في المجلد exec\NetAgent\Packages. مثال على تشغيل مثبّت عميل الشبكة باستخدام حزمة msi يتم كما يلي.

يتطلب تثبيت عميل الشبكة في الوضع الصامت قبول بنود اتفاقية ترخيص المستخدم النهائي. استخدم معلمة 1=EULA، إذا قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها.

مثال:
```
1=kscserver.mycompany.com EULA=1 SERVERADDRESS=qn DONT_USE_ANSWER_FILE/ "Kaspersky Network Agent.msi" msiexec /i
```

يمكنك أيضًا تحديد معلمات التثبيت الخاصة بحزمة msi. عن طريق إعداد ملف الاستجابة مقدمًا (الملف ذي الامتداد mst.). يظهر هذا الأمر كما يلي:

مثال:
```
test2.mst;test.mst=qn TRANSFORMS/ "Kaspersky Network Agent.msi" msiexec /i
```

يمكنك تحديد ملفات استجابة متعددة في أمر واحد.

إذا كنت تريد ترقية عميل الشبكة باستخدام Windows Installer، فقم بتشغيل الأمر التالي:

```
nag_inst.log\temp\windows\:vx c*qn /l/ "Kaspersky Network Agent.msi" msiexec /i
vomus /norestart=ALL REINSTALLMODE=REINSTALL
```

تكوين التثبيت الجزئي عبر setup.exe

عند تشغيل تثبيت التطبيقات عبر setup.exe، يمكنك إضافة القيم الخاصة بأي خصائص لـ MSI إلى حزمة MSI.

يظهر هذا الأمر كما يلي:

مثال:

```
"PROPERTYVALUE2=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTY_NAME1"v/
```

معلمات تثبيت خادم الإدارة

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت خادم الإدارة. جميع المعلمات اختيارية، ماعدا الخاصة باتفاقية ترخيص المستخدم النهائي (EULA) و PRIVACYPOLICY (سياسة الخصوصية).

معلمات تثبيت خادم الإدارة في الوضع الصامت

خاصية MSI	الوصف	القيم المتوفرة
EULA	الموافقة على شروط اتفاقية الترخيص (مطلوب)	• 1—لقد قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها. • قيمة أخرى أو بلا قيمة—لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت).
PRIVACYPOLICY	الموافقة على شروط سياسة الخصوصية (مطلوب)	• 1— أنني أدرك وأوافق على التعامل مع بياناتي ونقلها (بما في ذلك، نقلها إلى البلدان الثالثة) كما هو موضح في سياسة الخصوصية. أؤكد على أني قد قرأت سياسة الخصوصية وفهمتها بالكامل. • قيمة أخرى أو بلا قيمة— لا أوافق على بنود سياسة الخصوصية (لا يتم إجراء التثبيت).
INSTALLATIONMODETYPE	نوع تثبيت خادم الإدارة	• قياسي. • مخصص.
INSTALLDIR	مجلد تثبيت التطبيق	قيمة السلسلة.
ADDLOCAL	قائمة بالمكونات التي سيتم تثبيتها (مفصولة بفاصلة)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. قائمة الحد الأدنى من المكونات الكافية للتثبيت الصحيح لخادم الإدارة: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	حجم الشبكة	• NRT_1_100—من 1 إلى 100 جهاز. • NRT_100_1000—من 101 إلى 1000 جهاز. • NRT_GREATER_1000—أكثر من 1000 جهاز.
SRV_ACCOUNT_TYPE	طريقة تحديد المستخدم لتشغيل خدمة خادم الإدارة	• SrvAccountDefault—سيتم إنشاء حساب المستخدم تلقائيًا. • SrvAccountUser—يتم تحديد حساب المستخدم يدويًا.
SERVERACCOUNTNAME	اسم المستخدم للخدمة	قيمة السلسلة.
SERVERACCOUNTPWD	كلمة مرور المستخدم للخدمة	قيمة السلسلة.
DBTYPE	نوع قاعدة البيانات	• MySQL — سيتم استخدام قاعدة بيانات MySQL أو MariaDB • MSSQL— سيتم استخدام قاعدة بيانات Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	الاسم الكامل لخادم MySQL أو MariaDB	قيمة السلسلة.
MYSQLSERVERPORT	رقم منفذ الاتصال بخادم MySQL أو MariaDB	قيمة رقمية.
MYSQLDBNAME	اسم قاعدة بيانات خادم MySQL أو MariaDB	قيمة السلسلة.
MYSQLACCOUNTNAME	اسم المستخدم للاتصال بقاعدة بيانات خادم MySQL أو MariaDB	قيمة السلسلة.

خاصية MSI	الوصف	القيم المتوفرة
MYSQLACCOUNTPWD	كلمة مرور المستخدم للاتصال بقاعدة بيانات خادم MySQL أو MariaDB	قيمة السلسلة.
MSSQLCONNECTIONTYPE	نوع استخدام قاعدة بيانات MSSQL	• InstallMSSEE — التثبيت من حزمة. • ChooseExisting — استخدام الخادم المثبّت.
MSSQLSERVERNAME	الاسم الكامل لمثيل خادم SQL Server	قيمة السلسلة.
MSSQLDBNAME	اسم قاعدة بيانات خادم SQL Server	قيمة السلسلة.
MSSQLAUTHTYPE	طريقة مصادقة الاتصال بخادم SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	اسم المستخدم للاتصال بخادم SQL Server في وضع SQLServer	قيمة السلسلة.
MSSQLACCOUNTPWD	كلمة مرور المستخدم للاتصال بخادم SQL Server في وضع SQLServer	قيمة السلسلة.
CREATE_SHARE_TYPE	طريقة تحديد مجلد مشترك	• إنشاء—إنشاء مجلد مشترك جديد. في هذه الحالة، يجب تحديد الخصائص التالية: • SHARELOCALPATH — المسار إلى مجلد محلي. • SHAREFOLDERNAME — اسم الشبكة لمجلد ما • Null — يجب تحديد خاصية EXISTSHAREFOLDERNAME.
EXISTSHAREFOLDERNAME	المسار الكامل لمجلد مشترك موجود	قيمة السلسلة.
SERVERPORT	رقم المنفذ الخاص بالاتصال بخادم الإدارة	قيمة رقمية.
SERVERSSLPORT	رقم منفذ إنشاء اتصال SSL بخادم الإدارة	قيمة رقمية.
SERVERADDRESS	عنوان خادم الإدارة	قيمة السلسلة.
SERVERCERT2048BITS	حجم المفتاح لشهادة خادم الإدارة (بوحدات البت)	• 1—حجم المفتاح لشهادة خادم الإدارة هو 2048 بت. • 0—حجم المفتاح لشهادة خادم الإدارة هو 1024 بت. • إذا لم يتم تحديد قيمة، فيكون حجم المفتاح لشهادة خادم الإدارة هو 2048 بت.
MOBILESERVERADDRESS	عنوان خادم الإدارة للاتصال بالأجهزة المحمولة، يتم تجاهله إن لم يتم تحديد مكوّن MobileSupport	قيمة السلسلة.

إعدادات تثبيت عميل الشبكة

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت عميل الشبكة. وجميع المعلمات اختيارية باستثناء SERVERADDRESS.

خصائص MSI

خاصية MSI	الوصف	القيم المتوفرة
DONT_USE_ANSWER_FILE	معلمات تثبيت القراءة لملف الاستجابة	• 1 • خالٍ
INSTALLDIR	مجلد التثبيت	
SERVERADDRESS	عنوان خادم الإدارة (مطلوب)	
SERVERPORT	رقم منفذ الاتصال بخادم الإدارة	
SERVERSSLPORT	عدد المنافذ لاتصال SSL	
USESSL	سواء يتم استخدام اتصال SSL أم لا	• 1 • خالٍ
OPENUDPPORT	سواء يتم فتح منفذ UDP أم لا	• 1 • خالٍ
UDPPORT	رقم منفذ UDP	
USEPROXY	سواء يتم استخدام خادم وكيل أم لا	• 1 • خالٍ
PROXYADDRESS	عنوان الوكيل	

خاصية MSI	الوصف	القيم المتوفرة
PROXYPORT	رقم منفذ الاتصال بخادم الإدارة	
PROXYLOGIN	حساب للاتصال بخادم وكيل	
PROXYPASSWORD	كلمة مرور الحساب للاتصال بالخادم الوكيل. لا تقم بتحديد أي من التفاصيل للحسابات المميزة في معلمات حزم التثبيت.	
GATEWAYMODE	وضع استخدام عبّارة الاتصال	• 0 — عدم استخدام بوابة الاتصال • 1 — استخدم عميل الشبكة هذا كبوابة اتصال • 2 — الاتصال بخادم الإدارة باستخدام بوابة الاتصال
GATEWAYADDRESS	عنوان بوابة الاتصال	
CERTSELECTION	طريقة تلقي شهادة	• GetOnFirstConnection — تلقي شهادة من خادم الإدارة. • GetExistent —تحديد شهادة موجودة. إذا تم تحديد هذا الخيار، فيجب تحديد خاصية CERTFILE.
CERTFILE	مسار إلى ملف الشهادة	
VMVDI	تمكين الوضع الديناميكي لـ VDI	• 1 • خالٍ
LAUNCHPROGRAM	ما إذا كان سيتم تشغيل خدمة عميل الشبكة بعد التثبيت	• 1 • خالٍ

البنية التحتية الافتراضية

يدعم Kaspersky Security Center استخدام الأجهزة الظاهرية. يمكنك تثبيت عميل الشبكة وتطبيق الأمان على كل جهاز ظاهري، كما يمكنك حماية الأجهزة الظاهرية على مستوى مراقب الأجهزة الظاهرية. في الحالة الأولى، يمكنك استخدام إما تطبيق أمان قياسي أو Kaspersky Security for Virtualization Light Agent لحماية الأجهزة الظاهرية الخاصة بك. في الحالة الثانية، يمكنك استخدام Kaspersky Security for Virtualization Agentless .

Kaspersky Security Center يدعم عمليات عودة الأجهزة الافتراضية إلى حالتها السابقة.

نصائح لتقليل الحمل على الأجهزة الظاهرية

عند تثبيت عميل شبكة على جهاز ظاهري، ننصحك بالتفكير في تعطيل بعض مزايا Kaspersky Security Center التي يبدو أنها ذات فائدة بسيطة للأجهزة الظاهرية.

عند تثبيت عميل شبكة على جهاز ظاهري أو على قالب مخصص لإنشاء أجهزة ظاهرية، نحن ننصح بالإجراءات التالية:

- إذا كنت تجري تثبيتًا عن بُعد، ففي نافذة الخصائص الخاصة بحزمة تثبيت عميل الشبكة، في قسم **خيارات متقدمة)** حدد خيار **تحسين إعدادات البنية الأساسية لسطح المكتب الافتراضي (VDI)**.
- إذا كنت تُجري تثبيتًا تفاعليًا من خلال معالج، فمن نافذة المعالج، حدد خيار **تحسين إعدادات عميل الشبكة للبنية الأساسية الظاهرية**.

تحديد هذه الخيارات سيبدّل إعدادات عميل الشبكة وبذلك تظل المزايا التالية معطلة بشكل افتراضي (قبل تطبيق سياسة):

- استرجاع معلومات حول البرامج المثبتة
- استرجاع معلومات حول الأجهزة
- استرجاع معلومات حول الثغرات الأمنية المكتشفة
- استرجاع معلومات حول التحديثات المطلوبة

غالبًا ما تكون هذه المزايا غير ضرورية على الأجهزة الظاهرية لأنها تستخدم برنامج موحد وجهاز ظاهري.

يمكن التراجع عن تعطيل المزايا. إذا كانت أي من المزايا المعطلة مطلوبة، يمكنك تمكينها عبر سياسة عميل الشبكة أو عبر الإعدادات المحلية لعميل الشبكة. تتوفر الإعدادات المحلية لعميل الشبكة عبر قائمة السياق الخاصة بالجهاز ذي الصلة في وحدة تحكم الإدارة.

دعم الأجهزة الظاهرية الديناميكية

يدعم Kaspersky Security Center الأجهزة الافتراضية الديناميكية. إذا تم نشر بنية أساسية ظاهرية على شبكة المؤسسة، فيمكن استخدام أجهزة ظاهرية ديناميكية (مؤقتة) في حالات محددة. يتم إنشاء الأجهزة الظاهرية الديناميكية بأسماء فريدة بناءً على القالب الذي تم تحضيره بواسطة المسؤول. يعمل المستخدم على جهاز ظاهري لفترة، ثم بعد أن يتم إيقافه، ستتم إزالة هذا الجهاز الظاهري من البنية الأساسية. إذا تم نشر Kaspersky Security Center على شبكة مؤسسة، فستتم إضافة جهاز ظاهري مثبّت عليه عميل الشبكة إلى قاعدة بيانات خادم الإدارة. بعد إيقاف جهاز ظاهري، يجب حذف الإدخال المقابل أيضًا من قاعدة بيانات خادم الإدارة.

لتفعيل ميزة الحذف التلقائي للإدخالات على الأجهزة الظاهرية، عند تثبيت عميل الشبكة على قالب لأجهزة ظاهرية ديناميكية، حدد خيار **تمكين الوضع الديناميكي لـ VDI**:

- بالنسبة للتثبيت عن بُعد، في نافذة خصائص حزمة تثبيت عميل الشبكة (القسم **خيارات متقدمة**)
- للتثبيت التفاعلي – في معالج تثبيت عميل الشبكة

تجنب تحديد خيار **تمكين الوضع الديناميكي لـ VDI** عند تثبيت عميل الشبكة على الأجهزة الفعلية.

إذا أردت تخزين الأحداث من الأجهزة الظاهرية الديناميكية على خادم الإدارة لبعض الوقت بعد إزالة هذه الأجهزة الظاهرية، ففي نافذة خصائص خادم الإدارة وفي القسم **مستودع الأحداث** حدد خيار **تخزين الأحداث بعد حذف الأجهزة** وحدد الحد الأقصى لمدّة تخزين الأحداث (بالأيام).

لا نوصي بتمكين تشفير محرك الأقراص على الأجهزة الافتراضية الديناميكية.

دعم نسخ الأجهزة الظاهرية

عملية نسخ جهاز ظاهري باستخدام عميل شبكة مثبّت أو إنشاء واحد من قالب باستخدام عميل شبكة مثبّت هي عملية مشابهة لنشر عملاء الشبكة عن طريق التقاط صورة قرص ثابت ونسخها. لذلك، بشكل عام، عند نسخ الأجهزة الافتراضية، تحتاج إلى تنفيذ نفس الإجراءات كما هو الحال عند نشر عميل الشبكة عن طريق نسخ صورة قرص.

ولكن، الحالتان الموضحتان أدناه تعرضان عميل الشبكة، الذي يكتشف النسخ تلقائيًا. بسبب الأسباب الموضحة أعلاه، ليس عليك إجراء العمليات المعقدة الموضحة ضمن "النشر عن طريق التقاط صورة القرص الثابت لجهاز ما ونسخها":

- تم تحديد خيار **تمكين الوضع الديناميكي لـ VDI** عندما تم تثبيت عميل الشبكة—بعد كل إعادة تشغيل لنظام التشغيل، سيتم التعرف على الجهاز الظاهري كجهاز جديد، بغض النظر عما إذا كان تم نسخه أم لا.
- أن يكون واحد من مراقبي الأجهزة الظاهرية التالية قيد الاستخدام VMware™ أو HyperV® أو Xen®: اكتشف عميل الشبكة عملية نسخ للجهاز الظاهري عن طريق معرّفات الأجهزة الظاهرية التي تم تغييرها.

تحليل التغييرات في الأجهزة الظاهرية ليست موثوق بها تمامًا. قبل تطبيق هذه الطريقة بشكل واسع، يجب عليك اختبارها على مجموعة صغيرة من الأجهزة الظاهرية الخاصة بإصدار مراقب الأجهزة الظاهرية المستخدم حاليًا في مؤسستك.

دعم عودة نظام الملفات الخاص بالأجهزة المثبّت عليها عميل الشبكة إلى حالته السابقة

يُعتبر Kaspersky Security Center تطبيقًا موزَّعًا. ستؤدي عودة نظام الملفات إلى الحالة السابقة على جهاز مثبّت عليه عميل الشبكة إلى عدم مزامنة البيانات وعمل Kaspersky Security Center بشكل غير صحيح.

يمكن إرجاع نظام الملفات (أو جزء منه) في الحالات التالية:

- عند نسخ صورة من القرص الثابت.
- عند استعادة حالة الجهاز الظاهري بواسطة البنية الأساسية الظاهرية.
- عند استعادة بيانات من نسخة احتياطية أو نقطة استرداد.

السيناريوهات التي يؤثر فيها برنامج جهة خارجية على الأجهزة المثبّت عليها عميل شبكة على المجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ هي فقط السيناريوهات الحرجة لـ Kaspersky Security Center. لذلك، يجب عليك دائمًا استثناء هذا المجلد من إجراء الاسترجاع، إن أمكن.

ولأن قواعد مكان العمل الخاصة ببعض المؤسسات تعمل على عودة نظام الملفات على الأجهزة إلى حالته السابقة، فقد تمت إضافة دعم عودة نظام الملفات على الأجهزة المثبّت عليها عميل شبكة إلى حالته السابقة إلى Kaspersky Security Center، بدءًا من الإصدار 10 من Maintenance Release 1 (يجب أن يكون خادم الإدارة وعملاء الشبكة من الإصدار 10 من Maintenance Release 1 أو الإصدارات الأحدث). عند اكتشاف ذلك، يتم إعادة توصيل هذه الأجهزة تلقائيًا إلى خادم الإدارة مع تطهير كامل للبيانات وإجراء مزامنة كاملة.

بشكل افتراضي، يتم تمكين دعم اكتشاف عودة نظام الملفات إلى حالته السابقة في Kaspersky Security Center 15.1.

على قدر الإمكان، تجنب إعادة مجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ إلى حالته السابقة على جهاز مثبّت عليه عميل شبكة، لأن إعادة المزامنة الكاملة للبيانات تتطلب كمية كبيرة من المصادر.

عودة حالة النظام إلى حالتها السابقة غير مسموح بها إطلاقًا على جهاز مثبّت عليه خادم الإدارة. كما لا تُستخدم عودة قاعدة البيانات إلى حالتها السابقة بواسطة خادم الإدارة.

يمكنك استعادة حالة خادم الإدارة من النسخ الاحتياطي عن طريق أداة klbackup المساعدة القياسية فقط.

حول ملفات التعريف الخاصة باتصال المستخدمين المتواجدين خارج المكتب

قد يحتاج مستخدمو الكمبيوتر المحمول خارج المكتب (يُشار إليهم فيما بعد باسم "الأجهزة") إلى تغيير طريقة الاتصال بخادم الإدارة أو التبديل بين خوادم الإدارة بناءً على الموقع الحالي للجهاز على شبكة المؤسسة.

إن ملفات تعريف الاتصال مدعومة فقط للأجهزة التي تعمل بنظام Windows و macOS.

استخدام عناوين مختلفة لخادم إدارة واحد

الأجهزة المثبت عليها عميل الشبكة يمكنها الاتصال بخادم الإدارة إما من إنترانت المؤسسة أو من الإنترنت. قد يتطلب هذا الموقف من عميل الشبكة استخدام عناوين مختلفة للاتصال بخادم الإدارة: عنوان خادم الإدارة الخارجي للاتصال بالإنترنت وعنوان خادم الإدارة الداخلي للاتصال بالشبكة الداخلية.

للقيام بذلك، يجب عليك إضافة ملف تعريف (للاتصال بخادم الإدارة من الإنترنت) إلى سياسة عميل الشبكة. أضف ملف التعريف في خصائص السياسة (قسم **الاتصال**، القسم الفرعي **ملفات تعريف الاتصال**). في نافذة إنشاء ملف التعريف، يجب عليك تعطيل خيار **الاستخدام لاستلام التحديثات فقط**، وتحديد خيار **مزامنة إعدادات الاتصال مع إعدادات خادم الإدارة المحددة في ملف التعريف هذا**. إذا كنت تستخدم بوابة اتصال للوصول إلى خادم الإدارة (على سبيل المثال تكوين Kaspersky Security Center كما هو موضح في الوصول إلى الإنترنت: عميل الشبكة كبوابة اتصال في منطقة الأجهزة الموصلة مباشرة بالإنترنت)، فيجب عيك تحديد عنوان بوابة الاتصال في الحقل المقابل لملف تعريف الاتصال.

التبديل بين خوادم الإدارة بناءً على الشبكة الحالية

إذا كان للمؤسسة مكاتب متعددة بها خوادم إدارة مختلفة وتنتقل بعض الأجهزة المثبّت عليها عميل الشبكة فيما بينها، فأنت تحتاج لتوصيل عميل الشبكة بخادم الإدارة الخاص بالشبكة المحلية في المكتب الذي يوجد به الجهاز حاليًا.

في هذه الحالة، يجب إنشاء ملف تعريف للاتصال بخادم الإدارة في خصائص سياسة عميل الشبكة لكل مكتب من المكاتب، ماعدا المكتب الرئيسي الذي يوجد به خادم الإدارة الرئيسي. يجب عليك تحديد عناوين خوادم الإدارة في ملفات تعريف الاتصال وتمكين أو تعطيل خيار **الاستخدام لاستلام التحديثات فقط**:

- حدد الخيار إذا كنت تريد مزامنة عميل الشبكة باستخدام خادم الإدارة الرئيسي، بينما تستخدم الخادم المحلي لتنزيل التحديثات فقط.
- قم تعطيل هذا الخيار إذا كان يلزم إدارة عميل الشبكة بالكامل بواسطة خادم الإدارة المحلي.

بعد ذلك، يجب عليك إعداد شروط التحويل إلى ملفات التعريف التي تم إنشاؤها حديثًا: على الأقل شرط واحد لكل مكتب من المكاتب، ما عدا المكتب الرئيسي. يتكون غرض كل شرط من الشروط من الكشف عن العناصر الخاصة لبيئة شبكة مكتب ما. إذا تحقق شرط ما، يتم تنشيط ملف التعريف المقابل له. إن لم يتحقق شرط من الشروط، يتم تبديل عميل الشبكة إلى خادم الإدارة الرئيسي.

نشر ميزة إدارة الجهاز المحمول

يوفر هذا القسم معلومات حول النشر الأولي لميزة إدارة الأجهزة المحمولة.

توصيل أجهزة KES بخادم الإدارة

بالاعتماد على الطريقة المستخدمة لاتصال الأجهزة بخادم الإدارة، يتوفر نظاما نشر لـ Kaspersky Device Management for iOS لأجهزة KES:

- نظام نشر باستخدام الاتصال المباشر للأجهزة بخادم الإدارة
- مخطط النشر الذي يتضمن الخادم الوكيل العكسي الذي يدعم تفويض Kerberos المقيد

الاتصال المباشر للأجهزة بخادم الإدارة

يمكن لأجهزة KES الاتصال مباشرةً بمنفذ 13292 الخاص بخادم الإدارة.

بناءً على الطريقة المستخدمة للمصادقة، يتوفر خياران لاتصال أجهزة KES بخادم الإدارة:

- توصيل الأجهزة باستخدام شهادة مستخدم
- توصيل الأجهزة بدون استخدام شهادة مستخدم

توصيل جهاز باستخدام شهادة مستخدم

عند توصيل جهاز باستخدام شهادة مستخدم، يقترن الجهاز بحساب المستخدم الذي تم إسناد الشهادة المقابلة له عبر أدوات خادم الإدارة.

في هذه الحالة، سيتم استخدام مصادقة SSL ثنائية الاتجاه (مصادقة تبادلية). ستتم مصادقة كلاً من خادم الإدارة والجهاز باستخدام الشهادات.

توصيل جهاز بدون استخدام شهادة مستخدم

عند توصيل جهاز بدون شهادة مستخدم، لن يقترن هذا الجهاز بأي من حسابات المستخدم على خادم الإدارة. ولكن، عندما يتلقى الجهاز أي شهادة، سيقترن الجهاز بالمستخدم الذي تم إسناد الشهادة المقابلة له عبر أدوات خادم الإدارة.

عند توصل ذلك الجهاز بخادم الإدارة، سيتم تطبيق مصادقة SSL أحادية الاتجاه، وهذا يعني مصادقة خادم الإدارة فقط باستخدام الشهادة. بعد استرداد الجهاز شهادة المستخدم، سيتغير نوع المصادقة إلى مصادقة SSL ثنائية الاتجاه (مصادقة SSL ثنائية الاتجاه، مصادقة تبادلية).

نظام توصيل أجهزة KES بالخادم الذي يتضمن تفويض Kerberos المقيّد (KCD)

يعمل نظام توصيل أجهزة KES بخادم الإدارة الذي يتضمن تفويض Kerberos المقيّد (KCD) على ما يلي:

- التكامل مع خادم وكيل عكسي يدعم KCD.
- استخدام تفويض Kerberos المقيّد (يُشار إليه فيما بعد باسم KCD) لمصادقة الأجهزة المحمولة.
- التكامل مع البنية الأساسية للمفتاح العام (يُشار إليها فيما بعد باسم PKI) لتطبيق شهادات المستخدم.

عند استخدام نظام الاتصال هذا، الرجاء ملاحظة ما يلي:

- يجب أن يكون نوع اتصال أجهزة KES بالخادم الوكيل العكسي "مصادقة SSL ثنائية الاتجاه"، أي أن الجهاز يجب أن يتصل بالخادم الوكيل العكسي عبر شهادة المستخدم الشخصية الخاصة به. للقيام بذلك، أنت في حاجة لدمج شهادة المستخدم في حزمة تثبيت Kaspersky Endpoint Security for Android، التي تم تثبيتها على الجهاز. يجب إنشاء حزمة KES هذه بواسطة خادم الإدارة خصيصًا لهذا الجهاز (المستخدم).
- يجب عليك تحديد الشهادة الخاصة (المخصصة) بدلاً من شهادة الخادم الافتراضية لبروتوكول الجهاز المحمول:

  1. في نافذة خصائص خادم الإدارة، في قسم **الإعدادات**، حدد خانة الاختيار **فتح منفذ للأجهزة المحمولة** ثم حدد **إضافة شهادة** من القائمة المنسدلة.
  2. في النافذة التي تفتح، حدد الشهادة ذاتها التي تم تعيينها على الخادم الوكيل العكسي عند نشر نقطة الوصول إلى بروتوكول الجهاز المحمول على خادم الإدارة.

- يجب إصدار شهادات المستخدم لأجهزة KES بواسطة هيئة إصدار الشهادات (CA) الخاصة بالمجال. ضع في اعتبارك في حالة احتواء المجال على هيئات إصدار شهادات جذر متعددة، يجب إصدار شهادات المستخدم بواسطة هيئة إصدار الشهادات (CA)، التي تم تعيينها في النشر على الخادم الوكيل العكسي.

  يمكنك التأكد أن شهادة المستخدم متوافقة مع المتطلب الموضح أعلاه عن طريق استخدام طريقة من الطرق التالية:

  - حدد شهادة المستخدم الخاصة في معالج الحزمة الجديدة وفي معالج تثبيت الشهادة.
  - دمج خادم الإدارة مع البنية الأساسية للمفتاح العام (PKI) وتحديد الإعداد المقابل في قواعد إصدار الشهادات:

    1. في شجرة وحدة التحكم، قم بتوسيع المجلد **إدارة الجهاز المحمول**، وحدد المجلد الفرعي **الشهادات**.
    2. في مساحة عمل المجلد **الشهادات**، انقر فوق الزر **تكوين قواعد إصدار الشهادات** لفتح النافذة **قواعد إصدار الشهادات**.
    3. في القسم **التكامل مع PKI**، قم بتكوين التكامل مع البنية الأساسية للمفتاح العام (PKI).
    4. في القسم **إصدار شهادات المحمول**، حدد مصدر الشهادات.

يوجد أدناه مثال لإعداد تفويض Kerberos المقيّد (KCD) مع الافتراضيات التالية:

- يتم تعيين نقطة الوصول إلى بروتوكول الجهاز المحمول على خادم الإدارة إلى المنفذ 13292.
- اسم الجهاز المزود بالخادم الوكيل العكسي هو firewall.mydom.local.
- اسم الجهاز المثبّت عليه خادم الإدارة هو ksc.mydom.local.
- اسم النشر الخارجي لنقطة الوصول إلى بروتوكول الجهاز المحمول هو kes4mob.mydom.global.

حساب المجال لخادم الإدارة

يجب عليك إنشاء حساب مجال (على سبيل المثال KSCMobileSrvcUsr) الذي ستعمل خدمة خادم الإدارة بموجبه. يمكنك تحديد حساب لخادم الإدارة عند تثبيت خادم الإدارة أو عبر الأداة المساعدة klsrvswch. توجد الأداة المساعدة klsrvswch في مجلد التثبيت الخاص بخادم الإدارة. مسار التثبيت الافتراضي: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

يجب تحديد حساب مجال للأسباب التالية:

- الميزة إدارة أجهزة KES هي جزء متكامل من خادم الإدارة.
- لضمان العمل الصحيح لتفويض Kerberos المقيّد (KCD)، يجب أن تعمل جهة الاستلام (أي خادم الإدارة) أسفل حساب مجال.

الاسم الأساسي للخدمة لـ http/kes4mob.mydom.local

في المجال، أسفل حساب KSCMobileSrvcUsr، قم بإضافة SPN لنشر خدمة بروتوكول الجهاز المحمول على المنفذ 13292 الخاص بالجهاز المثبّت عليه خادم الإدارة. بالنسبة لجهاز kes4mob.mydom.local المثبّت عليه خادم الإدارة، سيظهر الاسم كمل يلي:

```
KSCMobileSrvcUsr\13292 mydom:setspn -a http/kes4mob.mydom.local
```

تكوين خصائص المجال للجهاز باستخدام الخادم الوكيل العكسي (firewall.mydom.local)

لتفويض حركة المرور، يجب عليك اعتماد الجهاز الذي يحتوي على الخادم الوكيل العكسي (firewall.mydom.local) إلى الخدمة المحددة بواسطة SPN (13292:http/kes4mob.mydom.local).

لاعتماد الخدمة التي تحتوي على الخادم الوكيل العكسي إلى الخدمة المحددة بواسطة SPN (13292:http/kes4mob.mydom.local)، يجب أن ينفذ المسؤول الإجراءات التالية:

1. في أداة الإضافة في Microsoft Management Console التي تحمل الاسم "مستخدمو وأجهزة كمبيوتر Active Directory"، حدد الجهاز المثبّت عليه الخادم الوكيل العكسي (firewall.mydom.local).
2. في خصائص الجهاز، من علامة التبويب **التفويض**، قم بتعيين مؤشر التبديل **اعتماد هذا الكمبيوتر للتفويض إلى الخدمة المحددة فقط** إلى **استخدام أي بروتوكول مصادقة**.
3. في قائمة **الخدمات التي يمكن لهذا الجهاز تقديم بيانات الاعتماد المفوضة لها**، قم بإضافة 13292:SPN http/kes4mob.mydom.local.

شهادة خاصة (مخصصة) لعملية النشر (kes4mob.mydom.global)

لنشر بروتوكول الجهاز المحمول الخاص بخدام الإدارة، يجب عليك إصدار شهادة خاصة (مخصصة) لـ FQDN kes4mob.mydom.global وحدد شهادة الخادم الافتراضية في إعدادات بروتوكول الجهاز المحمول الخاص بخادم الإدارة في وحدة تحكم الإدارة. للقيام بذلك، في نافذة الخصائص الخاصة بخادم الإدارة، في قسم **الإعدادات**، حدد خانة الاختيار **فتح منفذ للأجهزة المحمولة** ثم حدد **إضافة شهادة** من القائمة المنسدلة.

الرجاء ملاحظة أن حاوية شهادة الخادم (ملف امتداده p12 أو pfx) يجب أن يحتوي أيضًا على سلسلة الشهادات الجذر (المفاتيح العامة).

تكوين النشر على الخادم الوكيل العكسي

على الخادم الوكيل العكسي، بالنسبة لحركة المرور التي تنتقل من جهة الجهاز المحمول إلى المنفذ 13292 الخاص بـ kes4mob.mydom.global، يجب عليك تكوين KCD على SPN (13292:http/kes4mob.mydom.local)، باستخدام شهادة الخادم التي تم إصدارها لـ FQND kes4mob.mydom.global. الرجاء ملاحظة أن النشر ونقطة الوصول المنشورة (المنفذ 13292 الخاص بخادم الإدارة) يجب أن تتشارك شهادة الخادم نفسها.

استخدام مراسلة Firebase Cloud

لضمان تسليم الأوامر إلى أجهزة KES التي تتم إدارتها بواسطة نظام تشغيل Android في الوقت المناسب، يستخدم Kaspersky Security Center آلية إرسال الإخطارات. يتم تبادل الإخطارات الفورية بين أجهزة KES وخادم الإدارة من خلال Firebase Cloud Messaging (المشار إليه فيما يلي باسم FCM). في وحدة تحكم إدارة Kaspersky Security Center، يمكنك تحديد إعدادات Firebase Cloud Messaging لتوصيل أجهزة KES بالخدمة.

لاستعادة إعدادات مراسلة Google Firebase Cloud، يجب أن تمتلك حساب.

لتمكين استخدام مراسلة FCM:

1. في وحدة تحكم الإدارة، حدد العقدة **إدارة الجهاز المحمول**، والمجلد **الأجهزة المحمولة**.
2. من قائمة سياق المجلد **الأجهزة المحمولة**، حدد **خصائص**.
3. في خصائص المجلد، حدد القسم **إعدادات Firebase Cloud Messaging**.
4. في الحقل **رقم مشروع Firebase**، حدد معرف مرسل FCM.
5. في الحقل **ملف المفتاح الخاص (بتنسيق JSON)**، حدد ملف المفتاح الخاص.

في المزامنة التالية مع خادم الإدارة، ستتصل أجهزة KES التي تمت إدارتها بواسطة أنظمة التشغيل Android بمراسلة Firebase Cloud.

يمكنك تحرير إعدادات Firebase Cloud Messaging من خلال النقر فوق الزر **إعادة تعيين الإعدادات**.

عند التبديل إلى مشروع Firebase مختلف، فإنك تحتاج إلى الانتظار لمدة 10 دقائق لاستئناف FCM.

تعمل خدمة FCM في نطاق العناوين التالي:

- من جهة جهاز KES، مطلوب الوصول إلى المنافذ: 443 (HTTPS) و5228 (HTTPS) و5229 (HTTPS) و5230 (HTTPS) الخاصة بالعناوين التالية:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - كل عناوين IP المُدرجة في ASN الخاص بـ Google لـ 15169
- من جهة خادم الإدارة، مطلوب الوصول إلى المنفذ 443 (HTTPS) الخاص بالعناوين التالية:
  - fcm.googleapis.com
  - كل عناوين IP المُدرجة في ASN الخاص بـ Google لـ 15169

إذا تم تحديد إعدادات الخادم الوكيل (**متقدم / تكوين الاتصال بالإنترنت**) في خصائص خادم الإدارة في وحدة تحكم الإدارة، فسيتم استخدامها للتفاعل مع FCM.

تكوين FCM: الحصول على معرف المرسل وملف المفتاح الخاص

لتكوين FCM:

1. التسجيل على بوابة Google.
2. انتقل إلى وحدة تحكم Firebase.
3. قم بأحد الإجراءات التالية:
   - لإنشاء مشروع جديد، انقر فوق **إنشاء مشروع** واتبع التعليمات التي تظهر على الشاشة.
   - افتح مشروعًا موجودًا.
4. انقر على أيقونة الترس واختر **إعدادات المشروع**.
   تفتح النافذة **إعدادات المشروع**.
5. حدد علامة التبويب **المراسلة السحابية**.
6. استرجع معرف المرسل ذي الصلة من الحقل **معرف المرسل** في القسم **Firebase Cloud Messaging API (V1)**.
7. حدد علامة التبويب **حسابات الخدمة** وانقر فوق **إنشاء مفتاح خاص جديد**.
8. في النافذة التي تفتح، انقر فوق **إنشاء مفتاح** لإنشاء ملف مفتاح خاص وتنزيله.

تم تكوين Firebase Cloud Messaging الآن.

التكامل مع البنية الأساسية للمفاتيح العامة

التكامل مع البنية الأساسية للمفتاح العام (يُشار إليه فيما بعد باسم PKI) يُقصد به بشكل أساسي تسهيل إصدار شهادات المستخدم الخاصة بالمجال بواسطة خادم الإدارة.

يمكن للمسؤول تعيين شهادة مجال لمستخدم ما في وحدة تحكم الإدارة. يمكن القيام بهذا باستخدام واحدة من الطرق التالية:

- قم بتعيين شهادة خاصة (مخصصة) للمستخدم من ملف في معالج تثبيت الشهادة.
- القيام بالتكامل مع PKI وتعيين PKI للعمل كمصدر للشهادات لنوع محدد من الشهادات أو لكل أنواع الشهادات.

تتوفر إعدادات التكامل مع PKI في مساحة عمل المجلد **إدارة الجهاز المحمول / الشهادات** من خلال النقر فوق الرابط **التكامل مع البنية الأساسية للمفتاح العام**.

المبدأ العام للتكامل مع PKI لإصدار شهادات المستخدم الخاصة بالمجال

في وحدة تحكم الإدارة، انقر فوق الرابط **التكامل مع البنية الأساسية للمفتاح العام** في مساحة عمل المجلد **إدارة الجهاز المحمول / الشهادات** لتحديد حساب المجال الذي سيُستخدم بواسطة خادم الإدارة لإصدار شهادات عميل المجال عبر هيئة إصدار الشهادات الخاصة بالمجال (يُشار إليه فيما بعد باسم الحساب الذي يتم أسفله إجراء التكامل مع PKI).

الرجاء ملاحظة ما يلي:

- تقدم لك إعدادات التكامل مع PKI إمكانية تحديد القالب الافتراضي لكل أنواع الشهادات. لاحظ أن قواعد إصدار الشهادات (المتوفرة في مساحة عمل المجلد **إدارة الجهاز المحمول / الشهادات** عن طريق النقر فوق الزر **تكوين قواعد إصدار الشهادات**) تتيح لك تحديد قالب فردي لكل نوع من أنواع الشهادات.
- يجب تثبيت شهادة وكيل تسجيل (EA) خاصة على الجهاز المثبت عليه خادم الإدارة، في مستودع الشهادات الخاص بالحساب الذي سيتم التكامل مع PKI أسفله. يتم إصدار شهادة عميل التسجيل (EA) بواسطة مسؤول CA (هيئة إصدار الشهادات) الخاصة بالمجال.

يجب أن يفي الحساب الذي سيتم التكامل مع PKI أسفله بالمعايير التالية:

- أن يكون مستخدم مجال.
- أن يكون مسؤول محلي للجهاز المثبّت عليه خادم الإدارة الذي يتم بدء التكامل مع PKI منه.
- أن يملك حق تسجيل الدخول كخدمة.
- يجب أن يعمل الجهاز المثبّت عليه خادم الإدارة مرة واحدة على الأقل أسفل هذا الحساب لإنشاء ملف تعريف مستخدم دائم.

Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (يُشار إليه فيما بعد بخادم الويب) هو مكوّن من مكونات Kaspersky Security Center. تم تصميم خادم الويب لنشر حزم التثبيت المستقلة وحزم التثبيت المستقلة للأجهزة المحمولة والملفات من المجلد المشترك.

يتم نشر حزم التثبيت التي تم إنشاؤها على خادم الويب تلقائيًا ثم تتم إزالتها بعد التنزيل الأول. ويمكن للمسؤول إرسال الرابط الجديد إلى المستخدم بأي طريقة مناسبة: على سبيل المثال عبر البريد الإلكتروني.

عن طريق النقر على الرابط، يمكن للمستخدم تنزيل المعلومات المطلوبة على الجهاز المحمول.

إعدادات خادم الويب

إذا كان ضبط خادم الويب مطلوبًا، فتتيح لك خصائصه تغيير المنافذ لـ HTTP (8060) وHTTPS (8061). بالإضافة إلى تغيير المنافذ، يمكنك استبدال شهادة الخادم لـ HTTPS وتغير FQDN الخاص بخادم الويب الخاص بـ HTTP.

عمل روتيني آخر

يوفر هذا القسم توصيات حول العمل الروتيني باستخدام Kaspersky Security Center.

مراقبة إشارات المرور والأحداث المسجلة في وحدة تحكم الإدارة

تتيح لك وحدة تحكم الإدارة التقييم السريع للحالة الحالية لـ Kaspersky Security Center والأجهزة المدارة عن طريق التحقق من إشارات حركة المرور. يتم عرض إشارات حركة المرور في مساحة العمل لعقدة **خادم الإدارة**، في علامة التبويب **المراقبة**. توفر علامة التبويب ستة لوحات معلومات مع إشارات حركة المرور والأحداث المسجلة. إشارة حركة المرور هي شريط عمودي ملون في الجزء الأيسر من اللوحة. تتوافق كل لوحة بها إشارات حركة المرور مع نطاق وظيفي محدد لـ Kaspersky Security Center (انظر الجدول أدناه).

النطاقات المغطاة بإشارات حركة المرور في وحدة تحكم الإدارة

اسم اللوحة	نطاق إشارة المرور
النشر	تثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة في شبكة مؤسسة
نظام الإدارة	بنية مجموعات الإدارة. فحص الشبكة. قواعد نقل الجهاز
إعدادات الحماية	وظائف تطبيق الأمان: حالة الحماية، فحص البرامج الضارة
تحديث	التحديثات والتصحيحات
المراقبة	حالة الحماية
خادم الإدارة	مزايا وخصائص خادم الإدارة

قد تكون كل إشارة حركة مرور أي من هذه الألوان الخمسة (انظر الجدول الموجود أدناه). يعتمد لون إشارة حركة المرور على الحالة الحالية لـ Kaspersky Security Center وعلى الأحداث التي تم الدخول إليها.

الرموز اللونية لإشارات حركة المرور

الحالة	لون إشارة حركة المرور	معنى لون إشارة حركة المرور
معلوماتي	أخضر	تدخل المسؤول غير مطلوب.
تحذير	أصفر	تدخل المسؤول مطلوب.
حرج	أحمر	تمت مصادفة مشكلات خطيرة. تدخل المسؤول مطلوب لحلها.
معلوماتي	أزرق فاتح	الأحداث التي تم الدخول إليها لا تتعلق بالتهديدات المحتملة أو الفعلية للأمان الأجهزة المدارة.
معلوماتي	رمادي	تفاصيل الأحداث غير متوفرة أو لم يتم استردادها بعد.

هدف المسؤول هو الإبقاء على إشارات حركة مرور في جميع أجزاء المعلومات على علامة التبويب **المراقبة** باللون الأخضر.

تعرض لوحات المعلومات أيضًا الأحداث المسجلة التي تؤثر على إشارات حركة المرور وحالة Kaspersky Security Center (انظر الجدول أدناه).

الاسم والوصف وألوان إشارات حرمة المرور للأحداث المسجلة

لون إشارة حركة المرور	اسم العرض لنوع الحدث	نوع الحدث	الوصف
أحمر	**انتهت صلاحية الترخيص على 1% جهاز (أجهزة)**	IDS_AK_STATUS_LIC_EXPAIRED	تقع الأحداث من هذا النوع عندما يقترب انتهاء صلاحية الترخيص التجاري. يتحقق Kaspersky Security Center مرة واحدة يوميًا مما إذا كانت صلاحية الترخيص قد انتهت على الأجهزة. عند انتهاء صلاحية الترخيص التجاري، يوفر Kaspersky Security Center الوظائف الأساسية فقط. لمتابعة استخدام Kaspersky Security Center، يرجى تجديد ترخيصك التجاري.
أحمر	**تطبيق الأمان لا يعمل على: 1% جهاز (أجهزة)**	IDS_AK_STATUS_AV_NOT_RUNNING	تقع الأحداث من هذا النوع عندما لا يكون تطبيق الأمان المُثبت على الجهاز قيد التشغيل. تأكد من تشغيل Kaspersky Endpoint Security على الجهاز.
أحمر	**الحماية مُعطَّلة على: 1% جهاز (أجهزة)**	IDS_AK_STATUS_RTP_NOT_RUNNING	تقع الأحداث من هذا النوع عندما يتم تعطيل تطبيق الأمان على الجهاز لفترة أطول من الفترة الزمنية المحددة. تحقق من الحالة الحالية للحماية في الوقت الحقيقي على الجهاز وتأكد من تمكين جميع مكونات الحماية التي تحتاجها.
أحمر	**تم اكتشاف ثغرات أمنية في البرنامج على الأجهزة**	IDS_AK_STATUS_VULNERABILITIES_FOUND	تقع الأحداث من هذا النوع عندما تكتشف مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة ثغرات أمنية بمستوى الخطورة المحدد في التطبيقات المُثبتة على الجهاز. تحقق من قائمة التحديثات المتوفرة في المجلد الفرعي **Software updates** المضمن في المجلد **Application management**. يحتوي هذا المجلد على قائمة بالتحديثات لتطبيقات Microsoft ومنتجات موردي البرامج الآخرين المستردة بواسطة خادم الإدارة، التي يمكن توزيعها إلى الأجهزة. بعد عرض معلومات عن التحديثات المتوفرة، قم بتثبيتها على الجهاز.
أحمر	**تم تسجيل الأحداث الحرجة على خادم الإدارة**	IDS_AK_STATUS_EVENTS_OCCURED	تقع الأحداث من هذا النوع عند اكتشاف أحداث حرجة لخادم الإدارة. تحقق من قائمة الأحداث المخزنة على خادم الإدارة، ثم قم بإصلاح الأحداث الحرجة واحدًا تلو الآخر.

لون إشارة حركة المرور	اسم العرض لنوع الحدث	نوع الحدث	الوصف
أحمر	**تم تسجيل الأخطاء في الأحداث الموجودة على خادم الإدارة**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	تقع الأحداث من هذا النوع عند تسجيل أخطاء غير متوقعة على جانب خادم الإدارة. تحقق من قائمة الأحداث المخزنة على خادم الإدارة، ثم أصلح الأخطاء واحدًا تلو الآخر.
أحمر	**فقد الاتصال بعدد 1% جهاز (أجهزة)**	IDS_AK_STATUS_ADM_LOST_CONTROL1	تقع الأحداث من هذا النوع عند فقدان الاتصال بين خادم الإدارة والجهاز. اعرض قائمة الأجهزة غير المتصلة وحاول إعادة توصيلها.
أحمر	**لم يتصل 1% جهاز (أجهزة) بخادم الإدارة منذ وقت طويل**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	تقع الأحداث من هذا النوع عندما لا يكون الجهاز متصلاً بخادم الإدارة خلال الفترة الزمنية المحددة، بسبب إيقاف تشغيل الجهاز. تأكد من تشغيل الجهاز وتشغيل عميل الشبكة.
أحمر	**هناك جهاز (أجهزة) 1% حالته تختلف عن "موافق"**	IDS_AK_STATUS_HOST_NOT_OK	تقع الأحداث من هذا النوع عندما تتغير الحالة جيدة للجهاز المتصل بخادم الإدارة إلى حرجة" أو تحذير. يمكنك استكشاف المشكلة وإصلاحها باستخدام الأداة المساعدة للتشخيص عن بُعد في Kaspersky Security Center.
أحمر	**قواعد البيانات قديمة على: 1% جهاز (أجهزة)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	تقع الأحداث من هذا النوع عندما لا يتم تحديث قواعد بيانات مكافحة الفيروسات على الجهاز خلال الفترة الزمنية المحددة. اتبع التعليمات لتحديث قواعد بيانات Kaspersky.
أحمر	**الجهاز (الأجهزة) التي لم يتم فحص تحديثات Windows Update عليه منذ وقت طويل: 1%**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	تقع الأحداث من هذا النوع عندما لا يتم تشغيل مهمة مزامنة Windows Update خلال الفترة الزمنية المحددة. اتبع التعليمات لمزامنة التحديثات من Windows Update مع خادم الإدارة.
أحمر	**يلزم تثبيت 1% مكون إضافي (مكونات إضافية) ل Kaspersky Security Center**	IDS_AK_STATUS_PLUGINS_REQUIRED2	تقع الأحداث من هذا النوع عندما تحتاج إلى تثبيت مكونات إضافية لتطبيقات Kaspersky. يرجى تنزيل وتثبيت المكونات الإضافية للإدارة المطلوبة لتطبيق Kaspersky من صفحة ويب الدعم الفني من Kaspersky .

الوصول عن بُعد للأجهزة المدارة

هذا القسم يوفر معلومات حول الوصول للأجهزة المُدارة عن بُعد.

الاتصال عن بُعد بالأجهزة المدارة غير مدعوم عند الوصول إلى Kaspersky Security Center Web Console من جهاز يعمل بنظام التشغيل Microsoft Windows على معالجات Arm.

استخدام خيار "عدم قطع الاتصال بخادم الإدارة" لتوفير اتصال مستمر بين جهاز مُدار وخادم الإدارة

إذا كنت لا تستخدم خوادم الإرسال، فلن يوفر Kaspersky Security Center اتصالاً مستمراً بين الأجهزة المدارة وخادم الإدارة. يؤسس عملاء الشبكة على الأجهزة المدارة بشكل دوري اتصالات ومزامنة مع خادم الإدارة. يتم تحديد الفاصل الزمني بين جلسات المزامنة هذه في سياسية عميل الشبكة. إذا كانت المزامنة المبكرة مطلوبة، يرسل خادم الإدارة (أو نقطة توزيع إن كانت مستخدم) حزمة شبكة موقعة عبر شبكة IPv4 أو IPv6 إلى منفذ UDP لعميل الشبكة. رقم المنفذ هو 15000 بشكل افتراضي. إذا لم يكن هناك اتصال ممكن من خلال UDP بين خادم الإدارة وجهاز مُدار لأي سبب من الأسباب، فسيتم تشغيل المزامنة عند الاتصال المنتظم التالي لعميل الشبكة بخادم الإدارة خلال فترة المزامنة.

لا يمكن إجراء بعض العمليات بدون اتصال مبكر بين عميل الشبكة وخادم الإدارة مثل تشغيل المهام المحلية وإيقافها، أو تلقي إحصائيات تطبيق مُدار، أو إنشاء نفق. لحل هذه المشكلة، إذا كنت لا تستخدم خوادم الإرسال، فيمكنك استخدام الخيار **عدم قطع الاتصال عن خادم الإدارة** للتأكد من وجود اتصال دائم بين جهاز مُدار وخادم الإدارة.

لتوفير اتصال مستمر بين جهاز مُدار وخادم الإدارة:

1. في شجرة وحدة التحكم، افتح المجلد **الأجهزة المُدارة**.

2. في مساحة العمل الخاصة بالمجلد، حدد الجهاز المُدار الذي تريد توفير اتصال مستمر به.

3. في قائمة السياق الخاصة بالجهاز، حدد **خصائص**.

يتم فتح نافذة خصائص الجهاز المحدد.

4. في القسم **عام** في النافذة المعروضة، حدد الخيار **عدم قطع الاتصال عن خادم الإدارة**.

يتم إنشاء اتصال مستمر بين الجهاز المُدار وخادم الإدارة.

الحد الأقصى لعدد الأجهزة التي تم تحديد خيار **عدم قطع الاتصال عن خادم الإدارة** هو 300.

حول التحقق من وقت الاتصال بين جهاز ما وخادم الإدارة

عند إيقاف تشغيل جهاز ما، يقوم عميل الشبكة بإخطار خادم الإدارة بهذا الحدث. في وحدة تحكم الإدارة، يتم عرض هذا الجهاز كمتوقف التشغيل. ولكن، لا يمكن لعميل الشبكة إخطار خادم الإدارة بكل مثل هذه الأحداث. لذلك يقوم خادم الإدارة بشكل دوري بتحليل سمة **تم الاتصال بخادم الإدارة** (تُعرض قيمة هذه السمة في وحدة تحكم الإدارة، في خصائص الجهاز، في القسم **عام**) لكل جهاز ويقارنها مقابل الفاصل الزمني للمزامنة من الإعدادات الحالية لعميل الشبكة. في حالة عدم استجابة جهاز على مدى أكثر ثلاثة فواصل زمنية متتابعة للمزامنة، يتم تمييز هذا الجهاز كمتوقف التشغيل.

حول المزامنة المفروضة

على الرغم من قيام Kaspersky Security Center بمزامنة الحالة والإعدادات والمهام والسياسات الخاصة بالأجهزة المدارة تلقائيًا، في بعض الحالات يحتاج المسؤول لمعرفة بالضبط ما إذا قد تم إجراء المزامنة بالفعل أم لا لجهاز محدد في الوقت الحالي.

في قائمة السياق الخاصة بالأجهزة المُدارة في وحدة تحكم الإدارة، يحتوي عنصر القائمة **جميع& المهام** على الأمر**فرض المزامنة**. عندما ينفذ Kaspersky Security Center 15.1 هذا الأمر، يحاول خادم الإدارة الاتصال بالجهاز. إذا نجحت هذه المحاولة، فسيتم تنفيذ المزامنة المفروضة. وإلا، فسيتم فرض المزامنة فقط بعد إجراء الاتصال المجدول التالي بين عميل الشبكة وخادم الإدارة.

حول النفق

يتيح Kaspersky Security Center باتصالات TCP عبر الأنفاق من وحدة تحكم الإدارة عبر خادم الإدارة ثم عبر عميل الشبكة إلى منفذ محدد على جهاز مُدار. الأنفاق مصممة لتوصيل تطبيق عميل على جهاز مثبّت عليه وحدة تحكم الإدارة إلى منفذ TCP على جهاز مُدار—في حالة عدم إمكانية الاتصال المباشر بين وحدة تحكم الإدارة والجهاز المستهدف.

على سبيل المثال، تُستخدم الأنفاق لإجراء اتصالات بسطح مكتب بعيد، لكل من الاتصال بجلسة موجودة بالفعل، أو لإنشاء جلسة بعيدة جديدة.

يمكن أيضًا تمكين الأنفاق عن طريق استخدام أدوات خارجية. على سبيل المثال، يمكن للمسؤول تشغيل الأداة المساعدة putty وعميل VNC والأدوات الأخرى بهذه الطريقة.

دليل القياس

يقدم هذا القسم معلومات حول تغيير حجم Kaspersky Security Center.

حول هذا الدليل

يُعد دليل قياس Kaspersky Security Center 15.1 (المشار إليه كذلك باسم "Kaspersky Security Center") خاص بالمحترفين الذين يقومون بتثبيت Kaspersky Security Center وإدارته، بالإضافة إلى هؤلاء الذين يقدمون الدعم الفني للمؤسسات التي تستخدم Kaspersky Security Center.

يتم تقديم كل التوصيات والحسابات للشبكات التي يدير عليها Kaspersky Security Center حماية الأجهزة المثبّت عليها برنامج Kaspersky، بما في ذلك الأجهزة المحمولة. وفي حالة مراعاة الأجهزة المحمولة أو أي أجهزة أخرى مُدارة بشكل منفصل، يتم توضيح ذلك بشكل محدد.

للحصول على أداء مثالي والحفاظ عليه في ظروف التشغيل المختلفة، يجب عليك مراعاة عدد الأجهزة المتصلة بالشبكة ومخطط الشبكة ومجموعة ميزات Kaspersky Security Center التي تطلبها.

هذا الدليل يوفر المعلومات التالية:

- قيود Kaspersky Security Center
- حسابات عُقد مفتاح Kaspersky Security Center (خوادم الإدارة ونقاط التوزيع):
  - متطلبات الأجهزة لخوادم الإدارة ونقاط التوزيع
  - حساب رقم وتسلسل خوادم الإدارة
  - حساب رقم وتكوين نقاط التوزيع
- تكوين سجل الحدث في قاعدة البيانات بناءً على عدد الأجهزة المتصلة بالشبكة
- أفضل الممارسات الشائعة لتحسين الأداء
- تكوين مهام محددة تهدف إلى أداء مثالي لـ Kaspersky Security Center
- معدل حركة المرور (حمل الشبكة) بين خادم إدارة Kaspersky Security Center وكل جهاز محمي

يوصى بالرجوع إلى هذا الدليل في الحالات التالية:

- عند التخطيط للموارد قبل تثبيت Kaspersky Security Center
- عند التخطيط لتغييرات كبيرة على نطاق الشبكة التي تم نشر Kaspersky Security Center عليها
- عند التبديل من استخدام Kaspersky Security Center ضمن قطاع محدود من الشبكة (بيئة اختبار) إلى نشر Kaspersky Security Center على نطاق كامل على شبكة الشركة
- عند إجراء تغييرات على مجموعة من مزايا Kaspersky Security Center المستخدمة

معلومات حول قيود Kaspersky Security Center

يعرض الجدول التالي قيود الإصدار الحالي لـ Kaspersky Security Center .

قيود Kaspersky Security Center

نوع القيد	القيمة
العدد الأقصى للأجهزة المدارة لكل خادم إدارة	100,000
تم تحديد الحد الأقصى لعدد الأجهزة مع تحديد خيار **عدم قطع الاتصال عن خادم الإدارة**	300
الحد الأقصى لعدد مجموعات الإدارة	10,000
الحد الأقصى لعدد الأحداث التي سيتم تخزينها	45,000,000
الحد الأقصى لعدد السياسات	2000
الحد الأقصى لعدد المهام	2000
الحد الأقصى للعدد الإجمالي لعناصر الوحدات التنظيمية Active Directory، وحسابات المستخدمين، والأجهزة، ومجموعات الأمان)	1,000,000
الحد الأقصى لعدد ملفات التعريف في سياسة ما	100
الحد الأقصى لعدد خوادم الإدارة الثانوية على خادم إدارة أساسي واحد	500
الحد الأقصى لعدد خوادم الإدارة الافتراضية	500
الحد الأقصى لعدد الأجهزة التي يمكن أن تغطيها نقطة توزيع واحدة (تستطيع نقاط التوزيع تغطية الأجهزة غير المحمولة فقط)	10,000
الحد الأقصى لعدد الأجهزة التي قد تستخدم بوابة اتصال واحدة	10 000، بما في ذلك الأجهزة المحمولة
العدد الأقصى للأجهزة المحمولة لكل خادم إدارة	100 000 ناقص عدد الأجهزة المدارة الثابتة

حسابات خوادم الإدارة

يقدم هذا القسم متطلبات البرامج والأجهزة للأجهزة المستخدمة كخوادم إدارة. ويقدم أيضًا توصيات لحساب عدد وتسلسل خوادم الإدارة بناءً على تكوين شبكة المؤسسة.

حساب موارد الأجهزة لخادم الإدارة

يحتوي هذا القسم على حسابات توفر دليلاً لتخطيط موارد الأجهزة الخاصة بخادم الإدارة. التوصية حول حساب مساحة القرص عند استخدام ميزة إدارة الثغرات الأمنية والتصحيحات يتم تقديمها بشكل منفصل.

متطلبات الأجهزة الخاصة بنظام إدارة قواعد البيانات وخادم الإدارة

تقدم الجداول التالية الحد الأدنى المُوصي به من متطلبات الأجهزة إلى نظام إدارة قواعد البيانات وخادم الإدارة الذي تم الحصول عليه أثناء الاختبارات. للحصول على قائمة بأنظمة التشغيل وأنظمة إدارة قواعد البيانات المدعومة، يُرجى الرجوع إلى قائمة متطلبات الأجهزة والبرامج.

خادم الإدارة ونظام إدارة قاعدة البيانات على أجهزة مختلفة، وتحتوي الشبكة على 50000 جهاز

تكوين الجهاز المثبت عليه خادم الإدارة

الأجهزة	القيمة
وحدة المعالجة المركزية	4 نوى، 2500 ميجا هرتز
الذاكرة العشوائية	8 جيجابايت
محرك القرص الثابت	300 جيجابايت، RAID مستحسن
محول الشبكة	1 جيجابت

تكوين الجهاز المثبت عليه نظام إدارة قاعدة البيانات

الأجهزة	القيمة
وحدة المعالجة المركزية	4 نوى، 2500 ميجا هرتز
الذاكرة العشوائية	16 جيجابايت
محرك القرص الثابت	200 جيجابايت، SATA RAID
محول الشبكة	1 جيجابت

خادم الإدارة ونظام إدارة قاعدة البيانات على الجهاز نفسه، وتحتوي الشبكة على 50000 جهاز

تكوين الجهاز المثبت عليه خادم الإدارة ونظام إدارة قاعدة البيانات

الأجهزة	القيمة
وحدة المعالجة المركزية	8 مراكز معالجة، 2500 ميجا هرتز
الذاكرة العشوائية	16 جيجابايت
محرك القرص الثابت	500 جيجابايت، SATA RAID
محول الشبكة	1 جيجابت

خادم الإدارة ونظام إدارة قاعدة البيانات على أجهزة مختلفة، وتحتوي الشبكة على 100000 جهاز

تكوين الجهاز المثبت عليه خادم الإدارة

الأجهزة	القيمة
وحدة المعالجة المركزية	8 مراكز معالجة، 2.13 جيجاهرتز
الذاكرة العشوائية	8 جيجابايت
محرك القرص الثابت	1 تيرابايت، مع RAID
محول الشبكة	1 جيجابت

تكوين الجهاز المثبت عليه نظام إدارة قاعدة البيانات

الأجهزة	القيمة
وحدة المعالجة المركزية	8 مراكز معالجة، 2.53 جيجاهرتز
الذاكرة العشوائية	26 جيجابايت
محرك القرص الثابت	500 جيجابايت، SATA RAID
محول الشبكة	1 جيجابت

كانت الاختبارات تعمل بموجب الإعدادات التالية:

- التعيين التلقائي لنقاط التوزيع ممكّن على خادم الإدارة، أو يتم تعيين نقاط التوزيع يدويًا طبقًا للجدول الموصى به.
- تقوم مهمة النسخ الاحتياطي بحفظ النسخ الاحتياطية إلى ملف مورد موجود على خادم مخصص.
- تم تعيين الفاصل الزمني للمزامنة لعملاء الشبكة كما هو محدد في الجدول الموجود أدناه.

الفاصل الزمني للمزامنة لعملاء الشبكة

الفاصل الزمني للمزامنة (بالدقائق)	عدد الأجهزة المدارة
15	000,10
30	000,20
45	000,30
60	000,40
75	000,50
150	000,100

حساب مساحة قاعدة البيانات

يمكن حساب مقدار المساحة التقريبية التي يجب أن يتم حجزها في قاعدة البيانات باستخدام الصيغة التالية:

(F * N * A + 1.2 * E + 2.5 * C + 2.3 * 600)، كيلو بايت

حيث:

- C هو عدد الأجهزة.
- E هو عدد الأحداث المراد تخزينها.
- A هو إجمالي عدد كائنات Active Directory:
  - حسابات الجهاز
  - حسابات المستخدمين
  - الحسابات الخاصة بـ security groups
  - الوحدات التنظيمية لـ Active Directory

  إذا تم تعطيل فحص Active Directory، فيتم اعتبار A صفر.
- N هو متوسط عدد الملفات القابلة للتنفيذ التي تم جردها على جهاز نقطة النهاية.
- F هو عدد أجهزة نقطة النهاية، حيث تم جرد الملفات التنفيذية.

إذا كنت تخطط لتمكين إخطار خادم الإدارة على التطبيقات التي تقوم بتشغيلها (في إعدادات سياسة Kaspersky Endpoint Security)، فستحتاج إلى (C * 0.03) جيجابايت إضافية لتخزين المعلومات حول التطبيقات التي تقوم بتشغيلها في قاعدة البيانات.

إذا قام خادم الإدارة بتوزيع تحديثات Windows (وبالتالي تعمل كخادم Windows Server Update Services)، فستتطلب قاعدة البيانات مساحة إضافية بسعة 2.5 جيجابايت.

أثناء العمل، دائمًا ما تظهر مساحة غير مخصصة محددة في قاعدة البيانات. لذلك، غالبًا ما يبلغ الحجم الفعلي لملف قاعدة البيانات (افتراضيًا، الملف KAV.MDF إذا كنت تستخدم خادم SQL كـ DBMS) ضعفي مقدار حجم المساحة غير الشاغرة في قاعدة البيانات.

من غير المستحسن تحديد حجم سجل المعاملة بشكل صريح (بشكل افتراضي، الملف KAV_log.LDF إذا كنت تستخدم خادم SQL Server كنظام DBMS). ومن المستحسن ترك القيمة الافتراضية للمعلمة MAXSIZE. ومع ذلك، إذا كان يتعين عليك تحديد حجم هذا الملف، فيجب عليك مراعاة أن الحد الأدنى للقيمة الضرورية القياسية للمعلمة MAXSIZE في الملف KAV_log.LDF هي 20480 ميجابايت.

حساب مساحة القرص (مع أو بدون استخدام ميزة إدارة الثغرات الأمنية والتصحيحات)

حساب مساحة القرص بدون استخدام ميزة إدارة الثغرات الأمنية والتصحيحات

يمكن تقدير مساحة قرص خادم الإدارة المطلوبة لمجلد %ALLUSERSPROFILE\Application Data\KasperskyLab\adminkit بشكل تقريبي باستخدام المعادلة:

(A * E + 0.17 * C + 0.15 * 724), كيلو بايت

حيث:

- C هو عدد الأجهزة.
- E هو عدد الأحداث المراد تخزينها.
- A هو إجمالي عدد كائنات Active Directory:
  - حسابات الجهاز
  - حسابات المستخدمين
  - الحسابات الخاصة بـ security groups
  - الوحدات التنظيمية لـ Active Directory

إذا تم تعطيل فحص Active Directory، فيتم اعتبار A صفر.

حساب مساحة القرص الإضافية باستخدام ميزة إدارة الثغرات الأمنية والتصحيحات

- تحديثات. يتطلب المجلد المشترك مساحة 4 جيجابايت إضافية على الأقل لتخزين التحديثات.
- حزم التثبيت. إذا كانت بعض حزم التثبيت مخزنة على خادم الإدارة، سيتطلب المجلد المشترك مساحة إضافية من المساحة الخالية على القرص، تساوي الحجم الإجمالي لكل حزم التثبيت المتوفرة للتثبيت.
- مهام التثبيت عن بُعد. في حالة وجود مهام التثبيت عن بُعد على خادم الإدارة، فستحتاج إلى مساحة إضافية من المساحة الخالية على القرص (في المجلد %ALLUSERSPROFILE\Application Data\KasperskyLab\adminkit) تساوي إجمالي مساحة حزم التثبيت المراد تثبيتها.
- التصحيحات. في حالة تضمين خادم الإدارة في تثبيت التصحيحات، فستتطلب مساحة إضافية من مساحة القرص:
  - ينبغي أن يحتوي مجلد التصحيحات على قدر من مساحة القرص تساوي الحجم الإجمالي لكل التصحيحات التي تم تنزيلها. يتم تخزين التصحيحات بشكل افتراضي في المجلد %ALLUSERSPROFILE\Application Data\KasperskyLab\adminkit\1093\working.\wusfiles folder.

يمكنك استخدام الأداة المساعدة klsrvswch لتحديد مجلد مختلف لتخزين التصحيحات. توجد الأداة المساعدة klsrvswch في المجلد حيث تم تثبيت خادم الإدارة. مسار التثبيت الافتراضي: <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

في حالة استخدام خادم الإدارة كخادم WSUS، ننصحك بأن تقوم بتخصيص 100 جيجابايت لهذا المجلد.

- يجب أن يحتوي المجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit على مقدار من مساحة القرص مساوية للحجم الإجمالي لهذه التصحيحات المُشار إليها بواسطة المثيلات الحالية لمهام تثبيت التحديث (التصحيح) وإصلاح الثغرات الأمنية.

حساب رقم وتكوين خوادم الإدارة

لتقليل الحمل على خادم الإدارة الرئيسي، يمكنك تخصيص خادم إدارة منفصل لكل مجموعة إدارة. لا يمكن أن يتخطى عدد خوادم الإدارة الثانوية 500 خادم لكل خادم إدارة أساسي واحد.

نوصي بإنشاء تكوين خوادم الإدارة بالتطابق مع تكوين شبكة مؤسستك.

توصيات لتوصيل الأجهزة الافتراضية الديناميكية بـ Kaspersky Security Center

تستهلك الأجهزة الافتراضية الديناميكية (يشار إليها أيضًا باسم الأجهزة الافتراضية الديناميكية) موارد أكثر من الأجهزة الافتراضية الثابتة.

لمزيد من المعلومات حول الأجهزة الافتراضية الديناميكية، راجع دعم الأجهزة الافتراضية الديناميكية.

عند توصيل جهاز افتراضي ديناميكي جديد، ينشئ Kaspersky Security Center رمزًا لهذا الجهاز الظاهري الديناميكي في وحدة تحكم الإدارة وينقل الجهاز الظاهري الديناميكي إلى مجموعة الإدارة. بعد ذلك، يتم إضافة الجهاز الافتراضي الديناميكي إلى قاعدة بيانات خادم الإدارة. وتتم مزامنة خادم الإدارة بشكل كامل مع عميل الشبكة المثبت على الجهاز الافتراضي الديناميكي هذا.

في شبكة مؤسسة ما، يُنشئ عميل الشبكة قوائم الشبكة التالية لكل جهاز افتراضي ديناميكي:

- الأجهزة
- البرامج المثبتة
- الثغرات الأمنية المكتشفة
- أحداث وقوائم الملفات القابلة للتنفيذ الخاصة بمكون التحكم في التطبيق

ينقل عميل الشبكة قوائم الشبكة هذه إلى خادم الإدارة. يعتمد حجم قوائم الشبكة على المكونات المثبتة على الجهاز الافتراضي الديناميكي، وقد يؤثر على أداء Kaspersky Security Center ونظام إدارة قاعدة البيانات (DBMS). لاحظ أن التحميل يمكن أن ينمو بشكل غير خطي.

بعد انتهاء المستخدم من العمل مع الجهاز الظاهري الديناميكي وإيقاف تشغيله، تتم إزالة هذا الجهاز بعد ذلك من البنية التحتية الافتراضية وتتم إزالة الإدخالات المتعلقة بهذا الجهاز من قاعدة بيانات خادم الإدارة.

تستهلك كل هذه الإجراءات الكثير من موارد قاعدة بيانات Kaspersky Security Center وخادم الإدارة، ويمكن أن تقلل من أداء Kaspersky Security Center ونظام إدارة قاعدة البيانات (DBMS). نوصي بتوصيل ما يصل إلى 20 000 جهاز افتراضي ديناميكي بـ Kaspersky Security Center.

يمكنك توصيل أكثر من 20 000 جهاز افتراضي ديناميكي بـ Kaspersky Security Center إذا كانت الأجهزة الظاهرية الديناميكية المتصلة تؤدي عمليات قياسية (على سبيل المثال، تحديثات قاعدة البيانات) ولا تستهلك أكثر من 80 بالمائة من الذاكرة و 75-80 بالمائة من النوى المتوفرة.

يمكن أن يؤدي تغيير إعدادات السياسة أو البرنامج أو نظام التشغيل على الجهاز الظاهري الديناميكي إلى تقليل أو زيادة استهلاك الموارد. يعتبر استهلاك 80-95 في المائة من الموارد هو الأمثل.

حسابات نقاط التوزيع وبوابات الاتصال

يقدم هذا القسم متطلبات الأجهزة المستخدمة كنقاط توزيع بالإضافة إلى توصيات لحساب عدد نقاط التوزيع وبوابات الاتصال بالاعتماد على تكوين شبكة المؤسسة.

المتطلبات لنقطة توزيع

للتعامل مع ما يصل إلى 10 000 جهاز من أجهزة العملاء، يجب أن تستوفي نقطة التوزيع الحد الأدنى من المتطلبات التالية (يتم توفير تكوين لحامل الاختبار):

- وحدة المعالجة المركزية: Intel® Core™ i7-7700 CPU بسعة 3.60 جيجاهرتز و4 مراكز نواة.
- ذاكرة الوصول العشوائي: 8 جيجابايت
- مساحة التخزين الخالية: 120 جيجا بايت.

لا يُنصح بتعيين خادم الإدارة كنقطة توزيع، حيث سيؤدي ذلك إلى زيادة الحمل على خادم الإدارة.

في حالة تعليق أي من مهام التثبيت عن بُعد على خادم الإدارة، فسيتطلب أيضًا الجهاز المثبت عليه نقطة توزيع مساحة خالية كافية على القرص تساوي الحجم الإجمالي لحزم التثبيت المراد تثبيتها.

في حالة تعليق مثيل واحد أو أكثر من مثيلات مهمة تثبيت (تصحيح) التحديث وإصلاح الثغرات الأمنية على خادم الإدارة، فسيتطلب الجهاز المثبت عليه نقطة التوزيع مساحة خالية إضافية أيضًا، تساوي ضعف الحجم الإجمالي للتصحيحات المراد تثبيتها.

إذا كنت تستخدم النظام حيث تتلقى نقاط التوزيع تحديثات قاعد البيانات والوحدات النمطية لبرنامج التطبيق مباشرةً من خوادم تحديث Kaspersky، فيجب توصيل نقاط التوزيع بالإنترنت.

حساب عدد نقاط التوزيع وتكوينهم

كلما زاد عدد الأجهزة العميلة التي تحتوي عليها الشبكة، زاد عدد نقاط التوزيع المطلوبة بالنسبة لها. لا نوصي بتعطيل التعيين التلقائي لنقاط التوزيع. عند تمكين التعيين التلقائي لنقاط التوزيع، يقوم خادم الإدارة بتعيين نقاط التوزيع إذا كان عدد الأجهزة العميلة كبيرًا إلى حد ما ويقوم بتحديد تكوينهم.

استخدام نقاط التوزيع المعينة بشكل حصري

إذا كنت تخطط لاستخدام أجهزة محددة كنقاط توزيع (أي الخوادم المخصصة حصريًا)، فيمكنك إلغاء الاشتراك من استخدام التعيين التلقائي لنقاط التوزيع. وفي هذه الحالة، تأكد من أن الأجهزة التي تنوي تعيينها كنقاط توزيع تحتوي على حجم كافٍ من مساحة القرص الفارغة ولا يتم إيقاف تشغيلها بانتظام وتم تعطيل وضع السكون بها.

عدد نقاط التوزيع التي تم تعيينها حصريًا في شبكة تحتوي على مقطع شبكة واحد بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العميلة في مقطع الشبكة	عدد نقاط التوزيع
أقل من 300	0 (لا تقم بتعيين نقاط توزيع)
أكثر من 300	مقبول: (N/10 1 + 000)، موصى به: (N/5 2 + 000)، حيث N هو عدد الأجهزة المتصلة بالشبكة

عدد نقاط التوزيع التي تم تعيينها حصريًا في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العملية لكل مقطع شبكة	عدد نقاط التوزيع
أقل من 10	0 (لا تقم بتعيين نقاط توزيع)
10–100	1
أكثر من 100	مقبول: (N/10 1 + 000)، موصى به: (N/5 2 + 000)، حيث N هو عدد الأجهزة المتصلة بالشبكة

استخدام الأجهزة العميلة القياسية (محطات العمل) كنقاط توزيع

إذا كنت تخطط لاستخدام أجهزة عميلة قياسية (أي محطات العمل) كنقاط توزيع، فنوصيك بتعيين نقاط التوزيع كما هو موضح في الجداول أدناه لتجنب التحميل الزائد على قنوات الاتصال وخادم الإدارة:

عدد محطات العمل التي تعمل كنقاط توزيع في شبكة تحتوي على مقطع شبكة واحد بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العميلة في مقطع الشبكة	عدد نقاط التوزيع
أقل من 300	0 (لا تقم بتعيين نقاط توزيع)
أكثر من 300	(N/300 + 1)، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل

عدد محطات العمل التي تعمل كنقاط توزيع في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العملية لكل مقطع شبكة	عدد نقاط التوزيع
أقل من 10	0 (لا تقم بتعيين نقاط توزيع)
10–30	1
31–300	2
أكثر من 300	(N/300 + 1)، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل

في حالة إيقاف تشغيل نقطة توزيع (أو عدم توفرها لسبب آخر)، يمكن للأجهزة المُدارة الموجودة في نطاقها الوصول إلى خادم الإدارة للحصول على تحديثات.

حساب عدد بوابات الاتصال

إذا كنت تخطط لاستخدام بوابة اتصال، نوصي بتعيين جهاز خاص لهذه الوظيفة.

يمكن لبوابة الاتصال تغطية ما لا يزيد عن 10 000 جهاز من الأجهزة المدارة، بما في ذلك الأجهزة المحمولة.

تسجيل المعلومات حول أحداث المهام والسياسات

يقدم هذا القسم الحسابات المتعلقة بتخزين الأحداث في قاعدة بيانات خادم الإدارة ويقدم توصيات حول كيفية تقليل عدد الأحداث إلى أقل عدد، وبذلك يتم تقليل التحميل على خادم الإدارة.

بشكل افتراضي، تعمل خصائص كل مهمة وكل سياسة على تخزين كل الأحداث المتعلقة بتنفيذ المهام وتطبيق السياسة.

ومع ذلك، إذا كانت مهمة ما تعمل بشكلٍ متكرر (على سبيل المثال، أكثر من مرة أسبوعيًا) وعلى رقم كبير إلى حدٍ ما من الأجهزة (على سبيل المثال، ما يزيد عن 10 000 جهاز)، فقد يصبح عدد الأحداث كبيرًا للغاية ويمكن للأحداث أن تغمر قاعدة البيانات. في هذه الحالة، يوصى بتحديد أحد الخيارين الموجودين في إعدادات المهمة:

- **Save events related to task progress**. في هذه الحال، تتلقى قاعدة البيانات فقط المعلومات حول بدء المهمة والتقدُّم، وإكمالها (ناجحة، مع إرجاع تحذير أو خطأ) من كل جهاز يتم تشغيل المهمة عليه.
- **Save only task execution results**. في هذه الحالة، تتلقى قاعدة البيانات معلومات حول إكمال المهمة فقط (ناجحة، مع إرجاع تحذير أو خطأ) من كل جهاز يتم تشغيل المهمة عليه.

إذا تم تحديد سياسة لعدد كبير إلى حدٍ ما من الأجهزة (على سبيل المثال، ما يزيد عن 10 000)، فقد يصبح عدد الأحداث كبيرًا للغاية كذلك وقد تغمر الأحداث قاعدة البيانات. في هذه الحالة، من المستحسن اختيار أهم الأحداث الحرجة فقط في إعدادات السياسة وتمكين تسجيلها. يُنصح بإلغاء تمكين تسجيل كافة الأحداث الأخرى.

عند فعل ذلك، ستقلل من عدد الأحداث الموجودة في قاعدة البيانات، وتزيد من سرعة تنفيذ السيناريوهات المرتبطة بتحليل جدول الأحداث في قاعدة البيانات وخفض خطر الكتابة فوق الأحداث الحرجة بواسطة عدد كبير من الأحداث.

كما يمكنك تقليل مدة التخزين للأحداث المقترنة بمهمة أو بسياسة. الفترة الافتراضية هي 7 أيام للأحداث المتعلقة و30 يومًا للأحداث المتعلقة بالسياسة. عند تغيير فترة تخزين الحدث، ضع في اعتبارك إجراءات العمل في مكان مؤسستك ومقدار الوقت الذي يمكن أن يخصصه مسؤول النظام لتحليل كل حدث.

يُستحسن تعديل إعدادات تخزين الأحداث في أي من الحالات التالية:

- تحتل الأحداث المتعلقة بالتغييرات في الحالات الوسيطة للمهام والأحداث الجماعية المتعلقة بتطبيق السياسات حصة كبيرة من جميع الأحداث في قاعدة بيانات Kaspersky Security Center.
- يبدأ سجل أحداث Kaspersky في عرض إدخالات حول الإزالة التلقائية للأحداث عند تخطي القيد المحدد للعدد الإجمالي للأحداث المخزنة في قاعدة البيانات.

اختر خيارات تسجيل الأحداث بناءً على افتراض أنه يجب أن لا يتجاوز العدد المثالي للأحداث القادم من جهاز واحد كل يوم، 20 حدث. يجب عليك زيادة هذا الحد قليلاً، إذا لزم الأمر، ولكن إذا كان عدد الأجهزة الموجود في شبكتك صغير نسبيًا (أقل من 10 000).

الاعتبارات الخاصة والإعدادات المثالية الخاصة بمهام محددة

تخضع مهام محددة لاعتبارات خاصة متعلقة بعدد الأجهزة المتصلة بالشبكة. يقدم هذا القسم توصيات حول التكوين القياسي لإعدادات مثل هذه المهام.

يُعتبر اكتشاف الأجهزة ومهمة النسخ الاحتياطي للبيانات ومهمة صيانة خادم الإدارة والمهام الجماعية لتحديث Kaspersky Endpoint Security جزءًا من الوظائف الأساسية لتطبيق Kaspersky Security Center.

معدل تكرار اكتشاف الأجهزة

من غير المستحسن زيادة التكرار الافتراضي لاكتشاف الأجهزة إذ إنه قد يؤدي إلى حدوث تحميل زائد على وحدات التحكم في المجال. بدلاً من ذلك، يوصى بجدولة الاستقصاء بالحد الأدنى للتكرار المسموح به حسب احتياجات مؤسستك. التوصيات لحساب الجدولة المثالية مقدمة في الجدول الموجود أدناه.

جدول اكتشاف الشبكة

عدد الأجهزة المتصلة بالشبكة	التكرار الموصى به لاكتشاف الأجهزة
أقل من 10 000	التردد الافتراضي أو أقل
10 000 أو أكثر	مرة في اليوم أو أقل

مهمة النسخ الاحتياطي لبيانات خادم الإدارة ومهمة صيانة خادم الإدارة

يتوقف خادم الإدارة عن العمل عند تشغيل المهام التالية:

- النسخ الاحتياطي لبيانات خادم الإدارة
- صيانة خادم الإدارة

عند تشغيل هذه المهام، لا يمكن لقاعدة البيانات تلقي أي بيانات.

قد تضطر لإعادة جدولة هذه المهام حتى لا يتم تنفيذها في نفس وقت تنفيذ مهام خادم الإدارة الأخرى.

مهام جماعية لتحديث Kaspersky Endpoint Security

إذا كان خادم الإدارة يعمل كمصدر تحديث، فخيار الجدولة الموصى به لمهام تحديث المجموعة الخاصة بإصدار Kaspersky Endpoint Security 10 والإصدارات الأحدث هو **عند تنزيل تحديثات جديدة إلى المستودع** مع تحديد خانة الاختيار **استخدام التأخير العشوائي التلقائي لعمليات بدء تشغيل المهمة**.

إذا تم إنشاء مهمة محلية لتنزيل تحديثات من خوادم Kaspersky إلى المستودع على كل نقطة توزيع، فيُوصى بإجراء جدولة دورية لمهمة تحديث مجموعة Kaspersky Endpoint Security. يجب أن تكون قيمة الفترة العشوائية ساعة واحدة في هذه الحالة.

مهمة الجرد

يمكنك تقليل الحمل على قاعدة البيانات أثناء الحصول على معلومات عن الملفات القابلة للتنفيذ. ولفعل ذلك، نوصي بتشغيل مهمة جرد لتطبيق Kaspersky Endpoint Security على الأجهزة المرجعية التي تم تثبيت مجموعة قياسية من البرامج عليها.

يجب ألا يتجاوز عدد الملفات التنفيذية التي يستلمها خادم الإدارة من جهاز مفرد 150 000 جهاز. عند وصول Kaspersky Security Center إلى هذا الحد، لا يمكنه تلقي أي ملفات جديدة.

في المعتاد، لا يتخطى عدد ملفات جهاز عميل مشترك 60 000. عدد الملفات التنفيذية على خادم ملف يمكن أن يكون أكبر من أو يتخطى عقدة 150 000.

أوضحت قياسات الاختبار أن نتيجة مهمة المخزون كانت كما يلي على جهاز يعمل بنظام تشغيل Windows 7 مثبّت عليه Kaspersky Endpoint Security 11 وغير مثبت عليه تطبيقات جهة خارجية:

- عند إلغاء تحديد خانات الاختيار **مخزون الوحدات النمطية لـ DLL** و**مخزون الملفات النصية**: حوالي 3000 ملف.
- عند تحديد خانات الاختيار **مخزون الوحدات النمطية لـ DLL** و**مخزون الملفات النصية**: 10 000 إلى 20 000 ملف بناءً على عدد حزم خدمة نظام التشغيل المثبتة.
- عند تحديد خانة الاختيار **مخزون الملفات النصية**: تقريبًا 10 000 ملف.

تفاصيل حول انتشار حمل الشبكة بين خادم الإدارة والأجهزة المحمية

يقدم هذا القسم نتائج قياسات الاختبار الخاص بحركة مرور الشبكة مع مصف للظروف التي تم إجراء القياسات فيها. يمكنك الرجوع لهذه المعلومات عند التخطيط للبنية التحتية للشبكة وقدرة معدل نقل قنوات الشبكة داخل مؤسستك (أو بين خادم الإدارة والمؤسسة الأخرى التي سيتم حماية أجهزتها). معرفة قدرة معدل نقل الشبكة، يمكنك أيضًا تقدير الوقت التقريبي الذي ستستغرقه عملية نقل البيانات المختلفة.

استهلاك حركة المرور بموجب السيناريوهات المختلفة

يوضح الجدول الموجود أدناه نتائج اختبارات القياس التي تم إجراؤها على حركة المرور بين خادم الإدارة وجهاز مُدار في سيناريوهات مختلفة.

بشكل افتراضي، تتم مزامنة الأجهزة المثبت عليها خادم الإدارة كل 15 دقيقة أو على فواصل زمنية أطول. ولكن في حالة تعديل إعدادات سياسة أو مهمة ما على خادم الإدارة، تحدث مزامنة مبكرة على الأجهزة التي يمكن تطبيق السياسة (أو المهمة) عليها وبذلك يتم نقل الإعدادات الجديدة إلى الأجهزة.

معدل حركة المرور بين خادم الإدارة وجهاز مُدار

سيناريو	حركة المرور من خادم الإدارة إلى كل جهاز مُدار	حركة المرور من كل جهاز مُدار إلى خادم الإدارة
تثبيت Kaspersky Endpoint Security 11.7 for Windows مع قواعد بيانات محدّثة	390 ميجابايت	3.3 ميجابايت
تثبيت عميل الشبكة	75 ميجابايت	397 كيلوبايت
التثبيت المتزامن لعميل الشبكة و Kaspersky Endpoint Security 11.7 for Windows	459 ميجابايت	3.6 ميجابايت
التحديث المبدئي لقواعد بيانات مكافحة الفيروسات دون تحديث قواعد البيانات الموجودة في الحزمة (في حالة تعطيل مشاركة Kaspersky Security Network)	113 ميجابايت	1,8 ميجابايت
تحديث يومي لقواعد بيانات مكافحة الفيروسات (في حال تمكين مشاركة Kaspersky Security Network)	22 ميجابايت	373 ميجابايت
مزامنة مبدئية قبل تحديث قواعد البيانات على جهاز (نقل السياسات والمهام)	382 كيلوبايت	446 كيلوبايت
المزامنة الأولية بعد تحديث قواعد البيانات على جهاز	20 كيلوبايت	157 كيلوبايت
المزامنة بدون تغييرات على خادم الإدارة (حسب الجدول)	18 كيلوبايت	23 كيلوبايت
المزامنة عند تغيير إعداد واحد في سياسة مجموعة (بمجرد تغيير الإعداد)	19 كيلوبايت	20 كيلوبايت
المزامنة عند تغيير إعداد واحد في مهمة جماعية (بمجرد تغيير الإعداد)	14 كيلوبايت	11 كيلوبايت
المزامنة المفروضة	110 كيلوبايت	109 كيلوبايت
حدث **اكتشاف فيروس** (فيروس واحد)	44 كيلوبايت	50 كيلوبايت
حدث **اكتشاف فيروس** (10 فيروسات)	58 كيلوبايت	77 كيلوبايت
المرور مرة واحدة بعد تمكين قائمة سجل التطبيقات	حتى 10 كيلوبايت	حتى 12 كيلوبايت
المرور اليومي عندما يتم تمكين قائمة سجل التطبيقات	حتى 840 كيلوبايت	حتى 1 ميجابايت

متوسط استخدام حركة المرور كل 24 ساعة

فيما يلي متوسط استخدام حركة المرور على مدار 24 ساعة بين خادم الإدارة والجهاز المدار:

- تبلغ حركة المرور من خادم الإدارة إلى الجهاز المُدار 840 كيلو بايت.
- تبلغ حركة المرور من الجهاز المُدار إلى خادم الإدارة 1 ميغابايت.

تم قياس حركة المرور وفقًا للشروط التالية:

- يحتوي الجهاز المدار على عميل الشبكة و Kaspersky Endpoint Security 11.6 لنظام Windows المثبت.
- لم يتم تعيين نقطة توزيع للجهاز.
- لم يتم تمكين إدارة الثغرات الأمنية والتصحيحات.
- المعدل الزمني للمزامنة مع خادم الإدارة كان 15 دقيقة.

الاتصال بالدعم الفني

يصف هذا القسم كيفية الحصول على الدعم الفني والبنود التي تتوافر على أساسها.

كيفية الحصول على الدعم الفني

إذا لم تتمكن من العثور على حل لمشكلتك في مستندات Kaspersky Security Center أو في أحد مصادر المعلومات عن Kaspersky Security Center، يرجى الاتصال بالدعم الفني في Kaspersky. سيجيب أخصائيو خدمة الدعم الفني على كافة تساؤلاتك المتعلقة بتثبيت Kaspersky Security Center واستخدامه.

توفِّر Kaspersky الدعم لتطبيق Kaspersky Security Center أثناء دورة حياته (انظر صفحة دورة حياة دعم التطبيق). قبل الاتصال بالدعم الفني، يرجى قراءة قواعد الدعم .

يمكنك الاتصال بالدعم الفني بإحدى الطرق التالية:

- من خلال زيارة موقع الويب للدعم الفني
- عن طريق إرسال طلب إلى الدعم الفني من بوابة Kaspersky CompanyAccount

الدعم الفني من خلال Kaspersky CompanyAccount

حساب شركة Kaspersky هي بوابة للشركات التي تستخدم تطبيقات Kaspersky. تم تصميم بوابة Kaspersky CompanyAccount لتسهيل التفاعل بين المستخدمين والأخصائيين في Kaspersky من خلال طلبات عبر الإنترنت. يمكنك استخدام Kaspersky CompanyAccount لتتبع حالة طلباتك على الإنترنت وتخزين سجل لها أيضًا.

يمكنك تسجيل جميع موظفي المؤسسة الخاصة بك بحساب موحد على Kaspersky CompanyAccount. يسمح لك الحساب الموحد بإدارة الطلبات الإلكترونية المقدمة من الموظفين المسجلين إلى Kaspersky بصورة مركزية وكذلك إدارة امتيازات هؤلاء الموظفين عبر Kaspersky CompanyAccount.

تتاح بوابة Kaspersky CompanyAccount باللغات التالية:

- الإنجليزية
- الإسبانية
- الإيطالية
- الألمانية
- البولندية
- البرتغالية
- الروسية

- الفرنسية
- اليابانية

لتعلم المزيد بشأن حساب شركة Kaspersky، قم بزيارة موقع ويب الدعم الفني.

الحصول على ملفات تفريغ خادم الإدارة

تحتوي ملفات التفريغ الخاصة بخادم الإدارة على جميع المعلومات عن عمليات خادم الإدارة في وقت ما. يتم تخزين ملفات تفريغ خادم الإدارة في المجلد %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. يتم تخزين ملفات التفريغ طالما أن Kaspersky Security Center قيد الاستخدام، ويتم حذفها نهائيًا عند إزالته. لا يتم إرسال ملفات التفريغ إلى Kaspersky تلقائيًا.

في حالة تعطل خادم الإدارة، يمكنك الاتصال بالدعم الفني في Kaspersky. قد يطلب منك أخصائي الدعم الفني إرسال ملفات تفريغ خادم الإدارة لإجراء المزيد من التحليل في Kaspersky.

قد تحتوي ملفات التفريغ على بيانات شخصية. نوصي بحماية المعلومات من الوصول غير المصرح به قبل إرسالها إلى Kaspersky.

مصادر المعلومات المتعلقة بالتطبيق

صفحة Kaspersky Security Center على الموقع الإلكتروني لـ Kaspersky

في صفحة Kaspersky Security Center الموجودة في الموقع الإلكتروني لـ Kaspersky، يمكنك عرض معلومات عامة حول التطبيق ووظائفه ومزاياه.

صفحة Kaspersky Security Center على قاعدة المعارف

قاعدة المعارف هي قسم على الموقع الإلكتروني الخاص بالدعم الفني لـ Kaspersky.

على صفحة Kaspersky Security Center في قاعدة المعارف، يمكنك قراءة مقالات والتي تُقدم معلومات مفيدة وتوصيات وإجابات على الأسئلة المتكررة حول كيفية شراء التطبيق وتثبيته واستخدامه.

قد توفر المقالات الموجودة في قاعدة المعارف إجابات عن الأسئلة التي تتعلق بكل من Kaspersky Security Center وكذلك تطبيقات Kaspersky الأخرى. قد تشتمل أيضًا المقالات في قاعدة المعارف على أخبار الدعم الفني.

مناقشة تطبيقات Kaspersky مع المجتمع

إذا لم يكن سؤالك يتطلب توفير إجابة فورية، فيمكنك مناقشته مع خبراء Kaspersky والمستخدمين الآخرين في منتدانا.

في هذا المنتدى، يمكنك عرض موضوعات المناقشة، ونشر تعليقاتك، وإنشاء موضوعات جديدة للمناقشة.

يلزم وجود اتصال بالإنترنت للوصول إلى مصادر موقع الويب.

إذا لم تستطع العثور على حل لمشكلتك، قم بالاتصال بالدعم الفني.

مسرد المصطلحات

(AWS API) AWS Application Program Interface

واجهة برمجة التطبيق الخاصة بالنظام الأساسي AWS الذي يتم استخدامه بواسطة Kaspersky Security Center. وعلى نحو خاص، أدوات AWS API التي يتم استخدامها لاستقصاء قطاع السحابة وتثبيت عميل الشبكة على المثيلات.

HTTPS

بروتوكول أمان لنقل البيانات باستخدام التشفير بين مستعرض وخادم الويب. يتم استخدام HTTPS للوصول إلى المعلومات المقيدة، مثل بيانات الشركة أو البيانات المالية.

JavaScript

لغة برمجة تعمل على توسيع أداء صفحات الويب. يمكن لصفحات الويب التي تم إنشاؤها باستخدام JavaScript تنفيذ الوظائف (على سبيل المثال، تغيير عرض عناصر الواجهة أو فتح نوافذ إضافية) بدون تحديث صفحة الويب باستخدام البيانات الجديدة من مستعرض الويب. لعرض الصفحات التي تم إنشاؤها باستخدام JavaScript، قم بتكوين دعم JavaScript في تكوين المستعرض الخاص بك.

(KPSN) Kaspersky Private Security Network

تعد Kaspersky Private Security Network بمثابة الحل الذي يوفر لمستخدمي الأجهزة المثبت عليها تطبيقات Kaspersky إمكانية الوصول لقواعد بيانات السمعة لـ Kaspersky Security Network والبيانات الإحصائية الأخرى دون إرسال بيانات من أجهزتهم إلى Kaspersky Security Network. تم تصميم Kaspersky Private Security Network لعملاء الشركة الذين يتعذر عليهم المشاركة في Kaspersky Security Network لأحد الأسباب التالية:

- الأجهزة غير متصلة بالإنترنت.
- كان إرسال أي بيانات خارج الدولة أو شبكة اتصال محلية (LAN) لشركة محظور بموجب القانون أو سياسات أمان الشركة.

Kaspersky Security Center Operator

المستخدم الذي يقوم بمراقبة الحالة وتشغيل نظام الحماية المدار بواسطة Kaspersky Security Center.

Kaspersky Security Center Web Server

مكون Kaspersky Security Center المثبت معًا مع خادم الإدارة. تم تصميم خادم الويب لنقل حزم التثبيت المستقلة وملفات تعريف iOS MDM وملفات من المجلد المشترك، عبر أحد الشبكات.

(KSN) Kaspersky Security Network

بنية تحتية للخدمات السحابية التي توفر الوصول إلى قاعدة بيانات Kaspersky التي تحتوي على معلومات محدثة باستمرار حول سمعة الملفات وموارد الويب والبرامج. ويضمن استخدام Kaspersky Security Network الحصول على استجابات أسرع للتهديدات من قِبل تطبيقات Kaspersky، ويحسن من أداء بعض مكونات الحماية، ويقلل أيضًا من احتمالية ظهور حالات إيجابية زائفة.

(LWNGT) Lightweight Nagent

بروتوكول للتفاعل مع Kaspersky Endpoint Security على الأجهزة المحمولة. يعمل LWNGT (المعروف أيضًا باسم بروتوكول Mobile) كعميل شبكة دون تثبيت عميل الشبكة على الأجهزة المحمولة فعليًا.

SSL

بروتوكول تشفير البيانات المستخدمة في الإنترنت والشبكات المحلية. يتم استخدام طبقة مآخذ توصيل آمنة (SSL) في تطبيقات الويب لإنشاء اتصال آمن بين العميل والخادم.

أداة التحقق من سلامة نظام Kaspersky Security Center (SHV)

تم تصميم مكون Kaspersky Security Center للتحقق من إمكانية تشغيل نظام التشغيل في حالة التشغيل المتزامن لـ Kaspersky Security Center وNAP Microsoft.

إعدادات البرنامج

إعدادات التطبيق الشائعة لكافة أنواع المهام والتي تحكم بمجمل عمليات التطبيق، مثل: إعدادات أداء التطبيق وإعدادات التقارير وإعدادات النسخ الاحتياطي.

إعدادات المهمة

إعدادات التطبيق الخاصة بكل نوع من أنواع المهام.

استعادة بيانات خادم الإدارة

استعادة بيانات خادم الإدارة من المعلومات المحفوظة في النسخ الاحتياطي باستخدام الأداة النسخ الاحتياطي. تستطيع الأداة استعادة:

- قاعدة بيانات خادم الإدارة (السياسات والمهام وإعدادات التطبيق والأحداث المحفوظة على خادم الإدارة)
- معلومات تكوين عن بنية مجموعات الإدارة والأجهزة العميلة
- مستودع ملفات التثبيت للتثبيت البعيد للتطبيقات (محتوى المجلدات: الحزم وإزالة تثبيت التحديثات).
- شهادة خادم الإدارة

اكتشاف السحابة

يعد Cloud Discovery أحد مكونات حل Cloud Access Security Broker (CASB) الذي يحمي البنية التحتية السحابية للمؤسسة. تتولى Cloud Discovery إدارة وصول المستخدم إلى الخدمات السحابية. وتتضمن الخدمات السحابية، على سبيل المثال، Microsoft Teams وSalesforce وMicrosoft Office 365. يتم تجميع الخدمات السحابية في فئات، على سبيل المثال، تبادل البيانات والمراسلة والبريد الإلكتروني.

الأجهزة المدارة

أجهزة شبكة الشركة المضمنة في مجموعة إدارة.

الإدارة المباشرة للتطبيق

إدارة التطبيق من خلال واجهة محلية.

الإدارة المركزية للتطبيق

إدارة عن بُعد للتطبيق باستخدام خدمات الإدارة المتوفرة في Kaspersky Security Center.

الاستعادة

تغيير موقع الكائن الأصلي من العزل أو النسخ الاحتياطي إلى المجلد الأصلي الخاص به حيث تم تخزين الكائن قبل عزله أو تنظيفه أو حذفه أو نقله إلى مجلد يحدده المستخدم.

التثبيت الإجباري

طريقة للتثبيت عن بُعد لتطبيقات Kaspersky تسمح لك بتثبيت البرامج على أجهزة عميلة محددة. للحصول على تثبيت إجباري ناجح، يجب أن يكون لدى الحساب المستخدم للمهمة حقوق كافية لبدء التطبيقات عن بُعد على الأجهزة العميلة. ننصح بهذه الطريقة لتثبيت التطبيقات على الأجهزة التي تعمل بنظام تشغيل Microsoft Windows والتي تدعم هذه الوظيفة.

التثبيت المحلي

تثبيت تطبيق أمن على جهاز على شبكة الشركة الذي يفترض بدء تشغيل التثبيت اليدوي من حزمة توزيع تطبيق الأمان أو بدء التشغيل اليدوي لحزمة تثبيت منشورة كان قد تم تنزيلها مسبقًا على الجهاز.

التثبيت اليدوي

تثبيت تطبيق أمن على جهاز في شبكة الشركة من حزمة التثبيت. يتطلب التثبيت اليدوي مشاركة مسؤول أو متخصص تقنية معلومات آخر. ويتم إجراء التثبيت اليدوي عادة إذا تم إجراء التثبيت عن بُعد مع وجود خطأ.

التثبيت عن بُعد

تثبيت تطبيقات Kaspersky عن طريق استخدام الخدمات المقدمة بواسطة Kaspersky Security Center.

التحديث المتوفر

مجموعة من تحديثات الوحدات النمطية لتطبيق Kaspersky، تتضمن تحديثات هامة تراكمت على مدى فترة زمنية معينة وتتغير إلى البنية الهندسية للتطبيق.

التطبيق غير متوافق

تطبيق مضاد للفيروسات تابع لمطور من جهة خارجية أو أحد تطبيقات Kaspersky الذي لا يدعم الإدارة من خلال Kaspersky Security Center.

الثغرات الأمنية

خطأ في نظام التشغيل أو تطبيق مُستخدم من قبل مطورين محتالين لاختراق نظام التشغيل أو التطبيق وانتهاك سيادته. يؤدي وجود عدد كبير من الثغرات الأمنية في نظام التشغيل إلى عدم إمكانية الاعتماد عليه، نظرًا لأن الفيروسات التي اخترقت نظام التشغيل ربما تُحدث أعطالاً في النظام نفسه وفي التطبيقات المثبتة.

الحماية ضد فيروسات الشبكة

مجموعة من الإجراءات الفنية والمؤسسية التي تقلل من خطر السماح للفيروسات والبرامج الخبيثة من اختراق شبكة المؤسسة مما يمنع هجمات الشبكة والتصيد الاحتيالي وتهديدات أخرى. يزداد أمن الشبكة عندما تستخدم تطبيقات وخدمات الأمن وعندما تُطبق وتلتزم بسياسة أمن بيانات الشركة.

الشهادة المشتركة

شهادة تهدف إلى تحديد جهاز محمول المستخدم

المهمة

يتم تنفيذ الوظائف التي يتم إجراؤها بواسطة تطبيق Kaspersky كمهام، مثل: حماية الملفات في الوقت الحقيقي، والفحص الكامل لجهاز الكمبيوتر، وتحديث قاعدة البيانات.

الهوية وإدارة الوصول (IAM)

خدمة AWS التي تمكن إدارة وصول المستخدم لخدمات وموارد AWS الأخرى.

الوعي بموقع الشبكة (NLA)

خدمة Windows تساعد نظام التشغيل على تحديد الشبكة الحالية. يستشعر الوعي بموقع الشبكة (NLA) التغيرات في الشبكة ويعدل تكوين الأمان للجهاز.

انتشار الفيروس

سلسلة من المحاولات المتعمدة لإصابة الجهاز بالفيروس.

بوابة الاتصال

بوابة الاتصال هي عميل شبكة يعمل في وضع خاص. تقبل بوابة الاتصال الاتصالات من عملاء الشبكة الآخرين وتقوم بنقلها إلى خادم الإدارة من خلال اتصالها الخاص بالخادم. على عكس عميل الشبكة العادي، تنتظر بوابة الاتصال الاتصالات من خادم الإدارة بدلاً من إنشاء اتصالات بخادم الإدارة.

بيئة السحابة

يتم دمج الأجهزة الظاهرية التي تعتمد على نظام سحابة أساسي في شبكات.

تحديث

تمت استعادة إجراء استبدال أو إضافة ملفات جديدة (قواعد بيانات أو وحدات نمطية للتطبيق) من خوادم تحديث Kaspersky.

ترقية Kaspersky Security Center

إجراء تثبيت إصدار أحدث من Kaspersky Security Center على جهاز تم تثبيت إصدار سابق من هذا التطبيق عليه.

جهاز iOS MDM

جهاز محمول متصل بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM باستخدام البرتوكول iOS MDM. يمكن توصيل الأجهزة التي تعمل بنظام تشغيل iOS وإدارتها بواسطة البرتوكول iOS MDM.

جهاز KES

جهاز محمول متصل بتطبيق Kaspersky Security Center Administration Server ومُدار عبر تطبيق Kaspersky Endpoint Security for Android.

جهاز حماية UEFI

جهاز مزود بحل أو تطبيق من Kaspersky لواجهة البرامج الثابتة الموحدة القابلة للتوسيع مدمج على مستوى BIOS. تضمن الحماية المتكاملة أمن الجهاز من الوقت الذي يبدأ فيه تشغيل النظام، ولكن تبدأ الحماية على الأجهزة دون البرامج المتكاملة في العمل بعد بدء تطبيق الأمن فقط.

حالة الحماية

حالة الحماية الحالية التي تعكس مستوى أمان جهاز الكمبيوتر.

حالة حماية الشبكة

حالة الحماية الحالية، التي تُحدد سلامة أجهزة شبكة الشركة. تتضمن حالة حماية الشبكة هذه العوامل مثل تطبيقات الأمان المُثبتة واستخدام مفاتيح الترخيص وعدد التهديدات المُكتشفة وأنواعها.

حزمة التثبيت

مجموعة من الملفات التي يتم إنشاؤها للتثبيت عن بُعد لأحد تطبيقات Kaspersky باستخدام نظام الإدارة عن بُعد لـ Kaspersky Security Center. تحتوي حزمة التثبيت على مجموعة إعدادات ضرورية لتثبيت التطبيق وتشغيله فورًا بعد التثبيت. الإعدادات المقابلة للإعدادات الافتراضية للتطبيق. يتم إنشاء حزمة التثبيت باستخدام ملفات بامتداد .kpd و.kud المضمنة في مجموعة توزيع التطبيق.

حقوق المسؤول

مستوى حقوق وامتيازات المستخدم المطلوبة لإدارة كائنات Exchange ضمن مؤسسة Exchange.

خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

مكون Kaspersky Security Center المثبت على جهاز عميل والسماح باتصال الأجهزة المحمولة iOS بخادم الإدارة وإدارة الأجهزة المحمولة iOS من خلال إخطارات الرسائل من Apple (APN).

خادم الإدارة

يعمل أحد مكونات Kaspersky Security Center على تخزين كل تطبيقات Kaspersky المثبتة على شبكة اتصال الشركة بشكل مركزي. كما يمكن استخدامه لإدارة تلك التطبيقات.

خادم الإدارة الافتراضي

مكون Kaspersky Security Center تم تصميمه لإدارة نظام حماية شبكة منظمة العميل.

يُعد خادم الإدارة الافتراضي حالة خاصة من خادم الإدارة الثانوي ويشتمل على القيود التالية مقارنةً بخادم الإدارة الفعلي:

- لا يمكن إنشاء خادم إدارة افتراضي إلا على خادم إدارة أساسي.
- يستخدم خادم الإدارة الافتراضي قاعدة بيانات خادم الإدارة الرئيسية في تشغيله. مهام النسخ الاحتياطي للبيانات واستعادتها، بالإضافة إلى مهام البحث عن التحديثات والتنزيل، غير مدعومة على خادم الإدارة الافتراضي.
- لا يدعم خادم الإدارة الافتراضي إنشاء خوادم إدارة ثانوية (بما في ذلك الخوادم الافتراضية).

خادم الإدارة الرئيسي

خادم الإدارة الرئيسي هو خادم الإدارة الذي تم تحديده أثناء تثبيت عميل الشبكة. يمكن استخدام خادم الإدارة الرئيسي في إعدادات ملفات تعريف اتصال عميل الشبكة.

خادم الجهاز المحمول

مكون Kaspersky Security Center الذي يوفر وصولاً إلى الأجهزة المحمولة ويسمح لك بإدارتها من خلال وحدة التحكم في الإدارة.

خدمات تحديث خادم Windows (WSUS)

تطبيق يُستخدم لتوزيع التحديثات لتطبيقات Microsoft على أجهزة كمبيوتر المستخدم في شبكة منظمة.

خطورة الحدث

خصائص الحدث الذي تمت مواجهته أثناء تشغيل تطبيق Kaspersky. توجد مستويات الخطورة التالية:

- حدث حرج
- خلل وظيفي
- تحذير
- معلومات

يمكن أن يكون للأحداث من نفس النوع مستويات خطورة مختلفة اعتمادًا على الموقف الذي وقع فيه الحدث.

خوادم تحديث Kaspersky

خوادم HTTP(S) في Kaspersky والتي تقوم من خلالها تطبيقات Kaspersky بتنزيل تحديثات لقواعد البيانات والوحدات النمطية للتطبيق.

دليل التقوية

تهدف مجموعة من التوصيات والميزات لتكوين Kaspersky Security Center ومكوناته إلى تقليل مخاطر الاختراق.

دور IAM

مجموعة من حقوق إجراء طلبات خدمات مستندة إلى AWS. تكون أدوار IAM غير مرتبطة بمستخدم أو مجموعة محددة؛ فهي توفر حقوق وصول بدون مفاتيح وصول AWS IAM. يمكنك تعيين دور IAM لمستخدمي IAM ومثيلات EC2 وتطبيقات أو خدمات مستندة إلى AWS.

سياسة

وتحدد السياسة إعدادات التطبيق وتدير القدرة على تكوين هذا التطبيق على أجهزة كمبيوتر ضمن مجموعة الإدارة. يجب إنشاء سياسة فردية لكل تطبيق. يمكنك إنشاء سياسات متعددة للتطبيقات المثبتة على أجهزة الكمبيوتر في كل مجموعة إدارية، ولكن يمكن تطبيق سياسة واحدة فقط على كل تطبيق في الوقت نفسه ضمن مجموعة الإدارة.

شهادة خادم الإدارة

الشهادة التي يستخدمها خادم الإدارة للأغراض التالية:

- مصادقة خادم الإدارة عند الاتصال بوحدة تحكم الإدارة المستندة إلى MMC أو Kaspersky Security Center Web Console
- تفاعل آمن بين خادم الإدارة ووكلاء الشبكة على الأجهزة المدارة.
- مصادقة خوادم الإدارة عند توصيل خادم إدارة أساسي بخادم إدارة ثانوي

يتم إنشاء الشهادة تلقائيًا عند تثبيت خادم الإدارة، ومن ثم يتم تخزينها على خادم الإدارة.

صورة جهاز Amazon (AMI)

يحتوي القالب على تكوين البرامج الضروري لتشغيل الجهاز الظاهري. يمكن إنشاء العديد من المثيلات بناءً على AMI واحدة.

عتبة نشاط الفيروس

الحد الأقصى المسموح به لعدد الأحداث من نوع محدد خلال فترة زمنية محددة؛ وعندما يتم تجاوز هذا العدد، يفسر هذا الأمر على أنه زيادة في نشاط الفيروس وكتهديد بانتشار الفيروس. تعتبر هذه الميزة هامة أثناء فترات انتشار الفيروسات حيث أنها تعمل على تمكين المسؤولين من الاستجابة السريعة لتهديدات هجوم الفيروسات.

عميل الشبكة

مكون Kaspersky Security Center الذي يُمكن التفاعل بين خادم الإدارة وتطبيقات Kaspersky التي يتم تثبيتها على عقدة شبكة معينة (محطة عمل أو خادم). يُعد هذا المكون مشتركًا بين جميع تطبيقات الشركة لـ Microsoft® Windows®. تتوفر إصدارات منفصلة من عميل الشبكة لتطبيقات Kaspersky التي تم تطويرها لأنظمة Unix-like OS وmacOS.

عميل خادم الإدارة (الجهاز العميل)

جهاز أو خادم أو محطة عمل يتم عليه تثبيت عميل الشبكة وتشغيل تطبيقات Kaspersky المُدارة.

فترة الترخيص

الفترة الزمنية التي يمكنك خلالها الوصول إلى ميزات التطبيق وحقوق استخدام خدمات إضافية. وتعتمد الخدمات التي يمكنك استخدامها على نوع الترخيص.

قواعد بيانات مكافحة الفيروسات

قواعد البيانات التي تحتوي على معلومات حول التهديدات الأمنية التي تهدد الجهاز والمعروفة لـ Kaspersky وقت إصدار قواعد بيانات مكافحة الفيروسات. تسمح الإدخالات في قواعد بيانات مكافحة الفيروسات باكتشاف الرمز الضار في الكائنات التي تم فحصها. يتم إنشاء قواعد بيانات مكافحة الفيروسات بواسطة أخصائيي Kaspersky ويتم تحديثها كل ساعة.

مالك الجهاز

مالك الجهاز هو مستخدم يمكن للمسؤول الاتصال به عند الحاجة إلى إجراء عمليات محددة على الجهاز.

متجر التطبيقات

مكون Kaspersky Security Center. يُستخدم متجر التطبيقات لتثبيت التطبيقات على الأجهزة التي تعمل بنظام Android والمملوكة بواسطة المستخدم. يتيح لك متجر التطبيقات نشر ملفات APK الخاصة بالتطبيقات وروابط التطبيقات في Google Play.

مثيل Amazon EC2

تم إنشاء جهاز ظاهري بناءً على صورة AMI باستخدام Amazon Web Services.

مجال البث

مساحة منطقية لشبكة تتمكن فيها كل العقد من تبادل البيانات باستخدام قناة بث على مستوى OSI (النموذج المرجعي الأساسي لترابط النظم المفتوحة).

مجلد النسخ الاحتياطي

مجلد خاص لتخزين نُسخ بيانات خادم الإدارة التي تم إنشاؤها باستخدام الأداة النسخ الاحتياطي.

مجموعة الإدارة

مجموعة من الأجهزة التي تم تجميعها بحسب الوظيفة وبحسب تطبيقات Kaspersky المثبتة. أجهزة تم تجميعها ككيان فردي لسهولة الإدارة. يمكن أن تتضمن المجموعة مجموعات أخرى. يمكن إنشاء سياسات جماعية ومهام جماعية لكل تطبيق يتم تثبيته في مجموعة.

مجموعة التطبيقات المرخصة

مجموعة من التطبيقات التي تم إنشاؤها على أساس معايير محددة بواسطة المسؤول (على سبيل المثال بواسطة البائع) حيث يتم الاحتفاظ بإحصاءات عمليات التثبيت على الأجهزة العميلة لها.

محطة عمل المسؤول

جهاز مثبت عليه وحدة تحكم الإدارة أو تستخدمه لفتح Kaspersky Security Center Web Console. يقدم هذا المكون واجهة إدارة Kaspersky Security Center.

يتم استخدام محطة عمل المسؤول لتكوين وإدارة جهة خادم Kaspersky Security Center. باستخدام محطة عمل المسؤول، يقوم المسؤول بتأسيس وإدارة نظام حماية مركزي ضد الفيروسات لشبكة اتصال محلية (LAN) بشركة إلى تطبيقات Kaspersky.

مسؤول Kaspersky Security Center

الشخص المسؤول عن إدارة عمليات التطبيق من خلال نظام Kaspersky Security Center للإدارة المركزية عن بُعد.

مسؤول العميل

عضو فريق بمنظمة عميلة مسؤول عن مراقبة حالة الحماية ضد الفيروسات.

مسؤول موفر الخدمة

عضو فريق في موفر خدمة الحماية ضد الفيروسات. يقوم هذا المسؤول بوظائف التثبيت والصيانة لأنظمة الحماية ضد الفيروسات بناءً على منتجات الحماية ضد الفيروسات من Kaspersky وكذلك تقديم الدعم الفني للعملاء.

مستخدم IAM

مستخدم خدمات AWS. قد يملك مستخدم IAM الحقوق التي تمكنه من إجراء استقصاء قطاع السحابة.

مستخدمين داخليين

تُستخدم حسابات المستخدمين الداخليين للعمل مع خوادم الإدارة الافتراضية. يمنح Kaspersky Security Center حقوق المستخدمين الفعليين للمستخدمين الداخليين للتطبيق.

يتم إنشاء واستخدام حسابات المستخدمين الداخليين فقط ضمن Kaspersky Security Center. لا يتم نقل أي بيانات عن المستخدمين الداخليين إلى نظام التشغيل. Kaspersky Security Center يصادق المستخدمين الداخليين.

مستودع الأحداث

جزء من قاعدة بيانات خادم الإدارة المخصصة لتخزين معلومات حول الأحداث التي تظهر في Kaspersky Security Center.

مستوى أهمية التصحيح

سمة التصحيح يوجد خمسة مستويات لأهمية تصحيحات Microsoft وتصحيحات الجهات الخارجية:

- حرج
- مرتفع
- متوسط
- منخفض
- غير معروف

يتم تحديد مستوى أهمية أي تصحيح لجهة خارجية أو أحد تصحيحات Microsoft بحسب مستوى الخطورة الأقل تفضيلًا بين الثغرات الأمنية التي ينبغي للتصحيحات إصلاحها.

مفتاح الترخيص الإضافي (أو الاحتياطي)

مفتاح يُصادق على حق استخدام التطبيق لكن لا يتم استخدامه حاليًا.

مفتاح مفعل

مفتاح الترخيص الذي يستخدمه التطبيق حاليًا.

مفتاح وصول AWS IAM

تركيبة تتكون من معرف مفتاح (يبدو وكأنه "AKIAIOSFODNN7EXAMPLE") ومفتاح سري (يبدو وكأنه "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). ينتمي هذا الاقتران إلى مستخدم IAM ويستخدم للحصول وصول إلى خدمات AWS.

مكون الإدارة الإضافي

مكون متخصص يوفر الواجهة لإدارة التطبيق من خلال وحدة تحكم الإدارة. كل تطبيق به مكون إضافي خاص. وهو موجود في جميع تطبيقات Kaspersky التي يمكن إدارتها باستخدام Kaspersky Security Center.

ملف المفتاح

ملف بتنسيق xxxxxxxx.key يُسهل من استخدام تطبيق Kaspersky ضمن ترخيص تجريبي أو تجاري.

ملف تعريف iOS MDM

مجموعة من الإعدادات لاتصال الأجهزة المحمولة iOS بخادم الإدارة. يقوم المستخدم بتثبيت ملف تعريف iOS MDM بجهاز محمول، ثم يتم توصيل هذا الجهاز بخادم الإدارة.

ملف تعريف التزويد

مجموعة من الإعدادات لتشغيل التطبيقات على الأجهزة المحمولة iOS. يحتوي ملف التزويد على معلومات حول الترخيص، فهو مرتبط بتطبيق معين.

ملف تعريف التكوين

سياسة تحتوي على مجموعة من الإعدادات والقيود للجهاز المحمول iOS MDM.

منطقة الأجهزة الموصلة مباشرة بالإنترنت (DMZ)

منطقة الأجهزة الموصولة مباشرة بالإنترنت هي جزء من شبكة محلية تحتوي على خوادم التي تستجيب إلى الطلبات من شبكة الويب العالمية. لضمان أمن الشبكة المحلية للمنظمة، فإن الوصول إلى شبكة الاتصال المحلية (LAN) من منطقة الأجهزة الموصلة مباشرة بالإنترنت محمي بجدار حماية.

مهمة جماعية

مهمة محددة لمجموعة إدارة ويتم تنفيذها على جميع الأجهزة العميلة المضمنة في مجموعة الإدارة هذه.

مهمة لأجهزة محددة

مهمة معينة لمجموعة من الأجهزة العميلة من مجموعات الإدارة الحاكمة ويتم تنفيذها على هذه الأجهزة.

مهمة محلية

مهمة محددة وجاري تشغيلها على جهاز كمبيوتر عميل واحد.

موفر خدمة الحماية ضد الفيروسات

مؤسسة توفر خدمات الحماية ضد الفيروسات لمنظمة عميلة استنادًا إلى حلول Kaspersky.

نسخ احتياطي لبيانات خادم الإدارة

نسخ بيانات خادم الإدارة لعمل نسخة احتياطية وللاسترداد اللاحق بواسطة أداة النسخ الاحتياطي. تستطيع الأداة حفظ:

- قاعدة بيانات خادم الإدارة (السياسات والمهام وإعدادات التطبيق والأحداث المحفوظة على خادم الإدارة)
- معلومات تكوين عن بنية مجموعات الإدارة والأجهزة العميلة
- مستودع ملفات التثبيت للتثبيت البعيد للتطبيقات (محتوى المجلدات: الحزم وإزالة تثبيت التحديثات).
- شهادة خادم الإدارة

نقطة توزيع

جهاز كمبيوتر مثبت عليه عميل الشبكة ويتم استخدامه لتوزيع التحديث، وتثبيت التطبيقات عن بُعد، والحصول على المعلومات حول أجهزة الكمبيوتر في مجموعة إدارة و/أو مجال البث. تم تصميم نقاط التوزيع لتقليل التحميل على خادم الإدارة أثناء توزيع التحديثات ولتحسين حركة الشبكة. يمكن تعيين نقاط التوزيع تلقائيًا، بواسطة خادم الإدارة أو يدويًا أو بواسطة المسؤول. كانت نقطة التوزيع تعرف فيما سبق بوكيل التحديث.

هجوم الوسيط

الوسيط. هجوم على البنية التحتية لتكنولوجيا المعلومات لمؤسسة يقرصن فيه أحد المتسللين رابط الاتصال بين نقطتي وصول ويرحله ويُعدّل الاتصال بين نقاط الوصول هذه إذا لزم الأمر.

وحدة التحكم الخاصة بإدارة AWS

واجهة الويب لعرض موارد AWS وإدارتها. تتوفر وحدة التحكم الخاصة بإدارة AWS على الويب على الموقع الإلكتروني https://aws.amazon.com/console/.

وحدة تحكم الإدارة

أحد مكونات Kaspersky Security Center المستندة إلى Windows (وتسمى أيضًا وحدة تحكم الإدارة المستندة إلى MMC). يوفر هذا المكون واجهة مستخدم للخدمات الإدارية لخادم الإدارة وعميل الشبكة.

وكيل المصادقة

واجهة تسمح بإكمال عملية المصادقة للوصول إلى محركات الأقراص الثابتة المشفرة وتمهيد نظام التشغيل بعد تشفير محرك القرص الثابت القابل للتشغيل.

معلومات حول التعليمات البرمجية الخاصة بطرف ثالث

معلومات حول التعليمات البرمجية للجهات الخارجية في الملف legal_notices.txt، في المجلد تثبيت التطبيق.

إشعارات العلامة التجارية

العلامات التجارية وعلامات الخدمة المسجلة تعود ملكيتها لمالكيها المعنيين.

Adobe وAcrobat وFlash و Shockwave وPostScript هم علامات تجارية مسجلة أو علامات تجارية لشركة Adobe في الولايات المتحدة و/أو بلدان أخرى.

إن AMD وAMD64 هي علامات تجارية أو علامات تجارية مسجلة لشركة Advanced Micro Devices, Inc.

تعد Amazon و Amazon Web Services و AWS و Amazon EC2 و AWS Marketplace علامات تجارية لشركة Amazon.com، Inc. أو الشركات التابعة لها.

Apache هي إما علامة تجارية مسجلة أو علامة تجارية لشركة Apache Software Foundation في الولايات المتحدة و/أو بلدان أخرى.

Apple وAirPlay وAirDrop وAirPrint وApp Store وApple Configurator وAppleScript وFaceTime وFileVault وiBook وiBooks وiCloud وiPad وiPhone وiTunes وLeopard وmacOS وMac وMac OS وOS X وSafari وSnow Leopard وTiger وQuickTime وTouch ID علامات تجارية مملوكة لشركة Apple Inc.

Arm علامة تجارية مسجلة لشركة Arm Limited (أو الشركات التابعة لها) في الولايات المتحدة و/أو في أماكن آخر.

كلمة Bluetooth وعلامتها وشعاراتها تعتبر مملوكة لشركة Bluetooth SIG, Inc.

Ubuntu وLTS علامتان تجاريتان مسجلتان لشركة Canonical Ltd.

Cisco Systems وCisco وCisco Jabber وIOS علامات تجارية مسجلة أو علامات تجارية لشركة Cisco Systems, Inc. و/أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى محددة.

Citrix وXenServer إما علامتان تجاريتان مسجلتان أو علامتان تجاريتان لشركة Cloud Software Group, Inc. و/أو الشركات التابعة لها في الولايات المتحدة و/أو بلدان أخرى.

Corel هي علامة تجارية أو علامة تجارية مسجلة لصالح شركة Corel و/أو شركاتها التابعة في كندا، و/أو الولايات المتحدة و/أو بلدان أخرى.

تعد Cloudflare وشعار Cloudflare و Cloudflare Workers علامات تجارية و/أو علامات تجارية مسجلة لشركة Cloudflare، Inc. في الولايات المتحدة وولايات قضائية أخرى.

Dropbox هي علامة تجارية مملوكة لشركة Dropbox، Inc.

Radmin هي علامة تجارية مسجلة لشركة Famatech.

Firebird هي علامة تجارية مسجلة لمؤسسة Firebird Foundation.

Foxit هي علامة تجارية مسجلة لشركة Foxit Corporation.

إن FreeBSD علامة تجارية مسجلة لمؤسسة FreeBSD foundation.

Google وAndroid وChrome وChromium وDalvik وFirebase وGoogle Chrome وGoogle Earth وGoogle Play وGoogle Maps وHangouts وGoogle Public DNS وYouTube علامات تجارية لشركة Google LLC.

تُعد EulerOS و FusionCompute و FusionSphere علامات تجارية لشركة Huawei Technologies Co.، Ltd.

Intel وCore وXeon علامات تجارية لشركة Intel Corporation أو الشركات التابعة لها.

إن IBM وQRadar علامات تجارية تابعة لشركة International Business Machines Corporation، مسجلة في العديد من البلدان حول العالم.

وعلامة Node.js هي علامة تجارية تابعة لشركة Joyent, Inc.

شركة Linux هي علامة تجارية مسجلة لصالح لشركة Linus Torvalds في الولايات المتحدة الأمريكية وبلدان أخرى.

تعد Logitech إما علامة تجارية مسجلة أو علامة تجارية لشركة Logitech في الولايات المتحدة و/أو البلدان الأخرى.

تُعد Microsoft وActive Directory وActiveSync وBitLocker وExcel وForefront وInternet Explorer وInfoPath وHyper-V وMicrosoft Edge وMultiPoint وMS-DOS و365 Office وPowerShell وPowerPoint وSharePoint وSQL Server وOneNote وOutlook وSkype وTahoma وVisio وWin32 وWindows وWindows PowerShell وWindows Media وWindows Mobile وWindows Server وWindows Phone وWindows Vista وWindows Azure علامات تجارية مسجلة لمجموعة شركات Microsoft.

تعد CVE علامة تجارية مسجلة لشركة MITER Corporation.

تُعد Mozilla و Firefox و Thunderbird علامات تجارية مملوكة لمؤسسة Mozilla Foundation في الولايات المتحدة وبلدان أخرى.

تُعد Novell علامة تجارية مسجلة لشركة Novell Enterprises Inc. في الولايات المتحدة الأمريكية وبلدان أخرى.

NetWare علامة تجارية مسجلة لشركة Novell Inc. في الولايات المتحدة الأمريكية وبلدان أخرى.

OpenVPN علامة تجارية مسجلة لشركة OpenVPN, Inc.

OpenSSL علامة تجارية مملوكة لمؤسسة OpenSSL Software Foundation.

إن Oracle وJava وJavaScript وTouchDown علامات تجارية مسجلة لشركة Oracle و/أو شركاتها التابعة.

Parallels وشعار Parallels وCoherence علامات تجارية أو علامات تجارية مسجلة لشركة Parallels International GmbH.

تُعد Chef علامة تجارية أو علامة تجارية مسجلة لشركة Progress Software Corporation و/أو إحدى الشركات التابعة لها أو الشركات التابعة لها في الولايات المتحدة و/أو البلدان الأخرى.

تُعد Puppet علامة تجارية أو علامة تجارية مسجلة لشركة Puppet, Inc.

تُعد Python علامة تجارية أو ماركة مسجلة لشركة Python Software Foundation.

Red Hat وFedora وRed Hat Enterprise Linux علامات تجارية أو علامات تجارية مسجلة لشركة Red Hat, Inc. أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

Ansible علامة تجارية مسجلة لشركة Red Hat Inc. في الولايات المتحدة وبلدان أخرى.

CentOS علامة تجارية أو علامة تجارية مسجلة لشركة Red Hat, Inc. و/أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

إن BlackBerry مملوكة لشركة Research In Motion Limited ومسجلة في الولايات المتحدة ويمكن أن تكون معلقة أو مسجلة في بلدان أخرى.

Rocky Linux علامة تجارية مسجلة لشركة Rocky Enterprise Software Foundation.

SAMSUNG علامة تجارية لشركة SAMSUNG في الولايات المتحدة أو بلدان أخرى.

Debian هي علامة تجارية مسجلة لشركة Software in the Public Interest, Inc.

SPL وSplunk هي علامات تجارية مسجلة لشركة Splunk, Inc. في الولايات المتحدة الأمريكية وبلدان أخرى.

SUSE هي علامة تجارية مسجلة لشركة SUSE LLC في الولايات المتحدة الأمريكية وبلدان أخرى.

Symbian هي علامة تجارية مملوكة لشركة Symbian Foundation Ltd.

إن OpenAPI علامة تجارية لمؤسسة Linux Foundation.

تُعد UNIX علامة تجارية مسجلة في الولايات المتحدة الأمريكية وبلدان أخرى، ومرخصة بشكل حصري من خلال شركة X/Open المحدودة.

إن Zabbix علامة تجارية مسجلة لصالح Zabbix SIA.

المشكلات المعروفة

Kaspersky Security Center Web Console يحتوي على عدد من القيود التي ليست حرجة لتشغيل التطبيق:

- 9838414: قد تظل عملية تثبيت Network Agent for Microsoft Windows على معالجات Arm باستخدام حزمة تثبيت مستقلة عالقة عند خطوة **يجري فحص الاتصال بخادم الإدارة**، على الرغم من اتصال الجهاز بنجاح بخادم الإدارة واكتمال التثبيت. وإذا ظلت عملية التثبيت عالقة عند هذه الخطوة، يمكنك إغلاق نافذة التثبيت. تم تثبيت Network Agent for Microsoft على معالجات Arm بالفعل.

- 9978211: خيار **Use Network Agent as a connection gateway in DMZ** غير مدعوم في نظام التشغيل Microsoft Windows على معالجات Arm.

- لا يتم نشر التغييرات التي يتم إجراؤها على جدول المهام على الأجهزة المُدارة إذا كان الجدول يستخدم الإعداد **By days of week**. وإذا كنت بحاجة إلى تغيير الجدول، فاحذف المهمة الحالية وأنشئ مهمة جديدة بالإعدادات المحدثة.

- لا تتوفر معلومات عن مكونات التطبيق المدارة إذا تم تثبيت عميل الشبكة على نظام التشغيل Microsoft Windows XP.

- يعرض وحدة التحكم القسم الفرعي **Alerts** في قسم **Monitoring & reporting** في القائمة الرئيسية فقط إذا أضفت مفتاح ترخيص لحل EDR Optimum إلى مستودع خادم الإدارة عن طريق إدخال رمز التفعيل.

- لضمان قوة التشفير، يجب توقيع شهادة خادم الإدارة باستخدام SHA-2 وأن يكون الحد الأدنى لطول المفتاح 2048. إذا كنت بحاجة إلى إعادة إصدار الشهادة، فراجع قاعدة معارف Kaspersky Security Center.

- إذا أنشأت مهمة باستخدام **إعدادات الجدولة كل N من الأيام** وحسب أيام الأسبوع في Kaspersky Security Center 15.1 Web Console، ثم فتحت المهمة في الإصدارات السابقة من Kaspersky Security Center Web Console أو وحدة تحكم الإدارة في Kaspersky Security Center (على سبيل المثال، عندما يتم تطبيق المهمة أيضًا على خوادم الإدارة الثانوية التي يمكن أن تكون مستندة إلى Linux وWindows)، قد يتم عرض إعدادات الجدولة بشكل غير صحيح، أو قد يحدث خطأ.

- عند تكوين التصدير إلى أنظمة SIEM في Kaspersky Security Center Web Console، وتحديد بروتوكول UDP، يتم إرجاع خطأ بعد النقر على الزر **Check connection**، لأن بروتوكول UDP لا ينشئ اتصالاً ولا يمكن ضمان تسليم البيانات.

- عند تشغيل مهمة لإزالة عميل الشبكة من جهاز يعتمد على بنية Arm وتشغيل Astra Linux Special Edition RUSB.10015-01 (التحديث التشغيلي 1.7)، تتم إزالة عميل الشبكة بنجاح، لكن تم تجميد حالة المهمة للتقدم الحالي في قائمة المهام.

- لا تزال نافذة الخصائص الخاصة بسياسة Kaspersky Device Management for iOS تحتوي على قسم **إعدادات أجهزة EAS**، على الرغم من أن Exchange ActiveSync لم يعد مدعومًا.

- يفشل الاتصال بشبكة KSN عبر HTTPS إذا تم تثبيت Kaspersky Security Center على جهاز به رموز سيريلية في اسم الجهاز وتم تمكين عميل KSN على خادم الإدارة.

- عند محاولة تغيير خصائص حساب مستخدم مع تمكين الخيار **Request authentication to check for permission to modify user accounts**، ثم النقر فوق **Cancel** في النافذة **Account protection**، يحدث خطأ غير متوقع.

- إذا قمت بتغيير الوقت أو المنطقة الزمنية على جهازك، فيجب عليك إعادة تشغيل خدمة Kaspersky Security Center Web Console.

- إذا تم استخدام خادم وكيل على الجهاز، وتم تعيين متغيرات بيئة الخادم الوكيل، فقد يتوقف برنامج تثبيت Kaspersky Security Center Web Console بشكل تام.

- عندما تقوم باستيراد تنزيل التحديثات إلى مستودعات نقاط التوزيع أو مهمة التحقق من صحة التحديث، يتم تمكين الخيار **تحديد الأجهزة التي سيتم تعيين المهمة لها**. ولا يمكن تعيين هذه المهام لتحديد جهاز أو أجهزة معينة. إذا قمت بتعيين تنزيل التحديثات إلى مستودعات نقاط التوزيع أو مهمة التحقق من صحة التحديث لأجهزة معينة، فسيتم استيراد المهمة بشكل غير صحيح.

- إذا قمت بإجراء استقصاء Active Directory باستخدام نقطة توزيع Linux مُثبت عليها الإصدار 15 من عميل الشبكة، يمكنك استقصاء مجالات Active Directory فقط التي تحدد العنوان وبيانات اعتماد المستخدم لها. لا يتوفر استقصاء مجال Active Directory الحالي ومجال Active Directory الرئيسي.

- قد لا يتم العثور على الأجهزة العميلة بعد تشغيل استقصاء شبكة Windows.

- في معالج **إضافة خادم الإدارة الثانوي**، إذا قمت بتحديد حساب مع تمكين التحقق المكون من خطوتين للمصادقة على الخادم الثانوي المستقبلي، فسينتهي المعالج بخطأ. لحل هذه المشكلة، حدد حسابًا تم تعطيل التحقق من خطوتين له أو أنشئ التسلسل الهرمي من الخادم الثانوي المستقبلي.

- أثناء تسجيل الدخول إلى Kaspersky Security Center Web Console، إذا كنت تستخدم مصادقة المجال، وتحدد خادم إدارة افتراضي للاتصال به، ثم تقوم بتسجيل الخروج، ومحاولة تسجيل الدخول إلى مخدم الإدارة الأساسي، فسيتصل Kaspersky Security Center Web Console بخادم الإدارة الافتراضي. للاتصال بمخدم الإدارة الأساسي، أعد فتح المتصفح.

- استقصاء شبكة Quick/Full Windows يُنتج نتيجة فارغة.

- في حالة تثبيت Kaspersky Security Center Web Console باستخدام إدارة الهوية والوصول، فمن ثم عليك تغيير خادم إدارة Kaspersky Security Center Web Console، ولن تحصل إدارة الهوية والوصول على معلومات بشأن خادم الإدارة الجديد.

- يرسل الجهاز المُدار الذي يحتوي على أكثر من محول شبكة واحد معلومات خادم الإدارة حول عنوان MAC لمحول الشبكة غير المستخدم للاتصال بخادم الإدارة.

- يفشل اختبار الاتصال بنظام SIEM عند تحديد تنسيق بيانات CEF.

- لا تعمل مصادقة NTLM لحسابات المستخدمين داخل مجموعة "المستخدمون المحميون".